New Models for Interference and Broadcast Channels with Confidential Messages

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 model for the interference channel with confidential messages (IC-CM) is introduced, where each receiver, besides his noisy observations, is provided with a fixed-length subset, of his choosing, of noiseless observations for the transmitted codewords of both users, making confidential communication more challenging than the previous such model. In addition, in the same spirit, a broadcast channel with confidential messages (BC-CM), where the receivers noiselessly tap into subsets of their choice of the transmitted codeword, is considered. Achievable strong secrecy rate regions for both models are derived. In both models, the size of the subset quantifies a secure rate trade-off between the two receivers. The case of the new BC-CM model with one receiver's noisy observations are degraded with respect to the other receiver, and only the degraded receiver is provided with the subset of noiseless observations, is highlighted. In this case, the receiver with the degraded noisy observations has a positive rate after a certain threshold of his noiseless observations, i.e., with the aid of these symbols.**

I. Introduction

The wiretap channel (WTC) models a legitimate transmitter and receiver communicating in the presence of a wiretapper who observes the legitimate communication through a noisy channel [1]. Reference [2] has introduced WTC II which models a WTC with a noiseless main channel and a wiretapper who taps into a fixed subset of her choice of the transmitted bits [2]. The WTC II hence models a wiretapper more capable than the classical observer. Interestingly, the secrecy capacity for the WTC II does not increase when this more capable wiretapper is replaced with a binary erasure wiretapper channel [2].

Reference [3] has introduced a noisy main channel to the WTC II, and derived inner and outer bounds for its secrecy capacity. Later, reference [4] has derived the secrecy capacity for the model, showing that the secrecy capacity, once again, does not increase by replacing the more capable wiretapper with an erasure channel. Recently, reference [5] has introduced a new model for the WTC, in which the wiretapper noiselessly observes a subset of the transmitted symbols of her choice and observes the remaining symbols through a noisy channel, and derived its strong secrecy capacity. The new WTC model is extended to the multiple access channel in [6].

In this paper, we study the extension of the new WTC model in [5] to the interference channel with confidential messages (IC-CM) and broadcast channel with confidential messages (BC-CM) [7], [8]. We first consider a new IC-CM model, with each receiver, besides his noisy observations, is provided with noiseless observations for a subset, of his choice, of the transmitted codewords of both users. Next, we propose a BC-CM where each receiver chooses a subset of the transmitted codeword to noiselessly observe. We derive achievable strong secrecy rate regions for both models. Achievability is established by solving a dual secret key agreement problem in the source model and converting the solution to the original model [5], [9]. We observe that the rate regions highlight the role of the size of the subset at each receiver which induces a trade-off between their rates.

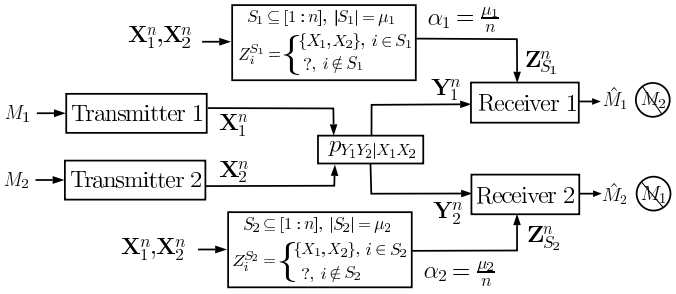

Fig. 1. The new interference channel with confidential messages model.

We further focus on a special case of the new BC-CM, with one receiver's noisy observations are degraded versions of the other receiver's noisy observations, and only the degraded receiver is provided with a subset of noiseless observations. In the achievable rate region for this case, the receiver with the degraded noisy observations achieves a positive secrecy rate after a certain threshold on his noiseless observations, i.e., the weaker receiver is aided to the point of achieving a positive rate by the symbols he chooses to tap.

Notation: p_X^U denotes a uniform distribution over X. We use $[1:n] \triangleq \{1, \cdots, n\}$. $A_S \triangleq \{A_i\}_{i \in S}$, $S \subseteq \mathbb{N}$. $\mathbb{1}_{\mathcal{A}}$ denotes the indicator function. $\mathbb{V}(p_X, q_X)$, $\mathbb{D}(p_X||q_X)$ denote the total variation distance and K-L divergence between p_X and q_X.

II. Channel Models

A. Interference Channel with Confidential Messages

Consider the model in Fig. 1. The channel $p_{Y_1Y_2|X_1X_2}$ is a discrete memoryless channel (DMC) with two finite input alphabets $\mathcal{X}_1, \mathcal{X}_2$, and two finite output alphabets $\mathcal{Y}_1, \mathcal{Y}_2$. Transmitter $j, j = 1, 2$, wishes to send a message M_j reliably

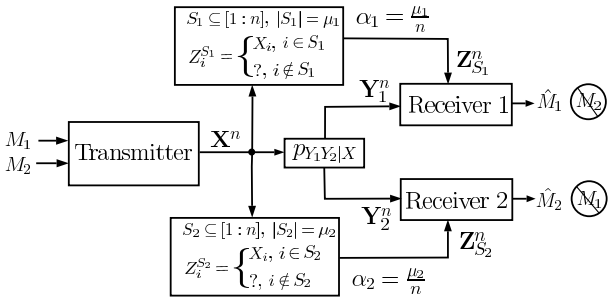

Fig. 2. The new broadcast channel with confidential messages model.

to receiver j, while keeping M_j secret from the other user's receiver. $M_j, j = 1, 2$, are independent and uniform over $[1 : 2^{nR_j}]$. Transmitter j maps M_j into $\mathbf{X}_j^n \triangleq [X_{j,1}, \cdots, X_{j,n}] \in \mathcal{X}_j^n$ using a stochastic encoder. Receiver j, $j = 1, 2$, besides observing $\mathbf{Y}_j^n \triangleq [Y_{j,1}, \cdots, Y_{j,n}] \in \mathcal{Y}_j^n$, chooses the subset $S_j \in \mathcal{S}_j$, $\mathcal{S}_j \triangleq \{S_j \subseteq [1 : n] : |S_j| = \mu_j, \alpha_j = \frac{\mu_j}{n}\}$, and observes $\mathbf{Z}_{S_j}^n = [Z_1^{S_j}, \cdots, Z_n^{S_j}] \in \mathcal{Z}^n$, $\mathcal{Z} \triangleq \{\mathcal{X}_1 \times \mathcal{X}_2\} \cup \{?\}$,

$$Z_i^{S_j} = \{X_{1,i}, X_{2,i}\} \text{ if } i \in S_j, \text{ and } Z_i^{S_j} = ?, \text{ otherwise.} \quad (1)$$

Receiver j, upon observing $\mathbf{Y}_j^n, \mathbf{Z}_{S_j}^n$, outputs the estimate $\hat{M}_j$.

