An Investigation of Using Loop-back Mechanism for Channel Reciprocity Enhancement in Secret Key Generation

An Investigation of Using Loop-back Mechanism for Channel Reciprocity Enhancement in Secret Key Generation

Linning PENG, Guyue LI, Junqing ZHANG, Roger WOODS, Ming LIU and Aiqun HU

Abstract—Physical layer security key generation exploits unpredictable features from wireless channels to achieve high security, which requires high reciprocity in order to set up symmetric keys between two users. This paper investigates enhancing the channel reciprocity using a loop-back scheme with multiple frequency bands in time-division duplex (TDD) communication systems, in order to mitigate the effect of hardware fingerprint interference and synchronization offset. The scheme is evaluated to be robust to passive eavesdropping and active Man-in-the-Middle attack through both theoretical analyses and practical measurements. A secret key generation protocol is subsequently designed. The performance of the proposed secret key generation method is then evaluated through both numerical simulation and experiments. Results demonstrate that the proposed scheme can effectively mitigate non-reciprocity and outperforms the classical TDD scheme in both key disagreement rate and key generation rate.

Index Terms—channel reciprocity, channel state information, hardware fingerprint, physical layer security, secret key generation, loop-back transmission, OFDM, USRP.

1 Introduction

Secure communication with a shared secret key has become a hot research topic in wireless communications [1], [2], [3]. Conventional key distribution schemes, such as the Diffie-Hellman key exchange, rely on the complex mathematical algorithms and protocols [4], and usually require a public key infrastructure (PKI). These schemes may not be applicable in future massive low-cost and decentralized networks such as the Internet of Things (IoT). Exploiting physical layer (PHY) channel information for secret key generation is a potential complementary technology; it extracts secret keys from the randomness of wireless channel that has independent variation and reciprocal properties [5], [6].

In PHY-information-based key generation, a pair of legitimate transceivers measure channel state information (CSI), which usually varies continually during the communication [2]. However, the difference between the measured CSI in each side of the two transceivers consequently leads to key disagreements [7], [8]. The causes of CSI non-reciprocity can be categorized as follows.

- **Channel variations between measurements:** In time division duplex (TDD) systems, uplink (UL) and downlink (DL) channels are measured at different time slots. The relative movements between users will cause CSI variations in half-duplex measurements [9], [10].
- **Hardware fingerprint interference:** Due to the manufacturing deviation of radio components, the features of the hardware are inherently different at each device, including non-linearity of power amplifier, transceiver filter characteristic, receiver auto gain control (AGC) response and antenna coupling mismatch [11], [12], [13].
- **System synchronization errors:** The oscillators at transmitter and receiver deviate in terms of frequency and phase, which will result in synchronization errors, and consequently yield CSI non-reciprocity.
- **Non-reciprocity in frequency-division duplex (FDD) systems:** In FDD systems, since the UL and DL transmissions are carried out in different frequency bands, their channel features will not be reciprocal, which creates challenges for applying key generation methods.

Due to these practical issues, CSI non-reciprocity will play a significant part in secret key generation. In order to effectively implement a key generation method in practical scenarios, it is imperative to find solutions that enhance the CSI reciprocity. This represents the main motivation of this work.

1.1 Related Work

In his seminal paper [14], Wyner introduced the wire-tap channel and wireless information theoretic secrecy. In [15] and [16], the possibility of generating common randomness at two distant terminals was presented. Inspired by this work, secret capacity of wireless channels has been ex-

- *L. Peng, G. Li and A. Hu are with the School of Cyber Science and Engineering, Southeast University, No.2 Sipailou, Nanjing, China. E-mail: {pengln,guyuelee,aqhu}@ seu.edu.cn*
- *J. Zhang is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom.Email: junqing.zhang@liverpool.ac.uk*
- *R. Woods is with School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast, BT9 5AH, United Kingdom.Email: r.woods@qub.ac.uk*
- *M. Liu is with the Beijing Key Lab of Transportation Data Analysis and Mining, Beijing Jiaotong University, No.3 Shangyuancun, Beijing, China.Email: mingliu@bjtu.edu.cn*

Manuscript received xxx xxx, xxxx; revised xxx xxx, xxxx.

plored [17], [18], [19] and more recently, secure transmission with multiple-antenna technologies has been presented [20], [21]. In addition, the secret capacity when the eavesdropper is very close to the legitimate receiver, has been also studied [20].

Key generation can exploit different properties of wireless channel, including received signal strength (RSS), channel phase, and CSI [22], [23]. RSS has been widely applied for key extraction in the practical implementation as it is readily available [2], [9], [24], [25], [26], [27], [28], [29], [30]. RSS-based key generation is affected by the channel variations between the measurements in TDD systems, which can be alleviated by fractional interpolation filtering [9], [27]. The major drawback of the RSS-based systems is the low key generation speed, which is due to the fact that RSS is a single dimension parameter and each packet can only produce one RSS value. In order to increase the speed, a multi-band RSS scheme using IEEE 802.15.4 was proposed to obtain the frequency-selective fading of the channel [3].

Channel phase has also been investigated for key generation. The work in [31] proposed to exploit the phase variations of the multi-path channel to achieve a much higher speed than RSS-based systems. However, channel phase can be very vulnerable to hardware fingerprint interference and synchronization. Although stochastic synchronization algorithms can be employed to compensate the synchronization error, the residual synchronization errors in both frequency and time domain affect the channel phase variations.

Orthogonal frequency division multiplexing (OFDM) can obtain channel responses in both time and frequency domains, which can be employed to achieve a much higher speed [32], [33]. However, the OFDM system is also subject to synchronization errors, which will affect the accuracy of channel estimation. Recent work in [33] and [34] analyzed the influence of the time synchronization error on the OFDM-based secret key extraction from theoretical and experimental aspects, respectively. Precoding techniques are proposed to compensate the transceiver non-reciprocity with a priori knowledge [35]. The compensation and calibration techniques at transmitter side was widely studied in wireless TDD communication systems [12], [13], [35]. A channel gain complement mechanism was designed to assist the secret key extraction with the help of subcarrier amplitude information in [36], which can achieve a speed of 90 bits per packet with 3-bit quantization. With the help of a priori information, the channel gain complement process can reduce the CSI non-reciprocity caused by hardware fingerprint interference. However, this process requires sophisticated non-reciprocity learning, which will increase the implementation complexity.

There are also research efforts to apply key generation in FDD systems. A scheme named Joint Randomness Not Shared by Others (JRNSO) was designed with a loop-back mechanism [37], which acts to mitigate the hardware fingerprint interference. Each transceiver uses a different transmission band and exchanges the estimated CSI using its own band. With the help of loop-back transmission, both transceivers can obtain equivalent CSI. Furthermore, an improved loop-back scheme was proposed in [38] to realize loop-back transmission in high-speed mobility scenario. With the help of sophisticated design of loop-back transmission with appropriate time slots, CSI non-reciprocity caused from channel variations could be partly eliminated [38]. Although private keys have been introduced in JRNSO [37], [38], their security breach has not been carefully investigated.

As with all wireless communications approaches, key generation is also vulnerable to passive eavesdropping [5], [20], [25], [28], [39], [40] and active attacks [41], [42]. As communication theory indicates, eavesdroppers experience an uncorrelated channel from legitimate users located half wavelength away, which may not always true in a practical environment because of insufficient multi-path [40]. An active Man-in-the-Middle (MitM) attack has been reported in [41] that affects the RSS-based key bit extraction by spoofing received packets between legitimate users. Moreover, authors in [42] investigated an active pilot contamination attack in OFDM-based secret key extraction, by injecting the same pilot sequences to the uplink communications.

1.2 Overview

Channel reciprocity is essential for users to agree on the same keys. This paper presents a detailed investigation of using loop-back mechanism for TDD key extraction to improve the channel reciprocity. In particular, we take into account of the hardware fingerprint interference and phase offset, and analyze their effects on the channel reciprocity. The main contributions are as follows.

- To the best of the authors' knowledge, for the first time, a passive eavesdropping attack has been created which completely cracks the JRNSO scheme.
- A secure loop-back key generation scheme referred to as LB-TDD, is proposed for TDD systems. The scheme can mitigate the hardware fingerprint interference and consequently improve the channel reciprocity. It is proved to be robust to both passive eavesdropping and active MitM attack, analyzed from information theoretical perspective and practical measurements.
- Extensive simulation is carried out and the LB-TDD scheme is evaluated to outperform the classical TDD scheme and JRNSO in terms of KDR and security level.
- A practical LB-TDD key generation system is developed using USRP N210 software defined radio (SDR) platform. We demonstrate the advantages of CSI reciprocity improvement of using LB-TDD scheme by real experiments.

The rest of this paper is organized as follows. Section 2 presents the system model. Section 3 introduces the existing JRNSO scheme and discusses the attack strategy. Section 4 presents the proposed LB-TDD scheme, and analyzes its robustness to passive eavesdropping and active attack. In Section 5, a key generation protocol is designed. Section 6 presents simulation results and analyses, and Section 7 validates the system with experimental studies. Section 8 concludes the paper.

2 System Model

2.1 MB-PHY Model

A common setting with two legitimate users, i.e., Alice and Bob, and an attacker, Eve, is considered in this paper.

