Research Article

Wiretap Channel with Rate-Limited Channel State Information

Xinxing Yin, Liang Pang, and Zhi Xue

Department of Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Correspondence should be addressed to Xinxing Yin; yinxinxing@sjtu.edu.cn

Received 21 March 2014; Revised 12 July 2014; Accepted 21 July 2014

Academic Editor: Qinggang Meng

Copyright © 2015 Xinxing Yin et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We revisit a channel coding problem where the channel state information (CSI) is rate-limited (or coded) and available to the channel encoder. A wiretapper is added into this model, and the confidential message is intended only for the legal receiver and should be kept from being eavesdropped by the wiretapper. Equivocation analysis is provided to evaluate the level of information leakage to the wiretapper. We characterize an achievable rate-equivocation region as well as an outer bound for this security model. To achieve the rate-equivocation triples, we propose an efficient coding scheme, in which the coded CSI serves as the CSI for the channel encoder, based on *Gel'fand and Pinsker's coding* and *Wyner's random coding*. Furthermore, an example of Gaussian wiretap channel with rate-limited CSI is presented, of which a lower bound on the secrecy capacity is obtained. By simulation, we find there exists an optimal rate of the coded CSI at which the biggest secrecy transmission rate of the Gaussian case is achieved.

1. Introduction

The problem of coding for channels with CSI has been studied actively. In these models, CSI is generated by nature and provided to the transmitter and/or to the receiver in a causal or noncausal manner. Shannon first studied the discrete memoryless channel (DMC) with causal CSI only at the encoder and got its capacity [1]. It was found that the capacity was the same as the capacity of the DMC without CSI. The problem where CSI was only noncausally known to the channel encoder was solved by Gel'fand and Pinsker [2]. They showed a different capacity expression from [1] and provided a different coding strategy which was now known as *Gel'fand and Pinsker's coding*. The key idea of *Gel'fand and Pinsker's coding* is that the codeword chosen for the transmitted message is jointly typical with the state sequence. Actually, the capacity for the causal case in [1] can be got from [2] by letting the auxiliary random variable be independent of CSI. Some other extended channel models with CSI at both the encoder and the decoder were studied in [3–7]. Among them, Heegard and El Gamal first investigated a more practical channel with the unique feature that CSI at encoder and decoder was subject to a rate constraint [3]. The motivation of this unique feature, that is, rate-limited CSI, was that

CSI was transmitted over way-side channels for which only limited resources (bandwidth, operation time, memory, etc.) of the system were allocated. They only gave inner bounds on the capacity region for this model. Rosenzweig et al. then revisited this model and gave the capacity region of the model with rate-limited CSI at encoder and full CSI at the decoder [4]. For the model where CSI was fully known at the encoder and rate-limited at the decoder, capacity region was obtained in [5].

It is known that secure information transmission is an essential communication requirement. The above state-dependent channel models [1–7] considered no secrecy constraint. Recently, the works [8–15] have introduced the wiretapper in channels with CSI to model a safe communication model. Chen and Vinck explored the discrete memoryless wiretap channel with noncausal CSI and presented an achievable rate-equivocation region [8]. The region was established using a combination of *Gel'fand and Pinsker's coding* and *Wyner's random coding*. They showed that CSI helped to get a larger secrecy capacity for the Gaussian wiretap channel. In [9], an achievable rate-equivocation region for the Gaussian wiretap with side information was given. The authors proposed a perfect-secrecy-achieving coding strategy for the model based on code-partition technique.

FIGURE 1: Wiretap channel with rate-limited channel state information at the encoder.

The code-partition technique divided a random code into bins so that high rates could be achieved with asymptotic perfect secrecy. Dai and Luo improved the results of [8] by providing upper bounds on the secrecy capacity [10]. Liu and Chen got a lower bound on the secrecy capacity of the model where CSI was available noncausally at both the encoder and the decoder [11], and an upper bound was established by [12]. Action-dependent channel models involving secrecy were studied in [13–15]. Dai et al. provided the inner and outer bounds on the capacity-equivocation region for the wiretap channel with action-dependent states [13]. Then, they extended the model by adding a noiseless feedback link between the transmitter and receiver [14], in which the feedback served as a secret key. We restricted the rate of the feedback by introducing a rate-limited feedback link and obtained the corresponding capacity-equivocation region. Then, we explored information embedding on the actions in wiretap channel where part of the message was embedded on the actions [15] and characterized the tradeoff between the sum secrecy rate and the information embedding rate.

We are motivated to revisit a state-dependent channel model by adding a wiretapper (shown in Figure 1), that is, discrete memoryless wiretap channel with rate-limited channel state information. The CSI is known to the encoder and not known to the decoder. In our setup, the CSI at the encoder is subject to a rate constraint R_s , as in the work [3]. Note that the CSI in previous works considered that secrecy constraint [8, 10] was rate-unlimited, which is different from our rate-limited setup. However, we will later see that the model in [8, 10] is actually a special case of our model. In addition, the confidential message is intended only for the receiver and should be kept secret from the wiretapper as much as possible.

To the best of our knowledge, the model in Figure 1 involving secure information transmission has not been explored. Our goal is to characterize the inner and outer bounds on the capacity-equivocation region of the model. Particularly, we are interested in getting the corresponding bounds on the secrecy capacity for which perfect secrecy is realized. The perfect secrecy means that no information is leaked to the wiretapper. We also provide efficient coding schemes to achieve the rate-equivocation triple by means of *Gelfand and Pinsker's coding* and *Wyner's random coding*. Moreover, an example of Gaussian wiretap channel with rate-limited CSI is given and its lower bound on the secrecy capacity is also calculated. The simulation results show that there exists an optimal rate of the coded CSI at which the

biggest secrecy transmission rate of the Gaussian example is achieved.

