This is a peer-reviewed, accepted author manuscript of the following research conference paper: Khan, R., & Asif, R. (2021). Reflective in-band full duplex NOMA communications for secure 5G networks. In 2021 International Conference on Smart Applications, Communications and Networking (SmartNets) [21202227] IEEE. https://doi.org/10.1109/SmartNets50376.2021.9555418

Reflective In-Band Full Duplex NOMA Communications for Secure 5G Networks

Rabia Khan*† and Rameez Asif*†
*Department of Electronics and Electrical Engineering, University of Strathclyde, Glasgow, UK
†Power Networks Demonstration Centre (PNDC), University of Strathclyde, Glasgow, UK
Email: {rabia.khan, rameez.asif}@strath.ac.uk

***Abstract*—In the context of Internet-of-Things (IoT), big Data analytic and the interconnected world, the scientific revolution is increasing the demand for an improved spectrum utilization. An efficient use of the existing spectrum is required for high data-rate transmission. There are several potential ways of solving the challenges of spectrum scarcity. In-Band Full Duplex (IBFD) and Non-Orthogonal Multiple Access (NOMA) are two techniques that can improve the spectral efficiency (SE) in a 5G and Beyond (5GB) cellular networks. This paper proposes a spectral efficient IBFD scheme, Reflective In-Band Full-Duplex (R-IBFD) algorithm for relay selection to improve security of the system with minimum interference. The interference is basically reduced by the addition of orthogonality between the transmitted and received signal in the IBFD mode. The proposed R-IBFD is evaluated with IBFD, Device-to-Device (D2D) and Artificial Noise (AN). Secrecy Outage Probability (SOP) and throughput is analysed for R-IBFD. The simulation results present the comparison between the R-IBFD and conventional decode-and-forward IBFD communication with one or more users operated as a relay.**

***Keywords*—** Artificial noise, Full Duplex, Reflective In-Band Full Duplex, In-Band Full Duplex, Decode-and-Forward, Secrecy outage probability, secrecy capacity, security and secrecy outage probability.

I. Introduction

Orthogonal multiple access techniques (OMA) are classical methods to serve each user in separate orthogonal resource block. It has been used in the previous versions of the technologies, a continuous improvement in the technology has been detected with the passage of time and the demand of the current age [1]. The spectral efficiency is the key component for next-generation networks (NGN), therefore the conventional OMA procedures; TDMA, FDMA (including OFDMA), and CDMA cannot complete the demand of the future obligation of technology. Though, they can still be used for several applications requirements including high data rate, low latency, energy efficiency, Quality of Service (QoS) and outage etc. Application of TDMA involves careful timing synchronization, particularly for up-link [1] traffic. The QoS diminished while proceeding from 1st generation to 3rd degeneration due to the upsurge in the number of operators which caused high self-interference. The 4G-LTE communication is founded on OFDMA technique. OFDM systems the basis of all latest multiple access techniques. Due to some drawbacks of OFDM, including power loss in self-interference, spurious radiation and intermodulation distortion, for LTE up-link transmission SC-FDMA is used in [1].

Now the focus is towards Non-orthogonal Multiple Access (NOMA) as a key multiple access scheme aspirant for 5G. It offers higher spectral efficiency [2], higher cell-edge throughput and ultra low latency as compared to the conventional OMA techniques. Power domain NOMA allows multiple users to concurrently communicate using the same frequency and time, but transmit at different power level. At the broadcaster side, multiplexing is allowed using superposition coding [3]. Meanwhile, at the receiver side, the multi-user separation techniques, such as Successive Interference Cancellation (SIC), can be employed to decode the communications [2].

The industrial development necessitates the smart way of presentation available natural resources. Recently, several countries have installed 5G cellular with high frequency ranges of the spectrum. Sophisticated use of the residual electromagnetic spectrum leads to improved spectral efficiency [14]. Many approaches can be made by guiding the high-quality throughput with the prevailing proposed technologies like In-Band Full Duplex (IBFD). IBFD focuses on the efficient utilization of the spectrum for developing a system with better Spectral Efficiency (SE) by reusing spectrum [14]. The present presentation of 5G, generally based on the Orthogonal Frequency Division Multiple Access (OFDMA) and Half Duplex (HD). The 4G system is likewise based on TDMA, OFDMA and HD. The replacement of the existing 4G setup with 5G is comparatively easier and inexpensive. Keeping the consideration of spectrum limitation, it will be better to extend the system further by using IBFD for the 5G beyond technologies.