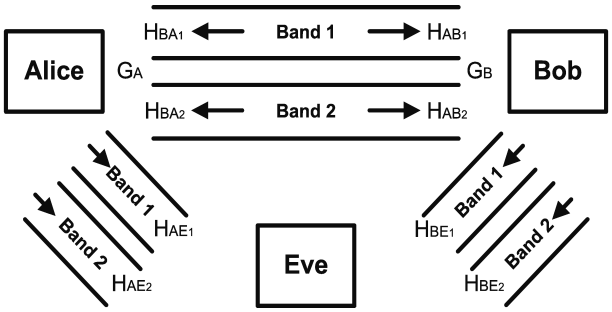


Fig. 1. System model with two frequency bands.

Fig. 1 illustrates the system model where Alice and Bob are operating at two frequency bands (Band 1 and Band 2). In the TDD systems with multi-carrier modulations, the multi-band (MB)-PHY can be implemented by selecting different subcarriers for each transmission. Eve knows the exact key extraction protocol and the parameters used by legitimate users.

CSI in the frequency domain between transmitter u and receiver v is denoted as H_{uv_i}, where $\{u, v\} = \{A, B, E\}$ represent Alice, Bob or Eve, respectively, and i is the index of the frequency band. The frequency responses of different bands will be independent when they are out of the coherence bandwidth in a frequency-selective fading channel, which is given as

$$H_{uv_i}^{(t)} \neq H_{uv_j}^{(t)}, \quad \forall i \neq j. \tag{1}$$

For the same link, the channel reciprocity holds and we have

$$H_{uv_i}^{(t)} = H_{vu_i}^{(t)}. \tag{2}$$

In this paper, we employed the OFDM system as an example to obtain the CSI. OFDM has been adopted in many commercial wireless systems, such as IEEE 802.11 a/g/n/ac, LTE, etc.

2.2 CSI Non-Reciprocity

Channel reciprocity implies that the channel responses at the two ends of the same link are reciprocal. However, the real measurements are subject to hardware noise, non-simultaneous measurements, and hardware imperfection. While the former two factors have been studied in the previous work, e.g., [43], the effect of the hardware imperfection has not been evaluated for the key generation systems [20], [31], [32].

Due to the manufacture deviation, hardware fingerprints exist even with the same manufacturer and production [44], [45], [46], which will have oscillator differences and introduce subcarrier frequency errors [45]. The frequency difference will result in phase shift, denoted as φ_{uv}. As the frequency difference between two transceivers are mutually inverse, $\varphi_{uv} \cdot \varphi_{vu}$ can equal 1. Moreover, there can be amplifier non-linear behavior, transceiver filter characteristics and gain imbalance features [44]. In this paper, we consider hardware fingerprint only with transceiver filter characteristics and gain imbalance features for simplicity. Their influences are simplified as G_u.

The phase offset and hardware fingerprints will impact the channel measurements. We use an equivalent channel gain to represent the effect, which is given as

$$\widetilde{H}_{uv_i}^{(t)} = G_u H_{uv_i}^{(t)} \varphi_{uv}. \tag{3}$$

This paper, for the first time, evaluated the effect of hardware fingerprint and phase offset on key generation by theoretical modelling, simulation and experiments.

3 JRNSO Scheme for FDD Systems

In this section, the existing JRNSO loop-back scheme is introduced. Then an attack strategy is presented and the security of JRNSO scheme is analyzed. Finally the deficiencies of JRNSO scheme for FDD systems is discussed.

3.1 Description of JRNSO Scheme

The JRNSO scheme was designed to apply key generation in FDD systems [37]. As the hardware fingerprint G_u is not considered in their work, it is set to 1 in the following analysis. In order to simplify the presentation, noise is not considered either. The scheme is explained as below.

- Step(1): At time t, Alice generates a private frequency-domain pilot $\mathcal{P}$ and transmits $\mathcal{P}$ to Bob via Band 1 and Bob receives it as $\mathcal{P}H_{AB_1}$. As Bob has no information about the private pilot $\mathcal{P}$, he cannot estimate the channel.
- Step(2): Simultaneously at time t, Bob generates a private pilot $\mathcal{Q}$ and transmits $\mathcal{Q}$ to Alice via Band 2 and Alice receives the signal as $\mathcal{Q}H_{BA_2}$. As Alice has no information about the private pilot $\mathcal{Q}$, she cannot estimate the channel.
- Step(3): At time $t + \tau$, where τ is the delay between two transmission, Bob transmits the signal received in Step(1) via Band 2. Alice receives the loop-back signal from Band 2 and obtains the signal: $\mathcal{P}H_{AB_1}H_{BA_2}$. As Alice knows the private pilot $\mathcal{P}$, she can estimate the composite CSI: $H_{AB_1}H_{BA_2}$.
- Step(4): Simultaneously at time $t+\tau$, Alice transmits the signal that received in Step(2) via Band 1. Bob receives the loop-back signal from Band 1 and obtains signal: $\mathcal{Q}H_{BA_2}H_{AB_1}$. As Bob knows the private pilot $\mathcal{Q}$, he can obtain the composite CSI: $H_{BA_2}H_{AB_1}$.

Through the above four steps, both Alice and Bob have the same composite CSI: $H_{BA_2}H_{AB_1}$, which can be exploited for secret key generation.

3.2 Attack Strategy

In [37], the authors consider that Eve does not know the private pilots $\mathcal{P}$ and $\mathcal{Q}$, thus Eve cannot calculate the CSI from $\mathcal{P}H_{AB_1}H_{BE_2}$ and $\mathcal{Q}H_{BA_2}H_{AE_1}$. Although Eve can hardly obtain H_{AB_1} and H_{BA_2}, we still find an attack to the JRNSO scheme by eavesdropping the above four steps.

The private pilot transmitted by Alice (Bob) in Step(1) (Step(2)) can be also received by Eve as $\mathcal{P}H_{AE_1}$ ($\mathcal{Q}H_{BE_2}$). In addition, in Step(3) and Step(4), Eve can observe $\mathcal{P}H_{AB_1}H_{BE_2}$ and $\mathcal{Q}H_{BA_2}H_{AE_1}$, respectively.

Eve can divide the signal obtained in Step(3) by the signal received in Step(2), which yields

$$\frac{\mathcal{P}H_{AB_1}H_{BE_2}}{\mathcal{Q}H_{BE_2}} = \frac{\mathcal{P}}{\mathcal{Q}}H_{AB_1}. \tag{4}$$

Then Eve divides the signal received in Step(4) by the signal received in Step(1), which can be given as

$$\frac{\mathcal{Q}H_{BA_2}H_{AE_1}}{\mathcal{P}H_{AE_1}} = \frac{\mathcal{Q}}{\mathcal{P}}H_{BA_2}. \tag{5}$$

Multiplying results in (4) and (5), Eve will get

$$\frac{\mathcal{P}}{\mathcal{Q}}H_{AB_1} \times \frac{\mathcal{Q}}{\mathcal{P}}H_{BA_2} = H_{AB_1}H_{BA_2}, \tag{6}$$

which is exactly the same information shared between Alice and Bob. Therefore, the JRNSO protocol is vulnerable to passive eavesdropping. A similar method can be adopted to attack other JRNSO-like schemes such as that proposed in [38].

The JRNSO scheme contains a "round-trip" signal transmission. The receiver obtains the signal at one band, and transmits the received signal back to the transmitter at another band. All these transmissions can be captured by Eve due to the open nature of the wireless medium and she can crack the system by the mechanism proposed here.

4 Loop-Back Scheme for TDD Systems

Although the JRNSO scheme has been proved to be vulnerable to passive eavesdropping in the FDD systems, we have designed a new scheme by applying the loop-back mechanism at two bands into TDD systems, termed LB-TDD scheme. The new scheme can improve the reciprocity of the measurements and is secure from the passive eavesdropping and active attacks.

4.1 LB-TDD Scheme

In the LB-TDD scheme, Alice and Bob use two bands for transmission and reception, which is illustrated in Fig. 2 and explained as follows.

- Step(1): At time t, Alice initially transmits the public pilot signal to Bob via Band 1. Bob obtains the CSI as

$$\widetilde{H}_{AB_1}^{(t)} = G_A H_{AB_1}^{(t)}\varphi_{AB} + \omega_{B_1}^{(t)}, \tag{7}$$

  where ω_{v_i} is the noise at receiver v at the i^{th} band.
- Step(2): At time $t+\tau$, Bob transmits the pilot signal to Alice via Band 1. Alice obtains the CSI as

$$\widetilde{H}_{BA_1}^{(t+\tau)} = G_B H_{BA_1}^{(t+\tau)}\varphi_{BA} + \omega_{A_1}^{(t+\tau)}. \tag{8}$$

- Step(3): At time $t+2\tau$, Bob transmits the signal received in Step(1) using Band 2 and Alice can receive the loop-back signal and obtains the CSI as

$$\begin{aligned}\widetilde{H}_{BA}^{(t+2\tau)} =& G_B\widetilde{H}_{AB_1}^{(t)}H_{BA_2}^{(t+2\tau)}\varphi_{BA} + \omega_{A_2}^{(t+2\tau)}\\ =& G_B G_A H_{AB_1}^{(t)}H_{BA_2}^{(t+2\tau)}\varphi_{AB}\varphi_{BA} +\\ & G_B\omega_{B_1}^{(t)}H_{BA_2}^{(t+2\tau)}\varphi_{BA} + \omega_{A_2}^{(t+2\tau)}.\end{aligned} \tag{9}$$

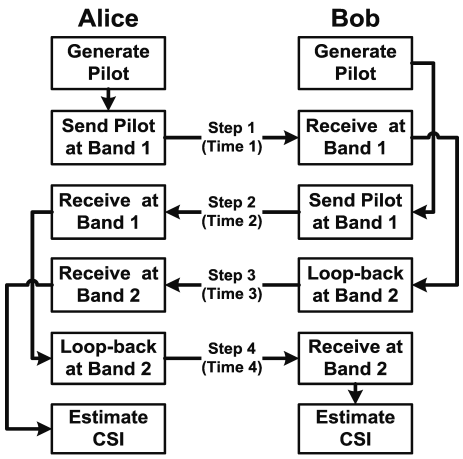


Fig. 2. Flowchart of LB-TDD scheme.

