A New Broadcast Wiretap Channel Model

Mohamed Nafea and Aylin Yener

Wireless Communications and Networking Laboratory (WCAN)
The School of Electrical Engineering and Computer Science
The Pennsylvania State University, University Park, PA 16802.
mnafea@psu.edu *yener@engr.psu.edu*

***Abstract*—A new broadcast wiretap channel (B-WTC) with a wiretapper who noiselessly taps into a fixed-length subset of the transmitted symbols of her choice, and observes the remainder through a noisy channel, is studied. An achievable strong secrecy rate region which extends Marton's inner bound to the proposed setting, is derived. Strong secrecy capacity regions for two classes of the new B-WTC, namely the new B-WTC with deterministic receivers, and the new B-WTC with degraded receivers and more noisy wiretapper, are identified. These results extend the recently proposed new wiretap channel model to the broadcast setting.**

I. Introduction

The wiretap channel II (WTC-II), introduced in [1], models a WTC with a noiseless main channel and a wiretapper who noiselessly taps into a fixed-length subset of her choice of the transmitted bits. Recently, reference [2] introduced a noisy main channel to the WTC-II model and derived inner and outer bounds for the secrecy capacity. Subsequently, reference [3] derived the secrecy capacity for this model. More recently, reference [4] introduced a new WTC and derived its strong secrecy capacity. In this model, the wiretapper, besides tapping into a subset of the transmitted symbols of her choice, observes the remainder through a noisy channel. The model subsumes both the classical WTC [5] and the WTC-II model [1] as special cases. The ability to choose a subset of the codeword as the wiretapper wishes makes this a more capable wiretapper as compared to the passive adversary in [5]. The noisy channel makes this a more realistic model compared to [1]. The new WTC was extended to the multiple access setting in [6].

In this paper, we extend this WTC model to the broadcast setting, proposing a new broadcast WTC (B-WTC). We derive an achievable strong secrecy rate region for the model which extends Marton's inner bound for the broadcast channel to the proposed setting. The derived rate region characterizes the secrecy penalty due to the additional capabilities at the wiretapper. Achievability is established using a similar approach as in [4], [6], [7] and requires extending the tools used in [6].

We characterize the strong secrecy capacity regions for two classes of the new B-WTC. We first consider the class with deterministic channels to the legitimate receivers. Second, we consider the class with degraded receivers and a certain range for the noiselessly tapped ratio by the wiretapper which results in the wiretapper being more noisy than both receivers. These results establish the optimality of the proposed achievability scheme for the two aforementioned classes of the new B-WTC.

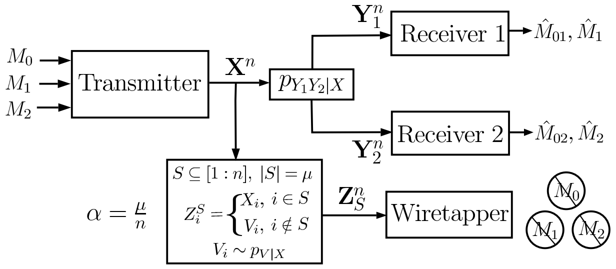

Fig. 1. The new two-user broadcast wiretap channel model.

Notation: For random variables (vectors) and their realizations, $A_{i:j} \triangleq \{A_i, \cdots, A_j\}$, $i < j$, and $A_S \triangleq \{A_i\}_{i \in S}$, $S \subseteq \mathbb{N}$. p_X^U denotes a uniform distribution over X. $\mathbb{1}_{\mathcal{A}}$ is the indicator function. $\mathbb{V}(p_X, q_X)$ and $\mathbb{D}(p_X||q_X)$ denote the total variation distance and K-L divergence between p_X, q_X.

II. Channel Model

Consider the model in Fig. 1. The main channel is a discrete memoryless channel (DMC) $\{\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2, p_{Y_1Y_2|X}\}$. The transmitter sends a common message M_0 to both receivers, a private message M_j to receiver j, $j = 1, 2$, while keeping $M_{0:2}$ secret from the wiretapper. $M_0, \{M_j\}_{j=1,2}$, are independent and uniform over $[1 : 2^{nR_0}], [1 : 2^{nR_j}]$. The transmitter maps $M_{0:2}$ to $\mathbf{X}^n \in \mathcal{X}^n$ using a stochastic encoder. Receiver j observes $\mathbf{Y}_j^n \in \mathcal{Y}_j^n$ and outputs the estimates $\hat{M}_{0,j}, \hat{M}_j$. The wiretapper chooses $S \in \mathcal{S}$, with $\mathcal{S} \triangleq \{S \subseteq [1 : n] : |S| = \mu, \alpha = \frac{\mu}{n}\}$, and observes $\mathbf{Z}_S^n = [Z_1^S, \cdots, Z_n^S] \in \mathcal{Z}^n$, where

$$Z_i^S = X_i, \text{ if } i \in S, \quad \text{and } Z_i^S = V_i, \text{ otherwise}, \qquad (1)$$

$\mathbf{V}^n \in \mathcal{V}^n$, $V_i \sim p_{V|X}$, $\mathcal{Z} \triangleq \mathcal{X} \cup \mathcal{V}$. An $(n, 2^{nR_0}, 2^{nR_1}, 2^{nR_2})$ code $\mathcal{C}_n$ consists of three message sets, a stochastic encoder $P_{\mathbf{X}^n|M_{0:2}\mathcal{C}_n}$, and two decoders. (R_0, R_1, R_2) is an achievable strong secrecy rate tuple if there is a sequence of codes s.t.

$$\lim_{n \to \infty} \mathbb{P}\Big(\bigcup_{j=1,2} (\hat{M}_{0,j}, \hat{M}_j) \neq (M_0, M_j) | \mathcal{C}_n \Big) = 0, \qquad (2)$$

$$\lim_{n \to \infty} \max_{S \in \mathcal{S}} I(M_0, M_1, M_2; \mathbf{Z}_S^n | \mathcal{C}_n) = 0. \qquad (3)$$

The strong secrecy capacity region is the closure of all achievable strong secrecy rate tuples (R_0, R_1, R_2).

III. Achievable Strong Secrecy Rate Region

Theorem 1 For $\alpha \in [0, 1]$, an achievable strong secrecy rate region for the new broadcast WTC in Fig. 1 is given by the convex hull of the rate tuples (R_0, R_1, R_2) which satisfy:

$$\begin{aligned} R_0 + R_j \leq \big[&I(U_0, U_j; Y_j) - I(U_0, U_j; V) \\ &- \alpha I(U_0, U_j; X|V)\big]^+, \qquad j = 1, 2, \end{aligned} \tag{4}$$

$$\begin{aligned} R_0 + R_1 + R_2 \leq \big[&\min\{I(U_0; Y_1), I(U_0; Y_2)\} \\ &+ I(U_1; Y_1|U_0) + I(U_2; Y_2|U_0) - I(U_1; U_2|U_0) \\ &- I(U_0, U_1, U_2; V) - \alpha I(U_0, U_1, U_2; X|V)\big]^+, \end{aligned} \tag{5}$$

$$\begin{aligned} 2R_0 + R_1 + R_2 \leq \big[&I(U_0, U_1; Y_1) + I(U_0, U_2; Y_2) \\ &- I(U_1; U_2|U_0) - I(U_0; V) - I(U_0, U_1, U_2; V) \\ &- \alpha[I(U_0; X|V) + I(U_0, U_1, U_2; X|V)]\big]^+, \end{aligned} \tag{6}$$

for some $p_{U_0U_1U_2XY_1Y_2V} = p_{U_0U_1U_2}\, p_{X|U_0U_1U_2}\, p_{Y_1Y_2V|X}$.

