



Aalborg Universitet

AALBORG UNIVERSITY
DENMARK

On the Secrecy Degrees of Freedom with Full Duplex Communication

Mahmood, Nurul Huda; Mogensen, Preben Elgaard

Published in:

Proceedings of the IEEE 2017 International Conference on Communications (ICC) workshops

Publication date:

2017

Document Version

Peer reviewed version

[Link to publication from Aalborg University](#)

Citation for published version (APA):

Mahmood, N. H., & Mogensen, P. E. (2017). On the Secrecy Degrees of Freedom with Full Duplex Communication. In Proceedings of the IEEE 2017 International Conference on Communications (ICC) workshops

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- ? Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- ? You may not further distribute the material or use it for any profit-making activity or commercial gain
- ? You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

On the Secrecy Degrees of Freedom with Full Duplex Communication

Nurul H. Mahmood¹ and Preben Mogensen^{1,2}

¹Wireless Communication Networks Section, Department of Electronic Systems, Aalborg University, Denmark.

²Nokia Bell Labs, Aalborg, Denmark.

Contact Email: fuadnh@ieee.org

Abstract—Full duplex communication enables simultaneous transmission from both ends of a communication link, thereby promising gains in terms of the throughput and the delay. Such compelling gains are conditioned on a number of design constraints. Generally, it has been shown that the throughput gain and the delay reduction of full duplex communication are somewhat limited in realistic network settings, leading researchers to study other possible applications of full duplex communication which can provide significantly higher gains over half duplex communication. Physical layer security is an example of such an application. The potential of full duplex nodes in improving the physical layer security of a communication link is investigated in this contribution. We specifically derive the information theoretic secrecy degrees of freedom measure for a pair of nodes communicating in full duplex mode. Moreover, closed form expressions for the instantaneous and ergodic throughput gain of full duplex communication over conventional half duplex is derived. The secrecy degrees of freedom with full duplex is shown to be *two* as opposed to that of *zero* in half duplex mode.

Index Terms—Full duplex, 5G, Physical layer security, secrecy degrees of freedom.

I. INTRODUCTION

Full duplex communication, i.e. simultaneous transmission and reception on the same radio resource, had historically been considered impossible due to the overwhelming self interference power at the receiver end. However, recent advances in hardware design have enabled a strong degree of self-interference cancellation (SIC). As a result, the strong loopback interference can be suppressed to within tolerable limits, making full duplex (FD) communication practically appealing. The doubling of transmission opportunities with FD communication leads to a 100% throughput (TP) gain over conventional half duplex (HD) under an ideal setting. Such lucrative gains make FD a potential key component of the fifth Generation (5G) radio access technology [1]–[3].

Until recently, most studies have investigated the potential of FD communication in providing TP gain [3]–[5], and/or improving the transmission latency [6]. The theoretical TP doubling with FD communication is conditioned on three strong assumptions, namely *i*) perfect SIC, *ii*)

available traffic at both ends to exploit the arising transmission opportunities, and *iii*) similar levels of network interference with FD and HD transmissions.

Though some works assume either perfect SIC [5] or the self interference power suppressed to a constant noise-floor like level [7], [8], in practice the residual loopback interference is a random power variable [4], [9]. Nevertheless, non-ideal SIC results in a reduction of the TP gain, which are further reduced when a practical downlink heavy traffic profile is considered instead of symmetric uplink/downlink traffic [6]. 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 and subsequently further reduction of the possible TP gains [3], [5] for a network of FD nodes.

Due to the somewhat limited TP gain and latency reduction potential, other applications of FD communication that can provide significantly higher gains over half duplex communication have recently been investigated. The requirement of having symmetric traffic in order to exploit FD opportunities have lead to studying FD transmission for scenarios with naturally symmetric traffic profile, such as backhaul communication [10]. Relays are also envisioned as a potential application area for FD communication, e.g., [11], [12].

