Physical Layer Security in Full-Duplex Cellular Networks

Ayda Babaei*, A. Hamid Aghvami*, Arman Shojaeifard†, and Kai-Kit Wong†
*Centre for Telecommunications Research, King's College London, London, United Kingdom
†Communications and Information Systems Group, University College London, London, United Kingdom
E-Mail: *ayda.babaei@kcl.ac.uk *hamid.aghvami@kcl.ac.uk †a.shojaeifard@ucl.ac.uk †kai-kit.wong@ucl.ac.uk

***Abstract*—In this work, we investigate the physical layer security (PHYLS) performance of full-duplex (FD) cellular networks, where the downlink (DL) and uplink (UL) occur over the same radio-frequency (RF) resources. Here, the locations of the base stations (BSs) and mobile terminals (MTs) are drawn from stationary Poisson point processes (PPPs). Moreover, the eavesdroppers (EDs) locations are unknown to the network, and are thus modeled from an independent PPP. We characterize the signal-to-interference-plus-noise ratio (SINR) distributions at the reference BS, MT, and most malicious EDs. Accordingly, we develop explicit expressions for the secrecy rates in both UL and DL of the FD cellular network under consideration. Our finding show that the choice of FD versus HD operation, in addition to improving the spectral efficiency, can enhance the secrecy rate, particularly for ultra-dense deployments.**

I. Introduction

Cellular networks have become increasingly dense in order to account for the rapid rise in mobile data traffic. Due to the broadcasting nature of wireless mediums, such networks have become more vulnerable to malicious listeners, rendering security an essential design criteria [1]. Conventionally, security measures have been implemented through the higher layers of the protocol stack using cryptographic authentication [2]. However, this approach introduces many challenges such as high cost and vulnerability to attacks [3], [4].

In order to overcome the aforementioned challenges, physical layer security (PHYLS) has emerged as an additional security measure to transmit data confidentially. Originally, Wyner presented the application of wiretrap channel for secrecy rate of a point-to-point communication channel [5]. Later on, Csiszar and Korner extended this work to broadcast channels transmitting both common and confidential messages [6]. According to these works, the secrecy rate can be guaranteed when the legitimate receiver enjoys a better channel than a potential eavesdropper (ED).

In the recent years, many works have analyzed the PHYLS performance in different wireless networks, such as the study of the achievable secrecy rate in the presence of artificial noise [7], relay wiretap channel [8], and with colluding EDs [9], [10]. Most works in the literature, however, study conventional half-duplex (HD) systems. With increasing number of users and data rate demands, full-duplex (FD) wireless communications, has become a topic of interest [11]. In FD systems, the downlink (DL) and (UL) occur over the same radio-frequency (RF) resources, hence, the spectral efficiency performance can be improved depending on the severity of the added interference [12], [13].

978-1-5386-3531-5/17/$31.00 © 2017 IEEE

Motivated by the above, in this work, we study the PHYLS performance of a FD cellular network. We define the system parameters, intended signals, interference terms, and received signal-to-interference-plus-noise ratio (SINR) distributions for each part of the network. Consequently, we derive the received rate for each element, and in turn the secrecy rate for both UL and DL modes of communications. By utilizing the proposed framework and with the aid of numerical simulations, we draw network design insights, including depicting the specific scenarios in which the FD mode of communications may improve the secrecy rate versus its HD counterpart.

II. System Model

In this work, we consider a FD cellular network where the base stations (BSs) and mobile terminals (MTs) are deployed according to independent stationary Poisson point processes (PPPs) ϕ_s and ϕ_m with spatial densities λ_s and λ_m, respectively. The locations of the EDs are not known to the network, therefore in this work, they are modelled according to a PPP ϕ_f with spatial density λ_f [14]. Moreover, the EDs are considered to operate independently which means they do not exchange their observations [9], [15].

Based on the Slivnyak-Mecke theorem [16], we perform the DL analysis for a typical MT o considered to be located at the center. Let $l \in \phi_s$, $k \in \phi_m$, and $j \in \phi_f$ denote the locations of the BS l, MT k, and ED j, respectively. We consider the cellular association strategy based on the maximum received SINR under global frequency reuse [17]. For single-tier deployments, this is equivalent to cellular association based on the closest transmitter-receiver distances. Mathematically, this can be expressed as

$$b = \arg\max\left(\|l-o\|^{-\alpha}\right),\ l \in \phi_s \tag{1}$$

where b, $\|.\|$ and α (> 2) denote the tagged BS, Euclidean distance, and path-loss exponent, respectively. The UL analysis, on the other hand, is performed at the tagged BS b.

