On the Ergodic Secrecy Capacity with Full Duplex Communication

Mahmood, Nurul Huda; Shafique Ansari, Imran; Mogensen, Preben Elgaard; Qaraqe, Khalid A.

Published in:
2017 IEEE International Conference on Communications (ICC)

DOI (link to publication from Publisher):
10.1109/ICC.2017.7997189

Publication date:
2017

Document Version
Version created as part of publication process; publisher's layout; not normally made publicly available

On the Ergodic Secrecy Capacity with Full Duplex Communication

Nurul H. Mahmood[1], Imran S. Ansari[2], Preben Mogensen[1,3], and Khalid A. Qaraqe[2]
[1]*Wireless Communication Networks Section, Department of Electronic Systems, Aalborg University, Denmark.*
[2]*Department of Electrical and Computer Engineering, Texas A&M University at Qatar (TAMUQ), Education City, Doha, Qatar.*
[3]*Nokia Bell Labs, Aalborg, Denmark.*
Contact Email: fuadnh@ieee.org

***Abstract*—Full duplex (FD) communication promises significant performance gains under ideal network settings. Generally, it has been shown that the throughput and delay gains of FD communication are somewhat limited in realistic conditions, leading researchers to study other possible applications where significantly higher gains over half duplex communication can be availed. The potential of FD nodes in improving the physical layer security of a communication link is investigated in this contribution. Specifically, we present a thorough analysis of the achievable secrecy rate for a transceiver pair in FD mode in the presence of a passive eavesdropper assuming a generic system model. The ergodic secrecy rate with FD communication is found to grow linearly with the log of the direct channel signal to noise ratio as opposed to the flattened out secrecy rate with conventional half duplex communication and irrespective of the eavesdropper channel strengths.**

***Index Terms*—Full duplex, 5G, Physical layer security, ergodic secrecy rate.**

I. Introduction

Full duplex communication, i.e., simultaneous transmission and reception on the same radio resource, can ideally allow doubling of the throughput over conventional half duplex transmissions. In that respect, it has the potential of becoming a key technology component in addressing the challenging design targets of the 5th Generation (5G) wireless system [1]. The potential of full duplex (FD) communication in providing a throughput (TP) gain [1], [2], and/or improving the transmission latency [3], [4] is well studied.

The compelling gains with FD communication are conditioned on: i) perfect self interference cancellation, ii) available traffic at both ends to exploit the arising transmission opportunities, and iii) similar levels of network interference with FD and half duplex (HD) transmissions. Considering practical SIC levels, i.e. self interference power suppressed to a constant noise-floor like level [5], result in a reduction of the TP gain, which are further limited when a practical downlink heavy traffic profile is considered. Finally, and perhaps most interestingly, simultaneous transmission from both ends result in an increase in the number of interference streams in the network, leading to higher inter-cell interference (ICI) for a network of FD nodes and subsequently further reduction of the possible TP gains [6].

Due to the somewhat limited TP gain and latency reduction, other potential applications of FD communication have started being investigated recently. The requirement of having symmetric traffic in order to exploit FD opportunities have lead to studying FD transmission for scenarios with symmetric traffic profile such as backhaul communication and cooperative communication. Physical layer security approach focusing on the inherent capacity of the propagation channel to secure the transmission against potential eavesdropper is also envisioned as a potential application area for FD communication.

The performance of secure FD relaying has recently been analyzed for single hop [7] and multi-hop [8] relays. However, reference [7] assumes non-negativity of the secrecy rate, whereas reference [8] assumes perfect SIC; both being optimistic. The authors in [9] show that FD relaying achieves significantly higher secrecy rates than HD relaying with optimal power allocation considering the amplify-and-forward (AF) relay. In the non-cooperative scenario, a transmit beamforming scheme for a full duplex base station (FD-BS) considering physical layer security guarantee for the system with multiple passive eavesdroppers is proposed in [10]. However, this contribution focuses on developing a transmission scheme to optimize the secrecy rate under simplified assumptions.

Main Contributions: The ergodic secrecy rate of FD communication is thoroughly analyzed in this contribution, and compared against that of an equivalent HD link. In particular, we present a closed form expression for the ergodic secrecy rate considering the generic Nakagami-m fading channel and non-ideal SIC. The strictly positive secrecy rate assumption is also relaxed. We show that the the ergodic secrecy rate grows linearly with the log of direct channel's signal to noise ratio (SNR) with FD transmission as opposed to flattened out secrecy rate in HD mode.

Organization: Section II introduces the system model. Closed form expressions for the ergodic secrecy rate of FD and HD communication modes have been numerically derived in Section III, followed by a discussion on the practical applications of the derived numerical results in Section IV. Numerical results demonstrating the validity of the analytical findings are presented in Section V. Finally, closing remarks and future outlook are covered in Section VI.

