SECRET KEY GENERATION SCHEME BASED ON DEEP LEARNING IN FDD MIMO SYSTEMS

Zheng WAN†, Kaizhi HUANG†, Nonmembers, and Lu CHEN†, Member

SUMMARY In this paper, a deep learning-based secret key generation scheme is proposed for FDD multiple-input and multiple-output (MIMO) systems. We built an encoder-decoder based convolutional neural network to characterize the wireless environment to learn the mapping relationship between the uplink and downlink channel. The designed neural network can accurately predict the downlink channel state information based on the estimated uplink channel state information without any information feedback. Random secret keys can be generated from downlink channel responses predicted by the neural network. Simulation results show that deep learning based SKG scheme can achieve significant performance improvement in terms of the key agreement ratio and achievable secret key rate.

key words: physical layer security, secret key generation, deep learning, FDD MIMO systems

1. Introduction

Secret key generation (SKG) based on wireless channel characteristics has attracted wide attention recently, which is considered one of the key technologies in the next generation wireless systems to safeguard data confidentiality. Compared to the public-key cryptography based on the computational security, physical layer secret keys generated from wireless channels have the potential to achieve information-theoretic security. Based on the reciprocity, spatial decorrelation and temporal variation of wireless channels, two legitimate users can obtain real-time updated secret keys through the steps of channel estimation, quantization, information reconciliation and privacy amplification [1]. Currently, most of the secret key generation studies focus on the time division duplex (TDD) system, while frequency division duplex (FDD) systems are widely deployed in mobile communications due to advantages of low latency, strong anti-interference capabilities and wide-area coverage. The reciprocity of wireless channels is no longer hold since the uplink channel and the downlink channel experience different fading in FDD systems. As a result, most reciprocal shared random sources used in TDD systems, such as received signal strength, channel impulse response and channel frequency response, are completely different between the uplink channel and downlink channel in FDD systems.

Several research works have been conducted to solve the above problems. First, spatial reciprocity between the uplink and downlink channel has been applied to explore new shared parameters [2], [3]. In [2], frequency-independent spatial parameters of each path were extracted, such as angle and delay, to generate shared keys. In [3], considering the statistical channel reciprocity based on the channel covariance in the angular domain, secret keys were generated from channel covariance matrix eigenvectors. Besides spatial reciprocity-based SKG schemes, another line of research was establishing a joint reciprocal shared random source using loop-back mechanism [4], [5]. In [4], the reciprocal composite channel gains were extracted through two rounds of channel sounding. In [5], the uplink channel state information (CSI) was estimated by two legitimate terminals. Furthermore, loop-back mechanism-based SKG schemes have been proved to be insecure because eavesdroppers can passively eavesdrop on confidential information through the attack strategy proposed in [6].

In this paper, we propose a novel deep learning based secret key generation scheme for FDD MIMO systems. Our main contributions are summarized as follows:

(1) A novel deep learning SKG scheme for FDD MIMO systems is proposed. This scheme diverts the computing overhead to the base station (BS) side. Compared with the existing SKG schemes, this scheme does not require high computational operations and is suitable for low-power terminals.

(2) An encoder-decoder based convolutional neural network (CNN) model is designed, which is driven by CSI data instead of relying on accurate wireless channel models. This neural network can learn the mapping relationship between the uplink and downlink channel to predict downlink CSI accurately.

(3) A complete secret key generation procedure is designed for FDD MIMO systems. Compared with the existing SKG solutions, this scheme can achieve significant performance improvement in terms of secret key agreement ratio and achievable secret key rate.

2. System Model

Considering a single-cell FDD MIMO system, where BS
equipped with $M$ antennas serves multiple user equipment (UE) deployed with a single antenna. Meanwhile, there is a passive eavesdropper Eve around UE trying to eavesdrop. In fact, other users are also treated as potential eavesdroppers. Assuming that Eve is more than several half wavelengths away from the legitimate user. Thus, the legitimate channel and eavesdropping channel are independent. The orthogonal frequency-division multiplexing (OFDM) modulation is employed with $N$ sub-carriers. The channel response $\mathbf{H}$ is a two-dimensional complex matrix of $N \times M$, i.e., $\mathbf{H} \in \mathbb{C}^{N \times M}$.

