Wireless Secrecy with Infrastructure–Aided Cooperation

Petar Popovski and Osvaldo Simeone

***Abstract*—A novel approach for ensuring confidential communications over infrastructure-based wireless networks is proposed and analyzed from an information-theoretic standpoint. The considered techniques leverage the finite-capacity backbone connecting the base stations and the possibility to schedule uplink/downlink transmissions in order to create intentional interference. Two different methods are studied, one based on source coding and one on channel coding arguments, and corresponding rates achievable with perfect secrecy are derived.**

I. Introduction

Collaborative transmission technology is widely regarded as a key enabler for advanced wireless networking. When targeting infrastructure networks, both cooperation between mobile stations (MSs) and base stations (BSs) have been considered. The latter case exploits the backbone connecting BSs and has been proved to yield significant throughput gains [1]. Besides providing throughput gains, cooperation has also been proved instrumental in enhancing the confidentiality of transmission [2]. In information-theoretic terms, *perfect security* implies the impossibility for a given eavesdropper E to harness any information about the transmitted message from its received signal [3]. This contrasts with traditional cryptography where security relies on the computational limitations of E. Analysis of secure communications in the sense of [3] has been carried out for single-link Gaussian [4] and fading [5] [6] channels, and for multi-user scenarios (see, e.g., [7]).

In this paper, we show that cooperative processing at the BSs can significantly improve the rate at which information can be exchanged confidentially. The basic idea is to schedule downlink BS transmissions at the same time as the concurrent uplink transmissions, so as to create intentional interference on the possible eavesdroppers and thus increase the secrecy of the uplink. This interference is partially known in advance to the receiving BS (uplink) thanks to the information exchanged over the finite–capacity backbone. The approach is similar to [8] [9] [2] [10], where artificial noise jams the reception of E, while using techniques to avoid interference at the intended receiver. In [8] this interference mitigation is obtained by exploiting the structure and reciprocity of multi-antenna fading channels, while [9] [10] leverage a high-capacity backbone between receiving and jamming antennas.

Here we first introduce a general framework which encompasses the schemes from [9] and [10]. We extend the study to the pertinent scenarios with finite–capacity backhaul[1] and propose two new secrecy schemes, each of them using a combined wireless/backbone transmission. Both schemes and the corresponding achievable rates are investigated and compared via analysis and simulations.

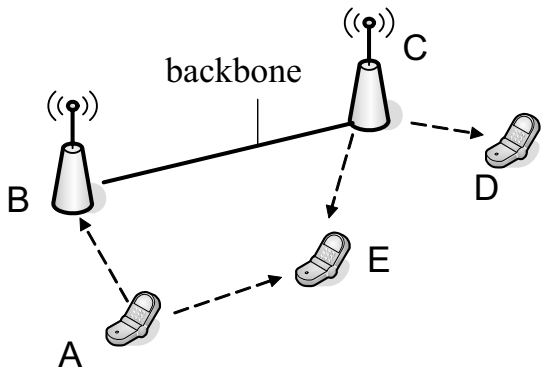

Fig. 1. Illustration of a system with cooperating base stations BS_1 and BS_2, a terminal T and an eavesdropping mobile station E.

II. Background

A. Scenario and system model

We focus on two adjacent cells as in Fig. 1 (the contribution of other cells is considered implicitly as additive noise), where the two BSs are connected by a high capacity, typically wired, backbone [1]. The BSs are termed B and C, respectively. The terminal A has a message to deliver to B under constraints of confidentiality with respect to the activity of an eavesdropper E. The eavesdropper is assumed to be within the transmission range of A (otherwise it would not pose any threat to the confidentiality of the message from A) and of the BS named C. In our scheme, the uplink transmission from A to B is 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 that our scheme is not intended to secure the communication $C - D$. We assume that E knows the codebooks used by A and C.

