LSTM-Based Channel Prediction for Secure Massive MIMO Communications Under Imperfect CSI

Tenghui Peng[1,2,3], Rongqing Zhang[1,2], Xiang Cheng[4], Liuqing Yang[5]
[1]School of Software Engineering, Tongji University, Shanghai, China
[2]Shandong Provincial Key Laboratory of Wireless Communication Technologies, Shandong University, China
[3]School of Electronics and Information Engineering, Tongji University, Shanghai, China
[4]State Key Laboratory of Advanced Optical Communication Systems and Networks, Peking University, Beijing, China
[5]Department of Electrical and Computer Engineering, Colorado State University, CO 80523, USA

Abstract*—In recent years, massive multiple-input multiple-output (MIMO) has been regarded as a promising technique in the fifth-generation (5G) communication systems. With the ability of focusing transmission beams on users, massive MIMO has a natural advantage in the field of physical layer security to improve the system secrecy performance. However, in practical mobile systems, the imperfect channel state information (CSI) caused by the channel estimation error and the transmission and processing delay will have a non-negligible impact on the system performance. In this paper, we investigate secure communications in a multi-user massive MIMO-enabled vehicular communication networks. Considering the influence of imperfect CSI on the secrecy performance, we derive a tight asymptotic lower bound of the system secrecy capacity under both perfect and imperfect CSI. Moreover, we further analyze the impact of vehicle speed on the system secrecy performance and propose a channel prediction scheme based on (Long Short-Term Memory) LSTM model to compensate for the negative effects of imperfect CSI, which can improve the system secrecy performance in high mobility scenario. Simulation results show that the imperfect CSI severely reduces the system secrecy capacity, but its negative effects can be effectively alleviated through the designed LSTM-based channel prediction and compensation scheme.

***Index Terms*—Massive MIMO, physical layer security, LSTM, channel prediction.**

I. Introduction

Most recently, massive MIMO has emerged as a promising solution in the 5G communication systems. By increasing the number of antennas, massive MIMO enables hundreds of antennas to serve dozens of user terminals simultaneously at the same frequency while retaining the advantages of traditional MIMO, and greatly improves the system capacity and energy efficiency through beam concentration and spatial multiplexing [1]. In addition, the channels of different users in massive MIMO system are nearly orthogonal, which reduces the inter-channel interference, and the large-scale antennas can also improve the robustness on the communication system against interference and attack [2], [3].

In addition, with the rapid development of modern communication systems, physical layer security, as a supplement to traditional encryption methods, has aroused extensive research interest in the field of information security in recent years [4], [5]. As for massive MIMO that can focus the energy beam on specific users, it has an advantage in terms of physical layer security [6]. That is, the receiving power of legitimate users is higher, while that of eavesdropping users is lower, and thus the system secrecy performance can be improved. Therefore, it is natural and critical to combine these two technologies to enhance the secrecy of future communication networks. However, it should be noted that once the pilot sequences (PSs) used to estimate channels are not orthogonal, pilot pollution will reduce the accuracy of channel estimation and thus seriously affect the performance of massive MIMO [7].

The Internet of vehicles (IoV) is an important technology in the future of intelligent driving. Composed by vehicles and basic communication units on the roadside, it is characterized by flexible networking, coexistence of multiple communication modes, fast node movement, and predictable trajectory [8]. While at the same time, the high-speed mobility of vehicles leads to the channels' fast time-varying characteristics, which also makes the influence of imperfect CSI more serious [9]. At present, studies on physical layer security in massive MIMO technology mostly consider the case of perfect CSI, but due to the large antenna scale, the imperfect CSI caused by the channel estimation error and the transmission and processing delay will have a more significant impact on the secrecy performance of massive MIMO [6]. Recently, deep learning methods have been successfully applied in the field of wireless communications, and effective results have been obtained in channel prediction schemes based on the deep learning algorithms [10]. Among them, long short-term memory (LSTM) is an efficient improved recurrent neural network (RNN), which has a good effect in solving the long-term dependence problems in general RNN and has been widely used in time series processing and voice processing.

In this paper, we investigate the physical layer security issue under imperfect CSI in a multi-user massive MIMO system. Considering the influence of imperfect CSI on the secrecy performance, we derive a tight asymptotic lower bound of the system secrecy capacity under both perfect and imperfect CSI. Moreover, we further analyze the impact of vehicle speed on the system secrecy performance. In order to compensate for the negative influence of imperfect CSI, we then propose a channel prediction scheme based on LSTM model, in which we exploit LSTM to extract the time correlation characteristic of channels, improve the

978-1-7281-5089-5/20/$31.00 ©2020 IEEE

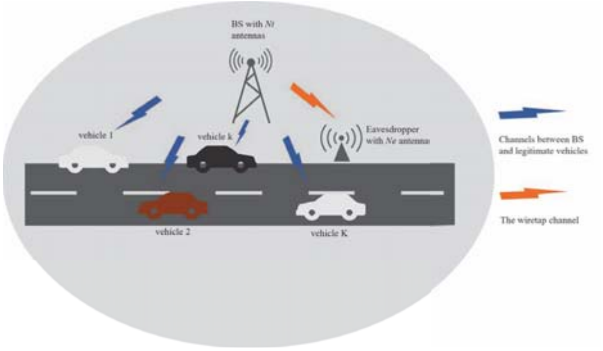

Fig. 1. The investigated massive MIMO system in vehicular networks.

accuracy of channel prediction, and thus enhance the system secrecy performance. Simulation results show that imperfect CSI severely reduces the system secrecy capacity, especially in high-speed environment, while our proposed channel prediction scheme effectively alleviates its negative influence.

