

Wireless Secrecy in Cellular Systems with Infrastructure–Aided Cooperation

Petar Popovski, *Member, IEEE* and Osvaldo Simeone, *Member, IEEE*

Abstract

In cellular systems, confidentiality of uplink transmission with respect to eavesdropping terminals can be ensured by creating intentional interference via scheduling of concurrent downlink transmissions. In this paper, this basic idea is explored from an information-theoretic standpoint by focusing on a two-cell scenario where the involved base stations are connected via a finite-capacity backbone link. A number of transmission strategies are considered that aim at improving uplink confidentiality under constraints on the downlink rate that acts as an interfering signal. The strategies differ mainly in the way the backbone link is exploited by the cooperating downlink- to the uplink-operated base stations. Achievable rates are derived for both the Gaussian (unfaded) and the fading cases, under different assumptions on the channel state information available at different nodes. Numerical results are also provided to corroborate the analysis. Extensions to scenarios with more than two cells are briefly discussed as well. Overall, the analysis reveals that a combination of scheduling and base station cooperation is a promising means to improve transmission confidentiality in cellular systems.

I. INTRODUCTION

The ability to ensure transmission confidentiality is becoming a crucial requirement of many wireless communications systems due to the increasing role of on-line transactions and new applications that exchange critical personal data. In information-theoretic terms, *perfect secrecy (or confidentiality)* implies the impossibility for a given eavesdropping terminal to harness any information about the transmitted message from its received signal [1]. This condition provides an even stronger guarantee than traditional cryptography, where secrecy relies on the computational limitations of the eavesdropper (also referred to as the *wiretapper*).

A. Information-Theoretic Secrecy

The concept of secure communications over noisy communication channels was defined in information-theoretic terms in [1] and later refined in [2]: therein, it is shown that it is potentially feasible to communicate with perfect secrecy to a legitimate receiver unless the wiretapper benefits from a "less noisy" channel from the source than the

Petar Popovski is with the Department of Electronic Systems, Aalborg University, Denmark and Oticon A/S, Smørum, Denmark, e-mail: petarp@es.aau.dk.

Osvaldo Simeone is with the Center for Wireless Communication and Signal Processing Research (CWCSRP) New Jersey Institute of Technology (NJIT), University Heights 07102 Newark, NJ, e-mail: osvaldo.simeone@njit.edu.

legitimate receiver. This result was confirmed by [3] which extended the results of [1] [2] from discrete-memoryless channels to Gaussian models, thus making an important step in the direction of fully accounting for the features of wireless networks. The results of [3] demonstrate that perfect secrecy requires the wiretapper to suffer from a worse signal-to-noise-ratio (SNR) than the intended receiver. These initial works lead to the fairly pessimistic conclusions that perfect secrecy via physical-layer (coding) techniques is rather demanding and ultimately hardly "practical".

Two more recent results have spurred a renewed interest in the field of information-theoretic secrecy. The first is due to Maurer [4] (and then [5]), who considered a more general model in which the two legitimate users and the wiretapper have access to correlated random variables (e.g., measurements from a noisy channel) and can communicate over a noiseless public channel. Maurer proves that by discussion over the public channel the two legitimate users can obtain a non-null shared key with perfect secrecy even when the wiretapper benefits from better channel conditions. The second class of results, of specific interest for this paper, stems from the observation that in *wireless networks*, due to time-varying fading, the situation naturally arises where the SNR at the wiretapper is (at least temporarily) worse than at the legitimate user. This idea was exploited in [19] [20] for a single-antenna point-to-point link in the presence of an eavesdropper and quasi-static or ergodic fading, respectively¹. Moreover, in wireless networks, interference can be judiciously generated so as to decrease the SNR (or more precisely SINR, signal-to-noise-plus-interference ratio) in given areas of interest [21]. In other words, fading and the superposition property of the wireless medium turn out to be potentially beneficial for secret communications, rendering, at least in principle, information-theoretic secrecy on wireless channel viable. The ideas and works recalled above have led to a number of extensions including multi-antenna (MIMO) links and/ or multi-user systems. A brief discussion of such previous works can be found in Appendix-A. This current paper can be seen as an application of the same basic principles in the context of cellular communications ².

B. Secure Communications in Cellular Systems

In this paper, we focus on secure communications for cellular systems, motivated by the fact that most of confidential transactions are expected to be conducted over such networks in the near future. Specifically, a novel basic approach to ensuring confidentiality is proposed that exploits uplink/ downlink scheduling of transmissions in adjacent cells and cooperation at the base station (BS) level. In so doing, we follow on the line of research opened by [16], where it was shown that cooperative transmission, beside being able to improve throughput or reliability (see, e. g., [15]), can also be instrumental in enhancing the confidentiality of transmission (for a basic relay network). BS cooperation is currently being widely investigated as a key enabler for high-data rate infrastructure networks (see, e.g., [18] [17]), and is made possible by the presence of high-capacity backbone links connecting the BSs.

¹With quasi-static fading channels the channel gains remain constant for the duration of a codeword, while in ergodic fading channels time-variability is such that a single codeword spans a large number of channel states. It is also noted that [20] assumes the presence of Channel State Information (CSI) at the transmitter, while this is not so for [19].

²Note that here we use the term cellular communications also for the WLAN-type systems in which an Access Point plays the role of the Base Station.

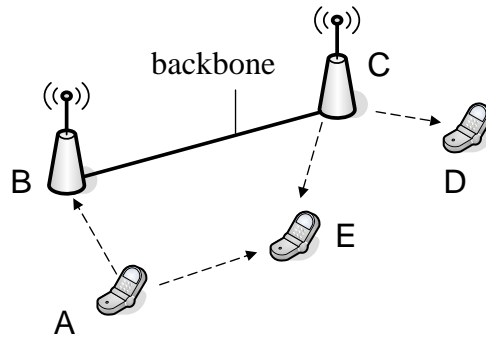


Fig. 1. Illustration of a system with cooperating base stations B and C, an uplink terminal A, an eavesdropping mobile station E and a downlink user D.

The main contribution of this work is to show that such technology can also bring significant gains in terms of secure communications.

The proposed techniques aim at securing uplink transmissions from terminals to a given BS. The basic idea is to schedule downlink BS transmissions at the same time as the concurrent uplink transmissions of interest, so as to create intentional interference on the possible eavesdroppers. Cooperation at the BS level is then used to convey information about the downlink transmission to the uplink-operated BS (uplink) over a finite-capacity backbone. This enables the uplink-operated BS to partially mitigate interference from the BS transmission. The approach is similar to [21] [22] [16] [23], where artificial noise jams the reception of the eavesdropper, while using techniques to avoid interference at the intended receiver. In [21] this interference mitigation is obtained by exploiting the structure and reciprocity of multi-antenna fading channels, while [22] [23] leverage a infinite-capacity backbone between receiving and jamming antennas. We propose several new schemes based on the above mentioned basic idea, each of them using a combined wireless/backbone transmission. The schemes and the corresponding achievable rates are investigated and compared via analysis and simulations.

II. SYSTEM MODEL AND BACKGROUND

In this section, we first introduce the scenario of interest and relevant quantities, and then investigate the reference case where no infrastructure is present to enable cooperation between the BSs.

A. Scenario

We focus on two adjacent cells served by single-antennas BSs as in Fig. 1, where the two BSs are connected by a high capacity, typically wired, backbone link. The BSs are termed B and C , respectively. Terminal A within the first cell has a message to deliver to B under constraints of confidentiality with respect to the activity of an eavesdropping terminal E . The eavesdropper is assumed to be within the transmission range of terminal A , as otherwise it would not pose any threat to the confidentiality of A 's message, but also of the adjacent BS C .

The main idea behind the considered transmission strategy is that the uplink transmission from A to B can be scheduled at the same time as the downlink transmission from C towards a given terminal D in its range. Hence, the transmission from C effectively acts as a jammer on the reception at E . Note this approach is not intended to secure the communication $C - D$. Also, notice that jamming is thereby accomplished without exploiting any additional system resource since it is obtained from a regular downlink transmission.

A few remarks on the virtues and limitations of the considered model are in order. First, we remark that, in the scenario at hand, the downlink transmission from B to A can be secured indirectly by letting terminal A communicate securely in uplink a one-time pad to B that B can use in the next downlink transmission. Therefore, our focus on the uplink transmission is not restrictive in this sense and may enable overall security in the system to be achieved. Moreover, the focus on a two-cell system is justified if one assumes that: (a) the wiretapper is not aware of the codebooks (i.e., modulation, coding) used in other surrounding cells: in this case, transmissions from other cells would have to be considered as Gaussian noise (see, e.g., [27]) and thus would be accounted for by our model; (b) no coordination via backhaul links is possible from B to other BSs. In the more complex case where such assumptions are violated, the analysis presented here provides the necessary tools for extensions, as we briefly discuss in Sec. VIII.

1) *System Model:* Formally, terminal A randomly selects a rate- R_A message W_A from the set $\{1, \dots, 2^{nR_A}\}$, and encodes it via a sequence of n complex channel inputs $\mathbf{X}_A = [X_{A,1} \cdots X_{A,n}] \in \mathbb{C}^n$ with normalized average power constraint $\mathbb{E}[|X_{A,i}|^2] = P_A$. Encoding takes place through a (possibly stochastic) mapping: $\mathbf{X}_A: \{1, \dots, 2^{nR_A}\} \rightarrow \mathbb{C}^n$ [1] [3]. Notice that vectors of n symbols are represented throughout the paper by bold letters. At the same time, BS C transmits a rate- R_C downlink message W_C , randomly selected from the set $\{1, \dots, 2^{nR_C}\}$, with an average power of P_C . The actual codebook used by C is assumed to be subject to design and thus depends on the specific cooperative strategy employed by BSs B and C . This will be specified for different proposed techniques in the following sections. The capacity of the backbone link is denoted by C_L and is measured in bit/symbol. We consider bandwidth that is normalized to 1 Hz, such that bit/symbol is equivalent to bit/second (bps). We assume full synchronization between the transmissions of A and C at the receiver of B . Finally, to account for a worst-case scenario, synchronization is also assumed at the receiver of eavesdropping terminal E , and the latter is endowed with information about the codebooks used by A and C .

