Secret Key Generation Using Reciprocity in Ultra-wideband Outdoor Wireless Channels

Jing jing Huang, Ting Jiang
Key Laboratory of Universal Wireless Communication, Ministry of Education
Beijing University of Posts and Telecommunications, Beijing, China
[e-mail: jingjinghuangbupt@gmail.com]
*Corresponding author: Ting Jiang

Received October 28, 2013; revised January 2, 2014; accepted January 22, 2014; published February 28, 2014

Abstract

To investigate schemes of secret key generation from Ultra-wideband (UWB) channel, we study a statistical characterization of UWB outdoor channel for a campus playground scenario based on extensive measurements. Moreover, an efficient secret key generation mechanism exploiting multipath relative delay is developed, and verification of this algorithm is conducted in UWB Line-of-sight (LOS) outdoor channels. For the first time, we compare key-mismatch probability of UWB indoor and outdoor environments. Simulation results demonstrate that the number of multipath proportionally affects key generation rate and key-mismatch probability. In comparison to the conventional method using received signal strength (RSS) as a common random source, our mechanism achieves better performance in terms of common secret bit generation. Simultaneously, security analysis indicates that the proposed scheme can still guarantee security even in the sparse outdoor physical environment free of many reflectors.

Keywords: UWB, secret key generation, multipath relative delay, reciprocity

A preliminary version of this paper has been accepted by IEEE MILCOM 2013, November 18-20, San Diego, USA. This version devotes to a concrete analysis of secret key generation in UWB outdoor wireless channels. The research was supported by National Science Foundation of China under grant no.61171176. We express our thanks to the anonymous reviewers for their thoughtful and constructive remarks that are helpful to improve the quality of this paper.

http://dx.doi.org/10.3837/tiis.2014.02.011

1. Introduction

Securing wireless communication remains a major concern in dynamic mobile environments due to the shared nature of wireless medium and lacking of fixed key management infrastructures. Unlike wired networks, traditional security algorithms and protocols [1] relying mainly on cryptography and other mathematical properties to support confidentiality and authentication, are inapplicable to wireless networks. For example, it is difficult for wireless networks to ensure availability of a certificated authority, which causes the necessity of having alternatives for establishing keys between authorized parties. Therefore, a novel notion of physical layer (PHY) based key generation [2] has been proposed and the resulting approaches serve as solutions to key establishment problem in wireless networks. Based on the reciprocity of radio wave propagation, two transceivers can exploit wireless channel characteristics, which are not available to adversaries in other locations, as a source of common randomness to achieve information-theoretical security [3]. The channel characteristics mentioned above include signal phase, time delay, channel impulse response (CIR) and received signal strength (RSS).

Much work on secret key generation in narrow band wireless communications has been carried out. Hershey et al. was the first who proposed a key generation scheme based on differential phase detection [4]. Since it is easy to acquire RSS values on most off-the-shelf radio devices, recent researches focus on using RSS for extracting shared secret bits between two transceivers [5]-[9]. However, this method suffers from some limitations such as low key bit generating rate and scalability problems. To overcome these issues, new schemes based on channel phase estimation were investigated in [10] [11], which allowed effective accumulation of channel phases across many nodes. In [12], the authors have proposed a bit extraction framework and an adaptive quantization approach achieving a key rate of 22 bits/sec at a bit disagreement rate of 2.2 percent. Multiple-antenna devices were also used to increase the bit generation rate by more than four times over single-antenna systems [13]. Similarly, channel response from multiple orthogonal frequency-division multiplexing (OFDM) subcarriers can achieve higher bit generation rate for both static and mobile cases [14]. Besides, the authors advanced the work in [7] to address low key bit rate as well as prohibitively high bit mismatch with an iterative distillation stage [15]. Most of these works can be referred to in [16], which presents a review of secret key generation exploiting wireless channel characteristics. Moreover, to strengthen wireless network security, a symmetric key generation algorithm based on an automatic repeat request (ARQ) transmission mechanism was designed in [17].

Concerning secret key extraction in UWB channels, in [18], a method called channel identification was proposed. Meanwhile, an approximation and upper bound on mutual information were derived to define the maximum size of shared key. M.G. Madiseh et al. improved the method of exploiting CIR with Low Density Parity Check (LDPC) decoders to reduce thermal noise effect and Hamming binary codes for public discussion in [19]. Verification of secret key generation from UWB channel properties was reported in [20]. To cope with successive nearly identical secret keys caused by high temporal correlations of UWB channels, beam forming technique is applied for facilitating enhancement of key randomness [21]. Additionally, frequency diversity can also increase key secrecy in wide band system [22]. In the previous works, secret key generation algorithms mostly exploited RSS to extract secret bits, which is limited in the probability of key agreement. Consequently, we need to investigate an efficient secret key generation scheme.

The body of this paper extends our prior research in [23].The primary difference is that we focus on a UWB outdoor scenario and compare the key-mismatch probability of UWB indoor and outdoor channels. Specifically, our main contribution is： We first study the UWB channel modeling for a Chinese campus playground scenario. We then develop a key generation mechanism using the multipath relative delay characteristic of the modeled channel and fully analyze its security. We finally perform simulation studies-that performance evaluations of key-mismatch probabilities, key rate under disparate number of multipath and key randomness are provided to validate the feasibility and efficiency of our mechanism. Furthermore, we consider the comparison of error probability in various conditions, such as different methods, indoor and outdoor channels.

The remainder of this paper is organized as follows. Section 2 gives problem formulation and preliminaries. Section 3 describes channel modeling which is employed within this study. Section 4 is devoted to an overview of the proposed secret key generation scheme. In Section 5, the performance of key generation algorithm is discussed. Conclusions and some possibilities for future work are presented in Section 6.

2. Preliminaries and Problem Formulation

In this section, we illustrate properties of fading channels, which will explain why we can extract secret key bits from wireless channels. Afterwards, we introduce the system model that is closely related to the secret key generation problem.