The broadcast nature of wireless transmission makes it vulnerable to be eavesdropped. Physical layer security focuses on the inherent capacity of the propagation channel to provide security in the physical layer itself. Physical layer security with FD nodes for cooperative and non-cooperative communication has started gaining attention in recent times. The performance of secure FD relaying has been analyzed for single hop and multi-hop relays in [11] and [12] respectively. On the other hand, a transmit beamforming scheme for a FD base station considering physical layer security guarantee for the system with multiple passive eavesdroppers is proposed in [13].

The residual self interference power is a key attribute of FD communication. Instead of considering perfect self

interference cancellation, some residual self interference power is assumed in this contribution. The secrecy potential of FD communication under such residual self interference power, expressed in terms of the secrecy degrees of freedom (s dof) is thoroughly analyzed in this contribution, and compared against that of equivalent HD links. In addition, we also present a closed form expression of the potential instantaneous and ergodic TP gain of FD transmissions over HD communication as a function of the residual self interference power.

The rest of this paper is organized as follows: Section II introduces the system model. An analysis of the secrecy degrees of freedom, and the TP gain of FD communication are respectively presented in Sections III and IV, followed by numerical results demonstrating the validity of the analytical findings in Section V. Finally, closing remarks and future outlook are covered in Section VI.

II. SYSTEM MODEL

Information theoretic security characterizes the fundamental ability of the physical layer to provide confidentiality. The secrecy rate is the rate at which two nodes communicate without an eavesdropper being able to decode this message. The secrecy degrees of freedom, which measures the pre-log factor of the secrecy rate, is a related information theoretic secrecy measure. Though a considerably coarse measure, the s dof analysis is tractable and provides valuable insights into the secrecy capacity behaviour in the asymptotic high SNR regime. The role of FD communication in enhancing the *physical layer security* under residual self interference power consideration, and the TP gains with FD radios, are analytically derived in this contribution.

We consider a single small cell with an active transceiver pair, *Alice* and *Bob*, in the presence of an eavesdropper node called *Eve*. An isolated cell is considered in order to focus the analysis on FD communication. Any out-of-cell interference would affect the desired receiver and the eavesdropper similarly, and hence does not have significant impact on the secrecy rate. Each node in the transceiver pair can operate in either FD or HD mode. When operating in FD mode, the appropriate SIC schemes are assumed to limit 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-ratios (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 and $\tilde{\varphi} \in \{\tilde{x}, \tilde{y}, \tilde{z}\}$ a unit mean rv similarly distributed as φ .

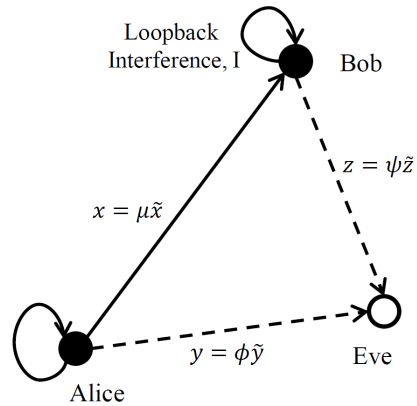


Fig. 1. System Model showing a standalone Full Duplex Transceiver pair in the presence of the eavesdropper.

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

$$\gamma_{FD} = \frac{X}{I+1}, \quad (1)$$

where I denotes the noise-normalized residual self interference power at the receiver end. In the case of HD nodes $I = 0$, and the SINR is simply given by the SNR, i.e., $\gamma_{HD} = X$.