II. System Model

We consider a small cell with an active transceiver pair, *Alice* and *Bob*, in the presence of an eavesdropper *Eve*. An isolated cell is considered in order to focus the analysis on

FD communication since any out-of-cell interference would on average affect Eve and the desired receiver similarly due to their relatively close distances. Alice and Bob can operate in either FD or HD mode. When operating in FD mode, the appropriate SIC schemes are assumed to suppress the loopback self interference power to within tolerable limits. The system model is depicted in Figure 1, with the random variables (rv) $\Pi \in \{X, Y, Z\}$ denoting the random signal-to-noise-ratio (SNR) of the respective channels among Alice, Bob, and Eve. The realizations $\varphi \in \{x, y, z\}$ of the respective rv Π is represented as $\varphi = \bar{\varphi}\tilde{\varphi}$, with $\bar{\varphi} \in \{\mu, \phi, \psi\}$ being the mean. $\tilde{\varphi}$ is a unit mean rv with the same distribution as φ.

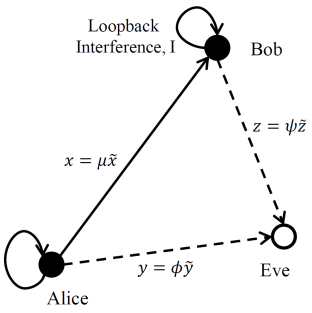

Fig. 1. System Model showing a standalone Full Duplex Transceiver pair in the presence of the eavesdropper.

A. Signal Model

1) Desired Signal Power: With FD communication, the desired signal to interference plus noise ratio (SINR) at Bob (and Alice) is denoted as $\gamma_{FD} = \frac{X}{I+1}$, where I denotes the noise-normalized residual self interference power at the receiver end following SIC. In the case of HD nodes, there is no residual self interference power (i.e, $I = 0$), and the SINR is simply given by the SNR as in $\gamma_{HD} = X$.

The desired signal amplitude is assumed to follow a Nakagami-m fading distribution that includes a wide range of other distributions as special case via its shape parameter m [11]. The SNR X is correspondingly distributed according to the following gamma distribution [11]

$$f_X(x; m, \mu) = \frac{m^m x^{m-1}}{\mu^m \Gamma(m)} \exp\left(-\frac{mx}{\mu}\right), \tag{1}$$

characterized by the parameter m and the mean SNR μ, and $\Gamma(m) \triangleq \int_0^\infty t^{m-1} \exp(-t)\, \mathrm{d}t$ is the Gamma function.

The cumulative distribution function (CDF) of X, defined as $F_X(x) = \int_0^x f_X(t)\, \mathrm{d}t$ is given by

$$F_X(x; m, \mu) = \frac{\gamma\left(m, \frac{mx}{\mu}\right)}{\Gamma(m)}, \tag{2}$$

where $\gamma(m, x) \triangleq \int_0^x t^{m-1} \exp(-t)\, \mathrm{d}t$ is the lower incomplete Gamma function [12, 6.5.2].

2) Signal Power at the Eavesdropper Node: Without loss of generality, we assume Alice to be the transmitting node in HD scenario. The eavesdropped message at Eve is received with the SNR $\beta_{HD} = Y$. In contrast, Alice and Bob transmit simultaneously in FD mode, resulting in an additional source of interference at Eve. The resulting SINR of the eavesdropped message at Eve from Alice and Bob are respectively given by

$$\beta_{FD,a} = \frac{Y}{Z+1}, \quad \beta_{FD,b} = \frac{Z}{Y+1}. \tag{3}$$

Since the eavesdropped signal amplitude is harder to characterize in practice due to Eve being an external node, it is assumed to follow the widely adopted Rayleigh fading distribution. The SNR Y (and Z) with mean $\phi(\psi)$ are correspondingly distributed according to the following exponential distributions [11]

$$f_Y(y; \phi) = \frac{1}{\phi} \exp\left(-\frac{y}{\phi}\right), \quad f_Z(z; \psi) = \frac{1}{\psi} \exp\left(-\frac{z}{\psi}\right).$$

In order to derive the distribution of β_{FD}[1], we first condition on the rv z in order to obtain

$$f_{\beta,FD}(u) = \frac{\exp\left(-\frac{u}{\phi}\right)}{\phi} \mathbb{E}_z\left[(z+1)\exp\left(-\frac{uz}{\phi}\right)\right], \tag{4}$$

where $\mathbb{E}[\cdot]$ is the expectation operator. Following some algebraic manipulations, the probability density function (PDF) of β_{FD} is derived as

$$f_{\beta,FD}(u) = \frac{\exp(-u/\phi)}{u\psi + \phi}\left[\frac{\phi\psi}{u\psi + \phi} + 1\right]. \tag{5}$$

Additionally, the CDF of β_{FD} evaluates to

$$F_{\beta,FD}(u) = 1 - \frac{\exp(-u/\phi)}{1 + u\frac{\psi}{\phi}}. \tag{6}$$

B. Secrecy Rate Analysis

Information theoretic security characterizes the fundamental ability of the physical layer to provide confidentiality. The secrecy rate is the rate at which two nodes can communicate without an eavesdropper being able to ovearhear the message. Following [13], we define the secrecy rate of the Alice-Bob link in the presence of Eve as the difference between the rates of the Alice-Bob and Alice-Eve links.