An $(n, 2^{nR_1}, 2^{nR_2})$ code $\mathcal{C}_n \triangleq \{\mathcal{C}_{1,n}, \mathcal{C}_{2,n}\}$ consists of two message sets, two stochastic encoders $P_{\mathbf{X}_j|M_j\mathcal{C}_{j,n}}$, $j = 1, 2$, and two decoders. (R_1, R_2) is an achievable strong secrecy rate pair if there is a sequence of codes $\{\mathcal{C}_n\}_{n\geq 1}$ such that

$$\lim_{n\to\infty} \mathbb{P}((\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)|\mathcal{C}_n) = 0, \quad (2)$$

$$\lim_{n\to\infty} \max_{S_2\in\mathcal{S}_2} I(M_1; \mathbf{Y}_2^n, \mathbf{Z}_{S_2}^n|\mathcal{C}_n) = 0 \quad (3)$$

$$\lim_{n\to\infty} \max_{S_1\in\mathcal{S}_1} I(M_2; \mathbf{Y}_1^n, \mathbf{Z}_{S_1}^n|\mathcal{C}_n) = 0. \quad (4)$$

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

B. Broadcast Channel with Confidential Messages

This model is described in Fig. 2. The channel $p_{Y_1Y_2|X}$ is a DMC with a finite input alphabet $\mathcal{X}$ and two finite output alphabets $\mathcal{Y}_1, \mathcal{Y}_2$. The transmitter sends a message M_j to receiver j, $j = 1, 2$, while keeping M_j secret from the other receiver. $M_j, j = 1, 2$, are independent and uniform over $[1 : 2^{nR_j}]$. The transmitter maps M_1, M_2 into the codeword $\mathbf{X}^n \in \mathcal{X}^n$ using a stochastic encoder. As in Section II-A, receiver j, $j = 1, 2$, (i) chooses the subset $S_j \in \mathcal{S}_j$, (ii) observes $\mathbf{Y}_j^n \in \mathcal{Y}_j^n$ and $\mathbf{Z}_{S_j}^n = [Z_1^{S_j}, \cdots, Z_n^{S_j}] \in \mathcal{Z}^n$, where

$$Z_i^{S_j} = X_i, \text{ if } i \in S_j, \text{ and } Z_i^{S_j} = ?, \text{ otherwise,} \quad (5)$$

$\mathcal{Z} \triangleq \mathcal{X} \cup \{?\}$, and (iii) outputs the estimate $\hat{M}_j$.

An $(n, 2^{nR_1}, 2^{nR_2})$ code $\mathcal{C}_n$ consists of two message sets, one stochastic encoder $P_{\mathbf{X}|M_1M_2\mathcal{C}_n}$, and two decoders. Strong secrecy rate pair (R_1, R_2) is achievable if there is a sequence of codes $\{\mathcal{C}_n\}$ such that (2)-(4) hold.

III. Main Results

Theorem 1 For $\alpha_1, \alpha_2 \in [0, 1]$, an achievable strong secrecy rate region for the new IC-CM in Fig. 1 is given by the convex hull of all rate pairs (R_1, R_2) satisfying:

$$R_1 \leq \big[I(U_1; Y_1) + \alpha_1 I(U_1; X_1, X_2|Y_1) - I(U_1; Y_2|U_2) - \alpha_2 I(U_1; X_1, X_2|U_2, Y_2)\big]^+, \quad (6)$$

$$R_2 \leq \big[I(U_2; Y_2) + \alpha_2 I(U_2; X_1, X_2|Y_2) - I(U_2; Y_1|U_1) - \alpha_1 I(U_2; X_1, X_2|U_1, Y_1)\big]^+, \quad (7)$$

for some $p_{U_1U_2X_1X_2Y_1Y_2} = p_{U_1}p_{U_2}p_{X_1|U_1}p_{X_2|U_2}p_{Y_1Y_2|X_1X_2}$.

Remark 1 Setting $\alpha_1 = \alpha_2 = 0$ in (6), (7) yields the achievable secrecy rate region for the IC-CM in [7], [8]. By comparing (6), (7), to the region in [7], [8], we notice that the term $\alpha_j I(U_j; X_1, X_2|Y_j), j = 1, 2$, represents the rate gain for user j due to his noiseless observations, and the term $\alpha_i I(U_j; X_1, X_2|U_i, Y_i), i = 1, 2,\ i \neq j$, represents the secrecy penalty at user j due to the noiseless observations of user i.

Theorem 2 For $\alpha_1, \alpha_2 \in [0, 1]$, an achievable strong secrecy rate region for the new BC-CM in Fig. 2 is given by the convex hull of all rate pairs (R_1, R_2) satisfying:

$$R_1 \leq \big[I(U_1; Y_1) + \alpha_1 I(U_1; X|Y_1) - I(U_1; U_2) - I(U_1; Y_2|U_2) - \alpha_2 I(U_1; X|U_2, Y_2)\big]^+, \quad (8)$$

$$R_2 \leq \big[I(U_2; Y_2) + \alpha_2 I(U_2; X|Y_2) - I(U_1; U_2) - I(U_2; Y_1|U_1) - \alpha_1 I(U_2; X|U_1, Y_1)\big]^+, \quad (9)$$

for some $p_{U_1U_2XY_1Y_2} = p_{U_1U_2}p_{X|U_1U_2}p_{Y_1Y_2|X}$.