The remainder of the paper is organized as follows. Section 2 describes the wiretap channel with rate-limited CSI and outlines the inner and outer bounds on the capacity-equivocation region. Section 3 calculates the corresponding bounds on the secrecy capacity and presents an example. Section 4 proposes a coding scheme to achieve the rate-equivocation triples and gives the outer bound proof. We conclude in Section 5 with a summary of the whole work and some future directions.

2. Channel Model and Main Results

In this section, the model of wiretap channel with rate-limited CSI is described. Then, we present the inner and outer bounds on the capacity-equivocation region.

2.1. Channel Model. In this paper, calligraphic letters, for example, $\mathcal{X}$, are used to denote the finite sets. We use $\|\mathcal{X}\|$ to denote the cardinality of the set $\mathcal{X}$. We use Z_i^j to denote the $(j - i + 1)$ vectors $(Z_i, Z_{i+1}, \dots, Z_j)$ of random variables for $1 \leq i \leq j$ and will always drop the subscript when $i = 1$. Besides, for $X \sim p(x)$ and $0 \leq \epsilon \leq 1$, the set of the typical N -sequences x^N is defined as $\mathcal{T}_X^N(\epsilon) = \{x^N : |\pi(x | x^N) - p(x)| \leq \epsilon p(x) \text{ for all } x \in \mathcal{X}\}$, where $\pi(x | x^N)$ denotes the frequency of occurrences of letter x in the sequence x^N . The set of the jointly typical sequences, for example, $\mathcal{T}_{XY}^N(\epsilon)$, follows similarly. The base of the log function in this paper is 2.

The channel model is described as follows. We consider the rate-limited CSI setup where a rate-limited description of the channel states is provided to the channel encoder. This setup is motivated by the limited capacity of the channel over which the channel states are transmitted. The input of the state encoder is the channel state S^N which is independently and identically distributed (i.i.d) $\sim p(s)$, and the output is $M_s \in \{1, 2, \dots, 2^{NR_s}\}$. The channel encoder encodes the messages M and M_s into X^N . The main channel is a DMC with discrete input alphabet $\mathcal{X} \times \mathcal{S}$ and output alphabet $\mathcal{Y}$. The channel is memoryless in the sense that $p(y^N | x^N, s^N) = \prod_{i=1}^N p(y_i | x_i, s_i)$, where $y^N \in \mathcal{Y}^N$, $x^N \in \mathcal{X}^N$, and $s^N \in \mathcal{S}^N$. The receiver decodes the message with the observation Y^N . The output of the decoder is $\hat{M}$. The probability of error for the decoder is defined as $P_e = \Pr\{\hat{M} \neq M\}$. The wiretap channel is also a DMC with input Y^N and output Z^N . The wiretap channel is memoryless in the sense that $p(z^N | y^N) = \prod_{i=1}^N p(z_i | y_i)$, where $z^N \in \mathcal{Z}^N$. The uncertainty of the message for the wiretapper is measured by $\lim_{N \rightarrow \infty} \Delta = \lim_{N \rightarrow \infty} (H(M | Z^N)/N)$.

A $(2^{NR}, 2^{NR_s}, N)$ code for the model in Figure 1 includes a state encoder, channel encoder, and decoder. The state encoder $g_1 : \mathcal{S}^N \rightarrow \mathcal{M}_s$ maps the state sequence s^N into m_s , where $m_s \in \mathcal{M}_s = \{1, 2, \dots, 2^{NR_s}\}$. The stochastic channel encoder g_2 is specified by a matrix of conditional probability

distributions $g_2(x^N | m, m_s)$, where $m \in \mathcal{M} = \{1, 2, \dots, 2^{NR}\}$. Note that $\sum_{x^N} g_2(x^N | m, m_s) = 1$ and $g_2(x^N | m, m_s)$ is the probability that the messages m and m_s are encoded as the channel input x^N . The decoder $g_3 : \mathcal{Y}^N \rightarrow \mathcal{M}$ maps the output sequence y^N into decoded message $\hat{m}$. Before stating the main results, we give the definitions of “achievable” and “secrecy capacity” as follows.

Definition 1. A rate-equivocation triple (R, R_s, R_e) is said to be *achievable* for the model in Figure 1 if there exists a $(2^{NR}, 2^{NR_s}, N)$ code such that

$$\lim_{N \rightarrow \infty} \frac{\log \|\mathcal{M}\|}{N} = R, \quad (1)$$

$$\lim_{N \rightarrow \infty} \frac{\log \|\mathcal{M}_s\|}{N} = R_s,$$

$$\lim_{N \rightarrow \infty} \frac{H(M | Z^N)}{N} \geq R_e, \quad (2)$$

$$P_e \leq \epsilon, \quad (3)$$

where ϵ is an arbitrary small positive real number, R is the rate of the message M , R_s is the rate of the coded message M_s , and R_e is the rate of equivocation. The capacity-equivocation region is defined as the convex closure of all achievable rate-equivocation triples (R, R_s, R_e) .

Definition 2. The *secrecy capacity* is the maximum rate at which the confidential message can be sent to the receiver in perfect secrecy with the constraint on R_s . The secrecy capacity is

$$C_s = \max_{(R, R_s, R_e=R) \in \mathcal{R}, R_s \geq \Gamma} R, \quad (4)$$

where $\mathcal{R}$ is the capacity-equivocation region and Γ is the constraint condition of rate R_s .

2.2. Main Results. We first give an achievable rate-equivocation region for the wiretap channel with rate-limited CSI and then present an outer bound. Some comments on the theorems are given subsequently. Further discussion about the results and comparison with other existing models are shown in Section 3.

Theorem 3. An inner bound on the capacity-equivocation region of the wiretap channel with rate-limited CSI is the set

$$\begin{aligned} \mathcal{R}_i = \{ & (R, R_s, R_e) : \\ & R \leq I(V; Y) - I(V; U), \\ & R_s \geq I(U; S), \\ & R_e \leq R, \\ & R_e \leq I(V; Y) - \max\{I(V; Z), I(V; U)\} \}, \end{aligned} \quad (5)$$

where $V \rightarrow (X, U) \rightarrow Y \rightarrow Z$ form a Markov chain.

