MIMO Multi-User Secrecy Rate Analysis

Giovanni Geraci, Sarabjot Singh, Jeffrey G. Andrews, Jinhong Yuan, and Iain B. Collings

***Abstract*—In this paper, we consider the broadcast channel with confidential messages and eavesdroppers (BCCE), where a multi-antenna base station simultaneously communicates to multiple potentially malicious users, in the presence of external eavesdroppers randomly located according to a Poisson point process (PPP). By using techniques from stochastic geometry and random matrix theory, we obtain explicit expressions for the secrecy outage probability and mean secrecy rate achievable with regularized channel inversion precoding. We show that both these metrics scale as $\frac{\lambda_e}{\sqrt{N}}$, where N is the number of transmit antennas and λ_e is the density of external eavesdroppers.**

***Index Terms*—Physical layer security, broadcast channel, linear precoding, stochastic geometry, random matrix theory.**

I. Introduction

Multiuser multiple-input multiple-output (MIMO) wireless techniques have received tremendous attention as a way to achieve high spectral efficiency in current mobile communication systems such as Long Term Evolution (LTE) [1]. Due to the broadcast nature of the physical medium, wireless multiuser communications are very susceptible to eavesdropping, and it is critical to secure the transmitted information. Security has traditionally been achieved at the network layer with cryptographic schemes. However, classical cryptography might not be suitable in large dynamic networks, since it requires key distribution and management, and complex encryption/decryption algorithms [2]. A method that exploits the characteristics of wireless channels, such as fading and noise, was proposed as an alternative to achieve perfect secrecy without requiring encryption keys [3], [4]. This technique is known as physical layer security, and it has recently become a very active area of research.

The underlying channel for multiuser MIMO wireless communications is referred to as the MIMO broadcast channel (BC) [5]. Physical layer security was considered to protect the confidentiality of data in the BC, by introducing the broadcast channel with confidential messages (BCC), where users can act maliciously as eavesdroppers [6], [7]. A large-system analysis of the secrecy rates achievable with regularized channel inversion (RCI) precoding in the BCC was performed via random matrix theory (RMT) tools in [8], [9], where the number of malicious users K and the number of antennas N was assumed to grow to infinity in a fixed ratio, and where eavesdropping was assumed from the malicious users only. The presence of external eavesdroppers and its effect on the secure connectivity in random wireless networks were studied, among others, in [10]–[12] via stochastic geometry (SG), but the system model did not account for the potentially malicious behavior of the users. In a practical scenario, both malicious users and external nodes can act as eavesdroppers. A physical layer security system designed by considering either one of them should be regarded as vulnerable. For these reasons, it is of critical importance to study broadcast channels with confidential messages and external eavesdroppers.

In this paper, we introduce the broadcast channel with confidential messages and eavesdroppers (BCCE) to model a scenario where both malicious users and randomly located external nodes can act as eavesdroppers. We use results from both stochastic geometry and random matrix theory to study the performance of RCI precoding in the BCCE. Stochastic geometry is a powerful tool to study a large network with a random distribution of external eavesdroppers [13], whereas random matrix theory enables a deterministic abstraction of the physical layer, for a fixed network topology [14]. We obtain the probability of secrecy outage and the mean secrecy rate achievable by RCI precoding in the BCCE under Rayleigh fading, for the two cases of non-colluding and colluding eavesdroppers. We find that both (i) the probability of secrecy outage, and (ii) the rate loss due to the presence of external eavesdroppers scale as $\frac{\lambda_e}{\sqrt{N}}$, where N is the number of transmit antennas and λ_e is the density of external eavesdroppers, irrespective of their collusion strategy.

II. System Model

In this section, we first recall some results on the MISO BCC, where malicious users connected to the network can act as eavedroppers. Then we introduce the MISO BCCE, where not only malicious users but also nodes external to the network can act as eavesdroppers. In this paper we consider a single cell scenario. Cellular networks are studied in [15].

A. Preliminaries: Broadcast Channel with Confidential Messages (BCC)

We first consider the downlink of a narrowband MISO BCC, consisting of a base station with N antennas, which simultaneously transmits K independent confidential messages to K spatially dispersed single-antenna users. In this model, transmission takes place over a block fading channel, and the transmitted signal is $\mathbf{x} = [x_1, \dots, x_N]^T \in \mathbb{C}^{N\times 1}$. We assume homogeneous users, i.e., each user experiences the same received signal power on average, thus the model assumes that their distances from the transmitter are the same and unitary.

G. Geraci and J. Yuan are with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, Australia (e-mail: g.geraci@student.unsw.edu.au, j.yuan@unsw.edu.au).

S. Singh and J. G. Andrews are with the Wireless Networking and Communications Group (WNCG), The University of Texas at Austin, TX (email: sarabjot@utexas.edu, jandrews@ece.utexas.edu).

I. B. Collings is with the Wireless and Networking Technologies Laboratory, CSIRO ICT Centre, Sydney, Australia (email: iain.collings@csiro.au).

This work was done while the first author was with the WNCG, The University of Texas at Austin, TX.