- Step(4): At time $t+3\tau$, Alice transmits the signal received in Step(2) using Band 2. Bob receives the loop-back signal and obtains the CSI as

$$\begin{aligned}\widetilde{H}_{AB}^{(t+3\tau)} =& G_A\widetilde{H}_{BA_1}^{(t+\tau)}H_{AB_2}^{(t+3\tau)}\varphi_{AB} + \omega_{B_2}^{(t+3\tau)}\\ =& G_A G_B H_{BA_1}^{(t+\tau)}H_{AB_2}^{(t+3\tau)}\varphi_{BA}\varphi_{AB} +\\ & G_A\omega_{B_1}^{(t+\tau)}H_{AB_2}^{(t+3\tau)}\varphi_{AB} + \omega_{B_2}^{(t+3\tau)}.\end{aligned} \tag{10}$$

A classical TDD-based key generation only consists of Step(1) and Step(2). Our proposed LB-TDD scheme includes Step(3) and Step(4), which are the loop-back processes. The common randomness finally shared between Alice and Bob is $G_A G_B H_{AB_1}^{(t)}H_{BA_2}^{(t)}\varphi_{BA}\varphi_{AB}$, which includes the hardware fingerprint and phase offset of the both users.

4.2 Theoretical Performance Analysis

In this section, we assume that the channel has perfect reciprocity and unity gain for theoretical analysis. In addition, receiver can perfectly eliminate phase offset φ_{uv}. The system model can then be simplified as

$$\widetilde{H}_{AB_1} = G_A H_{AB_1} + \omega_{B_1}, \tag{11}$$

$$\widetilde{H}_{BA_1} = G_B H_{BA_1} + \omega_{A_1}, \tag{12}$$

$$\widetilde{H}_{BA} = G_B H_{BA_2}\widetilde{H}_{AB_1} + \omega_{A_2}, \tag{13}$$

$$\widetilde{H}_{AB} = G_A H_{AB_2}\widetilde{H}_{BA_1} + \omega_{B_2}, \tag{14}$$

where

$$\begin{aligned}&\mathbb{E}[H_{uv_1}H_{uv_1}^{\mathcal{H}}] = \mathbb{E}[H_{uv_2}H_{uv_2}^{\mathcal{H}}] = r,\\ &\mathbb{E}[\omega_{u_1}{\omega_{u_1}}^{\mathcal{H}}] = n,\\ &\mathbb{E}[\omega_{u_2}{\omega_{u_2}}^{\mathcal{H}}] = n,\end{aligned}$$

and $\mathbb{E}(\cdot)$ is the expectation, the superscript $(\cdot)^{\mathcal{H}}$ is the conjugate transpose of matrix, r is the received signal power, and n is the noise power. We use a and b to denote the normalized hardware fingerprint at Alice and Bob, respectively.

In the classical TDD key generation system, the normalized mean square error (MSE) of the CSI measurement due

to the hardware fingerprint interferences and noise can be given as,

$$MSE_{\text{TDD}} = \frac{\mathbb{E}\left\{|\widetilde{H}_{AB_1} - \widetilde{H}_{BA_1}|^2\right\}}{\mathbb{E}\left\{|\widetilde{H}_{AB_1}|^2\right\}} = \frac{(a-b)^2 r + 2n}{a^2 r + n}. \quad (15)$$

In our LB-TDD system, the normalized MSE of the CSI measurement due to the hardware fingerprint interferences and noise can be written as

$$MSE_{\text{LB-TDD}} = \frac{\mathbb{E}\left\{|\widetilde{H}_{AB} - \widetilde{H}_{BA}|^2\right\}}{\mathbb{E}\left\{|\widetilde{H}_{AB}|^2\right\}} = \frac{a^2 rn + b^2 rn + 2n}{a^2 b^2 r^2 + b^2 rn + n}. \quad (16)$$

As shown in (15) and (16), the noise power is boosted after loop-back transmission. When the difference between a and b is small enough, the loop-back transmission will have a higher MSE than the classical solution. The MSE difference between the LB-TDD scheme and classical TDD scheme is given by

$$\begin{aligned} MSE &= MSE_{\text{TDD}} - MSE_{\text{LB-TDD}} \\ &= \frac{a^2(a-b)^2 b^2 r^3 + (-a^4 + 2a^2 b^2 - 2ab^3 + b^4) nr^2}{(a^2 r + n)(a^2 b^2 r^2 + b^2 rn + n)} \\ &+ \frac{(-2ab - a^2(1+n) + b^2(1+n)) nr}{(a^2 r + n)(a^2 b^2 r^2 + b^2 rn + n)}. \end{aligned} \quad (17)$$

The signal power r is fixed to unity and the noise power n varies to achieve different SNR values. In order to investigate the influence of the hardware fingerprint difference, i.e., $d = |a - b|$, we set the normalized hardware fingerprint deviation of Alice a to 1, and vary that of Bob b.

A numerical calculation is carried out in order to investigate the relationship between MSE deterioration and hardware fingerprint difference. Fig. 3 shows the MSE difference as the function of the SNR. The positive MSE values mean that the LB-TDD scheme improves the MSE against the mitigating hardware fingerprint effect. The negative values indicate performance degradation because the noise boost in loop-back transmission is more serious than the benefits. For each hardware fingerprint deviation d, there is a SNR-MSE trade-off point to determine whether we have MSE benefits from loop-back transmission. Typically, for d = 0.02, 0.04, 0.06, 0.08 and 0.10, we can get MSE benefits when SNR is higher than 18.0 dB, 15.7 dB, 13.9 dB, 12.6 dB and 11.8 dB, respectively.

4.3 Passive Attack Strategy

Passive eavesdropping is one of the most common attacks in the key generation area. Eavesdroppers can listen to all the exchanging steps and try to crack the keys. This section evaluates the security performance against passive eavesdropping using both theoretical analysis and practical measurements.

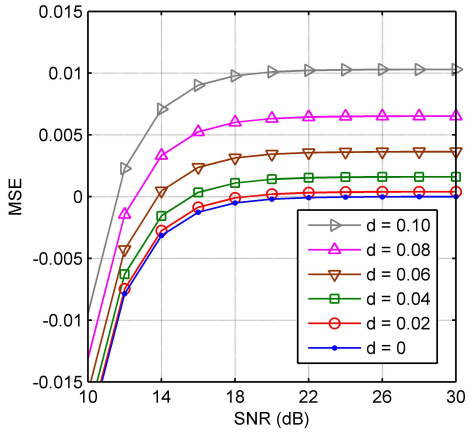


Fig. 3. MSE difference versus SNR.

4.3.1 *Theoretical Analysis*

The same attack strategies in JRNSO loop-back scheme does not work for our LB-TDD scheme. In the first two steps, Eve obtains the CSI H_{AE_1} and H_{BE_1}. In Step 3 and 4, Eve can eavesdrop the communication and obtain the CSI $H_{AB_1}H_{BE_2}$ and $H_{BA_1}H_{AE_2}$, respectively. However, in the LB-TDD scheme, due to the fact that transceivers transmit the loop-back signals via a different frequency band, the channel responses of eavesdroppers are not reciprocal, i.e., $H_{AE_1} \neq H_{AE_2}$ and $H_{BE_1} \neq H_{BE_2}$.

We then analyze how much information is revealed to eavesdroppers in key generation systems. A classical TDD model is used to investigate the effect of information leakage against the eavesdropping distance. For the simplification of notation, in this section we use $\widehat{H}_A$, $\widehat{H}_B$, and $\widehat{H}_E$ to denote the channel observation of Alice, Bob, and Eve, respectively. Hardware fingerprint interference and phase offset are not considered and the investigation can be treated as a reference model.

The maximum number of unique information bits extracted between Alice and Bob is the mutual information of the observed channels. Assuming correlated zero-mean complex Gaussian random vectors for the channels [20], we have

$$I_k = I(\widehat{H}_A; \widehat{H}_B) = \log_2 \frac{|\widehat{R}_{AA}||\widehat{R}_{BB}|}{|\widehat{R}_{AB}|}, \quad (18)$$

where $|x|$ is the determinant of x, and $\widehat{R}_{x_1 x_2} = \mathbb{E}\{\widehat{H}_{x_1}\widehat{H}_{x_2}^{\mathcal{H}}\}$ is the covariance matrix.