Remark 1 In Theorem 1, by setting $\alpha = 0$, we obtain the achievable rate region for the B-WTC in [7, Thm. 3]. That is, the terms in (4)-(6) multiplied by α determine the secrecy cost, with respect to the B-WTC, of the additional capability of the wiretapper to choose αn noiseless codeword symbols. In addition, setting $\alpha = 0$, $V =$ const., in (4)-(6) yields Marton's inner bound for the broadcast channel [8, Thm. 8.4].

Proof: (Theorem 1) We first assume the availability of common randomness at all terminals in the original model. We then introduce a dual multi-terminal secret key agreement problem in the source model which introduces a set of random variables similar to the variables introduced by the original channel model with the assumed randomness. Next, we derive rate conditions resulting in the induced distributions from the two models to be identical and hence, a solution, i.e., the encoder and decoders, for one model implies a solution for the other. We search for encoder and decoders that satisfy certain reliability and secrecy (independence) conditions for the dual source model and utilize the reverse encoder and decoders for the original channel model to achieve (2), (3). We finally remove the common randomness from the original model.

In the original model, along with stochastic encoding for secrecy, we utilize a combination of superposition and Marton coding [8, Chapter 8]. We hence define the correlated auxiliary variables U_0, U_1, U_2 according to $p_{U_{0:2}} p_{X|U_{0:2}}$. The message M_0 is represented by the codeword $\mathbf{U}_0$, while the message $M_j, j = 1, 2$, is superposed over M_0 through the codeword $\mathbf{U}_j$. Decoder j thus decodes M_0 from $\mathbf{U}_0$ and M_j from $\mathbf{U}_0\mathbf{U}_j$. In the dual model, we define the sources noisy observations according to the combined superposition and Marton coding.

Fix $p_{U_{0:2}X} = p_{U_{0:2}} p_{X|U_{0:2}}$, and let $p_{Y_{1:2}|U_{0:2}}$ be the distribution resulting from concatenating the DMCs $p_{X|U_{0:2}}, p_{Y_{1:2}|X}$, where $p_{Y_{1:2}|X}$ is the transition probability for the main channel in Fig. 1. We describe the following two protocols:

Protocol A: The protocol is described in Fig. 2. Let $\mathbf{U}_0^n$, $\mathbf{U}_1^n$,$\mathbf{U}_2^n$,$\mathbf{Y}_1^n$,$\mathbf{Y}_2^n$ be i.i.d. according to $p_{U_{0:2}} p_{Y_{1:2}|U_{0:2}}$. Source $\mathbf{U}_0$ is randomly and independently binned into the indices $M_0 = \mathcal{B}_{10}(\mathbf{U}_0)$, $C_0 = \mathcal{B}_{20}(\mathbf{U}_0)$, and source $\mathbf{U}_0\mathbf{U}_j, j = 1, 2$, is randomly and independently binned into $M_j = \mathcal{B}_{1j}(\mathbf{U}_0\mathbf{U}_j)$, $C_j = \mathcal{B}_{2j}(\mathbf{U}_0\mathbf{U}_j)$. $\mathcal{B}_{1t}, \mathcal{B}_{2t}$ are independent and uniform over $[1 : 2^{nR_t}], [1 : 2^{n\tilde{R}_t}]$, $t = 0, 1, 2$. Decoder j observes $C_0, C_j, \mathbf{Y}_j$ and outputs the estimates $\hat{\mathbf{U}}_{0,j}, \hat{\mathbf{U}}_j, \hat{M}_{0,j}, \hat{M}_j$. The wiretapper chooses $S \in \mathcal{S}$ and observes $\mathbf{Z}_S$ as in (1). The distribution of $\mathbf{Z}_S$ is only known to belong to the finite class $\{p_{\mathbf{Z}_S}\}_{S\in\mathcal{S}}$, with $|\mathcal{S}| < 2^{\alpha n}$. The induced joint distribution is

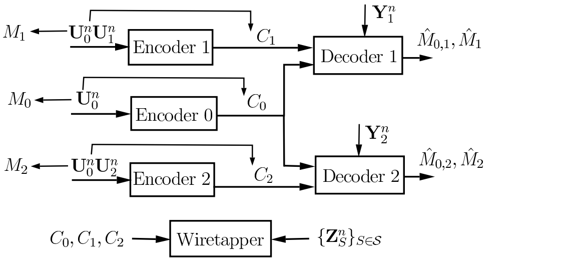
M_1
$\mathbf{U}_0^n\mathbf{U}_1^n$
Encoder 1
C_1
$\mathbf{Y}_1^n$
Decoder 1
$\hat{M}_{0,1}, \hat{M}_1$
M_0
$\mathbf{U}_0^n$
Encoder 0
C_0
M_2
$\mathbf{U}_0^n\mathbf{U}_2^n$
Encoder 2
C_2
$\mathbf{Y}_2^n$
Decoder 2
$\hat{M}_{0,2}, \hat{M}_2$
C_0, C_1, C_2
Wiretapper
$\{\mathbf{Z}_S^n\}_{S\in\mathcal{S}}$

Fig. 2. Multi-terminal secret key agreement problem in the source model.

$$\begin{aligned} &\tilde{P}_{M_{0:2}C_{0:2}\mathbf{U}_{0:2}\mathbf{Y}_{1:2}\mathbf{Z}_S\hat{\mathbf{U}}_{0,1}\hat{\mathbf{U}}_{0,2}\hat{\mathbf{U}}_{1:2}} = p_{\mathbf{U}_{0:2}\mathbf{Y}_{1:2}\mathbf{Z}_S} \tilde{P}_{\hat{\mathbf{U}}_{0,1}\hat{\mathbf{U}}_1|\mathbf{Y}_1C_{0:1}} \\ &\quad \times \tilde{P}_{\hat{\mathbf{U}}_{0,2}\hat{\mathbf{U}}_2|\mathbf{Y}_2C_0C_2} \mathbb{1}_{\{\mathcal{B}_{1j}(\mathbf{U}_0\mathbf{U}_j)=M_j, \mathcal{B}_{2j}(\mathbf{U}_0\mathbf{U}_j)=C_j, j=1,2\}} \\ &\quad \times \mathbb{1}_{\{\mathcal{B}_{10}(\mathbf{U}_0)=M_0, \mathcal{B}_{20}(\mathbf{U}_0)=C_0\}} = \tilde{P}_{M_{0:2}C_{0:2}} \tilde{P}_{\mathbf{U}_{0:2}|M_{0:2}C_{0:2}} \\ &\quad \times p_{\mathbf{Y}_{1:2}\mathbf{Z}_S|\mathbf{U}_{0:2}} \tilde{P}_{\hat{\mathbf{U}}_{0,1}\hat{\mathbf{U}}_1|\mathbf{Y}_1C_0C_1} \tilde{P}_{\hat{\mathbf{U}}_{0,2}\hat{\mathbf{U}}_2|\mathbf{Y}_2C_0C_2}. \end{aligned} \tag{7}$$

