The Multiple Access Wiretap Channel II with a Noisy Main Channel

Mohamed Nafea and Aylin Yener

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

***Abstract*—A two transmitter multiple access wiretap channel II (MAC-WT-II) with a discrete memoryless (DM) main channel is investigated. Two models for the wiretapper, who chooses a fixed-length subset of the channel uses and observes erasures outside this subset, are proposed. In the first model, in each position of the subset, the wiretapper noiselessly observes either the first or the second user's symbol, while in the second model, the wiretapper observes a noiseless superposition of the two symbols. Achievable strong secrecy rate regions for the two models are derived. The achievability is established by solving a dual secret key agreement problem in the source model. The secrecy of the keys in the dual source model is established by deriving a lemma which provides a doubly exponential convergence rate for the probability of the keys being uniform and independent from the wiretapper's observation. The results extend the recently examined WTC-II with a DM main channel to a multiple access setting.**

I. Introduction

The wiretap channel II (WTC-II), in which the legitimate terminals communicate over a noiseless channel while the wiretapper has perfect access to a fixed fraction of her choosing of the transmitted symbols, was introduced in [1]. This model while being similar to the discrete memoryless (DM) WTC with a noiseless main channel and binary erasure wiretapper channel, models a more capable wiretapper since she can select the positions of erasures. Reference [1] derived the capacity-equivocation region for the model and devised a coset coding scheme, i.e., a group code and its cosets were used as the subcodes for the wiretap code, which motivated the research on practical coding design for secrecy [2], [3].

Recently, reference [4] introduced a DM main channel to the WTC-II, and derived inner and outer bounds for its capacity-equivocation region. More recently, reference [5] characterized the secrecy capacity of this channel using a stronger version of Wyner's soft covering lemma [6].

In this paper, we extend the WTC-II with a DM main channel to a multiple access setting [7]. Two models for the wiretapper are proposed. The wiretapper in the first model observes either user in each tapped position, while in second model, she observes a noiseless superposition of the two users. Achievable strong secrecy rate regions for both models are derived by adopting the output statistics of random binning framework in [8], where an appropriate dual source coding problem is solved and the solution is converted to the original model using probability distribution approximation arguments.

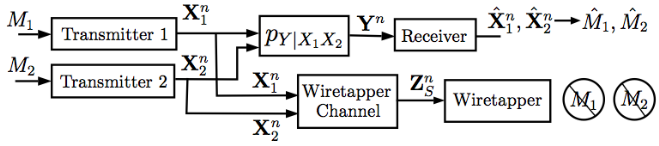

Fig. 1. The multiple access wiretap channel II with a noisy main channel.

Notation: For $S \subseteq \mathbb{N}$, $\mathbf{X}_S = \{X_i\}_{i \in S}$. p_X^U denotes a uniform distribution over X. $\mathbb{V}(p_X, q_X)$, $\mathbb{D}(p_X || q_X)$ denote the variational distance and K-L divergence between p_X and q_X. $\mathbf{Conv}(\mathcal{R})$ denotes the convex hull of region $\mathcal{R}$.

II. Channel Model

Consider the model in Fig. 1. The main channel consists of two finite input alphabets $\mathcal{X}_1, \mathcal{X}_2$, a finite output alphabet $\mathcal{Y}$, and transition probability $p_{Y|X_1X_2}$. Each transmitter wishes to reliably communicate an independent message to a common receiver and to keep it secret from the wiretapper. To do so, transmitter j maps its message M_j, uniformly distributed over $[\![1, 2^{nR_j}]\!]$, into the codeword $\mathbf{X}_j^n = [X_{j,1}, \cdots, X_{j,n}] \in \mathcal{X}_j^n$ using a stochastic encoder, $j = 1, 2$. The receiver observes $\mathbf{Y}^n \in \mathcal{Y}^n$ and outputs the estimates $\hat{M}_j, j = 1, 2$. We consider the following two models for the wiretapper channel.

Model I: The wiretapper chooses the subset $S_p \in \mathcal{S}_{\rm p}$ and the sequence $S_{\rm u} \in \{1, 2\}^\mu$, where $\mathcal{S}_{\rm p} = \{S_p : S_p \subseteq [\![1, n]\!], |S_p| = \mu\}$, $\mu \le n$, and $\alpha = \frac{\mu}{n} \in [0, 1]$. That is, S_p represents the subset of positions tapped by the wiretapper and $S_{\rm u}$ represents her sequence of decisions to observe *either the first or the second user* symbols. Let $S_p(k), S_{\rm u}(k)$ denote the kth elements of S_p and $S_{\rm u}$, and let S be a set of pairs which represents the wiretapper strategy, and defined as

$$S \triangleq \{(S_p(k), S_{\rm u}(k)) : k = 1, 2, \cdots, \mu\} \in \mathcal{S}, \quad (1)$$

where $\mathcal{S}$ is the set of all possible strategies for the wiretapper. The wiretapper observes $\mathbf{Z}_S^n = [Z_1^S \cdots Z_n^S] \in \mathcal{Z}^n$, where

$$Z_i^S = \begin{cases} X_{j,i}, & (i, j) \in S \\ ?, & \text{otherwise.} \end{cases} \quad (2)$$

Model II: The wiretapper chooses the subset $S \in \mathcal{S}$, with

$$\mathcal{S} \triangleq \left\{ S : S \subseteq [\![1, n]\!],\ |S| = \mu \le n,\ \alpha = \frac{\mu}{n} \in [0, 1] \right\}, \quad (3)$$

978-1-5090-1805-5/16/$31.00 ©2016 IEEE

and observes $\mathbf{Z}_S^n = [Z_1^S \ \cdots \ Z_n^S] \in \mathcal{Z}^n$, where

$$Z_i^S = \begin{cases} X_{1,i} + X_{2,i}, & i \in S \\ ?, & \text{otherwise}. \end{cases} \tag{4}$$

That is, the wiretapper observes a noiseless *superposition of the two symbols* in the subset S, and erasures otherwise.