The remainder of this paper is organized as follows. Section II describes the investigated system model and problem formulation. In Section III, we derive the ergodic secrecy capacity under perfect and imperfect CSI. Section IV specially analyzes the effect of vehicle speed and proposes a channel prediction scheme based on LSTM to compensate for the negative influence of imperfect CSI. In Section V, simulation results demonstrates the system secrecy performance under perfect and imperfect CSI, and the effectiveness of our channel prediction scheme. Section VI gives the conclusions.

II. System Model and Problem Formulation

A. System Scenario

As shown in Fig. 1, in the system model, a base station, K legitimate vehicles, and a malicious eavesdropper coexist. The BS aims to transmit signals to legitimate vehicles, equipping with N_t antennas. There is only one antenna on each legitimate vehicle. N_e antennas are equipped by the passive eavesdropper to wiretap the channels between the BS and the legitimate vehicles without launching any pilot contamination attacks. In our investigated scenario, N_t is much larger than N_e and K, i.e., $N_t \gg \max\{N_e, K\}$.

Quasi-static channels are assumed between the BS and different terminals, which means during one time slot the channel gains remain the same, while vary in different time slots. The channel matrix between the BS and different vehicles can be represented by $\mathbf{H} = \left[\mathbf{h}_1^H, \mathbf{h}_2^H, \cdots, \mathbf{h}_K^H\right]^H \in \mathbb{C}^{K \times N_t}$, where its row vector $\mathbf{h}_k^H$ denotes the channel between the BS and vehicle k. Also, we use $\mathbf{G} \in \mathbb{C}^{N_e \times N_t}$ to denote the channel gains between the BS and the eavesdropper. In our investigated channel model, uncorrelated Rayleigh fading is adopted. Therefore, we have that the vector $\mathbf{h}_k \in \mathbb{C}^{1 \times N_t}$ and matrix $\mathbf{G}$ are independent identically distributed complex Gaussian variables with zero mean and unit variance.

Let $\mathbf{s}(t) = [s_1(t), s_2(t), \cdots, s_K(t)] \in \mathbb{C}^{K \times 1}$ denote the required data symbols of K vehicles, where $\mathbf{s}(t) \sim \mathcal{CN}(0, \mathbf{I}_K)$. Under linear precoding, the transmit signals can be represented by

$$\mathbf{x}(t) = \sqrt{\frac{P_B}{\xi}} \mathbf{F}^H(t)\mathbf{s}(t) \tag{1}$$

where matrix $\mathbf{F}(t) = [\mathbf{f}_1^H(t), \mathbf{f}_2^H(t), \cdots, \mathbf{f}_K^H(t)]^H \in C^{K \times N_t}$ represents the precoding matrix, and maps the required data symbols, i.e., $\mathbf{s}(t)$, to N_t transmit antennas. Note that $\xi = \mathrm{E}\left[\mathrm{tr}\left\{\mathbf{F}^H\mathbf{F}\right\}\right]$ and P_B denote the power constraints of the precoding matrix and the BS transmit power, respectively.

Based on the definitions above, the resulting received signal at the k-th vehicle is given by:

$$\begin{aligned} y_k(t) &= \mathbf{h}_k(t)\mathbf{x}(t) + n_k(t) \\ &= \sqrt{\frac{P_B}{\xi}} \left[\mathbf{h}_k(t)\mathbf{f}_k^H(t)s_k(t) + \sum_{j \neq k} \mathbf{h}_k(t)\mathbf{f}_j^H(t)s_j(t)\right] \\ &\quad + n_k(t) \end{aligned} \tag{2}$$

where the first term represents the desired signal, the second term represents the multi-user interference, and $n_k(t) \sim \mathcal{CN}(0, \sigma_n^2)$ represents the additive Gaussian white noise with zero mean and σ_n^2 variance.

Similarly, the intercepted signal at the eavesdropper is denoted by

$$\mathbf{y}_e(t) = \mathbf{G}(t)\mathbf{x}(t) + \mathbf{n}_e(t) = \sqrt{\frac{P_B}{\xi}} \mathbf{G}(t)\mathbf{F}^H(t)\mathbf{s}(t) + \mathbf{n}_e(t) \tag{3}$$

where $\mathbf{n}_e(t) \sim \mathcal{CN}(\mathbf{0}, \sigma_n^2\mathbf{I}_{N_e})$ is the additive Gaussian white noise at the eavesdropper.