Protocol B: This protocol is the original model in Fig. 1 with added common randomness $\{C_t\}_{t=0,1,2}$ available to all terminals and uniform over $[1 : 2^{n\tilde{R}_t}]$. We utilize here the encoder and decoders in (7). The induced distribution is

$$\begin{aligned} P_{M_{0:2}C_{0:2}\mathbf{U}_{0:2}\mathbf{Y}_{1:2}\mathbf{Z}_S\hat{\mathbf{U}}_{0,1}\hat{\mathbf{U}}_{0,2}\hat{\mathbf{U}}_{1:2}} &= p^U_{M_{0:2}} p^U_{C_{0:2}} \tilde{P}_{\mathbf{U}_{0:2}|M_{0:2}C_{0:2}} \\ \times\, p_{\mathbf{Y}_{1:2}\mathbf{Z}_S|\mathbf{U}_{0:2}} \tilde{P}_{\hat{\mathbf{U}}_{0,1}\hat{\mathbf{U}}_1|\mathbf{Y}_1C_0C_1} &\tilde{P}_{\hat{\mathbf{U}}_{0,2}\hat{\mathbf{U}}_2|\mathbf{Y}_2C_0C_2}. \end{aligned} \tag{8}$$

Although C_i is available at receiver j, $i \neq j$, it is not used to decode M_0, M_j. At this stage, we ignore the $\hat{M}$ variables, as we introduce them later as deterministic functions of the $\hat{\mathbf{U}}$ variables. We next state the following two lemmas which extend Lemmas 1, 2 in [6] to *multiple correlated* sources.

Lemma 1 is a *one-shot* result which provides conditions for which random binning of *multiple correlated* sources results in a distribution for the bins that is close to independent uniform distributions. The convergence rate provided by Lemma 1, which is exponential, is used in converting a secrecy (independence) condition from the dual to the original model [4].

Lemma 1 Let $X_{1:T}$ be T *correlated* sources according to $p_{X_{1:T}}$. Each source $X_t \in \mathcal{X}_t$, $t \in [1 : T]$, is randomly binned into the indices $M_t = \mathcal{B}_{1t}(X_t), C_t = \mathcal{B}_{2t}(X_t)$, where $\mathcal{B}_{1t}, \mathcal{B}_{2t}$ are independent and uniformly distributed over $[1 : \tilde{M}_t], [1 : \tilde{C}_t]$. Let $\mathcal{B} \triangleq \{\mathcal{B}_{1t}(x_t), \mathcal{B}_{2t}(x_t) : t \in [1 : T], x_t \in \mathcal{X}_t\}$. Let $\mathcal{J} \triangleq \{J : J \subseteq [1 : T], J \neq \emptyset\}$. For $J \in \mathcal{J}$, $\gamma^{(J)} > 0$, define[1]

$$\begin{aligned} &\mathcal{D} \triangleq \{x_{1:T} \in \mathcal{X}_{1:T} : x_J \in \mathcal{D}_{\gamma^{(J)}}, \forall J \in \mathcal{J}\}, \quad \text{where,} \\ &\mathcal{D}_{\gamma^{(J)}} \triangleq \{x_J \in \mathcal{X}_J : -\log p_{X_J}(x_J) > \gamma^{(J)}\}, \end{aligned} \tag{9}$$

$\tilde{M}_J = \prod_{t\in J} \tilde{M}_t$, and $\tilde{C}_J = \prod_{t\in J} \tilde{C}_t$. Then, we have

$$\begin{aligned} &\mathbb{E}_{\mathcal{B}}\left(\mathbb{V}\left(P_{M_{1:T}C_{1:T}}, p^U_{M_{1:T}} p^U_{C_{1:T}}\right)\right) \\ &\qquad \leq \mathbb{P}_{p_{X_{1:T}}}\left(X_{1:T} \notin \mathcal{D}\right) + \frac{1}{2}\sum_{J\in\mathcal{J}} \sqrt{\tilde{M}_J \tilde{C}_J 2^{-\gamma^{(J)}}}, \end{aligned} \tag{10}$$

where P is the induced distribution over $M_{1:T}$ and $C_{1:T}$.

[1] For $J \in \mathcal{J}$, we use $\mathcal{X}_J$ to denote the Cartesian product $\prod_{t\in J} \mathcal{X}_t$.

Proof: See Appendix A. ■

Lemma 2 below is again a one-shot result which is used to establish the secrecy condition for protocol A. In particular, it provides a *doubly-exponential* convergence rate for the probability that $M_{0:2}, C_{0:2}$, are independent, uniform, and both are independent from $\mathbf{Z}_S$. This doubly-exponential rate is needed to ensure secrecy for the exponentially many choices of S. In the secrecy condition for the source model, we require $C_{0:2}$ to be independent from $\{M_{0:2}, \mathbf{Z}_S\}$ since, in the last step of the proof, after showing that this secrecy condition holds as well for protocol B, we need to eliminate $C_{0:2}$ by conditioning on a certain instance of it without disturbing the uniformity of the messages $M_{0:2}$ and their independence from $\mathbf{Z}_S$.

Lemma 2 Let $X_{1:T}$ be T correlated sources, which are correlated with the source $\{Z_S\} \triangleq \{\mathcal{Z}, p_{Z_S}\}, S \in \mathcal{S}$, according to $p_{X_{1:T}Z_S}$. All the alphabets of $\{\mathcal{X}_t\}_{t=1}^T, \mathcal{Z}, \mathcal{S}$, are finite. Each source X_t is randomly binned into the indices M_t, C_t as in Lemma 1. Let $\mathcal{P}$ be the set of all possible permutations of $[1:T]$. For all $\mathbf{p} \in \mathcal{P}$, $t \in [1:T]$, let $\gamma_t^{\mathbf{p}} > 0$, and define

$$\mathcal{D}_{\mathbf{p}}^S \triangleq \big\{(x_{1:T}, z) \in \mathcal{X}_{1:T} \times \mathcal{Z} : (x_{p_{1:t}}, z) \in \mathcal{D}_{\gamma_t^{\mathbf{p}}}^S, \forall t \in [1:T]\big\}$$

where $\mathbf{p} \triangleq [p_1 \cdots p_T]$, $x_{p_{1:t}} \triangleq \{x_{p_1}, \cdots, x_{p_t}\}$, $x_{p_{1:0}} = \emptyset$, and

$$\mathcal{D}_{\gamma_t^{\mathbf{p}}}^S \triangleq \big\{(x_{p_{1:t}}, z) : \log 1/p_{X_{p_t}|X_{p_{1:t-1}}Z_S}(x_{p_t}|x_{p_{1:t-1}},z) > \gamma_t^{\mathbf{p}}\big\}.$$