2.1 Properties of Fading Channel

In a multipath fading UWB wireless environment, there are three reasons why channel is regarded as the random source for secret key generation.

1) Reciprocity of radio wave propagation: The multipath characteristics of the radio channel are theoretically identical on both directions of a link. A transmitter-receiver pair can obtain these characteristics from the received signal.
2) Spatial variations: The property of the radio channel is unique to the location of the two endpoints of the link. Receivers at different locations cannot observe the same channel response information. This uniqueness offers potential security guarantee. Generally, an entity that is at least $\lambda/2$ (λ is the wavelength) away from the transmitter-receiver pair will experiences uncorrelated fading.
3) Temporal variations in the radio channel: The movements of the communication parties as well as other objects near the transmitter-receiver pair in the environment will make the channel change over time. Apparently, channel variations are beneficial for increasing the randomness of secret keys.

Hence, we can reap secrecy extraction utilizing the above wireless fading channel properties.

2.2 System Model

The secret key generation mechanism discussed in this paper based on the system model shown in **Fig. 1**, where transceiver A and B are legitimate parties which want to establish a key, and Eve is an adversary which aims to derive the key by intercept. Both A and B are supposed to be half-duplex in the sense that they cannot transmit and receive signals in the same time. A time-division duplex (TDD) system is employed and channel reciprocity is assumed during the coherence time, which is defined as the maximum time duration that the radio channel impulse response is stable. We only consider passive attack, assuming Eve can listen to the communication between legitimate transceiver A and transceiver B, and measure the channel between herself and A and B for key extraction. Nonetheless, Eve can neither jam the channel nor modify any message exchanged between A and B. Eve should not be very close (less than a few multiples of the wavelength of the radio waves being used to either transceiver A or B), which will ensure that Eve measures a different, uncorrelated radio channel. Furthermore, we assume that Eve cannot cause a person-in-middle attack, i.e., we do not authenticate transceiver A or B. Because there is a growing amount of work in authenticating [24] [25], we expect that these and future authentication mechanism can be used in conjunction with our secret key generation scheme to provide a strong security. **Fig. 1** shows the scenario of wireless communication between A, B and Eve. During the coherence time, the measured channel is common to a pair of legitimate communicating transceivers and is different for Eve located at a different position.

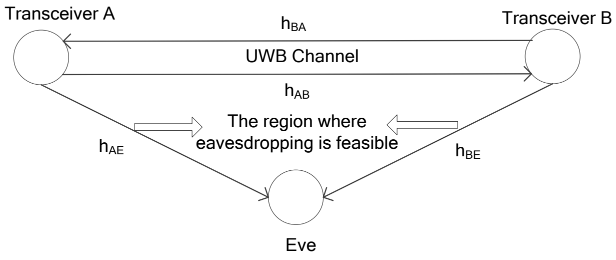


Fig. 1. An example of wireless communication between A, B and Eve: $h_{AB} = h_{BA} \neq h_{AE} \neq h_{BE}$

3. Channel Modeling

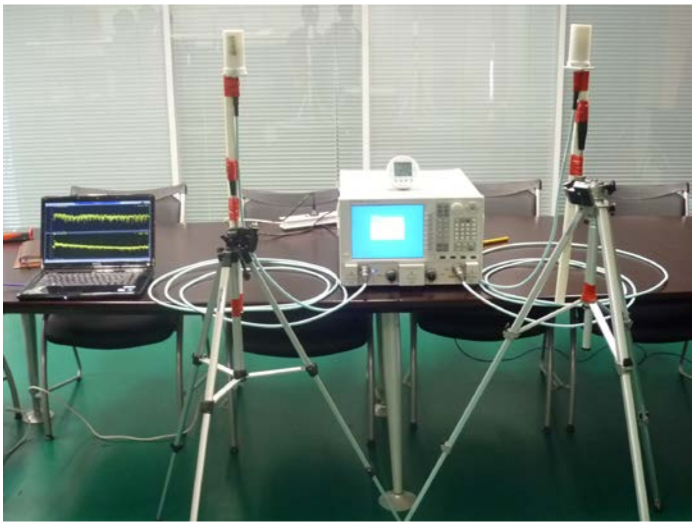


Fig. 2. Apparatus for the measurement system

In the procedure of modeling, measurements are firstly launched in our campus playground scenario. The measurement system consists of an Agilent N5242A PNA-L Network Analyzer, a pair of 0dBm gain, 2.3-18GHz omni-directional antennas, tripods and two 6-meter RF cables.

Measurements were remotely controlled by a laptop. The measured setup has been shown in **Fig.2**.