Remark 2 By setting $\alpha_1 = \alpha_2 = 0$ in (8), (9), we obtain the achievable secrecy rate region for the BC-CM in [7, Thm. 4].

For the new BC-CM model in Fig. 2, when $\alpha_1 = 0, \alpha_2 = \alpha$, and the channel $p_{Y_1Y_2|X}$ is degraded, i.e., $X - Y_1 - Y_2$ forms a Markov chain, we have the following achievable strong secrecy rate region, which follows from Theorem 2.

Corollary 1 For $\alpha \in [0, 1]$, an achievable strong secrecy rate region for the degraded BC-CM, with the degraded receiver is provided by αn noiseless transmitted symbols of his choice, is the convex hull of all rate pairs (R_1, R_2) satisfying:

$$R_1 \leq \big[I(U_1; Y_1|Y_2) - I(U_1; U_2|Y_2) - \alpha I(U_1; X|U_2, Y_2)\big]^+$$

$$R_2 \leq \big[\alpha I(U_2; X|Y_2) - I(U_1; U_2|Y_1) - I(U_2; Y_1|Y_2)\big]^+,$$

for some $p_{U_1U_2XY_1Y_2} = p_{U_1U_2}p_{X|U_1U_2}p_{Y_1|X}p_{Y_2|Y_1}$.

Remark 3 Unlike for the BC-CM in [7], where receiver 2 has zero rate, $R_2 = 0$, when Y_2 is degraded from Y_1, for the new BC-CM in Fig. 2 with $\alpha_1 = 0, \alpha_2 = \alpha$, and Y_2 is degraded with respect to Y_1, Corollary 1 implies that receiver 2 has a positive rate after a certain threshold on α. For example, by setting $U_1 = \text{const.}$, $U_2 = X$, and for $H(X|Y_2) \neq 0$, we have

$$R_2 > 0, \quad \text{if} \quad \frac{H(X|Y_2) - H(X|Y_1)}{H(X|Y_2)} < \alpha \leq 1.$$

In general, for the model in Corollary 1, $R_2 > 0$ if there exist U_1, U_2 such that $U_1U_2 - X - Y_1 - Y_2$ is a Markov chain, and

$$\alpha I(U_2; X|Y_2) > I(U_2; Y_1|Y_2) + I(U_1; U_2|Y_1). \quad (10)$$

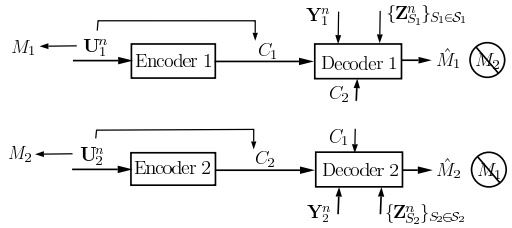

Fig. 3. Dual source model for the channel model in Fig. 2.

IV. Proofs for Theorems 1 and 2

We first prove Theorem 2. We adopt the achievability approach in [5], [6], [9]. In particular, we introduce an appropriate dual secret key agreement problem in the source model, which introduces a set of random variables that is similar to the variables introduced by the original channel model with an added common randomness available at all terminals. We then solve for encoders and decoders in the dual source model, and convert the solution to the original channel model by applying the reverse encoders and decoders to the channel model and using a set of probability distribution approximation arguments. We finally remove the common randomness from the original model by conditioning on a certain instance of that randomness, without disturbing the desired properties.

We use $A_{1:2}=(A_1,A_2)$ for random variables (vectors) and their realizations. Fix the distribution $p_{U_{1:2}X}=p_{U_{1:2}}p_{X|U_{1:2}}$. Let $p_{Y_{1:2}|U_{1:2}}$ be the distribution resulting from concatenating the two DMCs $p_{X|U_{1:2}}$, $p_{Y_{1:2}|X}$, i.e., $p(y_{1:2}|u_{1:2})=\sum_x p(y_{1:2}|x)p(x|u_{1:2})$, where $p_{Y_{1:2}|X}$ is the transition probability in Fig. 2. Next, we define the following two protocols and describe the joint distribution induced by each of them.

Protocol A: This protocol describes the dual secret key agreement problem in Fig. 3, where $\mathbf{U}_1^n,\mathbf{U}_2^n,\mathbf{Y}_1^n,\mathbf{Y}_2^n$ are i.i.d. sequences according to $p_{U_{1:2}}p_{Y_{1:2}|U_{1:2}}$. Note that the noisy observations at the source encoders, $\mathbf{U}_1,\mathbf{U}_2$, correspond to the correlated auxiliary variables utilized in Marton's coding to separately encode the messages M_1,M_2 [10, Chap. 8]. The source $\mathbf{U}_j$ is randomly and independently binned into the indices $M_j=\mathcal{B}_{1j}(\mathbf{U}_j)$, $C_j=\mathcal{B}_{2j}(\mathbf{U}_j)$, where $\mathcal{B}_{1j},\mathcal{B}_{2j}$ are independent and uniform over $[1:2^{n\tilde{R}_j}]$, $[1:2^{n\tilde{R}_j}], j=1,2$. Decoder j (i) observes $C_1,C_2,\mathbf{Y}_j$, (ii) chooses $S_j\in\mathcal{S}_j$ and observes $\mathbf{Z}_{S_j}$ as in (5), and (iii) outputs the estimates $\hat{\mathbf{U}}_j,\hat{M}_j$. The message C_j is public to decoder i, while the key M_j should be kept secret from decoder i, $i,j=1,2,\ i\neq j$. The realization of $S_j, j=1,2$, is unknown to the other decoder. The induced joint distribution for protocol A is