The complex channel coefficient between any two nodes U and V is denoted by h_{UV} , while the i -th symbol transmitted by node U is denoted by $X_{U,i}$ ($U \in \{A, C\}$ and $V \in \{B, D, E\}$). The signal received by B and E , respectively, at the i -th symbol ($i = 1, \dots, n$) reads:

$$Y_{B,i} = h_{AB}X_{A,i} + h_{CB}X_{C,i} + N_{B,i} \quad (1)$$

$$Y_{E,i} = h_{AE}X_{A,i} + h_{CE}X_{C,i} + N_{E,i} \quad (2)$$

Each noise component $N_{V,i}$ is a complex Gaussian white noise with unit power, so that if the node U transmits with power P_U , the corresponding received signal-to-noise ratio (SNR) at the node V is:

$$\gamma_{UV} = P_U |h_{UV}|^2. \quad (3)$$

In the most of the paper (Sec. III-VI), we focus on Gaussian (unfaded) channels, where the channel gains (3) are fixed and deterministic. In practice, these rates can be achieved, for given channel realizations, when channel state information is known at the receiver side, and all the channel gains of interest ($h_{AB}, h_{CB}, h_{AE}, h_{CE}$) are known to terminal A , while the channel gains h_{CB} and h_{CD} are known to the downlink-operated BS C . Also, E knows its channels h_{AE}, h_{CE} towards the corresponding transmitters. In Sec. VII, the analysis will be extended to a fading scenario under different assumptions on the channel state information at the transmitters' side.

Finally, the BS B decodes through a mapping $g(\mathbf{Y}_B): \mathbb{C}^n \rightarrow \{1, \dots, 2^{nR_A}\}$. According to standard definitions [1] [3], a rate $R_A = R_{A,s}$ is said to be *achievable with perfect secrecy* with respect to eavesdropper E if, as the number of samples per coding block $n \rightarrow \infty$: (a) the decoding error at BS B vanishes:

$$P_e = P[g(\mathbf{Y}_B) \neq W_A] \rightarrow 0; \quad (4)$$

(b) the uncertainty (equivocation) Δ of eavesdropper E regarding A 's message, measured as the conditional entropy of W_A given the signal received by E normalized over the unconditional entropy, satisfies:

$$\Delta = \frac{H(W_A | \mathbf{Y}_E)}{H(W_A)} \rightarrow 1. \quad (5)$$

B. Some Useful Functions

To simplify the presentation of the results in this paper, it is useful to define the following two functions. The first function $\mathcal{C}(\gamma_{UV})$ is the standard capacity of a Gaussian single link with source U and receiver V , and SNR equal to γ_{UV} :

$$\mathcal{C}(\gamma_{UV}) = \log(1 + \gamma_{UV}). \quad (6)$$

The second function $S_{U_1V}(R_{U_2})$ pertains to the performance of a multiple-access channel (MAC) with two users U_1 and U_2 and receiver V . It measures the supremum of the achievable rates from U_1 to V for a given transmission rate R_{U_2} of U_2 . Notice that rate R_{U_2} is not restricted to be within the MAC capacity region, that is, it is not necessarily decodable by V . Given the SNRs γ_{U_1V} and γ_{U_2V} , the function is given by:

$$S_{U_1V}(R_{U_2}) = \begin{cases} \mathcal{C}(\gamma_{U_1V}) & \text{if } R_{U_2} \leq \mathcal{C}\left(\frac{\gamma_{U_2V}}{1+\gamma_{U_1V}}\right) \\ \mathcal{C}(\gamma_{U_1V} + \gamma_{U_2V}) - R_{U_2} & \text{if } \mathcal{C}\left(\frac{\gamma_{U_2V}}{1+\gamma_{U_1V}}\right) < R_{U_2} \leq \mathcal{C}(\gamma_{U_2V}) \\ \mathcal{C}\left(\frac{\gamma_{U_1V}}{1+\gamma_{U_2V}}\right) & \text{if } R_{U_2} > \mathcal{C}(\gamma_{U_2V}) \end{cases} . \quad (7)$$

C. Perfect Secrecy Without Backbone Link ($C_L = 0$)

Here, we briefly discuss the baseline scenario where no backbone link exists between BSs B and C ($C_L = 0$). In such a case, no cooperation via the backbone link is possible, and we assume that the BS C transmits with a standard Gaussian codebook $\mathbf{X}_C(W_C) = [X_{C,1}(W_C) \cdots X_{C,n}(W_C)] \in \mathbb{C}^n$, where variables $X_{C,i}$ are generated as complex Gaussian independent with zero mean and power P_C . As explained above, this codebook conveys information to a downlink user D . Given this set-up, it can be readily seen that the considered approach coincides

with the strategy considered in [16] under the name *Noise-Forwarding (NF)*. It was shown therein that the secrecy capacity can be found by considering the compound multiple access channel (MAC), with two receivers B and E and two transmitters A and C . In particular, for the Gaussian case of interest here, and using the function (7), the result of [16] (Theorem 3) can be restated as follows.

Proposition 1: If BS C transmits in downlink with rate R_C and there is no backbone link ($C_L = 0$), the rate $R_{A,s}(R_C)$ is achievable with perfect secrecy with respect to eavesdropper E ³:

$$R_{A,s}(R_C) = (S_{AB}(R_C) - S_{AE}(R_C))^+, \quad (8)$$

with $S_{AB}(R_C)$ and $S_{AE}(R_C)$ defined in (7).

From (8) it can be seen that an increase in the secrecy rate can be obtained by either increasing the achievable rate $S_{AB}(R_C)$ to the intended destination B or hampering reception of the eavesdropper (decreasing $S_{AE}(R_C)$).

III. UPPER BOUND ON THE SECRECY RATE

Here, we are interested in evaluating an upper bound to the achievable secrecy rates. To this end, we consider an enhanced system in which the BS B is informed by a genie about the signal $\mathbf{X}_C(W_C)$ transmitted by BS C . Since we assume here that the codebook of C is known at B , this corresponds to assuming that the backhaul capacity is $C_L \geq R_C$ so that message W_C can be sent over the backhaul. As a result, BS B can effectively cancel the interference signal $\mathbf{X}_C(W_C)$ from the received signal (1) and the rate achievable in this enhanced system upper bounds that of the original model. With such a complete interference cancelation at B , the equivalent received signal is:

$$Y_{B,i} = h_{AB}X_{A,i} + N_{B,i}. \quad (9)$$

This implies that for any R_C we have:

$$S_{AB}(R_C) = S_{AB}(0) = \mathcal{C}(\gamma_{AB}), \quad (10)$$

from which the following proposition easily follows.

Proposition 2: If BS C transmits in downlink with rate R_C the rate $R_{A,s}(R_C)$ achievable with perfect secrecy is upper bounded by

$$R_{A,s}(R_C) \leq (\mathcal{C}(\gamma_{AB}) - S_{AE}(R_C))^+ \quad (11)$$

with $S_{AE}(R_C)$ defined in (7). This upper bound is achievable if $C_L \geq R_C$.

Proof: Follows directly from Theorem 3 of [16] (see discussion in Sec. II-C).

The upper bound (11) is plotted in Fig. 2 along with the capacity of the direct link $\mathcal{C}(\gamma_{AB})$ and the maximum achievable rate at the eavesdropper $S_{AE}(R_C)$ for $\gamma_{AB} = 7$, $\gamma_{AE} = 15$, $\gamma_{CE} = 10$. A relevant quantity that can be observed from the figure is the rate $R_x = \mathcal{C}(\gamma_{AB}) - R_{A,s}$. This can be interpreted as the *rate loss* that terminal A must sacrifice to the aim of ‘‘confounding’’ the eavesdropper E and thus achieving rate $R_{A,s}$ with perfect secrecy.

³We define $(x)^+ = x$ if $x > 0$ and $(x)^+ = 0$ otherwise.

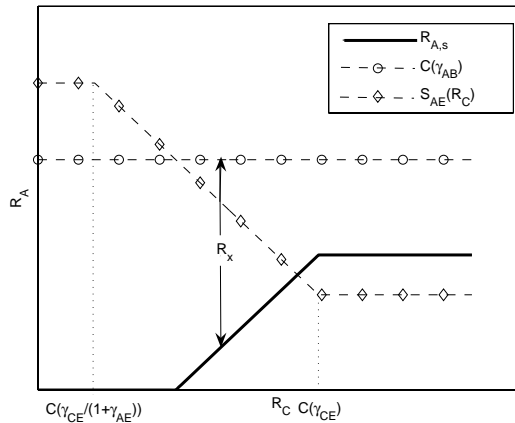


Fig. 2. Upper bound $R_{A,s}$ in Proposition 2. Here $R_x = \mathcal{C}(\gamma_{AB}) - R_{A,s}$ is the amount of information spent by A to “confound” the eavesdropper E in order to achieve a rate $R_{A,s}$ with perfect secrecy.

For this particular example, when $R_C = 0$, the single-user link $A - E$ is less noisy than the link $A - B$ and therefore the secrecy capacity is zero. As the downlink rate R_C increases, while the achievable rate $\mathcal{C}(\gamma_{AB})$ on the link $A - B$ is clearly unaffected (see (9)), the rate decodable by the eavesdropper $S_{AE}(R_C)$ decreases (for R_C large enough), and thus a positive secrecy rate is obtained as soon as $S_{AE}(R_C) < \mathcal{C}(\gamma_{AB})$. In particular, the secrecy rate $R_{A,s}$ increases linearly with R_C until it reaches the maximum value $\left(\mathcal{C}(\gamma_{AB}) - \mathcal{C}\left(\frac{\gamma_{AE}}{1+\gamma_{CE}}\right)\right)^+$ for $R_C \geq \mathcal{C}(\gamma_{CE})$. It can be easily seen that this value of $R_{A,s}$ corresponds to the case where the signal from C acts as a Gaussian noise with power γ_{CE} , which is known to be worst-case jammer on E (see, e.g., [26]).