If there exists $\delta \in (0, \frac{1}{2})$ s.t. for all $S \in \mathcal{S}$ and $\mathbf{p} \in \mathcal{P}$, $\mathbb{P}_{p_{X_{1:T}Z_S}}\big((X_{1:T}, Z_S) \in \mathcal{D}_{\mathbf{p}}^S\big) \geq 1 - \delta^2$, then, $\forall \epsilon \in [0,1]$,

$$\mathbb{P}_{\mathcal{B}}\big(\max_{S \in \mathcal{S}} \mathbb{D}(P_{M_{1:T}C_{1:T}Z_S}||p_{M_{1:T}}^U p_{C_{1:T}}^U p_{Z_S}) \geq T\tilde{\epsilon}\big)$$
$$\leq |\mathcal{S}||\mathcal{Z}| \min_{\mathbf{p} \in \mathcal{P}} \sum_{t=1}^T \exp\Big(\frac{-\epsilon^2(1-\delta)2^{\gamma_t^{\mathbf{p}}}}{3\tilde{M}_{p_t}\tilde{C}_{p_t}}\Big), \quad (11)$$

where $\tilde{\epsilon} = \max_t\{\epsilon + (\delta+\delta^2)\log(\tilde{M}_t\tilde{C}_t) + H_b(\delta^2)\}$, H_b is the binary entropy function, and P is the induced distribution.

Proof: See Appendix B. ■

We now apply Lemma 1 to the source model in Fig.2. Set $X_1 = \mathbf{U}_0$, $X_2 = \mathbf{U}_0\mathbf{U}_1$, $X_3 = \mathbf{U}_0\mathbf{U}_2$, $\tilde{M}_t = 2^{nR_t}$, $\tilde{C}_t = 2^{n\tilde{R}_t}$, $t = 0, 1, 2$, where $\mathbf{U}_{0:2}, M_{0:2}, C_{0:2}$ are as in protocol A. For $\epsilon' > 0, J \subseteq [1:3], J \neq \emptyset$, let $\gamma^{(J)} = (1-\epsilon')H(X_J)$. For $J = \{1\}$, using Hoeffding inequality [4, Lemma 5], we have

$$\mathbb{P}(X_1 \notin \mathcal{D}_{\gamma^{(\{1\})}}) = \mathbb{P}_{p_{\mathbf{U}_0}}\big(-\log p(\mathbf{U}_0) \leq \gamma^{(\{1\})}\big) =$$
$$\mathbb{P}\Big(\sum_{k=1}^n(-\log p(U_{0,k})) \leq n(1-\epsilon')H(U_0)\Big) \leq e^{-\beta^{(\{1\})}n},$$

where $\beta^{(\{1\})} > 0$. Similarly, for $J \subseteq [1:3], J \neq \emptyset$, $\exists \beta^{(J)} > 0$ s.t. $\mathbb{P}(X_J \notin \mathcal{D}_{\gamma^{(J)}}) \leq \exp(-\beta^{(J)}n)$. Using (9), $\exists \bar{\beta} > 0$ s.t.

$$\mathbb{P}(X_{1:3} \notin \mathcal{D}) \leq \sum_{J \subseteq [1:3], J \neq \emptyset} \mathbb{P}(X_J \notin \mathcal{D}_{\gamma^{(J)}}) \leq e^{-\bar{\beta}n}. \quad (12)$$

Substituting the choices for $\tilde{M}_t, \tilde{C}_t, \gamma^{(J)}$ and (12), in (10), if

$$R_0 + \tilde{R}_0 < (1-\epsilon')H(U_0)$$
$$R_0 + \tilde{R}_0 + R_j + \tilde{R}_j < (1-\epsilon')H(U_0U_j),\ j = 1, 2,$$
$$R_0 + \tilde{R}_0 + R_1 + \tilde{R}_1 + R_2 + \tilde{R}_2 < (1-\epsilon')H(U_{0:2}), \quad (13)$$

then, there exists $\beta > 0$ such that, for any $S \in \mathcal{S}$,

$$\mathbb{E}_{\mathcal{B}}\mathbb{V}\big(\tilde{P}_{M_{0:2}C_{0:2}}, p_{M_{0:2}}^U p_{C_{0:2}}^U\big) \leq \exp(-\beta n). \quad (14)$$

Now, for reliability of protocol A, we use Slepian-Wolf decoders at both users. Using [7, Lemma 1], for any $S \in \mathcal{S}$,

$$\lim_{n\to\infty} \mathbb{E}_{\mathcal{B}}\mathbb{V}\big(\tilde{P}_{M_{0:2}C_{0:2}\mathbf{U}_{0:2}\mathbf{Y}_{1:2}\mathbf{Z}_S}\mathbb{1}_{\{\hat{\mathbf{U}}_{0,1}=\hat{\mathbf{U}}_{0,2}=\mathbf{U}_0, \hat{\mathbf{U}}_j=\mathbf{U}_j, j=1,2\}}$$
$$, \tilde{P}_{M_{0:2}C_{0:2}\mathbf{U}_{0:2}\mathbf{Y}_{1:2}\mathbf{Z}_S\hat{\mathbf{U}}_{0,1}\hat{\mathbf{U}}_{0,2}\hat{\mathbf{U}}_{1:2}}\big) = 0, \quad \text{if for } j = 1, 2,$$
$$\tilde{R}_0 + \tilde{R}_j > H(U_0U_j|Y_j) \text{ and } \tilde{R}_j > H(U_j|U_0Y_j). \quad (15)$$

Next, in Lemma 2, set $X_1 = \mathbf{U}_0, X_2 = \mathbf{U}_0\mathbf{U}_1, X_3 = \mathbf{U}_0\mathbf{U}_2, \tilde{M}_t = 2^{nR_t}, \tilde{C}_t = 2^{n\tilde{R}_t}, t = 0, 1, 2,$ $Z_S = \mathbf{Z}_S, \forall S \in \mathcal{S}$; $\mathbf{U}_{0:2}, \mathbf{Z}_S, \mathcal{S}$ as in protocol A. Let us first consider $\mathbf{p} = \bar{\mathbf{p}} = [1:3]$. Since $p_{V|U_{0:2}}$ is a DMC, that results from concatenating the DMCs $p_{V|X}$, $p_{X|U_{0:2}}$, and $\mathbf{U}_{0:2}$ are i.i.d., then $\forall S \in \mathcal{S}$,

$$H(X_1|Z_S) = H(\mathbf{U}_0|\mathbf{X}_S\mathbf{V}_{S^c}) = H(\mathbf{U}_{0,S}|\mathbf{X}_S)$$
$$+ H(\mathbf{U}_{0,S^c}|\mathbf{V}_{S^c}) = \mu H(U_0|X) + (n-\mu)H(U_0|V)$$
$$H(X_2|X_1Z_S) = H(\mathbf{U}_0\mathbf{U}_1|\mathbf{U}_0\mathbf{X}_S\mathbf{V}_{S^c})$$
$$= \mu H(U_1|U_0X) + (n-\mu)H(U_1|U_0V)$$
$$H(X_3|X_{1:2}Z_S) = \mu H(U_2|U_{0:1}X) + (n-\mu)H(U_2|U_{0:1}V).$$