II. Related Work

The present research on FD shows that the use of FD in the transmission doubles the SE of the system. The transmission switching mode from HD to FD or vice versa for a Device-to-Device (D2D) communication is one of the approaches for preserving equilibrium between HD and FD [2], [5]. Beam-forming is one of the methods for FD. An exact design of beam-forming for the power allocation organization [6] amongst the transmitter-relay communication in the cognitive radio networks, is appropriate for providing the high rate to a particular near or a distant user. FD, D2D and NOMA communication together bring improved Ergodic Sum Rate (ESR) than HD [7]. However, the HD outstrips FD at high Signal to Noise Ratio (SNR) in the form of outage probability and in the delay-tolerant transmission [2], [7]. The security is desirable in each layer of the communication scheme. Each layer has different provisions of security in diverse perspective, due to the parallel motive of multiple associated objects in the 5G beyond technology [8], [9], [10]. The physical layer security (PLS) is one of the fears in any of the smart arrangement. The assembly of multiple devices together, broadcast nature of the system, big data and frequency sharing principals to a big security threat.

There are different types of eavesdropping in contradiction of the security of a communication system. The eavesdropper (Eve) can be passive or active, depending on the cyber-vector. It can also be amongst the reliable envisioned user or a stranger. Present algorithms are considerate for handling the security issues; however, the technological progression advances the security threats as well. The enactment of the technology everywhere including; banks, building, security systems, houses, schools, accounts, industries and transportation makes everything vulnerable. Hybrid eavesdropping (passive eavesdropping on the transmission source and the reactive

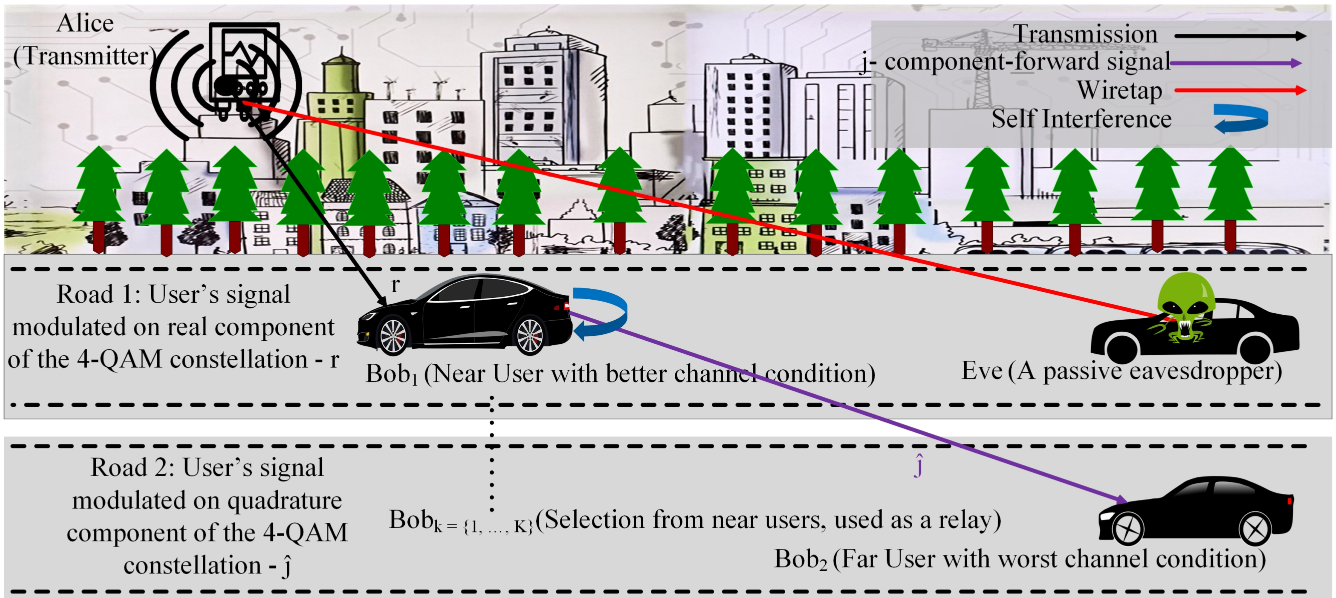

Fig. 1. The vehicular system where the best supported near vehicle amongst K near vehicles support one of the far vehicle Bob_2. The selected vehicle is named Bob_1. Bob_1 is in the IBFD mode, where the self interference is ideally prevented using proposed R-IBFD.

jamming on legitimate users) in FD-NOMA can be determined by a method of draining eavesdropper by adding cumulative decoding complexity and high energy consumption. It can diminish the effect of jamming and eavesdropping [3]. Conventional communication system permits dual communication with a transmission and a reception task named the Half Duplex (HD) communication. In HD, the channel is common for dual tasks, with orthogonal (different) time slots or frequency bands (out-of-band FD mode). The simultaneous transmission and reception is possible with the FD communication.