1) Secrecy Rate with HD: Considering the Alice-Bob link as the active HD link and assuming the Shannon rate can be achieved at every resource slot, the desired achievable rate between Alice and Bob is simply $R_x = \log(1 + x)$ whereas the unwanted eavesdropped rate at Eve is $R_y = \log(1 + y)$ (all logarithms are base 2). The instantaneous secrecy rate with HD transmissions is then given by $S_{HD} = \max\{R_x - R_y, 0\}$.

2) Secrecy Rate with FD: Alice and Bob can simultaneously communicate in FD modes, with both transmissions subject to potential overhearing by Eve. The achievable rate between Alice and Bob can be expressed as $R_{ab} = \log(1 + \gamma_{FD})$. Moreover, the achievable rate at Eve considering the transmission from Alice to Bob is $R_{ae} = \log(1 + \beta_{FD,a})$ with $\beta_{FD,a}$ given by Eq. (3). Consequently,

[1]The index is henceforth dropped as the usage is clear from the context.

the instantaneous secrecy rate of the Alice to Bob link with FD transmission is $S_{FD,a} = \max\{R_{ab} - R_{ae}, 0\}$.

On a similar note, the instantaneous secrecy rate of the reverse Bob to Alice link with FD transmissions is $S_{FD,b} = \max\{R_{ab} - R_{be}, 0\}$, where $R_{be} = \log(1 + \beta_{FD,b})$. Finally, the instantaneous secrecy rate of the considered system with FD communication is $S_{FD} = S_{FD,a} + S_{FD,b}$.

III. Ergodic Secrecy Rate Analysis

The ergodic secrecy rate (ESR) of half duplex and full duplex communication is respectively analysed in this section.

A. Ergodic Secrecy Rate Analysis for HD Communication

The ESR can be obtained by averaging S_{HD} over the distributions of the r.v.s x and y, and is derived as

$$\begin{aligned}\bar{S}_{HD} &= \mathbb{E}[S_{HD}] = \mathbb{E}[\log(1+x) - \log(1+y)]\Pr[x > y] \\ &= \underbrace{\log(e)\int_0^\infty \ln(1+x) f_X(x) F_Y(x)\,\mathrm{d}x}_{J_1} \\ &\quad + \underbrace{\log(e)\int_0^\infty \ln(1+y) f_Y(y) F_X(y)\,\mathrm{d}y}_{J_2} \\ &\quad - \underbrace{\log(e)\int_0^\infty \ln(1+y) f_Y(y)\,\mathrm{d}y}_{J_3}, \end{aligned} \tag{7}$$

where $\Pr[\cdot]$ denotes probability, and $F_Y(y) \triangleq 1 - \exp(-y/\phi)$ is the CDF of Y.

Since the direct evaluation of the integrals J_1, J_2, and J_3 in Eq. (7) are not straightforward, we will use the Meijer's G function to obtain a closed form expression. The Meijer's G function is a highly general class of integral function that can be used to represent a wide variety of functions and lends itself to succinct integral manipulations. The Meijer's G function, designated by the symbol $\mathrm{G}_{p,q}^{m,n}[x]$, is defined in [14, Eq. (5)]. Efficient implementations of the Meijer's G function is readily available in Mathematica and Matlab [15]. The representations of the logarithm and exponential function in terms of the Meijer's G function presented below [14, Eq. (11)]

$$\ln(1+x) = \mathrm{G}_{2,2}^{1,2}\left[x \,\middle|\, \begin{matrix}1,1\\1,0\end{matrix}\right], \quad e^{-x} = \mathrm{G}_{0,1}^{1,0}\left[x \,\middle|\, \begin{matrix}-\\0\end{matrix}\right]. \tag{8}$$

The lower incomplete Gamma function $\gamma(m,x)$ can similarly be represented as $\gamma(m,x) = \int_0^x t^{m-1}\mathrm{G}_{0,1}^{1,0}\left[t \,\middle|\, \begin{matrix}-\\0\end{matrix}\right]\mathrm{d}t = \mathrm{G}_{1,2}^{1,1}\left[x \,\middle|\, \begin{matrix}1\\m,0\end{matrix}\right]$ [16, Eq. (07.34.21.0002.01)].