$$\begin{aligned}\tilde{P}_{M_{1:2}C_{1:2}\mathbf{U}_{1:2}\mathbf{Y}_1\mathbf{Z}_{S_1}\mathbf{Y}_2\mathbf{Z}_{S_2}\hat{\mathbf{U}}_{1:2}} &= p_{\mathbf{U}_{1:2}\mathbf{Y}_1\mathbf{Z}_{S_1}\mathbf{Y}_2\mathbf{Z}_{S_2}}\times\\ &\tilde{P}_{\hat{\mathbf{U}}_1|\mathbf{Y}_1\mathbf{Z}_{S_1}C_1}\tilde{P}_{\hat{\mathbf{U}}_2|\mathbf{Y}_2\mathbf{Z}_{S_2}C_2}\mathbb{1}_{\{\mathcal{B}_{1j}(\mathbf{U}_j)=M_j,\mathcal{B}_{2j}(\mathbf{U}_j)=C_j,j=1,2,\}}\\ &=\tilde{P}_{M_{1:2}C_{1:2}}\tilde{P}_{\mathbf{U}_{1:2}|M_{1:2}C_{1:2}}\ p_{\mathbf{Y}_1\mathbf{Z}_{S_1}\mathbf{Y}_2\mathbf{Z}_{S_2}|\mathbf{U}_{1:2}}\\ &\qquad\times\tilde{P}_{\hat{\mathbf{U}}_1|\mathbf{Y}_1\mathbf{Z}_{S_1}C_1}\tilde{P}_{\hat{\mathbf{U}}_2|\mathbf{Y}_2\mathbf{Z}_SC_2}. \quad (11)\end{aligned}$$

Protocol B: This protocol describes the channel model in Fig. 2 with assumed common randomness $C_j, j=1,2$, uniformly distributed over $[1:2^{n\tilde{R}_j}]$, independent from all other variables, and available to all terminals. We utilize $\tilde{P}_{\mathbf{U}_{1:2}|M_{1:2}C_{1:2}}$ and $\tilde{P}_{\hat{\mathbf{U}}_1|\mathbf{Y}_1\mathbf{Z}_{S_1}C_1}$, $\tilde{P}_{\hat{\mathbf{U}}_2|\mathbf{Y}_2\mathbf{Z}_{S_2}C_2}$ in (11) as the encoder and decoders for this protocol. The induced joint distribution for protocol B is given by

$$\begin{aligned}P_{M_{1:2}C_{1:2}\mathbf{U}_{1:2}\mathbf{Y}_1\mathbf{Z}_{S_1}\mathbf{Y}_2\mathbf{Z}_{S_2}\hat{\mathbf{U}}_{1:2}} &= p^U_{M_{1:2}}p^U_{C_{1:2}}\tilde{P}_{\mathbf{U}_{1:2}|M_{1:2}C_{1:2}}\\ &\times p_{\mathbf{Y}_1\mathbf{Z}_{S_1}\mathbf{Y}_2\mathbf{Z}_{S_2}|\mathbf{U}_{1:2}}\tilde{P}_{\hat{\mathbf{U}}_1|\mathbf{Y}_1\mathbf{Z}_{S_1}C_1}\tilde{P}_{\hat{\mathbf{U}}_2|\mathbf{Y}_2\mathbf{Z}_{S_2}C_2}. \quad (12)\end{aligned}$$

In the channel model in protocol B, although the common randomness C_i is available at receiver j, $i,j=1,2$, $i\neq j$, it is not utilized for decoding M_j. The encoders in the source model are chosen accordingly, c.f. (11). The $\hat{M}$ variables are deterministic functions of the $\hat{\mathbf{U}}$ random variables, and we will introduce them later to the joint distributions of the two protocols after fixing the binning functions. Before continuing with the proof, we state the following two lemmas.

Lemma 1 provides the tool we utilize to establish closeness of joint distributions from the two protocols, in total variation distance sense, in order to convert the desired properties from the dual source model in protocol A to the original channel model in protocol B. The *exponential* convergence rate provided by the lemma is utilized, along with the Borel-Cantelli lemma and the union bound, to convert secrecy (independence) conditions, measured in K-L divergence, from the source to the channel model. Lemma 1 generalizes [6, Lemma 1] to the case of two *correlated* sources. The proof for the general case of multiple (more than two) correlated sources is given in [11].

Lemma 1 Let $X_j\in\mathcal{X}_j, j=1,2$, be two *correlated* sources according to $p_{X_{1:2}}$. Source X_j is randomly and independently binned into the indices $M_j=\mathcal{B}_{1j}(X_j), C_j=\mathcal{B}_{2j}(X_j)$, where $\mathcal{B}_{1j},\mathcal{B}_{2j}$ are independent and uniform over $[1:M_j],[1:\tilde{C}_j]$. Let $\mathcal{B}\triangleq\{\mathcal{B}_{1j}(x_j),\mathcal{B}_{2j}(x_j)\}_{x_j\in\mathcal{X}_j,j=1,2}$. For $\gamma_1,\gamma_2,\gamma_{1,2}>0$, let $\mathcal{D}\triangleq\{x_{1:2}\in\mathcal{X}_1\times\mathcal{X}_2: x_j\in\mathcal{D}_{\gamma_j}, x_{1:2}\in\mathcal{D}_{\gamma_{1,2}}, j=1,2\}$,

$$\begin{aligned}\mathcal{D}_{\gamma_j}&\triangleq\{x_j\in\mathcal{X}_j: -\log p_{X_j}(x_j)>\gamma_j\},\quad j=1,2,\\ \mathcal{D}_{\gamma_{1,2}}&\triangleq\{x_{1:2}\in\mathcal{X}_1\times\mathcal{X}_2: -\log p_{X_{1:2}}(x_{1:2})>\gamma_{1,2}\}.\end{aligned}$$

Let P be the induced distribution over $M_{1:2},C_{1:2}$. We have,

$$\begin{aligned}&\mathbb{E}_{\mathcal{B}}(\mathbb{V}(P_{M_{1:2}C_{1:2}},p^U_{M_{1:2}}p^U_{C_{1:2}}))\le\mathbb{P}_{p_{X_{1:2}}}(X_{1:2}\notin\mathcal{D})+\\ &\frac{1}{2}\sum_{j=1,2}\left(\tilde{M}_j\tilde{C}_j2^{-\gamma_j}\right)^{1/2}+\frac{1}{2}\left(\tilde{M}_1\tilde{M}_2\tilde{C}_1\tilde{C}_2 2^{-\gamma_{1,2}}\right)^{1/2}. \quad (13)\end{aligned}$$

Next, we state the following lemma by which we establish secrecy conditions for the source model. The convergence rate provided by the lemma is *doubly-exponential* which is utilized, along with the union bound, to ensure secrecy against the exponentially many choices of the subset S_j at decoder j.