According to [7], [8], the uplink and downlink channels share the same propagation environment and the underlying physical paths are the same. Therefore, there is an inherent mapping relationship between uplink and downlink channel [9]. Nevertheless, the actual wireless channel tends to be much more complicated and the mapping relationship between uplink and downlink channel is difficult to be expressed by existing mathematical tools. Therefore, we approximate the mapping function by leveraging universal function approximate ability of deep learning [10], which is driven by CSI data instead of relying on accurate wireless channel models.

3. Deep Learning Based SKG Scheme in FDD MIMO Systems

In this section, we elaborate on the deep learning based secret key generation scheme for FDD MIMO systems. This scheme mainly includes four steps, the BS and UE can generate identical secret key streams after these four steps.

3.1 CNN Model Design

Considering that the output and input dimensions of the neural network are the same, we design a encoder-decoder architecture-based convolutional neural network model for uplink to downlink mapping, as shown in Fig. 1. The input of the CNN is uplink channel state information (UL-CSI), downlink channel state information (DL-CSI) predicted by the neural network can be written as

$$\hat{\mathbf{H}}_d = f_{\text{pre}} (f_{\text{ex}} (\mathbf{H}_u; \Psi_{\text{En}}); \Psi_{\text{De}})$$

where $\Psi = \{\Psi_{\text{En}}, \Psi_{\text{De}}\}$ represents the parameters in encoder and decoder module. $f_{\text{ex}}$ and $f_{\text{pre}}$ denote a cascade of the nonlinear transformation of encoder and decoder, respectively. The encoder utilizes a fully convolutional network to extract environmental information from UL-CSI. Specifically, the encoder consists of three modules, each of them containing two sequential Conv-BN-Relu-Maxpool blocks. Conv indicates a 3 × 3 convolution layer with stride 1, BN is batch normalization [10] used to increase the generalization capability of the model. Relu is Rectified linear unit activation function and Maxpool represents a $2 \times 2$ max-pooling layer. To avoid the overfitting of neural networks, the dropout technology is adopted in the final layer of the encoder. Then, the decoder converts the extracted features to predict DL-CSI through up-sampling. Specifically, the decoder consists of a transposed convolution layer and two sequential convolution layer. After multiple transposed convolutions, the spatial resolution of the feature map is restored. Two convolutional layers are used to make the sparse feature map after up-sampling more dense. Finally, a kernel of size 1 × 1 is used in the final convolutional layer to obtain the same dimensional output as the DL-CSI.

3.2 CNN Model Training

Before off-line training, the BS and UE send public pilots to each other to estimate channel responses $\hat{\mathbf{H}}$ by the least square algorithm. Then, the UE feeds back DL-CSI $\hat{\mathbf{H}}_d$ to BS. After collecting a sufficient amount of CSI data in different coherence time, the BS takes UL-CSI $\hat{\mathbf{H}}_u$ as input and DL-CSI $\hat{\mathbf{H}}_d$ as output to train the neural network. Note that CSI matrix is complex valued matrix, we deem it as a real valued matrix with two channels, in which the real values are put in the first channel and the imaginary values in the second channel.

The error back propagation algorithm is employed to train the neural network. For a regression task, the mean squared error (MSE) is used as the loss function to minimize the difference between $\hat{\mathbf{H}}_d$ and $\hat{\mathbf{H}}_d$, which is given by

$$\text{Loss}(\phi) = \frac{1}{K} \sum_k \|\hat{\mathbf{H}}_d - \mathbf{H}_d\|_2^2$$

where $K$ and operation $\|\|_2$ denote the number of training samples in one batch and Euclidean norm, respectively. The adaptive moment estimation optimizer is employed to reversely learn and revise the weight parameters in the network layer by layer until the neural network converges.