Theorem 4. An outer bound on the capacity-equivocation region of the wiretap channel with rate-limited CSI is the set

$$\begin{aligned} \mathcal{R}_o = \{ & (R, R_s, R_e) : \\ & R \leq I(V; Y) - I(V; S | U), \\ & R_s \geq I(U; S), \\ & R_e \leq R, \\ & R_e \leq I(V; Y) - I(V; S | K_2) - I(K_2; Z | K_1) \}, \end{aligned} \quad (6)$$

where $U \rightarrow V \rightarrow S, U \rightarrow K_2 \rightarrow K_1$, and $(V, K_1, K_2) \rightarrow (X, U) \rightarrow Y \rightarrow Z$ form Markov chains.

We have the following comments:

- (1) The sets $\mathcal{R}_i$ and $\mathcal{R}_o$ are convex; the proof is similar to the proof of Proposition 1 in [5].
- (2) Theorem 3 tells that any rate-equivocation triple belonging to $\mathcal{R}_i$ is achievable. Theorem 4 tells that all achievable rate-equivocation triples are contained in $\mathcal{R}_o$. The capacity-equivocation region of the model in Figure 1 is between $\mathcal{R}_i$ and $\mathcal{R}_o$.
- (3) Equivocation was introduced by Wyner [16] to measure the amount of information leaked to the wiretapper. It is always wished that as large as possible equivocation for the wiretapper can be achieved at any acceptable rate of reliable transmission to the legitimate receiver. From the formulas of $\mathcal{R}_i$, it is obvious that if $(R, R_s, R_e = I(V; Y) - \max\{I(V; Z), I(V; U)\})$ is achievable, the rate-equivocation triples (R, R_s, R'_e) are also achievable for every $R'_e \leq I(V; Y) - \max\{I(V; Z), I(V; U)\}$. This reminds us that it is sufficient to show that $(R, R_s, R_e = I(V; Y) - \max\{I(V; Z), I(V; U)\})$ is achievable.
- (4) We are considerably interested in finding the maximum secrecy rate when $R_e = R$ which implies perfect secrecy. It is explained as follows. Since $\lim_{N \rightarrow \infty} (H(M | Z^N)/N) \geq R_e$ and $\lim_{N \rightarrow \infty} (H(M)/N) = R$, we can get $\lim_{N \rightarrow \infty} (H(M | Z^N)/N) \geq \lim_{N \rightarrow \infty} (H(M)/N)$ when $R_e = R$. Since conditioning does not increase entropy, we have $\lim_{N \rightarrow \infty} (H(M | Z^N)/N) = \lim_{N \rightarrow \infty} (H(M)/N)$, which indicates that no information was leaked to the wiretapper.
- (5) The proof of the two theorems is given in Section 4, in which we construct a coding scheme to achieve the rate-equivocation triple in $\mathcal{R}_i$ based on *Gelfand and Pinsker's coding* and *Wyner's random coding*. We also give the identification of the auxiliary random variables in the outer bound proof.

Further discussion about the theorems and the comparison with other existing results are given in Section 3.

3. Discussion and Gaussian Example

In this section, we first calculate the lower and upper bounds on the secrecy capacity of the model in Figure 1. Subsequently, we compare our results with other existing state-dependent channel models. Then, we provide a (physically) degraded example of Gaussian wiretap channel with rate-limited CSI and calculate a lower bound on the secrecy capacity subject to a rate constraint on R_s . By simulation, we find that there exists an optimal rate of the coded CSI at which the biggest secrecy transmission rate of the Gaussian example is achieved.

3.1. Discussion and Comparison. The lower and upper bounds on the secrecy capacity are presented in Corollary 5.

Corollary 5. *The lower and upper bounds on the secrecy capacity of wiretap channel with rate-limited CSI are*

$$C_l = \max_{p(u,v,x,s), R_s \geq I(U;S)} \{I(V;Y) - \max\{I(V;Z), I(V;U)\}\}, \quad (7)$$

$$C_u = \max_{p(u,v,k_1,k_2,x,s), R_s \geq I(U;S)} \min\{I(V;Y) - I(V;S|U), \\ I(V;Y) - I(V;S|K_2) - I(K_2;Z|K_1)\}, \quad (8)$$

respectively.

Proof. We first prove (8). According to the definition of formula (4), we let $R_e = R$ in $\mathcal{R}_o$ and then get the upper bounds on R subject to $R_s \geq I(U;S)$ as follows. Consider

$$R \leq I(V;Y) - I(V;S|U), \quad (9)$$

$$R \leq I(V;Y) - I(V;S|K_2) - I(K_2;Z|K_1).$$

Based on the definition of secrecy capacity, (9), we prove (8). Similarly, substituting $R_e = R$ into $\mathcal{R}_i$, we get the upper bounds on R subject to $R_s \geq I(U;S)$ as

$$R \leq I(V;Y) - I(V;U), \quad (10)$$

$$R \leq I(V;Y) - \max\{I(V;Z), I(V;U)\}. \quad (11)$$

Formula (10) can be obtained from (11). Hence, according to the definition of secrecy capacity and (11), formula (7) is proved. $\square$

The comparison of the secrecy capacity between [10] and our results is given as follows. We first present Dai's main results in [10].

Dai and Luo [10] characterized the lower and upper bounds on the secrecy capacity of wiretap channel with full and noncausal CSI at the encoder, depicted in Figure 2, as

$$C_{\text{ldai}} = \max_{p(v,x,s)} \{I(V;Y) - \max\{I(V;Z), I(V;S)\}\}, \quad (12)$$

$$C_{\text{udai}} = \max_{p(v,k_1,k_2,x,s)} \min\{I(V;Y) - I(V;S), \\ I(V;Y) - I(K_2;Z|K_1)\}, \quad (13)$$

respectively.