Lemma 2 *[6, Lemma 2]:* Let $X_j\in\mathcal{X}_j$, $j=1,2$, be two correlated sources, both correlated with the source $\{Z_S\}\triangleq\{\mathcal{Z},p_{Z_S}\}, S\in\mathcal{S}$, according to $p_{X_{1:2}Z_S}$. $|\mathcal{X}_1|,|\mathcal{X}_2|,|\mathcal{Z}|,|\mathcal{S}|<\infty$. X_j is randomly binned into M_j,C_j as in Lemma 1. For $\gamma_j,\gamma_{i,j}>0, j,i=1,2, i\neq j$, and any $S\in\mathcal{S}$, define

$$\begin{aligned}&\mathcal{D}^S_j\triangleq\left\{(x_{1:2},z)\in\mathcal{X}_1\times\mathcal{X}_2\times\mathcal{Z}: (x_j,z)\in\mathcal{D}^S_{\gamma_j},(x_{1:2},z)\right.\\ &\left.\in\mathcal{D}^S_{\gamma_{i,j}}\right\},\ \text{where } \mathcal{D}^S_{\gamma_j}\triangleq\left\{(x_j,z): -\log p_{X_j|Z_S}(x_j|z)>\gamma_j\right\},\\ &\text{and } \mathcal{D}^S_{\gamma_{i,j}}\triangleq\left\{(x_{1:2},z): -\log p_{X_i|X_jZ_S}(x_i|x_j,z)>\gamma_{i,j}\right\}.\end{aligned}$$

If there exists $\delta \in (0, \frac{1}{2})$ such that for $j = 1, 2$, and all $S \in \mathcal{S}$, $\mathbb{P}_{p_{X_{1:2}Z_S}}\big((X_{1:2}, Z_S) \in \mathcal{D}_j^S\big) \geq 1 - \delta^2$, then, $\forall \epsilon \in [0, 1]$,

$$\mathbb{P}_{\mathcal{B}}\Big(\max_{S\in\mathcal{S}} \mathbb{D}(P_{M_{1:2}C_{1:2}Z_S}||p^U_{M_{1:2}}p^U_{C_{1:2}}p_{Z_S}) \geq 2\tilde{\epsilon}\Big) \leq$$
$$|\mathcal{S}||\mathcal{Z}| \min_{j,i=1,2,i\neq j}\Big\{e^{\left(\frac{-\epsilon^2(1-\delta)2^{\gamma_j}}{3\tilde{M}_j\tilde{C}_j}\right)} + e^{\left(\frac{-\epsilon^2(1-\delta)2^{\gamma_{i,j}}}{3\tilde{M}_i\tilde{C}_i}\right)}\Big\}, \quad (14)$$

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

We divide the remainder of the proof into the following steps:

A. Closeness of joint induced distributions

In Lemma 1, set $X_1 = \mathbf{U}_1, X_2 = \mathbf{U}_2, \tilde{M}_1 = 2^{nR_1}, \tilde{C}_1 = 2^{n\tilde{R}_1}, \tilde{M}_2 = 1, \tilde{C}_2 = 2^{n\tilde{R}_2}$, where $\mathbf{U}_{1:2}$ are defined as in protocol A. For $\epsilon' > 0$, by setting $\gamma_j = n(1-\epsilon')H(U_j), j = 1, 2, \gamma_{1,2} = n(1-\epsilon')H(U_{1:2})$, and using Hoeffding's inequality [5, Lemma 5], we have $\mathbb{P}_{p_{\mathbf{U}_{1:2}}}(\mathbf{U}_{1:2} \notin \mathcal{D}) \leq \exp(-\beta_1' n)$, where $\beta_1' > 0$. By substituting the choices for $\tilde{M}_j, \tilde{C}_j, \gamma_j, j = 1, 2$, and $\gamma_{1,2}$ in (13), there exists $\beta_1 > 0$ such that

$$\mathbb{E}_{\mathcal{B}}(\mathbb{V}(\tilde{P}_{M_1C_{1:2}}, p^U_{M_1}p^U_{C_{1:2}})) \leq \exp(-\beta_1 n), \quad (15)$$

as long as, $R_1 + \tilde{R}_1 \leq (1-\epsilon')H(U_1)$, $\tilde{R}_2 \leq (1-\epsilon')H(U_2)$

$$R_1 + \tilde{R}_1 + \tilde{R}_2 \leq (1-\epsilon')H(U_1U_2). \quad (16)$$

Similarly, by setting $X_1 = \mathbf{U}_1, X_2 = \mathbf{U}_2, \tilde{M}_1 = 1, \tilde{C}_1 = 2^{n\tilde{R}_1}, \tilde{M}_2 = 2^{nR_2}, \tilde{C}_2 = 2^{n\tilde{R}_2}$ in Lemma 1, $\exists \beta_2 > 0$ s.t.

$$\mathbb{E}_{\mathcal{B}}(\mathbb{V}(\tilde{P}_{M_2C_{1:2}}, p^U_{M_2}p^U_{C_{1:2}})) \leq \exp(-\beta_2 n), \quad (17)$$

as long as, $\tilde{R}_1 \leq (1-\epsilon')H(U_1)$, $R_2 + \tilde{R}_2 \leq (1-\epsilon')H(U_2)$

$$\tilde{R}_1 + R_2 + \tilde{R}_2 \leq (1-\epsilon')H(U_1U_2). \quad (18)$$

Using (11), (12), (15) and (17), we have, for $j = 1, 2$, $S_j \in \mathcal{S}_j$,

$$\mathbb{E}_{\mathcal{B}}\mathbb{V}(\tilde{P}_{M_jC_{1:2}\mathbf{U}_j\mathbf{Y}_j\mathbf{Z}_{S_j}\hat{\mathbf{U}}_j}, P_{M_jC_{1:2}\mathbf{U}_j\mathbf{Y}_j\mathbf{Z}_{S_j}\hat{\mathbf{U}}_j}) \leq e^{-\beta_j n}.$$