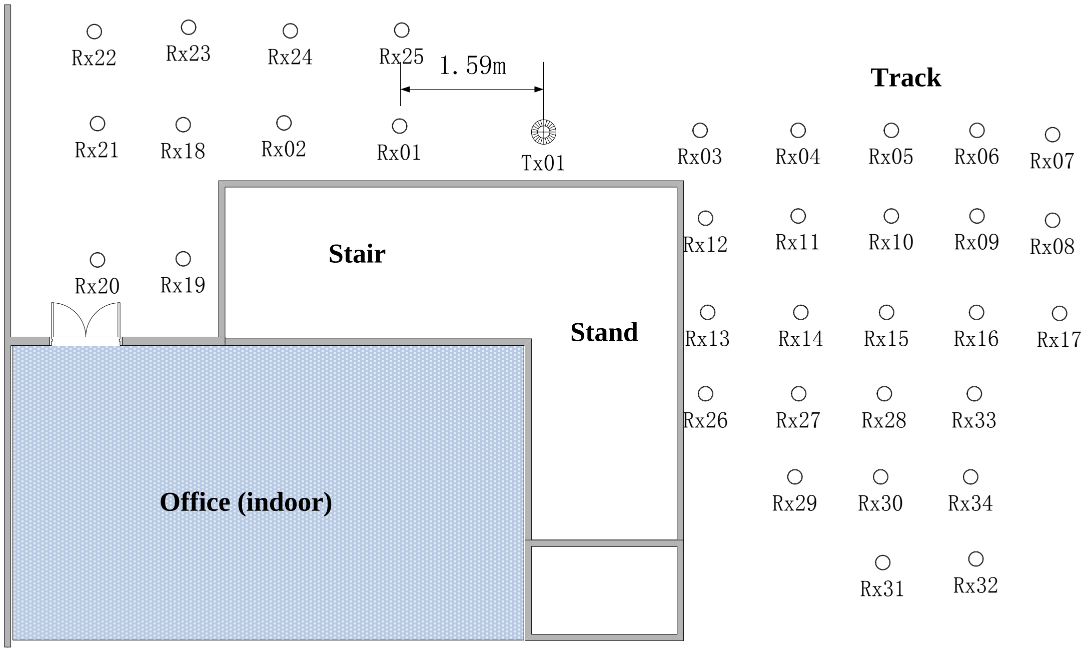


Fig. 3. Representations of the layout of measurement antennas in the playground corner of Beijing university of posts and telecommunications

Fig. 3. illustrates the topology of the playground corner and the transmitter and receivers deployment. The texture of the wall of the stand is concrete and the texture of the track is plastic. The vector network analyzer (VNA) sweeps the frequency response from 2.3 GHz to 11 GHz in 5600 linearly distributed points. In order to extract small fading parameters, the receiver moves in the transmitter vicinity where this field is divided to multiple 2cm×2cm grids. By a post-process of measured data with a windowing technique and inverse fast Fourier transformation (IFFT), we modeled the UWB outdoor channel based on the modified S-V model [26]-[28].The UWB channel impulse response $h(t)$ is

$$h(t) = \sum_{l=0}^{L}\sum_{k=0}^{K} \alpha_{k,l} \exp(j\phi_{k,l})\delta(t - T_l - \tau_{k,l}) \tag{1}$$

where L is the number of clusters, K is the number of rays within a cluster, $\alpha_{k,l}$ is the tap weight of the $k-th$ path in the $l-th$ cluster, T_l is the delay of the $l-th$ cluster, $\tau_{k,l}$ is the delay of the $k-th$ path of the $l-th$ cluster relative to T_l, and phase $\phi_{k,l}$ is uniformly distributed in $[0-2\pi]$. Due to the uniform distribution of phase, this parameter can be ignored for parameter extraction in modeling.

The number of clusters L is modeled as a random variable with small mean value. It is assumed to be Poisson-distributed with probability density function (PDF)

$$pdf_L(L) = \frac{(\overline{L})^L}{L!}\exp(-\overline{L}) \tag{2}$$

so that the mean $\overline{L}$ completely characterizes the distribution.

The distribution of the cluster arrival time T_l is given by a Poisson process

$$p(T_l \mid T_{l-1}) = \Lambda \exp\left[-\Lambda(T_l - T_{l-1})\right], l > 0 \tag{3}$$

where Λ is the cluster arrival rate.

The ray arrival time $\tau_{k,l}$ can be given by a mixture of two Poisson processes

$$p(\tau_{k,l} \mid \tau_{k-1,l}) = \beta\lambda_1 \exp[-\lambda_1(\tau_{k,l} - \tau_{k-1,l})] + (1-\beta)\lambda_2 \exp[-\lambda_2(\tau_{k,l} - \tau_{k-1,l})], k > 0 \tag{4}$$

where β is the mixture probability, and λ_1, λ_2 are the ray arrival rates.

The distribution of the small scale amplitudes is Nakagami

$$pdf(x) = \frac{2}{\Gamma(m)}\left(\frac{m}{\Omega}\right)^m x^{2m-1} \exp\left(-\frac{m}{\Omega}x^2\right) \tag{5}$$

where m is the Nakagami m-factor, $\Gamma(m)$ is the gamma function, and Ω is the mean-square value of the ampltitude. The parameter m is modeled as a lognormally distributed variable, whose logarithm has a mean μ_m and standard deviation σ_m. Both of these can have delay dependence.

Table 1 shows parameters of the UWB channel model for our campus playground corner scenario. The parameters listed in this table can be summarized as follows:

Table 1. Parameters of the channel model in UWB outdoor environment (1-12 meter, LOS)

Parameters	Value(6-9GHZ)	Value(4.2-4.8GHZ)
$\bar{L}$	4.9	3.9
κ	0.2	5.33
σ_s	2.9	3.42
Λ (1/ns)	0.101	0.038
$\lambda_1, \lambda_2 (1/ns), \beta$	0.0799, 1.4115, 0.0232	0.0709, 0.7893, 0.0358
Γ (ns)	13.2	28.53
γ (ns)	0.69	4.43
σ_c (dB)	0.2	1.2
σ_r (dB)	2.01	2.71
μ_m	-0.85	-0.82
σ_m	0.24	0.24

1) $\bar{L}$, mean number of clusters
2) κ, frequency dependence of the pathloss
3) σ_s, shadowing standard deviation
4) Λ, inter-cluster arrival rate
5) λ_1, λ_2, β, ray arrival rates
6) Γ, inter-cluster decay rate
7) γ, ray decay rate
8) σ_c, cluster log-normal standard deviation
9) σ_r, ray log-normal standard deviation
10) μ_m, Nakagami m factor mean
11) σ_m, Nakagami m factor standard deviation

We can utilize the values of the above parameters in **Table 1** to generate channel impulse response for completing simulation in section 5.

4. The Proposed Solution

In this section, we present our key generation mechanism for extracting secret bits from UWB outdoor wireless channel based on multipath relative delay and offer security analysis of the scheme.