By Hoeffding inequality and the definition of $\mathcal{D}_{\bar{\mathbf{p}}}^S$, with $\bar{\epsilon} > 0$,

$$\gamma_1^{\bar{\mathbf{p}}} = (1-\bar{\epsilon})[\mu H(U_0|X) + (n-\mu)H(U_0|V)]$$
$$\gamma_2^{\bar{\mathbf{p}}} = (1-\bar{\epsilon})[\mu H(U_1|U_0X) + (n-\mu)H(U_1|U_0V)]$$
$$\gamma_3^{\bar{\mathbf{p}}} = (1-\bar{\epsilon})[\mu H(U_2|U_0U_1X) + (n-\mu)H(U_2|U_0U_1V)],$$

$\exists \beta_{\bar{\mathbf{p}}} > 0$ s.t. $\mathbb{P}((X_{1:3}, Z_S) \notin \mathcal{D}_{\bar{\mathbf{p}}}^S) \leq \exp(-\beta_{\bar{\mathbf{p}}}n)$.

Similarly, for any $\mathbf{p}$ which is a permutation of $[1:3]$, letting $\gamma_t^{\mathbf{p}} = (1-\bar{\epsilon}) \min_{S \in \mathcal{S}} H(X_{p_t}|X_{p_{1:t-1}}Z_S)$, with $X_{p_{1:0}} = \emptyset$, $\exists \beta_{\mathbf{p}} > 0$ s.t. $\mathbb{P}((X_{1:3}, Z_S) \notin \mathcal{D}_{\mathbf{p}}^S) \leq \exp(-\beta_{\mathbf{p}}n)$. Taking $\delta^2 = e^{-\tilde{\beta}n}$, $\tilde{\beta} = \min_{\mathbf{p}} \beta_{\mathbf{p}}$, we have $\mathbb{P}\big((X_{1:3}, Z_S) \notin \mathcal{D}_{\mathbf{p}}^S\big) \leq \delta^2$ for all $\mathbf{p}$. Note that $\lim_{n\to\infty} \delta^2 = 0$, and hence, for n large enough, $\delta^2 \in (0, \frac{1}{4})$. Thus, the conditions of Lemma 2 are satisfied.

Substituting the choices for $\tilde{M}_t, \tilde{C}_t, \gamma_t^{\mathbf{p}}$, for $t = 1, 2, 3$, and all $\mathbf{p}$, and $|\mathcal{S}||\mathcal{Z}^n| \leq e^{n\left[\ln 2 + \ln(|\mathcal{X}|+|\mathcal{V}|)\right]}$ in (11), we have, $\forall \epsilon, \epsilon_1 > 0$, $\tilde{\epsilon} = \epsilon + \epsilon_1$, $\exists n^* \in \mathbb{N}, \kappa_\epsilon, \tilde{\kappa} > 0$ s.t. $\forall n \geq n^*$,

$$\mathbb{P}(\max_{S \in \mathcal{S}} \mathbb{D}(\tilde{P}_{M_{0:2}C_{0:2}\mathbf{Z}_S}||p_{M_{0:2}}^U p_{C_{0:2}}^U p_{\mathbf{Z}_S}) \geq 3\tilde{\epsilon}) \leq e^{-\kappa_\epsilon e^{\tilde{\kappa}n}},$$
$$\text{if } R_0 + \tilde{R}_0 < (1-\bar{\epsilon})\left[\alpha H(U_0|X) + (1-\alpha)H(U_0|V)\right]$$
$$R_0 + \tilde{R}_0 + R_j + \tilde{R}_j < (1-\bar{\epsilon})\big[\alpha H(U_0U_j|X)$$
$$+ (1-\alpha)H(U_0U_j|V)\big],\ j = 1, 2,$$
$$R_0 + \tilde{R}_0 + R_1 + \tilde{R}_1 + R_2 + \tilde{R}_2 < (1-\bar{\epsilon})\times$$
$$\left[\alpha H(U_0U_1U_2|X) + (1-\alpha)H(U_0U_1U_2|V)\right]. \quad (16)$$

Note that for each $\mathbf{p} \in \mathcal{P}$, Lemma 2 results in the maximum binning rate $R_{p_1} + \tilde{R}_{p_1}$ for the source X_{p_1}, and then the maximum conditional binning rate for the source X_{p_2} given $R_{p_1} + \tilde{R}_{p_1}$, and so on and so forth, so that the probability in the left hand side of (11) is vanishing. That is, for each $\mathbf{p}$, Lemma 2 results in one corner point in the binning rate region for the sources $X_{1:T}$ such that $M_{1:T}, C_{1:T}$ are independent, uniform, and all are independent from the wiretapper's observation.

By the Borel-Cantelli lemma, it follows from (14), (16) that

$$\lim_{n\to\infty} \mathbb{P}(\mathbb{V}(\tilde{P}_{M_{0:2}C_{0:2}}, p^U_{M_{0:2}} p^U_{C_{0:2}}) > 0) = 0, \tag{17}$$

$$\lim_{n\to\infty} \mathbb{P}(\max_{S\in\mathcal{S}} \mathbb{D}(\tilde{P}_{M_{0:2}C_{0:2}\mathbf{Z}_S} || p^U_{M_{0:2}} p^U_{C_{0:2}} p_{\mathbf{Z}_S}) > 0) = 0. \tag{18}$$

Using similar steps as in [4], we first use (14), (17) to show that (15), (18) hold as well for protocol B. That is,

$$\lim_{n\to\infty} \mathbb{P}_{\mathcal{B}}(\max_{S\in\mathcal{S}} \mathbb{D}(P_{M_{0:2}C_{0:2}\mathbf{Z}_S} || p^U_{M_{0:2}} p^U_{C_{0:2}} p_{\mathbf{Z}_S}) > 0) = 0,$$

$$\lim_{n\to\infty} \mathbb{E}_{\mathcal{B}} \mathbb{V}\big(P_{M_{0:2}C_{0:2}\mathbf{U}_{0:2}\mathbf{Y}_{1:2}\mathbf{Z}_S} \mathbb{1}_{\{\hat{\mathbf{U}}_{0,1}=\hat{\mathbf{U}}_{0,2}=\mathbf{U}_0, \hat{\mathbf{U}}_j=\mathbf{U}_j, j=1,2\}}, P_{M_{0:2}C_{0:2}\mathbf{U}_{0:2}\mathbf{Y}_{1:2}\mathbf{Z}_S\hat{\mathbf{U}}_{0,1}\hat{\mathbf{U}}_{0,2}\hat{\mathbf{U}}_{1:2}}\big) = 0. \tag{19}$$