Finally, two remarks on the case at hand of large-capacity backbone link ($C_L \geq R_C$) are in order, that will be compared in the next sections with the complementary case where $C_L < R_C$. (a) With a large-capacity backbone, the secrecy rate $R_{A,s}$ is a non-decreasing function of the downlink rate R_C . (b) With a large-capacity backbone, the value of the inter-BS channel gain γ_{CB} is irrelevant to the system performance. This clearly contrasts with the case of $C_L = 0$ studied in Sec. II-C: for instance, for the chosen SNRs in the example on Fig. 2, if in addition we assume $\gamma_{CB} \leq \gamma_{CE}$, it can be seen from (8) that with $C_L = 0$ the secrecy rate $R_{A,s}$ is identically zero.

When $0 < C_L < R_C$, the information received by B via the backhaul is not enough to completely eliminate the interference from the BS C to the BS B . In this case, B should be able to use the backhaul capacity C_L to at least partially cancel the interference from the BS C . In the following two sections we describe different strategies that can be used by the BS C in order to provide the adjacent BS B with some information about the downlink transmitted waveform \mathbf{X}_C that enables interference mitigation at B and thus improvement of the secrecy rate $R_{A,s}$ (recall the discussion about (8)).

IV. QUANTIZATION-BASED TRANSMISSION STRATEGIES

In this section, we describe two strategies based on source coding arguments (quantization) for transferring information from C to B , while the next section proposes strategies based on channel coding principles. For the strategies considered in this section, we assume, as above, that the BS C employs a standard randomly generated Gaussian codebook.

A. Elementary Quantization

The first considered approach is based on quantizing the downlink codeword $\mathbf{X}_C(W_C)$ via a rate- C_L Gaussian codebook. Quantization/compression is done by using standard joint typicality-based vector quantization [25] and does not exploit here any side information available at the receiver (*elementary quantization*). Given its optimality in a rate-distortion sense, here we consider a Gaussian test channel, which we represent for convenience in the forward form [24]:

$$\hat{X}_{C,i} = X_{C,i} + Q_i, \quad (12)$$

where Q_i is i.i.d. complex Gaussian quantization noise with power σ_Q^2 . From basic rate-distortion theory, it follows that the following condition should be satisfied:

$$I(X_C; \hat{X}_C) = C_L \quad (13)$$

which, as mentioned above, reflects the fact that the quantization process at C is oblivious to the fact that there is a parallel wireless link between C and B that conveys side information. Since $I(X_C; \hat{X}_C) = \log_2(1 + P_C/\sigma_Q^2)$, the quantization error power σ_Q^2 can be found from (13) as $\sigma_Q^2 = P_C/(2^{C_L} - 1)$, such that the SNR on the equivalent channel (12) reads

$$\gamma_Q = \frac{P_C}{\sigma_Q^2} = 2^{C_L} - 1. \quad (14)$$

It is remarked that the quantization codebook is assumed to be known to the BS B , which uses the received index from the backbone link to decompress the signal into $\hat{\mathbf{X}}_C$. The following proposition provides the rate achievable with this strategy (see proof in Appendix-B).

Proposition 3: If BS C transmits in downlink with rate R_C , the elementary quantization-based strategy achieves with perfect secrecy the rate $R_{A,s}(R_C)$ given by:

$$R_{A,s}(R_C) = \left(S_{AB}^{EQ}(R_C) - S_{AE}(R_C) \right)^+ \quad (15)$$

with $S_{AE}(R_C)$ defined in (7),

$$S_{AB}^{EQ}(R_C) = \begin{cases} \mathcal{C}(\gamma_{AB}) & \text{if } R_C \leq \mathcal{C}\left(\frac{\gamma_{CB}}{1+\gamma_{AB}} + \gamma_Q\right) \\ \mathcal{C}_{sum} - R_C & \text{if } \mathcal{C}\left(\frac{\gamma_{CB}}{1+\gamma_{AB}} + \gamma_Q\right) < R_C \leq \mathcal{C}(\gamma_{CB} + \gamma_Q) \\ \mathcal{C}_{sum} - \mathcal{C}(\gamma_{CB} + \gamma_Q) & \text{if } R_C > \mathcal{C}(\gamma_{CB} + \gamma_Q) \end{cases} \quad (16)$$

and $\mathcal{C}_{sum} = \log_2(2^{C_L}(1 + \gamma_{AB}) + \gamma_{CB})$.

It can be seen that, unlike the large-backbone case of Proposition 2, here the achievable rate (15) is not a monotonically increasing function of R_C since the latter affects (decreases) also $S_{AB}^{EQ}(R_C)$. Moreover, it can be shown that only for $C_L \rightarrow \infty$, the rate (15) tends to the large-backbone secrecy rate (11) due to the residual quantization noise for any finite C_L . In practice (and in our evaluations in Sections VI and VII), whenever the instantaneous rate $R_C \geq C_L$, then we do not use quantization, but transfer the message completely over the backhaul.

B. Wyner–Ziv Quantization

The approach presented above can be improved by designing the quantization scheme according to Wyner-Ziv compression with side information at the decoder [28] (*Wyner-Ziv quantization*). In fact, the wireless signal Y_B received by BS B is correlated with the signal X_C transmitted by BS C and can thus be used as side information at the decoder. From [28], the following relationship should now hold:

$$I(X_C; \hat{X}_C | Y_B) = C_L. \quad (17)$$

By using the Gaussian forward test channel (12), the power of the quantization noise σ_Q^2 and the respective equivalent quantization SNR γ_Q can be easily derived (see Appendix-C) leading to the equivalent SNR

$$\gamma_Q = \frac{P_C}{\sigma_q^2} = (2^{C_L} - 1) \left(1 + \frac{\gamma_{CB}}{1 + \gamma_{AB}} \right). \quad (18)$$

Achievable rates with Wyner-Ziv compression then follow directly from Proposition 3 by simply replacing γ_Q in (14) with (18). It is noted that if $\gamma_{CB} = 0$, this scheme has clearly no advantage over the elementary quantization considered above due to the absence of useful side information at the receiver.

V. SUPERPOSITION CODING-BASED TRANSMISSION STRATEGIES

Here we investigate a channel coding-based strategy to exploit the backbone link with capacity satisfying the condition $C_L < R_C$. The strategy is based on rate-splitting encoding at BS C so that, differently from the previous sections, here C changes the format of its wireless transmission to facilitate the transfer of information over the backbone. It is also noted that this assumption requires downlink terminal D to modify its decoding strategy accordingly (see details below). The message W_C is transmitted by sending two independent messages W_{C1} , W_{C2} with rates R_{C1} , R_{C2} , respectively such that:

$$R_C = R_{C1} + R_{C2}, \quad (19)$$

where R_C is determined by the capacity of the downlink transmission by C :

$$R_C = \mathcal{C}(\gamma_{CD}). \quad (20)$$

The two messages are combined by using superposition coding, such that the i th symbol sent by C is:

$$X_{C,i} = \sqrt{\alpha} X_{C1,i} + \sqrt{1 - \alpha} X_{C2,i}, \quad (21)$$

where α is the power-division coefficient and $0 \leq \alpha \leq 1$. Notice that, unlike the previously described quantization-based scheme, here the downlink channel gain γ_{CD} plays an important role, since any modification in the design

of the transmission scheme at BS C (i.e., rates (R_{C1}, R_{C2}) and coefficient α) has to guarantee successful decoding at terminal D . To elaborate, we assume that decoding at D is carried out via successive interference cancellation, such that W_{C1} is first decoded and subtracted and then W_{C2} is decoded. Such a decoding imposes the following conditions on rates (R_{C1}, R_{C2}) and coefficient α :

$$R_{C1} = \log_2 \left(1 + \frac{\alpha\gamma_{CD}}{1 + (1 - \alpha)\gamma_{CD}} \right) \quad (22)$$

$$R_{C2} = \log_2(1 + (1 - \alpha)\gamma_{CD}). \quad (23)$$

It can be easily seen that for any $0 \leq \alpha \leq 1$, condition (20) is satisfied ($R_{C1} + R_{C2} = \mathcal{C}(\gamma_{CD})$) and we have freedom to chose α .

The basic idea of this strategy is to send one of the messages, either W_{C1} or W_{C2} (i.e., either the one decoded first or last by downlink user D), over the backbone. This implies either $R_{C1} = C_L$ or $R_{C2} = C_L$, respectively. It is noted that once either of the latter condition is specified, this choice, by way of (22)-(23), uniquely determines the value of α and, from (19), the remaining rate. As we will see in the next sections, the choice of which message to send over the backbone drastically impact the achievable secrecy rate, and neither strategy dominates the other.

A. Sending the Message Decoded Last by D (W_{C2})

In this first case, we set $R_{C2} = C_L$, which, from (23), determines the following value of α :

$$\alpha = \alpha_2 = 1 - \frac{2^{C_L} - 1}{\gamma_{CD}}, \quad (24)$$

and the rate $R_{C1} = R_C - C_L$. BS B can then uses W_{C2} to cancel $\mathbf{X}_{C2}(W_{C2})$ from its wireless received signal \mathbf{Y}_B , such that the resulting received wireless signal at B at the instance i is given by:

$$Y_{B,i} = h_{AB}X_{A,i} + h_{CB}\sqrt{\alpha_2}X_{C1,i} + N_{B,i}. \quad (25)$$

The following lemma follows (see proof in Appendix-D).