As Bob and Eve are stationary, the secret key capacity due to the eavesdropping [20] can be given as

$$I_{sk} = I(\widehat{H}_A; \widehat{H}_B | \widehat{H}_E) = \log_2 \frac{|\widehat{R}_{AE}||\widehat{R}_{BE}|}{|\widehat{R}_{EE}||\widehat{R}_{ABE}|}. \quad (19)$$

An upper band of the maximum number of unique information bits is represented as [15]

$$C(A; B||E) \leq \min\left[I_k, I_{sk}\right]. \quad (20)$$

When Eve is closer to Bob, I_{sk} gradually decreases due to the increased correlation between $\widehat{H}_E$ and $\widehat{H}_B$. Therefore, the available safe key can be evaluated by means of a ratio

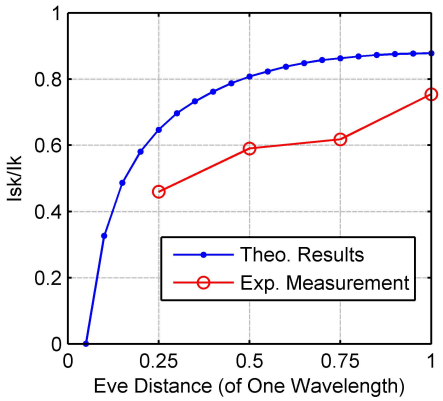


Fig. 4. η versus eavesdropper distance.

of secret mutual information in (19) divided by mutual information without eavesdropping in (18):

$$\eta = I_{sk}/I_k. \tag{21}$$

Theoretical work claims that key generation is secure from passive eavesdropping when eavesdroppers are located more than half wavelength away from the legitimate users. We focus on eavesdroppers within one wavelength of the legitimate parties. Without loss of generality, Eve is assumed to be located close to Bob, i.e.,

$$|C_B - C_E| < 1, \tag{22}$$

where $C_u = [x_u,\ y_u]$ is the 2-D antenna coordinate of user u in wavelength. Alice is in the far field of Bob and Eve. Therefore, the transmission channel between Alice to Bob and that between Alice to Eve can be treated as the same. As the distance is very short between Bob and Eve, we use an azimuth MIMO channel model [47] to simulate the multi-path environment. The complex-valued baseband channel impulse response [47] is given as

$$h_{uv} = \sum_{l=1}^{N_{\text{path}}} h_l \cdot \exp\left[j(k_l \cdot C_u + k_l' \cdot C_v)\right], \tag{23}$$

where N_{path} is the number of the paths, $k_l = 2\pi[\cos\phi_l,\ \sin\phi_l]$ and h_l are the complex baseband gain of l^{th} path.

Following the model in (23), a complex Gaussian Rayleigh channel is generated with N_{path} set to 128 and SNR given as 20 dB. The relationship between η and eavesdropper distance in wavelength is depicted in Fig. 4. When the distance between Eve and Bob is less than $1/2$ wavelength, the secret mutual information I_{sk} decreases dramatically. It is clear that when Eve is close enough to Bob, i.e., within $1/4$ wavelength, the key generation system can barely ensure the security of the generated secret keys. When distance between Eve and Bob is larger than $1/2$ wavelength, the revealed information is relatively small.

4.3.2 *Practical Measurements*

We also carried out practical measurements to reveal the $\eta = I_{sk}/I_k$ in real environments. Existing work indicated that RSS observed by eavesdropper located greater than

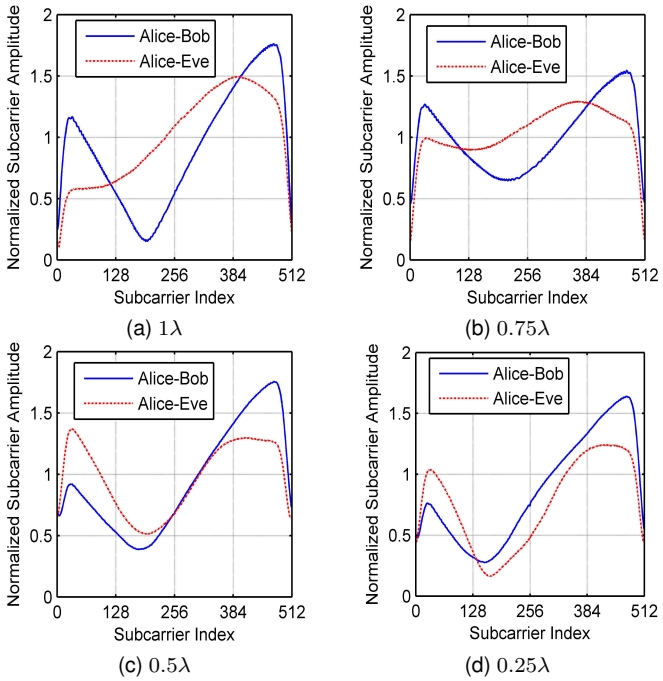


Fig. 5. CSI snapshots of Bob and Eve with different distances between them.

half-wavelength away still has a strong correlation to that of the legitimate users [48]. The inherent feature of multi-path fading is the core factor that ensures the security of key generation in the wireless channel. The OFDM system can simultaneously measure CSI across a wide bandwidth and is used to investigate the correlation of the CSI between the eavesdropper and legitimate users.

We used a Rohde & Schwarz SMW200A vector signal generator as the signal source for Alice; it was continuously transmitting OFDM probing signals at a carrier frequency of 2.485 GHz. Two receivers, Bob and Eve, were positioned very close to each other within one wavelength, i.e. approximately 12 cm for 2.485 GHz carrier frequency. Bob and Eve simultaneously captured the OFDM probing signal, and I_{sk} and I_k were calculated from the measured results. The phases of CSI are subject to synchronization offset, which can hardly be completely eliminated in real measurements. Therefore, only the amplitude results of CSI were used for I_{sk} and I_k calculation.

The measurements were carried out at four different eavesdropping distances, including 1λ, 0.75λ, 0.5λ and 0.25λ. Snapshots of CSI with different distance configurations are shown in Fig. 5 as examples and $\eta = I_{sk}/I_k$ calculated from measurements is depicted in Fig. 4. As expected, the secret mutual information I_{sk} gradually reduces when Eve is closer to Bob. The measured results have a deviation from the theoretical curve though, which is probably due to the insufficient multi-path in the environment.

4.4 Active Attack Strategy

Thanks to the orthogonality among subcarriers in the OFDM-based key generation, Eve cannot use the same MitM attack introduced in [41]. Therefore, Eve has to imitate the OFDM probing symbols for active MitM attack. A

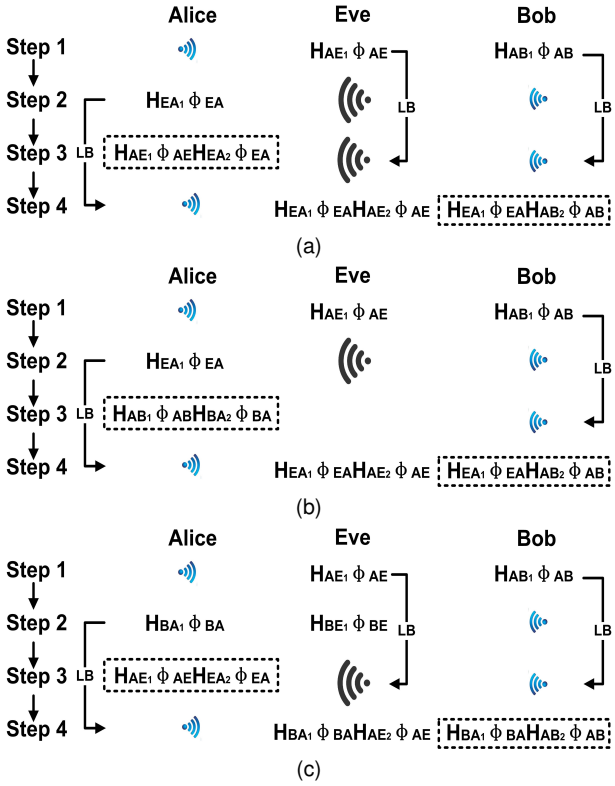


Fig. 6. Possible active MitM attack procedures in LB-TDD scheme.

possible active attack strategy similar to [42] is considered in this paper. We neglect the hardware fingerprint difference, i.e. $G_A = G_B = G_E = 1$, for this analysis.

In a classical TDD-based key generation system, Eve listens to the transmissions and obtains CSI $H_{AE_1}\varphi_{AE}$ when Alice is sending OFDM probing symbols to Bob at Step(1) of Fig. 2. At Step(2), Eve can inject OFDM probing symbols with higher transmission power in order to initiate an active attack. Alice thus obtains CSI $H_{EA_1}\varphi_{EA}$ because the jamming signal is much stronger than that from Bob. As Alice has no prior information of φ_{BA}, she cannot find the change of carrier frequency offset in $H_{EA_1}\varphi_{EA}$. When the multi-path effect of the wireless channel is not significant, H_{EA_1} can be occasionally correlated to H_{BA_1}, especially when Eve is close to Bob. In this case, Eve has a good chance to obtain the information of final secret key bits from the eavesdropped CSI $H_{AE_1}\varphi_{AE}$.

Possible active MitM attacks in the LB-TDD scheme are depicted in Fig. 6, with the transmissions and CSI measurements obtained by Alice, Bob and Eve illustrated. As shown in Fig. 6(a), Eve jams the transmission in both Step(2) and Step(3). After the four steps, Alice, Bob and Eve will obtain $H_{AE_1}\varphi_{AE}H_{EA_2}\varphi_{EA}$, $H_{EA_1}\varphi_{EA}H_{AB_2}\varphi_{AB}$ and $H_{EA_1}\varphi_{EA}H_{AE_2}\varphi_{AE}$, respectively. The CSI finally obtained by Alice inherently has a zero subcarrier frequency offset because $\varphi_{AE} \cdot \varphi_{EA} = 1$. However, the final CSI obtained by Bob will have a residual carrier frequency offset because $\varphi_{EA} \cdot \varphi_{AB} \neq 1$. Hence, Bob can quickly discover that the communication has been actively attacked. Furthermore, Bob can also easily detect an active attack if Eve only attacks in Step(2), as shown in Fig. 6(b).