Formally, A randomly selects a message W_A from the set $\{1, ..., 2^{nR_A}\}$ 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 $\mathrm{E}[|X_{A,i}|^2] = P_A$ through a (possibly

P. Popovski is with the Department of Electronic Systems, Aalborg University, Denmark. E-mail: petarp@es.aau.dk

O. Simeone is with the New Jersey Institute of Technology, USA. E-mail: osvaldo.simeone@njit.edu

[1]We refer the reader to [11] for a review of related information-theoretic analyses on cellular systems with finite-capacity backhaul. We will use the terms "backbone" and "backhaul" interchangeably.

stochastic) mapping: $\mathbf{X}_A$: $\{1,...,2^{nR_A}\}\rightarrow \mathbb{C}^n$ (vectors of n symbols are represented by bold letters). At the same time, C transmits a downlink message W_C randomly selected from $\{1,...,2^{nR_C}\}$, with an average power of P_C. The actual codebook used by C depends on how the backbone is exploited, as seen in the following sections. The capacity of the backhaul link is denoted by C_L. We assume full synchronization between the transmissions of A and C at the receiver of B, as well as at the receiver of E (the latter is rather an unfavorable assumption for our security scheme).

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 $X_{U,i}$. In our case $U \in \{A, C\}$ and $V \in \{B, D, E\}$. The signal received by B and E, respectively, at the $i-$th symbol ($i = 1, ..., n$) 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, such that if the node U transmits with power P_U, the received SNR at the node V is:

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

All channel gains are assumed constant during transmission of a codeword and known at the receive side. When deriving the rates that can be achieved with perfect secrecy, we will assume that all the channel gains of interest h_{AB}, h_{CB}, h_{AE}, h_{CE} are fixed, deterministic and known to A, while the channel gains h_{CB} and h_{CD} are known to C. Finally, the capacity of a Gaussian channel with SNR equal to x is denoted as

$$\mathcal{C}(x) = \log(1 + x) \quad (4)$$

The base station B decodes through a mapping $g(\mathbf{Y}_B)$: $\mathbb{C}^n \rightarrow \{1, ..., 2^{nR_A}\}$. A rate $R_A = R_{A,s}$ is said to be achievable with perfect secrecy with respect to E if for $n \rightarrow \infty$, the decoding error vanishes $P_e = P[g(\mathbf{Y}_B) \neq W_A] \rightarrow 0$ and the uncertainty Δ, measured as the conditional entropy of W_A at E normalized over the unconditional entropy satisfies $\Delta = \frac{H(W_A|\mathbf{Y}_E)}{H(W_A)} \rightarrow 1$.

The following function will be useful: Let V be a multiple–access channel (MAC) with two users U_1 and U_2, then:

$$S_{U_1V}(R_{U_2}) \quad (5)$$

denotes the supremum of the achievable rates from U_1 to V for a given transmission rate R_{U_2}, which is not necessarily decodable by V (i. e., it might not belong to the corresponding MAC capacity region). For the case of AWGN, given the SNRs γ_{U_1V} and γ_{U_2V}, the function is given by:

$$S_{U_1V}(R_{U_2}) = \begin{cases} \mathcal{C}(\gamma_{U_1V}) & \text{if } R_{U_2} \leq \mathcal{C}\left(\frac{\gamma_{U_2V}}{1+\gamma_{U_1V}}\right) \\ \mathcal{C}(\gamma_{U_1V}+\gamma_{U_2V})-R_{U_2} & \text{if } \mathcal{C}\left(\frac{\gamma_{U_2V}}{1+\gamma_{U_1V}}\right) < R_{U_2} \leq \mathcal{C}(\gamma_{U_2V}) \\ \mathcal{C}\left(\frac{\gamma_{U_1V}}{1+\gamma_{U_2V}}\right) & \text{if } R_{U_2} > \mathcal{C}(\gamma_{U_2V}) \end{cases} \quad (6)$$

B. Perfect secrecy without a backhaul link ($C_L = 0$)

In this section, we consider a basic scenario with no backhaul link ($C_L = 0$). In such a case, the base station C transmits with a given 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 complex Gaussian independent with zero mean and power P_C. This codebook conveys information to a downlink user D. The considered approach coincides with the one considered in [2] 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 (6), the result of [2] (Theorem 3) can be restated as follows.