FIGURE 2: Wiretap channel with full CSI at the encoder.

The comparison is listed below.

- (1) The lower bounds (7) and (12) share the same expression. We note that, in the rate-limited CSI setup, CSI is not directly known to the channel encoder. The CSI is encoded by the state encoder, and it is the coded version that serves as the channel states to the channel encoder. In the coding scheme (presented in Section 4), the coded CSI U serves as the CSI S in the jointly typical encoding. Based on this observation, it is easy to see that (7) and (12) share the same expression (without considering the constraint on rate of the coded CSI).
- (2) For deriving the upper bounds (8) and (13), the auxiliary random variables are different. In [10], there are three auxiliary random variables K_2 , K_1 , and V , while there are four auxiliary random variables K_2 , K_1 , U , and V in our derivations. The detailed expression of these random variables is given in Section 4.
- (3) Besides, in Theorem 4, we have the Markov chain $U \rightarrow V \rightarrow S$. Then,

$$\begin{aligned} I(V;S|U) &= I(V,U;S) - I(U;S) \\ &= I(V;S) + I(U;S|V) - I(U;S) \quad (14) \\ &= I(V;S) - I(U;S), \end{aligned}$$

where (14) is from the Markov chain $U \rightarrow V \rightarrow S$. If we let U be independent of S , the conditional mutual information $I(V;S|U) = I(V;S)$. In this case, it is easy to see $C_u \leq C_{\text{udai}}$.

3.2. Gaussian Example. In this subsection, we look at the (physically) degraded Gaussian wiretap channel with rate-limited CSI shown in Figure 3. We treat $\eta_1 \sim \mathcal{N}(0, N_1)$ and $\eta_2 \sim \mathcal{N}(0, N_2)$ in Figure 3 as noise. Let $S \sim \mathcal{N}(0, Q)$ and $U = S$. Similarly to [8, 9], consider $V = X + \alpha U$, where X and U are independent from each other and X is distributed as $X \sim \mathcal{N}(0, P)$. The parameter α is to be determined. We assume that the correlation coefficient of X and S is ρ_{XS} . Then, using similar derivations in [8, 9], we have

$$\begin{aligned} I(V;Y) &= \log(f(N_1)), \\ I(V;Z) &= \log(f(N_1 + N_2)), \\ I(V;U) &= I(V;S) = \Lambda_1, \\ I(U;S) &= H(S) = \Lambda_2, \end{aligned} \quad (15)$$

FIGURE 3: Gaussian wiretap channel with rate-limited channel state information at the encoder.

where

$$f(N) = \left[\left(P + \alpha^2 Q + 2\alpha(PQ)^{1/2} \rho_{XS} \right) \times \left(P + Q + N + 2(PQ)^{1/2} \rho_{XS} \right) \times \left((1 - \alpha)^2 PQ (1 - \rho_{XS}^2) \right) + N \left(P + \alpha^2 Q + 2\alpha(PQ)^{1/2} \rho_{XS} \right) \right]^{-1/2}, \quad (16)$$

$$\Lambda_1 = \log \left[\frac{P + \alpha^2 Q + 2\alpha(PQ)^{1/2} \rho_{XS}}{P(1 - \rho_{XS}^2)} \right]^{1/2},$$

$$\Lambda_2 = \log (2\pi e Q)^{1/2}.$$

Note that the expressions of $I(V; Y)$, $I(V; Z)$, $I(V; U)$ are the same as those in [8, 9], and the difference is that here we have the rate constraint on R_s ; that is, $R_s \geq \Lambda_2$.

Applying Corollary 5, we get the lower bound on the secrecy capacity of the Gaussian case as

$$C_{IG}(\alpha) = \min \{ \log f(N_1) - \log f(N_1 + N_2), \log f(N_1) - \Lambda_1 \}, \quad (17)$$

which is subject to the constraint $R_s \geq \Lambda_2$. The graph of $C_{IG}(\alpha)$ as a function of α for fixed P, Q, N_1, N_2 , and ρ_{XS} is presented in Figure 4. It can be seen that, for the six cases in Figure 4, the lower bound on the secrecy capacity achieves the maximum value at different values of α . By setting a proper value to the parameter α , we can achieve the maximum value of $C_{IG}(\alpha)$. Besides, we see that when the noise power of the wiretap channel decreases (or the noise power of the main channel increases), $C_{IG}(\alpha)$ is reduced. This is straightforward.

Moreover, if we let $R_s = I(U; S)$, the lower bound C_{IG} can be expressed as a function of R_s when P, N_1, N_2, ρ_{XS} , and α are fixed. When P, N_1, N_2, ρ_{XS} , and α are fixed at certain values, the graph of $C_{IG}(R_s)$ as a function of R_s is depicted in Figure 5. Five different cases are considered:

- (1) $P = N_1 = N_2 = 1, \rho_{XS} = 0, \alpha = 1$. The noise power of the main channel and wiretap is big, and variable X is independent of S ; that is, $\rho_{XS} = 0$;
- (2) $P = N_1 = N_2 = 1, \rho_{XS} = 0.5, \alpha = 0.35$. The noise power of the main channel and wiretap is big, and variable X is not independent of S ;

FIGURE 4: $C_{IG}(\alpha)$ as a function of α .

- (3) $P = 1, N_1 = N_2 = 0.5, \rho_{XS} = 0.5, \alpha = 1$. The noise power of the main channel and wiretap is small, and variable X is not independent of S ;
- (4) $P = N_1 = 1, N_2 = 0.5, \rho_{XS} = 0.5, \alpha = 0.85$. Wiretap channel is less noisy than main channel, and variable X is not independent of S ;
- (5) $P = N_2 = 1, N_1 = 0.5, \rho_{XS} = 0.5, \alpha = 0.85$. Main channel is less noisy than wiretap channel, and variable X is not independent of S .