FD permits a device to transmit and receive the signal in the identical frequency band and time slot. The Out-of-Band FD (OBFD) and the In-Band FD (IBFD) are two types of FD communication systems, where the transmission and reception take place together in the same time and frequency slot. IBFD is superior to conventional HD in terms of system reliability, sum rate, network capacity and other theoretical aspects [11]. FD and D2D communication have common characteristics including better performance at short distances and reduced self-interference at low power transmit signals [12], [11].

Several approaches have been proposed for the assessment of the interference problem including: RF digital interference cancellation [11], advance antennas cancellation and digital base band, channel estimation and power allocation [4] offers the possible answers for FD. Hybrid resources that shift the mode between FD and HD have been developed for emerging the radio resources and simultaneously enlightening the SE. Separated resources are needed like antennas for the distinct transmission with the least possible interference. If the devices are too close then this can be a waste of using frequency band, especially if the data for communication is massive. The use of additional devices like a relay may also increase the system complexity. Therefore, it has been observed [13] that D2D communication is reliable when devices are close. It is possible for the BS to grant approval for D2D communication in the same cell only. When the distance between D2D increases the throughput decreases significantly. FD can improve the traditional wireless communication to a better extent in terms of: loss of data due to high congestion, hidden terminals, time delay and SE. The key idea [16] behind the usage of IBFD communication is to make heterogeneous dense network with high capacity and flexible relaying modes. The quantitative analysis of theoretical and practical placement shows that at the cost of enlarged complexity, FD provides diversity, high throughput, low symbol error rate and decrease the use of HD. The D2D IBFD communication becomes better with the increase of in-cell communication ratio that provides to bandwidth efficiency.

In this paper, we proposed an R-IBFD with NOMA for 5G communications. Similar to conventional NOMA with IBFD, Alice broadcasts signal to all users but with different modulation approach. No direct link has been considered between Alice and far user Bob_2 and 4-QPSK is used as modulation technique. In R-IBFD, source modulates users' signal on the real component of the 4-QPSK constellation mapping and add complex AN to make a complex transmission signal. Selected near-user Bob_1, amongst K users, forwards the signal of far-user after adding AN for the R-IBFD cooperative communication.

III. System Model

We consider a system with an R-IBFD D2D cooperative communication for a Downlink (DL) System as given in fig. 1. The considered scenario consist of a source (Alice), the nearest receiver/s (Bob_k, $k = \{1, \cdots, K\}$), the far receiver (Bob_2) and the eavesdropper (Eve). For the same scheme, multiple vehicles can be considered, however, to avoid a cumbersome system, we consider 2 vehicles, one of the nearest Bob_k will be used as a relay to cooperate in forwarding the signal to the further vehicle. The first vehicle will be chosen with the relay selection scheme [16]. There is no direct connection between Alice and Bob_2.

Alice, Bob_2 and Eve contains a single antenna excluding Bob_1 or Bob_k. P_T is the total transmission power, for each transmission power will be divided amongst the users with power domain NOMA i.e. $\alpha_1 + \alpha_2 = 1$ where α_1 and α_2 are the power allocation coefficients. The power coefficients are allocated with respect to the distances $d_{Bob_1} < d_{Bob_2} \approx d_{Eve}$ and the channel conditions $g_e \approx g_{Bob_2} < g_{Bob_1}$ of each vehicle from Alice, statistically. As per consideration, each Bob is facing a Rayleigh fading channel and their Channel State Information (CSI) is considered to be known by Alice and Bob_1. Considerately, Eve does not have the legitimate user's CSI information. Eve can detect Bob_2's signal only due to their approximately same channel conditions. The other channels, included in the transmission are g_{12} and g_{11} are the channels for the

R-IBFD transmission in the IBFD mode from Bob_1 to Bob_2 and the SI channel from Bob_1 to itself.

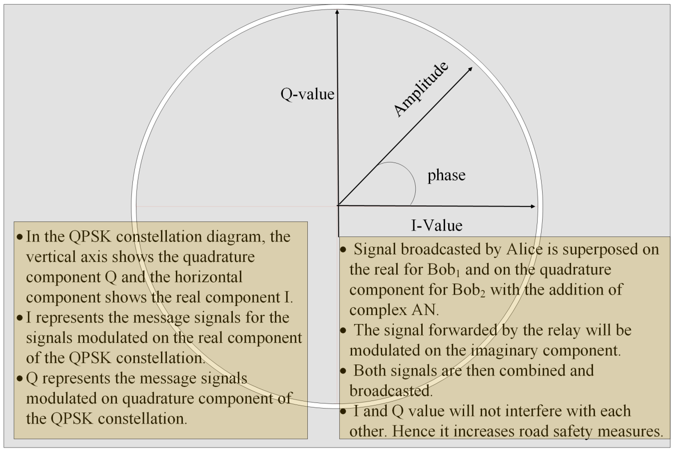

Fig. 2. The exploration of signals' modulation.