978-1-4799-2003-7/14/$31.00 ©2014 IEEE

The received signal at user k is given by

$$y_k = \sum_{j=1}^{N} h_{k,j} x_j + n_k \tag{1}$$

where $h_{k,j} \sim \mathcal{CN}(0,1)$ is the i.i.d. channel between the j^{th} transmit antenna element and the k^{th} user, and $n_k \sim \mathcal{CN}(0,\sigma^2)$ is the noise seen at the k^{th} receiver. The corresponding vector equation is

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} \tag{2}$$

where $\mathbf{H} = [\mathbf{h}_1, \ldots, \mathbf{h}_K]^\dagger$ is the $K \times N$ channel matrix. We assume $\mathbb{E}[\mathbf{n}\mathbf{n}^\dagger] = \sigma^2 \mathbf{I}_K$, where $\mathbf{I}_K$ is the $K \times K$ identity matrix, define the SNR $\rho \triangleq 1/\sigma^2$, and impose the long-term power constraint $\mathbb{E}[\|\mathbf{x}\|^2] = 1$. For each user k, we denote by $\mathcal{M}_k = \{1, \ldots, k-1, k+1, \ldots, K\}$ the set of remaining users. In general, the behavior of the users cannot be determined by the BS. As a worst-case scenario, we assume that for each user k, all users in $\mathcal{M}_k$ can cooperate to jointly eavesdrop on its signal. Since the set of malicious users $\mathcal{M}_k$ can perform joint processing, they can be seen as a single equivalent malicious user M_k with $K-1$ receive antennas.

In this paper, we consider regularized channel inversion (RCI) precoding. In RCI precoding, the transmitted vector $\mathbf{x}$ is obtained at the BS by performing a linear processing on the vector of confidential messages $\mathbf{u} = [u_1, \ldots, u_K]^T$, whose entries are chosen independently, satisfying $\mathbb{E}[|u_k|^2] = 1$. The transmitted signal $\mathbf{x}$ after RCI precoding can be written as $\mathbf{x} = \mathbf{W}\mathbf{u}$, where $\mathbf{W} = [\mathbf{w}_1, \ldots, \mathbf{w}_K]$ is the $N \times K$ RCI precoding matrix, given by [16]

$$\mathbf{W} = \frac{1}{\sqrt{\zeta}} \mathbf{H}^\dagger \left(\mathbf{H}\mathbf{H}^\dagger + N\xi \mathbf{I}_K \right)^{-1} \tag{3}$$

and $\zeta = \text{tr}\left\{ \mathbf{H}^\dagger \mathbf{H} \left(\mathbf{H}^\dagger \mathbf{H} + N\xi \mathbf{I}_N \right)^{-2} \right\}$ is a long-term power normalization constant. The function of the regularization parameter $\xi \in \mathbb{R}$ is to achieve a tradeoff between the signal power at the legitimate user and the crosstalk at the other unintended users for each message.

Due to cooperation, interference cancellation can be performed at the equivalent malicious user M_k, which does not see any undesired signal term apart from the received noise. As a result, a secrecy rate achievable for user k by RCI precoding is given by [8]

$$R_{\text{BCC},k} = \left[\log_2\left(1+\gamma_k\right) - \log_2\left(1+\gamma_{M_k}\right) \right]^+, \tag{4}$$

where $[\cdot]^+ \triangleq \max(\cdot, 0)$.

In (4), γ_k and γ_{M_k} are the signal-to-interference-plus-noise ratios for the message u_k at the legitimate receiver k and the equivalent malicious user M_k, respectively, given by

$$\gamma_k = \frac{\rho \left| \mathbf{h}_k^\dagger \mathbf{w}_k \right|^2}{1 + \rho \sum_{j \neq k} \left| \mathbf{h}_k^\dagger \mathbf{w}_j \right|^2} \quad \text{and} \quad \gamma_{M_k} = \rho \left\| \mathbf{H}_k \mathbf{w}_k \right\|^2, \tag{5}$$

and $\mathbf{H}_k$ is obtained from $\mathbf{H}$ by removing the k^{th} row.

The secrecy rate of the RCI precoder in the large-system regime was studied in [8], where both the number of receivers K and the number of transmit antennas N approach infinity, with their ratio $\beta = K/N$ being held constant. The value of β represents the network load. Let $\rho > 0$, $\beta > 0$, and let $R_{\text{BCC},k}$ be the secrecy rate achievable by RCI precoding in the BCC defined in (4). Then [8]

$$\left| R_{\text{BCC},k} - R^\circ_{\text{BCC}} \right| \xrightarrow{\text{a.s.}} 0, \quad \text{as} \quad N \to \infty, \quad \forall k \tag{6}$$

where R°_{BCC} denotes the secrecy rate in the large-system regime, given by

$$R^\circ_{\text{BCC}} = \left[\log_2 \frac{1+\gamma^\circ}{1+\gamma^\circ_M} \right]^+, \tag{7}$$

and where

$$\begin{aligned} \gamma^\circ &= g\left(\beta,\xi\right) \frac{\rho + \frac{\rho\xi}{\beta}\left[1+g\left(\beta,\xi\right)\right]^2}{\rho + \left[1+g\left(\beta,\xi\right)\right]^2} \\ \gamma^\circ_M &= \frac{\rho}{\left[1+g\left(\beta,\xi\right)\right]^2}, \end{aligned} \tag{8}$$

with $g\left(\beta,\xi\right) = \frac{1}{2}\left[\sqrt{\frac{(1-\beta)^2}{\xi^2} + \frac{2(1+\beta)}{\xi} + 1} + \frac{1-\beta}{\xi} - 1 \right]$.