Also, by the Borel-Cantelli lemma and Markov inequality, it follows from (15) and (17) that, for $j = 1, 2$,

$$\lim_{n\to\infty} \mathbb{P}_{\mathcal{B}}\big(\mathbb{V}(\tilde{P}_{M_jC_{1:2}}, p^U_{M_j}p^U_{C_{1:2}}) > 0\big) = 0. \quad (19)$$

B. Reliable decoding at source decoder j

In protocol A, for reliable communication of the source $\mathbf{U}_j$, decoder j employs Slepian-Wolf source decoder. Since $\mathbf{U}_j$ is i.i.d. and $p_{Y_j|U_{1:2}}$ is a DMC, then, for any $S_j \in \mathcal{S}_j$, $j = 1, 2$,

$$\begin{aligned} H(\mathbf{U}_j|\mathbf{Y}_j\mathbf{Z}_{S_j}) &= H(\mathbf{U}_{j,S_j}, \mathbf{U}_{j,S_j^c}|\mathbf{Y}_{j,S_j}, \mathbf{Y}_{j,S_j^c}, \mathbf{X}_{S_j}) \\ &= H(\mathbf{U}_{j,S_j}|\mathbf{X}_{S_j}, \mathbf{Y}_{j,S_j}) + H(\mathbf{U}_{j,S_j^c}|\mathbf{Y}_{j,S_j^c}) \\ &= \mu_j H(U_j|X) + (n-\mu_j)H(U_j|Y_j), \end{aligned} \quad (20)$$

where (20) follows since $U_j - X - Y_j$ forms a Markov chain. Using [9, Lemma 1], which is a variation on the Slepian-Wolf source coding theorem [10], for $j = 1, 2$, and any $S_j \in \mathcal{S}_j$,

$$\lim_{n\to\infty} \mathbb{E}_{\mathcal{B}}\big(\mathbb{V}(\tilde{P}_{M_jC_{1:2}\mathbf{U}_j\mathbf{Y}_j\mathbf{Z}_{S_j}\hat{\mathbf{U}}_j}, \tilde{P}_{M_jC_{1:2}\mathbf{U}_j\mathbf{Y}_j\mathbf{Z}_{S_j}}\mathbb{1}_{\{\hat{\mathbf{U}}_j=\mathbf{U}_j\}})\big) = 0, \quad (21)$$

as long as $\tilde{R}_j \geq \alpha_j H(U_j|X) + (1-\alpha_j)H(U_j|Y_j)$. (22)

C. Secrecy against source decoder j

Set $X_1 = \mathbf{U}_1, X_2 = \mathbf{U}_2, \tilde{M}_1 = 2^{nR_1}, \tilde{C}_1 = 2^{n\tilde{R}_1}, \tilde{M}_2 = 1, \tilde{C}_2 = 2^{n\tilde{R}_2}, \mathcal{S} = \mathcal{S}_2, Z_S = \mathbf{Y}_2\mathbf{Z}_{S_2}$ in Lemma 2; $\mathbf{U}_{1:2}$, $\mathbf{Y}_2$, $\mathcal{S}_2$, $\mathbf{Z}_{S_2}$ are as in protocol A. For $\epsilon'' > 0, j = 1, 2$, by choosing

$$\begin{aligned} \gamma_{1,2} &= (1-\epsilon'')[\mu_2 H(U_1|U_2X) + (n-\mu_2)H(U_1|U_2Y_2)] \\ \gamma_{2,1} &= (1-\epsilon'')[\mu_2 H(U_2|U_1X) + (n-\mu_2)H(U_2|U_1Y_2)], \\ \gamma_j &= (1-\epsilon'')[\mu_2 H(U_j|X) + (n-\mu_2)H(U_j|Y_2)], \end{aligned} \quad (23)$$

using Hoeffding's inequality, $\exists \tilde{\beta} > 0$ s.t. $\forall S_2 \in \mathcal{S}_2$, $j = 1, 2$,

$$\mathbb{P}_{p_{\mathbf{U}_{1:2}\mathbf{Y}_2\mathbf{Z}_{S_2}}}\big((\mathbf{U}_{1:2}, \mathbf{Y}_2\mathbf{Z}_{S_2}) \notin \mathcal{D}_j^{S_2}\big) \leq \exp(-\tilde{\beta}n) = \delta^2.$$

Note that $\lim_{n\to\infty} \delta^2 = 0$, and hence, for n sufficiently large, $\delta^2 \in (0, \frac{1}{4})$. Thus, the conditions of Lemma 2 are satisfied.

Substituting the choices for $\tilde{M}_1, \tilde{M}_2, \tilde{C}_1, \tilde{C}_2, \gamma_2, \gamma_{1,2}$, and $|\mathcal{S}_2||\mathcal{Z}^n| \leq (2(|\mathcal{X}|+1)|\mathcal{Y}_2|)^n$ in (14), we have, for all $\epsilon, \epsilon_1 > 0$, $\tilde{\epsilon} = \epsilon + \epsilon_1$, there exists $n^* \in \mathbb{N}$ and $\kappa_\epsilon, \tilde{\kappa} > 0$ s.t. $\forall n \geq n^*$,

$$\begin{aligned} &\mathbb{P}_{\mathcal{B}}\big(\max_{S_2\in\mathcal{S}_2} \mathbb{D}(\tilde{P}_{M_1C_{1:2}\mathbf{Y}_2\mathbf{Z}_{S_2}}||p^U_{M_1}p^U_{C_{1:2}}p_{\mathbf{Y}_2\mathbf{Z}_{S_2}}) \geq 2\tilde{\epsilon}\big) \\ &\qquad \leq \exp\big(-\kappa_\epsilon e^{\tilde{\kappa}n}\big), \qquad \text{as long as} \end{aligned} \quad (24)$$

$$R_1 + \tilde{R}_1 \leq (1-\epsilon'')[\alpha_2 H(U_1|U_2X) + (1-\alpha_2)H(U_1|U_2Y_2)]$$
$$\tilde{R}_2 \leq (1-\epsilon'')[\alpha_2 H(U_2|X) + (1-\alpha_2)H(U_2|Y_2)]. \quad (25)$$