Alice modulates the signals, different than the typical modulation of a signal. It modulates the signals of Bob_1 and Bob_2 on the real component of constellation and adds complex Artificial Noise (AN) to make the overall signal complex as shown in fig 2. Bob_1 decodes its own signal and modulates Bob_2's signal on the quadrature component, adds AN and forwards it to Bob_2. If Bob_1 receives the real component then it will forward the quadrature component only. This is to avoid the interference between the received and the forwarded signal in the IBFD mode at Bob_1. There is less interference of the signal at Bob_1 as compared to NOMA with DF-IBFD, the modulated signal is given as $x[t] = (\sqrt{\alpha_1}x_1[t] + \hat{j}\sqrt{\alpha_2}x_2[t])\sqrt{P_T}$, where x_1 and x_2 are the signals for the near and far user and P_T is the total power of transmission,. Due to the modulation technique, ideally there is no interference in the IBFD mode. According to the system model, the near IBFD mode vehicle Bob_1 receives high power signals of far users therefore it can assist far user Bob_2 with R-IBFD cooperative communication. After decoding its own signal from the total received signal Bob_1 adds AN A_2, null space of g_{12}, forwards the signal of Bob_2 by encoding it on the quadrature component, using R-IBFD, like a reflector, to assist Bob_2. For forwarding the signal, Bob_1 uses the power P_c. Bob_1's signal is modulated on real component and it forwards the signal of quadrature component.

A. *Addition of Artificial Noise for Improved Security*

AN is an efficient way for the protection of transmission signals from an Eve and other users [15]. AN system design depends on the receiver's channel but not on the Eve's channel. AN is generated prior to the transmission of signal by Alice and Bob_1 to degrade the Eve's channel. Both the signal x and the AN, A_n, are complex Gaussian in nature. In case of the fixed AN, the value of $||g_e A_n||$ might be smaller. To avoid this situation the value of AN is considered as the Gaussian random variable in the null space of g_n of the Bob's channels respectively, such that $g_n A_n$ is 0 [15]. The superposed signal by the Alice for the broadcast can be given as; $s_1[t] = \sqrt{g_1 P_T}(\sqrt{\alpha_1}x_1[t] + \sqrt{\alpha_2}x_2[t]) + A_1$. Likewise, Bob_1 add A_2 before forwarding the signal of Bob_2 as $s_2[t] = x_2[t]\hat{j} + A_2$.

B. *System Analysis*

The signal received by Bob_1 also includes the self-interference for its co-channel transmission as [17]:(2);

$$y_1[t] = K_1 {d_0}^{\gamma} {d_1}^{-\gamma}\left[\sqrt{g_1 P_T}\left(\sqrt{\alpha_1}x_1[t] + \sqrt{\alpha_2}x_2[t]\right)\right] + \sqrt{g_{11}[t]P_c}\,s[t]\hat{j} + w_1[t], \quad (1)$$

where $w_n \sim CN(0, \sigma^2)$ is the additive white Gaussian noise (AWGN) and $s[t]$ is the signal transmitted by Bob_1 (received along with the previous transmission) to Bob_3 in the IBFD mode, which causes self-interference, K_n is the Path loss factor for node n, d_0 is reference distance, P_c is the power allocated by Bob_1 and γ is the path loss exponent.

The total received signal at Bob_2 from Bob_1 is given in [17]:(5),

$$y_{12}[t] = K_{12} {d_0}^{\gamma} {d_{12}}^{-\gamma}\sqrt{g_{12}P_c}\,x_2\hat{j}[t-\tau] + w_2[t]. \quad (2)$$

In the above equation the signal received from Bob_1 contains only the real part, as $g_{12}A_2 = 0$. The IBFD cooperative communication is used for Bob_2; therefore, without the loss of generality a delay τ has been introduced.

Eve's received signal can be determined by adding AN in (2). Eve receives signal with high interference due to lack of information about AN and the modulation alteration used.

$$y_e[t] = K_{1e} {d_0}^{\gamma} {d_{1e}}^{-\gamma} g_{1e}[t]\left(\sqrt{P_c}x_2[t-\tau]\hat{j} + A_2\right) + w_e[t]. \quad (3)$$

IV. Performance Evaluation

For the evaluation of a system: capacity, secrecy capacity, secrecy outage probability and throughput are some of the important parameters to prove authenticity and usefulness of any system.

