An Adaptive Quantization Algorithm for Secret Key Generation using Radio Channel Measurements

Sana Tmar - Ben Hamida, Jean-Benoît Pierrot
CEA, LETI, MINATEC
17 rue des Martyrs,
38054 Grenoble, France
Email: [sana.ben-hamida, jean-benoit.pierrot]@cea.fr

Claude Castelluccia
INRIA Rhône-Alpes
655, Avenue de l´Europe, Montbonnot,
38334 Saint Ismier Cedex, France
Email: claude.castelluccia@inria.fr

***Abstract*—New approaches that generate secret keys from radio channel characteristics have been recently proposed. The security of these schemes usually relies on the reciprocity principle which states that the channel fluctuations can be a source of common randomness for two communicating peers and these fluctuations can't be measured by any eavesdropper. A validation of these properties for indoor environments is presented in this work. The shared keys are created by measuring the reciprocal channel features and converting this information to binary vectors using a quantization algorithm. This paper addresses the problem of quantization. It identifies an important weakness of existing key generation algorithms and it shows that the secret bits extraction has a significant impact on the robustness and security of these algorithms. A new adaptive quantization algorithm for secret key generation is presented. This method has the advantages to create sufficient long secret keys with a high key agreement ratio between authorized users without revealing information to the attacker. The new scheme is experimentally validated using Ultra Wide Band technology.**

Keywords: wireless sensor networks, physical layer, secret key generation, quantization, UWB

I. Introduction

Security protocols are generally based on cryptographic mechanisms to provide confidentiality, integrity and authentication. Therefore, a trusted third party must be developed to generate secret keys and such conditions are not suitable for wireless sensor networks. Hence, the need for new security schemes to establish secret keys at low cost are required.

A new approach, introduced in [11], uses physical layer features to derive secret keys. The security of these new schemes relies on the *reciprocity principle* that states that, in the absence of interferences and non-linear components, both the emitter and the receiver experience the same channel response (CR) [1]. This shared information can be used to generate a secret key. In addition, the channel fluctuations are intrinsically *spatially specific* in multipath radio environments. Due to the scatters effects, the waveforms travel differently from one location to another. As a result, an eavesdropper cannot obtain the similar channel response and thereafter will not be able to extract the shared secret key. This guarantees the secrecy of the generated key.

A signal-based key generation algorithms rely on several stages. First, each of the two parties must perform a channel estimation to obtain a signal that has the right properties (channel estimation phase). Secondly, this signal has to be converted into a binary vector, using a quantization algorithm (quantization phase). Finally, the two parties must agree on the same secret key (key agreement phase).

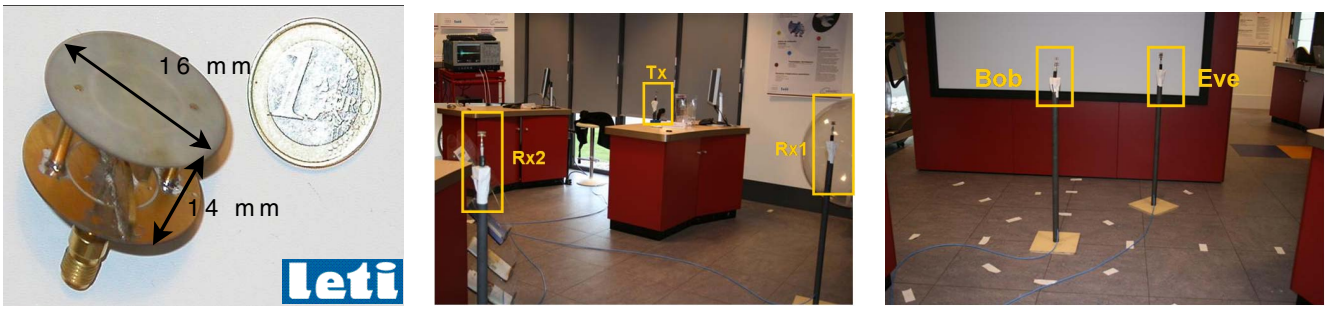
The contributions of this work are many-fold: First, the channel reciprocity and the spatial correlation principles using Ultra Wide Band channel measurements are verified. Second, the impact of quantization on the robustness of secret key scheme is evaluated. Third, a new extracting secret key algorithm based on an adaptive quantization is proposed. The performances of the solution are evaluated through experimentations. This paper is organized as follows: Section II summarizes some existing security methods based on physical layer. Section III outlines our set of measurements to verify the channel reciprocity and the spatial channel variations. Section IV exposes the impact of quantization on the secret key scheme. Section V describes our secret key generation and shows the evaluation of its performance, followed by a conclusion in the last section.