Let p_s and p_m denote the BS and MT (fixed) transmit powers, respectively. The DL channel power gains from the BS l at the MT k and ED j are $h_{l,k}$ and $h_{l,j}$, respectively. Further, we denote the UL channel power gains from the MT k at the BS l and ED j using $g_{k,l}$ and $g_{k,j}$, respectively. The cross-mode channel power gains from the BS l at the BS b, and from the MT k at the MT o are represented using $h_{l,b}$ and $g_{k,o}$, respectively. In addition, in the order given, the loop-back interference (LI) at the BS l and MT k are represented using $h_{l,l}$ and $g_{k,k}$. All channels are considered to undergo independent Rayleigh fading. Moreover, additive white Gaussian noise (AWGN) with variance σ^2 is considered at all receivers.

It should be noted that due to the cellular association process, the scheduled MTs are inherently correlated [18]. Here, conditioning on the spatial constraints, we assume that the set of scheduled MTs follows from an independent stationary PPP [19]. Further, we consider the most malicious ED which receives the strongest SINR and dominates other EDs [20].

The SINR in the DL at MT o can accordingly be written as

$$\gamma_o = \frac{X_o}{I_{d,d} + I_{u,d} + I_{o,o} + \sigma^2} \tag{2}$$

where

$$X_o = p_s h_{b,o} r_{b,o}^{-\alpha} \tag{3}$$

$$I_{d,d} = \sum_{l \in \phi^{(s)} \setminus \{b\}} p_s h_{l,o} r_{l,o}^{-\alpha} \tag{4}$$

$$I_{u,d} = \sum_{k \in \phi^{(m)} \setminus \{o\}} p_m g_{k,o} r_{k,o}^{-\alpha} \tag{5}$$

and

$$I_{o,o} = p_m g_{o,o}. \tag{6}$$

On the other hand, the SINR in the UL at BS b is given by

$$\gamma_b = \frac{X_b}{I_{u,u} + I_{d,u} + I_{b,b} + \sigma^2} \tag{7}$$

where

$$X_b = p_m g_{o,b} {r_{o,b}}^{-\alpha} \tag{8}$$

and

$$I_{u,u} = \sum_{k \in \phi^{(m)} \setminus \{o\}} p_m g_{k,b} {r_{k,b}}^{-\alpha} \tag{9}$$

$$I_{d,u} = \sum_{l \in \phi^{(s)} \setminus \{b\}} p_s h_{l,b} {r_{l,b}}^{-\alpha} \tag{10}$$

$$I_{b,b} = p_s h_{b,b}. \tag{11}$$

We define the SINR in DL at the most malicious ED e as

$$\gamma_e = \frac{X_e}{T_{d,d} + T_{u,d} + \sigma^2} \tag{12}$$

where

$$X_e = p_s h_{b,e} {r_{b,e}}^{-\alpha} \tag{13}$$

$$T_{d,d} = \sum_{l \in \phi^{(s)} \setminus \{b\}} p_s h_{l,e} {r_{l,e}}^{-\alpha} \tag{14}$$

and

$$T_{u,d} = \sum_{k \in \phi^{(m)}} p_m g_{k,e} r_{k,e}^{-\alpha}. \tag{15}$$

On the other side, the SINR in the UL at the most malicious ED c is given by

$$\gamma_c = \frac{X_c}{T_{u,u} + T_{d,u} + \sigma^2} \tag{16}$$

where

$$X_c = p_m g_{o,c} {r_{o,c}}^{-\alpha} \tag{17}$$

$$T_{u,u} = \sum_{k \in \phi^{(m)} \setminus \{o\}} p_m g_{k,c} r_{k,c}^{-\alpha} \tag{18}$$

and

$$T_{d,u} = \sum_{l \in \phi^{(s)}} p_s h_{l,c} r_{l,c}^{-\alpha}. \tag{19}$$

Note that, due to the passivity of the EDs, there is no LI at the ED side.

III. Analysis

Considering the parameters defined in the previous section, we may calculate the average rate through the following expression [21]

$$C = \mathbb{E}\{\log\{1+\gamma\}\} = \frac{1}{\ln(2)} \int_0^\infty \frac{1 - F_\gamma(x)}{1+x}\, \mathrm{d}x \tag{20}$$

where $F_\gamma(x)$ denotes the cumulative distribution function (CDF) of the received SINR γ. We start by studying the average rates in the DL as follows.