Proposition 1: If C transmits with rate R_C and $C_L = 0$, the rate $R_{A,s}(R_C)$ is achievable with perfect secrecy[2]:

$$R_{A,s}(R_C) = (S_{AB}(R_C) - S_{AE}(R_C))^+ \quad (7)$$

From (7) it can be seen that, for fixed γ_{AE}, γ_{CE} and R_C, the achievable secrecy rate is enhanced if the achievable rate $S_{AB}(R_C)$ increases The next sections show how such an increase can be achieved by exploiting the backhaul, and the corresponding impact on the secrecy capacity.

III. Perfect Secrecy with Large-Capacity Backhaul Link ($C_L \geq R_C$)

In this section, the large-capacity backhaul link implies $C_L \geq R_C$. As in the previous section, C transmits codewords from a given randomly generated Gaussian codebook. Since $C_L \geq R_C$, C can communicate the current codeword $\mathbf{X}_C(W_C)$ to B by using the backhaul. Therefore, B can effectively cancel $\mathbf{X}_C(W_C)$ from the received signal, leading to the equivalent received signal

$$Y_{B,i} = h_{AB}X_{A,i} + N_{B,i}, \quad (8)$$

This implies that for any R_C we have:

$$S_{AB}(R_C) = S_{AB}(0) = \mathcal{C}(\gamma_{AB}) \quad (9)$$

Proposition 2: If C transmits with rate R_C and $C_L \geq R_C$, the rate $R_{A,s}(R_C)$ is achievable with perfect secrecy:

$$R_{A,s}(R_C) = (\mathcal{C}(\gamma_{AB}) - S_{AE}(R_C))^+ \quad (10)$$

Proof: Follows directly from Theorem 3 of [2].

The rate (10) is plotted in Fig. 2 along with $\mathcal{C}(\gamma_{AB})$ and $S_{AE}(R_C)$. The specific numbers used for Fig. 2 are $\gamma_{AB} = 7, \gamma_{AE} = 15, \gamma_{CE} = 10$. The result can be interpreted in terms of the rate $R_x = \mathcal{C}(\gamma_{AB}) - R_{A,s}$ that the node A must devote to the aim of "confounding" the eavesdropper E and thus achieving rate $R_{A,s}$ with perfect secrecy. For this particular example, even if always $C_L \geq R_C$, the secrecy rate $R_{A,s}$ is zero until $S_{AE}(R_C) \geq \mathcal{C}(\gamma_{AE})$. As R_C increases, $R_{A,s}$ increases linearly and stays at the maximum value $(\mathcal{C}(\gamma_{AB}) - \mathcal{C}(\gamma_{AE}/(1 + \gamma_{BE})))^+$. This is because for $R_C \geq \mathcal{C}(\gamma_{CE})$, the signal from C acts as a Gaussian noise with power γ_{CE} and is thus the worst–case jammer on E [9]

[2]We define $(x)^+ = x$ if $x > 0$ and $(x)^+ = 0$ otherwise.

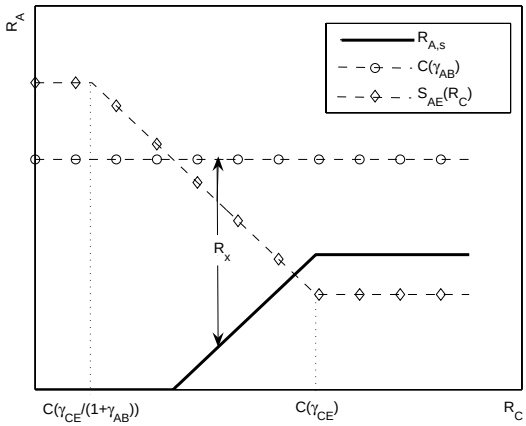

Fig. 2. The achievable secrecy rate $R_{A,s}$ in Proposition 2. Here $R_x = \mathcal{C}(\gamma_{AB}) - R_{A,s}$ is the amount of information spent by A to "confound" the eavesdropper E in order to achieve a rate $R_{A,s}$ with perfect secrecy.