An $(n, 2^{nR_1}, 2^{nR_2})$ channel code $\mathcal{C}_n$ consists of two message sets $\mathcal{M}_1 = [\![1, 2^{nR_1}]\!], \mathcal{M}_2 = [\![1, 2^{nR_2}]\!]$, two stochastic encoders $P_{\mathbf{X}_1^n|M_1,\mathcal{C}_n}, P_{\mathbf{X}_2^n|M_2,\mathcal{C}_n}$, and a decoder at the receiver. (R_1, R_2) is an achievable strong secrecy rate pair if there exists a sequence of $(n, 2^{nR_1}, 2^{nR_2})$ codes, $\{\mathcal{C}_n\}_{n\geq 1}$, such that (s.t.)

$$\lim_{n\to\infty} \mathbb{P}\big((\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)|\mathcal{C}_n\big) = 0, \quad \textbf{Reliability}, \tag{5}$$

$$\lim_{n\to\infty} \max_{S} I(M_1, M_2; \mathbf{Z}_S^n|\mathcal{C}_n) = 0, \quad \textbf{Strong Secrecy}. \tag{6}$$

III. Main Results

Theorem 1 *For $\alpha \in [0, 1]$, an achievable strong secrecy rate region for the MAC-WT-II with the wiretapper Model I is*

$$\begin{aligned} \mathcal{R}_\alpha^{\mathrm{I}} = \mathbf{Conv} \bigcup_{p_{U_1X_1}p_{U_2X_2}} \Big\{&(R_1, R_2) : \\ &R_1 \leq I(U_1; Y|U_2) - \alpha I(U_1; X_1), \\ &R_2 \leq I(U_2; Y|U_1) - \alpha I(U_2; X_2), \\ &R_1 + R_2 \leq I(U_1, U_2; Y) - \alpha I(U_1, U_2; X_1, X_2)\Big\}, \end{aligned} \tag{7}$$

where the union is over all distributions $p_{U_1X_1}p_{U_2X_2}$ which satisfy the Markov chains $U_1 - X_1 - Y$ and $U_2 - X_2 - Y$.

Theorem 2 *For $\alpha \in [0, 1]$, an achievable strong secrecy rate region for the MAC-WT-II with the wiretapper Model II is*

$$\begin{aligned} \mathcal{R}_\alpha^{\mathrm{II}} = \mathbf{Conv} \bigcup_{p_{U_1X_1}p_{U_2X_2}} \Big\{&(R_1, R_2) : \\ &R_1 \leq I(U_1; Y|U_2) - \alpha I(U_1; X_1 + X_2), \\ &R_2 \leq I(U_2; Y|U_1) - \alpha I(U_2; X_1 + X_2), \\ &R_1 + R_2 \leq I(U_1, U_2; Y) - \alpha I(U_1, U_2; X_1 + X_2)\Big\}, \end{aligned} \tag{8}$$

where the union is over all distributions $p_{U_1X_1}p_{U_2X_2}$ which satisfy the Markov chains $U_1 - X_1 - Y$ and $U_2 - X_2 - Y$.

The proofs for Theorems 1, 2 are provided in Section IV.

Remark 1 *The individual rates in Theorem 1 represent the worst-case scenarios in which the wiretapper chooses to observe only one user's symbols in all the positions she taps.*

Remark 2 *$\mathcal{R}_\alpha^{\mathrm{I}} \subset \mathcal{R}_\alpha^{\mathrm{II}}$, as every $(R_1, R_2) \in \mathcal{R}_\alpha^{\mathrm{I}}$ also belongs to $\mathcal{R}_\alpha^{\mathrm{II}}$; $U_j - X_j - X_1 + X_2, j = 1, 2$, and $U_1U_2 - X_1X_2 - X_1 + X_2$ are Markov chains. This is not surprising since the wiretapper in Model I is more powerful.*

IV. Proofs for Theorem 1 and Theorem 2

We first prove Theorem 1. Let us first consider $U_1 = X_1$ and $U_2 = X_2$. We fix $p_{X_1X_2} = p_{X_1}p_{X_2}$ and describe two protocols, where each protocol defines a set of random variables and induces a joint distribution over them. Throughout the paper, we use the convention $A_{[1,2]} = (A_1, A_2)$ for random variables (vectors) and their realizations.

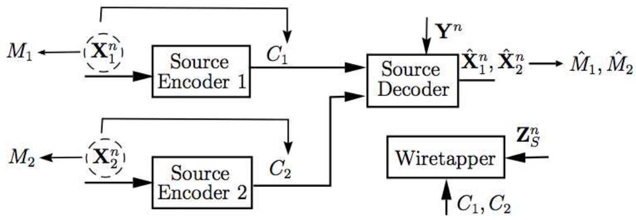

Fig. 2. Protocol A: Secret key agreement in the source model.

Protocol A: This protocol describes a dual secret key agreement problem in the source model, see Fig. 2. Let $\mathbf{X}_1, \mathbf{X}_2, \mathbf{Y}$ be i.i.d. according to the distribution $p_{X_1}p_{X_2}p_{Y|X_1X_2}$, where $p_{Y|X_1X_2}$ is the conditional probability of the main channel in Fig. 1. The sequence $\mathbf{X}_j, j = 1, 2$, observed at the jth encoder, is randomly and independently binned into the two indices $M_j = \mathcal{B}_1^{(j)}(\mathbf{X}_j)$, $C_j = \mathcal{B}_2^{(j)}(\mathbf{X}_j)$, where $\mathcal{B}_1^{(j)}, \mathcal{B}_2^{(j)}$ are uniform over $[\![1, 2^{nR_j}]\!]$, $[\![1, 2^{n\tilde{R}_j}]\!]$; each $\mathbf{x}_j \in \mathcal{X}_j^n$ is randomly and independently assigned to $m_j \in [\![1, 2^{nR_j}]\!]$, $c_j \in [\![1, 2^{n\tilde{R}_j}]\!]$. $C_j, j = 1, 2$, represent the messages transmitted noiselessly to the decoder and perfectly accessed by the wiretapper, while $M_j, j = 1, 2$, represent the confidential keys generated at the encoders and reconstructed at the decoder. The decoder, upon observing C_1, C_2 and the i.i.d. sequence $\mathbf{Y}$, outputs the estimates $\hat{\mathbf{X}}_1, \hat{\mathbf{X}}_2$, which are mapped to the estimates $\hat{M}_1, \hat{M}_2$. Let $\mathcal{S}$, $\mathbf{Z}_S, \forall S \in \mathcal{S}$, be defined as in (1), (2). The wiretapper chooses the strategy S whose realization is unknown to the other terminals, i.e., the wiretapper is a compound source $\mathbf{Z}_S \triangleq \{\mathcal{Z}, p_{\mathbf{Z}_S}\}$ whose distribution is only known to belong to the finite class $\{p_{\mathbf{Z}_S}\}_{S\in\mathcal{S}}$, where $|\mathcal{S}| \leq 2^{(1+\alpha)n}$.