1) Evaluating J_1: Substituting $F_Y(y) = 1 - \exp(-y/\phi)$ in Eq. (7), the integral J_1 can expands to

$$\begin{aligned} J_1 &= \underbrace{\log(e)\int_0^\infty \ln(1+x) f_X(x)\,\mathrm{d}x}_{J_{11}} \\ &\quad - \underbrace{\log(e)\int_0^\infty \ln(1+x)\exp(-x/\phi) f_X(x)\,\mathrm{d}x}_{J_{12}}. \end{aligned} \tag{9}$$

Further substituting the distribution $f_X(x)$ given by Eq. (1) into the above, and isolating the integral J_{11}, we obtain

$$\begin{aligned} J_{11} &= \log(e)\int_0^\infty \ln(1+x)\frac{m^m x^{m-1}}{\mu^m\Gamma(m)}\exp\left(-\frac{mx}{\mu}\right)\mathrm{d}x \\ &= \frac{\log(e)m^m}{\mu^m\Gamma(m)}\int_0^\infty x^{m-1}\mathrm{G}_{0,1}^{1,0}\left[\frac{mx}{\mu}\,\middle|\,\begin{matrix}-\\0\end{matrix}\right]\mathrm{G}_{2,2}^{1,2}\left[x\,\middle|\,\begin{matrix}1,1\\1,0\end{matrix}\right]\mathrm{d}x \\ &= \frac{\log(e)}{\Gamma(m)}\mathrm{G}_{3,2}^{1,3}\left[\frac{\mu}{m}\,\middle|\,\begin{matrix}1,1,1-m\\1,0\end{matrix}\right], \end{aligned} \tag{10}$$

where the last step is obtained using [14, Eq. (21)].

Following similar steps, the integral J_{12} in Eq. (9) can be evaluated in terms of the Meijer's G function as

$$J_{12} = \frac{\log(e)\left(1+\frac{\mu}{m\phi}\right)^{-m}}{\Gamma(m)}\mathrm{G}_{3,2}^{1,3}\left[\frac{\mu\phi}{m\phi+\mu}\,\middle|\,\begin{matrix}1,1,1-m\\1,0\end{matrix}\right]. \tag{11}$$

2) Evaluating J_2: The integral J_2 expands as

$$\begin{aligned} J_2 &= \log(e)\int_0^\infty \ln(1+y)\frac{1}{\phi}\exp\left(-\frac{y}{\phi}\right)\frac{\gamma(m,ym/\mu)}{\Gamma(m)}\,\mathrm{d}y \\ &= \frac{\log(e)}{\phi\Gamma(m)}\int_0^\infty \mathrm{G}_{2,2}^{1,2}\left[y\,\middle|\,\begin{matrix}1,1\\1,0\end{matrix}\right] \\ &\quad \times \mathrm{G}_{0,1}^{1,0}\left[\frac{y}{\phi}\,\middle|\,\begin{matrix}-\\0\end{matrix}\right]\mathrm{G}_{1,2}^{1,1}\left[\frac{my}{\mu}\,\middle|\,\begin{matrix}1\\m,0\end{matrix}\right]\mathrm{d}y, \end{aligned} \tag{12}$$

where the last step follows from substituting the logarithm, the exponential, and the lower incomplete gamma functions with their respective representation in terms of the Meijer's G function. The integral J_2 in Eq. (12) is an integration involving the product of three Meijer's G functions. The solution is a Meijer's G function of two variables that can be expressed in terms of the extended generalized bivariate Meijer's G function (EGBMGF), as introduced in [16, Eq. (07.34.21.0081.01)]. Applications of the EGBMGF have been demonstrated in [17], while its efficient implementation is readily available in Mathematica [17, Table II] and Matlab [18]. Using the EGBMGF, the integral J_2 can be obtained in closed form as

$$J_2 = \frac{\log(e)}{\Gamma(m)}\mathrm{G}_{1,0:2,2:1,1}^{1,0:1,2:1,1}\left[\begin{matrix}1\\-\end{matrix}\,\middle|\,\begin{matrix}1,1\\1,0\end{matrix}\,\middle|\,\begin{matrix}1\\m,0\end{matrix}\,\middle|\,\phi,\frac{m\phi}{\mu}\right]. \tag{13}$$

3) Evaluating J_3: The last integral J_3 in Eq. (7), which reads $J_3 = \frac{\log(e)}{\phi}\int_0^\infty \ln(1+y)\exp(-y/\phi)$ can be solved following similar steps as in Eq. (10) by substituting $m = 1$ and $\mu = \phi$, which results in $J_3 = \log(e)\mathrm{G}_{3,2}^{1,3}\left[\phi\,\middle|\,\begin{matrix}1,1,0\\1,0\end{matrix}\right]$.

Consolidating the integrals J_1, J_2, and J_3, the ESR in conventional HD mode is given in closed form by

$$\bar{S}_{HD} = J_{11} - J_{12} + J_2 - J_3. \tag{14}$$

B. Ergodic Secrecy Rate Analysis for FD Communication

With FD communication, the total instantaneous secrecy rate of our single user system is the sum of the instantaneous secrecy capacities of both the transmission directions, i.e. $S_{FD} = \underbrace{\max\{\log(1+\gamma_{FD}) - \log(1+\beta_{FD,a}), 0\}}_{S_{FD,a}}$

$$+\underbrace{\max\left\{\log(1+\gamma_{FD})-\log(1+\beta_{FD,b}),0\right\}}_{S_{FD,b}}.$$

The ergodic secrecy rate of the Alice to Bob link with FD transmission can be expanded as

$$\begin{aligned}\bar{S}_{FD,a} &= \underbrace{\int_0^\infty \log(1+x) f_{\gamma_{FD}}(x) F_{\beta_{FD,a}}(x)\,\mathrm{d}x}_{K_1} \\ &\quad + \underbrace{\int_0^\infty \log(1+u) f_{\beta_{FD,a}}(u) F_{\gamma_{FD}}(u)\,\mathrm{d}u}_{K_2} \\ &\quad - \underbrace{\int_0^\infty \log(1+u) f_{\beta_{FD,a}}(u)\,\mathrm{d}u}_{K_3}, \end{aligned} \tag{15}$$

where the PDF and CDF of γ_{FD} follows from Eqs. (1) and (2) with μ replaced by $\frac{\mu}{I+1}$, while the PDF and CDF of $\beta_{FD,a}$ have been derived in Section II-A.