[10]. It is easily seen that, with ideal backhaul, the secrecy rate is a non-decreasing function of the downlink rate R_C.

A final remark is in order. For the chosen SNRs in the example on Fig. 2, if in addition we assume $\gamma_{CB} \leq \gamma_{CE}$, then by using the results from II-B it can be shown that in the absence of the infrastructure, the secrecy rate $R_{A,s}$ is identically zero. Clearly, for ideal backhaul, we see that the value of γ_{CB} is irrelevant for determining $R_{A,s}$, which is not the case for finite C_L, as the next section shows.

IV. Perfect Secrecy with Finite–Capacity Backhaul Link ($C_L < R_C$)

When $C_L < R_C$, different strategies can be devised by base station C in order to provide B with information about the transmitted waveform $\mathbf{X}_C$, and thus improve the uplink rate $R_{A,s}$ (recall the discussion about (7)). Here we investigate two different strategies, one based on source coding arguments and one on channel coding.

A. Quantization–based strategy

With this strategy, the base station C employs, as in the previous sections, a randomly generated Gaussian codebook. The selected codeword $\mathbf{X}_C(W_C)$ is quantized via a rate-C_L Gaussian codebook defined by the test channel $\hat{X}_{C,i} = X_{C,i} + Q_i$ where Q_i is i.i.d. complex Gaussian quantization noise with power σ_q^2. The index is then sent over the backhaul link to B. The quantization codebook is assumed to be known to base station B, which decompresses the signal $\hat{\mathbf{X}}_C$. Overall, the equivalent signal seen at B over both the wireless and wired channel in a given time instant i can be written as

$$\tilde{Y}_{B,i} = \begin{bmatrix} Y_{B,i} \\ \hat{X}_{C,i} \end{bmatrix} = \begin{bmatrix} h_{AB} & h_{CB} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} X_{A,i} \\ X_{C,i} \end{bmatrix} + \begin{bmatrix} N_i \\ Q_i \end{bmatrix} \quad (11)$$

The quantization error power σ_Q^2 is found by imposing the condition $I(X_C; \hat{X}_C) = C_L$, which is necessary to have successful compression (via joint typicality vector quantization) with high probability. This entails $\sigma_Q^2 = P_C/(2^{C_L} - 1)$. and the equivalent SNR on the channel $\hat{X}_C$ in (11) is defined:

$$\gamma_Q = \frac{P_C}{\sigma_q^2} = 2^{C_L} - 1. \quad (12)$$

Let $S_{AB}^Q(R_C)$ denote the maximum achievable rates from A to B for a given transmission rate R_C when the quantization strategy is used (recall (6)). This follows from the MAC capacity region of the vector MAC channel (11):

$$S_{AB}^Q(R_C) = \begin{cases} \mathcal{C}(\gamma_{AB}) & \text{if } R_C \leq \mathcal{C}\left(\frac{\gamma_{CB}}{1+\gamma_{AB}} + \gamma_Q\right) \\ \mathcal{C}_{sum} - R_C & \text{if } \mathcal{C}\left(\frac{\gamma_{CB}}{1+\gamma_{AB}} + \gamma_Q\right) < R_C \leq \mathcal{C}(\gamma_{CB} + \gamma_Q) \\ \mathcal{C}_{sum} - \mathcal{C}(\gamma_{CB} + \gamma_Q) & \text{if } R_C > \mathcal{C}(\gamma_{CB} + \gamma_Q) \end{cases} \quad (13)$$

where

$$\mathcal{C}_{sum} = I(X_A, X_C; \tilde{Y}_B) = \log_2\left(2^{C_L}(1 + \gamma_{AB}) + \gamma_{CB}\right) \quad (14)$$

is the maximum sum-rate. The mutual information in (14) has been obtained by using the chain rule and the fact that, with known X_C, X_A is conditionally independent of $\hat{X}_C$, as

$$\begin{aligned} I(X_A, X_C; \tilde{Y}_B) &= I(X_C; \tilde{Y}_B) + I(X_A; \tilde{Y}_B | X_C) = \\ &= I(X_C; \tilde{Y}_B) + I(X_A; Y_B | X_C) = \\ &= \log_2\left(1 + \frac{\gamma_{CB}}{1 + \gamma_{AB}} + \gamma_Q\right) + \log_2(1 + \gamma_{AB}). \end{aligned}$$