A. *Computation of Secrecy Capacity*

Each node received a certain level of SINR or SNR depending on its channel condition and the interference. In this paper, SINR and SNR will be used interchangeably and is denoted as ζ. The respective received ζ of the Bob_2 and Eve are given as:

$$\zeta_2 = \min\left\{\frac{\zeta_{a1}}{\zeta_{11}+1}, \zeta_{12}\right\} \quad (4)$$

and

$$\zeta_e = \zeta_{re}, \quad (5)$$

where $\zeta_{a1} = \frac{\alpha_1 P_T}{G}{}_{a1}\sigma^2$, $\zeta_{11} = \frac{P_c G_{11}}{\sigma^2}$, $\zeta_{12} = \frac{\alpha_2 P_T}{G}{}_{12}\sigma^2$ and $\zeta_{1e} = \frac{\alpha_2 P_T}{G}{}_{1e}A_2 G_{1e} + \sigma^2$ which follows the exponential distribution with parameter $\lambda_{a1} = \frac{\alpha_1 P_T}{G}{}_{a1}\sigma^2$, $\lambda_{11} = \frac{a_2 G_{11}}{\sigma^2}$, $\lambda_{12} = \frac{\alpha_2 P_T}{G}{}_{12}\sigma^2$, $\lambda_{1e} = \frac{\alpha_2 P_T}{G}{}_{1e}A_2 + \sigma^2$ and $G_{ni} = K_{ni}{d_0}^{\gamma}{d_{ni}}^{-\gamma}g_{ni}$. For λ_{1e}, it is assumed that $\sigma^2 = \sigma^2/G_{1e}$. The subscripts 1, 2, 11, 12, $a1$ and $1e$ show the parameters for Bob_1 Bob_2, between Bob_1 and itself, Bob_1 and Bob_2, Alice and Bob_1, Bob_1 and Eve.

The achievable data rate for the Bob_2 and the Eve is given as:

$$R_2 = \log_2\left(1 + \min\left\{\frac{\zeta_{a1}}{\zeta_{11}+1}, \zeta_{12}\right\}\right), \quad (6)$$

and

$$R_{1e} = \log_2\left(1 + \zeta_{1e}\right). \quad (7)$$

The possible secrecy capacity of the system for R-IBFD system is given as

$$C_{sec} = \max\{0, R_2 - R_{1e}\}, \quad (8)$$

$$C_{sec} = \max\left\{0, \log_2\left(\frac{1 + \min\left\{\frac{\zeta_{a1}}{\zeta_{11}+1}, \zeta_{12}\right\}}{1 + \zeta_{1e}}\right)\right\}. \quad (9)$$

B. Relay Selection

For the better secrecy performance in the presence of Eve an opportunistic relay selection scheme is used [17]. The scheme is based on the selection of the relay amongst K relays that maximizes the secrecy capacity of the system

$$R_s = \arg \max_{k=1,\cdots,K} \left[\frac{1+\min\left\{\frac{\zeta_{a1}}{\zeta_{11}+1}, \zeta_{12}\right\}}{1+\zeta_{1e}} \right]. \tag{10}$$

where R_s is the selected user (Bob_1). Whilst selecting the user to relay the signal, the relay selection scheme is considering the channel between near users and the Eve.

A centralized approach is used in this paper, where the source or destination keeps record of the K relays and their CSI. Using the criteria of (10), the best relay for the transmission is decided.

C. Computation of Secrecy Outage Probability

For the derivation of proposed system's Secrecy Outage Probability (SOP), the min-max approached is used. The SOP for R-IBFD cooperative communication for the relay selection scheme is given as:

$$\begin{aligned} S_{op} &= Pr[C_{sec}^{R_s} < C_{th}] \\ &= Pr\left[\log_2\left(\frac{1+min\{\frac{\zeta_{a1}}{\zeta_{11}+1}, \zeta_{12}\}}{1+\zeta_{1e}}\right) < C_{th}\right], \\ &= \prod_{k=1}^{K}\int_0^\infty Pr\Big[\log_2\Big(1+min\Big\{\frac{\zeta_{a1}}{\zeta_{11}+1}, \zeta_{12}\Big\}\Big) < a+by\Big] \\ & f_{\zeta_{1e}}(y)dy, \\ &= \prod_{k=1}^{K}\int_0^\infty F_Z(a+by) f_{\zeta_{1e}}(y)dy. \end{aligned} \tag{11}$$

where $Pr[.]$, $f_X(.)$ and $F_X(.)$ are the notation for probability, Probability Density Function (PDF) and Cumulative Distributive Function (CDF). $a = 2^{C_{th}} - 1$, $b = 2^{C_{th}}$, $y = \gamma_{1e} \geq 0$ and $f_{\zeta_{1e}} = e^{-\frac{y}{\lambda_{1e}}}/\lambda_{1e}$. The CDF $F_Z(z)$ of the random variable Z is derived in Appendix A and is given as

$$F_Z(z) = 1 - \frac{\lambda_{a1}}{\lambda_{a1}+\lambda_{11}z} e^{-z(\frac{1}{\lambda_{a1}}+\frac{1}{\lambda_{12}})}. \tag{12}$$