4.1 Secret Key Generation Mechanism

Fig.4 is the block diagram of our mechanism. We use impulse radio UWB system. The following algorithm generates the secret key in four phases:

Step 1 Channel probing:

Transceiver A sends a training sequence $X(t)$ to transceiver B and then transceiver B sends the same training sequence to transceiver A. The training sequence should have a high self-correlation function and a low cross-correlation function, which is beneficial to the next extraction of multipath delay. In mathematic way, the strong self-correlation function means that if the sequence is multiplied by its delayed replica, after integral, the result approximates impulse function $\delta(t)$. We can express the self-correlation function using equation (6)

$$R_i(\tau) = \int_0^T x_i(t) x_i(t+\tau)\,dt \tag{6}$$

The weak cross-correlation function means that the cross-correlation function value of two sequences is approximate to zero. We can express the cross-correlation function using equation (7)

$$R_{ij}(\tau) = \int_0^T x_i(t) x_j(t+\tau)\,dt \tag{7}$$

Due to the reciprocity theorem that the signals transmitted between a transmitter and receiver pair experience the same fading in the coherence time, the time separation in one probing must be less than the channel coherence time. Two transceivers get measurements from the similar channel impulse response and they repeat the above procedure. Multiple rounds of channel probing should be run during different coherence time period, otherwise the randomness of the generated key bits is decreased.

Step 2 Extraction of multipath relative delay:

Suppose that the channel impulse response is $h(t)$, the received signal for A and B are $y_A(t) = h(t) * x(t) + n_A(t)$ and $y_B(t) = h(t) * x(t) + n_B(t)$ respectively, where $x(t)$ is a transmitted pulse, $n_A(t)$ and $n_B(t)$ are independent zero mean additive white Gaussian noise signals with mean powers of $\sigma^2 = N_0/2$ .Transceiver A and B estimate channel multipath delay τ_k according to their measured values y_A and y_B. A rake receiver is employed for the reception side. Extraction of multipath relative delay as well as combination of multipath components can be simultaneously conducted. The extraction scheme of multipath relative delay is provided in **Fig. 5**.

The delayed replica of the same transmitted signal at the receiver is multiplied by local training sequences to get output values, which would be compared with the preset threshold. If the output of the correlator is bigger than the threshold, the received signal is aligned in time with the training sequence, and the delay of the received signal here is an estimation of channel propagation delay. This indicates that the current path is an effective multipath component and, hence, the path should be outputted and combined with other detected multipath components. We choose m ($m \le L$) paths with high amplitude gains. Let the delay of these m paths be $\tau_1, \tau_2, ..., \tau_m$, then the relative delay between adjacent paths is $\tau_2 - \tau_1, \tau_3 - \tau_2, ..., \tau_m - \tau_{m-1}$. Assume the multipath resolution is $\Delta\tau$, and all the multipath delays are multiples of $\Delta\tau$. Then multipath relative delay components can be written in discrete form as follows:

$$\tau_2 - \tau_1 = (n_2 - n_1).\Delta\tau \tag{8}$$

$$\tau_3 - \tau_2 = (n_3 - n_2).\Delta\tau \tag{9}$$

$$\vdots \qquad \vdots$$

$$\tau_m - \tau_{m-1} = (n_m - n_{m-1}).\Delta\tau \tag{10}$$

The characteristic value of multipath relative delay is $n_2 - n_1$, $n_3 - n_2$, …, $n_m - n_{m-1}$.

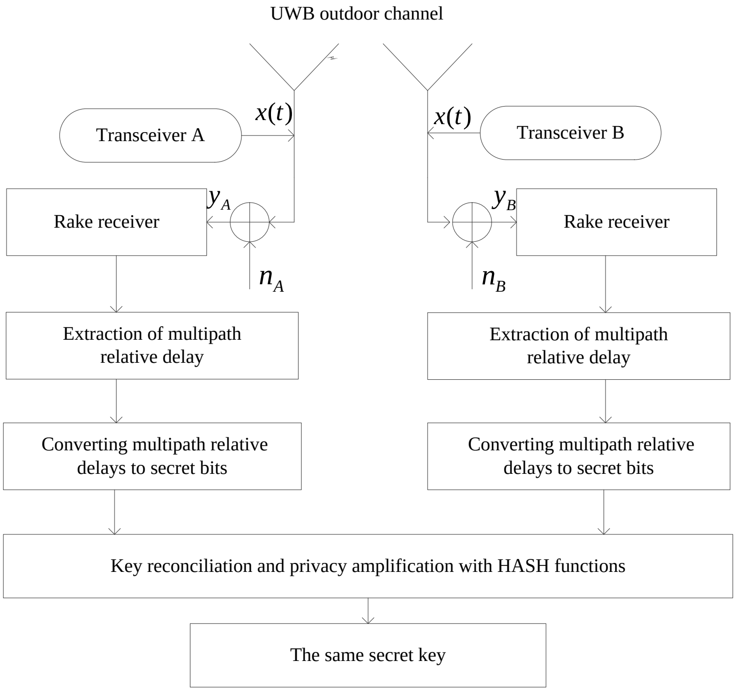

UWB outdoor channel
$x(t)$
Transceiver A
$x(t)$
Transceiver B
Rake receiver
y_A
n_A
y_B
Rake receiver
n_B
Extraction of multipath relative delay
Extraction of multipath relative delay
Converting multipath relative delays to secret bits
Converting multipath relative delays to secret bits
Key reconciliation and privacy amplification with HASH functions
The same secret key

Fig. 4. A block diagram of secret key generation mechanism based on multipath relative delay

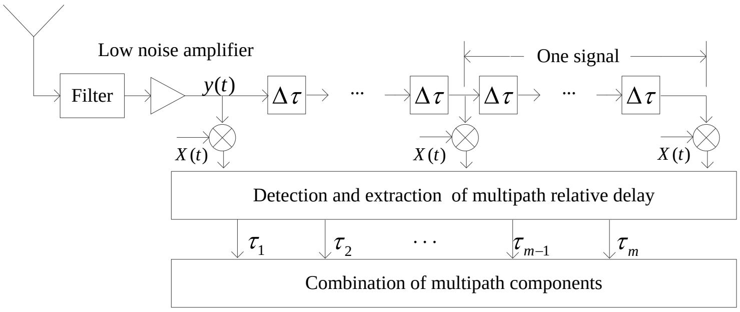


Fig. 5. An extraction scheme of multipath relative delay

Step 3 Converting multipath relative delays to secret bits:

Both transceivers convert their multipath relative delays to random key bits through quantization. For the sake of reducing the discrepancies that may result in key disagreement between two transceivers, the difference for relative delay minus mean delay is chosen as common random numbers, from which a key sequence can be extracted. In this phase, mean multipath delay is calculated by

$$\delta_{\text{mean-delay}} = \frac{n_m - n_1}{m-1} \tag{11}$$

Next, we compute the difference between relative delay and mean delay and compare the value with 0. The generation rule is

$$key = \begin{cases} 1, if\,(n_m - n_{m-1}) - \delta_{mean\_delay} \geq 0 \\ 0, if\,(n_m - n_{m-1}) - \delta_{mean\_delay} < 0 \end{cases}$$

As is shown above, $(m-1)$ key bits are generated in one channel estimation. The advantage of using the difference is improving key disagreement caused by noise. Although Eve can generate key bits based on the same method, she cannot obtain correct secret key bits due to lacking high correlation of evaluated multipath delay with legitimate transceivers.

Step 4 Key reconciliation and privacy amplification:

On account of estimation errors, half-duplex transmission and noise, a small number of bit discrepancies may exist. These error bits can be corrected using either error correcting codes [29] or the Cascade Protocol [30]. Note that some information might be revealed and used by the adversary to guess portions of the key because error-correcting information is public, moreover, due to the correlation in generated key bits, privacy amplification should be implemented to address the above problems. This is achieved by letting transceiver A and transceiver B use Hash functions to obtain fixed size small length output from long input streams.

4.2 Security Analysis of the Mechanism

To evaluate the security of generated secret key bits, we provide full security analysis of multipath relative delay method in three aspects as following:

1) In information theory, as we mentioned in Section 1, 2, properties of fading channel can be used as a source of common randomness to achieve information- theoretical security. Here, we rely on the multipath relative delay to extract secret bits. As discussed in Section 2-2, we consider the basic communication example as shown in Fig.1 for simplification. Suppose R_{AB} and R_{BA} denote the samples acquired at transceiver B and A. Let R_{AE} and R_{BE} denote the samples gotten at Eve, and K_{AB} is the key which transceiver A and B want to establish. Then the mutual information between legitimate transceivers is $I(R_{AB};R_{BA}) = K_{AB}$. In the course of key agreement of K_{AB}, the mutual information Eve can learn is $I = (R_{AE}, R_{BE}; K_{AB})$. Because channels between any two endpoints of links are independent, for any $\varepsilon > 0$, we can obtain $I(R_{AE}, R_{BE}; K_{AB}) \leq \varepsilon$. Therefore, this proves that the eavesdropper can barely achieve useful information from legitimate transceivers.

2) In simulation aspect, we verify the proposed method according to performance evaluation metrics. To make generated key bits secure, key-mismatch probability between legitimate transceivers must be lower than that of a legitimate transceiver and an eavesdropper, which can be proved by **Fig. 7**. Additionally, the generated secret bits must have independence. We check this using randomness test suit NIST in Section 5-2. Table 2 attests to the randomness of the generated key bit sequences. Moreover, from **Fig. 8**, we can see that secret key generation rates can also be guaranteed.

3) In practical side, take a UWB wireless system with 6.3GHz carrier frequency for an example. Due to spatial variation characteristic in Section 2-1, if the adversary is more than 23.8mm away from the legitimate nodes, it observes different channel variations such that no useful information is reveled to it. Even some little information is divulged, we can deal with this problem in privacy amplification step. During the process of channel modeling, although we have found that the outdoor environment are free of many reflectors, in which case the information observed by legitimate transceivers and the adversary would be correlated, the simulation results as shown in **Fig. 9** still indicate that our mechanism can achieve better key agreement performance than traditional RSS method.

5. Simulation Studies

In this section, the proposed key generation scheme using multipath relative delay is verified and compared with RSS-based method. In addition, comparison of key-mismatch probability between indoor and outdoor scenarios is reported.

The simulated channel model is the outdoor environment channel we have modeled in Section 3. Features of the channel are set in accordance to **Table 1**. Note that standard IEEE UWB channel models **[31]** can also be used for simulation. Additionally, some other parameters are:

1) Carrier frequency of 6.3GHz
2) Bandwidth of 600MHz
3) Sampling rate of 24GHz
4) Average moving speed of 4m/s, Doppler shift of 84Hz
5) Coherence time of 11.9ms
6) Distance between transceivers changes from 1m to 12m.

We adopt pulse position modulation and selective rake (S-RAKE) receiver with a strategy of equal gain combination (EGC). Performance evaluation metrics of the mechanism are presented in terms of key generation rate, key randomness and the probability that the transceivers fail to agree on the same key bits (i.e. probability of error or key-mismatch probability).

5.1 Key-mismatch Probability and Key Generation Rate

The first example considers the resulting secret bits from multipath relative delay. **Fig. 6** illustrates the converting process with a simplified example that the number of path is 6. For transceiver A, the multipath relative delay is $\Delta\tau$, $3\Delta\tau$, $5\Delta\tau$, $2\Delta\tau$, $5\Delta\tau$ and the mean delay is $3.2\Delta\tau$. According to the rule in step three, we can obtain secret key bits 00101. For transceiver B, the multipath relative delay is $2\Delta\tau$, $\Delta\tau$, $3\Delta\tau$, $2\Delta\tau$, $4\Delta\tau$ and the mean delay is $2.4\Delta\tau$. Similarly, we get secret key bits 00101. Hence, the two bit sequences have same secret bits. Note that sometimes the two sequences have different bits, we can correct the error bit in key reconciliation phase.