II. Related Work

In literature, several papers have been proposed for secret key generation using the physical layer features. A scheme for generating periodically secret keys based on deep fades has been proposed in [4]. This work requires frequent fluctuations on channel to create secret keys. So, when the channel is stationary and there are no deep fades, the emitter A and receiver B will observe temporal correlations on the generated keys which can be revealed by an attacker. Furthermore, the adversary can be active and generates artificial interferences to force one of the legitimate users to extract the secret key at a chosen moment. In [2], a secret key generation method is presented exploiting the reciprocity of Ultra Wide Band (UWB) channel. An approximation and upper bound on mutual information is found to define the maximum size of a shared key.

The paper [12], proposes a method suitable for OFDM systems. The secret keys are generated using the channel reciprocity and the time-variant frequency characteristics. In [5], it was shown that is possible to generate secret keys using the Bit Error Rates (BER) statistics. In [3], [7], [8], secret keys are generated exploiting the received signal strength indicator

978-1-4244-6273-5/09/$26.00 ©2009 IEEE



(a) (b) (c)

Fig. 1. The campaign of Measurements for indoor environment: (a) UWB Antenna. (b) Reciprocity measurement (Tx: transmitter, Rx: receiver) (c) Eavesdropping & spatial correlation measurements

(RSSI) profile. The channel fluctuations are created artificially by an electronic steerable parasitic antenna (ESPAR). In [6], the authors show that it is possible to extract secret keys based on the measurements of arrival time difference at both authorised users. However, this solution requires a specific antenna like in [3], [5], [8], [7] and an overhead bandwidth for the exchange phase to generate secret key. It is shown in [10], that the secret key agreement can be ensured when the transceivers use LDPC decoders to resolve the differences between the reciprocal channel estimations. The paper [9] proposes to use the CR as a common source between the legitimate sides of the wireless link. The channel statistics are used for the quantization process. However, like most papers, no security analyses have been provided to verify the possible channels correlation between the attacker and authorised users. In this paper, an adaptive quantization algorithm is proposed that allows creating large shared information based on the multipath distribution. In this solution no specific antenna is required and the security analyses is provided by a real eavesdropping experience.

III. Preliminary Experiences

A campaign of measurements was performed to validate the UWB (Ultra Wide Band) channel reciprocity and the spatial correlation properties. The time domain channel measurement test-bed is mainly based on a pulse step generator, a wideband real-time digital oscilloscope, a power amplifier at transmitting side, and two low noise amplifiers at receiving side (the receiver and the attacker). On both Tx and Rx sides the same kind of antenna is used which is characterized to be omnidirectional (see figure 1a). The frequency band is between 3-9 GHz. An important requirement for this experience is that the radio channel must be stationary so, the movement was minimized. For these experiences, a known probe signal $x(t)$ is sent from Alice A to Bob B and then the mobile B sends the same probe to A. Since the radio communications are half duplex, there is a latency time between the two transmissions. The channel must be stationary during the exchange stage. Each party detects and samples the received signal $y(t)$:

$$Alice : y_A(t) = (h_{BA} * x)(t) + n_A(t)$$

$$Bob : y_B(t) = (h_{AB} * x)(t) + n_B(t)$$

where $h_{AB}(t)$ and $h_{BA}(t)$ are the CR, $n_M(t)$ is a normal zero mean noise, $M \in \{A, B\}$ and '$*$' indicates the convolution operation. Since each transceiver knows $x(t)$, the transmitted probe signal, A and B can estimate the channel response h. This process gives A and B a noisy estimation of the CR:

$$\hat{h}_M(t) = h_M(t) + n_M(t)$$

where n_M is a normal zero mean noise, h_M is the CR received by A (resp. B) when B (resp. A) sends a probe signal. Various processes have been applied to the collected data to eliminate the noise and the RF cables effects.