1) Evaluating K_1: Using Eqs. (1) and (6), the integral K_1 can be expanded as $K_1 = \underbrace{\int_0^\infty \log(1+x) f_{\gamma_{FD}}(x)\,\mathrm{d}x}_{K_{11}}$ $- \underbrace{\int_0^\infty \log(1+x) e^{\left(-\frac{x}{\phi}\right)} \left(1+\frac{x\psi}{\phi}\right)^{-1} f_{\gamma_{FD}}(x)\,\mathrm{d}x}_{K_{12}}$. Following the steps involved in evaluating J_{11}, the integral K_{11} can be expressed in closed form as

$$K_{11} = \frac{\log(e)}{\Gamma(m)} \mathrm{G}_{3,2}^{1,3}\left[\tilde{\mu}\,\middle|\,\begin{matrix}1,1,1-m\\1,0\end{matrix}\right], \tag{16}$$

where the constant $\tilde{\mu}$ is defined as $\tilde{\mu} = \frac{\mu}{(I+1)m}$.

On the other hand, the second integral $K_{12} = \frac{\log(e)}{\tilde{\mu}^m \Gamma(m)} \int_0^\infty \frac{x^{m-1}}{\left(1+\frac{\psi}{\phi}x\right)} \exp\left(-\left(\frac{1}{\tilde{\mu}}+\frac{1}{\phi}\right)x\right) \ln(1+x)\,\mathrm{d}x$ can be expanded as an integration involving a product of three Meijer's G functions; with a close form solution in terms of the EGBMGF as follows

$$\begin{aligned} K_{12} &= \frac{\log(e)}{\tilde{\mu}^m \Gamma(m)} \int_0^\infty x^{m-1} \mathrm{G}_{0,1}^{1,0}\left[\left(\frac{1}{\tilde{\mu}}+\frac{1}{\phi}\right)x\,\middle|\,\begin{matrix}-\\0\end{matrix}\right] \\ &\quad \times \mathrm{G}_{2,2}^{1,2}\left[x\,\middle|\,\begin{matrix}1,1\\1,0\end{matrix}\right] \mathrm{G}_{1,1}^{1,1}\left[\frac{\psi}{\phi}x\,\middle|\,\begin{matrix}0\\0\end{matrix}\right]\mathrm{d}x \\ &= \frac{\left(1+\frac{\tilde{\mu}}{\phi}\right)^{-m}}{\ln(2)\Gamma(m)} \mathrm{G}_{1,0:2,2:1,1}^{1,0:1,2:1,1}\left[\begin{matrix}m\\-\end{matrix}\,\middle|\,\begin{matrix}1,1\\1,0\end{matrix}\,\middle|\,\begin{matrix}0\\0\end{matrix}\,\middle|\,\frac{\tilde{\mu}\phi}{\tilde{\mu}+\phi},\frac{\tilde{\mu}\psi}{\tilde{\mu}+\phi}\right], \end{aligned}$$

where the second step follows from the relation $(1+cx)^\alpha = \mathrm{G}_{1,1}^{1,1}\left[cx\,\middle|\,\begin{matrix}\alpha+1\\0\end{matrix}\right]/\Gamma(-\alpha)$ [14, Eq. (10)].

2) Evaluating K_2: Substituting the respective gamma CDF and the PDF of the SINR β_{FD} at the eavesdropper derived in Eq. (5), the integral K_2 is expanded as a product of four distinct terms that can be represented as four different Meijer's G functions. However, an integration involving four Meijer's G functions is not readily solvable. To overcome this limitation, we proposed to approximate the gamma parameter m with its closest integer. In that case, the CDF of the rv X can be expressed using the recurrence relation $\gamma(m+1,x) = m\gamma(m,x) - x^m\exp(-x)$ for integer positive m as $\frac{\gamma(m,x)}{\Gamma(m)} = 1-\exp(-x)\sum_{n=0}^{m-1}\frac{x^n}{n!}$ [12, Eq. (6.5.13)]. We can then approximate the integral K_2 as $K_2 \approx \int_0^\infty \log(1+u)\left(1-\exp\left(-\frac{u}{\tilde{\mu}}\right)\sum_{n=0}^{m-1}\frac{u^n}{\tilde{\mu}^n n!}\right) f_{\beta_{FD,a}}(u)\,\mathrm{d}u$. Following some further algebraic manipulations, K_2 is subsequently solved as

