A Secret Key Generation Method Based on CSI in OFDM-FDD System

Xiaohua Wu*, Yuexing Peng*, Chunjing Hu*, Hui Zhao*and Lei Shu†

* Key Laboratory of Universal Wireless Communication, Ministry Education

Beijing University of Posts and Telecommunications, Beijing China, 100876

Email: { wxhbupt, victor.pen} @gmail.com, { hucj, hzhao} @bupt.edu.cn

†Guangdong Petrochemical Equipment Fault Diagnosis Key Lab,

Guangdong University of Petrochemical Technology, 525000 Guangdong, China

Email: lei.shu@lab.gdupt.edu.cn

***Abstract*—Channel reciprocity is an inherent feature of time division duplex (TDD) system while in frequency division duplex (FDD) system it is limited due to different frequencies being used for the uplink and the downlink. As a consequence, channel reciprocity-based secret generating methods used in TDD systems cannot be applied directly to FDD systems. In this paper, we present a novel secret key generation method for FDD system, for which the communication pair estimate the channel state information (CSI) of the same time in the uplink by a specially designed forwarding strategy and generate the secret key from the CSI estimates. Numerical simulations are implemented to verify the effectiveness of the proposed method.**

***Index Terms*—channel state information, FDD system, Physical-layer security, secret key generation.**

I. Introduction

Due to the inherently shared nature of the wireless medium, the security of the wireless communication network is threatened by eavesdropping, modifying, and impersonating. To protect the confidentiality, integrity, and authenticity of the communication, secret keys must be established for securing wireless networks. Traditional establishment of cryptographic key is addressed above the physical layer. However, with the emergence of decentralized networks, higher-layer security techniques, such as Authentication and Key Agreement security protocol used in third-generation mobile system, are complex and difficult to implement. Therefore, many researchers pay attention to study the fundamental ability of the physical layer to provide secure wireless communications, which is known as physical layer security[1].

Researchers have found that the legitimate terminals could generate secret keys by this way [2][3]: communication pair could observe a common random source which is inaccessible to an eavesdropper, then they generate a common secret key based on their dependent observations after mutual communication over a public error-free channel since their observations are dependent but not identical due to the observation noise. The eavesdropper may observe the transmissions on the public channel, but will not get any useful information about secret key generated by the legitimate terminals.

In wireless network, this common random source could be the wireless fading channel, that is, the communication pair could share the same CSI and generate a common secret key from the shared CSI when the channel measurement is done within the channel coherent time. The shared CSI in TDD system would not be leaked to the third part due to its following characteristics:

- Reciprocity: The properties of the channel (e.g., fadings, phase shifts, and delays) are the same for both uplink and downlink in any time.
- Randomness: The multipath channel changes both in time domain and frequency domain, that is channel not only changes over time, but also changes with carrier frequency.
- Privacy: The multipath properties of the radio channel are unique to the locations of the two nodes of the link. An eavesdropper at a third location more

978-1-4799-2851-4/13/$31.00 ©2013IEEE

than a few wavelengths from either node will measure a different and uncorrelated radio channel [4].
Based on these characteristics of channel, many secret key generation methods have been proposed for TDD systems [5]-[7].

However, in FDD system, since the uplink and the downlink are allocated with different frequencies, the channel impulse response (CIR) of uplink and downlink are no longer reciprocal as that in the TDD system. Therefore, the features of CSI used in [5]-[7] to generate secret key could not be directly used in FDD system. Recently, several methods have been developed for FDD systems [8][9]. In [8] a secret key generation method is proposed by utilizing the angle and delay which are believed to hold the reciprocity in FDD systems. However, the angle of path is very hard to estimate reliably, and the agreement ratio of the secret key is around 10^{-3} even in high signal-to-noise ratio (SNR) condition, which is not good enough for practical applications. In [9], the secret key generation method termed JRNSO (Joint Randomness Not Shared by Others) and a loop back approach is proposed for FDD systems. It utilizes a sequence of private pilots which are known only by the transmitter, and these pilots are fed back without any processing after the receiver received it from the transmitter. Through the loop back approach both the two legitimate terminals can estimate the CIR of the combinatorial channel which is the combination of uplink and downlink. If the loop back time is short enough, the CIR of the combinatorial channel hold reciprocity, then the secret key can be generated. A special JRNSO period is allocated to generate the secret key and is separated from the data transmission periods with enough time gap. In order to avoid the leakage of CIR information, the time gap between the JRNSO period and data transmission period should be more than channels coherent time which degrades spectrum efficiency greatly.