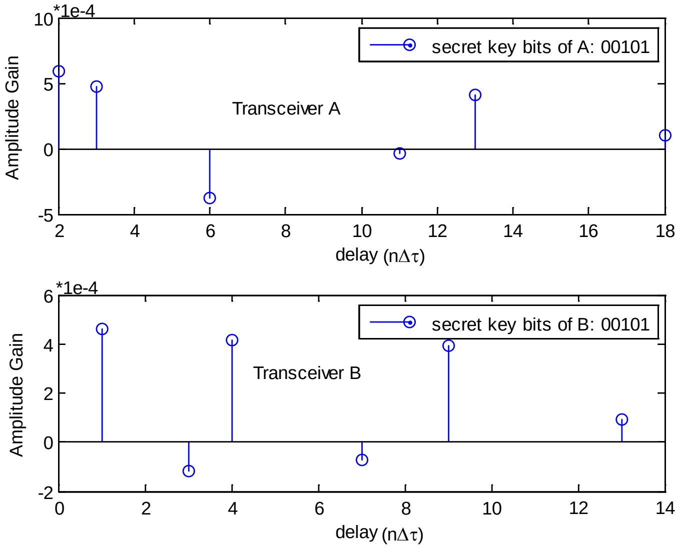


Fig. 6. Converting multipath relative delays into bits when m=6

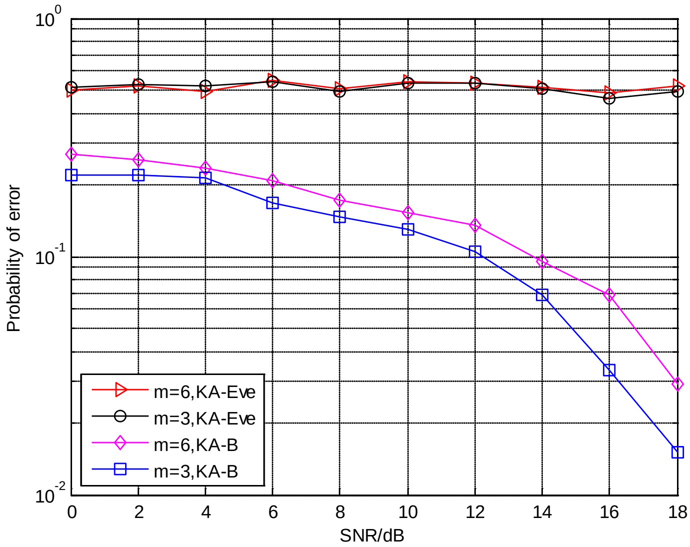


Fig. 7. Probability of error for receivers based on different m paths

Fig. 7 shows the probability of error for key generation between transceiver A and B and Eve as a function of signal noise ratio (SNR). The error probability for key generation between transceiver A and B (KA-B) decreases as SNR increases, while the probability of error for transceiver A and Eve (KA-Eve) is always from 0.5 to 0.6, proving the low key-mismatch probability of legitimate nodes but high key-mismatch probability between legitimate users and eavesdroppers. This can be clearly observed from the curves.

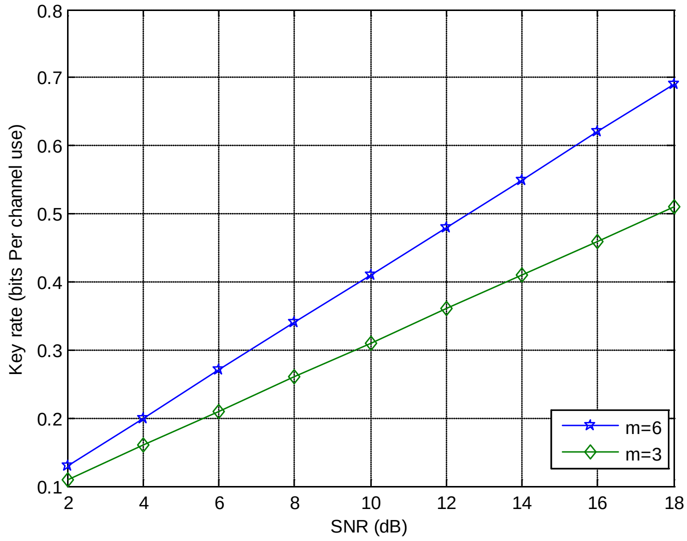


Fig. 8. Comparison of key rates under different m paths

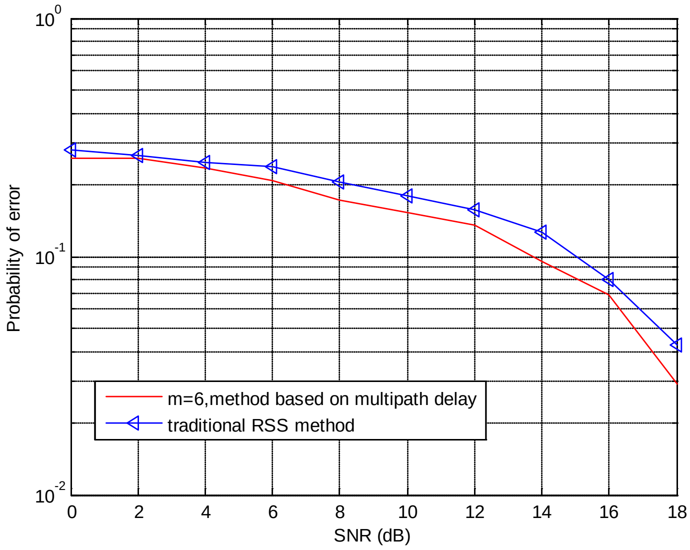


Fig. 9. Comparison of error probability with method of multipath relative delay and RSS-based method

In **Fig. 8**, we compare the key rates as a function of SNR corresponding to extracting different number of multipath. The gain in the secret key rate increases as SNR increases. Although the maximum key rate under m=3 is just 0.51, given that the number of multipath and cluster in sparse outdoor scenario is not so much as in a cluttered (e.g., indoor) environment, this rate is an acceptable rate with corresponding error probability. It can be seen from the Figures 6, 7 and 8 that m paths can generate (m-1) key bits, and m is proportional to key generation rate and key-mismatch probability, which illustrates a trade-off between key generation rate and key agreement probability.