Lemma 1: If BS C transmits in downlink with rate R_C using the superposition coding scheme with (24), the maximum rate achievable on the link A - B is given by:

$$S_{AB}^{(\alpha_2)}(R_C) = \begin{cases} \min\{\mathcal{C}(\gamma_{AB}), \mathcal{C}(\gamma_{AB} + \alpha_2\gamma_{CB}) - (R_C - C_L)\} & \text{if } R_C - C_L < \mathcal{C}(\alpha_2\gamma_{CB}) \\ \mathcal{C}\left(\frac{\gamma_{AB}}{1 + \alpha_2\gamma_{CB}}\right) & \text{otherwise} \end{cases} \quad (26)$$

B. Sending the Message Decoded First by D (W_{C1})

When W_{C1} is sent over the backbone, we set $R_{C1} = C_L$, resulting in

$$\alpha = \alpha_1 = \frac{1 - 2^{-C_L}}{1 - 1/(1 + \gamma_{CD})} \quad (27)$$

and $R_{C2} = R_C - C_L$. After cancelling out $\mathbf{X}_{C1}(W_{C1})$, the multiple access channel at B is given as:

$$Y_{B,i} = h_{AB}X_{A,i} + h_{CB}(1 - \sqrt{\alpha_1})X_{C2,i} + N_{B,i}. \quad (28)$$

The following result follows from the same arguments as in Appendix-D.

Lemma 2: If BS C transmits in downlink with rate R_C using the superposition coding scheme with (27), the maximum rate achievable on the link A - B is given by:

$$S_{AB}^{(\alpha_1)}(R_C) = \begin{cases} \min\{\mathcal{C}(\gamma_{AB}), \mathcal{C}(\gamma_{AB} + (1 - \alpha_1)\gamma_{CB}) - (R_C - C_L)\} & \text{if } R_C - C_L < \mathcal{C}((1 - \alpha_1)\gamma_{CB}) \\ \mathcal{C}\left(\frac{\gamma_{AB}}{1 + (1 - \alpha_1)\gamma_{CB}}\right) & \text{otherwise} \end{cases} \quad (29)$$

C. Achievable Secrecy Rate with Superposition Coding

Accounting for both options of sending either W_{C1} or W_{C2} over the backbone, we can now state the following result.

Proposition 4: If BS C transmits in downlink with rate R_C , the superposition-based strategy achieves the following rate $R_{A,s}(R_C)$ with perfect secrecy:

$$R_{A,s}(R_C) = \left(S_{AB}^{SUP}(R_C) - S_{AE}(R_C) \right)^+ \quad (30)$$

with

$$S_{AB}^{SUP}(R_C) = \max_{i=1,2} \left\{ S_{AB}^{(\alpha_i)}(R_C) \right\}, \quad (31)$$

where $S_{AB}^{(\alpha_i)}(R_C)$ are defined in (26) and (29), and $S_{AE}(R_C)$ is given by (7).

The proposition follows from Lemmas 2 and 1 and similar arguments as in the proof of Proposition 1 [16]. In particular, following such arguments, one should calculate the maximum rate decodable by the eavesdropper E for given R_C and for the rate splitting strategy. It can be shown that this maximum rate is indeed $S_{AE}(R_C)$ as in (30), that is, it is the same rate that we would have if BS C had used a single-rate Gaussian codebook. This is because from (19),(22), and (23), it can be proved that any of the superposed messages is decodable if and only if the other is.

A final remark concerns a comparison between the superposition strategy and elementary quantization. It can be shown by comparing (30) and (16) (with (14)) that for downlink rate $R_C \rightarrow \infty$ the performance of both scheme coincide since $S_{AB}^{SUP}(R_C) \rightarrow S_{AB}^{EQ}(R_C) = C_{sum} - \mathcal{C}(\gamma_{CB} + \gamma_Q)$.

D. Some Comments on the Superposition Strategy

The achievable secrecy rate (30) contains a maximization over the choice of which message should be sent over the backhaul link. This choice is made so as to optimize the maximum achievable rate on the link A - B (31). In this regard, some general conclusion can be drawn by noticing that from the assumption $R_C = \mathcal{C}(\gamma_{CD}) \geq C_L$ it can be verified that

$$\alpha_2 \geq 1 - \alpha_1. \quad (32)$$

Then the following observations can be made:

- For *large* downlink rates R_C , such that:

$$R_C \geq C_L + \mathcal{C}(\alpha_2\gamma_{CB}) = \mathcal{C}(2^{C_L}\gamma_{CB}) \stackrel{(a)}{\geq} C_L + \mathcal{C}((1 - \alpha_1)\gamma_{CB}) \quad (33)$$

where (a) follows from (32) it follows from Lemmas 1 and 2 that

$$S_{AB}^{(\alpha_2)}(R_C) = \mathcal{C}\left(\frac{\gamma_{AB}}{1 + \alpha_2\gamma_{CB}}\right) \leq \mathcal{C}\left(\frac{\gamma_{AB}}{1 + (1 - \alpha_1)\gamma_{CB}}\right) = S_{AB}^{(\alpha_1)}(R_C) \quad (34)$$

which means that sending X_{C1} over the backbone offers higher achievable rates R_A .

- For *low* downlink rates R_C , such that:

$$R_C \leq C_L + \mathcal{C}((1 - \alpha_1)\gamma_{CB}) \leq C_L + \mathcal{C}(\alpha_2\gamma_{CB}) \quad (35)$$

it follows from Lemmas 1 and 2 that

$$\begin{aligned} S_{AB}^{(\alpha_2)}(R_C) &= \min\{\mathcal{C}(\gamma_{AB}), \mathcal{C}(\gamma_{AB} + \alpha_2\gamma_{CB}) - (R_C - C_L)\} \\ S_{AB}^{(\alpha_1)}(R_C) &= \min\{\mathcal{C}(\gamma_{AB}), \mathcal{C}(\gamma_{AB} + (1 - \alpha_1)\gamma_{CB}) - (R_C - C_L)\} \\ \text{thus } S_{AB}^{(\alpha_2)}(R_C) &\geq S_{AB}^{(\alpha_1)}(R_C) \end{aligned} \quad (36)$$

which means that sending X_{C2} over the backbone offers higher achievable rates R_A .

We give an intuitive explanation of the previous result. Note that if a signal contains two superposed messages and one of those messages is known a priori, then this is equivalent to cancelling power from the composite message. For example, if in (21) the message W_{C1} is known, then we cancel the signal $\sqrt{\alpha}X_{C1}$, which corresponds to the power of αP_C . Now we can ask the following question: If we fix the condition $R_{C1} + R_{C2} = R_C$ and we set one of the rates (R_{C1} or R_{C2}) to be equal to C_L , then in which case we can cancel the maximal amount of power from the composite message? From the previous discussions, if $R_{Cj} = C_L$ then we determine $\alpha = \alpha_j$. If W_{C2} is sent over the backhaul then $j = 2$ and the amount of power cancelled is $(1 - \alpha_2)P_C$. If $j = 1$, the amount of power cancelled is $\alpha_1 P_C$. Hence, using the condition (32), we conclude that sending W_{C2} over the backhaul implies minimal possible cancellation of power from the composite message (and thus at the receiver B) and the remaining power of the wireless signal from C at B is largest possible. At relatively low R_C , this effect increases the interval of values for R_C that are completely decodable at B and that is why sending W_{C2} over the backhaul gives higher achievable rate $S_{AB}(R_C)$. However, when the rate R_C is large and thus not completely decodable at B , then X_{C1} acts as a noise and such a high remaining power harms the rate achievable for large R_C . On the other hand, when W_{C1} is sent over the backbone, the uncanceled part of the composite message has minimum possible power, which is desirable when that portion of the signal sent by C is undecodable and has to be treated as noise.

VI. NUMERICAL EXAMPLES

In this section we provide some numerical examples for the performance of the proposed confidential transmission schemes when all the wireless channels are deterministic (unfaded), as assumed in the previous sections. We will use the following acronyms: *EQ* for Elementary Quantization, *WZ* for Wyner–Ziv quantization, and *SUP* for transmission based on superposition coding. In the cases $R_C \leq C_L$, the message from C is completely transferred via the backhaul, such that all the schemes behave identically.

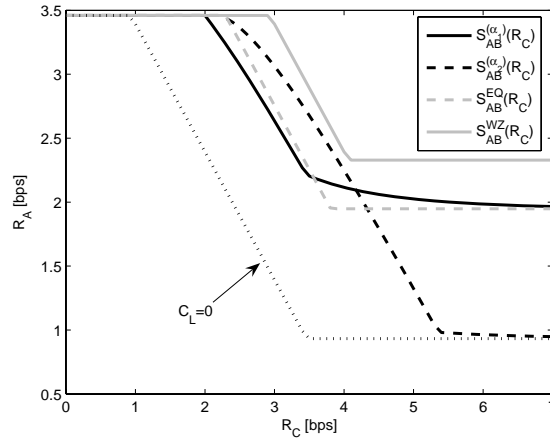


Fig. 3. Maximum achievable rates from A to B (without confidentiality constraints) $S_{AB}^{(\alpha_1)}(R_C)$, $S_{AB}^{(\alpha_2)}(R_C)$, $S_{AB}^{EQ}(R_C)$ and $S_{AB}^{WZ}(R_C)$ with $\gamma_{AB} = \gamma_{CB} = 10$ [dB] and $C_L = 2$ [bps]. As a reference, the function $S_{AB}(R_C)$ with $C_L = 0$ is also shown.