It can be seen that, in general, when R_s is small, $C_{IG}(R_s)$ increases with R_s . However, there exists an optimal value of R_s at which $C_{IG}(R_s)$ is the biggest. When R_s is bigger than the optimal value, $C_{IG}(R_s)$ decreases. On the one hand, we see that, for case 1 where variable X is independent of S , secrecy rate $C_{IG}(R_s)$ decreases sharply with the CSI rate R_s (when R_s passes the optimal value). On the other hand, when variable X is not independent of S (case 2–5), $C_{IG}(R_s)$ decreases slowly with R_s .

Besides, comparing cases 2 and 3, we find that the smaller the noise power is, the higher the secrecy rate $C_{IG}(R_s)$ is. This means if information transmission happens in good channels, we can achieve higher secrecy transmission rate.

Furthermore, comparing cases 4 and 5, it can be seen that when the main channel is less noisy than the wiretap channel, higher secrecy rate $C_{IG}(R_s)$ is achieved. This result is straightforward since the main channel is better than the wiretap channel.

FIGURE 5: $C_{IG}(R_s)$ as a function of R_s .

4. Proof of Theorems 3 and 4

In this section, two theorems in Section 2 are proved. To show Theorem 3, we construct a coding scheme to achieve the rate-equivocation triple in $\mathcal{R}_i$ based on *Gel'fand and Pinsker's coding* and *Wyner's random coding* and give the equivocation analysis in Section 4.1. Then, we prove Theorem 4 and give the identification of the auxiliary random variables in Section 4.2.

4.1. Proof of Theorem 3. We show that all triples $(R, R_s, R_e) \in \mathcal{R}_i$ are achievable. Concretely, we need to prove that any rate-equivocation triple $(R, R_s, R_e) \in \mathcal{R}_i$ and decoding error probability P_e satisfy

$$\begin{aligned}
 R &= \lim_{N \rightarrow \infty} \frac{\log \|\mathcal{M}\|}{N}, \\
 R_s &= \lim_{N \rightarrow \infty} \frac{\log \|\mathcal{M}_s\|}{N}, \\
 R_e &\leq \lim_{N \rightarrow \infty} \frac{H(M | Z^N)}{N}, \\
 P_e &\leq \epsilon.
 \end{aligned} \tag{18}$$

It is obvious that if $(R, R_s, R_e = I(V; Y) - \max(I(V; Z), I(V; U)))$ is achievable, the rate-equivocation triples (R, R_s, R'_e) are also achievable for every $R'_e \leq I(V; Y) - \max(I(V; Z), I(V; U))$. Therefore, we try to prove $(R, R_s, R_e = I(V; Y) - \max(I(V; Z), I(V; U)))$ is achievable.

Let $R = I(V; Y) - I(V; U) - \lambda$, where λ is a fixed positive number. Since $R_e \leq R$, we can get $\lambda \leq \max(I(V; Z), I(V; U)) - I(V; U)$. For each $m_s \in \{1, 2, \dots, 2^{NR_s}\}$, an i.i.d sequence

FIGURE 6: Codebook structure.

$u^N(m_s)$ is generated according to $p(u^N) = \prod_{i=1}^N p(u_i)$. We find a $u^N(m_s)$ such that $(u^N(m_s), s^N) \in \mathcal{T}_{US}^N$. Let the message M be uniformly distributed over $\mathcal{M}$. Then, we generate $2^{N(I(V; Y) - \epsilon)}$ i.i.d codewords v^N according to $p(v^N) = \prod_{i=1}^N p(v_i)$. These codewords are put into 2^{NR} bins such that each bin contains $2^{N(I(V; Y) - R - \epsilon)}$ codewords. The index of the bin is denoted by $t_b \in \{1, 2, \dots, 2^{NR}\}$. The codewords in each bin are put into $\|T_{sb}\| = 2^{N(\max(I(V; Z), I(V; U)) - I(V; Z) + \epsilon_1)}$ subbins which are indexed by $t_{sb} \in \{1, 2, \dots, 2^{N(\max(I(V; Z), I(V; U)) - I(V; Z) + \epsilon_1)}\}$. The number of the codewords in each subbin is $2^{N(I(V; Y) - R - \epsilon)} / \|T_{sb}\|$. We use t_v to index the codeword in the subbin. The codebook structure is presented in Figure 6.

To send m , the transmitter tries to find a $v^N(t_b, t_{sb}, t_v)$ such that $(v^N(t_b, t_{sb}, t_v), u^N(m_s)) \in \mathcal{T}_{VU}^N$ in the bin indexed by $t_b = m$. Then, the input sequence of the main channel is generated by $p(x^N | v^N, s^N) = \prod_{i=1}^N p(x_i | v_i, s_i)$.

To decode the message, the decoder finds a unique codeword $v^N(\hat{t}_b, \hat{t}_{sb}, \hat{t}_v)$ such that $(v^N(\hat{t}_b, \hat{t}_{sb}, \hat{t}_v), y^N) \in \mathcal{T}_{VY}^N$ and outputs $\hat{m} = \hat{t}_b$. Since the number of the codewords v^N is $2^{N(I(V; Y) - \epsilon)}$, this decoding step succeeds with high probability. Moreover, the number of $u^N(m_s)$ is $2^{NR_s} \geq 2^{NI(U; S)}$, so we can find a $u^N(m_s)$ such that $(u^N(m_s), s^N) \in \mathcal{T}_{US}^N$ with high probability. Similarly, since each bin contains $2^{N(I(V; Y) - R - \epsilon)} = 2^{N(I(V; U) + \lambda - \epsilon)}$ codewords v^N , the error probability of finding

a $v^N(t_b, t_{sb}, t_v)$ such that $(v^N(t_b, t_{sb}, t_v), u^N(m_s)) \in \mathcal{T}_{VU}^N$ in a given bin indexed by t_b approaches zero.