In order to reduce the risk of being detected, Eve can only inject a jamming signal in Step(3), as shown in Fig. 6(c). In this case, both Alice and Bob can obtain a CSI without a carrier frequency offset. However, the CSI obtained by Eve is $H_{BA_1}\varphi_{BA}H_{AE_2}\varphi_{AE}$. Since $\varphi_{BA} \cdot \varphi_{AE} \neq 1$ and there is no pilot symbol for frequency offset estimation, Eve will have to carry out blind frequency offset estimation which is very complex when the number of subcarrier is large.

The frequency offset at the receiver causes significant inter-carrier interference in OFDM systems [45], [49]. In order to compensate the frequency offset, pilots are carefully designed and an advanced frequency offset estimation algorithm is implemented at the receiver. In the LB-TDD scheme, thanks to the loop-back transmission, the residual carrier frequency offset is normally eliminated at both Alice and Bob. However, Eve cannot accurately estimate the carrier frequency offset so there will be residual $\varphi_{EA}\varphi_{AB}$.

In summary, thanks to the loop-back transmission, legitimate users can quickly detect the active attack due to the abnormal change of the carrier frequency offset. Moreover, the LB-TDD scheme can inherently overcome the carrier frequency offset without additional training sequence. This advantage further enhances the security of CSI exchanging process between Alice and Bob.

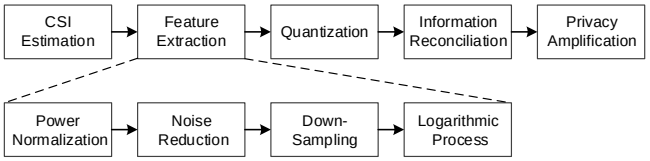


Fig. 7. Proposed secret key generation protocol.

5 LB-TDD Key Generation Scheme

In this section, we designed the protocol of LB-TDD scheme, which is consisted of five steps: CSI estimation, feature extraction, quantization, information reconciliation, and privacy amplification, as illustrated in Fig. 7.

5.1 CSI Estimation

Let's take one loop as an example to explain the channel estimation. The user u will first transmit public pilot symbols S to user v via Band 1, which can be given as

$$Y_v(m) = G_u H_{uv_1}(m) S(m) \varphi_{uv} + \omega_{v_1}(m), \tag{24}$$

where m is the subcarrier index. User v will then loop the received signal back to user u via Band 2, which can be written as

$$Y_u(m) = G_v H_{vu_2}(m) Y_v(m) \varphi_{vu} + \omega_{u_2}(m). \tag{25}$$

Finally, user u can obtain the CSI through least square (LS) estimation [50]

$$\widetilde{H}_{uv}(m) = \frac{Y_u(m)}{S(m)}. \tag{26}$$

5.2 Feature Extraction

We designed a feature extraction method to improve the quality of the channel estimation, which is shown in Fig. 7 and includes power normalization, noise reduction, downsampling, and logarithmic process.

In practical mobile communications systems, the user received power may differ. The power of the channel estimation is firstly normalized as follows,

$$\widetilde{H}_{uv}^{\text{Norm}}(m) = \frac{\widetilde{H}_{uv}(m)}{\sqrt{\sum_{i=1}^{N} |\widetilde{H}_{uv}(i)|^2}}. \tag{27}$$

In addition, the received loop-back signal contains noise factors, ω_{v_1}, and, ω_{v_2}, in both transmissions, which affect the estimation accuracy. We adopted a moving average filter leveraging the correlation of channel response among adjacent subcarriers [51] to mitigate noise effect and smooth normalized CSI, which is given as

$$\bar{H}_{uv}^{\text{Norm}}(m) = \frac{\sum_{i=m-\frac{L}{2}+1}^{m+\frac{L}{2}} \widetilde{H}_{uv}^{\text{Norm}}(i)}{L}, \tag{28}$$

where L is the size of the moving window. Moreover, since the channel responses of subcarriers within the coherence bandwidth are correlated, we can downsample the channel responses with a sampling factor D. This is written as:

$$\bar{H}_{uv}^{\text{Down}}(m) = \bar{H}_{uv}^{\text{Norm}}\big((m-1)D+1\big). \tag{29}$$

Finally, in order to increase the dynamic range of the amplitude for quantization, we transform $\bar{H}_{uv}^{\text{Down}}$ from linear scale to logarithmic scale by

$$H_{uv}^{\text{Log}}(m) = 10\log_{10}\bar{H}_{uv}^{\text{Down}}(m). \tag{30}$$

5.3 Quantization

Quantization schemes convert analogue values into binary sequence by comparing with reference thresholds, q_i. For instance, the order-1 quantization with a gap, q_g, is represented as

$$k_m = \begin{cases} 1 & H_{uv}^{\text{Log}}(m) \geq q_1 + q_g \\ dropped & q_1 - q_g < H_{uv}^{\text{Log}}(m) < q_1 + q_g \\ 0 & H_{uv}^{\text{Log}}(m) \leq q_1 - q_g \end{cases}, \tag{31}$$

where q_1 is the threshold for order-1 quantization; k_m is quantified binary. When high-order quantization is adopted, multiple thresholds $[q_1, q_2, \cdots]$ can be designed based on the dynamic range of $H_{uv}^{\text{Log}}(m)$. A higher quantization order will increase the secret key generation rate but will result in serious key disagreement. Quantization orders and gaps should be carefully selected to balance the secret key generation rate and key disagreement.

5.4 Information Reconciliation

After the quantization process, Alice and Bob will exchange the information of their discarded channel measurements. They will use a mapping table to maintain the same channel measurements.

TABLE 1
Channel model

Channel	Multi-path delay (ms)	Averaged power of each path (dB)
Alice to Bob	[0 0.31 0.71 1.09 1.73 2.51]	[0 -1 -9 -10 -15 -20]
Alice to Eve	[0 0.05 0.11 0.17 0.29 0.31]	[0 -3 -10 -18 -26 -32]
Bob to Eve	[0 0.1 0.2 0.3 0.5 0.7]	[0 -3.6 -7.2 -10.8 -18 -25.2]
Alice HF	[0 0.065 0.13 0.185]	[0 -5 -7 -10]
Bob HF	[0 0.065 0.13]	[0 -4 -10]

TABLE 2
Simulation parameter

Parameters	Values
OFDM symbol length (with CP)	128 us
Subcarrier frequency spacing	15 KHz
Bandwidth	10 MHz
FFT size	1024
Carrier frequency at band 1	1.8 GHz
Carrier frequency at band 2	2.0 GHz
Span for moving average filter (L)	30
Downsample factor (D)	8

TABLE 3
Quantization threshold

Quantization Order	Threshold q_i
Order-1	(- 2)
Order-2	(-4, -2, 0)
Order-3	(-8, -6, -4, -2, 0, 2, 4)

5.5 Privacy Amplification

After information reconciliation, privacy amplification is employed to remove the revealed information from the generated key bits. Similar to [52] and [53], a cryptographic hash function is employed for privacy amplification.

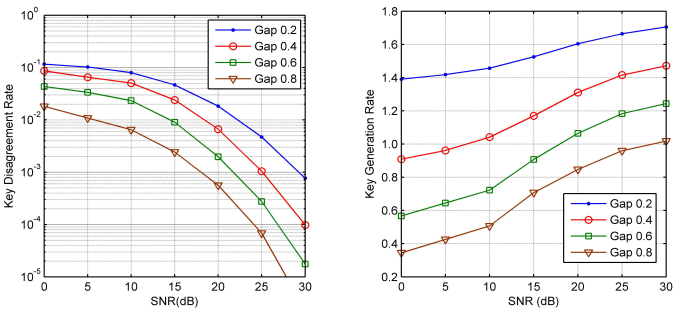
6 Simulation with LTE Model

In this section, we analyze the performance of the proposed LB-TDD scheme and compare it with the classical TDD and JRNSO schemes with extensive simulation.

6.1 Simulation Parameters

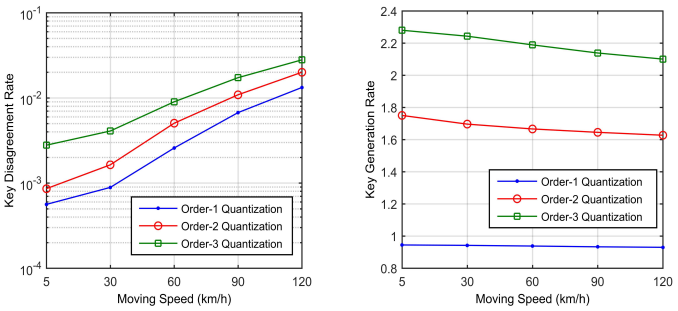
Table 1 lists simulation parameters including path delay and the average power of each path of Alice, Bob and Eve. These parameters are recommended by the ITU Vehicular Type A channel model [54]. The effect of hardware fingerprint is modeled as a filter with different taps in the time domain, and the filter parameters are also shown in Table 1. We used an LTE transceiver model [55] and the simulation parameters are given in Table 2. Finally, quantization thresholds are shown in Table 3.