B. Imperfect CSI

The influence of imperfect CSI on the system security performance is mainly composed of the following two factors: channel estimation error and outdated CSI.

In a practical communication system, the BS utilizes PSs received from vehicles to estimate the corresponding CSI, and then conducts channel precoding and transmit through N_t antennas using the estimated CSI [7]. We use $\mathbf{\Theta} = [\boldsymbol{\theta}_1, \boldsymbol{\theta}_2 \cdots, \boldsymbol{\theta}_K] \in \mathcal{C}^{\tau \times K}$ to represent the PS matrix transmitted by the vehicles, where $\boldsymbol{\theta}_k \in C^{\tau \times 1}$ denotes vehicle k's PS, and τ denotes the length of every PS. We use $\mathbf{W}(t) \in \mathbb{C}^{\tau \times N_t}$ to denote the additive Gaussian white noise during the channel estimation process, note that each of its entries has zero mean and variance σ_w^2.

We denote the PSs received by the BS as

$$\mathbf{Y}(t) = \mathbf{\Theta}\mathbf{H}(t) + \mathbf{W}(t) \tag{4}$$

based on the definitions above.

The BS multiplies $\mathbf{\Theta}^H$ to (4) to distinguish PSs sent from different vehicles, i.e., for the PS of the k-th vehicle

$$\mathbf{z}_k(t) = \mathbf{h}_k(t) + \theta_k^H\mathbf{W}(t) \tag{5}$$

For the whole system, we have

$$\mathbf{Z}(t)=\boldsymbol{\Theta}^{H}\mathbf{Y}(t)=\mathbf{H}(t)+\boldsymbol{\Theta}^{H}\mathbf{W}(t) \tag{6}$$

With minimum mean square error(MMSE) channel estimation method, we can use (7) to represent the real CSI

$$\begin{aligned}\mathbf{h}_k(t)&=\hat{\mathbf{h}}_k(t)+\mathbf{n}_{k,\mathrm{MMSE}}(t)\\&=\left(1+\sigma_w^2\right)^{-1}\mathbf{z}_k(t)+\mathbf{n}_{k,\mathrm{MMSE}}(t)\end{aligned} \tag{7}$$

where $\mathbf{n}_{k,\mathrm{MMSE}}(t)$ represents the channel estimation error and independent of $\hat{\mathbf{h}}_k(t)$. Note that $\hat{\mathbf{h}}_k(t)\sim\mathcal{CN}\left(0,\sigma_{\hat{h}}^2\right)$ and $\mathbf{n}_{k,\mathrm{MMSE}}(t)\sim\mathcal{CN}\left(0,\sigma_{n_{\mathrm{MMSE}}}^2\right)$, where

$$\sigma_{\hat{h}}^2=\left(1+\sigma_w^2\right)^{-1} \tag{8}$$

and

$$\sigma_{n_{\mathrm{MMSE}}}^2=\left(1+\sigma_w^2\right)^{-1}\sigma_w^2 \tag{9}$$

To discuss about the outdated CSI, we first define T_d as the delay between the outdated channel and the real-time channel, which means that the time interval between when the BS receives the PSs and when it completes the channel estimation and starts transmitting data is T_d. We have defined $\mathbf{H}(t)$ as a complex Gaussian process with unit variance and zero mean, therefore, the autocorrelation function of the channel can be used to characterize the time variation of the channel [11]. Based on Jake's model [9], we have

$$\rho_{T_d}=J_0\left(2\pi f_D T_d\right) \tag{10}$$

where $J_0\left(\cdot\right)$ denotes the zeroth-order Bessel function of the first kind. Also,

$$f_D=\frac{v}{c}f_c \tag{11}$$

is the maximum Doppler spread, where v denotes the velocity of the vehicles, $c=3\times10^8$ m/s is the speed of light, and f_c denotes the carrier frequency. We know that the decrease of ρ_{T_d} will cause the correlation between the outdated channel and the real-time channel to reduce. That is, when $\rho_{T_d}=1$, the outdated channel effect will be eliminated.

According to the definition of factor ρ_{T_d}, we can use

$$\mathbf{H}(t+T_d)=\rho_{T_d}\mathbf{H}(t)+\sqrt{1-\rho_{T_d}^2}\mathbf{E}(t+T_d) \tag{12}$$

to denote the correlation between the outdated channel $\mathbf{H}(t)$ and the real-time channel $\mathbf{H}(t+T_d)$, where $\mathbf{E}(t+T_d)$ is a random variable independent identically distributed with $\mathbf{H}(t)$.