B. Broadcast Channel with Confidential Messages and External Eavesdroppers (BCCE)

We now consider the MISO BCCE, by including external single-antenna eavesdroppers in the system. The external eavesdroppers are assumed to be distributed on the two-dimensional plane according to a Poisson point process (PPP) Φ_e of density λ_e. Fig. 1 shows an example of BCCE, where the BS is at the origin, and the users lie on a disc of radius 1. As a worst-case scenario, we assume that each eavesdropper can cancel the interference caused by the remaining $K-1$ messages. Assuming that the BS lies at the origin, the SINR $\gamma_{e,k}$ for the k^{th} message at a generic eavesdropper located at e is then given by

$$\gamma_{e,k} = \frac{\left| \mathbf{h}_e^\dagger \mathbf{w}_k \right|^2}{\|e\|^\eta \sigma^2} \tag{9}$$

where $\mathbf{h}_e^\dagger$ is the channel vector between the base station and the eavesdropper in e, and it takes into account the Rayleigh fading, and η is the path loss exponent. In this paper we assume $\eta = 4$, which is a reasonable value in a shadowed urban area [17]. The analysis for the general case can be found in the longer version of this paper [18].

The precoding vector $\mathbf{w}_k$ is calculated independently of $\mathbf{h}_e^\dagger$, therefore they are independent isotropic random vectors. The channel $\mathbf{h}_e^\dagger$ has unit norm, whereas the precoding vector $\mathbf{w}_k$ has norm $\frac{1}{\sqrt{K}}$ because it is obtained after the normalization $\|\mathbf{W}\|^2 = \sum_{k=1}^{K} \|\mathbf{w}_k\|^2 = 1$. The inner product $\mathbf{h}_e^\dagger \mathbf{w}_k$ is a linear combination of N complex normal random variables, therefore $\left| \mathbf{h}_e^\dagger \mathbf{w}_k \right|^2 \sim \exp(\frac{1}{K})$.

In the following, we consider two types of external eavesdroppers, namely non-colluding eavesdroppers and colluding eavesdroppers. In the non-colluding case, the eavesdroppers individually overhear the communication without centralized processing. In the colluding eavesdroppers case, all eavesdroppers are able to jointly process their received message at a central data processing unit, and they can, therefore, be seen

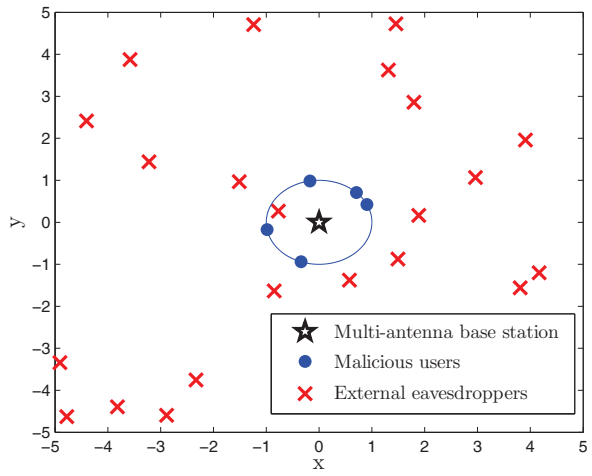

Fig. 1. Example of a BCCE with $K = 5$ malicious users and a density of external eavesdroppers $\lambda_e = 0.2$.

as a single multi-antenna eavesdropper. The secrecy rate R_k achievable by the k^{th} user in the BCCE is given by

$$R_k = \left[\log_2\left(1+\gamma_k\right) - \log_2\left(1+\max\left(\gamma_{M_k}, \gamma_{E,k}\right)\right)\right]^+, \tag{10}$$

where $\gamma_{E,k}$ is the SINR at the eavesdoppers for the k^{th} message. The secrecy rate R_k is therefore affected by the maximum of the SINR γ_{M_k} at the alliance of malicious users and the SINR $\gamma_{E,k}$ at the alliance of external eavesdroppers. In the case of non-colluding eavesdroppers, $\gamma_{E,k}$ is the SINR at the strongest eavesdropper. After interference cancellation, each eavesdropper receives the useful signal embedded in noise, and the optimal receive strategy at the colluding eavesdroppers is maximal ratio combining (MRC) which yields to an SINR $\gamma_{E,k} = \sum_{e\in\Phi_e} \gamma_{e,k}$ given by the sum of the SINRs $\gamma_{e,k}$ at all eavesdroppers.

III. Probability of Secrecy Outage

In this section, we derive the secrecy outage probability, i.e., the probability that the secrecy rate R_k achievable by user k with RCI precoding in the BCCE is zero, for both cases of non-colluding and colluding eavesdroppers. Then we study the secrecy outage probability in the large-system regime, where the number of users K and the number of transmit antennas N both grow to infinity in a fixed ratio β. We determine how the number of antennas N must scale in order to guarantee a given secrecy outage probability. The secrecy outage probability for user k is defined as

$$\mathcal{O}_k \triangleq \mathbb{P}(R_k = 0) = \begin{cases} 1 & \text{if } \gamma_k \le \gamma_{M_k} \\ \mathbb{P}(\gamma_{E,k} \ge \gamma_k \,|\, \gamma_k) & \text{otherwise} \end{cases} \tag{11}$$

In most cases, RCI precoding ensures $\gamma_k > \gamma_{M_k}$ [8], and therefore, the secrecy outage probability is often given by the probability that R_k is driven to zero by the presence of external eavesdroppers.