We focus on analyzing the uncertainty of M given the wiretapper's observation Z^N . Consider

$$\begin{aligned}
H(M | Z^N) &= H(M, Z^N) - H(Z^N) \\
&= H(M, Z^N, V^N) - H(V^N | M, Z^N) \\
&\quad - H(Z^N) \\
&= H(M, V^N) + H(Z^N | M, V^N) \\
&\quad - H(V^N | M, Z^N) - H(Z^N) \\
&\geq H(V^N) + H(Z^N | V^N) \\
&\quad - H(V^N | M, Z^N) - H(Z^N) \\
&\geq H(V^N) - I(V^N; Z^N) \\
&\quad - H(T_{sb}, V^N | M, Z^N) \\
&= H(V^N) - I(V^N; Z^N) - H(T_{sb} | M, Z^N) \\
&\quad - H(V^N | M, Z^N, T_{sb}) \\
&\geq I(V^N; Y^N) - I(V^N; Z^N) \\
&\quad - H(T_{sb}) - H(V^N | M, Z^N, T_{sb}) \\
&\geq NI(V; Y) - NI(V; Z) \\
&\quad - H(T_{sb}) - H(V^N | M, Z^N, T_{sb}), \tag{20}
\end{aligned}$$

where (19) is from the Markov chain $M \rightarrow V^N \rightarrow Z^N$ and (20) is from the fact that the codewords v^N are i.i.d and the channels are discrete memoryless.

Next, we bound $H(T_{sb})$ and $H(V^N | M, Z^N, T_{sb})$ in (20). Since $\|\mathcal{T}_{sb}\| = 2^{N(\max\{I(V;U), I(V;Z)\} - I(V;Z) + \epsilon_1)}$, we have $H(T_{sb}) \leq \log \|\mathcal{T}_{sb}\| = N(\max\{I(V;U), I(V;Z)\} - I(V;Z) + \epsilon_1)$.

The explanation for bounding $(1/N)H(V^N | M, Z^N, T_{sb})$ is presented as follows. We first show that, given M and T_{sb} , the probability of error for Z^N to decode V^N satisfies $P'_e \leq \nu$. Here, ν is small for sufficiently large N . Given the knowledge of M and T_{sb} , the total number of possible codewords of V^N is

$$\begin{aligned}
\frac{2^{N(I(V;Y) - R - \epsilon)}}{\|\mathcal{T}_{sb}\|} &= \frac{2^{N(I(V;Y) - R - \epsilon)}}{2^{N(\max\{I(V;Z), I(V;U)\} - I(V;Z) + \epsilon_1)}} \\
&= 2^{N(I(V;U) + \lambda - \epsilon - \max\{I(V;Z), I(V;U)\} + I(V;Z) - \epsilon_1)} \\
&\leq 2^{N(I(V;Z) - \epsilon - \epsilon_1)} \\
&\leq 2^{NI(V;Z)}, \tag{22}
\end{aligned}$$

where (21) is from $\lambda \leq \max\{I(V;Z), I(V;U)\} - I(V;U)$. Based on (22), we can easily show that a unique codeword $v^N(t_b, t_{sb}, t_v)$ exists such that $(v^N(t_b, t_{sb}, t_v), z^N) \in T_{VZ}^N$ with high probability. This indicates that the probability of error for Z^N to decode V^N satisfies $P'_e \leq \nu$. Therefore, by Fano's inequality, we obtain

$$\begin{aligned}
&\frac{1}{N}H(V^N | M, Z^N, T_{sb}) \\
&\leq \frac{1}{N} \left(1 + P'_e \log \left(\frac{2^{N(I(V;Y) - R - \epsilon)}}{\|\mathcal{T}_{sb}\|} \right) \right) \leq \nu', \tag{23}
\end{aligned}$$

where ν' is small for sufficiently large N .

Substituting these two results into (20) and utilizing (2), we finish the proof of $\lim_{N \rightarrow \infty} \Delta \geq R_e$ for the model in Figure 1 with rate-limited CSI. The proof of Theorem 3 is completed.

4.2. Proof of Theorem 4. We need to prove that all achievable rate-equivocation triples (R, R_s, R_e) are contained in $\mathcal{R}_o$. Precisely, for any triple (R, R_s, R_e) satisfying (1), (2), and (3), we need to show

$$R \leq I(V; Y) - I(V; S | U), \tag{24}$$

$$R_s \geq I(U; S), \tag{25}$$

$$R_e \leq R, \tag{26}$$

$$R_e \leq I(V; Y) - I(V; S | K_2) - I(K_2; Z | K_1). \tag{27}$$

Condition (24) is proved as follows. Consider

$$\begin{aligned}
R &= \lim_{N \rightarrow \infty} \frac{\log \|\mathcal{M}\|}{N} \\
&= \lim_{N \rightarrow \infty} \frac{H(M)}{N} \\
&= \lim_{N \rightarrow \infty} \frac{1}{N} [I(M; Y^N) + H(M | Y^N)] \\
&\leq \lim_{N \rightarrow \infty} \frac{1}{N} [I(M; Y^N) + \delta(P_e)], \tag{28}
\end{aligned}$$

where (28) is from the fact that M is uniformly distributed over $\mathcal{M}$ and (29) is from Fano's inequality. The term $I(M; Y^N)$ is calculated as follows. Consider

$$I(M; Y^N) = I(M; Y^N) - I(M; S^N) \tag{30}$$

$$= I(M; Y^N) - I(M; S^N | M_s) \tag{31}$$

$$\begin{aligned}
&= \sum_{i=1}^N I(M; Y_i | Y_{i+1}^N) - \sum_{i=1}^N I(M; S_i | S^{i-1}, M_s) \\
&= \sum_{i=1}^N [I(M, S^{i-1}, M_s; Y_i | Y_{i+1}^N) \\
&\quad - I(S^{i-1}, M_s; Y_i | M, Y_{i+1}^N)] \\
&\quad - \sum_{i=1}^N [I(M, Y_{i+1}^N; S_i | S^{i-1}, M_s) \\
&\quad - I(Y_{i+1}^N; S_i | M, S^{i-1}, M_s)] \\
&= \sum_{i=1}^N [I(M, S^{i-1}, M_s; Y_i | Y_{i+1}^N) \\
&\quad - I(M, Y_{i+1}^N; S_i | S^{i-1}, M_s)] \\
&\leq \sum_{i=1}^N [I(M, S^{i-1}, M_s; Y_{i+1}^N; Y_i) \\
&\quad - I(M, Y_{i+1}^N, S^{i-1}, M_s; S_i | S^{i-1}, M_s)] \\
&\leq \sum_{i=1}^N [I(V_i; Y_i) - I(V_i; S_i | U_i)].
\end{aligned} \tag{32}$$