Substituting the required parameter and considering $\zeta_{a1} = \zeta_{12}$ the SOP is given as

$$\begin{aligned} S_{op} &= \prod_{k=1}^{K}\int_0^\infty 1 - \frac{\lambda_{a1}}{\lambda_{a1}+\lambda_{11}z} e^{-z(\frac{1}{\lambda_{a1}}+\frac{1}{\lambda_{12}})} \frac{e^{-\frac{y}{\lambda_{1e}}}}{\lambda_{1e}} dy. \\ &= \left(\frac{e^{-\frac{2a}{\zeta_{a1}}}}{b\zeta_{1e}\zeta_{11}}\Big(be^{\frac{2a}{\zeta_{a1}}}\zeta_{1e}\zeta_{11} + e^L\Gamma\zeta_{a1} + e^L\zeta_{a1}\log \right. \\ & \left(\frac{1}{\zeta_{1e}} + \frac{2b}{\zeta_{a1}}\right) - e^L\zeta_{a1}\log\left(\frac{b\zeta_{11}}{a\zeta_{11}+\zeta_{a1}}\right) - \zeta_{a1} \\ & \left. 1F1^{(1,0,0)}[1,1,L]\Big)\right)^K. \end{aligned} \tag{13}$$

The above expression is the conditional expression with $\text{Re}[p] > 0$ and $\text{Re}[1/\zeta_{1e} + 2b/\zeta_{a1}] \geq 0$ where $L = \frac{(2b\zeta_{1e}+\zeta_{a1})(a\zeta_{11}+\zeta_{a1})}{b\zeta_{1e}\zeta_{11}\zeta_{a1}}$, Γ =EulerGamma and $1F1[1,0,0]$ is the Kummer confluent Hypergeometric function. Wolfram Mathematica software is used for the derivations of this paper.

D. Secrecy Throughput Evaluation

Throughput is another significant system parameter that can clarify the authenticity of a system. The throughput in a R-IBFD system, when the relay uses its internal power for the transmission of $Bob_2's$ signal is given as

$$\mathcal{TP} = C_{th}(1 - S_{op}). \tag{14}$$

V. Numerical Results

In this section, we discuss the simulated results comparison between the proposed R-IBFD and DF-IBFD cooperative communication system. For the simulation of the systems' comparison, Rayleigh flat fading channel and 16-QAM has been considered. Other numerical values that have been used for the simulation are given as; d_{a1} = 0.2 m, d_{12} = 0.8 m, γ = 2, P_T = 1 W, P_1 = 0.2 W and P_2 = 0.8 W. In this paper, Matlab is used as a simulation tool for the comparison between the proposed and the baseline scheme.

For the fair comparison between R-IBFD and DF-IBFD, all selected parameters are same including AN. The only difference is the interference level during the IBFD mode in both techniques.

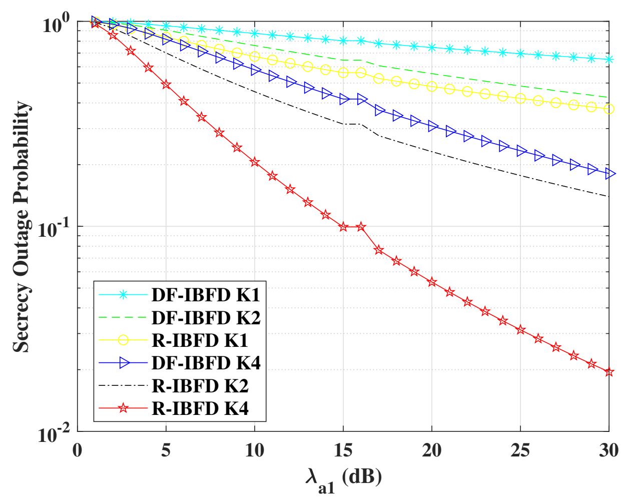

Fig. 3. Secrecy outage probability comparison for Reflective In-Band Full Duplex (R-IBFD) and Decode-and-Forward In-Band Full Duplex (DF-IBFD) with $C_{th} = 1$, $\zeta_{12} = \zeta_{11} = 12dB$, K=1, 2 and 4 and ζ_{1e} is calculated with respect to Rayleigh flat fading and respective interference.

Fig. 3, shows the comparison for the secrecy outage probability offered by DF-IBFD and R-IBFD. In figure 3, the transmitted powers of Alice P_1 and the relay P_2 are chosen according to NOMA power allocation strategy. To show the different response with respect to the number of K relays present for selection, we simulated the results for K=1, 2 and 4. SOP result for both algorithms decreases with the increase of SNR. However, R-IBFD outperforms DF-IBFD, due to less interference in the R-IBFD. For proposed technique the ζ_{1e} is approximately equal to 0 due to high interference at Eve. According to the derived equation of outage probability ζ_{1e} must be greater than zero. Therefore, for simulation purpose we have considered $\zeta_{re} = 0.1$ for R-IBFD.