Theorem 1. *Let $F_{\gamma_o}(x)$ and $F_{\gamma_e}(x)$ denote the CDF of received SINR at the intended MT o and the most malicious ED e in the DL, respectively. The corresponding average rates from the reference BS b, at the intended* *user o and the most malicious ED e are represented by C_{γ_o} and C_{γ_e}, and derived in (21) and (22), respectively.*

$$C_{\gamma_o} = \frac{2\pi\lambda_s}{\ln(2)} \int_0^\infty \int_0^\infty \frac{1}{1+x} \exp\left(\frac{-x\sigma^2}{p_s r^{-\alpha}}\right) \cdot \mathscr{L}_{I_{d,d}}\left(\frac{x}{p_s r^{-\alpha}}\right) \mathscr{L}_{I_{u,d}}\left(\frac{x}{p_s r^{-\alpha}}\right) \mathrm{d}x \cdot r \exp(-\pi\lambda_s r^2)\,\mathrm{d}r \tag{21}$$

$$C_{\gamma_e} = \frac{1}{\ln(2)} \int_0^\infty \frac{1}{1+x} \left[1 - \exp\left(-2\pi\lambda_f \cdot \int_0^\infty \exp\left(\frac{-x\sigma^2}{p_s r^{-\alpha}}\right) \mathscr{L}_{T_{u,d}}\left(\frac{x}{p_s r^{-\alpha}}\right) \cdot \mathscr{L}_{T_{d,d}}\left(\frac{x}{p_s r^{-\alpha}}\right) r\,\mathrm{d}r\right)\right] \mathrm{d}x \tag{22}$$

Proof: See Appendix A.

In the next step, we calculate the average rates in the UL.

Theorem 2. *Let $F_{\gamma_b}(x)$ and $F_{\gamma_c}(x)$ denote the CDF of the received SINR at the intended BS b and the most malicious ED c in the UL, respectively. The corresponding average rates at the intended BS b and the most malicious ED c are represented by C_{γ_b} and C_{γ_c}, and derived in (23) and (24), respectively.*

$$C_{\gamma_b} = \frac{2\pi\lambda_s}{\ln(2)} \int_0^\infty \int_0^\infty \frac{1}{1+x} \exp\left(\frac{-x\sigma^2}{p_m r^{-\alpha}}\right) \cdot \mathscr{L}_{I_{u,u}}\left(\frac{x}{p_m r^{-\alpha}}\right) \mathscr{L}_{I_{d,u}}\left(\frac{x}{p_m r^{-\alpha}}\right) \mathrm{d}x \cdot r \exp\left(-\pi\lambda_s r^2\right)\mathrm{d}r \tag{23}$$

$$C_{\gamma_c} = \frac{1}{\ln(2)} \int_0^\infty \frac{1}{1+x} \left[1 - \exp\left(-2\pi\lambda_f \cdot \int_0^\infty \exp\left(\frac{-x\sigma^2}{p_m r^{-\alpha}}\right) \mathscr{L}_{T_{u,u}}\left(\frac{x}{p_m r^{-\alpha}}\right) \cdot \mathscr{L}_{T_{d,u}}\left(\frac{x}{p_m r^{-\alpha}}\right) r\,\mathrm{d}r\right)\right] \mathrm{d}x \tag{24}$$

Proof: See Appendix B.

Based on *Theorem 1* and *Theorem 2*, and applying the Jensen's inequality, $\mathbb{E}\{\max(X,Y)\} \geq \max\{\mathbb{E}\{X\},\mathbb{E}\{Y\}\}$, we can calculate the DL average secrecy rate at the reference MT by [9], [22]

$$S_{DL} = [C_{\gamma_o} - C_{\gamma_e}]^+ \tag{25}$$

where $[x]^+ = \max\{x,0\}$ represents the fact that the secrecy rate is lower bounded. Moreover, the UL average secrecy rate at the reference BS is given by

$$S_{UL} = [C_{\gamma_b} - C_{\gamma_c}]^+ \,. \tag{26}$$

Remark. *According to Theorem 1 and Theorem 2 and equations (25) and (26) we can observe that increasing the spatial density of BSs improves the DL and UL secrecy rates. Furthermore, we note that the FD over HD secrecy rate gain increases with greater BS deployment density and with having a less populated ED field. In such cases, the inherent trade-off between higher spatial reuse versus added interference is more favourable, hence, the FD system achieves a higher secrecy rate gain over its HD counterpart.*