The desired signal amplitude is assumed to follow a Nakagami- m fading distribution, which is a general fading distribution that includes a wide range of other distributions as special cases via its shape parameter m [14]. The SNR X is correspondingly distributed according to the following gamma distribution [14]

$$f_X(x; m, \mu) = \frac{m^m x^{m-1}}{\mu^m \Gamma(m)} \exp\left(-\frac{mx}{\mu}\right), \quad (2)$$

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

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

$$F_X(x; m, \mu) = \frac{\gamma\left(m, \frac{mx}{\mu}\right)}{\Gamma(m)}, \quad (3)$$

where $\gamma(m, x) \triangleq \int_0^x t^{m-1} \exp(-t) dt$ is the lower incomplete Gamma function [15, 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

$$\beta_{FD,a} = \frac{Y}{Z+1}, \quad \text{and} \quad \beta_{FD,b} = \frac{Z}{Y+1}. \quad (4)$$

The eavesdropper signal amplitude is assumed to follow the widely adopted Rayleigh fading distribution for analytical tractability. The SNR Y (and Z) with mean $\phi(\psi)$ are correspondingly distributed according to the following exponential distributions [14]

$$f_Y(y; \phi) = \frac{1}{\phi} \exp\left(-\frac{y}{\phi}\right), \quad \text{and} \quad f_Z(z; \psi) = \frac{1}{\psi} \exp\left(-\frac{z}{\psi}\right). \quad (5)$$

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

$$f_{\beta,FD}(u) = \frac{\exp\left(-\frac{u}{\phi}\right)}{\phi} \mathbb{E}_z \left[(z+1) \exp\left(-\frac{uz}{\phi}\right) \right], \quad (6)$$

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

$$f_{\beta,FD}(u) = \frac{\exp(-u/\phi)}{u\psi + \phi} \left[\frac{\phi\psi}{u\psi + \phi} + 1 \right]. \quad (7)$$

On a similar note, the CDF of β_{FD} defined as $F_{\beta,FD}(u) = \int_0^u f_{\beta,FD}(t) dt$ evaluates to

$$F_{\beta,FD}(u) = 1 - \frac{\exp(-u/\phi)}{1 + u\frac{\psi}{\phi}}. \quad (8)$$

B. Secrecy Rate with Full Duplex Communication

Following [16], we define the secrecy rate of a communicating pair in the presence of an eavesdropper as the difference between the source-destination and the source-eavesdropper rates. Let us consider the Alice to Bob link as the desired communication direction in conventional HD mode. Assuming the Shannon capacity can be achieved at each resource slot, the achievable rate of the source-destination link is $R_X = \log(1+x)$, where the logarithm is base 2. Similarly $R_Y = \log(1+y)$ denotes the source-eavesdropper achievable rate. The instantaneous secrecy capacity in the conventional HD mode is then defined as

$$\begin{aligned} S_{HD} &= \max(\log(1+x) - \log(1+y), 0) \\ &= \begin{cases} \log(1+x) - \log(1+y) & \text{if } x > y \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \quad (9)$$

With FD communication, Alice and Bob can communicate simultaneously with each other, subject to potential overhearing by Eve. The achievable rate between Alice and Bob can be expressed as $R_{ab} = \log(1 + \gamma_{FD})$, where γ_{FD} is given in Eq. (1). Similarly, the achievable rate

¹The index $\in \{a, b\}$ is henceforth dropped as the usage is clear from the context.

at Eve considering the transmission from Alice to Bob is $R_{ae} = \log(1 + \beta_{FD,a})$ with $\beta_{FD,a}$ given by Eq. (4). Thus, the instantaneous secrecy rate of the Alice to Bob link with FD transmissions is then expressed as

$$S_{FD,a} = \max\{R_{ab} - R_{ae}, 0\} \quad (10)$$

Similarly, the 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 given by $S_{FD} = S_{FD,a} + S_{FD,b}$.

C. Secrecy Degrees of Freedom

The degrees of freedom (dof) of a wireless link is an indication of the capacity pre-log factor in the capacity computation. Being a difference of two achievable rates, the secrecy rate easily lends itself to dof analysis. More specifically, the secrecy degrees of freedom (sdof) region is a characterization of the high SNR behaviour of the secrecy capacity. Following [17], we define the sdof with the ratios $\eta_\phi \triangleq \frac{\mu}{\phi}$ and $\eta_\psi \triangleq \frac{\mu}{\psi}$ fixed as

$$d_\varphi = \lim_{\{\mu, \phi, \psi\} \rightarrow \infty} \sup \frac{S_\varphi}{\log \mu}, \quad (11)$$

where $\varphi \in \{HD, FD\}$ denotes the transmission mode.