In this paper, a novel secret key generation method is proposed for OFDM-FDD systems. In the proposed method, only the uplink CSI of the same time, instead of the CIR of the combinatory channel, is estimated by both the user equipment (UE) and the base station (BS) through a specially designed forwarding method. In short, our contribution is summed up as below.

1) A novel physical-layer security method is proposed for FDD systems, which generates secret key with high agreement ratio and no leakage to the third one.

2) A special CSI probing method is proposed to estimate the uplink CSI of the same time by both the UE and the BS. The common CSI eases the generation of the common secret key with low complexity.

3) The proposed method flexibly supports all kinds of application scenarios, such as single- or multiple-antenna configuration, low-to-high moving speed, all kinds of multiple access schemes though OFDM is taken as an example to introduce the proposed method.

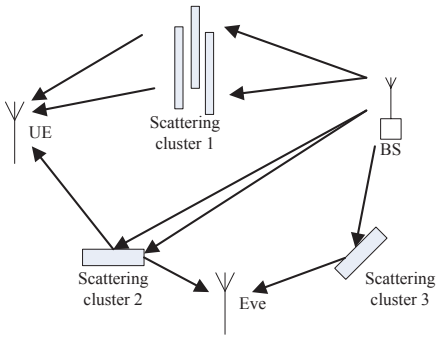

Fig. 1: The system model.

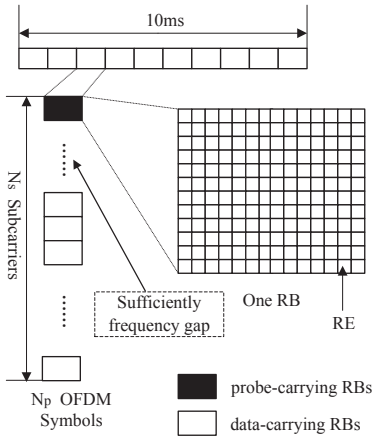

Fig. 2: FDD-OFDM frame structure.

The rest of the paper is organized as followed. The system model is introduced in Section II. The secret key generation method we proposed is presented in detail in Section III. In Section IV, numerical simulation is implemented to verify the performance of the proposed method, and we conclude the paper in Section V.

II. System Model

We consider an OFDM system with FDD mode where a legitimate UE communicates with the BS while a passive eavesdropper, Eve, tries to eavesdrop, which is shown in Figure 1.

As illustrated in Fig. 2, the N_s subcarriers are grouped into two types of resource blocks (RBs): the data-carrying RBs and the probe-carrying RBs. In the uplink, the UE transmit signal $\boldsymbol{X_{UE}}$ to the BS with working frequency f_{UL} , meanwhile the BS broadcasts

$\boldsymbol{X_{BS}}$ with working frequency f_{DL}. The received signals at the t-th OFDM symbol and the j-th subcarrier at the BS and the UE are shown as

$$R_{BS}(t,j) = H_{UL}(t,j)X_{UE}(t,j) + Z_{UL}(t,j) \quad (1)$$

$$R_{UE}(t,j) = H_{DL}(t,j)X_{BS}(t,j) + Z_{DL}(t,j) \quad (2)$$

where $H_{UL}(t,j)$ and $H_{DL}(t,j)$ are the channel frequency response (CFR) in the uplink and the downlink, respectively. $Z_{UL}(t,j)$ and $Z_{DL}(t,j)$ are the complex white Gaussian noise with zero mean and variance σ^2. If $X_{UE}(t,j)$ and $X_{BS}(t,j)$ are pilot symbols, the BS and the UE can obtain the CFR by channel estimation (CE) method as

$$\widehat{H}_{UL}(t,j) = H_{UL}(t,j) + \widehat{Z}_{UL}(t,j) \quad (3)$$

$$\widehat{H}_{DL}(t,j) = H_{DL}(t,j) + \widehat{Z}_{DL}(t,j) \quad (4)$$

where $\widehat{Z}_{UL}(t,j)$ and $\widehat{Z}_{DL}(t,j)$ are the CE errors.