Hence, we can represent the real-time channel of the k-th user at time $t+T_d$ by

$$\begin{aligned}\mathbf{h}_k(t+T_d)&=\rho_{T_d}\mathbf{h}_k(t)+\sqrt{1-\rho_{T_d}^2}\mathbf{e}_k(t+T_d)\\&=\rho_{T_d}\hat{\mathbf{h}}_k(t)+\tilde{\mathbf{e}}_k(t)\end{aligned} \tag{13}$$

based on (7) and (12), where $\tilde{\mathbf{e}}_{\mathbf{k}}(t)=\rho_{T_d}\mathbf{n}_{k,\mathrm{MMSE}}(t)+\sqrt{1-\rho_{T_d}^2}\mathbf{e}_k(t+T_d)$, satisfies $\tilde{\mathbf{e}}_k\sim\mathcal{CN}\left(0,\sigma_{\tilde{e}}^2\mathbf{I}_{N_t}\right)$, $\sigma_{\tilde{e}}^2=\rho_{T_d}^2\sigma_{n_{\mathrm{MMSE}}}^2+(1-\rho_{T_d}^2)=1-\rho_{T_d}^2\left(1+\sigma_w^2\right)^{-1}$.

III. Analysis of Ergodic Secrecy Capacity

In this section, we will give a performance analysis of ergodic secrecy capacity in the investigated multi-user massive MIMO scenario under certain linear precoding scheme, i.e., zero-forcing (ZF), which can achieve a better secrecy performance than the MF precoder [12].

According to (2), the ergodic secrecy capacity of vehicle k can be represented by

$$C_k=\mathrm{E}\left[\log_2\left(1+\frac{\gamma\left|\mathbf{h}_k\left(t+T_d\right)\mathbf{f}_k^H(t)\right|^2}{\xi+\gamma\sum_{j\neq k}\left|\mathbf{h}_k\left(t+T_d\right)\mathbf{f}_j^H(t)\right|^2}\right)\right] \tag{14}$$

where $\gamma=\frac{P}{\sigma^2}$ denoted the transmit SNR. On the other hand, according to (3), the ergodic secrecy capacity of the eavesdropper can be represented by

$$C_e=\mathrm{E}\left[\log_2\left(\det\left(I_{N_e}+\frac{\gamma}{\xi}\mathbf{G}\mathbf{F}^H\mathbf{F}\mathbf{G}^{\mathbf{H}}\right)\right)\right] \tag{15}$$

Firstly, in order to summarize some general results which will be used in the proof of the following section, we give **Lemma 1**.

Lemma 1. *Consider two random vectors* $\mathbf{a},\mathbf{a}\in\mathbb{C}^{1\times n}$*, which satisfy* $\mathbf{a}\in\mathcal{CN}(0,\sigma_a^2\mathbf{I}_n)$ *and* $\mathbf{b}\in\mathcal{CN}(0,\sigma_b^2\mathbf{I}_n)$*. Then we have the following four equations:*

- $\mathrm{E}\left[\mathbf{a}\mathbf{a}^H\right]=n\sigma_a^2$,
- $\mathrm{E}\left[\mathbf{a}\mathbf{b}^H\right]=0$,
- $\mathrm{var}\left[\mathbf{a}\mathbf{a}^H\right]=n\sigma_a^4$,
- $\mathrm{var}\left[\mathbf{a}\mathbf{b}^H\right]=n\sigma_a^2\sigma_b^2$.

Proof: Considering that based on the statistical characteristics of Rayleigh distributed vectors, we can easily prove these four equations, we omit the proof here. ■

A. Secrecy Capacity under Perfect CSI

In ZF precoding scheme, the precoding matrix can be represented by:

$$\mathbf{F}=\left(\mathbf{H}\mathbf{H}^{\mathbf{H}}\right)^{-1}\mathbf{H} \tag{16}$$

The interference between different vehicles can be eliminated wonderfully through such precoder, i.e., $\mathbf{h}_k\mathbf{f}_j^{\mathrm{H}}=0$ is always satisfied when $k\neq j$.

Under perfect CSI, the transmit power constraint of the precoding matrix can be given as $\xi=\frac{K}{N_t-K}$, the SINR of vehicle k can be represented by $\mathrm{SINR}_k=\frac{\gamma(N_t-K)}{K}$. Therefore the ergodic capacity of vehicle k is

$$C_k=\log_2\left(1+\frac{\gamma\left(N_t-K\right)}{K}\right) \tag{17}$$

On the other hand, we consider that the channel capacity of eavesdropper is given by

$$C_e=\mathrm{E}\left\{\log_2\left[\det\left(\mathbf{I}_{N_e}+\frac{\gamma}{\xi}\mathbf{G}\mathbf{H}^H\left(\mathbf{H}\mathbf{H}^H\right)^{-2}\mathbf{H}\mathbf{G}^H\right)\right]\right\} \tag{18}$$

Using **lemma 1**, we get $\mathrm{HH}^H \approx N_t \mathrm{I}_x$. Therefore, the channel capacity of eavesdropper can be represented by

$$C_e \approx \mathrm{E}\left\{\log_2\left[\det\left(\mathbf{I}_{N_c} + \frac{\gamma\left(N_t - K\right)}{N_t^2 K}\mathbf{G}\mathbf{H}^H\mathbf{H}\mathbf{G}^H\right)\right]\right\} \tag{19}$$