A. Non-colluding Eavesdroppers

In the case of non-colluding eavesdroppers, $\gamma_{E,k}$ is the SINR at the strongest eavesdropper E, given by

$$\gamma_{E,k} = \max_{e\in\Phi_e} \gamma_{e,k} = \max_{e\in\Phi_e} \frac{\left|\mathbf{h}_e^\dagger \mathbf{w}_k\right|^2}{\|e\|^\eta \sigma^2}. \tag{12}$$

In this case, $\mathcal{O}_k$ is the probability that any eavesdropper has an SINR greater than or equal to the SINR of the legitimate user k. We obtain the following result for the large-system secrecy outage probability $\mathcal{O}^\circ$ in the presence of non-colluding eavesdroppers.

Theorem 1. *The secrecy outage probability in the presence of non-colluding eavesdroppers satisfies*

$$|\mathcal{O}_k - \mathcal{O}^\circ| \xrightarrow{a.s.} 0, \quad as \;\; N\to\infty, \quad \forall k \tag{13}$$

where

$$\mathcal{O}^\circ = \begin{cases} 1 & \text{if } \gamma^\circ \le \gamma_M^\circ \\ 1 - \exp\left[-\frac{2\pi^{\frac{3}{2}}\lambda_e}{\eta\sqrt{N\beta\sigma^2\gamma^\circ}}\right] & \text{otherwise} \end{cases} \tag{14}$$

Proof: See Appendix A. ∎

Corollary 1. *If $\gamma^\circ > \gamma_M^\circ$, then (i) the number of transmit antennas required in order to guarantee a large-system secrecy outage probability $\mathcal{O}^\circ < \epsilon$ in the presence of non-colluding eavesdroppers is $N > \left(\frac{\mu\lambda_e}{\epsilon\sqrt{\gamma^\circ}}\right)^2$, where $\mu \triangleq \frac{\pi^{\frac{3}{2}}}{2\sqrt{\beta\sigma^2}}$, and (ii) the large-system secrecy outage probability $\mathcal{O}^\circ$ decays as $\frac{1}{\sqrt{N}}$.*

B. Colluding Eavesdroppers

The colluding eavesdroppers case represents a worst-case scenario. In this case, all eavesdroppers can perform joint processing, and they can therefore be seen as a single multi-antenna eavesdropper. After interference cancellation, each eavesdropper receives the useful signal embedded in noise, and the optimal receive strategy at the colluding eavesdroppers is maximal ratio combining (MRC). This yields to an SINR $\gamma_{E,k}$ at the colluding eavesdroppers given by

$$\gamma_{E,k} = \frac{1}{\sigma^2}\sum_{e\in\Phi_e} \|e\|^{-\eta}\left|\mathbf{h}_e^\dagger \mathbf{w}_k\right|^2. \tag{15}$$

We now obtain the large-system secrecy outage probability $\mathcal{O}^\circ$ in the presence of colluding eavesdroppers.

Theorem 2. *The secrecy outage probability in the presence of colluding eavesdroppers satisfies*

$$|\mathcal{O}_k - \mathcal{O}^\circ| \xrightarrow{a.s.} 0, \quad as \;\; N\to\infty, \quad \forall k \tag{16}$$

where

$$\mathcal{O}^\circ = \begin{cases} 1 & \text{if } \gamma^\circ \le \gamma_M^\circ \\ 1 - 2\mathrm{Q}\left(\mu\lambda_e\sqrt{\frac{\pi}{2N\gamma^\circ}}\right) & \text{otherwise} \end{cases} \tag{17}$$

Proof: See Appendix B. ∎

Corollary 2. *Let $\gamma^\circ > \gamma_M^\circ$ and $\eta = 4$, then (i) the number of transmit antennas required in order to guarantee a large-system secrecy outage probability $\mathcal{O}^\circ < \epsilon$ in the presence of*

colluding eavesdroppers is $N > \left(\frac{\mu\lambda_e}{\epsilon\sqrt{\gamma^\circ}}\right)^2$*, and (ii) the large-system outage probability* $\mathcal{O}^\circ$ *decays as* $\frac{1}{\sqrt{N}}$.

Remark 1. *By comparing the results in Corollary 1 and Corollary 2, we can conclude that (i) the collusion among eavesdroppers does not significantly affect the number of transmit antennas* N *required to meet a given probability of secrecy outage in the large-system regime, and (ii) increasing the density of eavesdroppers* λ_e *by* n *times requires a value of* N n^2 *times as large in order to meet a given probability of secrecy outage.*

IV. Mean Secrecy Rates

In this section, we derive the mean secrecy rates, averaged over the location of the external eavesdroppers, achievable by RCI precoding in the BCCE, for both cases of non-colluding and colluding eavesdroppers. We then derive a bound on the secrecy rate loss due to the presence of external eavesdroppers.

We now obtain the large-system mean secrecy rate R° achievable by RCI precoding in the BCCE.