The CSI is usually used to generate secret key on the base that the CSI holds reciprocity between UL (uplink) and DL (downlink). In order to evaluate the reciprocity of the CSI, we resort to the metrics of correlation coefficient of CSI. The correlation coefficient of the real part of the CFR is defined as [10]

$$\rho_{Hr}(\Delta t, \Delta f) = \frac{J_0(2\pi f_m \Delta t)}{\sqrt{1 + (2\pi\tau_{rms}\Delta f)^2}} \quad (5)$$

where $J_0(\cdot)$ is the first kind zero-order modified Bessel function, f_m is the maximum Doppler shift, Δt is the time deviation, Δf is the frequency deviation, and τ_{rms} is the rooted mean squared (rms) delay spread of channel.

Taking the CE error into consideration, the correlation coefficient of the real part of the CFR estimate is given by

$$\rho_{\widehat{H}r}(\Delta t, \Delta f) = \frac{J_0(2\pi f_d \Delta t)}{(1 + \frac{1}{SNR})\sqrt{1 + (2\pi\tau_{rms}\Delta f)^2}} \quad (6)$$

Traditionally the frequency gap between UL and DL is 190MHz, which is much larger than the coherence bandwidth. Thus reciprocity of CSI between the UL and the DL does not exist anymore for FDD systems.

III. Secret Key Generation Method For OFDM-FDD Systems

In this section we detail the proposed method to generate secret key for FDD systems based on a specially designed CSI probing scheme. The flow chart of the proposed method is illustrated in Fig. 3, which mainly contains four steps: channel information estimation, feature extraction, quantization, and information reconciliation.

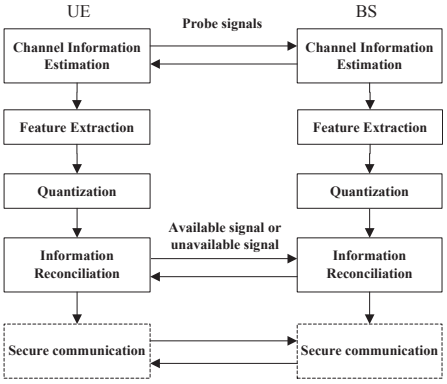

Fig. 3: Procedure of the proposed secret key generation in OFDM-FDD systems.

A. Channel Information Estimation

In order to obtain the UL channel information, both the UE and the BS transmit private probe signals, which are known only by the transmitter itself and only carried by probe-carrying RBs. What's more, the private probe signals should be placed as close as possible. The private probe signals transmitted by the BS are expressed by

$$X_{BS} = e^{j\theta}, \theta \sim U(-\pi, \pi) \quad (7)$$

Accordingly, the received signals at the UE can be written as

$$R_{UE1}(t_1, j) = e^{j\theta}H_{DL}(t_1, j) + n_{DL}(t_1, j) \quad (8)$$

At receiving probe signals from the BS, the UE forwards not only $R_{UE1}(t_1, j)$ and the conjugate of $R_{UE1}(t_1, j)$, but also its own private probe signals. These three signals can be expressed as

$$F_{UE1} = e^{j\theta}H_{DL}(t_1, j) + n_{DL}(t_1, j) \quad (9)$$

$$F_{UE2} = e^{-j\theta}H^*_{DL}(t_1, j) + n^*_{DL}(t_1, j) \quad (10)$$

$$X_{UE} = e^{j\varphi}, \varphi \sim U(-\pi, \pi) \quad (11)$$

It is worthy to note that these three signals are carried by the same RB, and they would be placed as close as possible. The received signals at the BS are then expressed as