Given that the value of N_t is greatly larger than K, i.e., $N_t \gg K$, in the massive MIMO system, thus we get $\frac{\gamma(N_t - K)}{N_t^2 K} \approx \frac{\gamma N_t}{N_t^2 K} = \frac{\gamma}{N_t K}$. Then we can rewrite the channel capacity of eavesdropper as

$$C_e \approx \mathrm{E}\left\{\log_2\left[\det\left(\mathbf{I}_{N_c} + \frac{\gamma}{N_t K}\mathbf{G}\mathbf{H}^H\mathbf{H}\mathbf{G}^H\right)\right]\right\} \tag{20}$$

Therefore, an asymptotic lower bound of the ergodic system secrecy capacity can be represented by (21) where $L_n^\alpha\left(x\right)$ is the generalized Laguerre polynomial of order n and given by [13]:

$$L_n^\alpha\left(x\right) = \frac{1}{n!}e^x x^{-\alpha}\frac{d^n}{dx^n}\left(e^{-x}x^{n+\alpha}\right) = \sum_{m=0}^{n}\left(-1\right)^m C_{n+\alpha}^{n-m}\frac{x^m}{m!} \tag{22}$$

B. Secrecy Capacity under Imperfect CSI

Under imperfect CSI, the SINR of vehicle k can be denoted by

$$\begin{aligned}\mathrm{SINR}_k^{imp} &= \frac{\frac{P_B}{\xi}\left|\mathbf{h}_k(t)\mathbf{f}_k^H(t)\right|^2}{\frac{P_B}{\xi}\sum_{j\neq k}\left|\mathbf{h}_k(t)\mathbf{f}_j^H(t)\right|^2 + \sigma_n^2} \\ &= \frac{\gamma\left|\mathbf{h}_k\left(t+T_d\right)\mathbf{f}_k^H(t)\right|^2}{\xi + \gamma\sum_{j\neq k}\left|\mathbf{h}_k(t)\mathbf{f}_j^H(t)\right|^2}\end{aligned} \tag{23}$$

For the numerator part,

$$\begin{aligned}\left|\mathbf{h}_k\left(t+T_d\right)\mathbf{f}_k^H(t)\right|^2 &= \left|\left(\rho\hat{\mathbf{h}}_k(t) + \tilde{\mathbf{e}}_k(t)\right)\mathbf{f}_k^H(t)\right|^2 \\ &= \rho^2 + \left|\tilde{\mathbf{e}}_k(t)\mathbf{f}_k^H(t)\right|^2\end{aligned} \tag{24}$$

For the denominator part,

$$\begin{aligned}\left|\mathbf{h}_k(t)\mathbf{f}_j^H(t)\right|_{k\neq j}^2 &= \left|\left(\rho\hat{\mathbf{h}}_k(t) + \tilde{\mathbf{e}}_k(t)\right)\mathbf{f}_j^H(t)\right|^2 \\ &= \left|\tilde{\mathbf{e}}_k(t)\mathbf{f}_j^H(t)\right|^2\end{aligned} \tag{25}$$

Given that $\tilde{\mathbf{E}}\mathbf{F}^H = \tilde{\mathbf{E}}\hat{\mathbf{H}}^H\left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H\right)^{-1} \approx \frac{1}{N_t\sigma_{\hat{h}}^2}\tilde{\mathbf{E}}\hat{\mathbf{H}}^H$, we get that $\left|\tilde{\mathbf{e}}_k(t)\mathbf{f}_k^H(t)\right|^2 = \frac{\sigma_{\tilde{e}}^2}{N_t\sigma_{\hat{h}}^2}$. Therefore, the channel capacity of vehicle k under imperfect CSI can be represented by

$$C_k \geq \log_2\left(1 + \frac{\gamma\left(\rho^2 N_t\sigma_{\hat{h}}^2 + \sigma_{\tilde{e}}^2\right)}{K\left(1 + \gamma\sigma_{\tilde{e}}^2\right)}\right) \tag{26}$$

Note that the channel capacity of eavesdropper is not effected by imperfect CSI, we have (27).

IV. Ergodic Secrecy Capacity Under High-speed Environment And Channel Prediction

In this section we will consider the effects of the speed on the secrecy capacity of system, and propose a channel prediction scheme based on LSTM algorithm in order to improve the system performance of ergodic secrecy capacity.

A. Influence of Increasing Speed

The high-speed mobility of vehicles leads to the fast time-varying characteristics of channels, which also brings great challenges to channel estimation and prediction [9], [11]. According to (27), the parameter

$$\rho_T^2\sigma_{\hat{h}}^2 = \frac{1}{1+\sigma_w^2}J_0\left(2\pi\frac{v}{c}f_c T\right) \tag{28}$$

can well characterize the influence of imperfect CSI on the physical layer security performance of the system. Specifically, speed is the most critical factor, which determines the correlation between the real channel and the outdated channel. The faster the speed, the more obvious the doppler effect, the lower the channel correlation, and the lower the channel capacity of legitimate vehicles.