Let $\mathbb{1}_{\{\mathbf{X},M,C,\{1,2\}\}} \triangleq \mathbb{1}\big\{\mathcal{B}_1^{(j)}(\mathbf{X}_j) = M_j, \mathcal{B}_2^{(j)}(\mathbf{X}_j) = C_j, \forall j = 1, 2\big\}$. The induced distribution for protocol A, is

$$\begin{aligned} &\tilde{P}_{M_{[1,2]}C_{[1,2]}\mathbf{X}_{[1,2]}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{[1,2]}} \\ &= p_{\mathbf{X}_{[1,2]}\mathbf{Y}\mathbf{Z}_S}\mathbb{1}_{\{\mathbf{X},M,C,\{1,2\}\}}\tilde{P}_{\hat{\mathbf{X}}_{[1,2]}|\mathbf{Y}C_{[1,2]}} = \tilde{P}_{M_{[1,2]}C_{[1,2]}} \\ &\quad \tilde{P}_{\mathbf{X}_{[1,2]}|M_{[1,2]}C_{[1,2]}}\, p_{\mathbf{Y}\mathbf{Z}_S|\mathbf{X}_{[1,2]}}\tilde{P}_{\hat{\mathbf{X}}_{[1,2]}|\mathbf{Y}C_{[1,2]}}. \end{aligned} \tag{9}$$

Protocol B: This protocol is defined as the main problem in Fig. 1, with assuming the availability of common randomness $C_j, j = 1, 2$, at all nodes, which is uniform over $[\![1, 2^{n\tilde{R}_j}]\!]$ and independent from all other variables. The encoders and decoder are defined as in (9). The induced joint distribution for protocol B, $P_{M_{[1,2]}C_{[1,2]}\mathbf{X}_{[1,2]}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{[1,2]}}$, is equal to

$$p^U_{M_{[1,2]}}p^U_{C_{[1,2]}}\tilde{P}_{\mathbf{X}_{[1,2]}|M_{[1,2]}C_{[1,2]}}p_{\mathbf{Y}\mathbf{Z}_S|\mathbf{X}_{[1,2]}}\tilde{P}_{\hat{\mathbf{X}}_{[1,2]}|\mathbf{Y}C_{[1,2]}}. \tag{10}$$

Notice that $\tilde{P}_{\mathbf{X}_{[1,2]}|M_{[1,2]}C_{[1,2]}}$ factors as $\tilde{P}_{\mathbf{X}_1|M_1C_1}\tilde{P}_{\mathbf{X}_2|M_2C_2}$, i.e., the common randomness C_i available at the jth transmitter, $i, j = 1, 2, i \neq j$, is not used to generate $\mathbf{X}_j$.

The induced distributions in (9), (10) are random due to the random binning. Also, we have ignored the $\hat{M}$ variables at this stage, as we will introduce them later as deterministic functions of the $\hat{\mathbf{X}}$ vectors after fixing the binning functions. The remaining steps are: (i) we derive rate conditions for protocol A such that its induced distribution in (9) is close in the variational distance sense to (10), and that protocol A is reliable and secure, (ii) we utilize the closeness of the two induced distributions to show that, under the same rate conditions, protocol B is reliable and secure as well, and finally (iii) we eliminate the assumed common randomness C_1, C_2 from protocol B by conditioning on certain instances of them.

We now state the following two lemmas by which we derive conditions on the rates $R_j, \tilde{R}_j, j = 1,2$, required for the closeness of the two induced distributions and the security of protocol A. In particular, Lemma 1 provides an *exponential decay* of the average variational distance between the two induced distributions, which is used to show a convergence in probability result needed in the proof. Lemma 2 provides a *doubly-exponential decay* of the probability of not achieving secrecy for protocol A, which is needed, with the union bound, to guarantee secrecy for the exponentially many choices of S.

Lemma 1 *Let $X_1 \triangleq \{\mathcal{X}_1, p_{X_1}\}$, $X_2 \triangleq \{\mathcal{X}_2, p_{X_2}\}$ be two independent sources. The source $X_j, j = 1,2$, is randomly binned into $M_j = \mathcal{B}_1^{(j)}(X_j)$, $C_j = \mathcal{B}_2^{(j)}(X_j)$, where $\mathcal{B}_1^{(j)}, \mathcal{B}_2^{(j)}$ are independent and uniform over $[\![1, \tilde{M}_j]\!]$, $[\![1, \tilde{C}_j]\!]$. Let $\mathcal{B} \triangleq \{\mathcal{B}_1^{(j)}(x_j), \mathcal{B}_2^{(j)}(x_j)\}_{j=1,2,x_j\in\mathcal{X}_j}$, and for $\gamma_j > 0, j = 1,2$, define $\mathcal{D}_{\gamma_j} \triangleq \{x_j \in \mathcal{X}_j : \log\frac{1}{p_{X_j}(x_j)} > \gamma_j\}$. Then, we have*

$$\mathbb{E}_{\mathcal{B}}\mathbb{V}\big(P_{M_{[1,2]}C_{[1,2]}}, p^U_{M_{[1,2]}}p^U_{C_{[1,2]}}\big) \leq \sum_{j=1,2}\big[\mathbb{P}(X_j \notin \mathcal{D}_{\gamma_j}) + 1/2(\tilde{M}_j\tilde{C}_j2^{-\gamma_j})^{\frac{1}{2}}\big],$$ *P is the induced distribution.* (11)

Proof: Using the triangle inequality, we obtain

$$\mathbb{V}(P_{M_{[1,2]}C_{[1,2]}}, p^U_{M_{[1,2]}}p^U_{C_{[1,2]}}) \leq \sum_{j=1,2}\mathbb{V}(P_{M_jC_j}, p^U_{M_j}p^U_{C_j}).$$

Using [9, Appendix. A], we have, for $j = 1,2$,

$$\mathbb{E}_{\mathcal{B}}\big(\mathbb{V}(P_{M_jC_j}, p^U_{M_j}p^U_{C_j})\big) \leq \mathbb{P}(X_j \notin \mathcal{D}_{\gamma_j}) + \frac{1}{2}\sqrt{\tilde{M}_j\tilde{C}_j2^{-\gamma_j}}.$$