Theorem 3. *The mean secrecy rate achievable for user* k *by RCI precoding in the BCCE satisfies*

$$|\mathbb{E}_{\Phi_e}[R_k] - R^\circ| \xrightarrow{a.s.} 0, \quad as \quad N \to \infty, \quad \forall k, \tag{18}$$

where R° *denotes the mean secrecy rate in the large-system regime, given by*

$$R^\circ = \begin{cases} 0 & \text{if } \gamma^\circ \le \gamma_M^\circ \\ \log_2 \dfrac{(1+\gamma^\circ)^{1-\mathcal{O}^\circ}}{(1+\gamma_M^\circ)^{1-\mathcal{P}^\circ}} & \text{otherwise} \\ -\displaystyle\int_{\gamma_M^\circ}^{\gamma^\circ} \log_2(1+y) f_{\gamma_{E,k}}(y)\, dy & \end{cases} \tag{19}$$

In (19), $\mathcal{P}^\circ$ *is the probability that the SINR* $\gamma_{E,k}$ *at the external eavesdroppers is greater than or equal to the large-system SINR* γ_M° *at the malicious users, given by*

$$\begin{aligned} \mathcal{P}^\circ &\triangleq \mathbb{P}(\gamma_{E,k} \ge \gamma_M^\circ) \\ &= \begin{cases} 1 - \exp\left(-\frac{\mu\lambda_e}{\sqrt{N\gamma_M^\circ}}\right) & \text{n.c.e.} \\ 1 - 2\mathrm{Q}\left(\mu\lambda_e\sqrt{\frac{\pi}{2N\gamma_M^\circ}}\right) & \text{c.e.} \end{cases} \end{aligned} \tag{20}$$

where "n.c.e" and "c.e." stand for "non-colluding eavesdroppers" and "colluding eavesdroppers", respectively, and $f_{\gamma_{E,k}}(y)$ *is the distribution of the SINR at the external eavesdroppers, given by*

$$f_{\gamma_{E,k}}(y) = \begin{cases} \frac{\mu\lambda_e y^{-\frac{3}{2}}}{2\sqrt{N}} \exp\left(-\frac{\mu\lambda_e}{\sqrt{Ny}}\right) & \text{n.c.e.} \\ \frac{\mu\lambda_e y^{-\frac{3}{2}}}{2\sqrt{N}} \exp\left(-\frac{\pi\mu^2\lambda_e^2}{4Ny}\right) & \text{c.e.} \end{cases} \tag{21}$$

Proof: See Appendix C. ∎

By comparing the large-system mean secrecy rate of the BCCE in (19) to the large-system secrecy rate of the BCC without external eavesdroppers in (7), we can evaluate the secrecy rate loss Δ_e due to the presence of external eavesdroppers, defined as

$$\Delta_e \triangleq R^\circ_{\text{BCC}} - R^\circ. \tag{22}$$

We now obtain an upper bound on the secrecy rate loss Δ_e.

Corollary 3. *The secrecy rate loss* Δ_e *due to the presence of external eavesdroppers satisfies*

$$\Delta_e \le \Delta_e^{UB} \triangleq \frac{\nu\lambda_e}{\sqrt{N}}, \tag{23}$$

where ν *is a constant independent of* N*,* λ_e*, and of the cooperation strategy at the eavesdroppers, given by*

$$\nu = \mu\left[\frac{R^\circ_{BCC}}{\sqrt{\gamma^\circ}} + \left(\sqrt{\gamma^\circ} - \sqrt{\gamma^\circ_M}\right)^+\right]. \tag{24}$$

Proof: See Appendix D. ∎

Remark 2. *It follows from Corollary 3 that, irrespective of the collusion strategy at the external eavesdroppers, (i) as the number* N *of transmit antennas grows, the secrecy rate loss* Δ_e *tends to zero as* $\frac{1}{\sqrt{N}}$*, and (ii) increasing the density of eavesdroppers* λ_e *by a factor* n *requires increasing* N *by a factor* n^2 *in order to meet a given value of* Δ_e^{UB}.

V. Numerical Results

In this section, we provide simulation results to show the probability of secrecy outage and the secrecy rate with RCI precoding in the BCCE under various conditions. In the simulations, the value of ξ that maximizes R°_{BCC} was used. The optimal value for ξ in the BCCE is studied in the longer version of this paper [18].

In Fig. 2 we compare the simulated probability of outage $\mathcal{O}_k$ under non-colluding and colluding eavesdroppers, respectively, to the large-system results $\mathcal{O}^\circ$ provided in Theorem 1 and Theorem 2, respectively. We observe that for $\lambda_e = 0.1$ and small probabilities of secrecy outage, (i) $N > \left(\frac{\mu\lambda_e}{0.1\sqrt{\gamma^\circ}}\right)^2 = 34$ yields to a secrecy outage probability smaller than 0.1, (ii) the secrecy outage probability decays as $\frac{1}{\sqrt{N}}$, and (iii) the collusion of eavesdroppers does not significantly affect the probability of secrecy outage. All these observations are consistent with Corollary 1, Corollary 2, and Remark 1.