Fig. 4, shows the increasing throughput with SNR for DF-IBFD and R-IBFD schemes. To demonstrate a diverse scenario with respect to the number of relays K, this paper presents the results for K=1, 2 and 4 . Throughput of R-IBFD is higher due to its low SOP as compared to DF-IBFD algorithm. It can be seen from figures that with $K = 4$ the throughput is optimum. The level of throughput depends on the relay(s) selection. Also the proposed R-IBFD with $K = 2$ performs better than DF-IBFD with $K = 4$. Minimum interference in R-IBFD makes it reliable. It is due to the fact that in

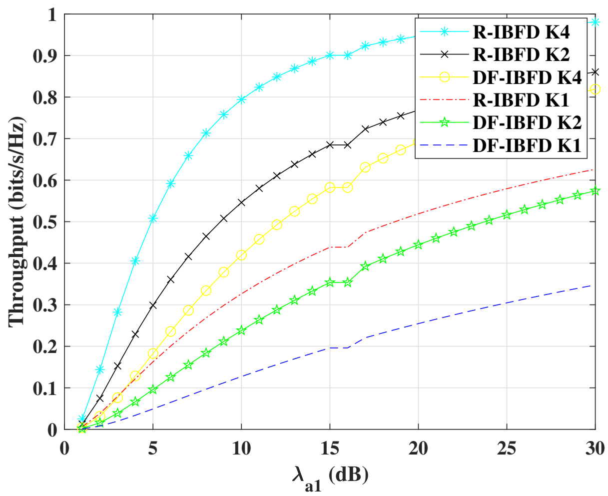

Fig. 4. Throughput comparison for Reflective In-Band Full Duplex (R-IBFD) and Decode-and-Forward IBFD (DF-IBFD) with $C_{th} = 1$, $\zeta_{12} = \zeta_{11} = 12dB$, K=1, 2 and 4 and ζ_{1e} is calculated with respect to Rayleigh flat fading and respective interference.

R-IBFD, the message signal uses half bandwidth for the transmission comparatively.

VI. Conclusion

Security and spectral efficiency is compulsory in the future 5G communication systems. This paper addresses the challenges in 5G networks and proposed an R-IBFD algorithm with NOMA to diminish interference and expand the security of an spectral efficient IBFD system. The proposed system improved the SOP and throughput. In the proposed system model, IBFD algorithm is used to save time and bandwidth with the D2D communication. R-IBFD ideally removed the interference in the IBFD mode, therefore, improved the secrecy capacity, SOP and throughput. The comparison of R-IBFD and DF-IBFD is given in section V which shows that the proposed R-IBFD outperforms DF-IBFD scheme with the choice of K relays.

The security management is the challenging concern in the modern system due the connection of secure devices with the cloud. The main advantage of the proposed R-IBFD system is the improvement of the system security due to high interference on the signal received by Eve. It is a basic system that can be extended with other algorithms which are used in the existing literature with DF-IBFD.

Appendix

Derivation for the CDF of $F_Z(z)$

The CDF of the random variable Z, recall that $Z = min\left\{\frac{\zeta_{a1}}{\zeta_{11}+1}, \zeta_{12}\right\}$. For simplicity of the derivation, consider $L = \frac{\zeta_{a1}}{\zeta_{11}+1}$ and $M = \zeta_{12}$. As we know that

$$\begin{aligned} F_Z(z) &= Pr[min(L,M) < z] \\ &= 1 - Pr[min(L,M) < z] \\ &= 1 - Pr[L > z]Pr[M > z] \\ &= 1 - (1 - F_L(z))(1 - F_M(z)). \end{aligned} \tag{A.15}$$

The above equation shows the requirement of CDF of F_L and F_M for obtaining the CDF of Z.

The CDF of F_L is calculated as

$$\begin{aligned} F_L &= Pr\left[\frac{\zeta_{a1}}{\zeta_{11}+1} < z\right] \\ &= \int_{-0}^{\infty} F_{\zeta_{a1}}(l(m+1)) f_{\zeta_{11}}(m)dm \end{aligned} \tag{A.16}$$

By substituting $F_{\zeta_{a1}} = 1 - e^{\frac{-l}{\lambda_{a1}}}$ and $f_{\zeta_{11}}(l) = e^{-\frac{l}{\lambda_{1e}}}/\lambda_{11}$ in the above equation we get

$$F_L = 1 - \frac{\lambda_{a1}}{\lambda_{ar} + \lambda_{11} l} e^{-\frac{l}{\lambda_{a1}}} \tag{A.17}$$

After plugging the obtained CDF of F_L and $F_M = 1 - e^{\frac{-l}{\lambda_{12}}}$ we obtain

$$F_Z(z) = 1 - \frac{\lambda_{a1}}{\lambda_{a1} + \lambda_{11} z} e^{-z\left(\frac{1}{\lambda_{a1}} + \frac{1}{\lambda_{12}}\right)}. \tag{A.18}$$

Acknowledgement

This research work is funded by the University of Strathclyde in Glasgow, UK under the 'Knowledge Exchange Fellowship' program.