III. SECRECY DEGREES OF FREEDOM ANALYSIS

The secrecy degrees of freedom measures the pre-log factor of the achievable secrecy capacity. In this section, we characterize the sdof with HD and FD communication.

A. Secrecy Degrees of Freedom Analysis of Half Duplex Communication

In HD mode, the instantaneous secrecy capacity given by Eq. (9) can be rewritten as $(\log(1+x) - \log(1+y)) \Pr[x > y]$, where $\Pr[\cdot]$ is the probability measure. In the asymptotic SNR regime $\log(1+x) - \log(1+y) \rightarrow \log(\frac{x}{y})$ as $\{\mu, \phi\} \rightarrow \infty$ with the ratio η_ϕ fixed. Being a probability measure, $\Pr[x > y] < 1$, which in turn implies

$$\lim_{\{\mu, \phi\} \rightarrow \infty} S_{HD} < \log\left(\frac{x}{y}\right). \quad (12)$$

Observing the rv $\frac{x}{y}$, we can deduce that $\Pr[\frac{x}{y} < \theta] = \Pr[y > \frac{x}{\theta}] = \mathbb{E}_X \left[\exp\left(-\frac{x}{\theta\phi}\right) \right]$, where the last step follows from the complimentary CDF of the exponential rv Y (the CDF is given by Eq. (5)). The preceding expectation is by definition the Laplace Transform (LT) of the gamma distributed rv X , and is given by [14]

$$\mathcal{M}_X(s) = \mathbb{E}_X[\exp(-sx)] = \left(1 + \frac{\mu s}{m}\right)^{-m}. \quad (13)$$

Substituting the above result, we obtain $\Pr[\frac{x}{y} < \theta] = (1 + \frac{\eta_\phi}{m\theta})^{-m}$. Using this formulation, it can be deduced that, in the asymptotic SNR regime, $\Pr[\frac{x}{y} < \infty] = 1$ as long as the ratio η_ϕ is bounded. We therefore have

$$\lim_{\{\mu, \phi\} \rightarrow \infty} S_{HD} < \infty, \quad (14)$$

i.e., the instantaneous secrecy capacity with HD communication is asymptotically bounded for a bounded η_ϕ . Consequently, with a bounded instantaneous secrecy capacity, the sdof of HD communication is by definition zero, i.e.

$$d_{HD} = \lim_{\mu \rightarrow \infty} \sup \frac{S_{HD}}{\log \mu} = 0. \quad (15)$$

B. Secrecy Degrees of Freedom Analysis of Full Duplex Communication

The instantaneous secrecy capacity in FD mode is given in terms of the SINRs γ_{FD} , $\beta_{FD,a}$ and $\beta_{FD,b}$ as

$$S_{FD} = \max\{\log(1 + \gamma_{fd}) - \log(1 + \beta_{FD,a}), 0\} + \max\{\log(1 + \gamma_{fd}) - \log(1 + \beta_{FD,b}), 0\}.$$

To derive the sdof, let us look into the involved SINR figures, namely γ_{FD} , $\beta_{FD,a}$ and $\beta_{FD,b}$, in the asymptotic regime. We can observe from Eq. (8) that, by letting $\{\phi, \psi\} \rightarrow \infty$, with the ratios $\eta_\phi = \frac{\mu}{\phi}$ and $\eta_\psi = \frac{\mu}{\psi}$ fixed (which also implies bounded $\frac{\phi}{\psi}$), the SINRs $\beta_{FD,a}$ and $\beta_{FD,b}$ remain bounded. In other words, $\Pr[\beta_{FD,a} < \infty] = 1$ and $\Pr[\beta_{FD,b} < \infty] = 1$.