We start by considering the maximum achievable rates with no confidentiality constraints from terminal A to BS B , namely $S_{AB}^{EQ}(R_C)$ (16) (14); $S_{WZ}^{EQ}(R_C)$ (16) (18); $S_{AB}^{(\alpha_1)}(R_C)$ (29) and $S_{AB}^{(\alpha_2)}(R_C)$ (26). These figures are relevant as the improvement in the maximal achievable rate from A to B is a direct indicator of the effectiveness of a particular strategy. Fig. 3 depicts such rates versus the downlink rate R_C . For the chosen parameters ($\gamma_{AB} = \gamma_{CB} = 10$ [dB] and $C_L = 2$ [bps]), WZ is to be preferred for any value of the downlink rate R_C . Moreover, by appropriately selecting which message is sent over the backbone (W_{C1} or W_{C2}), that is choosing between $S_{AB}^{(\alpha_1)}(R_C)$ and $S_{AB}^{(\alpha_2)}(R_C)$, the SUP strategy outperforms the EQ for any R_C . On this note, confirming the discussion of Sec. 3, we have that for lower R_C it is more convenient to send W_{C2} over the backbone ($S_{AB}^{(\alpha_2)}(R_C) > S_{AB}^{(\alpha_1)}(R_C)$) and viceversa for larger R_C . Finally, we remark that, as pointed out in Section V-C, if the rate R_C is large enough, the EQ strategy obtains a constant secrecy rate R_C , which coincides with the asymptotic achievable for of the SUP strategy.

Fig. 4 shows the achievable rate without confidentiality constraints (as Fig. 3) versus the SNR between the BSs γ_{CB} . Here it can be seen that, for low values of γ_{CB} the SUP strategy outperforms the WZ strategy. The U-shape of all the curves versus γ_{CB} can be explained similarly to the arguments used to study interference channels with weak and strong interference. Consider for instance the case $C_L = 0$. For low γ_{CB} , BS B cannot decode R_C , but the wireless interference from C at B is weak, which makes the achievable rate $A - B$ high. As γ_{CB} increases, but still not sufficiently as to make rate R_C decodable at B , the achievable rate on link $A - B$ drops. However, for strong interference γ_{CB} , BS B can decode R_C and then subtract it, thus causing low (if any) penalty to the rate from A to B .

Fig. 5 depicts the derived secrecy rates for different values of C_L versus the downlink rate R_C for $\gamma_{AB} = \gamma_{CB} = \gamma_{AE} = \gamma_{CE} = 20$ [dB]. Note that with such a choice of SNRs the Noise-Forwarding strategy [16] ($C_L = 0$) offers a zero secrecy rate, which implies that in this case the presence of the backbone offers markedly improved secrecy.

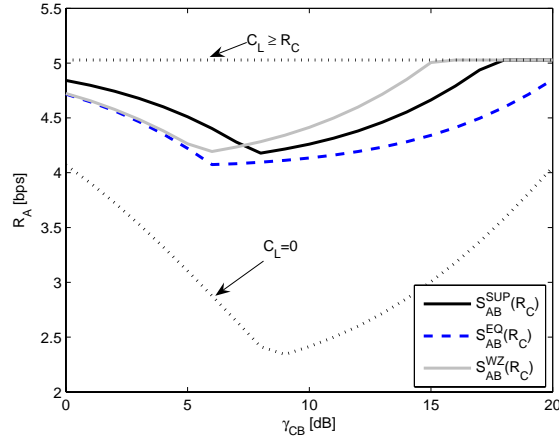


Fig. 4. Maximum achievable rates from A to B (without confidentiality constraints) $S_{AB}^{(\alpha_1)}(R_C)$, $S_{AB}^{(\alpha_2)}(R_C)$, $S_{AB}^{EQ}(R_C)$ and $S_{AB}^{WZ}(R_C)$ with $\gamma_{AB} = 15$ [dB], $C_L = 2$ [bps] and $R_C = 3$ [bps]. As a reference, we have plotted the line $S_{AB}(R_C)$ with $C_L = 0$ and $S_{AB}(R_C) = \mathcal{C}(\gamma_{AB})$ for $C_L \geq R_C$.

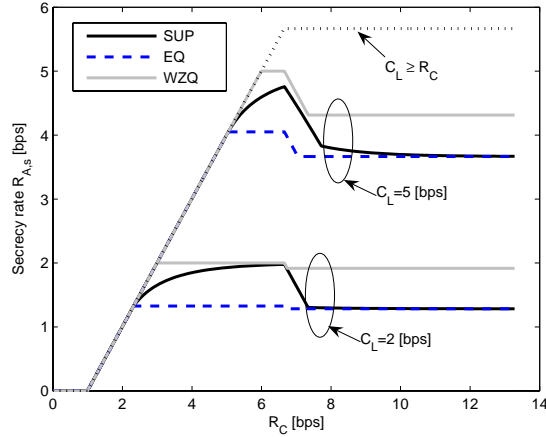


Fig. 5. Achievable secrecy rates by superposition, elementary quantization and Wyner-Ziv quantization for different C_L versus R_C ($\gamma_{AB} = \gamma_{CB} = \gamma_{AE} = \gamma_{CE} = 20$ [dB]).

Moreover, for small downlink rates R_C , all proposed strategies have the same achievable secrecy rate as in the case of large backbone capacity studied in Section III ($C_L > R_C$) up to a certain value of R_C , which is the largest for the WZ strategy. Finally, as pointed out above, WZ offers substantial gains with respect to EQ, and, given the large value of γ_{CB} in this example, also with respect to SUP (where SUP and EQ have the same performance for large R_C).

Finally, Fig. 6 succinctly illustrates the relation between the maximal achievable rates and the achievable secrecy rates for the schemes with superposition and Wyner-Ziv quantization. The link parameters had been chosen in a way that shows that no scheme is superior for all the values of R_C .

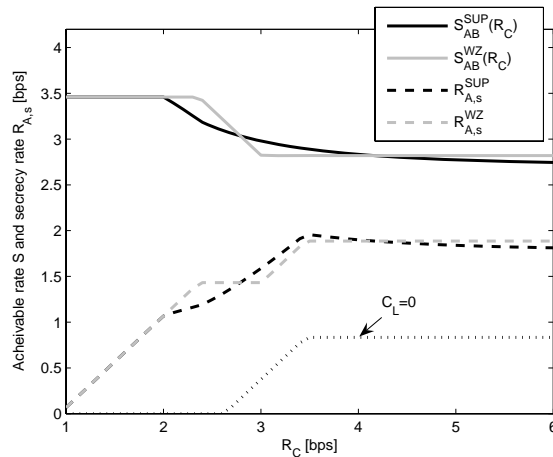


Fig. 6. Maximum achievable rates from A to B (without confidentiality constraints) and the achievable secrecy rates by superposition and Wyner-Ziv quantization with $C_L = 2$, $\gamma_{AB} = \gamma_{AE} = \gamma_{CE} = 10$ [dB] and $\gamma_{CB} = 5$. As a reference, the achievable secrecy rate with $C_L = 0$ is also shown.

VII. EXTENSION TO FADING CHANNELS

In this section, we turn the attention to fading channels and reconsider the performance of the proposed transmission strategies under different assumptions regarding the channel state information available at different nodes.

A. Scenario and Performance Measures

The inter-BS link $C - B$ is considered to be a line-of-sight and thus does not experience fading, i. e., γ_{CB} is constant, while the other links are faded. We assume that a fading link h_{UV} features Rayleigh fading, such that the SNR of the link γ_{UV} is independently and exponentially distributed with average value $\bar{\gamma}_{UV}$. Furthermore, we consider block fading, such that a fading channel stays constant for a sufficient number of symbols n , where for coding purposes n can be assumed to be infinity. It is noted that the assumption regarding the inter-BS link γ_{CB} is a reasonable if, e.g., the BSs are sufficiently elevated with respect to the rest of the network. As far as channel state information is concerned, terminal A is assumed to know the channel gains γ_{AB} (and the constant γ_{CB}), beside the downlink rate R_C , so that it can calculate (and transmit at) the maximum instantaneous achievable rate $S_{AB}(R_C)$ in (7). Other assumptions will be differently specified below for two scenarios, one in which we measure the outage probability and the other in which we assess the scheduling performance.

1) *No Channel State Information about: Outage Probability:* This scenario relies on the realistic assumption that the instantaneous fading channel to the eavesdropper γ_{AE} and γ_{CE} are not known to terminal A and BS C . In such a case, no non-zero rate is achievable with perfect secrecy, and therefore one has to resort to the concept of outage probability [19], [23]. In particular, given a target secrecy rate $R_{A,s}$, the outage probability is defined as the probability that such $R_{A,s}$ is not achievable for the given transmission technique. It is noted that, for each fading realization, the value of R_C is selected as here selected as (20), which requires BS C to know the instantaneous

downlink channel $\gamma_{CD} - D$.

2) *Full Channel State Information: Scheduling Performance*: In this second scenario, we assume full channel state information about all the fading channels at both terminal A and BS C . Given the full channel state information, it is relevant here to generalize the model to include M_u uplink users A_1, A_2, \dots, A_{M_u} that have data to transmit to B and M_d downlink users D_1, D_2, \dots, D_{M_d} potentially receiving from BS C . The goal is to analyze the impact of different scheduling and transmission strategies on the performance of the network at hand over fading channels. As throughout the paper, of particular interest is the impact of design choices on the trade-off between the downlink (R_C) and the uplink secrecy rate ($R_{A,s}$).