Recalling the results in Proposition 1, we can state:

Proposition 3: If C transmits with rate R_C and a quantization–based strategy is used, the rate $R_{A,s}(R_C)$ is achievable with perfect secrecy:

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

From the results of Proposition 2, it can be seen that the secrecy rate with $C_L < R_C$ des not increase with R_C. It is also easy to show that for $C_L \to \infty$, the rate (15) equals (10).

B. Superposition–based strategy

Here we investigate a channel coding-based strategy to exploit the non-ideal backhaul link. The strategy is based on a rate–splitting encoding at C so that, differently from the previous sections, here C makes provisions to facilitate the transmission of information over the backhaul. The message W_C is transmitted by sending two independent messages W_{C1}, W_{C2} with rates R_{C1}, R_{C2}, respectively such that:

$$R_C = R_{C1} + R_{C2}. \quad (16)$$

In particular, the two messages are combined by using superposition coding, such that the ith symbol sent by C is:

$$X_{C,i} = \sqrt{\alpha} X_{C1,i} + \sqrt{1 - \alpha} X_{C2,i}, \quad (17)$$

where α is the power–division coefficient and $0 \leq \alpha \leq 1$. In order to select a power allocation α that is consistent with the rate allocation (R_{C1}, R_{C2}), we need to account for the downlink channel γ_{CD} between C and D. In particular, to simplify the problem, we assume that messages W_{C1} and W_{C2} are decoded, in this specific order, by using sequential decoding at D, such that their rates are selected as

$$R_{C1} = \log_2\left(1 + \frac{\alpha\gamma_{CD}}{1 + (1 - \alpha)\gamma_{CD}}\right) \quad (18)$$

$$R_{C2} = \log_2(1 + (1 - \alpha)\gamma_{CD}) \quad (19)$$

$$R_C = \log_2(1 + \gamma_{CD}) \quad (20)$$

While broadcasting the messages W_{C1} W_{C2} over the wireless medium, C also transmits one of those messages through the

backhaul. The objective is, for given fixed R_C, to determine the design of the superposition coding (α, R_{C1}, R_{C2}) and the information sent over the backhaul link in order to maximize the achievable secrecy rate $R_{A,s}$ on the link $A-B$. For deriving $R_{A,s}$, it is known from Proposition 1 that one should attempt to maximize the achievable rate between A and B for given R_C (i.e., $S_{AB}(R_C)$). Then, it should be (trivially) noted that C should transmit over the backhaul at the maximum possible rate C_L. Thus, one of the rates R_{C1} or R_{C2} should be equal to C_L and the other $R_C - C_L$. With the transmission of type (17), there are two options, namely sending either W_{C2} or W_{C1} over the backhaul.

1) W_{C2} sent over the backhaul link: In this case we set $R_{C2} = C_L$, which, from (19), results in

$$\alpha = \alpha_2 = 1 - \frac{2^{C_L} - 1}{\gamma_{CD}} \tag{21}$$

and also implies $R_{C1} = R_C - C_L$. After B uses W_{C2} to cancel $\mathbf{X}_{C2}(W_{C2})$, the received signal at B is:

$$Y_{B,i} = h_{AB}X_{A,i} + h_{CB}\sqrt{\alpha_2}X_{C1,i} + N_{B,i} \tag{22}$$

with the following MAC capacity region:

$$R_A \leq \mathcal{C}(\gamma_{AB}) \tag{23}$$

$$R_{C1} = R_C - C_L \leq \mathcal{C}(\alpha_2\gamma_{CB}) \tag{24}$$

$$R_A + R_C - C_L \leq \mathcal{C}(\gamma_{AB} + \alpha_2\gamma_{CB}) \tag{25}$$

In order to evaluate the maximum rate R_A for a given R_C, we have to assume two different cases: (*i*) $R_C - C_L \leq \mathcal{C}(\alpha_2\gamma_{CB})$: This condition is equivalent to

$$R_C \leq \mathcal{C}\left(2^{C_L}\gamma_{CB}\right) \tag{26}$$

In this case, the maximum achievable rate $A-B$ is:

$$S_{AB}^{(\alpha_2)}(R_C) = \min\{\mathcal{C}(\gamma_{AB}), \mathcal{C}(\gamma_{AB} + \alpha_2\gamma_{CB}) - (R_C - C_L)\}; \tag{27}$$