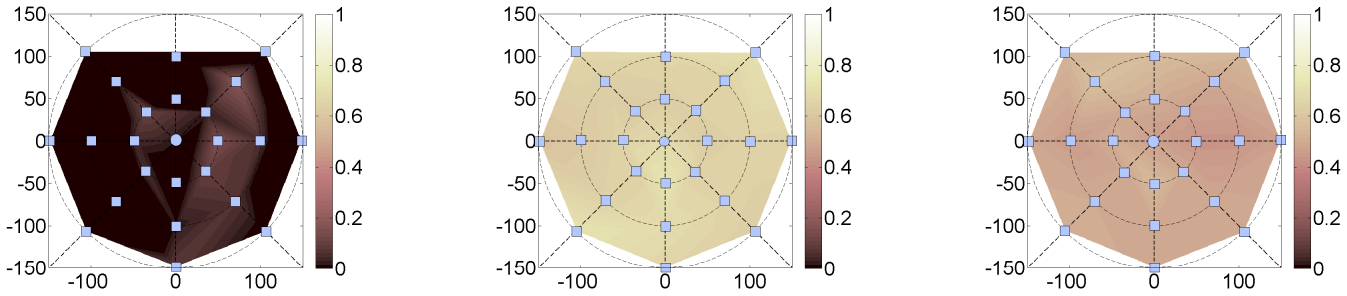
We use the correlation coefficient to show the likelihood relation between the experimental data. The correlation coefficient ρ_{XY} between two random variables X and Y with the expected values μ_X and μ_Y and the standard deviations σ_X and σ_Y is defined as follows:

$$\rho_{X,Y} = \frac{E((X - \mu_X)(Y - \mu_Y))}{\sigma_X \sigma_Y}$$

A. Reciprocity Validation

This test was evaluated to confirm the fact that the channel impulse response from A to B is similar to the channel impulse response from B to A during the channel coherence time: $h_{AB}(t) \equiv h_{BA}(t)$. Figure 1b shows the experimental environment for reciprocity test. As depicted in figure 1b, the distance between the source A (Tx) and the receiver B (Rx1) is more than 5m and an eavesdropper E (Rx2) is in the vicinity. The measurement was performed in one direction (from A to B) after that the antenna was switched so the channel information can be also collected in the reversed path (from B to A). Figure 3 shows the reciprocity measurement results. It is clear from the figure 3a that the signal received by B experiences the same fluctuations and strength as the signal received by A. These signals are highly correlated as shown in figure 3b. In fact the correlation coefficient (ρ_{AB}) is equal to 0.953. However, the signal received by E has a very little correlation with the signal received by A and B ($\rho_{AE} = 0$ and $\rho_{BE} = -0.024$).

978-1-4244-6273-5/09/$26.00 ©2009 IEEE



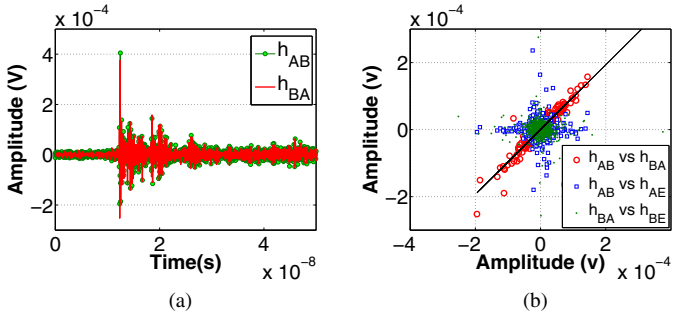
(a) (b) (c)

Fig. 2. The central point corresponds to the receiver, the cubic points are the attacker locations and the circles represent the distance (50cm, 1m and 150cm) (a) Spatial Correlation of the CIR (b) and (c) The key agreement ratio between Bob and Eve ((b)1^{st} method (c)2^{nd} method of quantization).

B. Spatial Correlation

This scenario was tested to validate the channel spatial variation, (i.e. that the CRs vary from location to another). In this experience, the attacker E moves around the receiver B which was kept stationary. As it is depicted in figure 1c, the attacker emplacements are controlled and tagged by several "indicators", the distance between the attacker and the receiver varies from 50cm to 1.50m. In total 23 impulse CRs corresponding to every location have been collected.

The correlation coefficients were defined to study the relation between different Bob and Eve's channel responses. The different correlation coefficients are shown in figure 2a. This cartography proves that the CR is independent from one location to another and therefore is intrinsically spatially specific. Some surfaces of the maps are less correlated (darker) than others due to the presence of many scatters near the attacker which consequently creates constructive or destructive information. We deduce that the received signal depends on clutters in the indoor environment, and therefore the shared information is dependant on the surrounding. So, the secret key generation based on physical layer would not work in a free-space environment.