$$\begin{aligned} K_2 &= K_3 - \sum_{\alpha=1}^{2}\frac{\psi^{\alpha-1}}{\phi}\sum_{n=0}^{m-1}\frac{1}{\tilde{\mu}^n n!}\int_0^\infty u^n\ln(1+u) \\ &\quad \times \exp\left(-\left(\frac{1}{\tilde{\mu}}+\frac{1}{\phi}\right)u\right)\left(1+\frac{\psi}{\phi}u\right)^{-\alpha}\mathrm{d}u \\ &= K_3 - \underbrace{\sum_{\alpha=1}^{2}\frac{\tilde{\mu}\psi^{\alpha-1}}{\ln(2)(\tilde{\mu}+\phi)}\sum_{n=0}^{m-1}\frac{\left(1+\frac{\tilde{\mu}}{\phi}\right)^{-n}}{n!}}_{\cdots} \\ &\quad \underbrace{\times \mathrm{G}_{1,0:2,2:1,1}^{1,0:1,2:1,1}\left[\begin{matrix}n+1\\-\end{matrix}\,\middle|\,\begin{matrix}1,1\\1,0\end{matrix}\,\middle|\,\begin{matrix}1-\alpha\\0\end{matrix}\,\middle|\,\frac{\tilde{\mu}\phi}{\tilde{\mu}+\phi},\frac{\tilde{\mu}\psi}{\tilde{\mu}+\phi}\right]}_{K_2'}. \end{aligned} \tag{17}$$

Final Expression for $\bar{S}_{FD,a}$: Ultimately, the final expression for ergodic secrecy rate for the Alice to Bob link with FD transmission is given in terms of K_{11}, K_{12}, and K_2' derived above as $\bar{S}_{FD,a} = K_{11} - K_{12} - K_2'$. The expression for $\bar{S}_{FD,b}$, i.e. the ergodic secrecy rate for the reverse direction (Bob to Alice), can be similarly derived with ψ and ϕ replacing each other.

IV. Applications of the Secrecy Result Findings

Applications of the derived ergodic secrecy rate findings in an emerging 5G system are briefly outlined in this section.

A. Applications in Device to Device Communication

Future 5G system envisions direct device-to-device (D2D) communication as one of the key technologies to accommodate the demanding design requirements. FD communication has been proposed for such D2D communications, especially considering the close range of the devices and the symmetric nature of the traffic profile in both directions [19].

Due to its very nature, D2D communication cannot guarantee the same level of security as do cellular networks. The findings presented in this work demonstrates that a very high degree of physical layer security can be achieved by enabling FD communication between the D2D nodes. Hence, alongside the desirable gains in terms of TP, latency, and device discovery time, FD can also solve an important technical challenge in D2D communication, namely ensuring confidentiality.

B. Applications in Cellular Networks with BS FD

Despite the potential benefits of FD communication, it may not be readily available for commercial deployment at the UE level in the recent future due to size, power, and cost constraints. An intermediate proposal is to equip only the base stations with FD capabilities, and is termed as a base station full duplex (BS-FD) architecture [1].

The investigations in this contribution have revealed that the simultaneous transmission from both end of a FD communication link is the main contributor to the enhanced physical layer security. Such a finding can be utilized to accord protection to an UE scheduled in the uplink direction in need of strong physical layer security in a BS-FD network.

In the downlink direction, the BS with FD capability can schedule an UE in close vicinity of the uplink UE, as depicted in Figure 2. The eavesdropped signal at any eavesdropper in the vicinity of the scheduled uplink UE will be masked by the simultaneous downlink transmission to another nearby UE, thereby resulting in the strong secrecy rate demonstrated in this paper. Note however that, the downlink scheduled UE would also be affected by the uplink transmission. The transmission in the downlink direction must therefore be either *artificial noise*, or transmitted with a sufficiently low data rate. Hence the enhanced physical layer security for the BS-FD network setup is achieved at the expense of sacrificing the downlink data rate.

C. Applications in Conventional HD Cellular Networks

The concept of scheduling users to enhance the secrecy rate can be further extended to conventional HD networks as shown in Figure 2. An UE scheduled in the uplink direction in need of strong physical layer security can be concurrently scheduled with a nearby UE, also in the uplink direction. Let us term the two UEs as the *protected* and the *protecting* UE respectively.

If the BS is equipped with interference cancellation or interference suppression type receivers, the traffic of both the UEs can be simultaneously decoded with a well designed radio resource management technique such as link and/or rank adaptation. On the other hand, the *protecting* UE can be scheduled with traffic that is already known at the BS, which would make the resulting interference easily treatable.

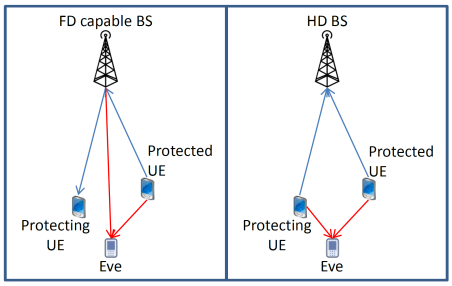

Fig. 2. Enhancing Physical layer security though scheduling to induce a FD-like scenario at the eavesdropper node.