(*ii*) $R_C - C_L \leq \mathcal{C}((1-\alpha_2)\gamma_{CB})$: In this case, B can only decode W_{C2}, but not W_{C1}, such that X_{C1} should be treated as noise at A, resulting in:

$$S_{AB}^{(\alpha_2)}(R_C) = \mathcal{C}\left(\frac{\gamma_{AB}}{1 + \alpha_2\gamma_{CB}}\right) \tag{28}$$

Note that, while for the third region in (6) the maximum achievable rate is constant (independent of R_C), in (28) $S_{AB}^{(\alpha_2)}(R_C)$ depends on R_C through α_2.

2) W_{C1} sent over the backhaul link: When W_{C1} is sent over the backhaul, we set $R_{C1} = C_L$, resulting in

$$\alpha = \alpha_1 = \frac{1 - 2^{-C_L}}{1 - 1/(1 + \gamma_{CD})} \tag{29}$$

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

$$Y_{B,i} = h_{AB}X_{A,i} + h_{CB}(1 - \sqrt{\alpha_1})X_{C2,i} + N_{B,i} \tag{30}$$

Using similar arguments as for the case when X_{C2} is sent over the backhaul, the maximal achievable rate $A-B$ is: (*i*) $R_C \leq \mathcal{C}(\gamma_{CB})$:

$$S_{AB}^{(\alpha_1)}(R_C) = \min\{\mathcal{C}(\gamma_{AB}), \mathcal{C}(\gamma_{AB} + (1-\alpha_1)\gamma_{CB}) - (R_C - C_L)\}; \tag{31}$$

(*ii*) $R_C > \mathcal{C}(\gamma_{CB})$:

$$S_{AB}^{(\alpha_1)}(R_C) = \mathcal{C}\left(\frac{\gamma_{AB}}{1 + (1-\alpha_1)\gamma_{CB}}\right) \tag{32}$$

Some further comment on the optimizations entailed by (37) is in order. From the assumption $R_C > C_L$ it follows that

$$\alpha_2 > 1 - \alpha_1, \tag{33}$$

which implies that for large R_C, sending X_{C21} over the backhaul offers higher achievable rates R_A, that is:

$$S_{AB}^{(\alpha_1)}(R_C) > S_{AB}^{(\alpha_2)}(R_C) \quad \text{for} \quad R_C > \mathcal{C}(\gamma_{CB}) \tag{34}$$

On the other hand, if R_C is chosen such that:

$$\mathcal{C}(\gamma_{AB}) = \mathcal{C}(\gamma_{AB} + \alpha_2\gamma_{CB}) - (R_C - C_L) \tag{35}$$

then (33) implies that $\mathcal{C}(\gamma_{AB} + (1-\alpha_1)\gamma_{CB}) - (R_C - C_L) < \mathcal{C}(\gamma_{AB} + \alpha_2\gamma_{CB}) - (R_C - C_L)$ and therefore:

$$S_{AB}^{(\alpha_2)}(R_C) > S_{AB}^{(\alpha_1)}(R_C). \tag{36}$$

3) Achievable secrecy rate: For deriving the secrecy rate achievable with the superposition strategy, the following should be noted. For given R_C and for the rate splitting strategy, it can be shown that the maximum rate $S_{AE}(R_C)$ decodable by E from A is the same that we would have if A used a single-rate Gaussian codebook. This is because from (16),(18), and (19), it can be proved that any of the superposed messages is decodable if and only if the other is. Therefore, $S_{AE}(R_C)$ is defined as in (6) and we can state:

Proposition 4: If C transmits with rate R_C and a superposition-based strategy is used, the rate $R_{A,s}(R_C)$ is achievable with perfect secrecy:

$$R_{A,s}(R_C) = \left(\max_{i=1,2}\left\{S_{AB}^{(\alpha_i)}(R_C)\right\} - S_{AE}(R_C)\right)^+ \tag{37}$$

V. Numerical Results

Here we provide some numerical examples for performance of the proposed confidential transmission schemes in the presence of a finite–capacity backbone. We start by considering the maximum achievable rates from A to B (with no confidentiality constraints) $S_{AB}^{Q}(R_C)$ (13) (quantization–based scheme), $S_{AB}^{(\alpha_1)}(R_C)$ (31)-(32) and $S_{AB}^{(\alpha_2)}(R_C)$ (27)-(28) (superposition scheme) for given parameters γ_{AB}, γ_{CB}, C_L. Compared to the case with $C_L = 0$, it can be seen that exploiting the backhaul link largely improve the achievable rates to the intended destination B, which in turn from Proposition 1 enhances the secrecy rate (see Fig. 4 and discussion below). It can also be concluded that, 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 superposition coding approach outperforms the quantization-based approach for any R_C. . On this note, we have that for lower R_C it is more convenient to send W_{C2} over the backhaul ($S_{AB}^{(\alpha_2)}(R_C) > S_{AB}^{(\alpha_1)}(R_C)$) and viceversa for larger R_C. This can be explained by noticing that selection of the message to be sent over the backhaul corresponds to an amount of power that is cancelled from the signal $h_{CB}X_C$ at the receiver of B. Therefore, if W_{C2} is sent over the backbone (Sec. IV-B1),

then the optimal choice of α_2 in (37) is such that a minimal amount of power is cancelled and the remaining wireless power of the signal from C ($|h_{CB}|^2 P_C \alpha_2$) is maximum. Such a high remaining power provides larger decodable rates R_C to be transmitted from C to B, see (26), and that is why $S_{AB}^{(\alpha_2)}(R_C) > S_{AB}^{(\alpha_1)}(R_C)$ for relatively lower R_C. However, when (26) is violated, then X_{C1} acts as a noise and such a high power harms the rate achievable for large R_C. On the other hand, when W_{C1} is sent over the backhaul, the remaining power $|h_{CB}|^2 P_C(1-\alpha_1)$ is minimum possible, which lowers the achievable rates R_A at low R_C. Nevertheless, for very large and undecodable R_C, the uncancelled wireless signal from C starts to act as a noise and it therefore allows rates R_A that are superior to the case with α_2. A final important remark on Fig. 3 is that, if the rate R_C is large enough to be undecodable, the quantization strategy obtains a constant secrecy rate R_C, which can be proved (the proof is omitted here) to coincide with the asymptotic achievable for $R_C \to \infty$ of the superposition strategy.

Fig. 4 depicts the secrecy rates that are achievable for different values of C_L and the two proposed strategies. The first thing to be noted is that the secrecy rates are markedly improved for both strategies when $C_L > 0$ compared to the Noise–Forwarding strategy [2] ($C_L = 0$). Up to certain rate R_C, all proposed strategies have the same achievable secrecy rate as the case of ideal backhaul link ($C_L > R_C$). This maximum value of R_C at hand is larger for the superposition than for the quantization strategy. This is because, even when $R_C > C_L$, the superposition strategy can still admit some uncancelled wireless power without degrading the rate S_{AB}. Moreover, it is seen that, if C_L is sufficiently large, then, for some values of R_C, both strategies are able to attain the secrecy rate that is attainable in the case of ideal backhaul.

As a final remark, it should be noted that the price to be paid for the better secrecy performance of the superposition strategy is that C should explicitly account for the rate of A to B when transmitting to D and create the codebooks accordingly. For the quantization strategy, the transmission $C-D$ is oblivious with respect to the secrecy objective, which could be an asset for practical system implementation.