■

Lemma 2 *Let $X_1 \triangleq \{\mathcal{X}_1, p_{X_1}\}$, $X_2 \triangleq \{\mathcal{X}_2, p_{X_2}\}$ be two independent sources, both correlated with the compound source $\{Z_S\} \triangleq \{\mathcal{Z}, p_{Z_S}\}, S \in \mathcal{S}$, where $|\mathcal{X}_1|, |\mathcal{X}_2|, |\mathcal{Z}|, |\mathcal{S}| < \infty$. The source X_j is randomly binned into M_j, C_j as in Lemma 1. For $\gamma_j, \gamma_{ij} > 0, i,j = 1,2, i \neq j$, and any $S \in \mathcal{S}$, define*

$$\mathcal{D}_j^S \triangleq \big\{(x_{[1,2]}, z) \in \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Z} : (x_j, z) \in \mathcal{D}^S_{\gamma_j}, (x_{[1,2]}, z) \in \mathcal{D}^S_{\gamma_{ij}}\big\},$$ *where* $$\mathcal{D}^S_{\gamma_j} \triangleq \big\{(x_j, z) : -\log p_{X_j|Z_S}(x_j|z) > \gamma_j\big\},$$ *and* $$\mathcal{D}^S_{\gamma_{ij}} \triangleq \big\{(x_{[1,2]}, z) : -\log p_{X_i|X_jZ_S}(x_i|x_j, z) > \gamma_{ij}\big\}.$$

If $\exists\delta \in]0, \frac{1}{2}[$ s.t. $\forall S$, $\min_{j=1,2}\mathbb{P}_{p_{X_{[1,2]}Z_S}}\big((X_{[1,2]}, Z_S) \in \mathcal{D}_j^S\big) \geq 1 - \delta^2$, then, we have, for every $\epsilon \in [0,1]$, that

$$\mathbb{P}_{\mathcal{B}}\Big(\max_{S\in\mathcal{S}}\mathbb{D}(P_{M_{[1,2]}C_{[1,2]}Z_S}||p^U_{M_{[1,2]}}p^U_{C_{[1,2]}}p_{Z_S}) \geq 2\tilde{\epsilon}\Big) \leq |\mathcal{S}||\mathcal{Z}|\min_{i,j=1,2,i\neq j}\Big\{e^{\left(\frac{-\epsilon^2(1-\delta)2^{\gamma_j}}{3\tilde{M}_j\tilde{C}_j}\right)} + e^{\left(\frac{-\epsilon^2(1-\delta)2^{\gamma_{ij}}}{3\tilde{M}_i\tilde{C}_i}\right)}\Big\}, \quad (12)$$

where $\tilde{\epsilon} = \max_{j=1,2}\{\epsilon + (\delta+\delta^2)\log(\tilde{M}_j\tilde{C}_j) + H_b(\delta^2)\}$, H_b is the binary entropy function, and P is the induced distribution.

Proof: See the Appendix. ■

We now use Lemma 1 to establish the closeness of the induced distributions. In Lemma 1, set $X_j = \mathbf{X}_j$, $\tilde{M}_j = 2^{nR_j}$, $\tilde{C}_j = 2^{n\tilde{R}_j}$, $\gamma_j = n(1-\epsilon')H(X_j), j = 1,2$ ($\mathbf{X}_j$ is defined as in protocol A). Note that for $\gamma_j < \infty$, any $\mathbf{x}_j$ with $p(\mathbf{x}_j) = 0$ belongs to $\mathcal{D}_{\gamma_j}, j = 1,2$, by definition. Thus, in order to calculate $\mathbb{P}(\mathcal{D}^c_{\gamma_j})$, we only consider $\mathbf{x}_j$s with $p(\mathbf{x}_j) > 0$. Without loss of generality, let $p(x_j) > 0$, $\forall x_j \in \mathcal{X}_j$. Let $p_{j,\min} = \min_{x_j} p(x_j)$. The random variables $\log\frac{1}{p(X_{j,i})}, i \in [\![1, n]\!]$, are i.i.d. and each is bounded by the interval $[0, \log\frac{1}{p_{j,\min}}]$. Using Hoeffding inequality [10], for any $\epsilon' > 0$, $\exists\beta_j > 0$ s.t.

$$\mathbb{P}(\mathcal{D}^c_{\gamma_j}) = \mathbb{P}\Big(\sum_{k=1}^n\log\frac{1}{p(X_{j,k})} \leq (1-\epsilon')nH(X_j)\Big) \leq e^{-\beta_jn}.$$

Using (11), if $R_j + \tilde{R}_j < (1-\epsilon')H(X_j), \forall j$, then $\exists\beta > 0$ s.t.

$$\mathbb{E}_{\mathcal{B}}\mathbb{V}(\tilde{P}_{M_{[1,2]}C_{[1,2]}\mathbf{X}_{[1,2]}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{[1,2]}}, P_{M_{[1,2]}C_{[1,2]}\mathbf{X}_{[1,2]}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{[1,2]}}) = \mathbb{E}_{\mathcal{B}}\mathbb{V}(\tilde{P}_{M_{[1,2]}C_{[1,2]}}, p^U_{M_{[1,2]}}p^U_{C_{[1,2]}}) \leq 4\exp(-\beta n). \quad (13)$$

For reliability for protocol A, we use Slepian-Wolf decoder, which implies that $\lim_{n\to\infty}\mathbb{E}_{\mathcal{B}}\mathbb{P}_{\tilde{P}}(\hat{\mathbf{X}}_{[1,2]} \neq \mathbf{X}_{[1,2]}) = 0$ if $\tilde{R}_1 \geq H(X_1|X_2, Y)$, $\tilde{R}_2 > H(X_2|X_1, Y)$ and $\tilde{R}_1 + \tilde{R}_2 > H(X_{[1,2]}|Y)$ [11, Theorem 10.3]. Thus, $\forall S$ [8, Lemma 1]

$$\lim_{n\to\infty}\mathbb{E}_{\mathcal{B}}\mathbb{V}\big(\tilde{P}_{M_{[1,2]}C_{[1,2]}\mathbf{X}_{[1,2]}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{[1,2]}}, \tilde{P}_{M_{[1,2]}C_{[1,2]}\mathbf{X}_{[1,2]}\mathbf{Y}\mathbf{Z}_S}\mathbb{1}\{\hat{\mathbf{X}}_{[1,2]} = \mathbf{X}_{[1,2]}\}\big) = 0. \quad (14)$$

Next, we use Lemma 2 to establish secrecy for protocol A. In Lemma 2, for $j = 1,2$, set $X_j = \mathbf{X}_j$ ($\mathbf{X}_j$ is defined as in protocol A), $\tilde{M}_j = 2^{nR_j}$, $\tilde{C}_j = 2^{n\tilde{R}_j}$, $Z_S = \mathbf{Z}_S, \forall S \in \mathcal{S}$; $\mathcal{S}, \mathbf{Z}_S$ are defined as in (1), (2). For $\bar{\epsilon} > 0$, $i = 1,2, i \neq j$, set

$$\gamma_j = (1-\bar{\epsilon})\min_{S\in\mathcal{S}}H(\mathbf{X}_j|\mathbf{Z}_S) = (1-\bar{\epsilon})(n-\mu)H(X_j),$$
$$\gamma_{ij} = (1-\bar{\epsilon})\min_{S\in\mathcal{S}}H(\mathbf{X}_i|\mathbf{X}_j, \mathbf{Z}_S) = (1-\bar{\epsilon})(n-\mu)H(X_i).$$