$$\begin{aligned} R_{BS1}(t_2, k) = {} & e^{j\theta}H_{DL}(t_1, j)H_{UL}(t_2, k) \\ & + n_{DL}(t_1, j)H_{UL}(t_2, k) + n_{UL}(t_2, k) \end{aligned} \quad (12)$$

$$\begin{aligned} R_{BS2}(t_2, l) = {} & e^{-j\theta}H^*_{DL}(t_1, j)H_{UL}(t_2, l) \\ & + n^*_{DL}(t_1, j)H_{UL}(t_2, l) + n_{UL}(t_2, l) \end{aligned} \quad (13)$$

$$R_{BS3}(t_2, m) = e^{j\varphi}H_{UL}(t_2, m) + n_{UL}(t_2, m) \quad (14)$$

Similarly the BS forwards the signal $R_{BS3}(t_2, m)$ and the conjugate of $R_{BS3}(t_2, m)$, and the UE receives the following signals

$$\begin{aligned} R_{UE2}(t_3, x) &= e^{j\varphi} H_{UL}(t_2, m) H_{DL}(t_3, x) \\ &\quad + n_{UL}(t_2, m) H_{DL}(t_3, x) + n_{DL}(t_3, x) \end{aligned} \tag{15}$$

$$\begin{aligned} R_{UE3}(t_3, y) &= e^{-j\varphi} H^*_{UL}(t_2, m) H_{DL}(t_3, y) \\ &\quad + n^*_{UL}(t_2, m) H_{DL}(t_3, y) + n_{DL}(t_3, y) \end{aligned} \tag{16}$$

After receiving forwarded probe signals, both the UE and the BS estimate the combinatorial CFR as below

$$\begin{cases} H_1^{UE}(t_3, x) = H_{UL}(t_2, m) H_{DL}(t_3, x) \\ \qquad\qquad + W_1^{UE}(t_3, x) \\ H_2^{UE}(t_3, y) = H^*_{UL}(t_2, n) H_{DL}(t_3, y) \\ \qquad\qquad + W_2^{UE}(t_3, y) \end{cases} \tag{17}$$

$$\begin{cases} H_1^{BS}(t_2, k) = H_{DL}(t_1, j_1) H_{UL}(t_2, k) \\ \qquad\qquad + W_1^{BS}(t_2, k) \\ H_2^{BS}(t_2, l) = H^*_{DL}(t_1, j_2) H_{UL}(t_2, l) \\ \qquad\qquad + W_2^{BS}(t_2, l) \end{cases} \tag{18}$$

where $W_1^{UE}(t_3, x)$, $W_2^{UE}(t_3, y)$, $W_1^{BS}(t_2, k)$ and $W_2^{BS}(t_2, l)$ are CE errors.

B. Feature Extraction

We assume that x and y are close enough, then $H_{DL}(t_3, x)$ and $H_{DL}(t_3, y)$ are approximately the same, and both UE and BS can estimate the uplink CFR by the following method.

$$\begin{aligned} H_{UL}^{UE}(t_3, x) &= \frac{H_1^{UE}(t_3, x)}{H_2^{UE}(t_3, y)} \\ &= \frac{H_{UL}(t_2, m)}{H^*_{UL}(t_2, n)} + W_{UE}(t_3, x) \end{aligned} \tag{19}$$

$$\begin{aligned} H_{UL}^{BS}(t_2, k) &= \frac{H_1^{BS}(t_2, k)}{H_2^{BS*}(t_2, l)} \\ &= \frac{H_{UL}(t_2, k)}{H^*_{UL}(t_2, l)} + W_{BS}(t_2, k) \end{aligned} \tag{20}$$

If k, l, m, n are close enough too, then $H_{UL}(t_2, k)$, $H_{UL}(t_2, l)$, $H_{UL}(t_2, m)$ and $H_{UL}(t_2, n)$ are also approximately the same, Thus both the UE and the BS obtain the noisy estimate of the uplink CSI as bellow.

$$\begin{aligned} \widehat{H}_{UL}^{UE}(t_3, x) &= \sqrt{H_{UL}^{UE}(t_3, x)} \\ &= \frac{H_{UL}(t_2, m)}{|H_{UL}(t_2, m)|} + Z_{UE}(t_3, x) \end{aligned} \tag{21}$$

$$\begin{aligned} \widehat{H}_{UL}^{BS}(t_2, k) &= \sqrt{H_{UL}^{BS}(t_2, k)} \\ &= \frac{H_{UL}(t_2, m)}{|H_{UL}(t_2, m)|} + Z_{BS}(t_2, k) \end{aligned} \tag{22}$$

where $Z_{UE}(t_3, x)$ and $Z_{BS}(t_2, k)$ are the independent estimation noise.