Regarding uplink scheduling, we assume that the uplink user A_{i^*} is selected so as to maximize the uplink rate:

$$i^* = \max_i \gamma_{A_i B} \quad (37)$$

More interesting is the scheduling of the downlink transmissions from C , for which we define two different types of schedulers:

- *Max R_C* scheduler: In this case the scheduled user D_{j^*} is selected so as to maximize the downlink rate:

$$j^* = \max_j \gamma_{CD_j} \quad (38)$$

- *MaxSec* scheduler: In this case the selection of the user D_{j^*} is done so as to maximize the uplink secrecy rate $R_{A,s}$. Accordingly, the selection of D_{j^*} depends on which method is used by C to communicate over the backbone. If WZ quantization is used, the scheduler is denoted *MaxSec $_{WZ}$* and we have:

$$j^{*,WZ} = \max_j R_{A,s}^{WZ}(\log_2(1 + \gamma_{CD_j})), \quad (39)$$

while if superposition is used, the scheduler is denoted *MaxSec $_{SUP}$* and:

$$j^{*,SUP} = \max_j R_{A,s}^{sup}(\log_2(1 + \gamma_{CD_j})). \quad (40)$$

Note that, in general $j^{*,WZ} \neq j^{*,SUP}$. Our results for the fading channels confirm that WZ is always outperforming EQ in terms of achievable secrecy rate and we have not plotted EQ in order to contribute to the clarity of the figures. Performance evaluation is then carried out by calculating the average secrecy rate $\bar{R}_{A,s}(\mathcal{S})$ and the average downlink rate $\bar{R}_C(\mathcal{S})$, where the average is taken with respect to the fading channels ($\gamma_{A_i^* B}$, $\gamma_{A_i^* E}$, γ_{CE} , $\gamma_{CD_{j^*}}$) given the scheduler $\mathcal{S} \in \{\text{Max}R_C, \text{MaxSec}_{sup}, \text{MaxSec}_{WZ}\}$.

B. Numerical Results

We now present some numerical results for the two considered scenarios.

1) *Outage Probability*: Fig. 7 depicts the outage probability as a function of the backbone capacity C_L for $\bar{\gamma}_{AB} = \bar{\gamma}_{AE} = \bar{\gamma}_{CE} = \bar{\gamma}_{CD} = 15$ [dB], $\gamma_{CB} = 15$ [dB], $R_{A,s} = 1$ [bps]. We recall that the value R_C is selected according to the instantaneous SNR γ_{CD} as (20). The line $C_L \geq R_C$ is obtained by assuming that C_L is large enough to accommodate any rate R_C (strictly speaking, $C_L \rightarrow \infty$). It can be seen that, as C_L increases, the outage probability of all the strategies approaches this asymptotic performance, as it becomes highly probable that the

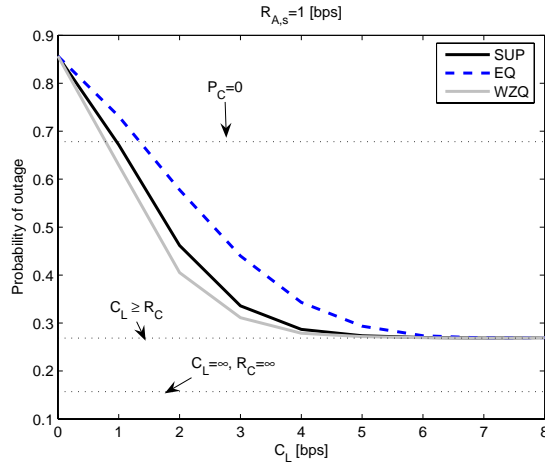


Fig. 7. Secrecy outage probability vs. the backhaul capacity C_L . The average values of the fading links are $\bar{\gamma}_{AB} = \bar{\gamma}_{AE} = \bar{\gamma}_{CE} = \bar{\gamma}_{CD} = 15$ [dB]. The constant value γ_{CB} is 15 [dB]. The line $P_C = 0$ refers to the case when no cooperative interference from C takes place. The target secrecy rate is $R_{A,s} = 1$ [bps].

given C_L can accommodate the rate $\mathcal{C}(\gamma_{CD})$. The lower bound on the outage probability is obtained by assuming that C sends pure Gaussian noise (which is the worst jamming signal, see, e.g., [26]), that is perfectly transferred through the backbone ($C_L = \infty, R_C = \infty$). Another reference performance is set by the case $P_C = 0$, where no downlink transmission takes place. For low values of C_L , the proposed schemes can actually be outperformed by such solution. This is because, for low C_L , the downlink transmission impairs not only reception at the eavesdropper E , but also at the BS B .

Fig. 8 depicts the outage probability as a function of the inter-BS SNR γ_{CB} for $\bar{\gamma}_{AB} = \bar{\gamma}_{AE} = \bar{\gamma}_{CE} = \bar{\gamma}_{CD} = 15$ [dB], $R_{A,s} = 1$ [bps] and $C_L = 2$ [bps]. The U-shape of the curves for the proposed strategies can be explained by resorting to similar arguments as for Fig. 4 (see Sec. VI). Following this remark, we note from Fig. 8 that the gain in terms of outage probability of all strategies with respect to the case $C_L = 0$ is most relevant in the regime of weak/strong interference from BS C (i. e. low/high γ_{CB}). In fact, it is in this regime that the interference from BS C to B (due to the realizations where $R_C > C_L$) has the least impact on the performance of the link $A - B$.

2) *Scheduling performance*: Turning to the average rates that can be achieved in the scenario of full channel state information, Fig. 9 considered the downlink rates in terms of the ratios $\frac{\bar{R}_C(\text{MaxSec}_{sup})}{R_C(\text{Max}R_C)}$ and $\frac{\bar{R}_C(\text{MaxSec}_{WZ})}{R_C(\text{Max}R_C)}$ for $\bar{\gamma}_{AB} = \bar{\gamma}_{AE} = \bar{\gamma}_{CD} = \bar{\gamma}_{CE} = 15$, $\gamma_{CB} = 5$ [dB]. These ratio demonstrate which fraction of the maximal average downlink throughput is achieved if the scheduler at C aims to maximize the secrecy of the transmission $A - B$. Equivalently, the complement to one of such ratios measure the fractional rate loss due to the requirement of maximizing the secrecy of the transmission $A - B$. The results show that at high C_L , maximum secrecy is coherent with maximal rate R_C . However, from Fig. 9 it is seen that for lower C_L maximal secrecy is not always achieved by maximizing R_C , which is in accordance with the observations from Fig. 5. Regarding the SUP strategy, there is one degenerative effect, which can be explained by observing the SUP curve on Fig. 5. It can be seen (on the figure

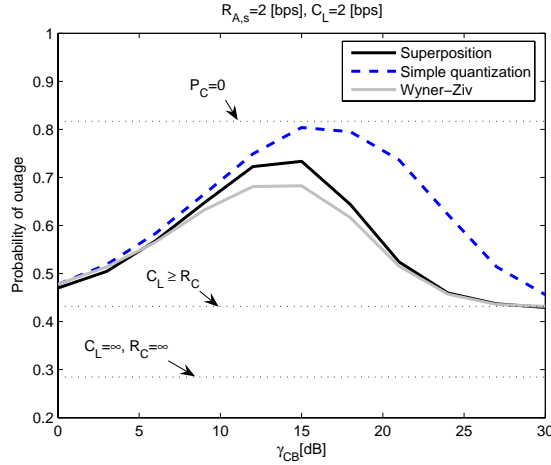


Fig. 8. Secrecy outage probability vs. the SNR γ_{CB} . The average values of the fading links are $\bar{\gamma}_{AB} = \bar{\gamma}_{AE} = \bar{\gamma}_{CE} = \bar{\gamma}_{CD} = 15$ [dB]. The constant value γ_{CB} is 15 [dB]. The line $P_C = 0$ refers to the case when no cooperative interference from C takes place. The target secrecy rate is $R_{A,s} = 2$ [bps]. The backhaul has $C_L = 2$ [bps], except for the reference line with $C_L = \infty$.

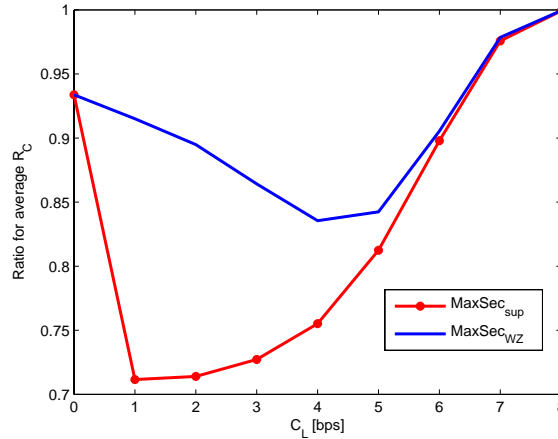


Fig. 9. Ratios $\frac{\bar{R}_C(\text{MaxSec}_{\text{SUP}})}{\bar{R}_C(\text{Max}R_C)}$ and $\frac{\bar{R}_C(\text{MaxSec}_{\text{WZ}})}{\bar{R}_C(\text{Max}R_C)}$. The parameters are $\bar{\gamma}_{AB} = \bar{\gamma}_{AE} = \bar{\gamma}_{CD} = \bar{\gamma}_{CE} = 15$ [dB]. The constant SNR is $\gamma_{CB} = 5$ [dB].

not discernible for $C_L = 2$) that for large R_C , the secrecy rate of the SUP scheme slowly decreases towards the asymptotic value (achieved for $R_C \rightarrow \infty$), while for the quantization schemes there are finite values of R_C after which the secrecy rate becomes constant. Hence, the scheduler that maximizes the secrecy tends to select lower rates R_C when SUP is applied. Nevertheless, when $C_L = 0$, both SUP and WZ operate in identical way.