$$\leq \sum_{i=1}^N [I(V_i; Y_i) - I(V_i; S_i | U_i)]. \tag{33}$$

In the above derivation, formula (30) is from the fact that the message is independent of the state sequence. Therefore, we have $I(M; S^N) = 0$. Formula (31) is from the fact that $I(M; S^N | M_s) = 0$ which is proved in (35). Consider

$$\begin{aligned}
I(M; S^N | M_s) &= H(M | M_s) - H(M | S^N, M_s) \\
&\leq H(M) - H(M | S^N) \\
&= I(M; S^N) \\
&= 0,
\end{aligned} \tag{34}$$

$$= 0, \tag{35}$$

where (34) is from the fact that M_s is a function of S^N and the fact that conditioning does not increase entropy. Formula (32) is from the sum equality in (36). One has

$$\sum_{i=1}^N I(S^{i-1}, M_s; Y_i | M, Y_{i+1}^N) = \sum_{i=1}^N I(Y_{i+1}^N; S_i | M, S^{i-1}, M_s). \tag{36}$$

The sum equality (36) can be proved using similar methods in [13, 17]. Formula (33) is from defining $V_i = (M, S^{i-1}, M_s, Y_{i+1}^N)$ and $U_i = (S^{i-1}, M_s)$.

Condition (25) is proved as follows. Consider

$$\begin{aligned}
R_s &= \frac{\log \|\mathcal{M}_s\|}{N} \\
&\geq \frac{H(M_s)}{N} \\
&= \frac{1}{N} I(M_s; S^N)
\end{aligned} \tag{37}$$

$$\begin{aligned}
&= \frac{1}{N} \sum_{i=1}^N I(M_s; S_i | S^{i-1}) \\
&= \frac{1}{N} \sum_{i=1}^N I(M_s, S^{i-1}; S_i) \\
&= \frac{1}{N} \sum_{i=1}^N I(U_i; S_i),
\end{aligned} \tag{38}$$

where (37) is from the fact that S_i is independent of S^{i-1} .

Condition (26) is proved as follows. Consider

$$R_e \leq \lim_{N \rightarrow \infty} \frac{H(M | Z^N)}{N} \tag{39}$$

$$\begin{aligned}
&\leq \lim_{N \rightarrow \infty} \frac{H(M)}{N} \\
&= R,
\end{aligned} \tag{40}$$

where (39) is from (2).

To prove condition (27), we consider

$$\begin{aligned}
H(M | Z^N) &= H(M | Z^N) - H(M | Y^N) + H(M | Y^N) \\
&= H(M | Z^N) - H(M) + H(M) \\
&\quad - H(M | Y^N) + H(M | Y^N) \\
&= I(M; Y^N) - I(M; Z^N) + H(M | Y^N) \\
&\leq I(M; Y^N) - I(M; Z^N) + \delta(P_e).
\end{aligned} \tag{41}$$

The first two terms in (41) are calculated as follows.

From (32), one has

$$\begin{aligned}
I(M; Y^N) &= \sum_{i=1}^N [I(M, S^{i-1}, M_s; Y_i | Y_{i+1}^N) \\
&\quad - I(M, Y_{i+1}^N; S_i | S^{i-1}, M_s)].
\end{aligned} \tag{42}$$

Similarly, we can get

$$\begin{aligned}
I(M; Z^N) &= \sum_{i=1}^N [I(M, S^{i-1}, M_s; Z_i | Z_{i+1}^N) \\
&\quad - I(M, Z_{i+1}^N; S_i | S^{i-1}, M_s)].
\end{aligned} \tag{43}$$

Then, we substitute (42) and (43) into (41) and get

$$\begin{aligned}
& H(M | Z^N) \\
& \leq I(M; Y^N) - I(M; Z^N) + \delta(P_e) \\
& = \sum_{i=1}^N [I(M, S^{i-1}, M_s; Y_i | Y_{i+1}^N) \\
& \quad - I(M, Y_{i+1}^N; S_i | S^{i-1}, M_s)] \\
& \quad - \sum_{i=1}^N [I(M, S^{i-1}, M_s; Z_i | Z_{i+1}^N) \\
& \quad - I(M, Z_{i+1}^N; S_i | S^{i-1}, M_s)] + \delta(P_e) \\
& = \sum_{i=1}^N [I(M, S^{i-1}, M_s; Y_i | Y_{i+1}^N) \\
& \quad - I(M, Z_{i+1}^N, Y_{i+1}^N; S_i | S^{i-1}, M_s)] \\
& \quad - \sum_{i=1}^N [I(M, S^{i-1}, M_s; Z_i | Z_{i+1}^N) \\
& \quad - I(M, Z_{i+1}^N; S_i | S^{i-1}, M_s)] + \delta(P_e) \\
& = \sum_{i=1}^N [I(M, S^{i-1}, M_s; Y_i | Y_{i+1}^N) \\
& \quad - I(Y_{i+1}^N; S_i | M, Z_{i+1}^N, S^{i-1}, M_s)] \\
& \quad - \sum_{i=1}^N I(M, S^{i-1}, M_s; Z_i | Z_{i+1}^N) + \delta(P_e) \\
& \leq \sum_{i=1}^N [I(M, S^{i-1}, M_s; Y_{i+1}^N; Y_i) \\
& \quad - I(Y_{i+1}^N, M, S^{i-1}, M_s; S_i | M, Z_{i+1}^N, S^{i-1}, M_s)] \\
& \quad - \sum_{i=1}^N I(M, S^{i-1}, M_s, Z_{i+1}^N; Z_i | Z_{i+1}^N) + \delta(P_e) \\
& = \sum_{i=1}^N [I(V_i; Y_i) - I(V_i; S_i | K_{2i})] \\
& \quad - \sum_{i=1}^N I(K_{2i}; Z_i | K_{1i}) + \delta(P_e),
\end{aligned} \tag{44}$$