In the physical layer security scenario, as we have mentioned in Section III, if the eavesdropper is stationary, the imperfect CSI will has no effect on the information the eavesdropper can wiretap. Then, when the speed reaches a certain level, $\rho_T^2\sigma_{\hat{h}}^2 \approx 0$, the influence of imperfect CSI on the system is so serious that normal communication is almost impossible. In the presence of eavesdroppers, it becomes more difficult to achieve secure communication.

Therefore, we hope to explore a new channel prediction scheme to overcome the negative impact of speed on channel security performance by improving the accuracy of channel prediction at high speed, so as to adapt to the high-speed moving characteristics of internet of vehicles scenarios.

B. Channel Prediction Based on LSTM

The BS sends data to the vehicles at the time of $t + T_d$. However, due to delays during transmission and processing, and the influence of channel estimation errors, the CSI used by the BS in the process of coding and transmission is imperfect. We define T as the length of a frame, then we can store CSI in multiple frames to utilize the time-dependent characteristics of massive MIMO, thus predict the CSI of $t + T_d$.

Considering LSTM's good performance in processing time sequences, we design a channel prediction scheme based on LSTM algorithm. LSTM is a classical improved RNN algorithm. Different from RNN, which is only sensitive to short-term input, LSTM has an excellent learning result on both long-term and short-term inputs by adding structure including cell states.

As shown in Fig. 2, suppose we use CSI of the previous L time slots to train the network, that is, the input of the network can be expressed as

$$\mathbf{H}^{(L)}(t) = \left[\mathbf{H}(t), \mathbf{H}(t-T), \cdots, \mathbf{H}(t-(L-1)T)\right] \in \mathbb{C}^{K\times N_t\times L} \tag{29}$$

We define the weight matrix of the network as

$$\mathbf{W} = \left[\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_{L-1}\right] \in C^{N_t\times L} \tag{30}$$

And the output of the network is $\overline{\mathbf{H}}\left(t+T_d\right)$, which represent the predicted value of $\mathbf{H}\left(t+T_d\right)$.

$$C_s \gtrapprox \left\{ K\log_2 \left\{ 1 + \frac{\gamma(N_t - K)}{K} \right\} - \left(m\log_2 \left(\frac{\gamma}{K} \right) + \log_2 (m!) + \log_2 \left\{ L_m^{n-m} \left(-\frac{K}{\gamma} \right) \right\} \right) \right\}^+ \tag{21}$$

$$C_s^{\text{imp}} \gtrapprox \left\{ K\log_2 \left\{ 1 + \frac{\gamma(\rho_{T_d}^2 \sigma_{\hat{h}}^2 N_t + \sigma_{\tilde{e}}^2)}{K(1+\gamma\sigma_{\tilde{e}}^2)} \right\} - \left(m\log_2 \left(\frac{\gamma}{K} \right) + \log_2 (m!) + \log_2 \left\{ L_m^{n-m} \left(-\frac{K}{\gamma} \right) \right\} \right) \right\}^+ \tag{27}$$

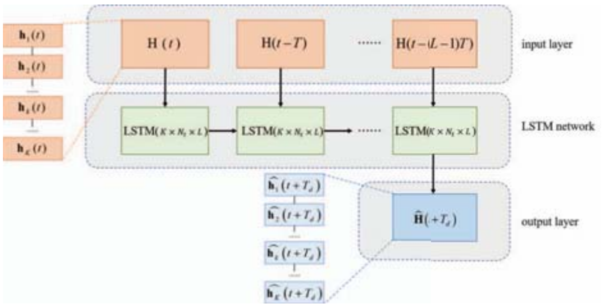
$\mathbf{h}_1(t)$
$\mathbf{h}_2(t)$
$\mathbf{h}_k(t)$
$\mathbf{h}_K(t)$
H (t)
H$(t-T)$
······
H$(t-(L-1)T)$
input layer
LSTM$(K \times N_t \times L)$
LSTM$(K \times N_t \times L)$
······
LSTM$(K \times N_t \times L)$
LSTM network
$\widehat{\mathbf{h}}_1(t+T_d)$
$\widehat{\mathbf{h}}_2(t+T_d)$
$\widehat{\mathbf{h}}_k(t+T_d)$
$\widehat{\mathbf{h}}_K(t+T_d)$
$\widehat{\mathbf{H}}(+T_d)$
output layer

Fig. 2. Overall architecture of the LSTM. The input layer includes L CSI matrixes, each of which are split into K vectors before inputting into the LSTM network. The output is a matrix of CSI in time slot $t+T_d$.

It is worth noting that although we only use one simple matrix $\mathbf{W}$ to represent the weights inside the network, in fact, the calculation of the parameters inside the LSTM is very complex.

LSTM uses two doors to control the content of cell states: forget gate, which determines how much of the cell state of the previous moment can be retained to the current moment, and input gate, which determines the how much of the current input is saved to the cell state. Also, LSTM uses output gate to control how much of the cell state can be output to current output value. In the training process, there are 8 groups of parameters that LSTM needs to learn, which are: weight matrix and bias item of forget gate, input gate, output gate, and cell state calculation [14].