The average secrecy rates from A to B are then shown in Fig. 10-11 in terms of the ratios $\frac{\bar{R}_{A,s}(\text{MaxSec}_{\text{SUP}})}{\bar{R}_{A,s}(\text{Max}R_C)}$ and $\frac{\bar{R}_{A,s}(\text{MaxSec}_{\text{WZ}})}{\bar{R}_{A,s}(\text{Max}R_C)}$. Thus, the figures shows, for each transmission method (WZ or SUP), how much the secrecy rate is improved if the scheduler at C determines the downlink user (and the corresponding rate R_C) in order to maximize the instantaneous rate $R_{A,s}$ rather than the downlink rate R_C . It can be seen that for a weak link

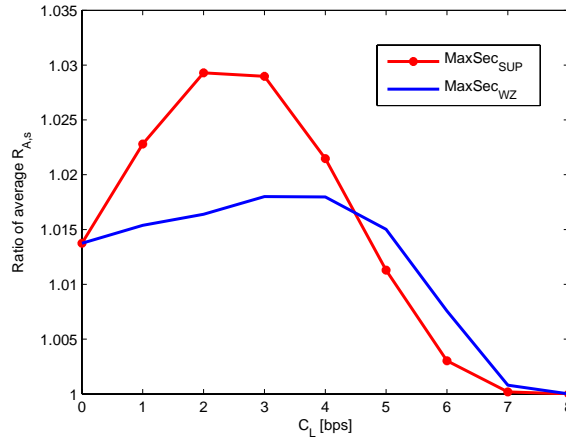


Fig. 10. Ratios $\frac{\bar{R}_{A,s}(MaxSec_{sup})}{\bar{R}_{A,s}(MaxR_C)}$ and $\frac{\bar{R}_{A,s}(MaxSec_{WZ})}{\bar{R}_{A,s}(MaxR_C)}$. The parameters are $\bar{\gamma}_{AB} = \bar{\gamma}_{AE} = \bar{\gamma}_{CD} = \bar{\gamma}_{CE} = 15$ [dB]. The constant SNR is $\gamma_{CB} = 5$ [dB].

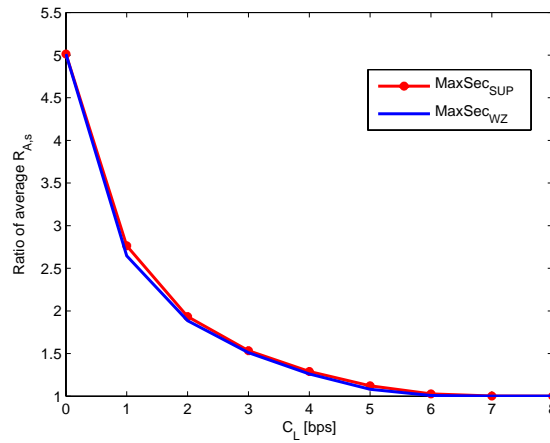


Fig. 11. Ratios $\frac{\bar{R}_{A,s}(MaxSec_{sup})}{\bar{R}_{A,s}(MaxR_C)}$ and $\frac{\bar{R}_{A,s}(MaxSec_{WZ})}{\bar{R}_{A,s}(MaxR_C)}$. The parameters are $\bar{\gamma}_{AB} = \bar{\gamma}_{AE} = \bar{\gamma}_{CD} = \bar{\gamma}_{CE} = 15$ [dB]. The constant SNR is $\gamma_{CB} = 20$ [dB].

$C - B$ (low γ_{CB}), as on Fig. 10 (where $\gamma_{CB} = 5$ [dB]), the gain in the secrecy rate for the *MaxSec* schedulers is insignificant, which means that application of opportunistic scheduler *MaxR_C* at C will be also good for the security of the link $A - B$. Conversely, for a strong link $C - B$, the results on Fig. 11 show that the secrecy of the link $A - B$ can be boosted by selecting appropriate non-maximal R_C and in this case the opportunistic downlink scheduler at C is not compatible with the secrecy requirements.

VIII. DISCUSSION

In this section, we further discuss the limitations of the considered model as well as possible ways to extend the analysis to scenarios with less restrictive assumptions.

It can be observed that the proposed schemes are effective in securing the area that is covered by the transmission of BS C , e.g., to obtain statistically improved confidentiality with respect to all eavesdroppers E that are within the transmission radius of BS C . If one was instead interested in securing communications with respect to a specific eavesdropper E , the model at hand would be hardly applicable, as the eavesdropper is a passive agent that is generally hard to locate. If E is not interfered by C , our analysis applies having set $h_{CE} = 0$: In this case, the presented schemes will experience worse statistics for the achieved secrecy rate. As an example, if $h_{CE} = 0$ and $C_L \geq R_C$, the model boils down to the fading wiretap channel [19] [20], in which the achievable secrecy rate depends purely on the relative quality of the fading conditions on the main link $A - B$ and wiretap link $A - E$.

Now we turn to the scenarios with more than two cells. Consider at first a situation where, beside the cell of interest with BS B and terminal A , we are interested in modelling the interference coming from m adjacent cells, with BSs C_1, C_2, \dots, C_m , assumed to be operated for simplicity in downlink with rates R_{C_1}, \dots, R_{C_m} . Define as $C_{L,i}$ the backhaul capacity from BS C_i to B . Notice that we could account for some of the m other cells being operated in uplink by appropriately redefining the channel gains and taking $C_{L,i} = 0$ for that specific cell (no backhaul link exists between users and BSs). As explained in Section II-A, the more complex and interesting case arises when the eavesdropper is aware of the codebooks used by BSs C_1, C_2, \dots, C_m . Under this assumption, we discuss here the extension of Proposition 2 that sets an upper bound to the achievable secrecy rate and corresponds to setting $C_{L,i} \geq R_{C_i}$ for all $i = 1, 2, \dots, m$. Following the proof of Proposition 2, it is not difficult to see that the following upper bound holds (recall (11)):

$$R_{A,s}(R_C) \leq (\mathcal{C}(\gamma_{AB}) - S_{AE}(R_{C_1}, \dots, R_{C_m}))^+, \quad (41)$$

where $S_{AE}(R_{C_1}, \dots, R_{C_m})$ generalizes the function $S_{AE}(R_C)$ in (7) and is defined as the capacity from A to E in the presence of interferers with known (Gaussian) codebooks of rates R_{C_1}, \dots, R_{C_m} . Notice that the result of Proposition 1 corresponding to $C_{L,i} = 0$ could also be easily extended along the same lines. Evaluation of the function $S_{AE}(R_{C_1}, \dots, R_{C_m})$ is far from being straightforward, especially for large m , but a computationally efficient procedure is described in [29], to which we refer for further details.

The upper bound (41) is achievable, as explained above and similarly to Proposition 2, if $C_{L,i} \geq R_{C_i}$ for all $i = 1, 2, \dots, m$. If any of these conditions is not satisfied, then one could exploit the backhaul capacity $C_{L,i}$ in order to mitigate the interference from C_i to B via quantization-based or superposition coding-based strategies, as done above for the two-cell case. A more practical approach that does not require demanding system-wide synchronization assumptions is for the BS B to select a single “partner” BS C_i to secure only the area covered by C_i . In this case, the eavesdropper and B treat the asynchronous interference coming from other cells as background Gaussian noise. How to select such a partner BS is a natural research question for the future work.

Consider now the case where multiple terminals, say A_1, A_2, \dots, A_M , are interested in accessing base station B with information-theoretic secrecy guarantees. Should the BS C be inactive ($P_C = 0$), the scenario would revert to the model extensively studied in [6]. With the transmission from BS C , extension of our results would require the combination of the approaches of [29] and [6]. This appears to be feasible but not straightforward and is left for

future research. Further on, if we consider a multicell system in which we want to secure several simultaneous uplink transmissions, each one to a different BS B_k , then the extension of the proposed schemes requires a substantial investigation. For example, consider the case where the backhaul links are with unequal capacity. If the BS C_j has a backhaul of $C_{Li} < R_{Cj}$ towards B_i and a backhaul of $C_{Lk} < R_{Cj}$ towards another uplink receiver B_k , then it is not straightforward to extend the proposed schemes (e. g. the one with superposition coding) to enable efficient partial interference cancellation at both BSs, B_i and B_k .

Finally, we remark that the presence of a backhaul link between the BSs could be exploited not only for enhancing secrecy, as elaborated upon in this paper, but also to increase the system throughput via multicell processing [18]. Investigation of the trade-offs between the two strategies and goals, namely secrecy via simultaneous uplink/downlink transmissions and throughput via multicell processing, is deemed to be outside the scope of this paper.

IX. CONCLUSIONS

Optimized scheduling and multi-cell BS cooperation are becoming increasingly standard features of current and future wireless infrastructure (cellular) networks. This work has advanced the notion that such technologies can play an important role in ensuring confidentiality (security) of wireless transmissions. From the analysis of several transmission strategies under different assumptions regarding propagation channels and corresponding channel state information, a number of conclusions have been drawn. In particular, a technique based on Wyner-Ziv compression over the backbone link connecting the BSs has proved to be the most promising, with the added benefit of requiring no modifications on the uplink/ downlink transmissions of a conventional cellular systems. When complexity of Wyner-Ziv encoding is an issue, one could resort to simpler quantization schemes with a performance loss that depends on the network topology. Or else, if willing to modify the downlink transmission/ reception strategy for the sake of ensuring uplink confidentiality, one could opt for channel coding (rather than source coding) based techniques which perform close (or even better than) Wyner-Ziv under some circumstances.

There are several interesting extensions of this work. A first issue, briefly discussed in Sec. VIII, is the extension to multiple cooperating BSs, which raises the question how to organize the transmission/receive schedule for the BSs in order to maximize the secrecy effect, while not degrading the throughput. A second aspect would be to derive tighter upper bound than the one considered here by, e.g., leveraging more sophisticated genie-aided strategies. Finally, the study can be extended to consider colluding eavesdroppers, which attempt to jointly decode the desired signal and the interference from the downlink transmissions.