Next, we apply the selection lemma [4, Lemma 3] to (19) to show the existence of a binning realization $\mathbf{b}^*$, with a corresponding joint distribution p^* for protocol B, such that

$$\lim_{n\to\infty} \mathbb{V}(p^*_{M_{0:2}C_{0:2}\mathbf{U}_{0:2}\mathbf{Y}_{1:2}\mathbf{Z}_S} \mathbb{1}_{\{\hat{\mathbf{U}}_{0,1}=\hat{\mathbf{U}}_{0,2}=\mathbf{U}_0, \hat{\mathbf{U}}_j=\mathbf{U}_j, j=1,2\}}, p^*_{M_{0:2}C_{0:2}\mathbf{U}_{0:2}\mathbf{Y}_{1:2}\mathbf{Z}_S\hat{\mathbf{U}}_{0,1}\hat{\mathbf{U}}_{0,2}\hat{\mathbf{U}}_{1:2}}) = 0, \text{ and} \tag{20}$$

$$\lim_{n\to\infty} \mathbb{1}_{\{\max_{S\in\mathcal{S}} \mathbb{D}(p^*_{M_{0:2}C_{0:2}\mathbf{Z}_S} || p^U_{M_{0:2}} p^U_{C_{0:2}} p_{\mathbf{Z}_S}) > 0\}} = 0, \tag{21}$$

$M_0 = b^*_{10}(\mathbf{U}_0)$, $C_0 = b^*_{20}(\mathbf{U}_0)$, $M_j = b^*_{1j}(\mathbf{U}_0\mathbf{U}_j)$, and $C_j = b^*_{2j}(\mathbf{U}_0\mathbf{U}_j)$, $j = 1, 2$. We finally introduce the $\hat{M}$ variables to (20), and use the union bound with (21), to show that

$$\lim_{n\to\infty} \mathbb{E}_{C_{0:2}}\big(\mathbb{P}_{p^*}\big(\bigcup_{j=1,2} (\hat{M}_{0,j}, \hat{M}_j) \neq (M_0, M_j) | C_{0:2}\big)\big) = 0$$

$$\lim_{n\to\infty} \mathbb{P}_{C_{0:2}}\big(\max_{S\in\mathcal{S}} \mathbb{D}(p^*_{M_{0:2}\mathbf{Z}_S|C_{0:2}} || p^U_{M_{0:2}} p^*_{\mathbf{Z}_S|C_{0:2}}) > 0\big) = 0,$$

which are used to show the existence of $c^*_{0:2}$ such that both the reliability and secrecy constraints in (2), (3) hold.

Let $\tilde{p}^*$ be the distribution in protocol A that corresponds to the binning realization $\mathbf{b}^*$. We identify $\tilde{p}^*(\mathbf{u}_{0:2}|m_{0:2}, c^*{}_{0:2})$ and $(\tilde{p}^*(\hat{\mathbf{u}}_{0,j}, \hat{\mathbf{u}}_j|\mathbf{y}_j, c^*_0, c^*_j), b^*_{10}(\hat{\mathbf{u}}_{0,j}), b^*_{1j}(\hat{\mathbf{u}}_{0,j}, \hat{\mathbf{u}}_j), j = 1, 2)$ as the encoder and decoders for the original model. Finally, applying Fourier-Motzkin elimination to the rate conditions in (13), (15), (16) results in the rate region in (4)-(6). The convex hull follows by time sharing independent codes. ■

IV. Secrecy Capacity Regions

We characterize the strong secrecy capacity regions for two classes of the new B-WTC. We consider the case of no common message ($M_0 = 0$). To establish the capacity results, we (i) use similar steps as in [4, Sec. V] to show that the secrecy capacity of the new B-WTC is upper bounded by the secrecy capacity when the wiretapper observes the outputs of two DMCs, where the first DMC is an erasure channel with erasure probability $(1-\alpha)$ and the second is $p_{V|X}$, (ii) use the upper bound for the discrete memoryless (DM) B-WTC in [9], and finally (iii) evaluate the achievable rate region in (4)-(6). We omit the details of the proofs due to space limitations.

A. New B-WTC with Deterministic Receivers

We consider the class of the new B-WTC in Fig. 1 with both Y_1 and Y_2 are deterministic functions of the input X.

Theorem 2 For $\alpha \in [0, 1]$, the strong secrecy capacity of the new B-WTC with deterministic receivers is the set of all rate pairs (R_1, R_2) satisfying

$$\begin{aligned} R_j &\leq (1-\alpha)H(Y_j|V), \quad j = 1, 2, \\ R_1 + R_2 &\leq (1-\alpha)H(Y_1, Y_2|V). \end{aligned} \tag{22}$$

For achievability, we set $U_0 =$ const., $U_j = Y_j$, in (4)-(6).

B. New B-WTC with Degraded Receivers

We next consider the class of the new B-WTC with Y_2 is a degraded version of Y_1, i.e., $X - Y_1 - Y_2$ forms a Markov chain, and the wiretapper in the DM B-WTC whose secrecy capacity upper bounds that of the new B-WTC, is more noisy than both receivers; $\forall U$ s.t. $U - X - Y_2V$ is a Markov chain,

$$\alpha I(U; X|V) \leq I(U; Y_2) - I(U; V). \tag{23}$$

Theorem 3 For $\alpha \in [0, 1]$ such that (23) holds, the strong secrecy capacity of the new B-WTC with degraded receivers is the set of all rate pairs (R_1, R_2) satisfying

$$\begin{aligned} R_1 &\leq I(X; Y_1|U, Q) - I(X; V|U, Q) - \alpha H(X|V, U, Q), \\ R_2 &\leq I(U; Y_2|Q) - I(U; V|Q) - \alpha I(U; X|V, Q), \end{aligned} \tag{24}$$

so that $Q - U - X - Y_1Y_2V$ forms a Markov chain.

Note that Q represents a time sharing random variable. For achievability, we set $U_0 = U_2 = U$ and $U_1 = X$ in (4)-(6).

V. Conclusion

In this paper, we have extended the recently proposed new WTC model in [4] to the broadcast setting. In particular, we have considered a broadcast WTC with a wiretapper who noiselessly taps into a subset of her choice of the transmitted symbols and observes the remaining symbols through a noisy channel. We have derived an achievable strong secrecy rate region for the model, which extends Marton's inner bound and characterizes the secrecy penalty due to the noiseless observations at the wiretapper. We also have characterized the secrecy capacity for two classes of the new broadcast WTC.