As for the formula calculation of the forward propagation and training algorithm of LSTM network, previous researches have been detailed and comprehensive [15], and thus in this paper we will not repeat it.

V. Simulation Results

In this section, we will evaluate the influence of several factors on the ergodic secrecy capacity through simulation and test the performance of our channel prediction scheme at the same time. An isolated system including a BS, K vehicles and an eavesdropper is assumed. The channel correlation between different time slots is depicted by Jake's model [9]. We set the vehicles' average speed as v, the duration of a time slot as $T = 0.01s$, and the centre carrier frequency as f_c=2GHZ. Also, we only consider the small-scale fading in our model and define the path-loss gain as 1 for convenience.

We use $\{\mathbf{H}(t), \mathbf{H}(t-T), \cdots, \mathbf{H}\,(t-(L-1)T)\}$ to denote the vehicles' real CSI sequence at different time slots. We first generate $\mathbf{H}\,(t-(L-1)T)$ and then generate $\mathbf{H}\,(t-(L-2)T)$ based on the recursion formula of 1st order autoregressive model (AR(1)) [**?**], thus to guarantee the channel correlation between different time slots. Repeating the procedure:

$$\begin{aligned} \mathbf{H}(t-(L-i)T) = &\rho_T \mathbf{H}(t-[L-(i-1)]\,T) \\ &+ \sqrt{1-\rho_T^2}\mathbf{E}(t-(L-i)T) \end{aligned} \tag{31}$$

then we can obtain the sequence of channels. For convenience, $T_d = T$ is assumed. Thus, by using the recursion formula, we can also obtain the real channel at time $t+T_d$.

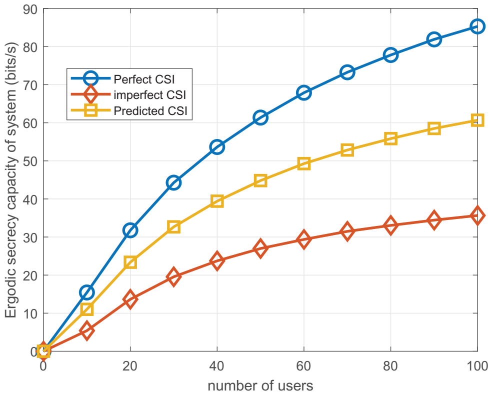

Fig. 3. Ergodic system secrecy capacity vs. number of vehicles K. Parameters: SNR = 10dB, N_t = 128, N_e = 8, L = 20, σ_w^2 = 1, $v = 10m/s$.

A. Ergodic capacity vs. K

In Fig. 3, we aim at analyzing the relationship between the ergodic capacities and the number of the legitimate vehicles, i.e., K. As K increases, the secrecy capacity first increases. However, when K increases to a certain level, the capacity increases more and more slowly. For a multi-user massive MIMO system, given that different channels are orthogonal, an increasing number of users can serve more users and better exploit the advantages of massive MIMO to increase the system capacity. However, another phenomenon is that as K increases, the interference between different users becomes increasingly worse at the same time, and that is why the growing speed of channel capacity decreases.

B. Ergodic capacity vs. SNR

As shown in Fig. 4, when SNR increases, the ergodic system secrecy capacity first increases. When SNR reaches a certain value, as it continues to increase, the system secrecy capacity starts to decrease, until it finally reduces to 0.

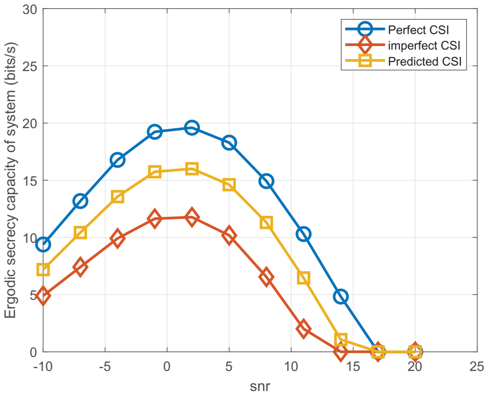

Fig. 4. Ergodic system secrecy capacity vs. SNR. Parameters: SNR = 10dB, $N_t = 128$, $L = 20$, $N_e = 8$, $K = 8$, $\sigma_w^2 = 1$, $v = 10m/s$.

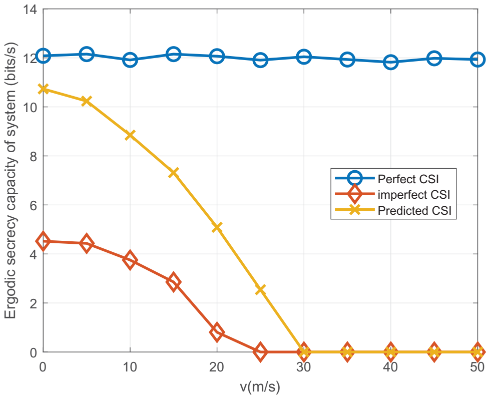

Fig. 5. Ergodic system secrecy capacity vs. speed v. Parameters: $N_t = 128$, $L = 20$, $N_e = 8$, $K = 8$, $\sigma_w^2 = 1$.