(a) (b)

Fig. 3. Reciprocity measurement using UWB transceivers (a)Signal received by Alice (Tx) and Bob (Rx1) (b)Spatial channels correlation

IV. Studying the Impact of Quantization Phase

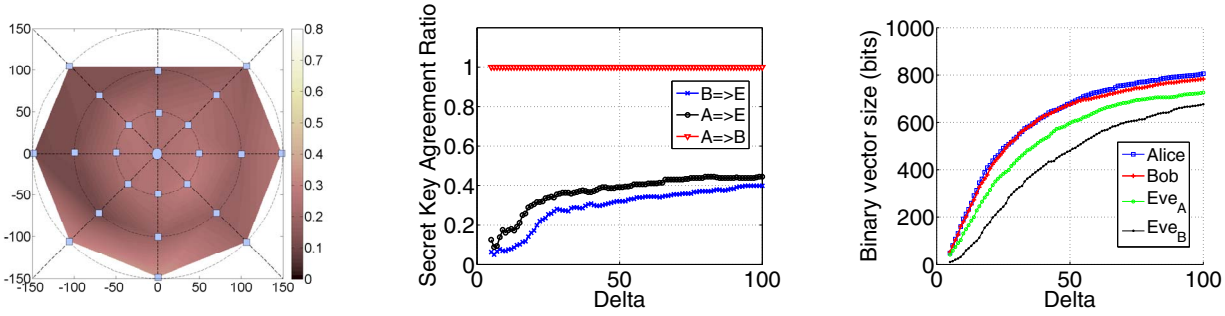
The quantization procedure is necessary to convert the channel estimations into bit vectors but using a fixed threshold can be critical for security. In this section, some existing binary conversion schemes is examined to show their impact on the secret key generation. These analyses use the data collected during the previous described experiences.

The first bits extraction is based on fixed threshold which is set by A and B like in [3], [6], [5]. The principle of this algorithm is as follows: A and B compare the estimated received signal to the shared threshold, if the amplitude of the i^{th} sample is below the threshold L the bit is set to 0 else it is set to 1. This principle was implemented and the results are shown in figure 2b. The key agreement ratio between the receiver B and the attacker E is very high despite that the CIRs are totally decorrelated. In some cases, the binary generated sequence is not really random. It is often composed of bursts of "1111..1" or "000...0". This is particularly true when the channel is not variable enough. Therefore, the key is not secret and an attacker can easily 'break' the secret key.

In order to benefit from the CIR variations, a "censoring" quantization was tested. This scheme uses 2 thresholds (L^+ and L^-) computed from the channel statistics like in [9]. These limits are equal to the mean of the channel estimation, i.e. $L^+ = mean(\hat{h})$ is the positive limit whereas $L^- = -mean(\hat{h})$ is the negative indicator. The receiver parses its channel estimation to construct the binary vector (BV) as follows: $BV(i) = \begin{cases} 1 & \text{if } \hat{h}_M[i] \geq L^+ \\ 0 & \text{if } \hat{h}_M[i] \leq L^- \end{cases}$ This method has been applied to CIR traces. As shown in figure 2c the agreement ratio between Bob and Eve has decreased but not enough to guarantee that the attacker will not derive the secret key.

We can conclude that an arbitrary choice of the quantization method affects the key agreement ratio for both legitimate users and the attacker. In addition, an interesting result was observed, that the use of channel statistics as indicator for binary extraction can be advantageous. In fact it reduces the attacker information and guarantees that Alice and Bob will have similar binary vectors. However, it is important to adapt this parameter to the received signal such as Alice and Bob are able to extract the secret key even if the signal observes an important number of interferences.

978-1-4244-6273-5/09/$26.00 ©2009 IEEE



(a) (b) (c)

Fig. 4. (a)Cartography of key agreement ratio between B and E (b)Length of binary vectors (c)Agreement ratio for Eve when using $\hat{h}_{AE}$ and $\hat{h}_{BE}$

V. An Adaptive Quantization Scheme

In this section, we describe a new adaptive quantization scheme to generate secret keys between two wireless nodes. First, we present our algorithm. Then we evaluate it using real experimental data.