To reduce noises negative effect on CE, N private probe signals are transmitted within a RB, and N UL CSI estimates are obtained which are highly correlated. Stack the N UL CSI estimates into a vector and omit the time and subcarrier index for brevity, and we arrive at

$$\boldsymbol{H^{UE}} = [\widehat{H}_{UL}^{UE-1}, \widehat{H}_{UL}^{UE-2}, \cdots, \widehat{H}_{UL}^{UE-N})] \tag{23}$$

$$\boldsymbol{H^{BS}} = [\widehat{H}_{UL}^{BS-1}, \widehat{H}_{UL}^{BS-2}, \cdots, \widehat{H}_{UL}^{BS-N}] \tag{24}$$

C. Quantization

Firstly the real part and imaginary part of UL CSI are separated as below.

$$UE: \begin{cases} \boldsymbol{H_r^{UE}} = real(\boldsymbol{H^{UE}}) \\ \boldsymbol{H_i^{UE}} = imag(\boldsymbol{H^{UE}}) \end{cases} \tag{25}$$

$$BS: \begin{cases} \boldsymbol{H_r^{BS}} = real(\boldsymbol{H^{BS}}) \\ \boldsymbol{H_i^{BS}} = imag(\boldsymbol{H^{BS}}) \end{cases} \tag{26}$$

Then quantization is implemented to get the quantization bits.

$$UE: \begin{cases} Q_r^{UE} = Q\left(\boldsymbol{H_r^{UE}}\right) \\ Q_i^{UE} = Q\left(\boldsymbol{H_i^{UE}}\right) \end{cases} \tag{27}$$

$$BS: \begin{cases} Q_r^{BS} = Q\left(\boldsymbol{H_r^{BS}}\right) \\ Q_i^{BS} = Q\left(\boldsymbol{H_i^{BS}}\right) \end{cases} \tag{28}$$

where

$$Q(\boldsymbol{x}) = \begin{cases} 1, & \text{not less than } L \text{ components in } \boldsymbol{x} \\ & \text{whose amplitudes are above } q_+ \\ 0, & \text{else} \\ -1, & \text{not less than } L \text{ components in } \boldsymbol{x} \\ & \text{whose amplitudes are below } q_- \end{cases} \tag{29}$$

D. Information Reconciliation

To generate a common secret key, reconciliation is necessary. Firstly the UE checks its quantized bits. If both Q_r^{UE} and Q_i^{UE} are not zero, an available signal (e.g., 1) is sent to the BS. Otherwise an unavailable signal (e.g., 0) is sent. The BS performs the same process.

When available signal is received, quantized bits are mapped to secret key. One example of the mapping is illustrated in Table I.

TABLE I: One example of secret key mapping rule

Quantized bit	Secret key
1	1
-1	0

TABLE II: Parameters for the simulated OFDM system

Parameter	Value
OFDM symbol: Ts	71.4us
No. OFDM symbol per frame	14
Carrier frequency	UL:1.8GHz, DL:2.0GHz
Bandwidth: BW	10 MHz
Subcarrier interval	15 kHz
FFT size	1024
Vehicle speed	60, 120, 180 km/h
Channel estimation:	Least Square (LS)
Threshold:	q_+=0.3/0.5, q_-=-0.3/-0.5;
Channel model: 3GPP Veh. A [12]	Relative delay (ns): 0, 310, 710, 1090, 1730, 2510
	Average power (dB): 0, -1, -9, -10, -15, -20