By the Borel-Cantelli lemma, it follows from (24) that

$$\lim_{n\to\infty} \mathbb{P}_{\mathcal{B}}\big(\max_{S_2\in\mathcal{S}_2} \mathbb{D}(\tilde{P}_{M_1C_{1:2}\mathbf{Y}_2\mathbf{Z}_{S_2}}||p^U_{M_1}p^U_{C_{1:2}}p_{\mathbf{Y}_2\mathbf{Z}_{S_2}}) > 0\big) = 0 \quad (26)$$

Similarly, setting $X_1 = \mathbf{U}_1$, $X_2 = \mathbf{U}_2$, $\tilde{M}_1 = 1$, $\tilde{C}_1 = 2^{n\tilde{R}_1}$, $\tilde{M}_2 = 2^{nR_2}$, $\tilde{C}_2 = 2^{n\tilde{R}_2}$, $\mathcal{S} = \mathcal{S}_1$, $Z_S = \mathbf{Y}_1\mathbf{Z}_{S_1}$ in Lemma 2 and using the choices for $\gamma_1, \gamma_2, \gamma_{1,2}, \gamma_{2,1}$ in (23), but with replacing μ_2 and Y_2 by μ_1 and Y_1, gives

$$\lim_{n\to\infty} \mathbb{P}_{\mathcal{B}}\big(\max_{S_1\in\mathcal{S}_1} \mathbb{D}(\tilde{P}_{M_2C_{1:2}\mathbf{Y}_1\mathbf{Z}_{S_1}}||p^U_{M_2}p^U_{C_{1:2}}p_{\mathbf{Y}_1\mathbf{Z}_{S_1}}) > 0\big) = 0 \quad (27)$$

$$\begin{aligned} \text{if} \quad & R_2 + \tilde{R}_2 \leq \alpha_1 H(U_2|U_1X) + (1-\alpha_1)H(U_2|U_1Y_1) \\ & \tilde{R}_1 \leq \alpha_1 H(U_1|X) + (1-\alpha_1)H(U_1|Y_1). \end{aligned} \quad (28)$$

Note that we have considered two problems, where in each problem, one source encoder is communicating his key reliably to the corresponding decoder and securely from the other user's decoder, c.f. (21), (26), (27). In each of these two problems, the public messages $C_{1:2}$ are required to be independent from M_j and $\mathbf{Y}_j, \mathbf{Z}_{S_j}$, c.f. (26), (27). The reason is that, after converting these conditions to the channel model in protocol B, we need to eliminate the common randomness $C_{1:2}$ from the model by conditioning on a certain instance of it while preserving the uniformity of the message $M_j, j = 1, 2$, and its independence from the other receiver's observations.

D. Converting reliability and secrecy properties to protocol B

First, for the reliability conditions, using the triangle inequality, it follows from (15), (17), and (21), that, for $j = 1, 2$,

$$\lim_{n\to\infty} \mathbb{E}_{\mathcal{B}}\big(\mathbb{V}(P_{M_jC_{1:2}\mathbf{U}_j\mathbf{Y}_j\mathbf{Z}_{S_j}\hat{\mathbf{U}}_j}, P_{M_jC_{1:2}\mathbf{U}_j\mathbf{Y}_j\mathbf{Z}_{S_j}}\mathbb{1}_{\{\hat{\mathbf{U}}_j=\mathbf{U}_j\}})\big) = 0. \quad (29)$$

For the secrecy conditions, by the union bound, (19), (26),

$$\lim_{n\to\infty}\mathbb{P}_{\mathcal{B}}\big(\max_{S_2\in\mathcal{S}_2}\mathbb{D}(P_{M_1C_{1:2}\mathbf{Y}_2\mathbf{Z}_{S_2}}||p^U_{M_1}p^U_{C_{1:2}}p_{\mathbf{Y}_2\mathbf{Z}_{S_2}})>0\big)$$
$$\le\lim_{n\to\infty}\mathbb{P}_{\mathcal{B}}\big(\max_{S_2\in\mathcal{S}_2}\mathbb{D}(\tilde{P}_{M_1C_{1:2}\mathbf{Y}_2\mathbf{Z}_{S_2}}||p^U_{M_1}p^U_{C_{1:2}}p_{\mathbf{Y}_2\mathbf{Z}_{S_2}})>0\big)$$
$$+\lim_{n\to\infty}\mathbb{P}_{\mathcal{B}}\big(\mathbb{V}(\tilde{P}_{M_1C_{1:2}},p^U_{M_1}p^U_{C_{1:2}})>0\big)=0. \quad (30)$$

Similarly, using the union bound, (19) and (27), we have,

$$\lim_{n\to\infty}\mathbb{P}_{\mathcal{B}}\big(\max_{S_1\in\mathcal{S}_1}\mathbb{D}(P_{M_2C_{1:2}\mathbf{Y}_1\mathbf{Z}_{S_1}}||p^U_{M_2}p^U_{C_{1:2}}p_{\mathbf{Y}_1\mathbf{Z}_{S_1}})>0\big)=0. \quad (31)$$

Note that the reliability and secrecy conditions for the original channel model in protocol B, (29)-(31), are averaged over the random binning of the dual source model in protocol A, where this binning determines the encoders and decoders for the dual source model and hence the encoders and decoders for the original channel model as well, c.f., (12). By applying the selection lemma [12, Lemma 2.2] to (29)-(31), there is a binning realization $\mathbf{b}^*$, with a corresponding joint distribution p^* for the original channel model in protocol B such that

$$\lim_{n\to\infty}\mathbb{V}\big(p^*_{M_jC_{1:2}\mathbf{U}_j\mathbf{Y}_j\mathbf{Z}_{S_j}\hat{\mathbf{U}}_j},\ p^*_{M_jC_{1:2}\mathbf{U}_j\mathbf{Y}_j\mathbf{Z}_{S_j}}\mathbb{1}_{\{\hat{\mathbf{U}}_j=\mathbf{U}_j\}}\big)=0,\quad j=1,2, \quad (32)$$