IV. Numerical Results

Here, we present numerical examples in order to assess the PHYLS performance of FD versus HD cellular networks for different settings of system parameters. Specifically, we study the impact of BSs and EDs spatial densities on the corresponding secrecy rate gain within a two-time-slot period. The noise power is assumed to be zero and the path loss exponent is set to three. Moreover, the maximum transmit powers of base station and mobile terminals are taken to be 30 dBm and 23 dBm, respectively. Moreover, we take into account the case in which the receivers possess arbitrary interference cancelation capability. Specifically, each receiver is capable of suppressing the cross-mode interference within a radius of ζ [23].

First, we investigate the impact of EDs spatial density on the FD versus HD secrecy rate gain. As illustrated in Fig. 1, by increasing the density of EDs, the corresponding gain decreases. However, this drop is negligible up to an approximate density of 10^{-3}. Therefore, despite the increase in the population of EDs up to a certain point, by means of an advanced receiver, a significant increased secrecy rate of over 23% is achievable. We consider this critical point for our following example.

Next, we study the effect of different BS spatial densities in Fig. 2. It can be seen that the BS deployment density has a profound impact on the corresponding FD over HD secrecy rate gain. Specifically, for dense cellular environments, the FD system offers a better PHYL performance than one which is operating in HD mode. Moreover, with advanced interference mitigation strategies, the FD technology facilitates an increase of more than 20% in secrecy rate in comparison to a HD system. This outcome is particularly interesting with the emergence of ultra-dense cellular setups.

V. Conclusions

In this work, we studied the PHYLS performance in a FD cellular network. The BSs, MTs, and EDs were modeled according to the PPP-based abstraction model. We derived explicit expressions for the secrecy rate in the DL and UL. The proposed framework was utilized to study the FD versus HD secrecy rate gain. Our findings indicated that the FD operation allows for significant improvements in the secrecy rate, particularly for ultra-dense deployments.

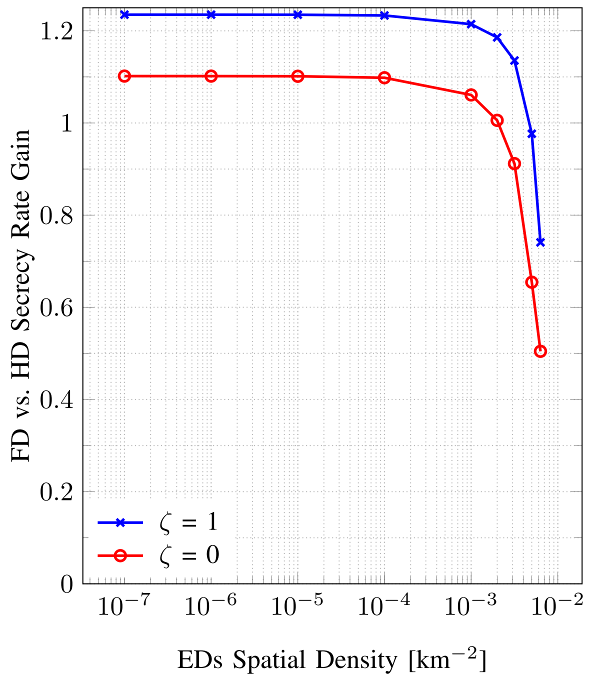

Fig. 1. Impact of EDs density on the FD versus HD secrecy rate gain. System parameters are: $\lambda_s = 10^{-4}$, $p_s = 30$ dBm, $p_m = 23$ dBm, $\alpha = 3$.