where (44) is from the Markov chain $S_i \rightarrow (S^{i-1}, M_s, Y_{i+1}^N) \rightarrow Z_{i+1}^N$ and (45) from defining $K_{2i} = (M, Z_{i+1}^N, S^{i-1}, M_s)$ and $K_{1i} = Z_{i+1}^N$.

To serve the single-letter characterization, let us introduce a time-sharing random variable J independent of

all other random variables and uniformly distributed over $\{1, 2, \dots, N\}$. Set

$$\begin{aligned}
U &= (U_J, J), & V &= (V_J, J), \\
K_2 &= (K_{2J}, J), & K_1 &= (K_{1J}, J) \\
S &= S_J, & X &= X_J, & Y &= Y_J, & Z &= Z_J.
\end{aligned} \tag{46}$$

Then, substituting the above new random variables into (33), (38), and (45), conditions (24), (25), and (27) are verified by standard time-sharing argument. From the definition of the auxiliary random variables, the Markov chains $U \rightarrow V \rightarrow S, U \rightarrow K_2 \rightarrow K_1$, and $(V, K_1, K_2) \rightarrow (X, U) \rightarrow Y \rightarrow Z$ are easily verified. We complete the proof of Theorem 4.

5. Conclusion

This paper has investigated the problem of rate-limited CSI in state-dependent channels under secrecy constraint. It is an extension of the rate-limited CSI setup without secrecy. This model is more general than the existing wiretap channel with full CSI at the transmitter. We proposed an achievable rate-equivocation region and an outer bound on the capacity-equivocation region. To achieve the rates, a proper coding scheme is constructed based on *Gel'fand and Pinsker's coding* and *Wyner's random coding*.

Our setup can be probably extended in the following directions.

- (i) In this current model as well as [1–7], the CSI is generated by nature. However, in some practical communication systems, the transmitter can take actions to affect the formation of the CSI. This idea called action-dependent states is from [18]. We can further explore the impact of the action-dependent states in the wiretap channel with rate-limited CSI.
- (ii) Only inner and outer bounds on the capacity-equivocation region are obtained at present. We can try to find some special cases where the two bounds match.
- (iii) In our model, the CSI is rate-limited and known to the encoder. We can study the model where the CSI is rate-limited and known to the decoder (or both the decoder and the encoder) under the secrecy constraint.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant nos. 61332010, 61171173, and 60932003.

References

- [1] C. E. Shannon, "Channels with side information at the transmitter," *Journal of Research and Development*, vol. 2, pp. 289–293, 1958.
- [2] S. I. Gelfand and M. S. Pinsker, "Coding for channel with random parameters," *Problems of Control and Information Theory*, vol. 9, no. 1, pp. 19–31, 1980.
- [3] C. Heegard and A. El Gamal, "On the capacity of computer memory with defects," *IEEE Transactions on Information Theory*, vol. 43, no. 6, pp. 1986–1992, 1997.
- [4] A. Rosenzweig, Y. Steinberg, and S. Shamai, "On channels with partial channel state information at the transmitter," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. 51, no. 5, pp. 1817–1830, 2005.
- [5] Y. Steinberg, "Coding for channels with rate-limited side information at the decoder, with applications," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4283–4295, 2008.
- [6] Y. Steinberg, "Coding for the degraded broadcast channel with random parameters, with causal and noncausal side information," *IEEE Transactions on Information Theory*, vol. 51, no. 8, pp. 2867–2877, 2005.
- [7] M. H. M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 439–441, 1983.
- [8] Y. Chen and A. J. H. Vinck, "Wiretap channel with side information," *IEEE Transactions on Information Theory*, vol. 54, no. 1, pp. 395–402, 2008.
- [9] C. Mitropant, A. J. Han Vinck, and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Transactions on Information Theory*, vol. 52, no. 5, pp. 2181–2190, 2006.
- [10] B. Dai and Y. Luo, "Some new results on the wiretap channel with side information," *Entropy*, vol. 14, no. 9, pp. 1671–1702, 2012.
- [11] W. Liu and B. Chen, "Wiretap channel with two-sided channel state information," in *Proceedings of the Conference Record of the 41st Asilomar Conference on Signals, Systems and Computers (ACSSC '07)*, pp. 893–897, Pacific Grove, Calif, USA, November 2007.
- [12] Y. Chia and A. El Gamal, "Wiretap channel with causal state information," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2838–2849, 2012.
- [13] B. Dai, A. J. H. Vinck, Y. Luo, and X. Tang, "Wiretap channel with action-dependent channel state information," *Entropy*, vol. 15, no. 2, pp. 445–473, 2013.
- [14] B. Dai, A. J. Han Vinck, and Y. Luo, "Wiretap channel in the presence of action-dependent states and noiseless feedback," *Journal of Applied Mathematics*, vol. 2013, Article ID 423619, 17 pages, 2013.
- [15] X. Yin and Z. Xue, "Wiretap channel with information embedding on actions," *Entropy*, vol. 16, no. 4, pp. 2105–2130, 2014.
- [16] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [17] I. Csisz and J. Köner, "Broadcast channels with confidential messages," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- [18] T. Weissman, "Capacity of channels with action-dependent states," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5396–5411, 2010.