Define $\overline{S}_j \triangleq \{k : (k,j) \in S\}$, i.e., $\overline{S}_j$ is the set of positions in which the wiretapper observes the jth transmitter's signal. Let $|\overline{S}_j| = \mu_j$, where $\mu_1 + \mu_2 = \mu$. For the tuples $(\mathbf{x}_{[1,2]}, \mathbf{z})$ with $p_{\mathbf{X}_j|\mathbf{Z}_S}(\mathbf{x}_j|\mathbf{z})$ and $p_{\mathbf{X}_i|\mathbf{X}_j\mathbf{Z}_S}(\mathbf{x}_i|\mathbf{x}_j, \mathbf{z}) > 0$, where $i,j = 1,2, i \neq j$, we have, for all $S \in \mathcal{S}$, that

$$p_{\mathbf{X}_j|\mathbf{Z}_S} = p_{\mathbf{X}_{j,\overline{S}_j}\mathbf{X}_{j,\overline{S}_j^c}|\mathbf{X}_{j,\overline{S}_j}\mathbf{X}_{i,\overline{S}_i}} = p_{\mathbf{X}_{j,\overline{S}_j^c}} = \prod_{k\in\overline{S}_j^c}p(x_{j,k}),$$
$$p_{\mathbf{X}_i|\mathbf{X}_j\mathbf{Z}_S} = p_{\mathbf{X}_{i,\overline{S}_i}\mathbf{X}_{i,\overline{S}_i^c}|\mathbf{X}_j\mathbf{X}_{i,\overline{S}_i}} = p_{\mathbf{X}_{i,\overline{S}_i^c}} = \prod_{k\in\overline{S}_i^c}p(x_{i,k}).$$

Using Hoeffding inequality and the definition of $\mathcal{D}^S_{\gamma_j}$, we have

$$\mathbb{P}\big((\mathbf{X}_j, \mathbf{Z}_S) \notin \mathcal{D}^S_{\gamma_j}\big) = \mathbb{P}\Big(\sum_{k\in\overline{S}_j^c}\log\frac{1}{p(X_{j,k})} \leq \gamma_j\Big) \leq \mathbb{P}\Big(\sum_{k\in\overline{S}_j^c}\log\frac{1}{p(X_{j,k})} \leq (1-\bar{\epsilon})(n-\mu_j)H(X_j)\Big) \leq e^{-\tilde{\beta}_jn},$$

where $\tilde{\beta}_j > 0$, $j = 1,2$. Similarly, for $i,j = 1,2, i \neq j$, there exists $\tilde{\beta}_{ij} > 0$ s.t. $\mathbb{P}\big((\mathbf{X}_{[1,2]}, \mathbf{Z}_S) \notin \mathcal{D}^S_{\gamma_{ij}}\big) \le \exp(-\tilde{\beta}_{ij} n)$. Taking $\delta^2 = 2\exp(-\tilde{\beta} n)$, where $\tilde{\beta} = \min\{\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_{12}, \tilde{\beta}_{21}\}$, gives $\mathbb{P}((\mathbf{X}_{[1,2]}, \mathbf{Z}_S) \notin \mathcal{D}^S_j) \le \delta^2$, for all $S \in \mathcal{S}$ and $j = 1, 2$. Note that $\lim_{n\to\infty} \delta^2 = 0$, and hence, for n sufficiently large, $\delta^2 \in]0, \frac{1}{4}[$. Using (12), we have, for every $\epsilon, \epsilon_1 > 0$, $\tilde{\epsilon} = \epsilon + \epsilon_1$, there exists $n^* \in \mathbb{N}$ and $\kappa_\epsilon, \tilde{\kappa} > 0$ s.t. for all $n \ge n^*$,

$$\mathbb{P}(\max_{S\in\mathcal{S}} \mathbb{D}(\tilde{P}_{M_{[1,2]}C_{[1,2]}\mathbf{Z}_S} || p^U_{M_{[1,2]}} p^U_{C_{[1,2]}} p_{\mathbf{Z}_S}) \ge 2\tilde{\epsilon}) \le e^{-\kappa_\epsilon e^{\tilde{\kappa} n}}$$
$$\text{when } R_j + \tilde{R}_j < (1-\bar{\epsilon})(1-\alpha)H(X_j), \ \forall j = 1, 2, \tag{15}$$

since $|\mathcal{S}||\mathcal{Z}^n| \le \exp(n[(1+\alpha)\ln 2 + \ln(|\mathcal{X}_1| + |\mathcal{X}_2| + 1)])$.

Let $D_n \triangleq \max_S \mathbb{D}\big(\tilde{P}_{M_{[1,2]}C_{[1,2]}\mathbf{Z}_S} || p^U_{M_{[1,2]}} p^U_{C_{[1,2]}} p_{\mathbf{Z}_S}\big)$, $\mathcal{K}_n \triangleq \{D_n \ge r\}$, $r > 0$. By (15), $\sum_{n=1}^{\infty} \mathbb{P}(\mathcal{K}_n) < \infty$. Thus, $\mathbb{P}(\mathcal{K}_n$ infinitely often (i.o.)$) = 0$ by the Borel-Cantelli lemma. This implies that $\forall r > 0$, $\mathbb{P}\big(\{D_n < r\} \text{ i.o.}\big) = 1$, i.e., D_n converges to 0 almost surely. Thus, as $n \to \infty$, we have

$$\mathbb{P}\big(\max_{S\in\mathcal{S}} \mathbb{D}(\tilde{P}_{M_{[1,2]}C_{[1,2]}\mathbf{Z}_S} || p^U_{M_{[1,2]}} p^U_{C_{[1,2]}} p_{\mathbf{Z}_S}) > 0\big) \to 0. \tag{16}$$

Now, we show that protocol B is also reliable and secure with the rate conditions above. (13) and (14) imply that

$$\lim_{n\to\infty} \mathbb{E}_{\mathcal{B}} \mathbb{V}(P_{M_{[1,2]}C_{[1,2]}\mathbf{X}_{[1,2]}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{[1,2]}}, P_{M_{[1,2]}C_{[1,2]}\mathbf{X}_{[1,2]}\mathbf{Y}\mathbf{Z}_S} \mathbb{1}\{\hat{\mathbf{X}}_{[1,2]} = \mathbf{X}_{[1,2]}\}) = 0. \tag{17}$$