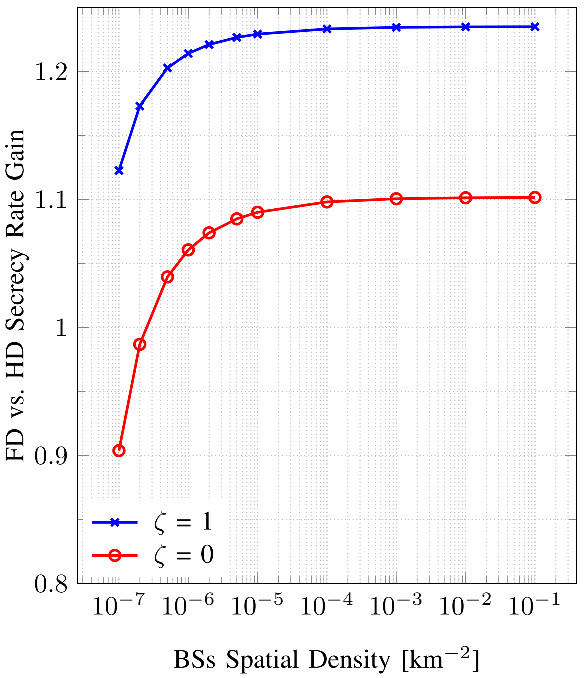

Fig. 2. Impact of BSs density on FD versus HD secrecy rate gain. System parameters are: $\lambda_f = 10^{-4}$, $p_s = 30$ dBm, $p_m = 23$ dBm, $\alpha = 3$.

VI. Appendix A

The CDF of received SINR at the intended user in the DL conditioned on $r_{b,o} = r$ is given by

$$\begin{aligned} &F_{\gamma_o|r_{b,o}=r}(x) = \Pr(\gamma_o < x|r_{b,o} = r) \\ &= 1 - \Pr\left(h_{b,o} > \frac{x}{p_s r^{-\alpha}}\left(I_{d,d} + I_{u,d} + I_{o,o} + \sigma^2\right)\right) \\ &\qquad = 1 - \exp\left(\frac{-x\sigma^2}{p_s r^{-\alpha}}\right)\mathscr{L}_{I_{d,d}}\left(\frac{x}{p_s r^{-\alpha}}\right) \\ &\qquad \cdot \mathscr{L}_{I_{u,d}}\left(\frac{x}{p_s r^{-\alpha}}\right)\mathscr{L}_{I_{o,o}}\left(\frac{x}{p_s r^{-\alpha}}\right). \end{aligned} \tag{27}$$

The probability density function (PDF) of the transmitter-receiver distance under the max-SINR cellular association strategy is given by

$$P_{r_{b,o}}(r) = 2\pi\lambda_s r \exp\left(-\pi\lambda_s r^2\right). \tag{28}$$

Hence, we can arrive at (21).

The CDF of received SINR at the most malicious ED in the DL $F_{\gamma_e}(x)$ is given by

$$\begin{aligned} &F_{\gamma_e}(x) = \Pr(\gamma_e < x) \\ &\qquad = \Pr\left(\max_{e\in\phi_f}\left\{\frac{p_s h_{b,e} r_{b,e}^{-\alpha}}{T_{d,d} + T_{u,d} + \sigma^2}\right\} < x\right) \\ &= \mathbb{E}_{\phi_f}\left\{\prod_{e\in\phi_f}\Pr\left(\frac{p_s h_{b,e} r_{b,e}^{-\alpha}}{T_{d,d} + T_{u,d} + \sigma^2} < x \mid \phi_f\right)\right\}. \end{aligned} \tag{29}$$

By employing the probability generating functional (PGFL) of a PPP and converting from Cartesian to polar coordinates, we can obtain

$$\begin{aligned} &F_{\gamma_e}(x) = \exp\Bigg(- 2\pi\lambda_f \\ &\cdot \int_0^\infty \left(1 - \Pr\left(\frac{p_s h_{b,e} r^{-\alpha}}{T_{d,d} + T_{u,d} + \sigma^2} < x\right)\right) r\,\mathrm{d}r\Bigg). \end{aligned} \tag{30}$$

The probability expression from the above can be expressed as

$$\begin{aligned} &1 - \Pr\left(\frac{p_s h_{b,e} r^{-\alpha}}{T_{d,d} + T_{u,d} + \sigma^2} < x\right) \\ &\quad = \Pr\left(h_{b,e} > \frac{x}{p_s r^{-\alpha}}\left(T_{d,d} + T_{u,d} + \sigma^2\right)\right) = \\ &\mathbb{E}_{T_{u,d}}\left\{\mathbb{E}_{T_{d,d}}\left\{\exp\left(\frac{-x}{p_s r^{-\alpha}}\left(T_{d,d} + T_{u,d} + \sigma^2\right)\right)\right\}\right\} \\ &= \exp\left(\frac{-x\sigma^2}{p_s r^{-\alpha}}\right)\mathscr{L}_{T_{d,d}}\left(\frac{x}{p_s r^{-\alpha}}\right)\mathscr{L}_{T_{u,d}}\left(\frac{x}{p_s r^{-\alpha}}\right) \end{aligned} \tag{31}$$

where $\mathscr{L}(.)$ represents the Laplace transform function.