Appendix A
Proof of Lemma 1

Recall that $\mathcal{J} = \{J : J \subseteq [1 : T], J \neq \emptyset\}$. For all $J \in \mathcal{J}$, let $\mathbb{1}_{\{x,m,c,J\}} = \mathbb{1}_{\{\mathcal{B}_{1t}(x_t)=m_t, \mathcal{B}_{2t}(x_t)=c_t, \forall t\in J\}}$. We have,

$$P(m_{1:T}, c_{1:T}) = \sum_{x_{1:T}\in\mathcal{X}_{1:T}} p(x_{1:T})\mathbb{1}_{\{x,m,c,[1:T]\}}. \tag{25}$$

Also, for $J \in \mathcal{J}$, $\mathbb{E}_{\mathcal{B}}\mathbb{1}_{\{x,m,c,J\}} = \prod_{t\in J} \frac{1}{\tilde{M}_t\tilde{C}_t} = (\tilde{M}_J\tilde{C}_J)^{-1}$. Let $P(m_{1:T}, c_{1:T}) = P_1(m_{1:T}, c_{1:T}) + P_2(m_{1:T}, c_{1:T})$, where

$$P_1(m_{1:T}, c_{1:T}) = \sum_{x_{1:T}} p(x_{1:T})\mathbb{1}_{\{x,m,c,[1:T]\}}\mathbb{1}_{\{x_{1:T}\notin\mathcal{D}\}} \tag{26}$$

$$P_2(m_{1:T}, c_{1:T}) = \sum_{x_{1:T}} p(x_{1:T})\mathbb{1}_{\{x,m,c,[1:T]\}}\mathbb{1}_{\{x_{1:T}\in\mathcal{D}\}}. \tag{27}$$

Using similar steps as in [4, (120)-(125)], we have

$$2\mathbb{E}_{\mathcal{B}}\mathbb{V}\left(P_{M_{1:T}C_{1:T}}, p^U_{M_{1:T}} p^U_{C_{1:T}}\right) \leq 2\mathbb{P}(X_{1:T} \notin \mathcal{D}) + \sum_{m_{1:T}, c_{1:T}} \mathbb{E}_{\mathcal{B}}\left|P_2(m_{1:T}, c_{1:T}) - \mathbb{E}_{\mathcal{B}}P_2(m_{1:T}, c_{1:T})\right|. \tag{28}$$

We partition $\mathcal{X}_{1:T}$ as follows. At the first iteration, $s=1, \forall J \in \mathcal{J}$, pick the largest possible set $\mathcal{N}_{J,1}$ of sequences $x_{1:T}$ that have different coordinates in each position of J, and at least one other position, i.e., $\mathcal{N}_{J,1}$ is on the form $\{x_{1:T} : \bar{x}_{1:T} \in \mathcal{N}_{J,1} \Rightarrow x_{J^c} \neq \bar{x}_{J^c},\ \forall t \in J, x_t \neq \bar{x}_t\}$. Note that, for $J \in \mathcal{J}$, the largest set $\mathcal{N}_{J,1}$ is not unique. Choose $\{\mathcal{N}_{J,1}\}_{J\in\mathcal{J}}$ such that they do not overlap. We repeat the process, such that $\mathcal{N}_{J,s} \cap \mathcal{N}_{J',s'} = \emptyset$ for $s \neq s'$ or $J \neq J'$, and for $x_{1:T} \in \mathcal{N}_{J,s}, x'_{1:T} \in \mathcal{N}_{J,s'}, x_{J^c} \neq x'_{J^c}$, until we run out of sequences in $\mathcal{X}_{1:T}$. Let N be the number of iterations. Thus $\mathcal{X}_{1:T} = \cup_{s=1}^{N} \cup_{J\in\mathcal{J}} \mathcal{N}_{J,s}$. Thus, $P_2(m_{1:T}, c_{1:T}) = \sum_{s=1}^{N} \sum_{J\in\mathcal{J}} \bar{P}^{J,s}_{2,m_{1:T},c_{1:T}}$, where

$$\bar{P}^{J,s}_{2,m_{1:T},c_{1:T}} = \sum_{x_{1:T}\in\mathcal{N}_{J,s}} p(x_{1:T}) \mathbb{1}_{\{x,m,c,[1:T]\}} \mathbb{1}_{\{x_{1:T}\in\mathcal{D}\}}.$$

Thus, using the triangle inequality, we have

$$\sum_{m_{1:T},c_{1:T}} \mathbb{E}_{\mathcal{B}} \left| P_2(m_{1:T},c_{1:T}) - \mathbb{E}_{\mathcal{B}} P_2(m_{1:T},c_{1:T}) \right| \leq \sum_{s,J} \sum_{m_{1:T},c_{1:T}} \mathbb{E}_{\mathcal{B}} \Big| \bar{P}^{J,s}_{2,m_{1:T},c_{1:T}} - \mathbb{E}_{\mathcal{B}} \bar{P}^{J,s}_{2,m_{1:T},c_{1:T}} \Big|. \quad (29)$$

Note that $\sum_{m_{J^c},c_{J^c}} \mathbb{1}_{\{x,m,c,[1:T]\}} = \mathbb{1}_{\{x,m,c,J\}}$. Define

$$P^{J,s}_{2,m_J,c_J} \triangleq \sum_{x_{1:T}\in\mathcal{N}_{J,s}} p(x_{1:T}) \mathbb{1}_{\{x,m,c,J\}} \mathbb{1}_{\{x_{1:T}\in\mathcal{D}\}}, \quad (30)$$

and hence, $\sum_{m_{J^c},c_{J^c}} \bar{P}^{J,s}_{2,m_{1:T},c_{1:T}} = P^{J,s}_{2,m_J,c_J}$. We also have

$$\mathbb{E}_{\mathcal{B}} \bar{P}^{J,s}_{2,m_{1:T},c_{1:T}} = (\tilde{M}_{J^c}\tilde{C}_{J^c})^{-1}\, \mathbb{E}_{\mathcal{B}_J} P^{J,s}_{2,m_J,c_J}, \quad (31)$$

$$\mathbb{P}_{\mathcal{B}}\Big(\bar{P}^{J,s}_{2,m_{1:T},c_{1:T}} > (\tilde{M}_{J^c}\tilde{C}_{J^c})^{-1}\ P^{J,s}_{2,m_J,c_J} \Big) \leq \mathbb{P}_{\mathcal{B}}\Big(\sum_{m_{J^c},c_{J^c}} \bar{P}^{J,s}_{2,m_{1:T},c_{1:T}} > P^{J,s}_{2,m_J,c_J} \Big) = 0, \quad (32)$$

where $\mathcal{B}_J \triangleq \{\mathcal{B}_{1t}(x_t), \mathcal{B}_{2t}(x_t), \forall x_t \in \mathcal{X}_t, t \in J\}$. From (32), $\mathbb{P}_{\mathcal{B}}\big(\bar{P}^{J,s}_{2,m_{1:T},c_{1:T}} \leq (\tilde{M}_{J^c}\tilde{C}_{J^c})^{-1} P^{J,s}_{2,m_J,c_J} \big) = 1$. Using the law of total expectation and (31), (29) is further upper bounded by

$$\sum_{s,J} \sum_{m_J,c_J} \mathbb{E}_{\mathcal{B}_J} \Big(\big(P^{J,s}_{2,m_J,c_J} - \mathbb{E}_{\mathcal{B}_J} P^{J,s}_{2,m_J,c_J} \big)^2 \Big)^{1/2} \leq \sum_{s,J} \sum_{m_J,c_J} \big(\mathbb{V}\mathrm{ar}_{\mathcal{B}_J} P^{J,s}_{2,m_J,c_J} \big)^{1/2}, \quad (33)$$