$$\text{and}\ \lim_{n\to\infty}\mathbb{1}_{\big\{\max_{S_2\in\mathcal{S}_2}\mathbb{D}(p^*_{M_1C_{1:2}\mathbf{Y}_2\mathbf{Z}_{S_2}}||p^U_{M_1}p^U_{C_{1:2}}p_{\mathbf{Y}_2\mathbf{Z}_{S_2}})>0\big\}}=0,$$

$$\lim_{n\to\infty}\mathbb{1}_{\big\{\max_{S_1\in\mathcal{S}_1}\mathbb{D}(p^*_{M_2C_{1:2}\mathbf{Y}_1\mathbf{Z}_{S_1}}||p^U_{M_2}p^U_{C_{1:2}}p_{\mathbf{Y}_1\mathbf{Z}_{S_1}})>0\big\}}=0, \quad (33)$$

where $M_j=b^*_{1j}(\mathbf{U}_j)$ and $C_j=b^*_{2j}(\mathbf{U}_j)$, $j=1,2$.

E. Eliminating the common randomness

By introducing the $\hat{M}$ variables to the distributions in (32) as deterministic functions of the $\hat{\mathbf{U}}$ variables, we have [5],

$$\lim_{n\to\infty}\mathbb{E}_{C_{1:2}}\big(\mathbb{P}_{p^*}(\hat{M}_j\neq M_j|C_{1:2})\big)=0,\quad j=1,2. \quad (34)$$

We also have, using the union bound and (33), that

$$\lim_{n\to\infty}\mathbb{P}_{C_{1:2}}\big(\max_{S_2\in\mathcal{S}_2}\mathbb{D}(p^*_{M_1\mathbf{Y}_2\mathbf{Z}_{S_2}|C_{1:2}}||p^U_{M_1}p^*_{\mathbf{Y}_2\mathbf{Z}_{S_2}|C_{1:2}})>0\big)$$
$$\le\lim_{n\to\infty}\mathbb{1}_{\big\{\max_{S_2\in\mathcal{S}_2}\mathbb{D}(p^*_{M_1C_{1:2}\mathbf{Y}_2\mathbf{Z}_{S_2}}||p^U_{M_1}p^U_{C_{1:2}}p_{\mathbf{Y}_2\mathbf{Z}_{S_2}})>0\big\}}$$
$$+\lim_{n\to\infty}\mathbb{P}\big(\max_{S_2\in\mathcal{S}_2}\mathbb{D}(p^*_{M_1\mathbf{Y}_2\mathbf{Z}_{S_2}|C_{1:2}}||p^U_{M_1}p^*_{\mathbf{Y}_2\mathbf{Z}_{S_2}|C_{1:2}})>0,$$
$$\text{and}\ \forall S_2,\ p^*_{M_1C_{1:2}\mathbf{Y}_2\mathbf{Z}_{S_2}}=p^U_{M_1}p^U_{C_{1:2}}p_{\mathbf{Y}_2\mathbf{Z}_{S_2}}\big)=0, \quad (35)$$

as the second probability in (35) is equal to zero. Similarly,

$$\lim_{n\to\infty}\mathbb{P}_{C_{1:2}}\big(\max_{S_1\in\mathcal{S}_1}\mathbb{D}(p^*_{M_2\mathbf{Y}_1\mathbf{Z}_{S_1}|C_{1:2}}||p^U_{M_2}p^*_{\mathbf{Y}_1\mathbf{Z}_{S_1}|C_{1:2}})>0\big)=0. \quad (36)$$

Applying the selection lemma to (34)-(36) results in the existence of $c^*_{1:2}$ such that the reliability and secrecy constraints in (2)-(4) are satisfied. We hence identify the encoder and decoders for the original model as $p(\mathbf{x}|\mathbf{u}_{1:2})\tilde{p}^*(\mathbf{u}_{1:2}|m_{1:2},c^*_{1:2})$ and $(\tilde{p}^*(\hat{\mathbf{u}}_j|\mathbf{y}_j,\mathbf{z},c^*_j),b^*_{1j}(\hat{\mathbf{u}}_j),j=1,2)$; $\tilde{p}^*$ is the induced distribution in protocol A that corresponds to the binning $\mathbf{b}^*$.

Finally, combining the rate conditions in (16), (18), (22), (25) and (28), while taking $\epsilon',\epsilon''\to\infty$, results in the rate region in (8)-(9). The convex hull follows by time sharing independent codes. This completes the proof for Theorem 2.

The proof for Theorem 1 follows similar steps as in the proof for Theorem 2. The difference is that the auxiliary variables U_1, U_2 are independent, where at the beginning in the proof, we fix the distribution $p_{U_{1:2}X_{1:2}}$ which factorizes as $p_{U_1}p_{U_2}p_{X_1|U_1}p_{X_2|U_2}$. Note that Lemmas 1, 2, hold for the case of independent sources as well.

V. Conclusion

In this paper, we have studied a new model for the two-user interference channel with confidential messages (IC-CM), where the receivers, besides their noisy observations, are provided with fixed-length subsets of their choice of noiseless observations for transmitted codeword symbols of the both users. We have also proposed a new broadcast channel with confidential messages (BC-CM) model, with each receiver is provided with a subset of his choice of noiseless observations for the transmitted codeword. We have derived achievable strong secrecy rate regions for the two models. For both models, the size of the subset at each receiver gives rise to a trade-off between the rates of the two receivers, which is demonstrated in the derived rate regions. We have also highlighted the special case of the new BC-CM, with one receiver's noisy observations are degraded with respect to the other receiver, and only this degraded receiver is provided with a subset of noiseless observations. The achievable rate region for this case shows that the receiver, with the degraded noisy observations, achieves a positive secrecy rate after a certain threshold on the ratio of his noiseless observations.

References

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

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

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

[4] 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.

[5] 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.

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

[7] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2493–2507, 2008.

[8] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. 55, no. 10, pp. 4529–4542, 2009.

[9] 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.

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

[11] M. Nafea and A. Yener, "A new broadcast wiretap channel model," *IEEE Int. Symp. Info. Theory, ISIT'17*, June 2017.

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