Secrecy Enhancement by Antenna Selection and FD Communication with Randomly Located Eavesdroppers

Gaojie Chen, Justin P Coon, Marco Di Renzo

Secrecy Enhancement by Antenna Selection and FD Communication with Randomly Located Eavesdroppers

Gaojie Chen and Justin Coon
Department of Engineering Science,
University of Oxford, OX1 3PJ, United Kingdom.
Email: {gaojie.chen and justin.coon}@eng.ox.ac.uk

Marco Di Renzo
Laboratory of Signals and Systems (L2S)
University Paris-Sud XI, France.
Email: marco.direnzo@lss.supelec.fr

***Abstract*—This paper investigates the secrecy connectivity probability for wireless networks with transmit antenna selection in the presence of randomly located eavesdroppers. Firstly, we propose an antenna selection scheme for use at the base station with a half-duplex receiver to enhance secrecy connectivity performance. Then in order to further improve the secrecy connectivity, a full-duplex (FD) receiver, which broadcasts a jamming signal while receiving the downlink message, is considered in this work. The probabilities of secrecy connectivity are given in the closed form and integral form for half-duplex and full-duplex receivers, respectively. The derived analytical results are verified by Monte Carlo simulations. The resulting analysis shows that the application of antenna selection at the transmitting base station and full-duplex communication at the receiving terminal leads to significant improvements in secrecy connectivity.**

***Index Terms*—Physical layer security, stochastic geometry, secrecy connectivity, antenna selection, full-duplex**

I. Introduction

Unlike a traditional cryptographic system [1], physical layer security is based on Shannon theory using channel coding to achieve secure transmission. Due to the broadcast nature of wireless communications, both the intended receiver and eavesdropper may receive data from the source. But if the capacity of the intended data transmission channel is higher than that of the eavesdropping channel, the data can be transmitted at a rate close to the intended channel capacity so that only the intended receiver can successfully decode the data. This is the principle of physical layer security, where the level of security is quantified by the secrecy capacity which is the capacity difference between the intended data transmission and eavesdropping channels.

Based on information-theoretic security (ITS), more recently, many works have considered ITS over wireless channels, from cooperative relay and jammer networks [2], [3], buffer-added relay network [4], multiple-input multiple-output communications [5], [6], full-duplex networks [7], cognitive radio networks [8], distributed beamforming [9], [10], among other topics. However, all these works not only assumed a small number of nodes, but also assumed the locations of eavesdroppers are known. It is impossible to obtain the location of eavesdroppers in practice. For this reason, in 2006, Haenggi provided a powerful method to model the random location distribution of the nodes in wireless networks [11], [12].

The impact of random eavesdroppers' locations to secrecy performance has been investigated [13]–[17]. Actually, the location distribution of unknown eavesdroppers can be described accurately by using the Poisson point process (PPP) or binomial point process (BPP). In [13], the locations of multiple legitimate pairs and eavesdroppers have been assumed as independent two-dimensional Poisson point processes, and the average secrecy throughput in such a wireless network has been studied. Then, the multiple input multiple output (MIMO) transmission with beamforming scheme was considered in [14], [15] to enhance the secrecy performance. In order to further improve the secrecy performance, [16], [17] exploited artificial noise against randomly distributed eavesdroppers. However, the complexity of the system is dramatically increased by using multiple antennas with beamforming. Therefore, in our paper, we consider the transmit antenna selection scheme to replace the beamforming technique, which not only can improve the secrecy performance, but also can achieve full diversity. Furthermore, full-duplex transmission, which was previously considered difficult to implement due to the associated self-interference, is now an attractive alternative in physical layer secrecy [7] because of the recent advances in the fields of antenna technology and signal processing [18]. Therefore, full-duplex antenna at the user equipment was considered.

In this paper, we investigate secrecy connectivity in wireless networks with randomly located eavesdroppers. Then in order to enhance secrecy connectivity, transmit antenna selection and full-duplex communication at the receiving terminal are considered in our work. The contributions of the paper as follows:

- We propose the transmit antenna selection scheme at base station and full-duplex receiver to enhance the secrecy connectivity in the present multiple randomly located eavesdroppers.
- We obtain a closed-form and integral closed-form expression of the secrecy connectivity probability for the half and full-duplex receivers with the antenna selection scheme.