3.3 DL-CSI Prediction Based on the Estimated UL-CSI

In the on-line prediction stage, the parameters of pre-trained network model have been fixed. The UE only send one uplink public pilot, which is utilized to estimate the UL-CSI. Then the estimated UL-CSI $\hat{\mathbf{H}}_u$ feed forward to the pre-trained network to predict DL-CSI $\hat{\mathbf{H}}_d$. To evaluate the accuracy of network model, we use Pearson correlation coefficient as performance metric. Compared to MSE, the correlation coefficient $\rho$ can provide highly intuitive results, which is given as

$$\rho = \frac{\mathbb{E}[ (\hat{\mathbf{H}}_d - \bar{\mathbf{H}}_d)(\hat{\mathbf{H}}_d - \bar{\mathbf{H}}_d) ]}{\sigma_{\hat{\mathbf{H}}_d} \sigma_{\hat{\mathbf{H}}_d}}$$

where $\mu$ and $\sigma$ denote the mean and standard deviation, respectively. $\mathbb{E} [\cdot]$ denotes expectation operation.

Without loss of generality, assuming that Eve can hear the DL-CSI $\hat{H}_d$ fed back by the UE. Meanwhile, Eve also knows the complete training process. Thus, Eve try to train the neural network model to predict the DL-CSI $\hat{H}_e$. Under the condition of passive eavesdropping, the achievable secret key rate $R_s$ can be written as

$$R_s = \frac{1}{T} I(\hat{H}_d; \hat{H}_d | \hat{H}_e)$$

(4)

where $I(\hat{H}_d; \hat{H}_d | \hat{H}_e)$ denotes the conditional mutual information between $\hat{H}_d$ and $\hat{H}_d$ given $\hat{H}_e$. $T$ is a coherence time.

3.4 Secret Key Generation Based on the DL-CSI

Next, uniform quantization algorithms [1] is adopted to quantize sequences into secret keys. Then, BCH code is used for information reconciliation to agree inconsistent bits. At last, privacy amplification is deployed to eliminate the leaked information, which can be realized by SHA-128 universal hash function [1].

4. Simulation Results

In this section, we evaluate the performance of deep learning based SKG scheme for FDD MIMO systems via numerical simulation. In this simulation, we use the quasi deterministic radio channel generator (QuaDRiGa) [11] to simulate multipath fading channels. The QuaDRiGa channel model supports spatial consistency as specified by the 3GPP 38.901, where the position of the scattering clusters is a function of the UE’s position. In multi-frequency simulations, the cluster delays and angles are independent of the carriers frequency. Therefore, there exists the underlying spatial reciprocity in the uplink and downlink channel response. Specifically, we focus on the urban macro line-of-sight (LOS) scenario with 6 clusters, where small scale fading decorrelation distance is set to 5m and per-clusters delay spread is disabled. BS is equipped with 64 antennas whose antenna spacing is separated with half wavelength. UE is equipped with a single antenna. The uplink carrier frequency is 1.25G Hz and downlink carrier frequency is set to 1.27G Hz. Simulation parameters are listed in Table 1.

In this scenario, the BS is fixedly deployed at a height of 25m. The users are randomly distributed in a circle, whose center and radius are the BS and 20m, respectively. CSI datasets are generated when every user is randomly distributed at 10,000 different locations. Note that the physical environment and spatial distribution of scattering clusters do not change for every sampling. To form training and testing datasets, for 10,000 simulation samples, 9,500 samples are applied for training, the rest of them are applied for verification and test, respectively. We use MATLAB Deep Learning Toolbox to train and test. The batch size and epochs are set to 95 and 100, respectively. The learning rate is initialized with 0.001 and is decayed by a factor of 0.1 every 20 epochs.