Fig. 9 plots error probability for key generation exploiting different channel characteristics.

The proposed scheme extracting multipath relative delay is superior to the method based on RSS, since the set of decision thresholds for RSS may enforce uncertainty of key generation. What is more, the advantage is much greater at high SNR.

Given that cost, from system aspect, there is no extra cost for multipath delay method compared with RSS scheme, because impulse radio UWB system can use rake reception technique to extract different channel characteristics. But from algorithm complexity and operation time sides, the cost of multipath delay method is somewhat higher than that of RSS scheme. After all, the former method gains better performance in terms of key-mismatch probability. In fact, as mentioned, using S-RAKE receiver and an EGC strategy, we have made a tradeoff between cost and performance for multipath relative delay method. Moreover, with the assist of advanced computers, the processing time can be further reduced. Therefore, it is worthwhile achieving lower key-mismatch probability at the cost of computation complexity and processing time for some requirement.

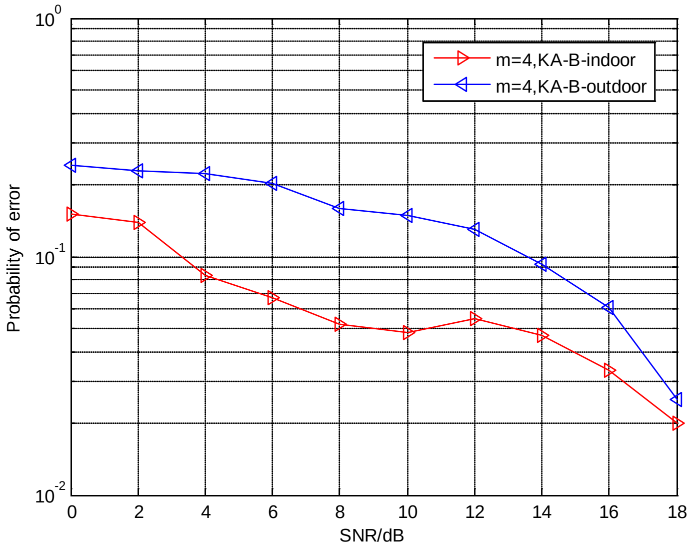


Fig. 10 Comparison of error probability with method of multipath relative delay over UWB indoor and outdoor wireless channels when m=4

Fig. 10 presents the results of key-mismatch probability in UWB indoor and outdoor channels. Note that the indoor channel is residential channel and its error probability has been stated in [23]. It can be seen that transceivers can achieve better key agreement in indoor UWB channel than outdoor UWB channel. This is caused by outdoor sparse physical environment. The number of multipath and clusters in outdoor environments is smaller than that in indoor scenarios, which gives rise to disadvantage of extracting multipath delay.

5.2 Key Randomness

It's important to ensure the randomness of secret keys. Hence we employ a widely used randomness test suit NIST to verify the randomness of our generated secret key bits [32]. In the test, we randomly select 80 key sequences generated from our simulation and calculate their p-values. To pass the test, all p-values must be greater than 0.01. Due to the limitation of bit length, we run eight tests from 16 different statistical tests. The results listed in **Table 2** show that the generated key bit streams pass the test and the entropy of the key bit sequences is close to a truly random sequence.

Table 2. Results of NIST

Test	P-value
Frequency	0.21
BlockFrequency	0.05
Cumulative sum(Fwd)	0.19
Cumulative sum(Rev)	0.17
Runs	0.41
Longest run	0.5
Approximate Entropy	0.63
Serial	0.52, 0.42

6. Conclusion

In this paper, we have modeled UWB outdoor channels based on the measurements in a Chinese campus playground scenario. A key generation scheme exploiting multipath relative delay was developed and verified over the modeled channel. Simulation results have shown that the proposed method is feasible in terms of performance evaluation metrics for it can achieve a relatively lower key-mismatch probability comparing with RSS-based method, and obtain an acceptable key rate with corresponding key-mismatch probability and also pass the randomness test. Additionally, results indicate that error probability under indoor (residential) UWB channel is lower than that in UWB outdoor channel for the campus playground scenario. Moreover, security analysis has also been provided. Further study may be required into active attack and key generation with combination of multiple channel characteristics to improve security capabilities. We would like to explore these in our future work.

References

[1] W. Diffie, and M. E. Hellman, "New directions in cryptography," *IEEE Trans on Information Theory*, vol.22, no.6, pp. 644-654, 1976. Article (CrossRef Link)

[2] J. E. Hershey, A. A. Hassan, and Yarlagadda, R, "Unconventional cryptographic keying variable management," *IEEE Trans on Communications*, vol.43, no.1, pp. 3-6, Jan. 1995. Article (CrossRef Link)

[3] R. Ahlswede, and I. Csiszar, "Common randomness in information theory and cryptography. I. secret sharing," *IEEE Trans on Information Theory*, vol.39, no.4, pp. 1121-1132, 1993. Article (CrossRef Link)

[4] A. A. Hassan, W. E. Stark, and J. E. Hershey, "Cryptographic key agreement for mobile radio", *Digital Signal Processing*, vol. 6, pp. 207-212, 1996. Article (CrossRef Link)

[5] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. of ACM CCS'07*, Alexandria, USA, pp. 401-410, Oct. 2007. Article (CrossRef Link)

[6] S. Mathur, W. Trappe, N. Mandayam, and C. Ye, "Radio telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. of ACM MobiCom'08*, San Francisco, USA, pp. 128-139, Sept. 2008. Article (CrossRef Link)

[7] S. Jana, S. N. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. of ACM MobiCom'09*, pp. 321-332, Sept. 2009. Article (CrossRef Link)