V. Numerical Results

The ergodic secrecy rate findings with FD and HD communication are numerically validated through Matlab® based Monte Carlo simulations in this Section. At least $100,000$ independent snapshots of each scenario are simulated to ensure statistical reliability. Unless stated otherwise, the following simulation parameters are assumed to reflect a typical propagation scenario: gamma parameter $m = 2$, residual self interference $I = 1$ and $\phi = \psi$ (Eve equidistant from Alice and Bob).

A. Ergodic Secrecy Rate as a Function of μ and ϕ

The ESR of FD and HD communication for different ratios of the desired and eavesdropper channel SNR (i.e. $\frac{\mu}{\phi}$) with respect to (w.r.t.) the mean SNR μ are presented in Fig. 3. Weak, medium, and strong eavesdropper channels are considered, corresponding to $\frac{\mu}{\phi} = [10, 0, \text{ and } -10]$ dB.

Some surprising findings are revealed. First of all, FD is found to considerably enhance the physical layer secrecy rate over conventional HD communication. This is due to the simultaneous transmission from both the transmitter and the receiver, which generates an additional source of interference at Eve. The resulting interference acts as a natural deterrent to eavesdropping attempt, thereby enhancing the physical layer security potential of FD communication.

Secondly, it is interesting to note that the ESR in FD mode is almost independent of the strength towards the eavesdropper channel, especially at higher mean SNR values. In contrast, the ESR with HD is strongly dependent on the eavesdropper channel strength relative to the desired channel, and is found to approach zero even at $\frac{\mu}{\phi} = 10$ dB.

Finally, the slope of the ESR curves are also distinctly different for FD and HD communication. In conventional HD mode, the ESR is found to flatten out and converge to a constant as $\mu \to \infty$. On the other hand, the ESR with FD communication is observed to grow linearly w.r.t. μ (in dB).

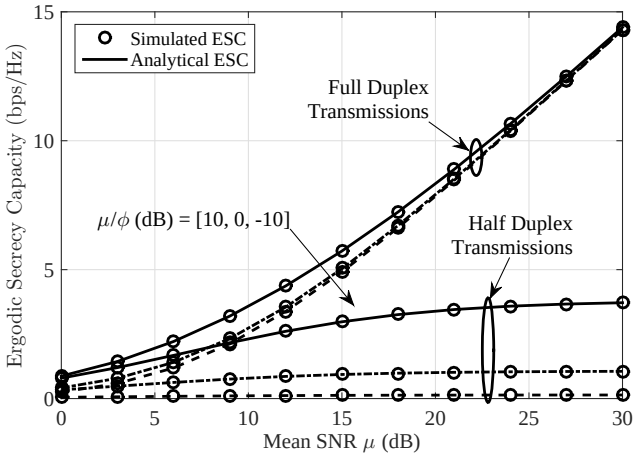

Fig. 3. The ergodic secrecy rate of full duplex and half duplex communication for different values of μ and ϕ.

B. Ergodic Secrecy Rate as a Function of the Residual Self Interference Power I

The residual self interference power I is an important parameter for FD communication. In this subsection, we explore its impact on the ergodic secrecy rate. The ESR corresponding to perfect SIC ($\frac{I}{N} = 0$), SIC to the level of noise floor ($\frac{I}{N} = 1$), and $\frac{I}{N} = 10$ are presented w.r.t. μ in Fig. 4. Furthermore, asymmetricity in the eavesdropper channel is

also considered by choosing $\psi/\phi = [2, 5]$, while $\eta = \frac{\mu}{\phi}$ is set at 10 dB.

First of all, asymmetricity in the eavesdropper channel, i.e., having $\phi \neq \psi$, has little impact on the ESR, especially at higher values of μ. In contrast, the residual self interference power plays an important role. In fact, for lower values of μ, the ESR in FD mode is lower than that of HD mode with $\frac{I}{N}$ set to 10 dB. This reiterates the well know maxim for FD communication that significant gains with FD communication requires a strong direct link (i.e., large μ) and sufficient isolation of the self interference power.

Though not shown in Fig. 4, the plots for different $\frac{I}{N}$ values are found to converge to the same secrecy rate as $\mu \to \infty$, which further reveals that the ESR in FD mode is independent of the residual self interference power I as $\mu \to \infty$.