APPENDIX A

A BRIEF REVIEW OF THE LITERATURE ON WIRELESS SECRECY

Here we cite a few of the most relevant works concerning multi-antenna and/ or multi-user wireless systems with secrecy constraints. The secrecy capacity of a MIMO wiretap channel was studied in [12] [13] [14]. Turning to multi-user channels, a scenario with two users communicating over a Gaussian multiple-access channel to a common receiver, or among them over a Gaussian two-way channel, with an external wiretapper was studied in

[6]. A different multiple access scenario in which each user is interested in keeping its message secret to the other user is investigated in [7]. A fading broadcast model is studied in [8] where the transmitter communicates with two receivers while keeping one ignorant regarding the message intended for the other. An extension of this latter work is considered in [9], where the transmitter is endowed with multiple antennas. Interference channels in which two users communicate to two distinct destinations while keeping the message secret from the other receiver are studied in [10] (see also [30]). Finally, an extension of such work is considered in [11], in which one of the two transmitter has "cognitive" capabilities (i.e., it knows a priori the message of the other user).

APPENDIX B

PROOF OF PROPOSITION 3

The equivalent signal seen at BS B over both the wireless and wired channels in a given time instant i can be written as a vector MAC channel:

$$\tilde{Y}_{B,i} = \begin{bmatrix} Y_{B,i} \\ \hat{X}_{C,i} \end{bmatrix} = \begin{bmatrix} h_{AB} & h_{CB} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} X_{A,i} \\ X_{C,i} \end{bmatrix} + \begin{bmatrix} N_i \\ Q_i \end{bmatrix}. \quad (42)$$

Let $S_{AB}^{EQ}(R_C)$ denote the maximum achievable rates from A to B for a given transmission rate R_C when the quantization strategy is used (recall (7)). In order to determine $S_{AB}^{EQ}(R_C)$, we have to examine the achievable region for the vector MAC channel with output (42):

$$R_{AB} < I(X_A; \tilde{Y}_B | X_C) \quad (43a)$$

$$R_{CB} < I(X_C; \tilde{Y}_B | X_A) \quad (43b)$$

$$R_{AB} + R_{CB} < I(X_A, X_C; \tilde{Y}_B) \quad (43c)$$

where we have dropped the index i for simplicity) and X_A represents normally-distributed complex signal transmitted by A . The first mutual information term can be determined as follows:

$$I(X_A; \tilde{Y}_B | X_C) = I(X_A; Y_B, \hat{X}_C | X_C) = I(X_A; Y_B | X_C) + I(X_A; \hat{X}_C | X_C, Y_B) = I(X_A, Y_B | X_C) = \mathcal{C}(\gamma_{AB}) \quad (43d)$$

since \hat{X}_C is conditionally independent of X_A when X_C is given and therefore $I(X_A; \hat{X}_C | X_C, Y_B) = 0$. The second bound leads to:

$$I(X_C; \tilde{Y}_B | X_A) = \mathcal{C}(\gamma_{CB} + \gamma_Q) \quad (44)$$

while the third condition is:

$$I(X_A, X_C; \tilde{Y}_B) = \quad (45)$$

$$= I(X_C; \tilde{Y}_B) + I(X_A; \tilde{Y}_B | X_C) = \quad (46)$$

$$\stackrel{(a)}{=} \mathcal{C} \left(\frac{\gamma_{CB}}{1 + \gamma_{AB}} + \gamma_Q \right) + I(X_A; Y_B | X_C) \quad (47)$$

$$= \mathcal{C} \left(\frac{\gamma_{CB}}{1 + \gamma_{AB}} + \gamma_Q \right) + \mathcal{C}(\gamma_{AB}) \quad (48)$$

$$= \log_2 (2^{C_L} (1 + \gamma_{AB}) + \gamma_{CB}) \quad (49)$$

where (a) follows again from X_A being conditionally independent of \hat{X}_C for given X_C . The rate $S_{AB}^{EQ}(R_C)$ in (3) then easily follows.

APPENDIX C PROOF OF (50)

Using the same model for the vector MAC channel as in (42), we can write:

$$\begin{aligned} C_L &= I(X_C; \hat{X}_C | Y_B) = I(X_C; \hat{X}_C, Y_B) - I(X_C; Y_B) = \\ &= \mathcal{C} \left(\frac{\gamma_{CB}}{1 + \gamma_{AB}} + \gamma_Q \right) - \mathcal{C} \left(\frac{\gamma_{CB}}{1 + \gamma_{AB}} \right) = \\ &= \log_2 \left(1 + \frac{\gamma_Q}{1 + \frac{\gamma_{CB}}{1 + \gamma_{AB}}} \right) \end{aligned} \quad (50)$$

and thus (50) easily follows.

APPENDIX D PROOF OF LEMMA 1

Similarly to Appendix-A, we need to determine the maximal achievable rate $S_{AB}^{(\alpha_2)}(R_C)$. After $\mathbf{X}_{C2}(W_{C2})$ is canceled at B , the resulting MA channel at B is:

$$Y_B = h_{AB}X_A + h_{CB}\sqrt{\alpha_2}X_{C1} + N_B. \quad (51)$$

We can first determine the capacity region of this MA channel:

$$R_A < \mathcal{C}(\gamma_{AB}) \quad (52)$$

$$R_{C1} = R_C - C_L < \mathcal{C}(\alpha_2\gamma_{CB}) \quad (53)$$

$$R_A + R_C - C_L < \mathcal{C}(\gamma_{AB} + \alpha_2\gamma_{CB}), \quad (54)$$

Recall that the goal is to find the maximal achievable rate R_A for given R_C . However, we assume that $R_C = R_{C1} + R_C^2$ and in this case it is fixed $R_{C2} = C_L$, such that R_C varies due to R_{C1} . Hence, our problem transforms into finding the maximal achievable rate R_A for given R_{C1} by considering the MA channel (51). Depending on the value of R_{C1} we have two cases to consider: when R_{C1} is decodable at B ($R_C - C_L < \mathcal{C}(\alpha_2\gamma_{CB})$) and when

R_{C1} is not ($R_C - C_L \geq \mathcal{C}(\alpha_2 \gamma_{CB})$). But this situation is identical to the one described in Section II-B, such that we can easily arrive to (26).

REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 339–348, May 1978.
- [3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel," *IEEE Trans. Inform. Theory*, vol. 24, pp. 451–456, Jul. 1978.
- [4] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, May 1993.
- [5] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography—Part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121–1132, July 1993.
- [6] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming," submitted [arXiv:cs/0610103v1].
- [7] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 976–1002, March 2008.
- [8] Y. Liang, H. V. Poor, S. Shamai (Shitz), "Secrecy capacity region of parallel broadcast channels," in *Proc. IEEE Information Theory and Applications Workshop (ITW 2007)*, pp. 245–250, Jan. 29– Feb. 2, 2007.
- [9] R. Liu and H. V. Poor, "Multiple antenna secure broadcast over wireless networks," in *Proc. of the First International Workshop on Information Theory for Sensor Networks*, Santa Fe, NM, June 18 - 20, 2007.
- [10] R. Liu, I. Maric, P. Spasojevic, R.D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.
- [11] Y. Liang, A. Somekh-Baruch, H.V. Poor, S. Shamai (Shitz), S. Verdu, "Cognitive interference channels with confidential messages," submitted [arXiv:0710.2018].
- [12] A. Khisti and G. Wornell, "The MIMOME channel," in *Proc. 45th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, Sept. 26–28, 2007.
- [13] F. Oggier, B. Hassibi, "The secrecy capacity of the 2x2 MIMO wiretap channel," in *Proc. 45th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, Sept. 26–28, 2007.
- [14] Tie Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wiretap channel," submitted [arXiv:0710.4105v1].
- [15] G. Kramer, I. Maric and R. D. Yates, *Cooperative Communications*, Foundations and Trends in Networking (FnT), Now Publishers, Jun. 2007.
- [16] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," submitted [arXiv:cs/0612044v1]
- [17] S. Shamai (Shitz), O. Somekh, O. Simeone, A. Sanderovich, B.M. Zaidel and H. V. Poor, "Cooperative multi-cell networks: impact of limited-capacity backbone and inter-users links," in *Proc. Joint Workshop on Coding and Communications*, Dürnstein, Austria, October 14 - 16, 2007.
- [18] O. Somekh, O. Simeone, Y. Bar-Ness, A. Haimovich, U. Spagnolini and S. Shamai, "An information theoretic view of distributed antenna processing in cellular systems," in *Distributed Antenna Systems*, Auerbach Publications, CRC Press, 2007.
- [19] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, 2006.
- [20] P. K. Gopala, L. Lai, H. El Gamal, "On the secrecy capacity of fading channels," submitted [arXiv:cs/0702112v1]
- [21] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Techn. Conference*, vol. 3, pp. 1906–1910, Sept. 2005.
- [22] M. L. Jørgensen, B. Yanakiev, G. E. Kirkelund, P. Popovski, H. Yomo, T. Larsen, "Shout to secure: physical–layer wireless secrecy with known interference", in *Proc. IEEE Globecom 2007*.
- [23] O. Simeone and P. Popovski, "Secure communications via cooperative base stations," to appear in *IEEE Commun. Letters*.
- [24] R. Gallager, *Information Theory and Reliable Communication*. John Wiley & Sons, Inc., 1968.

- [25] T. Cover and J. Thomas. *Elements of Information Theory*. Wiley-Interscience; 2nd edition, 2006.
- [26] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 3072-3081, Nov. 2001.
- [27] R. Tandra and A. Sahai, "Is interference like noise when you know its codebook?" in *Proc. IEEE International Symposium on Information Theory (ISIT 2006)*, pp. 2220 –2224, Seattle, USA, July 2006.
- [28] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inform. Theory*, vol. 22, no. 1, pp. 1-10, Jan 1976.
- [29] A. S. Motahari and A. K. Khandani, "To decode the interference or to Consider it as noise," submitted [arXiv:0711.3176].
- [30] R. D. Yates, D. Tse and Z. Li, "Secret Communication on Interference Channels," in *Proc. IEEE International Symposium on Information Theory (ISIT2008)*, Toronto, Ontario, Canada, July 6–11, 2008.