[8] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation for

fading wireless channels," *IEEE Trans on Antennas and Propagation*, vol.53, no.11, pp. 3776-3784, Nov. 2005. Article (CrossRef Link)

[9] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans on Information Forensics and Security*, vol.5, no.2, pp. 240-254, Jun. 2010. Article (CrossRef Link)

[10] Q. Wang, H. Su, and K. Ren, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. of IEEE INFOCOM'11*, Shanghai, China, pp. 1422-1430, Apr.2011. Article (CrossRef Link)

[11] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrow band fading channels," *IEEE Journal on selected areas in communications*, vol.30, no.9, pp. 1666-1674, Oct. 2012. Article (CrossRef Link)

[12] N. Patwari, J. Croft, S. Jana, and S. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans on Mobile Computing*, vol.9, no.1, pp. 17-30, Jan. 2010. Article (CrossRef Link)

[13] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. of IEEE INFOCOM'10*, San Diego, USA, pp. 1837-1845, Mar. 2010. Article (CrossRef Link)

[14] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. of IEEE INFOCOM'13*, Turin, Italy, pp. 3048-3056, Apr. 2013. Article (CrossRef Link)

[15] S. Premnath, S. Jana, J. Croft, P. Gowda, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans on Mobile Computing*, vol.12, no.5, pp. 917-930, May. 2013. Article (CrossRef Link)

[16] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Magazine of Wireless Communications*, vol.18, issue.4, pp. 6-12, Aug. 2011. Article (CrossRef Link)

[17] Y. S. Khiabani, and S.Wei, "Design and analysis of an ARQ based symmetric key generation algorithm," in *Proc. of IEEE MILCOM'11*, Baltimore, USA, pp. 1273-1278, Nov. 2011. Article (CrossRef Link)

[18] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: secret sharing using reciprocity in UWB channels," *IEEE Trans on Information Forensics and Security*, vol.2, no.3, pp. 364-375, 2007. Article (CrossRef Link)

[19] M. G. Madiseh, M. L. McGuire, S. S. Neville, L. Cai, and M. Horie, "Secret key generation and agreement in UWB communication channels," in *Proc. of IEEE GLOBECOM'08*, New Orleans, USA, pp. 1-5, Nov. 2008. Article (CrossRef Link)

[20] M. G. Madiseh, S. He, M. L. McGuire, S. Neville, and X. Dong, "Verification of secret key generation from UWB channel observations," in *Proc. IEEE Int. Conf. Communications*, Dresden, Germany, pp. 1-5, Jun. 2009. Article (CrossRef Link)

[21] M. G. Madiseh, S. W. Neville, and M. L. Mcguire, "Applying beamforming to address temporal correlation in wireless channel characterization-based secret key generation," *IEEE Trans on Information Forensics and Security*, vol.7, no.4, pp. 1278-1287, 2012. Article (CrossRef Link)

[22] P. Huang, and X. Wang, "Fast secret key generation in static wireless networks: a virtual channel approach," in *Proc. of IEEE INFOCOM'13*, Turin, Italy, pp. 2292-2300, Apr. 2013. Article (CrossRef Link)

[23] J. J. Huang, and T. Jiang, "Secret key generation exploiting Ultra-wideband indoor wireless channel characteristics," in *Proc. of IEEE MILCOM'13*, San Diego, USA, Nov. 2013.

[24] V. Brik, S. Banerjee, M. Gruteser, and S. Paradis, "Wireless device identification with radiometric signatures," in *Proc. of ACM MobiCom'08*, San Francisco, USA, pp. 116-127, Sept. 2008. Article (CrossRef Link)

[25] S. Jana, and S. Kasera, "On fast and accurate detection of unauthorized access points using clock skews," in *Proc. of ACM MobiCom'08*, San Francisco, USA, pp. 104-115, Sept. 2008. Article (CrossRef Link)

[26] T. Santos, J. Karedal, P. Almers, F. Tufvesson, and A. F. Molisch, "Modeling the ultra-wideband

outdoor channel-measurements and parameter extraction method," *IEEE Trans. on Wireless Communications*, vol.9, no.1, pp. 282-290, Jan. 2010. Article (CrossRef Link)

[27] T. Santos, F. Tufvesson, and A. F. Molisch, "Modeling the Ultra-Wideband Outdoor Channel: Model Specification and Validation," *IEEE Trans. on Wireless Communications*, vol.9, no.6, pp. 1987-1997, Jun. 2010. Article (CrossRef Link)

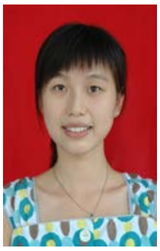
[28] C-C. Chong, Y. Kim, and S-S. Lee, "A modified S–V clustering channel model for the UWB indoor residential environment," in *Proc. of IEEE Veh. Technol. Conf*, Stockholm, Sweden, May 30-Jun 1. 2005. Article (CrossRef Link)

[29] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM Journal of Computing*, vol.38, no.1, pp. 97-139, 2008. Article (CrossRef Link)

[30] G. Brassard, and L. Salvail, "Secret key reconciliation by public discussion," *Lecture notes in Computer Science*, 765: 410-423, 1994. Article (CrossRef Link)

[31] J. Foerster, "Channel modeling sub-committee report (final)", Feb. 2003.

[32] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Hechert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," in *Proc. of* 800th ed., *National Institute of Standards and Technology*, May. 2001.



Jing jing Huang received her B.E and M.S degree in communication engineering from Nan Chang University of Aeronautics, Jiang Xi province, China in 2007 and 2010 respectively. From 2010 to 2012, she was a teacher in communication department at An Hui University of Technology. Now, she is a Ph.D. student, majoring in communication and information system, at Beijing University of Posts and Telecommunications. Her research interests are primarily in Internet of things and wireless network security.

Ting Jiang is currently a professor of Key Laboratory of Universal Wireless Communication, Ministry of Education at Beijing University of Posts and Telecommunications. His research interests include short range communication, wireless sensor network, information security and signal processing.