The remainder of the paper is organized as follows: Section II presents the system model and problem formulation; Section III and IV analyze the secrecy outage probability for half-duplex and full-duplex UE with antenna selection, respectively; Section V gives numerical simulations to verify the analysis; finally, Section VI summarizes the paper.

II. System Model and Problem Formulation

A. System Model

In this section, we consider a secure transmission from the base station (BS) to one operating legitimate user equipment (UE)[1]. Without loss of generality, we locate the BS at the origin of a circle and locate the UE at a fixed point. A circle of radius R $\mathcal{V} \subset \mathbb{R}^2$ containing M identical eavesdroppers which are uniformly distributed according to a spatial binomial point process (BPP), Φ and the density of eavesdroppers outside of $\mathcal{V}$ is zero have been considered as Fig. 1. To be specific, we assume the BS is equipped with K antennas with half-duplex mode; M passive eavesdroppers are equipped with a single antenna which performs half-duplex mode so that they do not transmit and receive simultaneously; the operating legitimate UE is equipped with a hyper-duplex antenna which can easily switch between the HD and FD mode according to the system performance. We assume that eavesdroppers do not collude in this model.

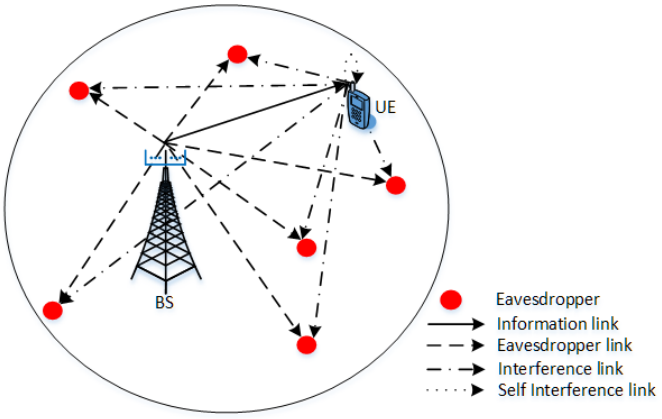

Fig. 1. The wireless network with randomly located eavesdroppers.

In our work, all channels are assumed to undergo path loss and independent Rayleigh fading effects as $h_{ij} = O_{ij} d_{ij}^{-\alpha/2}$, where α and d_{ij} denote the pathloss exponent and the distance between two nodes, i and j, respectively. The fading coefficient O_{ij} is a complex Gaussian random variable with unit variance. Therefore, the corresponding channel gains $|h_{ij}|^2$ are independently exponentially distributed with mean value λ_{ij}, and the average channel power is defined as $\lambda_{ij} = E[|h_{ij}|^2] = d_{ij}^{-\alpha}$, where $E[\cdot]$ denotes expectation. We assume that the channels are quasi-static so that the channel coefficients remain unchanged during one packet duration but independently vary from one packet time to another.

[1]If there are several users in the target cell, only one user is operated through user scheduling (e.g. random user selection).

B. Secrecy Connectivity

We now define secrecy connectivity based on classical wireless wiretap system with multiple random eavesdroppers and the FD UE. The model for an HD UE can be inferred from the FD case, as we will discuss later. We assume that the channel state information (CSI) between the BS and the UE is known by the BS[2]. Therefore, the BS is able to send x_s to the receiver UE by selected antenna ith at the time slot t, and the same time the receiver sends jamming signal x_j to potential eavesdroppers. Therefore, the received signal at the UE can be written as:

$$y_{B_i U}(t) = \sqrt{P_B} h_{B_i U}(t) x_s(t) + \sqrt{P_U} h_{UU}(t) x_j(t) + n_U(t), \tag{1}$$

and the eavesdropper E_e intercepts the signal from the BS as

$$y_{B_i E_e}(t) = \sqrt{P_B} h_{B_i E_e}(t) x_s(t) + \sqrt{P_U} h_{U E_e}(t) x_j(t) + n_E(t), \tag{2}$$

where P_B and P_U denote the transmission power for the BS and the UE, respectively, and n_U and n_E denote the additive white Gaussian noise (AWGN) noise at nodes U and E_e, respectively. For notational convenience, the time index t is ignored below unless otherwise noted necessary. In order to design the network parameters to achieve the maximum level of secrecy, we consider a worst-case assumption[3], namely, $\sigma_E^2 \to 0$, as done in [19]–[21]. Therefore, based on the antenna selection at the BS, the end-to-end capacities from the BS to the UE and from the BS to the worst-case E_* can be obtained as:

$$\begin{aligned} C_{BU} &= \log_2 \left(1 + \frac{P_B \max\limits_{i \in K} (|h_{B_i U}|^2)}{P_U |h_{UU}|^2 + \sigma_U^2} \right), \\ C_{UE_*} &= \log_2 \left(1 + \max_{e \in \Phi} \left(\frac{\frac{P_B |h_{B_* E_e}|^2}{d_{BE_j}^{\alpha}}}{\frac{P_U |h_{U E_e}|^2}{d_{UE_j}^{\alpha}}} \right) \right), \end{aligned} \tag{3}$$

where $B_* = \arg \max\limits_{i \in K} (|h_{B_i U}|^2)$. Then the probability of secrecy connectivity is the probability to have a positive secrecy capacity, which can be defined as (see [22])

$$P_{sc} = \mathbb{P}(C_{BU} - C_{BE_*} > 0), \tag{4}$$

where $\mathbb{P}(\cdot)$ denotes the probability operator.

III. Secrecy Outage Probability for a Half-duplex UE

In this section, we study the secrecy outage probability with antenna selection at the BS. According to (1) and (2) without the second left term[4], the end-to-end SNR at the UE and the

[2]This can be achieved by feeding back CSI from the UE to the BS directly.

[3]Note that we consider the worst-case which means the eavesdroppers know the CSI between the BS and eavesdroppers and between the FD UE and eavesdroppers.

[4]Self interference does not exist in the HD receiver. And the interference also does not exist in the eavesdroppers.

worst eavesdropper can be obtained as:

$$\gamma_{BU} = P_B \max_{i\in K}\left(\frac{|h_{B_iU}|^2}{d_{BU}^{\alpha}}\right), \tag{5}$$

$$\gamma_{BE_*} = P_B \max_{e\in M}\left(\frac{|h_{B_*E_e}|^2}{d_{BE_e}^{\alpha}}\right), \tag{6}$$

respectively. Thus, the secrecy outage probability is given by

$$P_{so}^{(H)}(z) = \mathbb{P}\left(\frac{\max\limits_{i\in K}\left(\frac{|h_{B_iU}|^2}{d_{BU}^{\alpha}}\right)}{\max\limits_{e\in M}\left(\frac{|h_{B_*E_e}|^2}{d_{BE_e}^{\alpha}}\right)} < 1\right). \tag{7}$$

We assume all channels are independent and identically distributed (i.i.d.); consequently, the cumulative distribution function (CDF) of γ_{BU} is given by

$$F_{\gamma_{BU}}(x) = \left(1 - e^{\frac{x}{d_{BU}^{\alpha}}}\right)^K = \sum_{i=0}^{K} C_K^i (-1)^i e^{-\frac{ix}{d_{BU}^{\alpha}}}, \tag{8}$$

where $C_K^i = K!/[i!(K-i)!]$ is the binomial coefficient. Then, the CDF of γ_{BE} can be calculated to be

$$\begin{aligned} F_Y(y) &= \mathbb{P}\left(\max_{e\in\Phi}\left(\frac{|h_{B_*E_e}|^2}{d_{BE_e}^{\alpha}}\right) < y\right) \\ &\overset{(a)}{=} E_\Phi\left[\prod_{e\in\Phi}\mathbb{P}\left(|h_{B_*E_e}|^2 < y d_{BE_e}^{\alpha} \mid \Phi\right)\right] \\ &= E_\Phi\left[\prod_{e\in\Phi}\left(1 - e^{-y d_{BE_e}^{\alpha}}\right)\right] \\ &\overset{(b)}{=} \left(\frac{1}{\pi R^2}\int_0^R\int_0^{2\pi} r\left(1 - e^{-y d_{BE_e}^{\alpha}}\right) d\theta dr\right)^M \\ &\overset{(c)}{=} \left(1 - \frac{2\gamma(yR^{\alpha}, 2/\alpha)}{\alpha R^2 y^{\alpha/2}}\right)^M, \end{aligned} \tag{9}$$

where $\gamma(\cdot,\cdot)$ denotes the incomplete gamma function, (a) follows from the independence of the random variables $\{|h_{B_*E_e}|^2; E_e \in \Phi\}$, (b) holds by using the a Euclidean metric, and (c) can be obtained by (3.381.8) in [23].