In Fig. 3 we compare the simulated ergodic per-user secrecy rate under non-colluding and colluding eavesdroppers, to the large-system results from Theorem 3, for $\beta = 1$, $\rho = 10$dB, and various values of λ_e. We note that the accuracy of the large-system analysis increases with N. Moreover, we observe that the expectation of the per-user secrecy rate increases with N, and this benefit is more for larger values of λ_e. This happens because the mean received power at each external eavesdropper scales as $\frac{1}{\beta N}$, hence having more transmit antennas makes the system more robust against external eavesdroppers.

In Fig. 4 we compare the simulated per-user secrecy rate of (i) the BCCE with non-colluding eavesdroppers, (ii) the BCCE with colluding eavesdroppers, and (iii) the BCC without external eavesdroppers, for $\beta = 1$, $\rho = 10$dB, and various values of λ_e. We note that in the BCC, the per-user secrecy rate is almost constant with N, for a fixed network load β. On

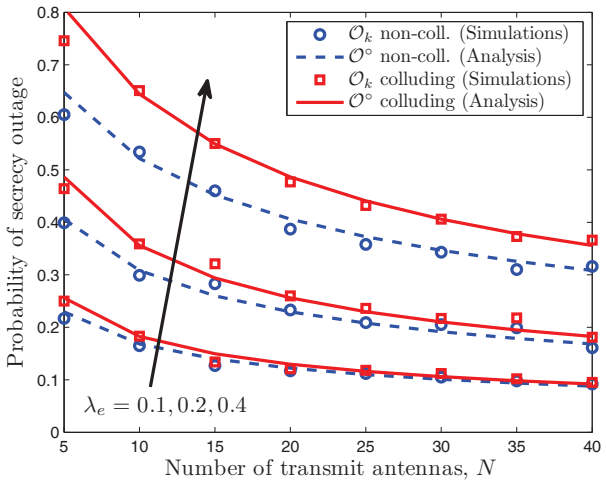

Fig. 2. Comparison between the simulated probability of outage $\mathcal{O}_k$ and the large-system results $\mathcal{O}^\circ$ provided in Theorem 1 and Theorem 2, for a network load $\beta = 1$, an SNR $\rho = 10$dB, and various values of λ_e.

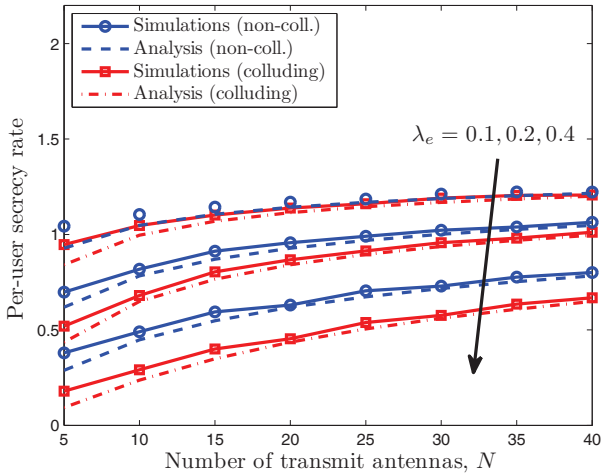

Fig. 3. Comparison between the simulated ergodic per-user secrecy rate $\mathbb{E}[R_k]$ under non-colluding and colluding eavesdroppers, and the large-system results R° from Theorem 3, for a network load $\beta = 1$, an SNR $\rho = 10$dB, and various values of λ_e.

the other hand, the per-user secrecy rate of the BCCE increases with N. Again, this happens because the mean received power at each external eavesdropper scales as $\frac{1}{\beta N}$, hence having more transmit antennas makes the system more robust against external eavesdroppers. We also note that for higher densities of eavesdroppers λ_e, larger values of N are required to achieve a given per-user secrecy rate of the BCCE. More precisely, increasing λ_e by a factor 2, requires increasing N by a factor 4. Moreover, the collusion of external eavesdroppers does not affect the scaling law of the mean rate. These observations are consistent with Remark 2.

VI. Conclusion

In this paper, we introduced the broadcast channel with confidential messages and external eavesdroppers (BCCE), where

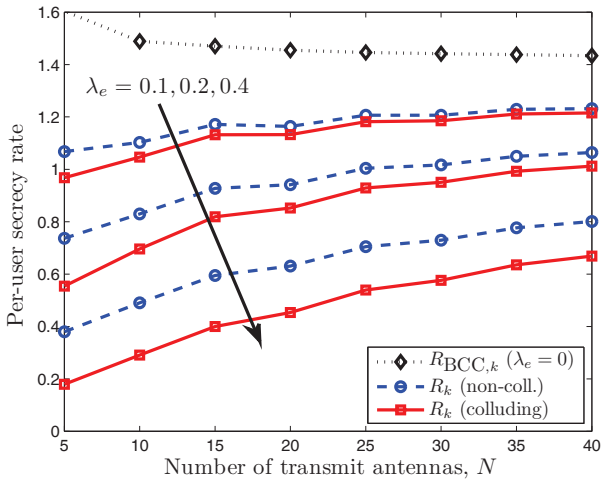

Fig. 4. Comparison between the simulated ergodic per-user secrecy rates of: (i) the BCCE with non-colluding eavesdroppers, (ii) the BCCE with colluding eavesdroppers, and (iii) the BCC without external eavesdroppers, for a network load $\beta = 1$, an SNR $\rho = 10$dB, and various values of λ_e.

a multi-antenna base station simultaneously communicates to multiple malicious users, in the presence of randomly located external eavesdroppers. We showed that under Rayleigh fading a large number of transmit antennas N drives both the probability of secrecy outage and the rate loss due to the presence of external eavesdroppers to zero. Increasing the density of eavesdroppers λ_e by a factor n requires increasing N by a factor n^2 to meet a given probability of secrecy outage and a given mean secrecy rate. Using the developed analysis, we clearly established the importance of the number of transmit antennas at the BS to make communications robust against malicious users and external eavesdropping nodes.