On the other hand, we can rewrite the SINR of the Alice to Bob channel as $\gamma_{FD} = \frac{x}{I+1} = \mu\tilde{x}/(I+1)$, where \tilde{x} is a unit mean gamma distributed rv. This allows us to represent the secrecy capacity $S_{FD,a}$ of the Alice to Bob link in the asymptotic SNR regime as

$$\begin{aligned} \lim_{\{\mu, \phi, \psi\} \rightarrow \infty} S_{FD,a} &= \\ \max \left\{ \log(\mu) - \log \left(\frac{(1 + \beta_{FD,a})(I+1)}{\tilde{x}} \right), 0 \right\} \\ &= \log(\mu) - \xi_a, \end{aligned} \quad (16)$$

where $\xi_a = \log \left(\frac{(1 + \beta_{FD,a})(I+1)}{\tilde{x}} \right)$. Since $\Pr[\beta_{FD,a} < \infty] = 1$, the variable ξ_a is bounded with probability 1, i.e., $\Pr[\xi_a < \infty] = 1$. The secrecy capacity $S_{FD,b}$ of the reverse Bob to Alice link in the asymptotic SNR regime can similarly be expressed as

$$\lim_{\{\mu, \phi, \psi\} \rightarrow \infty} S_{FD,b} = \log(\mu) - \xi_b,$$

with $\xi_b = \log \left(\frac{(1 + \beta_{FD,b})(I+1)}{\tilde{x}} \right)$ and $\Pr[\xi_b < \infty] = 1$.

Consolidating the above discussion, the sdof with FD

communication is then derived as

$$\begin{aligned} d_{FD} &= \lim_{\mu \rightarrow \infty} \sup \frac{S_{FD,a} + S_{FD,b}}{\log(\mu)} \\ &= \lim_{\mu \rightarrow \infty} \frac{2 \log(\mu) - \xi_a - \xi_b}{\log(\mu)} = 2. \end{aligned} \quad (17)$$

Hence, we can observe that the degrees of freedom of FD communication (which is 2 [9]) is fully maintained even in the physical layer security aspect. This is in contrast with conventional HD communication, where the dof (which is equal to *one*) is fully lost when the sdof is considered.

IV. THROUGHPUT ANALYSIS OF A FD RADIO

In this section, we complement the earlier presented secrecy degrees of freedom findings with an analysis of the throughput gain of FD over HD communication in the presence of residual self interference power. While the throughput gain with FD nodes have been analysed in a number of contributions in the literature [1]–[5], the novelty in this contribution is the presentation of a closed form expressions for the ergodic and the instantaneous TP gains with FD communication.

A. Ergodic Throughput Gain Analysis

The ergodic throughput can be obtained by taking the expectation of the instantaneous TP over the SINR distributions. With FD communication, the ergodic TP is formulated as

$$\bar{R}_{FD} = 2 \int_0^\infty \log(1+x) f_{\gamma_{FD}}(x) dx, \quad (18)$$

where the factor 2 accounts for simultaneous transmission and reception across both uplink and downlink directions.

The Meijer's G function, designated by the symbol $G_{p,q}^{m,n}[x]$ and defined in [18, Eq. (5)], is a highly general class of integral function that can represent a wide variety of functions and lends itself to succinct integral manipulations. In order to evaluate the ergodic TP, we will use the representations of the logarithm and exponential function in terms of the Meijer's G function presented below [18, Eq. (11)]

$$\ln(1+x) = G_{2,2}^{1,2} \left[x \left| \begin{matrix} 1, 1 \\ 1, 0 \end{matrix} \right. \right] \quad \text{and} \quad e^{-x} = G_{0,1}^{1,0} \left[x \left| \begin{matrix} - \\ 0 \end{matrix} \right. \right].$$