From the calculations above, one can deduce that the secrecy outage probability of the HD UE can be obtained as

$$\begin{aligned} P_{so}^{(H)} &= \mathbb{P}\left(\frac{\gamma_{BU}}{\gamma_{BE}} < 1\right) \\ &= 1 - \sum_{i=0}^{K} C_K^i (-1)^{i+1} \frac{i}{d_{BU}^{\alpha}} \int_0^{\infty} e^{-\frac{ix}{d_{BU}^{\alpha}}} \\ &\quad \times \left(1 - \frac{2\gamma(xR^{\alpha}, 2/\alpha)}{\alpha R^2 x^{\alpha/2}}\right)^M dx \\ &\overset{(a)}{=} 1 - \sum_{i=0}^{K} C_K^i (-1)^{i+1} \frac{2\sqrt{iM} d_{BU}}{R} \mathrm{K}_1\left(\frac{2\sqrt{iM} d_{BU}}{R}\right), \end{aligned} \tag{10}$$

where $\mathrm{K}_1(x)$ is the first order modified Bessel function of the second kind and (a) holds when $\alpha = 2$. Closed-form results for $P_{so}^{(H)}$ are not available for general α; hence, we constrain this analysis to the practical case where $\alpha = 2$, which is representative of line-of-sight (LOS) conditions. Indeed, we will show later that low secrecy outage probabilities result for a fairly small BS/UE separation, thus lending credence to the focus on the LOS scenario.

IV. Secrecy Outage Probability for a Full-duplex UE

In this section, the secrecy outage probability for a full-duplex UE is investigated. By using (3), the secrecy outage probability can be written as

$$P_{so}^{(F)}(z) = \mathbb{P}\left(\frac{\frac{P_B \max\limits_{i\in K}(|h_{B_iU}|^2)}{|h_{UU}|^2+1}}{\max\limits_{e\in\Phi}\left(\frac{\frac{|h_{B_*E_e}|^2}{d_{BE_e}^{\alpha}}}{\frac{|h_{UE_e}|^2}{d_{UE_e}^{\alpha}}}\right)} < 1\right), \tag{11}$$

where, for brevity and ease of exposition, we let $P_B = P_U$[5]. Now we let $x_1 = P_B \max\limits_{i\in K}(|h_{B_iU}|^2)$ and $x_2 = |h_{UU}|^2$. Therefore, the CDF and probability density function (PDF) of x_1 and x_2 can be written as

$$\begin{aligned} F_{x_1}(x_1) &= \sum_{i=0}^{K} C_K^i (-1)^i e^{-\frac{ix_1 d_{BU}^{\alpha}}{P_B}} \\ f_{x_2}(x_2) &= 1/\lambda_{uu} e^{-x_2/\lambda_{uu}}, \end{aligned} \tag{12}$$

respectively, where λ_{uu} is the SNR of residual self-interference. The CDF and PDF of $x = \frac{x_1}{x_2+1}$ are given by

$$\begin{aligned} F_x(x) &= \int_0^{\infty} F_{x_1}(x(x_2+1)) f_{x_2}(x_2) dx_2 \\ &= \sum_{i=0}^{K} C_K^i (-1)^i \frac{\frac{P_B}{d_{BU}^{\alpha}} e^{-\frac{ixd_{BU}^{\alpha}}{P_B}}}{\frac{P_B}{d_{BU}^{\alpha}} + ix\lambda_{uu}} \end{aligned} \tag{13}$$

and

$$\begin{aligned} f_x(x) = &\sum_{i=0}^{K} C_K^i (-1)^{i+1} \\ &\frac{(P_B + ix\lambda_{uu} d_{BU}^{\alpha} + P_B\lambda_{uu}) i e^{-\frac{ixd_{BU}^{\alpha}}{P_B}}}{d_{BU}^{\alpha}(\frac{P_B}{d_{BU}^{\alpha}} + ix\lambda_{UU})^2}. \end{aligned} \tag{14}$$