Appendix

A. Sketch of proof of Theorem 1

If $\gamma_k \leq \gamma_{M_k}$, then R_k in (10) is zero w.p. 1. If $\gamma_k > \gamma_{M_k}$, we have $\gamma_{E,k} = \max_e \gamma_{e,k}$, therefore

$$\begin{aligned}\mathcal{O}_k &= \mathbb{P}\left(\gamma_{E,k} \geq \gamma_k \,\middle|\, \gamma_k\right) \\ &= 1 - \mathbb{E}_{\Phi_e}\left[\prod_{x\in\Phi_e}\left[1 - \mathbb{P}\left(\gamma_{x,k} \geq \gamma_k \,\middle|\, \gamma_k\right)\right]\right] \\ &= 1 - \exp\left[-2\pi\lambda_e \int_0^\infty y \exp\left(-N\beta\sigma^2\gamma_k\, y^\eta\right) dy\right] \\ &= 1 - \exp\left[-\frac{2\pi\lambda_e \Gamma\left(\frac{2}{\eta}\right)}{\eta(N\beta\sigma^2\gamma_k)^{\frac{2}{\eta}}}\right]. \end{aligned} \tag{25}$$

Theorem 1 then follows by noting that $|\gamma_k - \gamma^\circ| \xrightarrow{a.s.} 0$ and $|\gamma_{M_k} - \gamma_M^\circ| \xrightarrow{a.s.} 0$ as $N \to \infty$, and by the continuous mapping theorem [19].

B. Sketch of proof of Theorem 2

For the case of colluding eavesdroppers, the Laplace transform of the SINR is [20]

$$\begin{aligned}\mathcal{L}_{\gamma_{E,k}}(s) &= \mathbb{E}\left[\exp\left(-\frac{s}{\sigma^2}\sum_{x\in\Phi_e}\|x\|^{-4}\left|\mathbf{h}_x^\dagger\mathbf{w}_k\right|^2\right)\right]\\ &= \exp\left\{-2\pi\lambda_e\int_{\mathbb{R}^2}\mathbb{E}_{\mathbf{h}}\left[1-\exp\left(-\frac{s}{\sigma^2}\left|\mathbf{h}_x^\dagger\mathbf{w}_k\right|^2\|x\|^{-4}\right)\right]x\,dx\right\}\\ &= \exp\left(-\frac{\pi^2\lambda_e}{2}\sqrt{\frac{s}{N\beta\sigma^2}}\right). \end{aligned} \tag{26}$$

By inverse transform one can obtain the pdf [21]

$$f_{\gamma_{E,k}}(y) = \frac{\pi^{\frac{3}{2}}\lambda_e y^{-\frac{3}{2}}}{4\sqrt{N\beta\sigma^2}}\exp\left(-\frac{\pi^4\lambda_e^2}{16N\beta\sigma^2 y}\right), \tag{27}$$

which integrated yields the cumulative distribution function $F_{\gamma_{E,k}}(y)$, from which the secrecy outage probability can be calculated as $\mathcal{O}_k = F_{\gamma_{E,k}}(\gamma_k)$. Theorem 2 follows by noting that $|\gamma_k - \gamma^\circ| \xrightarrow{a.s.} 0$ and $|\gamma_{M_k} - \gamma_M^\circ| \xrightarrow{a.s.} 0$ as $N\to\infty$, and by the continuous mapping theorem [19].

C. Sketch of proof of Theorem 3

We note from (10) that when $\gamma_k \le \gamma_{M_k}$, it is $R_k = 0$ $\forall\,\gamma_{E,k}$. When $\gamma_k > \gamma_{M_k}$, the mean secrecy rate is given by

$$\begin{aligned}&\mathbb{E}_{\Phi_e}\left[R_k|\gamma_k>\gamma_{M_k}\right]\\ &= \mathbb{E}_{\Phi_e}\left[\max\left[\log_2\left(1+\gamma_k\right)-\log_2\left(1+\max\left(\gamma_{E,k},\gamma_{M_k}\right)\right),0\right]\right]\\ &= \mathbb{P}\left(\gamma_{E,k}<\gamma_k\right)\log_2\left(1+\gamma_k\right)-\mathbb{P}\left(\gamma_{E,k}<\gamma_{M_k}\right)\log_2\left(1+\gamma_{M_k}\right)\\ &\quad-\int_{\gamma_{M_k}}^{\gamma_k}\log_2(1+y)f_{\gamma_{E,k}}(y)\,dy\\ &= \log_2\frac{\left(1+\gamma_k\right)^{1-\mathcal{O}_k}}{\left(1+\gamma_{M_k}\right)^{1-\mathcal{P}_k}}-\int_{\gamma_{M_k}}^{\gamma_k}\log_2(1+y)f_{\gamma_{E,k}}(y)\,dy\end{aligned} \tag{28}$$