Substituting $f_X(x)$ given by Eq. (2) and the above Meijer's G representations into Eq. (18), we obtain

$$\begin{aligned} \bar{R}_{FD} &= \log(e) \int_0^\infty \ln(1+x) \frac{x^{m-1}}{\tilde{\mu}^m \Gamma(m)} \exp\left(-\frac{mx}{\tilde{\mu}}\right) dx \\ &= \frac{\log(e)}{\tilde{\mu}^m \Gamma(m)} \int_0^\infty x^{m-1} G_{0,1}^{1,0} \left[\frac{x}{\tilde{\mu}} \left| \begin{matrix} - \\ 0 \end{matrix} \right. \right] G_{2,2}^{1,2} \left[x \left| \begin{matrix} 1, 1 \\ 1, 0 \end{matrix} \right. \right] dx \\ &\stackrel{(a)}{=} \frac{\log(e)}{\Gamma(m)} G_{3,2}^{1,3} \left[\tilde{\mu} \left| \begin{matrix} 1, 1, 1-m \\ 1, 0 \end{matrix} \right. \right], \end{aligned} \quad (19)$$

where $\tilde{\mu} \triangleq \frac{\mu}{(I+1)^m}$ is a constant, and step (a) follows from [18, Eq. (21)]. Following similar steps, the ergodic TP in the HD mode can be also expressed in closed-form as

$$\bar{R}_{HD} = \frac{\log(e)}{\Gamma(m)} G_{3,2}^{1,3} \left[\frac{\mu}{m} \middle| \begin{matrix} 1, 1, 1-m \\ 1, 0 \end{matrix} \right]. \quad (20)$$

Finally, the ergodic TP gain of FD communication over HD is thereby expressed in closed form as

$$\frac{\bar{R}_{FD} - \bar{R}_{HD}}{\bar{R}_{HD}} = \frac{2 G_{3,2}^{1,3} \left[\tilde{\mu} \middle| \begin{matrix} 1, 1, 1-m \\ 1, 0 \end{matrix} \right]}{G_{3,2}^{1,3} \left[\frac{\mu}{m} \middle| \begin{matrix} 1, 1, 1-m \\ 1, 0 \end{matrix} \right]} - 1. \quad (21)$$

B. Instantaneous Throughput Analysis

The ergodic TP analysis in the previous subsection provides an overview of the average TP behaviour with FD and HD communication. In order to analyse the performance of FD communication in greater details, we investigate the respective instantaneous TP behaviour in this section.

The probability of the instantaneous FD TP exceeding the HD TP is formulated as $\Pr[R_{FD} > R_{HD}] = \Pr[2 \log(1 + \gamma_{FD}) > \log(1 + x)]$. Following some algebraic manipulations and using the relation $\gamma_{FD} = \frac{x}{I+1}$, the probability is reduced to

$$\begin{aligned} \Pr[R_{FD} > R_{HD}] &= \Pr \left[\left(1 + \frac{x}{I+1} \right)^2 > 1 + x \right] \\ &= \Pr[\gamma_{FD} > I - 1] \\ &= \begin{cases} 1 & \text{when } I \leq 1 \\ 1 - \frac{\gamma \left(m, \frac{I-1}{\tilde{\mu}} \right)}{\Gamma(m)} & \text{when } I > 1. \end{cases} \end{aligned} \quad (22)$$

V. NUMERICAL RESULTS

The secrecy degrees of freedom and the throughput analysis of full duplex and half duplex 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 general simulation parameters are assumed to reflect a typical propagation scenario: gamma parameter for the desired signal channel $m = 2$ and noise-normalized residual self interference $I = 1$. Furthermore, Eve is considered equidistant from Alice and Bob, i.e. $\phi = \psi$.

A. Secrecy Degrees of Freedom Results

Being an asymptotic SNR characterization of the secrecy capacity, the sdoF is not readily amenable to numerical simulations. However, in order to demonstrate the validity of the analysis presented in Section III, the behaviour of

the maximum achievable secrecy rate normalized by the log of the SNR, i.e. $\max \frac{S}{\log(\mu)}$, is presented in Figure 2 as a function of the mean SNR μ in logarithmic value for different values of the residual self interference power I . It is observed that as $\mu \rightarrow \infty$, the ratio of the secrecy capacity over the SNR in logarithmic value converges to *two* for FD communication, whereas it approaches *zero* in the HD mode. Hence, the reported respective sdoF with FD and HD communication is clearly evident from the presented trend.