Letting $y = \max\limits_{e\in M}\left(\frac{|h_{B_*E_e}|^2}{d_{BE_e}^{\alpha}} / \frac{|h_{UE_e}|^2}{d_{UE_e}^{\alpha}}\right)$, it is possible to show that the CDF of y can be written as (15), which is shown at the top of the next page, where (a) follows from the independence of $\frac{|h_{B_*E_e}|^2}{|h_{UE_e}|^2}; E_e \in \Phi$, (b) holds since the CDF

$$F_\nu(\nu) = \mathbb{P}\left(\frac{|h_{B_*E_e}|^2}{|h_{UE_e}|^2} < \nu\right) = \frac{\nu}{\nu + d_{UE}^{\alpha}/d_{BE}^{\alpha}}, \tag{16}$$

and (c) holds by using the a Euclidean metric. For the case $\alpha = 2$, the CDF of y can be written as (17) at the top of this

[5]In fact, the secrecy outage for $P_B \neq P_U$ can be obtained by using the same analysis.

$$F_Y(y) = \mathbb{P}\left(\max_{e\in\Phi}\left(\frac{\frac{|h_{B_*E_e}|^2}{d^{\alpha}_{BE_e}}}{\frac{|h_{UE_e}|^2}{d^{\alpha}_{UE_e}}}\right) < y\right) = E_\Phi\left[\mathbb{P}\left(\max_{e\in\Phi}\left(\frac{|h_{B_*E_e}|^2 d^{-\alpha}_{BE_e}}{|h_{UE_e}|^2 d^{-\alpha}_{UE_e}}\right) < y \mid \Phi\right)\right] \overset{(a)}{=} E_\Phi\left[\prod_{e\in\Phi}\mathbb{P}\left(\frac{|h_{B_*E_e}|^2}{|h_{UE_e}|^2} < y\frac{d^{\alpha}_{BE_e}}{d^{\alpha}_{UE_e}} \mid \Phi\right)\right]$$
$$\overset{(b)}{=} E_\Phi\left[\prod_{e\in\Phi}\left(\frac{y d^{\alpha}_{BE_e}}{y d^{\alpha}_{BE_e} + d^{\alpha}_{UE_e}}\right)\right] \overset{(c)}{=} \left(\frac{1}{\pi R^2}\int_0^R\int_0^{2\pi} r\left(\frac{yr^{\alpha}}{yr^{\alpha} + (\sqrt{r^2 + d^2_{BU} - 2rd_{BU}\cos\theta})^{\alpha}}\right)d\theta dr\right)^M \tag{15}$$

$$F_Y(y) = \left(\frac{y}{R^2(y+1)^3}\left((-d^2_{BU} + \partial)(y+1) + d^2_{BU}(y-1)\ln\left(\frac{2yd^2_{BU}}{d^2_{BU}(y-1) + (1+y)(R^2(y+1)+\partial)}\right)\right)\right)^M, \tag{17}$$

page, where $\partial = \sqrt{d^4_{BU} + 2d^2_{BU}R^2(y-1) + R^4(y+1)^2}$. Then, by using (14) and (17), one can write the secrecy outage probability of the FD UE as

$$P^{(F)}_{so} = 1 - \int_0^{\infty} F_Y(x) f_x(x) dx. \tag{18}$$

Although (18) is in an integral form, it can easily be evaluated numerically using standard software packages.

In order to provide insight into the behaviour of this system, we analyze the case when the radius of the circular domain R grows large while keeping the distance d_{BU} constant. According to (15.c), when $R \to \infty$, the CDF of y can be written as

$$F^{R\to\infty}_Y(y) = \left(\frac{y}{y+1}\right)^M. \tag{19}$$

Substituting (14) and (19) into (18), we can easily get a close form when the number of eavesdroppers is given. For brevity, we only provide the secrecy outage probability when $M = 2$ for brevity. This result is given by (20) at the top of the next page, where

$$\psi_1 = -d^{3\alpha}_{BU}\lambda^2_{uu}i^3 + 2d^{2\alpha}_{BU}P_B\lambda_{uu}i^2 + (2\lambda_{uu} - 1)d^{\alpha}_{BU}P^2_B i - 2(\lambda_{uu} + 1)P^3_B, \tag{21}$$

$$\psi_2 = d^{3\alpha}_{BU}P_B\lambda^2_{uu}i^3 - (\lambda_{uu}+2)d^{2\alpha}_{BU}P^2_B\lambda_{uu}i^2 + d^{\alpha}_{BU}P^3_B i + P^4_B, \tag{22}$$

and $\mathrm{Ei}(1,a) = \int_1^{\infty}\frac{\exp(-ta)}{a}dt$ is the exponential integral function, which converges for $a > 0$. In the next section, we detail numerical results that verify this analysis.