4.1 Performance of CNN Model

In this subsection, we examine the performance of the neural network designed in this paper. Figure 2 depicts the correlation between DL-CSI predicted by BS and estimated by UE, which is calculated through Eq. (3). It is clear that the correlation after prediction by the neural network is much higher than that the direct method. One also can see that the correlation increases with the increase of the signal to noise ratio (SNR). The reason lies in that the interference of random noise on the mapping relationship between the uplink and downlink channel becomes smaller as the noise power decreases. Moreover, we compare the performance of the neural network model with the different frequency difference. It shows that the correlation shrinks when the uplink and downlink carrier frequency gap increases. This is due to the fact that the surrounding physical environment gradually shows differences in the absorption and reflection characteristics of electromagnetic waves as the frequency gap increases, resulting in the mapping relationship between the uplink channel and downlink channel gradually disappears. In addition, to further verify the robustness of our proposed CNN, we examine the prediction performance with different channel conditions. As shown in Fig. 2, the SNR in the training stage is set to 15dB, while it varies in the prediction stage. Obviously, it has little effect on the accuracy of prediction at different SNR. It indicates our proposed CNN has excellent generalization ability and robustness. This is because angle spread (AS) is narrow, the massive MIMO

| Table 1 | Secret key generation algorithm |
|---------|--------------------------------|
| Parameter | Value |
| Channel model | 3GPP 38.901 Uma LOS |
| Duplex method | FDD |
| Carrier frequency | UL:1.25GHz, DL:1.27GHz |
| Bandwidth | 3 MHz |
| Number of subcarriers | 72 |
| Antenna configuration of the BS | 64 antennas |
| Antenna configuration of the UE | Single antenna |
| Channel estimation | Least Square |

Fig. 2  The performance of the CNN versus SNR
channels exhibit sparsity in the angular domain. Based on the sparse structure in the channel, we can set the number of neurons in the middle hidden layer to be much fewer than that in the output layer, which forces CNN to compress the representation of the input. As a result, CNN can not only reduce the redundancy of network parameters but also become more functional and robust.

4.2 Performance of Key Disagreement Ratio

Next, we evaluate the performance of key disagreement ratio (KDR) between the BS and UE. Taking into account both the rate of SKG and the complexity of calculation, the quantization level is set to 1. Figure 3 plots the KDR against SNR for the proposed scheme and the loop-back based scheme proposed in [5]. It is obviously that the KDR based on deep learning is much lower than that in [5]. The is because this scheme takes advantage of the universal function approximation ability of neural network for uplink to downlink mapping, BS can accurately infer the DL-CSI from estimated UL-CSI, while the scheme proposed in [5] introduces more noises due to two rounds of channel sounding. We also compare the performance of KDR with the different frequency difference. Similarly, the mapping relationship between the uplink channel and downlink channel becomes less obvious as the frequency gap increases, resulting in the KDR increases as the frequency difference increases. Note that the KDR between Eve and BS always remains at 0.5 with the increase of the SNR, indicating that Eve cannot steal useful information from the shared secret key regardless of the signal strength. This is because there is no mapping relationship between eavesdropping channel and legitimate channel, thus the neural network trained by Eve cannot converge.

4.3 Performance of Achievable Secret Key Rate

Finally, we examine the performance of the achievable secret key rate. In this simulation, we utilize MATLAB Information Theoretical Estimator toolbox to calculate the mutual information of Eq. (4). Figure 4 compares the achievable secret key rate versus SNR with different frequency gap and antenna numbers. It shows that the achievable secret key rate increases as SNR increases. Meanwhile, as the number of antennas increases, the uncorrelated channel responses in the spatial domain used to extract secret keys increases. As a consequence, the achievable secret key rate increases. It is noted that due to the correlation between the antennas, the achievable secret key rate will not increase linearly with the increase in the number of antennas. Especially, we do not compare with the method in [5] for the reason that it has been proved to be vulnerable to passive eavesdropping [6]. This scheme makes full use of channel state information instead of only frequency-independent channel parameters, so it can generate secret keys with high rate.