Similar to the derivation of (16), Markov inequality and (13) imply that $\lim_{n\to\infty} \mathbb{P}(\mathbb{V}(\tilde{P}_{M_{[1,2]}C_{[1,2]}}, p^U_{M_{[1,2]}} p^U_{C_{[1,2]}}) > 0) = 0$. Thus, by the union bound and (16), we have

$$\begin{aligned}
&\lim_{n\to\infty} \mathbb{P}_{\mathcal{B}}\big(\max_{S\in\mathcal{S}} \mathbb{D}(P_{M_{[1,2]}C_{[1,2]}\mathbf{Z}_S} || p^U_{M_{[1,2]}} p^U_{C_{[1,2]}} p_{\mathbf{Z}_S}) > 0\big) \\
&\le \lim_{n\to\infty} \mathbb{P}\big(\max_{S\in\mathcal{S}} \mathbb{D}(\tilde{P}_{M_{[1,2]}C_{[1,2]}\mathbf{Z}_S} || p^U_{M_{[1,2]}} p^U_{C_{[1,2]}} p_{\mathbf{Z}_S}) > 0\big) \\
&+ \lim_{n\to\infty} \mathbb{P}\big(\mathbb{V}(\tilde{P}_{M_{[1,2]}C_{[1,2]}}, p^U_{M_{[1,2]}} p^U_{C_{[1,2]}}) > 0\big) = 0.
\end{aligned} \tag{18}$$

The selection lemma [12, Lemma 2.2] when applied to (17), (18), implies that there is at least one binning realization $\mathbf{b}^*$, with a corresponding joint distribution p^* for protocol B, s.t.,

$$\begin{aligned}
&\lim_{n\to\infty} \mathbb{1}\{\max_{S\in\mathcal{S}} \mathbb{D}(p^*_{M_{[1,2]}C_{[1,2]}\mathbf{Z}_S} || p^U_{M_{[1,2]}} p^U_{C_{[1,2]}} p_{\mathbf{Z}_S}) > 0\} = 0, \\
&\text{and } \lim_{n\to\infty} \mathbb{V}(p^*_{M_{[1,2]}C_{[1,2]}\mathbf{X}_{[1,2]}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{[1,2]}}, \\
&\quad p^*_{M_{[1,2]}C_{[1,2]}\mathbf{X}_{[1,2]}\mathbf{Y}\mathbf{Z}_S} \mathbb{1}\{\hat{\mathbf{X}}_{[1,2]} = \mathbf{X}_{[1,2]}\}) = 0,
\end{aligned} \tag{19}$$

with $M_j = b_1^{*(j)}(\mathbf{X}_j), C_j = b_2^{*(j)}(\mathbf{X}_j), j = 1, 2$. We introduce $p^*_{\hat{M}_{[1,2]}|\hat{\mathbf{X}}_{[1,2]}} = \mathbb{1}\{\hat{M}_j = b_1^{*(j)}(\hat{\mathbf{X}}_j), \forall j = 1, 2\}$ to (19). Then,

$$\begin{aligned}
\mathbb{E}_{C_{[1,2]}}\big(\mathbb{P}(\hat{M}_{[1,2]} \ne M_{[1,2]}|C_{[1,2]})\big) = \mathbb{V}\big(p^*_{M_{[1,2]}\hat{M}_{[1,2]}C_{[1,2]}}, \\
p^U_{M_{[1,2]}} p^U_{C_{[1,2]}} \mathbb{1}\{\hat{M}_{[1,2]} = M_{[1,2]}\}\big) \underset{n\to\infty}{\longrightarrow} 0,
\end{aligned} \tag{20}$$

follows from (19). Using the union bound, we also have

$$\begin{aligned}
&\mathbb{P}_{C_{[1,2]}}\big(\max_S \mathbb{D}(p^*_{M_{[1,2]}\mathbf{Z}_S|C_{[1,2]}} || p^U_{M_{[1,2]}} p^*_{\mathbf{Z}_S|C_{[1,2]}}) > 0\big) \\
&\le \mathbb{1}\{\max_S \mathbb{D}(p^*_{M_{[1,2]}C_{[1,2]}\mathbf{Z}_S} || p^U_{M_{[1,2]}} p^U_{C_{[1,2]}} p_{\mathbf{Z}_S}) > 0\} \\
&+ \mathbb{P}\big(\max_S \mathbb{D}(p^*_{M_{[1,2]}\mathbf{Z}_S|C_{[1,2]}} || p^U_{M_{[1,2]}} p^*_{\mathbf{Z}_S|C_{[1,2]}}) > 0, \text{ and} \\
&\quad \forall S,\ p^*_{M_{[1,2]}C_{[1,2]}\mathbf{Z}_S} = p^U_{M_{[1,2]}} p^U_{C_{[1,2]}} p_{\mathbf{Z}_S}\big) \underset{n\to\infty}{\longrightarrow} 0,
\end{aligned} \tag{21}$$

as the second term in the RHS of (21) is equal to zero.

Applying the selection lemma to (20), (21), implies that there is at least one $c^*_{[1,2]}$ s.t. both $\mathbb{P}(\hat{M}_{[1,2]} \ne M_{[1,2]}|C_{[1,2]} = c^*_{[1,2]})$ and $\max_S I(M_{[1,2]}; \mathbf{Z}_S|C_{[1,2]} = c^*_{[1,2]})$ converge to zero as $n \to \infty$. Let $\tilde{p}^*$ be the induced distribution for protocol A corresponding to $\mathbf{b}^*$. We use $\tilde{p}^*(\mathbf{x}_{[1,2]}|m_{[1,2]}, c^*_{[1,2]})$ as the encoder and $(\tilde{p}^*(\hat{\mathbf{x}}_{[1,2]}|\mathbf{y}, c^*_{[1,2]}), b_1^{*(j)}(\hat{\mathbf{x}}_j), j = 1, 2)$ as the decoder for the original model.

Combining the conditions $R_j + \tilde{R}_j < (1-\bar{\epsilon})(1-\alpha)H(X_j), j = 1, 2$, $\tilde{R}_1 \ge H(X_1|X_2Y)$, $\tilde{R}_2 \ge H(X_2|X_1Y)$, $\tilde{R}_1 + \tilde{R}_2 \ge H(X_{[1,2]}|Y)$, and taking $\bar{\epsilon} \to 0$, establish the achievability of the union over all $p_{X_1}p_{X_2}$ of the region of all pairs (R_1, R_2) satisfying $R_1 \le I(X_1; Y|X_2) - \alpha H(X_1)$, $R_2 \le I(X_2; Y|X_1) - \alpha H(X_2)$, and $R_1 + R_2 \le I(X_{[1,2]}; Y) - \alpha H(X_{[1,2]})$. By prefixing two independent channels, $p_{X_1|U_1}$, $p_{X_2|U_2}$, at the transmitters of the original model, we obtain the achievability of the union of the region in (7). The convex hull of the union follows by time sharing independent codes and the fact that maximizing the secrecy constraint over S in the whole block-length is upper bounded by its maximization over the individual segments of the time sharing.