A. Description

Let M be the user who wishes to create a secret key with another terminal which shares the same channel. We suppose that each node is able to estimate the channel using known signal probes. The length of the channel estimations $\hat{h}_M(t)$ can be different from a node to another but when we perform the correcting process the length of shared key will be identical. To simplify we will note that the channel estimation measured at a mobile M as $\hat{h}_M$. The expression $\hat{h}_M[i]$ corresponds to the estimation of the i^{th} sample. The following steps describe in detail the principle of the proposed key generation algorithm:

1) M proceeds by estimating the noise variance N in the environment. This operation can be done when no activity was observed in the neighbourhood. The noise N is adopted as the minimum threshold to reduce the probability of detecting bits by mistake.
2) During a period of time, the channel is estimated $\hat{h}_M$ using a known signal (*i.e.*: pilots and preamble in a standard communication packet)
3) M determines two thresholds $L^+ = max(\hat{h}_M)$ and $L^- = min(\hat{h}_M)$ that correspond respectively to the positive and the negative amplitude of the received signal.
4) M scans the sequence $\hat{h}_M$ to detect which samples cross the thresholds. If $\hat{h}_M[i] > L^+$ then the binary vector $BV_M(i) = 1$ else if $\hat{h}_M[i] < L^-$ then $BV_M(i) = 0$. The position of the extracted bits is saved on a table of positions.
5) Next, M adjusts the threshold values : $L^+ = L^+ + \frac{max(\hat{h}_M)}{\delta}$ and $L^- = L^- - \frac{min(\hat{h}_M)}{\delta}$ where δ is a protocol parameter.
6) The process of 4 and 5 are repeated until the noise level is reached or the length of binary vector is equal to the secret key length (fixed at 128, 256 bits, or more).
7) An error correcting scheme it used to guarantee that M has the same key candidate with the other terminal such as in [9]. We suppose that B is the receiver and A is the emitter. In this case, A sends to B the index positions table. B compares the two tables (the one it computed and the other one it received from A) to find the disagreement bits which will be discarded and sends to A the positions of deleted bits.
8) A eliminates the dissimilar bits and checks if the candidate key K_A is equal to K_B. For that, A chooses a random real number R then encrypts it with K_A and sends the message $S_A = E_{K_A}(R)$
9) B decrypts the received message $S_{R_B} = D_{K_B}(S_A)$ and sends $S_B = E_{K_B}(S_{R_B} + 1)$
10) A decrypts the received message $S_{R_A} = D_{K_A}(S_B)$ and verifies if S_{R_A} is equal to $R + 1$. Then, an acknowledgement is sent to B to confirm the agreement or disagreement result.

After the establishment of agreement between A and B, a renewal process is applied. A gets a random number X sufficient large and sends the encrypted result to B like in the 8^{th} step. Each node calculates $K = K_A \oplus X = K_B \oplus X$ where the $\oplus$ is bitwise XOR. The resulting key K will be used to encrypt the communication between A and B. In order to enhance security and confidentiality, this step is updated periodically or when detecting channel variation by examining the previous and the actual channel estimations.

B. Example

An example of the proposed quantization process is shown in figure 5 for the node A. The length of the sequence $\hat{h}$ is about 100 samples. The adjustment parameter noted δ is 5. First, A measures the noise's level (black lines). Second, the positive and negative thresholds $L^+(1)$ and $L^-(1)$ are fixed respectively to the highest and the lowest sample amplitudes. Then, A spares the samples to check whose are crossing the thresholds. The binary vector 'BV' and the ranking tables 'pos' are constructed as mentioned in the 4^{th} step. Finally, the thresholds are adjusted L^+ and L^- (red and blue lines) using the method cited in 5^{th} stage. We repeat the scanning process until reaching the noise level.

978-1-4244-6273-5/09/$26.00 ©2009 IEEE

C. Validation of the proposed solution

In this work, the proposed algorithm was implemented and evaluated using UWB experimental traces. These data were collected by the campaign of measurements presented in the section III. We test the attacker scenario presented in the figure 1c, where an eavesdropper moves in the receiver vicinity in order to extract channel estimation correlated to Bob's observations. We assume that the adversary E listen to all communication between the authorized users and it can measure the channel between herself and A and between herself and B. E applies the same quantization algorithm. As reported in figure 1c, the proposed solution has reduced considerably the key agreement ratio with the attacker compared to the existing quantization solutions shown in figures 2b and 2c.

An evaluation of the parameter δ (mentioned in the 5^{th} step) was tested to verify the impact on the secret key length and agreement ratio of the authorized users. Figure 4c shows the binary vector size using the proposed quantization for Alice, Bob and Eve. As depicted in this figure, the three peers have successively extracted sufficient large binary vectors. Due to the channel reciprocity, the curves of Alice and Bob (the legitimate users) are very close. It is clear that increasing the parameter δ results in a higher secret key length but it set-up also the secret key agreement of the attacker with the legitimate users Alice and Bob, as depicted in figure 4b. This figure shows the agreement ratio of the attacker; when he extracts the binary vectors from the channel estimations $\hat{h}_{AE}$ and $\hat{h}_{BE}$ and after receiving the exchanged data between A and B during the correctness process. As we can see the key agreement ratio of the attacker is very low; on the contrary, the ratio that A and B agree on the same keys is very high. It is equal to 1, i.e. that A and B have the same candidate keys.