where $\mathcal{P}_k \triangleq \mathbb{P}\left(\gamma_{E,k}\ge\gamma_{M_k}\right)$ is the probability that the SINR at the external eavesdroppers is greater than or equal to the SINR at the malicious users, and $f_{\gamma_{E,k}}(y)$ is the distribution of the SINR at the external eavesdroppers, given by (27) for colluding eavesdroppers, and by

$$f_{\gamma_{E,k}}(y) = \frac{\partial\mathbb{P}\left(\gamma_{E,k}<y\right)}{\partial y} = \frac{\pi^{\frac{3}{2}}\lambda_e y^{-\frac{3}{2}}}{4\sqrt{N\beta\sigma^2}}\exp\left(-\frac{\pi^{\frac{3}{2}}\lambda_e}{2\sqrt{N\beta\sigma^2 y}}\right) \tag{29}$$

for non-colluding eavesdroppers. Theorem 3 follows by replacing γ_k and γ_{M_k} with their respective deterministic equivalents γ° and γ_M°, by applying the continuous mapping theorem, the Markov inequality, and the Borel-Cantelli lemma [19].

D. Sketch of proof of Corollary 3

For $\gamma^\circ \le \gamma_M^\circ$, we have $R_{\text{BCC}}^\circ = 0$ and $R^\circ = 0$, therefore $\Delta_e = 0$. For $\gamma^\circ > \gamma_M^\circ$ and fixed ξ, irrespective of the cooperation strategy at the eavesdroppers, we have

$$\begin{aligned}\Delta_e &= \log(1+\gamma^\circ)^{\mathcal{O}^\circ}-\log(1+\gamma_M^\circ)^{\mathcal{P}^\circ}+\int_{\gamma_M^\circ}^{\gamma^\circ}\log_2(1+y)f_{\gamma_{E,k}}(y)\,dy\\ &\le \mathcal{O}^\circ R_{\text{BCC}}^\circ + \frac{\mu\lambda_e}{2\sqrt{N}}\int_{\gamma_M^\circ}^{\gamma^\circ} y^{-\frac{1}{2}}\,dy\\ &= \left[1-\exp\left(-\frac{\mu\lambda_e}{\sqrt{N\gamma^\circ}}\right)\right]R_{\text{BCC}}^\circ + \frac{\mu\lambda_e}{\sqrt{N}}\left(\sqrt{\gamma^\circ}-\sqrt{\gamma_M^\circ}\right)\\ &\le \mu\left[\frac{R_{\text{BCC}}^\circ}{\sqrt{\gamma^\circ}}+\left(\sqrt{\gamma^\circ}-\sqrt{\gamma_M^\circ}\right)\right]\frac{\lambda_e}{\sqrt{N}}.\end{aligned} \tag{30}$$

REFERENCES

[1] C. Lim, T. Yoo, B. Clerckx, B. Lee, and B. Shim, "Recent trend of multiuser MIMO in LTE-advanced," *IEEE Comms. Mag.*, vol. 51, no. 3, pp. 127–135, Mar. 2013.

[2] Y.-S. Shiu, S.-Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Comm.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[3] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[5] G. Caire and S. Shamai, "On the achievable throughput of a multiantenna Gaussian broadcast channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1691–1706, July 2003.

[6] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, pp. 1346–1359, Mar. 2013.

[7] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5669–5680, Sep. 2012.

[8] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, "Large system analysis of linear precoding in MISO broadcast channels with confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1660–1671, Sep. 2013.

[9] G. Geraci, A. Y. Al-nahari, J. Yuan, and I. B. Collings, "Linear precoding for broadcast channels with confidential messages under transmit-side channel correlation," *IEEE Comms. Letters*, vol. 17, no. 6, pp. 1164–1167, June 2013.

[10] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Dec. 2011.

[11] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[12] P. Pinto, J. Barros, and M. Win, "Secure communication in stochastic wireless networks – Part I: Connectivity," *IEEE Trans. Inf. Forensics and Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[13] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic geometry and its applications*, 2nd ed. New York, NY: Wiley & Sons, 1996.

[14] R. Couillet and M. Debbah, *Random Matrix Theory Methods for Wireless Communications*. Cambridge University Press, 2011.

[15] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," submitted to *IEEE Trans. Commun.*, 2013, available arXiv:1307.7211.

[16] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, "A vector-perturbation technique for near-capacity multiantenna multiuser communication - Part I: Channel inversion and regularization," *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 195–202, Jan. 2005.

[17] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 1st ed. IEEE Press, 1996.

[18] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in the broadcast channel with confidential messages and external eavesdroppers," to appear in *IEEE Trans. Wireless Commun.*, 2013, available arXiv:1306.2101.

[19] P. Billingsley, *Probability and measure,* 3rd ed. Hoboken, NJ: John Wiley & Sons, Inc., 1995.

[20] M. Haenggi, J. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.

[21] E. Sousa and J. Silvester, "Optimum transmission ranges in a direct-sequence spread-spectrum multihop packet radio network," *IEEE J. Sel. Areas Commun.*, vol. 8, no. 5, pp. 762–771, June 1990.