We used two metrics, namely key disagreement rate (KDR) and key generation rate (KGR), to evaluate the system performance. The KDR is defined as the total disagree key bits between two users divided by the total generated



(a) KDR (b) KGR

Fig. 8. KDR and KGR performance of LB-TDD scheme versus SNR with different quantization gaps (order-2 quantization and 5 km/h).



(a) KDR (b) KGR

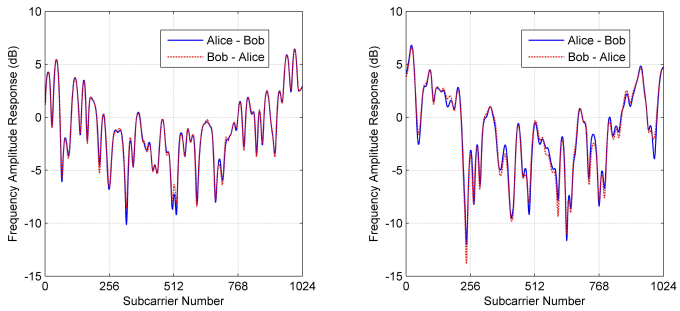
Fig. 9. KDR and KGR performance of LB-TDD scheme versus moving speed with different quantization orders (quantization gap of 0.2 and SNR of 30 dB).

key bits. In order to reveal the CSI reciprocity between different schemes, KDR was calculated before information reconciliation. The KGR is defined as the total generated key bit divided by the number of total used subcarriers.

6.2 Performance of the LB-TDD Scheme

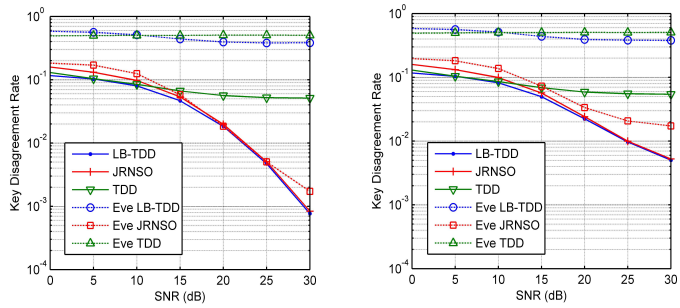
Fig. 8 shows the performance of KDR and KGR under different SNRs and quantization gaps, with an example setup of order-2 quantization and 5 km/h moving speed. With the targeted KDR of 1×10^{-3}, the required SNR is about 29 dB, 25 dB, 22 dB and 18 dB, for quantization gaps of 0.2, 0.4, 0.6 and 0.8, respectively. The obtained KGR is around 1.7, 1.4, 1.1 and 0.8 for each quantization gap with the desired SNR. KGR is reduced when the quantization gap is increased because more samples are dropped. On the other hand, increasing the quantization gap will significantly reduce the KDR. Therefore, the quantization gap needs to be optimized according to practical system settings.

Fig. 9 presents the KDR and KGR performance with respect to different quantization orders and moving speeds, with a quantization gap of 0.2 and SNR of 30 dB. Quantization order needs to be carefully selected, because it has opposite effects on the KDR and KGR. In addition, increasing the moving speed will cause more severe KDR. Fig. 10 shows the snapshots of the measured CSI between Alice and Bob under slow mobility (5 km/h) and high mobility (120 km/h). In high mobility scenario, the CSI measurements of the two channel links have obvious disagreement, which increases the KDR between Alice and Bob.



(a) 5 km/h (b) 120 km/h

Fig. 10. CSI snapshot of Alice and Bob in LB-TDD scheme.



(a) 5 km/h moving speed (b) 60 km/h moving speed

Fig. 11. KDR performance of different schemes.

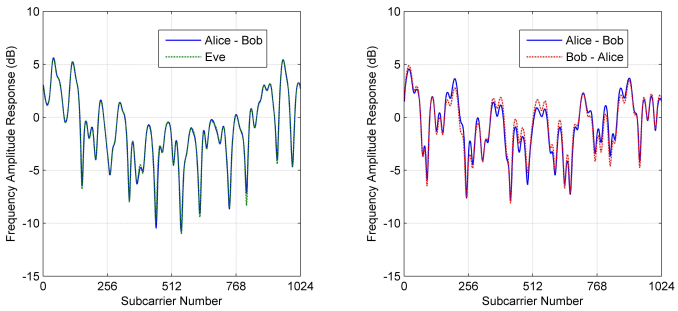
6.3 Comparisons of Different Schemes

We compare the performance of TDD, JRNSO and LB-TDD schemes in this section. Simulation parameters were configured as follows, an order-2 quantization, a quantization gap of 0.2, and two mobilities of 5 km/h and 60 km/h. We also simulated the eavesdropping process for the JRNSO scheme. Eve can obtain a CSI between Alice and Eve and also between Bob and Eve with a very high SNR (40 dB). Eve tries to crack the mutual CSI between Alice and Bob using the attack strategy discussed in Section 3.2.

Fig. 11 shows the comparison results. Alice and Bob obtain similar KDR performance when using the JRNSO and LB-TDD schemes. Both schemes outperforms the TDD scheme when the SNR is higher than 10 dB. However, in the JRNSO scheme, the KDR of Alice-Bob and KDR of Alice-Eve are very close, which means Eve can get a very similar observation and crack the mutual CSI between Alice and Bob. A snapshot of CSI obtained by Alice and Eve is presented in Fig. 12(a) as an example, where Eve obtains almost identical CSI as Alice. As a result, the JRNSO scheme cannot ensure the security of generated key bits. Fig. 12(b) presents a snapshot of CSI obtained by Alice and Bob in the classical TDD scheme. Due to the hardware fingerprint interference, the measured CSI has a significant difference. Hence, the LB-TDD scheme achieves better CSI reciprocity compared to the classical TDD scheme.

7 Practical Evaluation using USRP

A hardware testbed using USRP SDR platform was built to evaluate the performance of proposed scheme in a real environment.



(a) CSI obtained in JRNSO (b) CSI obtained in TDD

Fig. 12. CSI snapshots in the JRNSO and classical TDD schemes.

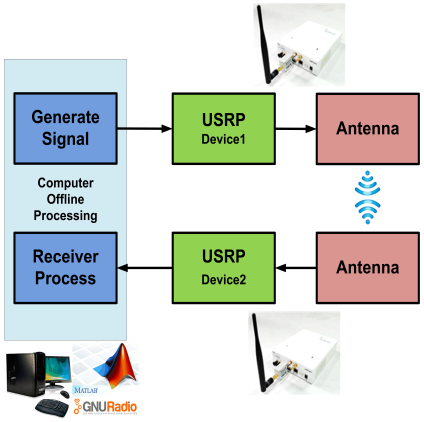


Fig. 13. Experimental setup.

7.1 Measurement Setup

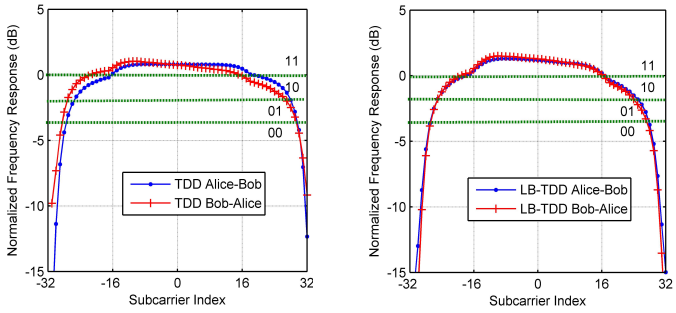
Two USRP N210 SDR platforms [56] were used as Alice and Bob, embedded with the CBX daughterboards with a carrier frequency range from 1.2 GHz to 6 GHz and a maximal bandwidth of 40 MHz. The experiments were carried out at the 2.4 GHz Industrial Scientific Medical (ISM) band. In LB-TDD schemes, we selected the Wi-Fi 2.4 GHz channel 1 (2.412 GHz) for Band 1 and channel 5 (2.432 GHz) for Band 2. Bandpass filters (Mini-Circuits, ZFBP-2400-s+, 2.3 GHz-2.5 GHz) were connected after the antennae in order to filter out-band interference.

The OFDM probing signal was generated in MATLAB and stored as a data stream file in the PC. We implemented the TDD and LB-TDD schemes using GNURadio software. The USRP receiver received the signal, which was transferred to the PC and processed by MATLAB. Our experimental setup is illustrated in Fig. 13, and key parameters of experimental setups are listed in Table 4.

We carried out extensive experiments in the laboratories at Southeast University, China under two scenarios, i.e., line-of-sight (LOS) and non-line-of-sight (NLOS). In LOS scenario, two USRP devices were placed in one room and close to each other. In NLOS scenario, two USRP devices were placed in two separated rooms with a distance of about 5 meters.

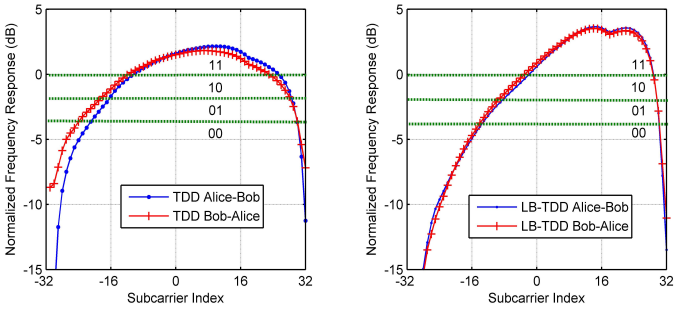
TABLE 4
Parameters for practical implementations

Parameters	Values
OFDM symbol length (with CP)	3.2 us
Subcarrier frequency spacing	390.625 KHz
Bandwidth	25 MHz
FFT size	64
Carrier frequency at band 1	2.412 GHz
Carrier frequency at band 2	2.432 GHz
Span for moving average filter (L)	30
Downsample factor (D)	2
Quantization threshold	(-4, -2, 0)
Quantization gap (q_g)	0.2



(a) TDD (b) LB-TDD

Fig. 14. CSI snapshots of Alice and Bob in the TDD and LB-TDD schemes in LOS scenarios.