V. Simulations

In this section, simulation results are given to verify the above analysis. In the simulations, we assume the noise variance $\sigma^2_U = 1$, the transmission-power-to-noise ratio $P_B/\sigma^2_U = P_U/\sigma^2_U = 50$ dB, and the simulation results are obtained by averaging over 10^5 independent Monte Carlo trials. The pathloss exponent is taken to be $\alpha = 2$.

Fig. 2 verifies the secrecy outage probabilities for the HD UE (cf. (10)), where we let $d_{BU} = 10$ m and $R = 100$ m. Both the simulation and theoretical results are presented, which are shown to perfectly match. Furthermore, it is clear from these results that the secrecy outage probability decreases as the number of transmit antennas increases. By analyzing (9) as M grows large, it is easy to see that the secrecy outage probability for the half-duplex case increases exponentially with $\sqrt{M}$.

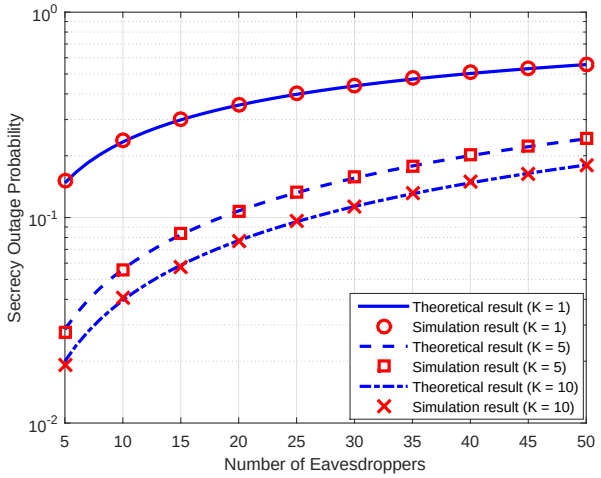

Fig. 2. Theoretical *vs* numerical secrecy outage probabilities for the HD UE in the presence of different numbers of eavesdroppers, where $d_{BU} = 10$ m and $R = 100$ m.

The comparison between the theoretical and numerically obtained secrecy outage probabilities for the FD UE is shown in Fig. 3, where we let $\lambda_{uu} = 5$ dB, $d_{BU} = 10$ m and $R = 50$ m. Again, the theoretical results generated with the help of (18) are well matched to the simulation results. Moreover, it is clear that the secrecy outage probability decreases as the number of eavesdroppers decreases or the number of transmit antennas increases. Again, this behavior is roughly exponential in M.

According to [18], radio transmissions always encounter a bandwidth constraint that limits maximum self-interference cancellation. Therefore, it is useful to consider how residual self-interference affects the secrecy connectivity performance of the FD scheme. Fig. 4 compares the secrecy outage probabilities for the HD and FD modes with respect to different λ_{uu}, where $d_{BU} = 10$ m, $R = 100$ m and $M = 30$. It is

$$P_{so}^{(F)R\to\infty} = 1 - \sum_{i=0}^{K} C_K^i (-1)^i \left(\frac{e^{\frac{id_{BU}^{\alpha}}{P_B}} \mathrm{Ei}(1, \frac{id_{BU}^{\alpha}}{P_B}) d_{BU}^{\alpha} i\psi + 2e^{\lambda_{uu}} \mathrm{Ei}(1, \frac{1}{\lambda_{uu}}) d_{BU}^{\alpha} P_B^3 \lambda_{uu} i + \psi_2}{d_{BU}^{3\alpha} P_B \lambda_{uu}^3 i^3 - 3d_{BU}^{2\alpha} P_B^2 \lambda_{uu}^2 i^2 + 3d_{BU}^{\alpha} P_B^3 \lambda_{uu} i - P_B^4} \right) \tag{20}$$