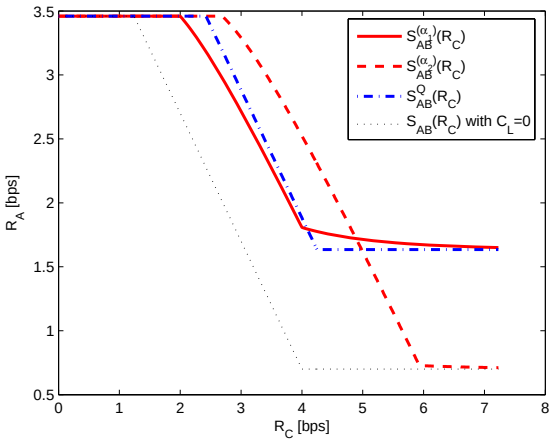

Fig. 3. Maximum achievable rates from A to B (without confidentiality constraints) $S_{AB}^{(\alpha_1)}(R_C)$, $S_{AB}^{(\alpha_2)}(R_C)$ and $S_{AB}^{Q}(R_C)$ with $\gamma_{AB} = 10, \gamma_{CB} = 15$ and $C_L = 2$ [bps]. As a reference, the function $S_{AB}(R_C)$ with $C_L = 0$ is also plotted.

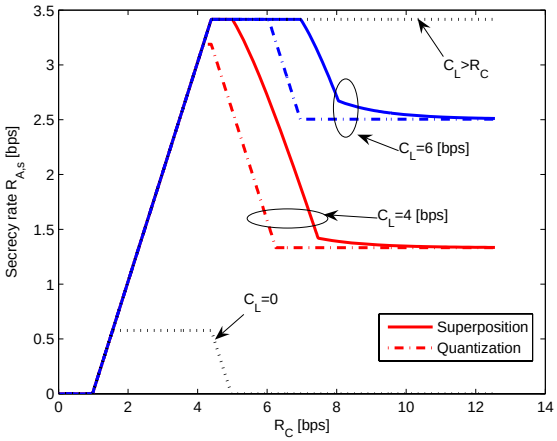

Fig. 4. Achievable secrecy rates by superposition and quantization for different C_L ($\gamma_{AB} = 30, \gamma_{CB} = 60, \gamma_{AE} = 40, \gamma_{CE} = 20$).

VI. Conclusions

In this paper, we have investigated the possibility to provide secure (confidential) communications in infrastructure networks by exploiting the simultaneous scheduling of uplink and downlink transmission. The intentionally generated interference is mitigated at the intended receiver by exploiting the finite-capacity backbone connecting the base stations. Two strategies have been proposed and their achievable rates with perfect secrecy compared. It has been shown that relevant advantages can be accrued by appropriately designing the transmission strategy to be used by the downlink interfering transmission via superposition coding, as compared to the use of basic single-rate codebooks.

References

[1] 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.

[2] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," submitted [arXiv:cs/0612044v1]

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

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel," *IEEE Trans. Inform. Theory*, vol. 24, pp. 451–456, Jul. 1978.

[5] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inform. Theory* (ISIT), 2006.

[6] P. K. Gopala, L. Lai, H. El Gamal, "On the secrecy capacity of fading channels," submitted [arXiv:cs/0702112v1]

[7] 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].

[8] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Techn. Conference*, vol. 3, pp. 1906-1910, Sept. 2005.

[9] M. L. Jørgensen, B. Yanakiev, G. E. Kirkelund, P. Popovski, H. Yomo, T. Larsen, "Shout to secure: physical–layer wireless security with known interference", in *Proc. IEEE Globecom 2007*.

[10] O. Simeone and P. Popovski,"Secure communications via cooperative base stations," to appear in *IEEE Commun. Letters*.

[11] S. Shamai, O. Somekh, O. Simeone, A. Sanderovich, B.M. Zaidel and H. V. Poor, "Cooperative multi-cell networks: impact of limited-capacity backhaul and inter-users links," in *Proc. Joint Workshop on Coding and Communications*, Dürnstein, Austria, October 14 - 16, 2007.