(a) TDD (b) LB-TDD

Fig. 15. CSI snapshots of Alice and Bob in the TDD and LB-TDD schemes in NLOS scenario.

7.2 Experimental Results

7.2.1 *Performance Analysis*

As shown in Fig. 14 and Fig. 15, there are slight differences between the Alice's and Bob's CSI in both schemes, which will cause a key disagreement after quantization. It can be observed that the CSI mismatch in the LB-LDD scheme is reduced with the help of loop-back transmission.

Fig. 16 shows the KDR and KGR performance in LOS and NLOS scenarios. The LB-TDD scheme outperforms the classical TDD scheme in terms of both KDR and KGR. For the LB-TDD scheme, the averaged KDR is about 3.9×10^{-3} in the LOS and 7.9×10^{-3} in the NLOS scenarios. Moreover, both LB-TDD and TDD systems achieve better KDR performance but a little worse KGR in the LOS scenario compared to those in the NLOS scenario. This is mainly because Alice and Bob can obtain better reciprocal CSI in the LOS scenario,

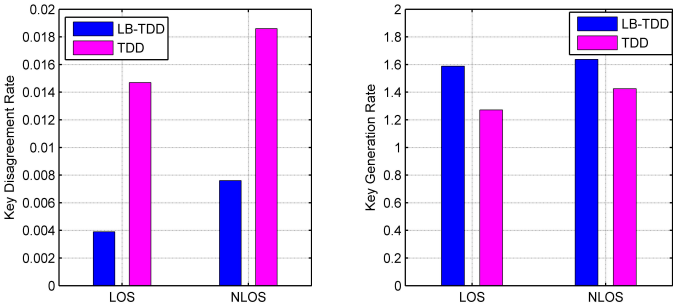


Fig. 16. KDR and KGR performance of LB-TDD and TDD schemes in real experiments.

but the multi-path effects are not as significant as those in the NLOS scenario.

7.2.2 Randomness Test and Discussion

The National Institute of Standards and Technology (NIST) random test suite [57] is widely adopted to evaluate the randomness of true-random and pseudo-random number generators. When the P-value test result is greater than the threshold usually chosen as 0.01, the sequence passes the test. Key generation is intrinsically a random number generator, so we also used the NIST test suite to evaluate the randomness of our generated key sequences.

Privacy amplification usually employs hash function. The output of the hash function is random/pseudo-random most of of the time. However, when the input is not random, it is subject to the dictionary attack and the attacker is likely to obtain the low-entropy key. Therefore, in this paper, we evaluate the randomness of the key sequence before carrying out the privacy amplification.

We evaluated the key randomness for systems with different downsample factors D for both our experimental and simulation data, which are shown in Table 5 and Table 6, respectively. The cells highlighted in light gray indicate a failure of the test. Since we are quantizing keys from the frequency domain, there is correlation between any two subcarriers within the coherence bandwidth. As shown in the tables, when the downsample factor $D = 16$ and $D = 128$, the key sequence generated from experimental and simulation data pass the NIST randomness tests, respectively, which indicates little correlation between these selected subcarriers. The downsample factors are different in the above two scenarios, because the channel conditions, namely, mulitpath levels, are different, which lead to different coherence bandwidth.

A larger downsample factor will select subcarriers with less correlation, which is beneficial for the randomness feature. On the other hand, large downsample factor will directly reduce the number of generated key bits because less subcarriers are kept for key extraction. An appropriate downsample factor, D, should be designed very carefully according to the channel condition in order to achieve a random yet fast key generation system.

8 Conclusions

A novel loop-back LB-TDD scheme has been proposed to enhance the channel reciprocity in secret key generation. We presented a new MB-PHY model with practical consideration of hardware fingerprint interference. An existing FDD loop-back scheme, namely JRNSO, was studied and a serious security risk was identified which did not apply to our proposed LB-TDD scheme. Through an extensive evaluation against passive eavesdropping and active MitM attack, the LB-TDD scheme was shown to be very secure and robust. In order to evaluate the performance of the proposed LB-TDD scheme, we prototyped our LB-TDD system, the classical TDD system and the JRNSO with an LTE model and undertook an extensive simulation and comparison. The LB-TDD system was shown to have a better performance in terms of security and channel reciprocity. Finally, we built a hardware evaluation system using the USRP SDR platform and verified our theoretical analyses using experimental results. Future work will focus on optimizations of the secret key generation method using CSI measurement in OFDM systems.

TABLE 5
NIST results of the experimental data with different downsample factor D

Test	D =2	D =4	D =8	D =16
Approx. Entropy	0	0.0066	0.0344	0.0832
Block Freq.	0	0.0132	0.0516	0.1359
Cum. Sums	0.0746	0.1083	0.0196	0.3241
DFT	0.0335	0.4851	0.0991	0.5536
Frequency	0.1470	0.0134	0.0923	0.0285
Longest Run of 1	0	0	0.0014	0.0854
Ranking	0.2919	0.2919	0.0249	0.2919
Runs	0	0.0480	0.0413	0.6185
Serial	0	0.0088	0.0416	0.0892
	0	0.0670	0.0604	0.8551

TABLE 6
NIST results of the simulation data with different downsample factor D

Test	D = 32	D = 64	D = 128	D = 256
Approx. Entropy	0	0.0116	0.0702	0.0987
Block Freq.	0.3842	0.1950	0.0983	0.6073
Cum. Sums	0.5219	0.4551	0.9112	0.8926
DFT	0.1468	0.0369	0.1317	0.4981
Frequency	0.0968	0.0905	0.0213	0.0320
Longest Run of 1	0	0	0.4160	0.1839
Ranking	0.0852	0.2919	0.2714	0.0391
Runs	0	0.0140	0.9778	0.7923
Serial	0	0.0144	0.0685	0.0997
	0	0.0178	0.8117	0.9101

Acknowledgments

This paper was presented in part at the IEEE International Conference on Communication and Telecommunications (ICCT 2017), Chengdu, China, Oct., 2017 [58]. This work was supported in part by National Key Basic Research Program of China (Chinese 973 Project 2013CB338003), National Natural Science Foundation of China (Grant No. 61571110, 61601114, 61602113) and Natural Science Foundation of Jiangsu Province (BK20160692).

REFERENCES

[1] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," IEEE Wireless Commun., vol. 18, no. 4, pp. 6–12, 2011.

[2] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," IEEE Trans. Mobile Comput., vol. 12, no. 5, pp. 917–930, 2013.

[3] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1779–1790, 2013.

[4] M. A. Tope and J. C. Mceachen, "Unconditionally secure communications over fading channels," in Proc. IEEE Military Communications Conference (Milcom'2001), Baltimore, MD, USA, Nov. 2001, pp. 54–58 vol.1.

[5] 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 Propag., vol. 53, no. 11, pp. 3776–3784, 2005.

[6] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," in Proc. IEEE International Conference on Ultra-Wideband, 2007, pp. 270–275.

[7] M. Stefer, M. Petermann, M. Schneider, D. Wbben, and K. D. Kammeyer, "Influence of non-reciprocal transceivers at 2.4 ghz in adaptive mimo-ofdm systems," in Proc. International Ofdm-Workshop, 2009.

[8] A. Bourdoux, B. Come, and N. Khaled, "Non-reciprocal transceivers in ofdm/sdma systems: impact and mitigation," in Proc. Radio and Wireless Conference, 2003, pp. 183–186.

[9] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," IEEE Trans. Mobile Comput., vol. 9, no. 1, pp. 17–30, 2009.

[10] G. Li, A. Hu, Y. Zou, and L. Peng, "A novel transform for secret key generation in time-varying tdd channel under hardware fingerprint deviation," in Proc. IEEE Vehicular Technology Conference (VTC'2015 fall), Boston, USA, Sep. 2016, pp. 1–5.

[11] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in Proc. ACM International Conference on Mobile Computing and Networking, San Francisco, CA, USA, sep 2008, pp. 116–127.

[12] T. C. W. Schenk and E. R. Fledderus, "Rf impairments in high-rate wireless systems - understanding the impact of tx/rx-asymmetry," in Proc. International Symposium on Communications, Control and Signal Processing, 2008, pp. 117–122.

[13] Y. Zou, O. Raeesi, R. Wichman, and A. Tolli, "Analysis of channel non-reciprocity due to transceiver and antenna coupling mismatches in tdd precoded multi-user mimo-ofdm downlink," in Proc. IEEE Vehicular Technology Conference (VTC'2014 fall), Vancouver, Canada, sep 2014, pp. 1–7.

[14] A. D. Wyner, "The wire-tap channel," Bell Labs Tech. J., vol. 54, no. 8, pp. 1355–1387, 2014.

[15] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," IEEE Trans. Inf. Theory, vol. 39, no. 4, pp. 1121–1132, 1993.