5. Conclusions

In this paper, we propose a novel deep learning based secret key generation scheme for FDD MIMO systems. Firstly, an encoder-decoder convolutional neural network is built to characterize the wireless environment to learn the mapping relationship between the uplink and downlink channel. Then, the convolutional neural network is trained for predicting DL-CSI. Finally, random secret keys are generated from the DL-CSI. Compared with the existing SKG schemes, this scheme can achieve significant performance improvement in terms of the key agreement ratio and achievable secret key rate. Moreover, this scheme does not require high computational operations and is suitable for low-power terminals. But this scheme has some limitations, the performance of prediction accuracy will decline when the radio environment changes significantly. We are trying to extend this scheme based on meta-learning to adapt to new wireless environments in future works.

Acknowledgments

This research was funded by the National Natural Science Foundation of China (Nos.61871404), Innovative Research Group Project of the National Natural Science Foundation
of China (Nos.61521003) and Key Universities and Academic Disciplines Contraction Project.

References

[1] J. Zhang, T.Q. Duong, A. Marshall, and R. Woods, “Key generation from wireless channels: A review,” IEEE Access, vol.4, pp.614–626, 2016. doi: 10.1109/access.2016.2521718.

[2] W. Wang, H. Jiang, X. Xia, P. Mu, and Q. Yin, “A wireless secret key generation method based on chinese remainder theorem in fdd systems,” Science China Information Sciences, vol.55, no.7, pp.1605–1616, 2012. doi: 10.1007/s11432-012-4570-2.

[3] B. Liu, A. Hu, and G. Li, “Secret key generation scheme based on the channel covariance matrix eigenvalues in fdd systems,” IEEE Communications Letters, vol.23, no.9, pp.1493–1496, 2019. doi: 10.1109/LCOMM.2019.2924420.

[4] S.J. Goldberg, Y.C. Shah, and A. Reznik, “Method and apparatus for performing jrnso in fdd, tdd and mimo communications,” Google Patents, 2013.

[5] X. Wu, Y. Peng, C. Hu, H. Zhao, and L. Shu, “A secret key generation method based on csi in ofdm-fdd system,” 2013 IEEE Globecom Workshops (GC Wkshps), pp.1297–1302, IEEE, 2013.

[6] L. Peng, G. Li, J. Zhang, R. Woods, M. Liu, and A. Hu, “An investigation of using loop-back mechanism for channel reciprocity enhancement in secret key generation,” IEEE Transactions on Mobile Computing, vol.18, no.3, pp.507–519, 2019. doi: 10.1109/tmc.2018.2842215.

[7] K. Hugl, K. Kalliola, and J. Laurila, “Spatial reciprocity of uplink and downlink radio channels in fdd systems,” Proc. COST, p.066, Citeseer, 2002.

[8] D. Vasisht, S. Kumar, H. Rahul, and D. Katabi, “Eliminating channel feedback in next-generation cellular networks,” Proceedings of the 2016 ACM SIGCOMM Conference, pp.398–411, 2016.

[9] M. Alrabeiah and A. Alkhateeb, “Deep learning for tdd and fdd massive mimo: Mapping channels in space and frequency,” 2019 53rd Asilomar Conference on Signals, Systems, and Computers, pp.1465–1470, IEEE, 2019.

[10] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” Nature, vol.521, pp.436–444, 2015. doi: 10.1038/nature14539.

[11] S. Jaeckel, L. Raschkowski, K. Borner, and L. Thiele, “Quadriga: A 3-d multi-cell channel model with time evolution for enabling virtual field trials,” IEEE Transactions on Antennas and Propagation, vol.62, no.6, pp.3242–3256, 2014. doi: 10.1109/TAP.2014.2310220.