where (33) follows from Jensen's inequality and the concavity of square root. For any s, J, $\mathbb{V}\mathrm{ar}_{\mathcal{B}_J}(P^{J,s}_{2,m_J,c_J})$ is given by

$$\begin{aligned}
&\mathbb{V}\mathrm{ar}_{\mathcal{B}_J} \sum_{x_{1:T}\in\mathcal{N}_{J,s}} p(x_{1:T}) \mathbb{1}_{\{x,m,c,J\}} \mathbb{1}_{\{x_{1:T}\in\mathcal{D}\}} \\
&= \sum_{x_{1:T}\in\mathcal{N}_{J,s}} \mathbb{V}\mathrm{ar}_{\mathcal{B}_J} \left(p(x_{1:T}) \mathbb{1}_{\{x,m,c,J\}} \mathbb{1}_{\{x_{1:T}\in\mathcal{D}\}} \right) && (34) \\
&\leq \sum_{x_{1:T}\in\mathcal{N}_{J,s}} p^2(x_{1:T}) \mathbb{1}_{\{x_{1:T}\in\mathcal{D}\}} \mathbb{E}_{\mathcal{B}_J} \mathbb{1}_{\{x,m,c,J\}} \\
&\leq \frac{1}{\tilde{M}_J\tilde{C}_J} \sum_{x_J\in\mathcal{N}_{J,s}} p^2(x_J) \mathbb{1}_{\{x_J\in\mathcal{D}_{\gamma^{(J)}}\}} \sum_{x_{J^c}\in\mathcal{N}_{J,s}} p^2(x_{J^c}|x_J) \\
&\leq 2^{-\gamma^{(J)}} (\tilde{M}_J\tilde{C}_J)^{-1} \sum_{x_{J^c}\in\mathcal{N}_{J,s}} p^2(x_{J^c}|x_J), && (35)
\end{aligned}$$

where (34) follows since $\{\mathbb{1}_{\{x,m,c,J\}}\}$ are independent due to the structure of the set $\mathcal{N}_{J,s}$ and the random binning, and (35) follows as for all $x_J \in \mathcal{D}_{\gamma^{(J)}}, p_{X_J}(x_J) \leq 2^{-\gamma^{(J)}}$. Lemma 1 follows by substituting (35) in (33), and noticing that

$$\sum_s \Big(\sum_{x_{J^c}\in\mathcal{N}_{J,s}} p^2(x_{J^c}|x_J) \Big)^{1/2} \leq \sum_s \sum_{x_{J^c}\in\mathcal{N}_{J,s}} p(x_{J^c}|x_J) \leq \sum_{x_{J^c}\in\mathcal{X}_{J^c}} p(x_{J^c}|x_J) = 1.$$

Appendix B
Proof of Lemma 2

We first consider $\bar{\mathbf{p}}$ that is the natural ordering of $[1:T]$. We prove the inequality in (11) for $\mathbf{p} = \bar{\mathbf{p}}$. Lemma 2 follows from a similar proof for all $\mathbf{p} \in \mathcal{P}$. For $\mathbf{p} = \bar{\mathbf{p}}$, we prove (11) by induction. For the base of induction, $T=1$, (11) reduces to the assertion in [4, Lemma 2]. Assume that (11) holds for $T = k-1$. The relative entropy in (11) at $T=k$ is given by

$$\begin{aligned}
&\mathbb{D}(P_{M_{1:k}C_{1:k}Z_S} || p^U_{M_{1:k}} p^U_{C_{1:k}} p_{Z_S}) \\
&\quad = \mathbb{D}(P_{M_{1:k}C_{1:k}Z_S} || P_{M_{1:k-1}C_{1:k-1}Z_S} p^U_{M_k} p^U_{C_k}) \\
&\qquad + \mathbb{D}(P_{M_{1:k-1}C_{1:k-1}Z_S} || p^U_{M_{1:k-1}} p^U_{C_{1:k-1}} p_{Z_S}). \quad (36)
\end{aligned}$$

Thus, the probability in (11), at $T=k$, is upper bounded by

$$\mathbb{P}_{\mathcal{B}}(\max_{S\in\mathcal{S}} \mathbb{D}(P_{M_{1:k-1}C_{1:k-1}Z_S} || p^U_{M_{1:k-1}} p^U_{C_{1:k-1}} p_{Z_S}) > (k-1)\tilde{\epsilon}) + \mathbb{P}_{\mathcal{B}}(\max_{S\in\mathcal{S}} \mathbb{D}(P_{M_{1:k}C_{1:k}Z_S} || P_{M_{1:k-1}C_{1:k-1}Z_S} p^U_{M_k} p^U_{C_k}) > \tilde{\epsilon}).$$

By the induction hypothesis, the first probability is upper bounded by $|\mathcal{S}||\mathcal{Z}| \sum_{t=1}^{k-1} \exp\left(\frac{-\epsilon^2(1-\delta)2^{\gamma_t^{\bar{\mathbf{p}}}}}{3\tilde{M}_t\tilde{C}_t} \right)$. Using similar analysis as in [6, Appendix B], we can show that the second probability is be upper bounded by $|\mathcal{S}||\mathcal{Z}| \exp\left(\frac{-\epsilon^2(1-\delta)2^{\gamma_k^{\bar{\mathbf{p}}}}}{3\tilde{M}_k\tilde{C}_k} \right)$. We conclude that (11) holds for $\mathbf{p} = \bar{\mathbf{p}}$. By rewriting (36) with the different permutations of $[1:k]$ and repeating the proof, the minimum over $\mathbf{p} \in \mathcal{P}$ in (11) follows, hence Lemma 2.

References

[1] L. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Sys. Tech. Journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[2] M. Nafea and A. Yener, "Wiretap channel II with a noisy main channel," *IEEE Int. Symp. Info. Theory, ISIT'15*, June 2015.

[3] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Semantic-security capacity for wiretap channels of type II," *IEEE Trans. Info. Theory*, vol. 62, no. 7, pp. 3863–3879, 2016.

[4] M. Nafea and A. Yener, "A new wiretap channel model and its strong secrecy capacity," *Submitted to IEEE Trans. Info. Theory*, 2016, arXiv preprint arXiv:1701.07007.

[5] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[6] M. Nafea and A. Yener, "A new multiple access wiretap channel model," *IEEE Info. Theory Workshop, ITW'16*, September 2016.

[7] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Info. Theory*, vol. 60, no. 11, pp. 6760–6786, 2014.

[8] A. El Gamal and Y.-H. Kim, *Network information theory*. Cambridge university press, 2011.

[9] M. Benammar and P. Piantanida, "Secrecy capacity region of some classes of wiretap broadcast channels," *IEEE Trans. Info. Theory*, vol. 61, no. 10, pp. 5564–5582, 2015.