The proof for Theorem 2 is similar to the proof of (7). The difference is that $\mathcal{S}$, $\mathbf{Z}_S, \forall S \in \mathcal{S}$, in protocol A are as in (3), (4). Applying Lemma 2 to protocol A, after prefixing the channels $p_{X_1|U_1}, p_{X_2|U_2}$, gives, $\forall S \in \mathcal{S}$ and $i, j = 1, 2, i \ne j$

$$\begin{aligned}
H(\mathbf{U}_j|\mathbf{Z}_S) &= n[(1-\alpha)H(U_j) + \alpha H(U_j|X_1 + X_2)] \\
H(\mathbf{U}_i|\mathbf{U}_j\mathbf{Z}_S) &= n[(1-\alpha)H(U_i) + \alpha H(U_{[1,2]}|X_1 + X_2) \\
&\quad - \alpha H(U_j|X_1 + X_2)],
\end{aligned}$$

which we use, along with Hoeffding inequality, to satisfy the conditions of the lemma and derive the rate conditions,

$$\begin{aligned}
&R_j + \tilde{R}_j < (1-\alpha)H(U_j) + \alpha H(U_j|X_1 + X_2), j = 1, 2, \\
&\sum_{j=1,2} R_j + \tilde{R}_j < (1-\alpha)H(U_{[1,2]}) + \alpha H(U_{[1,2]}|X_1 + X_2),
\end{aligned}$$

needed for secrecy. These conditions, combined with $\tilde{R}_1 \ge H(U_1|U_2Y)$, $\tilde{R}_2 \ge H(U_2|U_1Y)$, $\tilde{R}_1 + \tilde{R}_2 \ge H(U_{[1,2]}|Y)$ for the Slepian-Wolf decoder, and using time sharing establish (8).

Remark 3 By setting $j = 1, i = 2$, instead of the minimum, in the RHS of (12), Lemma 2 results in the maximum rate $R_1 + \tilde{R}_1$, and the corresponding rate $R_2 + \tilde{R}_2$ (according to the maximum sum rate) such that the probability in the LHS of (12) is vanishing. By switching i and j, the Lemma gives the maximum rate $R_2 + \tilde{R}_2$, and the corresponding rate $R_1 + \tilde{R}_1$ according to the maximum sum rate. Using this, one can deduce the maximum rate region, i.e., the maximum individual and sum rates, required for a vanishing probability.

V. Conclusion

In this paper, we have extended the WTC-II with a DM main channel [4] to a multiple access setting. We have proposed two models for the wiretapper and derived a strong secrecy achievable rate region for each. The achievable rate region for the model, where the wiretapper observes a noiseless superposition of the two signals in the positions of the subset she selects, is larger than the achievable region for the more powerful wiretapper who decides to perfectly access either the first or the second signal at each position. The tools we have used for achievability extend a set of tools, utilized for a single-user scenario in a recent work [9], to a multi-user setting. Future work includes upper bounds for these models and other multi-terminal setups with more capable wiretappers.

APPENDIX

For all S, $\mathbb{D}(P_{M_{[1,2]}C_{[1,2]}Z_S}||p^U_{M_{[1,2]}}p^U_{C_{[1,2]}}p_{Z_S})$ is equal to

$$E_{p_{Z_S}}\Big(\mathbb{D}(P_{M_{[1,2]}C_{[1,2]}|Z_S}||P_{M_1C_1|Z_S}p^U_{M_2}p^U_{C_2})\Big) + \mathbb{D}(p_{M_1C_1Z_S}||p^U_{M_1}p^U_{C_1}p_{Z_S}). \tag{22}$$

Thus, the probability in the LHS of (12) is upper bounded by

$$\mathbb{P}_{\mathcal{B}}\big(\max_{S\in\mathcal{S}}\mathbb{E}_{p_{Z_S}}\mathbb{D}(P_{M_{[1,2]}C_{[1,2]}|Z_S}||P_{M_1C_1|Z_S}p^U_{M_2}p^U_{C_2})>\tilde{\epsilon}\big) + \mathbb{P}_{\mathcal{B}}\big(\max_{S\in\mathcal{S}}\mathbb{D}(P_{M_1C_1Z_S}||p^U_{M_1}p^U_{C_1}p_{Z_S})>\tilde{\epsilon}\big). \tag{23}$$

We upper bound each term in (23). For all $S\in\mathcal{S}$, define

$$\mathcal{A}_S \triangleq \big\{z\in\mathcal{Z}:\mathbb{P}_{p_{X_{[1,2]}|Z_S}}\big((X_{[1,2]},z)\in\mathcal{D}^S_1\big)\geq 1-\delta\big\}.$$

Using Markov inequality, we have, for all $S\in\mathcal{S}$

$$\mathbb{P}_{p_{Z_S}}(\mathcal{A}^c_S)\leq\frac{1}{\delta}\mathbb{P}_{p_{X_{[1,2]}Z_S}}\big((X_{[1,2]},Z_S)\notin\mathcal{D}^S_1\big)\leq\delta. \tag{24}$$

Let $\mathbb{1}_{\{x,m,c,\mathcal{J}\}}\triangleq\mathbb{1}\{\mathcal{B}^{(j)}_1(x_j)=m_j,\mathcal{B}^{(j)}_2(x_j)=c_j,\forall j\in\mathcal{J}\}$, where $\mathcal{J}\subseteq\{1,2\}$, and let $\mathbb{1}_{\mathcal{D}^S_1}=\mathbb{1}\{(x_{[1,2]},z)\in\mathcal{D}^S_1\}$ and $\mathbb{1}_{(\mathcal{D}^S_1)^c}=\mathbb{1}\{(x_{[1,2]},z)\notin\mathcal{D}^S_1\}$. For any $m_{[1,2]},c_{[1,2]}$, $z\in\mathcal{Z}$, and $S\in\mathcal{S}$, define

$$P^S_1(m_{[1,2]},c_{[1,2]}|z)=\sum_{x_{[1,2]}}p(x_{[1,2]}|z)\mathbb{1}_{\{x,m,c,\{1,2\}\}}\mathbb{1}_{\mathcal{D}^S_1}$$
$$P^S_2(m_{[1,2]},c_{[1,2]}|z)=\sum_{x_{[1,2]}}p(x_{[1,2]}|z)\mathbb{1}_{\{x,m,c,\{1,2\}\}}\mathbb{1}_{(\mathcal{D}^S_1)^c},$$

hence $P_{M_{[1,2]}C_{[1,2]}|Z_S}=P^S_1+P^S_2$. For every $x_2\in\mathcal{X}_2$, define

$$U_{x_2}=\sum_{x_1\in\mathcal{X}_1}p(x_{[1,2]}|z)\mathbb{1}_{\{x,m,c,\{2\}\}}\mathbb{1}_{\mathcal{D}^S_1}.$$