[16] ——, "Common randomness in information theory and cryptography. ii. cr capacity," IEEE Trans. Inf. Theory, vol. 44, no. 1, pp. 225–240, 1998.

[17] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in Proc. IEEE International Symposium on Information Theory, 2006, pp. 356–360.

[18] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470–2492, 2008.

[19] Z. Mao, C. E. Koksal, and N. B. Shroff, "Towards achieving full secrecy rate in wireless networks: A control theoretic approach," in Proc. Information Theory and Applications Workshop, 2011, pp. 1–8.

[20] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal mimo wireless channels: Measurement and analysis," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 381–392, 2010.

[21] F. Renna, M. R. Bloch, and N. Laurenti, "Semi-blind key-agreement over mimo fading channels," IEEE Trans. Commun., vol. 61, no. 2, pp. 620–627, 2013.

[22] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," IEEE Access, vol. 4, no. 3, pp. 614–626, 2016.

[23] A. Ghosal, S. Halder, and S. Chessa, "Secure key design approaches using entropy harvesting in wireless sensor network: A survey," Journal of Network and Computer Applications, vol. 78, pp. 216–230, 2017.

[24] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in Proc. ACM Conference on Computer and Communications Security, Alexandria, VA, USA, Oct. 2007, pp. 401–410.

[25] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in Proc. ACM International Conference on Mobile Computing and Networking, San Francisco, CA, USA, sep 2008, pp. 128–139.

[26] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in Proc. ACM International Conference on Mobile Computing and Networking, Beijing, China, Sep. 2009, pp. 321–332.

[27] J. Croft, N. Patwari, and S. K. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors," in Proc. International Conference on Information Processing in Sensor Networks, 2010, pp. 70–81.

[28] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in Proc. IEEE INFOCOM, San Diego, CA, USA, mar 2010, pp. 1–9.

[29] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Extracting secret key from wireless link dynamics in vehicular environments," in Proc. IEEE INFOCOM, Turin, Italy, Apr. 2013, pp. 2283–2291.

[30] H. Liu, J. Yang, Y. Wang, Y. J. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," IEEE Trans. Mobile Comput., vol. 13, no. 12, pp. 2820–2835, 2014.

[31] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in Proc. IEEE INFOCOM, Shanghai, China, Apr. 2011, pp. 1422–1430.

[32] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," IEEE Trans. Inf. Forensics Security, vol. 7, no. 5, pp. 1484–1497, 2012.

[33] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual ofdm subcarriers," IEEE Trans. Commun., vol. 64, no. 6, pp. 2578–2588, 2016.

[34] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, and Y. Ding, "Experimental study on channel reciprocity in wireless key generation," in Proc. IEEE 17th Int. Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Edinburgh, UK, jul 2016, pp. 1–5.

[35] M. Petermann, M. Stefer, F. Ludwig, D. Wubben, M. Schneider, S. Paul, and K. D. Kammeyer, "Multi-user pre-processing in multi-antenna ofdm tdd systems with non-reciprocal transceivers," IEEE Trans. Commun., vol. 61, no. 9, pp. 3781–3793, 2013.

[36] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in Proc. IEEE INFOCOM, Turin, Italy, Apr. 2013, pp. 3048–3056.

[37] S. J. Goldberg, Y. C. Shah, and A. Reznik, "Method and apparatus for performing jrnso in fdd, tdd and mimo communications," 2013.

[38] X. Wu, Y. Peng, C. Hu, H. Zhao, and L. Shu, "A secret key generation method based on csi in ofdm-fdd system," in Proc. IEEE GLOBECOM Workshops, Austin, Tx, USA, dec 2014, pp. 1297–1302.

[39] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 240–254, 2010.

[40] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer security in wireless communications," IEEE Access, vol. 4, no. 99, pp. 4464–4477, 2016.

[41] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," in Proc. European Symposium on Research in Computer Security, 2012, pp. 235–252.
[42] S. Im, H. Jeon, J. Choi, and J. Ha, "Secret key agreement with large antenna arrays under the pilot contamination attack," IEEE Trans. Wireless Commun., vol. 14, no. 12, pp. 6579–6594, 2015.
[43] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," IEEE Communications Letters, vol. 21, no. 4, pp. 961–964, 2017.
[44] A. Zhu, P. J. Draxler, J. J. Yan, T. J. Brazil, D. F. Kimball, and P. M. Asbeck, "Open-loop digital predistorter for rf power amplifiers using dynamic deviation reduction-based volterra series," IEEE Trans. Microw. Theory Techn., vol. 56, no. 7, pp. 1524–1534, 2008.
[45] J. Proakis and M. Saiehi, Digital Communications (Fifth Edition). McGraw-Hill Education, 2012.
[46] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," Acm Computing Surveys, vol. 45, no. 1, pp. 1–29, 2012.
[47] M. A. Jensen and J. W. Wallace, "A review of antennas and propagation for mimo wireless communications," IEEE Trans. Antennas Propag., vol. 52, no. 11, pp. 2810–2824, 2004.
[48] M. Edman and A. Kiayias, "On passive inference attacks against physical-layer key extraction," in Proc. European Workshop on System Security, 2011, pp. 1–6.
[49] B. Ai, G. E. Jian-Hua, Y. Wang, S. Y. Yang, P. Liu, and G. Liu, "Frequency offset estimation for ofdm in wireless communications," IEEE Trans. Consum. Electron., vol. 50, no. 1, pp. 73–77, 2004.
[50] J.-J. Van De Beek, O. Edfors, M. Sandell, S. K. Wilson, and P. O. Borjesson, "On channel estimation in ofdm systems," in Proc. IEEE Vehicular Technology Conference (VTC'95), 1995, pp. 815 – 819.
[51] M. Liu, M. Crussiere, and J. F. Helard, "A novel data-aided channel estimation with reduced complexity for tds-ofdm systems," IEEE Trans. Broadcast., vol. 58, no. 2, pp. 247–260, 2012.
[52] J. Zhang, S. K. Kasera, and N. Patwari, "Mobility assisted secret key generation using wireless link signatures," in Proc. IEEE INFOCOM, San Diego, CA, USA, mar 2010, pp. 1–5.
[53] A. Ambekar, M. Hassan, and H. D. Schotten, "Improving channel reciprocity for effective key management systems," in Proc. International Symposium on Signals, Systems, and Electronics, 2012, pp. 1–4.
[54] ITU, "Itu-r m.1225, guidelines for evaluation of radio transmission technologies for imt-2000," 1997.
[55] 3GPP, "3gpp tr 36.814 v9.0.0, physical layer aspects," Mar. 2010.
[56] "http://www.ettus.com/."
[57] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Applied Physics Letters, vol. 22, no. 7, pp. 1645–179, 2000.
[58] L. Peng, G. Li, and A. Hu, "Channel reciprocity improvement of secret key generation with loop-back transmissions," in Proc. IEEE 17th Int. Conf. Communication Technology (ICCT), Chengdu, China, Oct. 2017, pp. 193–198.

Linning PENG received his PhD degrees from IETR (Electronics and Telecommunications Institute of Rennes) laboratory at INSA (National Institute of Applied Sciences) of Rennes, France, in 2014. From 2014, he has been a research associate with Southeast University, China. His research interests include Internet of Things, physical layer security in wired and wireless communications.

Guyue LI received the B.S. degree in Information Science and Technology and the Ph.D. degree in Information Security from Southeast University, Nanjing, China, in 2011 and 2016, respectively. She is currently a Lecturer at Southeast University. Her research interests include physical layer security, beamforming, artificial noise and blind source separation.

Junqing ZHANG received the B.Eng and M.Eng degrees in Electrical Engineering from Tianjin University, China in 2009 and 2012, respectively, and the Ph.D degree in Electronics and Electrical Engineering from Queen's University Belfast, UK in 2016. From Feb. 2016 to Jan. 2018, he was a Postdoctoral Research Fellow with Queen's University Belfast, UK. Since Feb. 2018, he has been a Tenure Track Fellow with University of Liverpool, UK. His research interests include Internet of Things, wireless security, physical layer security and key generation.

Roger WOODS (M'95-SM'01) received the B.Sc degree (Hons.) in Electrical and Electronic Engineering and the Ph.D. degree from the Queen's University of Belfast in 1985 and 1990, respectively. He is currently a Full Professor with Queen's University of Belfast, and Research Director of the Electronics and Computer Engineering cluster. His research interests are in accelerated data analytics and heterogeneous programmable systems for signal processing and wireless communication systems. He holds 4 patents and has authored over 220 papers. He is a member of the IEEE Signal Processing and Industrial Electronics Societies and is on the Advisory Board for the IEEE SPS Technical Committee on the Design and Implementation of Signal Processing Systems.

Ming LIU received the B.Eng. and M.Eng. degrees from Xi'an Jiaotong University, China, in 2004 and 2007, respectively, and the Ph.D. degree from the National Institute of Applied Sciences (INSA), Rennes, France, in 2011, all in Electrical Engineering. He was with the Institute of Electronics and Telecommunications of Rennes (IETR) as a postdoctoral researcher from 2011 to 2015. He is now with Beijing Jiaotong University, China, as an Associate Professor. His main research interests include massive MIMO, space-time coding and physical layer security.

Aiqun HU received the PhD degree from Southeast University, Nanjing, China in 1993. He is a Full Professor at Southeast University. His research interests are in wireless network technology and physical layer security of wireless communications. He has published extensively in high quality transactions and Chinese top level journals, and holds numerous patents in wireless technology.