Therefore, we have

$$F_{\gamma_e}(x) = \exp\Bigg(-2\pi\lambda_f \int_0^\infty \exp\left(\frac{-x\sigma^2}{p_s r^{-\alpha}}\right) \mathscr{L}_{T_{d,d}}\left(\frac{x}{p_s r^{-\alpha}}\right) \mathscr{L}_{T_{u,d}}\left(\frac{x}{p_s r^{-\alpha}}\right) r\,\mathrm{d}r \Bigg). \tag{32}$$

Hence, we arrive at (22).

VII. Appendix B

Using a similar approach to that in Appendix A, the corresponding intended and eavesdropping SINRs in the UL are respectively given by

$$F_{\gamma_b|r_{o,b}=r}(x) = 1 - \exp\left(\frac{-x\sigma^2}{p_m r^{-\alpha}}\right) \mathscr{L}_{I_{u,u}}\left(\frac{x}{p_m r^{-\alpha}}\right) \cdot \mathscr{L}_{I_{d,u}}\left(\frac{x}{p_m r^{-\alpha}}\right) \mathscr{L}_{I_{b,b}}\left(\frac{x}{p_m r^{-\alpha}}\right) \tag{33}$$

and

$$F_{\gamma_c}(x) = \exp\Bigg(-2\pi\lambda_f \int_0^\infty \exp\left(\frac{-x\sigma^2}{p_m r^{-\alpha}}\right) \mathscr{L}_{T_{u,u}}\left(\frac{x}{p_m r^{-\alpha}}\right) \mathscr{L}_{T_{d,u}}\left(\frac{x}{p_m r^{-\alpha}}\right) r\,\mathrm{d}r \Bigg). \tag{34}$$

Hence, we arrive at (23) and (24).

References

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

[2] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 40–47, Feb. 2012.

[3] B. Wang, Y. Wu, K. J. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 877–889, Apr. 2011.

[4] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

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

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

[7] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[8] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

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

[10] ——, "Secure communication in stochastic wireless networks part II: maximum rate and collusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.

[11] D. Nguyen, L. N. Tran, P. Pirinen, and M. Latva-aho, "On the spectral efficiency of full-duplex small cell wireless systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4896–4910, Sept. 2014.

[12] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.

[13] D. Nguyen, L. N. Tran, P. Pirinen, and M. Latva-aho, "Precoding for full duplex multiuser MIMO systems: Spectral and energy efficiency maximization," *IEEE Trans. Sig. Process.*, vol. 61, no. 16, pp. 4038–4050, Aug. 2013.

[14] P. C. Pinto and M. Z. Win, "Continuum percolation in the intrinsically secure communications graph," *CoRR*, vol. abs/1007.4002, 2010.

[15] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *IEEE INFOCOM*, Mar. 2012, pp. 1152–1160.

[16] D. Stoyan, *Stochastic Geometry and Its Applications*. Chichester New York: Wiley, 1995.

[17] M. Salem, A. Adinoyi, M. Rahman, H. Yanikomeroglu, D. Falconer, Y. D. Kim, E. Kim, and Y. C. Cheong, "An overview of radio resource management in relay-enhanced OFDMA-based networks," *IEEE Commun. Surveys Tuts.*, vol. 12, no. 3, pp. 422–438, Third 2010.

[18] H. ElSawy and E. Hossain, "On stochastic geometry modeling of cellular uplink transmission with truncated channel inversion power control," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4454–4469, Aug. 2014.

[19] A. Shojaeifard, K. K. Wong, M. D. Renzo, G. Zheng, K. A. Hamdi, and J. Tang, "Massive MIMO-enabled full-duplex cellular networks," *IEEE Trans. Commun.*, accepted 2017.

[20] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Sig. Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[21] L. Wang, K. K. Wong, M. Elkashlan, A. Nallanathan, and S. Lambotharan, "Secrecy and energy efficiency in massive MIMO aided heterogeneous C-RAN: A new look at interference," *IEEE J. Sel. Topics Sig. Process.*, vol. 10, no. 8, pp. 1375–1389, Dec. 2016.

[22] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[23] A. Shojaeifard, K. A. Hamdi, E. Alsusa, D. K. C. So, and J. Tang, "Exact SINR statistics in the presence of heterogeneous interferers," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6759–6773, Dec. 2015.