References

[1] R. Khan, D.N.K. Jayakody, "An Ultra-Reliable and Low Latency Communications Assisted Modulation Based Non-Orthogonal Multiple Access Scheme, " in *Physical Communication*, 101035, 7 Mar 2020.

[2] X. Yue, Y. Liu, S. Kang, A. Nallanathan and Z. Ding, "Exploiting Full/Half-Duplex User Relaying in NOMA Systems," in *IEEE Transactions on Communications*, vol. 66, no. 2, pp. 560-575, Feb. 2018.

[3] D. Xu, P. Ren and H. Lin, "Combat Hybrid Eavesdropping in Power-Domain NOMA: Joint Design of Timing Channel and Symbol Transformation," in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 4998-5012, June 2018.

[4] X. Chen et al., "When Full Duplex Wireless Meets Non-Orthogonal Multiple Access: Opportunities and Challenges," in *IEEE Wireless Communications*, vol. 26, no. 4, pp. 148-155, August 2019.

[5] S. Ata, E. Erdogan, "Secrecy outage probability of inter-vehicular cognitive radio networks," in *International Journal of Communication Systems* 2020 Mar;33(4):e4244.

[6] M. Mohammadi, B. K. Chalise, A. Hakimi, Z. Mobini, H. A. Suraweera and Z. Ding, "Beamforming Design and Power Allocation for Full-Duplex Non-Orthogonal Multiple Access Cognitive Relaying," in *IEEE Transactions on Communications*, vol. 66, no. 12, pp. 5952-5965, Dec. 2018.

[7] X. Li, M. Liu, C. Deng, P. T. Mathiopoulos, Z. Ding and Y. Liu, "Full-Duplex Cooperative NOMA Relaying Systems With I/Q Imbalance and Imperfect SIC," in *IEEE Wireless Communications Letters*, vol. 9, no. 1, pp. 17-20, Jan. 2020.

[8] R. Khan, P. Kumar, D. N. K. Jayakody and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196-248, First quarter 2020.

[9] Q. Ding, M. Liu and Y. Deng, "Secrecy Outage Probability Analysis for Full-Duplex Relaying Networks Based on Relay Selection Schemes," in *IEEE Access*, vol. 7, pp. 105987-105995, 2019, doi: 10.1109/ACCESS.2019.2932135.

[10] B. C. Nguyen ,N. N. Thang, T. M. Hoang, and L. Dung "Analysis of Outage Probability and Throughput for Energy Harvesting Full-Duplex Decode-and-Forward Vehicle-to-Vehicle Relay System," in *Wireless Communications and Mobile Computing*vol. 2020, Article ID 3539450, 10 pages, 2020. https://doi.org/10.1155/2020/3539450

[11] L. Zhang, M. Xiao, G. Wu, M. Alam, Y. Liang and S. Li, "A Survey of Advanced Techniques for Spectrum Sharing in 5G Networks," in *IEEE Wireless Communications*, vol. 24, no. 5, pp. 44-51, Oct 2017.

[12] D. T. Do, T.T. Nguyen, T. N. Nguyen, X. Li, Y. Liang and X. Li, "Uplink and Downlink NOMA Transmission Using Full-Duplex UAV," in *IEEE Access*, vol. 8, no. 5, pp. 164347-164364, 2020.

[13] S. Kim and W. Stark, "Full duplex device to device communication in cellular networks", *2014 International Conference on Computing, Networking and Communications (ICNC)*, Honolulu, HI, 2014, pp. 721-725, doi: 10.1109/ICCNC.2014.6785425.

[14] R. Khan, D.N.K. Jayakody, H. Pervaiz and R. Tafazolli, “ Modulation Based Non-Orthogonal Multiple Access for 5G Resilient Networks”, *IEEE Globecom Workshops (GC Wkshps)*(pp. 1-6). IEEE, Dec 2018.

[15] S. Goel and R. Negi, “Guaranteeing Secrecy using Artificial Noise,” in *IEEE Transactions on Wireless Communications*,vol. 7, no. 6, pp. 2180-2189, June 2008.

[16] K. Rabia, D.N.K. Jayakody, “Full Duplex Component-Forward Cooperative Communication for a Secure Wireless Communication System,” in *Electronics*, 9, 2102, Dec. 2020.

[17] Z. Zhang, Z. Ma, M. Xiao, Z. Ding and P. Fan, “Full-Duplex Device-to-Device-Aided Cooperative Non-orthogonal Multiple Access,” in *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4467-4471, May 2017.