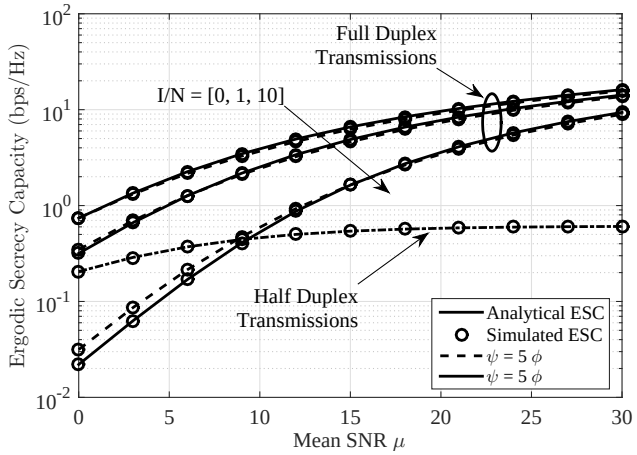

Fig. 4. The ergodic secrecy rate of full duplex and half duplex communication w.r.t. μ for different values of the self interference power I.

VI. Conclusions and Outlook

In this contribution, we have presented a thorough analysis of the potential of full duplex communication in enhancing the physical layer security of a wireless link. A closed form expression for the ergodic secrecy rate has been derived considering the Nakagami-m fading model. The findings are presented as a function of the eavesdropper channel strength and residual self interference power. Finally, numerical results via simulation demonstrating the validity of the derived results have been presented. The analytical findings are found to closely match the simulation results in all scenarios, thereby validating the accuracy of the derived results.

Contrary to the limited TP gain potential, FD communication is found to provide a high degree of physical layer security. In particular, the ergodic secrecy rate with full duplex communication is found to grow linearly with the log of the direct channel's SNR as opposed to the flattened out secrecy rate with conventional half duplex communication, irrespective of the eavesdropper channel strengths. Such compelling secrecy rates are found to be valid even with strong residual self interference power under moderate SNR conditions. As part of the future work, we plan to extend our study by analysing other physical layer security metrics such as the secure outage probability and the strictly positive secrecy probability.

Acknowledgment

Parts of this publication, specifically Sections III and V, were made possible by PDRA (PostDoctoral Research Award) grant # [PDRA1-1227-13029] from the Qatar National Research Fund (QNRF) (a member of Qatar Foundation (QF)). The statements made herein are solely the responsibility of the authors.

References

[1] A. Sabharwal *et al.*, "In-band full-duplex wireless: Challenges and opportunities," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

[2] E. Everett, A. Sahai, and A. Sabharwal, "Passive self-interference suppression for full-duplex infrastructure nodes," *IEEE Transactions on Wireless Communications*, vol. 13, no. 2, pp. 680–694, Feb. 2014.

[3] S. Talwar *et al.*, "Enabling technologies and architectures for 5G wireless," in *2014 IEEE MTT-S International Microwave Symposium (IMS2014)*, Florida, USA, Jun. 2014, pp. 1–4.

[4] M. G. Sarret *et al.*, "Analyzing the potential of full duplex in 5G ultra-dense small cell networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 284, Dec. 2016.

[5] Z. Tong and M. Haenggi, "Throughput analysis for wireless networks with full-duplex radios," in *Proc. WCNC*, New Orleans, USA, Mar. 2015, pp. 717 – 722.

[6] N. H. Mahmood, G. Berardinelli, F. Tavares, and P. Mogensen, "On the potential of full duplex communication in 5G small cell networks," in *Proc. IEEE 81st VTC-Spring*, Glasgow, Scotland, May 2015.

[7] H. Alves *et al.*, "On the performance of secure full-duplex relaying under composite fading channels," *IEEE Signal Processing Letters*, vol. 22, no. 7, pp. 867–870, Jul. 2015.

[8] J. H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Communications Letters*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[9] C. Dang *et al.*, "On secrecy rate and optimal power allocation of the full-duplex amplify-and-forward relay wire-tap channel," *IEEE Transactions on Vehicular Technology*, 2016.

[10] F. Zhu *et al.*, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[11] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*, 2nd ed. New Jersey, USA: John Wiley & Sons, Dec. 2005.

[12] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th ed., New York, USA, 1964.

[13] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[14] V. S. Adamchik and O. I. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in reduce system," in *Proc. of International Symposium on Symbolic and Algebraic Computation*, New York, USA, 1990, pp. 212–224.

[15] B. Oreshkin, "meijerG: Implements meijer G-function using interface with MuPAD," last visited on 22/8/2016. [Online]. Available: {https://se.mathworks.com/matlabcentral/fileexchange/31490-meijerg}

[16] Wolfram, "The wolfram functions site," last visited on 15/8/2016. [Online]. Available: {http://functions.wolfram.com/}

[17] I. S. Ansari *et al.*, "A new formula for the BER of binary modulations with dual-branch selection over generalized-K composite fading channels," *IEEE Transactions on Communications*, vol. 59, no. 10, pp. 2654–2658, Oct. 2011.

[18] H. Chergui, M. Benjillali, and S. Saoudi, "Performance analysis of project-and-forward relaying in mixed MIMO-pinhole and rayleigh dual-hop channel," *IEEE Communications Letters*, vol. 20, no. 3, pp. 610–613, Mar. 2016.

[19] E. Hossain and M. Hasan, "5G cellular: Key enabling technologies and research challenges," *IEEE Instrumentation & Measurement Magazine*, vol. 18, no. 3, pp. 11–21, Jun. 2015.