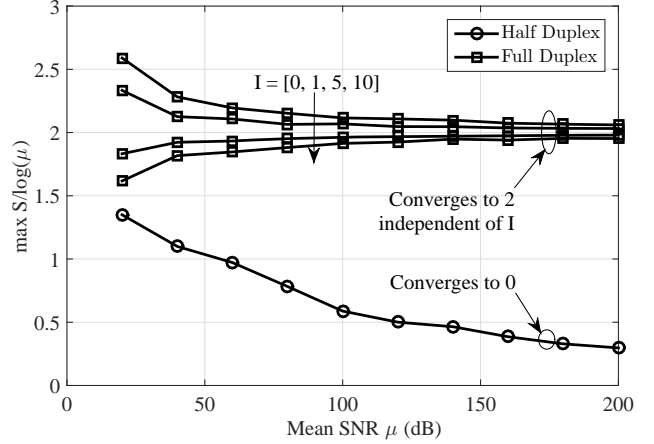


Fig. 2. The secrecy capacity normalized by the SNR in logarithmic value in the asymptotic SNR range.

B. Throughput Analysis

The ergodic TP gain of FD communication over conventional HD as a function of the residual self interference power I for different values of the mean SNR μ is presented in Figure 3. The presented ergodic TP curves showcase the inability to deliver the promised 100% TP gain of FD communication. In fact, such a gain is only achievable with either $I = 0$, or in the asymptotic high SNR regime as $\mu \rightarrow \infty$ for a given constant I .

Figure 4 presents the probabilities that the instantaneous TP with FD communication outperforms that with HD for different values of I and μ . In each instance, the area to the left of the curve indicates the region where HD outperforms FD, and vice versa. For all $I > 1$, there is a range of μ values for which $\Pr[R_{FD} > R_{HD}] \rightarrow 0$, whereas another range where $\Pr[R_{FD} > R_{HD}] \rightarrow 1$.

It can be observed from both Figures 3 and 4 that, in designing a FD node, the level SIC required for meaningful TP gain strongly depends on the operating SNR regime of the receiver.

VI. CONCLUSIONS AND OUTLOOK

The promise of doubling the network throughput makes full duplex communication an attractive feature for a 5G radio access technology. However, numerical findings have revealed that, the TP gains of FD are rather limited in a

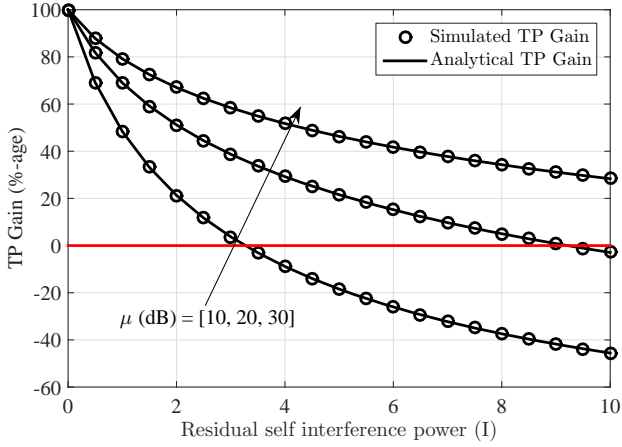


Fig. 3. The ergodic throughput gain of full duplex over half duplex communication for different mean SNR (μ) values.