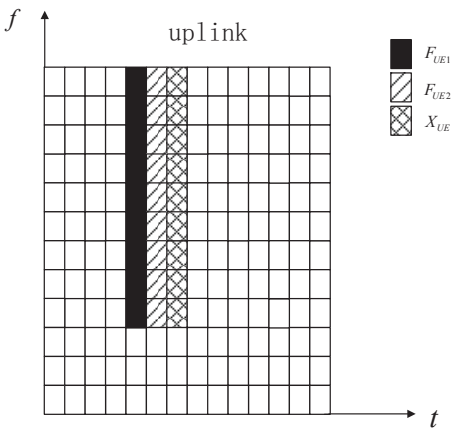

Fig. 4: Structure of RBs carrying prob signals.

IV. Simulation Results

The simulated OFDM-FDD system is the 3G-LTE system [11] whose main parameters are listed in Table II. ITU Veh. Type A [12] is adopted. The probe-carrying RB structure is shown in Fig. 4. In order to assure the CFR at the probe-carrying RBs fades independently from that at the data-carrying RBs, frequency gap of 5 RBs between these two types of RBs is set in the simulation, which results in the correlation coefficient of these two RBs being less than 0.3.

In Fig. 5 we present the secret key disagreement ratio between the BS and the UE when the vehicle speed is 60 km/h. From the figure we can see that the secret key disagreement ratio declines with the increase of L and q_+ and the decrease of q_-, and it can be less than 10^{-4} in high SNR.

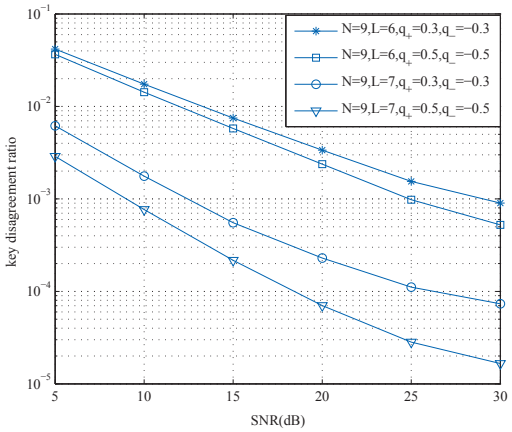

Fig. 5: Secret key disagreement ratio when vehicle speed is 60 km/h.

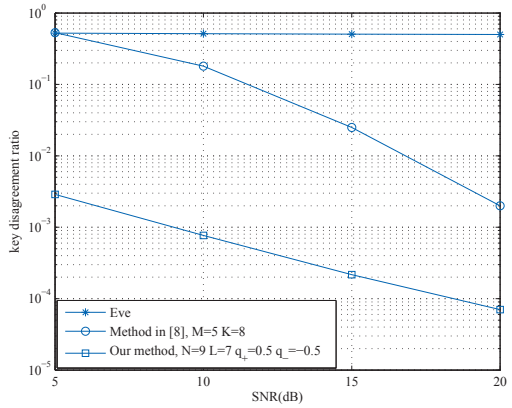

Fig. 6: Secret key disagreement ratio compared with proposed method and Eve.

Fig. 6 presents the secret key disagreement ratio compared with the reference method proposed in [8], where the performance at Eve is also presented. Simulation results show that our method outperforms the reference method, and Eve cannot obtain any information about the secret key.

In Fig. 7 the secret key bit rate is presented when the vehicle speed is 60 km/h. Though the secret key bit rate reduces with the increase of L and q_+ and the decrease of q_-, it is still acceptable. Clearly, more RBs are used, larger secret key bit rate can be achieved.

Fig. 8 presents the secret key disagreement ratio performance versus vehicle speed. From the curves the performance degrades gently with the increase of vehicle speed, which shows our method supports well high vehicle speed.