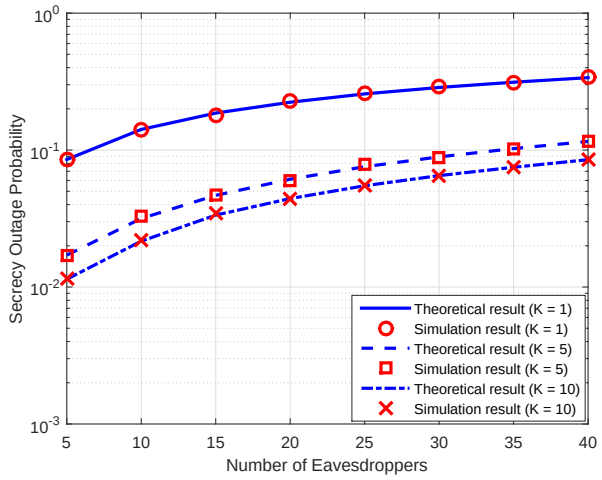

Fig. 3. Theoretical *vs* numerical secrecy outage probabilities for the FD UE in the presences of different numbers of eavesdroppers, where $d_{BU} = 10$ m and $R = 50$ m.

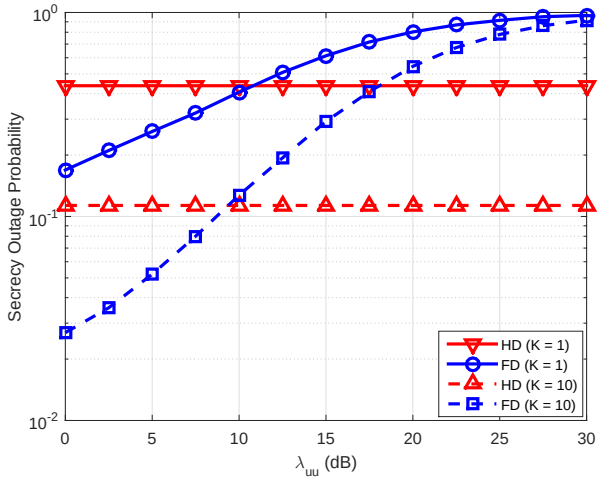

Fig. 4. Secrecy outage probability *vs* residual self-interference λ_{uu} for HD and FD modes with different numbers of transmit antennas, where $d_{BU} = 10$ m, $R = 100$ m and $M = 30$.

clearly shown that as the residual self-interference increases, the secrecy outage probability of the FD case is adversely affected. Obviously, there is no self-interference for the HD scheme; hence, the performance is constant for all λ_{uu} in this figure. Of more interest is the observation that the secrecy outage probabilities of the HD mode with the proposed antenna selection scheme ($K = 10$) or non-selection ($K = 1$) are always less than for the FD mode when λ_{uu} is less than about 11 dB. This information can be employed in practice to switch between HD and FD modes given the bandwidth constraints of the system. Since the available system bandwidth of modern communication links can change based on channel quality and the prescribed quality of service, this observation could be of great importance in future cellular networks [18].

Fig. 5 shows the secrecy outage probability of the FD UE plotted against the radius of the circular domain. Both the simulation and theoretical results for the secrecy outage probability are provided, which confirms the asymptotic result given in (20). Note that convergence to the asymptote is fairly fast (by about $R = 100$ m), which shows that the asymptotic result yields a good approximation for cellular networks operating with similar cell radii [24].

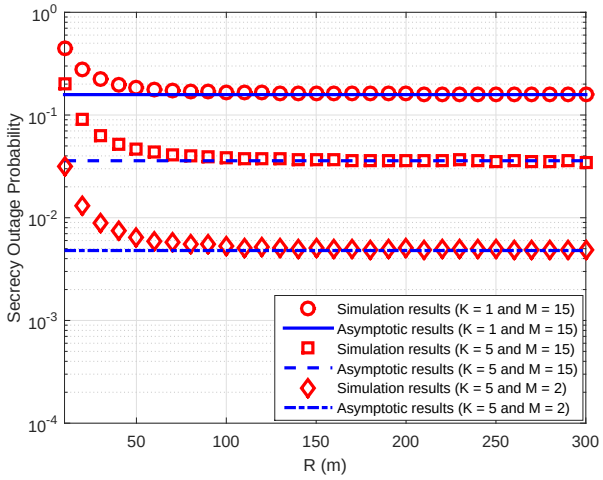

Fig. 5. The secrecy outage probability of the FD UE *vs* the radius of the circular domain.