It can be seen from (26) that, for each user, when SNR increases, not only its receiving power increases, but also the inter-user interference increases, which limits the growth of user capacity. When SNR grows to a certain value, the user capacity will converge to a constant value. However, for eavesdroppers, the increase of SNR will always bring the increase of eavesdropper capacity.

C. Ergodic capacity vs. v

In Fig. 5, we compare the relationship between ergodic secrecy capacity and speed respectively under perfect CSI, imperfect CSI and our channel prediction scheme based on LSTM.

In fact, in the figures of the previous two sections, we can also see that under the channel prediction scheme, the system security performance is greatly improved compared with imperfect CSI, but still weaker than perfect CSI. In addition, we also noticed that as the speed increased, the performance of the predicted solution decreased. When the speed is increased to a certain value, the channel prediction scheme still cannot solve the problem of low channel correlation, which is also worth further exploration in future research.

VI. Conclusions

In this paper, we investigated secure communications in a multi-user massive MIMO system. We considered the influence of imperfect CSI on the achieved seccrecy performance and derived a tight asymptotic lower bound for the system secrecy capacity under both perfect and imperfect CSI. Moreover, we analyzed the impact of vehicle speed on the secrecy performance of massive MIMO and proposed a channel prediction scheme based on LSTM to compensate for the negative effects of imperfect CSI. Simulation results showed that the imperfect CSI severely reduces the system secrecy capacity, but its negative effect can be effectively alleviated through the designed channel prediction scheme.

Acknowledgment

This work is supported in part by the National Natural Science Foundation of China under Grant 61901302, in part by the open research fund from Shandong Provincial Key Laboratory of Wireless Communication Technologies (No. SDKLWCT-2019-02), and in part by the National Science Foundation under Grant CPS-1932413 and ECCS-1935915.

References

[1] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, “Massive MIMO for Next Generation Wireless Systems,” *IEEE Communications Magazine*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[2] T. L. Marzetta, “Noncooperative Cellular Wireless with Unlimited Numbers of BS Antennas,” *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.

[3] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, “Energy and Spectral Efficiency of Very Large Multiuser MIMO Systems,” *IEEE Transactions on Communications*, vol. 61, no. 4, pp. 1436–1449, Apr. 2013.

[4] R. Zhang, L. Song, Z. Han, and B. Jiao, “Physical Layer Security for Two-Way Untrusted Relaying With Friendly Jammers,” *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[5] R. Zhang, X. Cheng, and L. Yang, “Cooperation via Spectrum Sharing for Physical Layer Security in Device-to-Device Communications Underlaying Cellular Networks,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5651–5663, Aug. 2016.

[6] T. Yang, R. Zhang, X. Cheng, and L. Yang, “Secure Massive MIMO Under Imperfect CSI: Performance Analysis and Channel Prediction,” in IEEE Transactions on Information Forensics and Security, vol. 14, no. 6, pp. 1610-1623, June 2019.

[7] A. H. Alqahtani, A. I. Sulyman and A. Alsanie, “Rateless Spacetime Block Code for Mitigating Pilot Contamination Effects in Multi-Cell Massive MIMO System with Lossy Links,” *IET Communications*, vol. 10, no. 16, pp. 2252–2259, Mar. 2016.

[8] F. Zeng, R. Zhang, X. Cheng, and L. Yang, “Channel Prediction Based Scheduling for Data Dissemination in VANETs,” *IEEE Communications Letters*, vol. 21, no. 6, pp. 1409–1412, Jun. 2017.

[9] M. Seyfi, S.Muhaidat, J. Liang, and M. Dianati, “Effect of Feedback Delay on the Performance of Cooperative Networks with Relay Selection,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 12, pp. 4161–4171, Dec. 2011.

[10] T. Wang, C. K. Wen, H. Wang, T. Jiang, and S. Jin, “Deep Learning for Wireless Physical Layer: Opportunities and Challenges,” *China Communications*, vol. 14, no. 11, pp. 92–111, Nov. 2017.

[11] K. E. Baddour and N. C. Beaulieu, “Autoregressive Modeling for Fading Channel Simulation,” *IEEE Transactions on Wireless Communications*, vol. 4, no. 4, pp. 1650–1662, Jul. 2005.

[12] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, “Secrecy Sum-Rates for Multi-User MIMO Regularized Channel Inversion Precoding,” *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, Nov. 2012.

[13] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, Academic Press, London, 5th edition, 1994.

[14] A. Gers, J. Schmidhuber, F. Cummins, “Learning to forget: Continual prediction with LSTM,” Neural Computation, vol. 12, no. 10, pp. 2451–2471, 2000.

[15] S. Hochreiter, J. Schmidhuber, “Long short-term memory,” Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997.