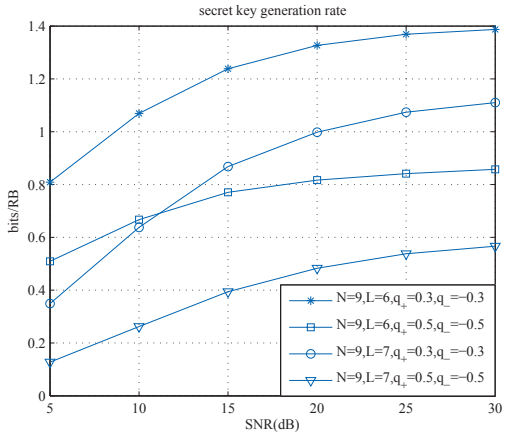

Fig. 7: Secret key generation rate when the vehicle speed is 60 km/h.

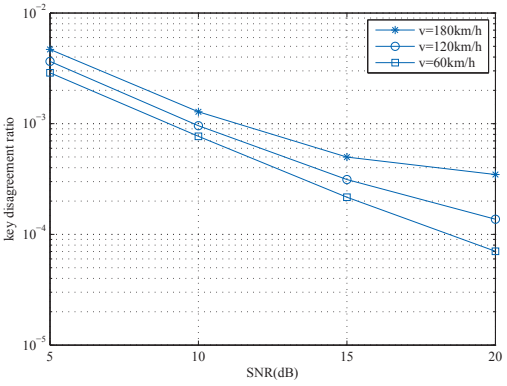

Fig. 8: Secret key disagreement ratio with different vehicle speeds (N=9, L=7, q_+=0.5, q_-=-0.5).

V. Conclusion

In FDD system the reciprocity of the CSI does not exist, and thus the CSI-based secret key generation methods, which work pretty well in TDD systems, cannot directly apply in FDD systems. In this paper, a novel secret key generation method is proposed for FDD systems by exploiting the uplink CSI of the same time, which is achieved by specially designed CSI probing scheme. Simulation results show the proposed method achieves high consistency and flexible support of high vehicle speed with low complexity.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 61171106, National Key Technology R&D Program of China under Grant 2012ZX03-004-001, and the fundamental research funds for the central universities.

References

[1] Debbah, M., E. Hesham, P. H. Vincent, and S. Shlomo, "Editorial:Wireless physical layer security," *Eurasip Journal on WirelessCommunications and Networking*, Vol. 2009, 2009.

[2] Maurer, U.M., "Secret key agreement by public discussion from common information," *Information Theory, IEEE Transactions on* , vol.39, no.3, pp.733-742, May 1993.

[3] Ahlswede, R.; Csiszar, I., "Common randomness in information theory and cryptography. I. Secret sharing," *Information Theory, IEEE Transactions on* , vol.39, no.4, pp.1121-1132, Jul 1993.

[4] G. D. Durgin. Space-Time Wireless Channels. Prentice Hall PTR, 2002.

[5] Chunxuan Ye; Reznik, A.; Shah, Y., "Extracting Secrecy from Jointly Gaussian Random Variables," *Information Theory, 2006 IEEE International Symposium on* , vol., no., pp.2593,2597, 9-14 July 2006.

[6] Patwari, N.; Croft, J.; Jana, S.; Kasera, S.K., "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements," *Mobile Computing, IEEE Transactions on* , vol.9, no.1, pp.17-30, Jan. 2010

[7] S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, "Radiotelepathy: Extracting a secret key from an unauthenticated wireless channel," *Proc. ACM Conf. Mobile Comput. Network.*, Sept. 2008.

[8] Wang W J, Jiang H Y, Xia X G, et al. A wireless secret key generation method based on Chinese remainder theorem in FDD systems. Sci China Inf Sci, 2012, 55: 1605C1616.

[9] Goldberg S J, Shah Y C, Reznik A. METHOD AND APPARATUS FOR PERFORMING JRNSO IN FDD, TDD AND MIMO COMMUNICATIONS: U.S. Patent Application 12/106,926[P]. 2008-4-21.

[10] Lee W C. Mobile communications engineering [M]. McGraw-Hill Professional, 1982.

[11] 3GPP TR 36.814 v1.4.1, Physical layer aspects (Release 9), Sept., 2009.

[12] ITU-R M.1225, Guidelines for evaluation of radio transmission technologies for IMT-2000, 1997.