VI. Conclusion

The channel reciprocity and spatial correlation are the key properties of signal-based key generation protocols. These concepts have been validated by a large campaign of measurements. The first important result of this paper concerns the spatial correlation of channel impulse responses. This parameter depends on multipath distribution and thus on the environment structure. So, the secret key generation based on physical layer must be avoided in free-space environments. Second, this paper demonstrates that the quantization phase, i.e. the conversion of samples to binary values, has a critical impact on the security of key generation process based on the physical layer. A new adaptive quantization scheme is proposed and evaluated. This new solution allows the authorized parties to share and agree on the same cryptographic key which is sufficient long. Finally, this work shows that with such algorithm an attacker sharing the same emitter or receiver's channel can not extract the same secret keys. It is clear that additional research should be performed as future work to attempt to "steal" the shared keys for secret key generation based on channel fluctuations.

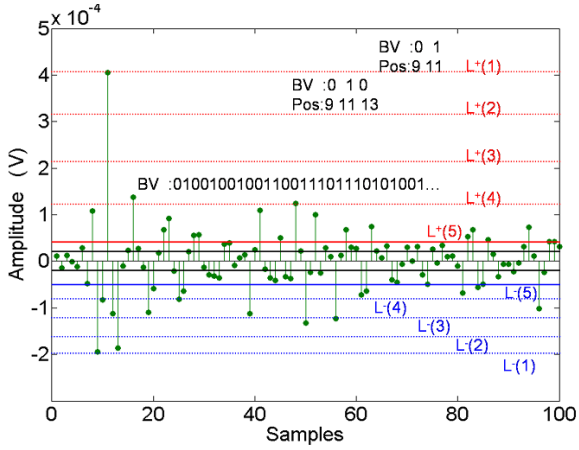


Fig. 5. Example of the proposed extracting binary vectors method

References

[1] G. Smith, "A direct derivation of a single-antenna reciprocity relation for the time domain," IEEE Transactions on Antennas and Propagation, vol. 52, 2004, pp. 1568-1577.

[2] R. Wilson, D. Tse, and R.A. Scholtz, "Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels," IEEE Transactions on Information Forensics and Security, vol. 2, 2007, pp. 364-375.

[3] T. Aono and al., "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," IEEE Transactions on Antennas and Propagation, vol. 53, 2005, pp. 3776-3784.

[4] B. Azimi-Sadjadi and al. "Robust key generation from signal envelopes in wireless networks," Proceedings of the 14th ACM conference on Computer and communications security, Alexandria,USA, 2007, pp. 401-410.

[5] T. Kitano and al., "A Private Key Agreement Scheme Based on Fluctuations of BER in wireless Communications," The 9th International Conference on Advanced Communication Technology, 2007, pp. 1495-1499

[6] A. Kitaura and al., "A Private Key Sharing Scheme Based on Multipath Time Delay in UWB Systems," International Conference on Communication Technology, 2006, pp. 1-4.

[7] A. Kitaura, H. Iwai, and H. Sasaoka, "A Scheme of Secret Key Agreement Based on Received Signal Strength Variation by Antenna Switching in Land Mobile Radio," The 9th International Conference on Advanced Communication Technology, 2007, pp. 1763-1767.

[8] S. Yasukawa, H. Iwai, and H. Sasaoka, "A secret key agreement scheme with multi-level quantization and parity check using fluctuation of radio channel property," IEEE International Symposium on Information Theory, 2008, pp. 732-736.

[9] S. Mathur and al., "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," Proceedings of the 14th ACM international conference on Mobile computing and networking, San Francisco, California, USA, 2008, pp. 128-139.

[10] M.G. Madiseh, M.L. McGuire, S.S. Neville, L. Cai, and M. Horie, "Secret Key Generation and Agreement in UWB Communication Channels," IEEE GLOBECOM 2008. pp. 1-5.

[11] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," IEEE Transactions on Communications, vol. 43, 1995, pp. 3-6.

[12] A. Kitaura and H. Sasaoka, "A Scheme of Private Key Agreement Based on the Channel Characteristics in OFDM Land Mobile Radio," Electronics and Communications in Japan, Part 3 (Fundamental Electronic Science), vol 88, No 9, p 1-10, 2005