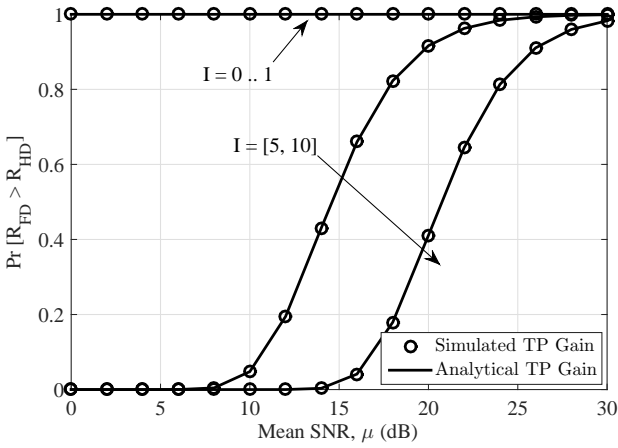


Fig. 4. Probabilities of FD communication outperforming HD communication for different antenna separation distances.

realistic setting due to a number of practical factors. The rather limited TP gains of FD communication have lead us to investigate other applications of FD, and in particular the potential of FD communication in enhancing the physical layer security of a wireless link. The information theoretic secrecy degrees of freedom measure, which is a characterization of the secrecy capacity in the asymptotic high SNR regime is also presented in this contribution. Furthermore, closed-form expressions for the instantaneous and ergodic TP gains with FD communication over conventional HD schemes considering a Nakagami- m fading channel have been derived.

The analytical findings are further complemented and validated through numerical simulation results; and are found to closely match the simulation results in all scenarios. Contrary to the limited TP gain potential, FD communication is found to provide a high degree of physical layer security. Specifically, the sdoF, i.e. the pre-log factor of the secrecy capacity, is found to be *two* compared to that of *zero* with conventional HD transmissions. As

part of the future work, we plan to extend our study by analysing other physical layer security metrics with FD communication, such as the secure outage probability and the strictly positive secrecy probability.

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] S. Hong *et al.*, "Applications of self-interference cancellation in 5G and beyond," *IEEE Communications Magazine*, pp. 114–121, Feb. 2014.
- [3] 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 Vehicular Technology Conference: VTC-Spring*, Glasgow, Scotland, May 2015.
- [4] 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.
- [5] X. Xie and X. Zhang, "Does full-duplex double the capacity of wireless networks?" in *Proc. The 33rd Annual IEEE International Conference on Computer Communications (INFOCOM'14)*, Toronto, Canada, Apr. 2014, pp. 253 – 261.
- [6] M. G. Sarret, G. Berardinelli, N. H. Mahmood, and P. Mogensen, "Can full duplex boost throughput and delay of 5G ultra-dense small cell networks?" in *Proc. IEEE 83rd Vehicular Technology Conference (VTC Spring)*, Nanjing, China, May 2016.
- [7] Z. Tong and M. Haenggi, "Throughput analysis for wireless networks with full-duplex radios," in *Proc. Wireless Communications and Networking Conference (WCNC)*, New Orleans, USA, Mar. 2015, pp. 717 – 722.
- [8] T. Riihonen, S. Werner, and R. Wichman, "Hybrid full-duplex/half-duplex relaying with transmit power adaptation," *IEEE Transactions on Wireless Communications*, vol. 10, no. 9, pp. 3074–3085, Sep. 2011.
- [9] N. H. Mahmood *et al.*, "Analysing self interference cancellation in full duplex radios," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, Doha, Qatar, Apr. 2016.
- [10] H. Tabassum, A. H. Sakr, , and E. Hossain, "Analysis of massive MIMO-enabled downlink wireless backhauling for full-duplex small cells," *IEEE Transactions on Communications*, vol. 64, no. 6, pp. 2354–2369, 2016.
- [11] 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.
- [12] 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.
- [13] 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.
- [14] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*, 2nd ed. New Jersey, USA: John Wiley & Sons, Dec. 2005.
- [15] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th ed., New York, USA, 1964.
- [16] 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.
- [17] X. He, A. Khisti, and A. Yener, "MIMO broadcast channel with arbitrarily varying eavesdropper channel: Secrecy degrees of freedom," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Houston, USA, Dec. 2011, pp. 1–5.
- [18] 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 (ISSAC' 90)*, New York, USA, 1990, pp. 212–224.