VI. Conclusion

In this paper, we proposed a method of enhancing secrecy connectivity performance in wireless networks with randomly located eavesdroppers, which relies on the use of transmit antenna selection at the base station and an FD scheme at the UE. Closed-form and integral expressions of the secrecy outage probability for the HD and FD UE modes have been obtained (respectively), and these results have been confirmed by numerical simulations. Furthermore, we developed an asymptotic theory of the secrecy outage probability for the FD UE mode. Our results provide useful insight and analytical tools as well as a solid basis for further study.

Acknowledgements

This work was supported by EPSRC grant number EP/N002350/1 ("Spatially Embedded Networks").

REFERENCES

[1] E. D. Silva, A. L. D. Santos, L. C. P. Albini, and M. Lima, "Identity based key management in mobile ad hoc networks: Techniques and applications," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 46–52, Oct. 2008.

[2] E. Tekin and A. Yener, "The general gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2735–2751, June 2008.

[3] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation," *IEEE Trans. Inform. Forensics and Security*, vol. 4, no. 2, pp. 242 – 256, June 2009.

[4] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inform. Forensics and Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.

[5] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Information Theory*, vol. 55, pp. 2547–2553, June 2009.

[6] H. Weingarten, T. Liu, S. Shamai, Y. Steinberg, and P. Viswanath, "The capacity region of the degraded multiple-input multiple-output compound broadcast channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 5011–5023, Nov. 2009.

[7] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inform. Forensics and Security*, vol. 10, no. 3, pp. 574–583, Apr. 2015.

[8] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Dual antenna selection in secure cognitive radio networks," *to appear IEEE Trans. Veh. Technol.*, 2016.

[9] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," *in Proc. 46th Ann. Allerton Conf. Communication, Control, and Computing, UIUC, Illinois*, Sep. 2008.

[10] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," *in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Taipei, Taiwan*, Apr. 2009.

[11] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. Inf. Theory, Toronto, Canada*, pp. 539–543, July 2008.

[12] P. C. Pinto, J. Barros, and M. Z. Win, "Physical-layer security in stochastic wireless networks," in *Proc. IEEE Int. Conf. Commun. Syst.,Guangzhou, China,*, pp. 974–979, Nov. 2008.

[13] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Transactions on Wireless Communications*, vol. 10, pp. 2764–2775, Aug. 2011.

[14] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. on Wireless Commun.*, vol. 13, pp. 2931–2943, May 2014.

[15] T. X. Zheng, H. M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Commun. Lett.*, vol. 18, pp. 1299–1302, Aug. 2014.

[16] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a poisson random field of eavesdroppers," in *Communications Workshops (ICC), 2011 IEEE International Conference on*, pp. 1–5, June 2011.

[17] T. X. Zheng, H. M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. on Commun.*, vol. 63, pp. 4347–4362, Nov. 2015.

[18] S. Hong, J. Brand, J. Choi, M. Jain, J. Mehlman, S. Katti, and P. Levis, "Applications of self-interference cancellation in 5G and beyond," *IEEE Commun. Magazine*, vol. 52, no. 2, pp. 114–121, Feb. 2014.

[19] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, pp. 1802–1814, Nov. 2013.

[20] C. Wang, H. M. Wang, X. G. Xia, and C. Liu, "Uncoordinated jammer selection for securing SIMOME wiretap channels: A stochastic geometry approach," *IEEE Transactions on Wireless Communications*, vol. 14, pp. 2596–2612, May 2015.

[21] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Transactions on Vehicular Technology*, vol. 62, pp. 2170–2181, June 2013.

[22] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks-part I: Connectivity," *IEEE Trans. Inf. Forensics and Security*, vol. 7, pp. 125–138, Feb. 2012.

[23] I. S. Gradshteyn and I. M. Ryzhik, "Table of integrals, series, and products," *Elsevier Academic Press*, 7th ed. 2007.

[24] E. Hossain and M. Hasan, "5G cellular: key enabling technologies and research challenges," *IEEE Instrumentation Measurement Magazine*, vol. 18, pp. 11–21, June 2015.