$\{U_{x_2}\}_{x_2\in\mathcal{X}_2}$ are independent. For $(x_{[1,2]},z)\in\mathcal{D}^S_1$, we have $(x_{[1,2]},z)\in\mathcal{D}^S_{\gamma_{21}}$ and $p(x_2|x_1,z)\leq 2^{-\gamma_{21}}$. Thus,

$$U_{x_2}\leq\sum_{x_1}p(x_1|z)p(x_2|x_1,z)\mathbb{1}\{(x_{[1,2]},z)\in\mathcal{D}^S_{\gamma_{21}}\}\leq 2^{-\gamma_{21}}.$$

Since $\mathbb{E}_{\mathcal{B}}\mathbb{1}_{\{x,m,c,\{2\}\}}=\frac{1}{\tilde{M}_2\tilde{C}_2},\forall x_2\in\mathcal{X}_2$, we have

$$\bar{m}=\sum_{x_2}\mathbb{E}_{\mathcal{B}}(U_{x_2})=\frac{1}{\tilde{M}_2\tilde{C}_2}\mathbb{P}_{p_{X_{[1,2]}|Z_S}}((X_{[1,2]},z)\in\mathcal{D}^S_1).$$

Also, notice that $\sum_{m_1c_1}P^S_1(m_{[1,2]},c_{[1,2]}|z)=\sum_{x_2}U_{x_2}$ since $\sum_{m_1c_1}\mathbb{1}_{\{x,m,c,\{1,2\}\}}=\mathbb{1}_{\{x,m,c,\{2\}\}}$. Using a variation of Chernoff bound [9, Lemma 3], we have, $\forall\epsilon\in[0,1]$, $z\in\mathcal{A}_S$,

$$\mathbb{P}_{\mathcal{B}}\Big(P^S_1(m_{[1,2]},c_{[1,2]}|z)\geq\frac{1+\epsilon}{\tilde{M}_2\tilde{C}_2}P_{M_1C_1|Z_S}(m_1,c_1|z)\Big)$$
$$\leq\mathbb{P}\Big(\sum_{x_2}U_{x_2}\geq\frac{1+\epsilon}{\tilde{M}_2\tilde{C}_2}\sum_{m_1c_1}P_{M_1C_1|Z_S}(m_1,c_1|z)\Big)$$
$$\leq\mathbb{P}\Big(\sum_{x_2}U_{x_2}\geq(1+\epsilon)\bar{m}\Big)\leq\exp\left(\frac{-\epsilon^2(1-\delta)2^{\gamma_{21}}}{3\tilde{M}_2\tilde{C}_2}\right), \tag{25}$$

where $\bar{m}\geq\frac{1-\delta}{\tilde{M}_2\tilde{C}_2},\forall z\in\mathcal{A}_S$. Let $\mathbf{b}=\{b^{(j)}_1,b^{(j)}_2,j=1,2\}$ be a realization of $\mathcal{B}$. Note that P^S_1 is identically distributed for all $m_{[1,2]},c_{[1,2]}$ due to the symmetry in the random binning.

We then define the class $\mathcal{G}$ of binning functions as

$$\mathcal{G}\triangleq\Big\{\mathbf{b}:P^S_1(m_{[1,2]},c_{[1,2]}|z)<\frac{1+\epsilon}{\tilde{M}_2\tilde{C}_2}P_{M_1C_1|Z_S}(m_1,c_1|z), \forall S\in\mathcal{S},\text{ and }\forall z\in\mathcal{A}_S\Big\}. \tag{26}$$

Using the union bound and (25), we have

$$\mathbb{P}_{\mathcal{B}}(\mathcal{G}^c)\leq|\mathcal{S}||\mathcal{Z}|\exp\left(\frac{-\epsilon^2(1-\delta)2^{\gamma_{21}}}{3\tilde{M}_2\tilde{C}_2}\right). \tag{27}$$

Let $M_j=b^{(j)}_1(X_j)$ and $C_j=b^{(j)}_2(X_j),j=1,2$. Using the same analysis as in [9, Appendix. B], we show that, for all $\mathbf{b}\in\mathcal{G}$, and $S\in\mathcal{S}$, we have

$$\mathbb{E}_{p_{Z_S}}\big(\mathbb{D}(P_{M_{[1,2]}C_{[1,2]}|Z_S}||P_{M_1C_1|Z_S}p^U_{M_2}p^U_{C_2})\big)\leq\epsilon+(\delta+\delta^2)\log(\tilde{M}_2\tilde{C}_2)+H_b(\delta^2)\leq\tilde{\epsilon}.$$

Thus, the first probability in (23) is upper bounded by $\mathbb{P}_{\mathcal{B}}(\mathcal{G}^c)$ in (27). Using similar arguments, we show that the second term in (23) is upper bounded by $|\mathcal{S}||\mathcal{Z}|e^{\left(\frac{-\epsilon^2(1-\delta)2^{\gamma_1}}{3\tilde{M}_1\tilde{C}_1}\right)}$. Finally, by rewriting (22) with switching the roles of (M_1,C_1) and (M_2,C_2) and repeating the proof, we obtain the second term in the minimum in (12), which completes the proof.

REFERENCES

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

[2] A. Thangaraj, et. al., "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Info. Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[3] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1725–1746, 2015.

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

[5] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Semantic-security capacity for wiretap channels of type II," *Submitted to IEEE Trans. Info. Theory*, 2015, arXiv pre-print arXiv:1509.03619v1.

[6] A. D. Wyner, "The common information of two dependent random variables," *IEEE Trans. Info. Theory*, vol. 21, no. 2, pp. 163–179, 1975.

[7] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[8] 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.

[9] M. Nafea and A. Yener, "A new wiretap channel model and its strong secrecy capacity," *Int. Symp. Info. Theory*, July 2016.

[10] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journ. Amer. Stat. Assoc.*, vol. 58, no. 301, pp. 13–30, 1963.

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

[12] M. Bloch and J. Barros, *Physical-layer security: From information theory to security engineering*. Cambridge University Press, 2011.