sensors

MDPI

Article

Interference Management with Reflective In-Band Full-Duplex NOMA for Secure 6G Wireless Communication Systems

Rabia Khan [1,*], Nyasha Tsiga [2] and Rameez Asif [3]

[1] Power Networks Demonstration Centre, University of Strathclyde, Glasgow G1 1XH, UK
[2] Mechanical Engineering, Moscow Automobile and Road Construction State Technical University (MADI), 125319 Moscow, Russia; tsiga.nyasha@yahoo.com
[3] School of Computing Sciences, University of East Anglia, Norwich Research Park, Norwich NR4 7TJ, UK; rameez.asif@uea.ac.uk
[*] Correspondence: rabia.khan@strath.ac.uk or rabsnt@outlook.com

Abstract: The electromagnetic spectrum is used as a medium for modern wireless communication. Most of the spectrum is being utilized by the existing communication system. For technological breakthroughs and fulfilling the demands of better utilization of such natural resources, a novel Reflective In-Band Full-Duplex (R-IBFD) cooperative communication scheme is proposed in this article that involves Full-Duplex (FD) and Non-Orthogonal Multiple Access (NOMA) technologies. The proposed R-IBFD provides efficient use of spectrum with better system parameters including Secrecy Outage Probability (SOP), throughput, data rate and secrecy capacity to fulfil the requirements of a smart city for 6th Generation (6thG or 6G). The proposed system targets the requirement of new algorithms that contribute towards better change and bring the technological revolution in the requirements of 6G. In this article, the proposed R-IBFD mainly contributes towards co-channel interference and security problem. The In-Band Full-Duplex mode devices face higher co-channel interference in between their own transmission and receiving antenna. R-IBFD minimizes the effect of such interference and assists in the security of a required wireless communication system. For a better understanding of the system contribution, the improvement of secrecy capacity and interference with R-IBFD is discussed with the help of SOP derivation, equations and simulation results. A machine learning genetic algorithm is one of the optimization tools which is being used to maximize the secrecy capacity.

Keywords: 6G; B5G; in-band full-duplex; reflective-in-band full-duplex; non-orthogonal multiple access; machine learning genetic algorithm; secrecy capacity

check for updates

Citation: Khan, R.; Tsiga, N.; Asif, R. Interference Management with Reflective In-Band Full-Duplex NOMA for Secure 6G Wireless Communication Systems. *Sensors* **2022**, *22*, 2508. https://doi.org/10.3390/s22072508

Academic Editors: Hao Wang, Małgorzata Kujawska, Vijayakumar Varadarajan, Han-Chieh Chao, Lidia Dobrescu, Sheng-Lyang Jang, Yi Wu, Wen-Cheng Lai, Adam W. Skorek and Rashmi Bhardwaj

Received: 3 January 2022
Accepted: 22 March 2022
Published: 25 March 2022

1. Introduction

The progression of technology requires a smart way of enactment of the available state of the resources with the new and smart algorithms. Recently, 5G is implemented in metropolitan cities of the world using high-frequency ranges of the spectrum. High frequencies are considered harmful for the health and well-being [1]. Sophisticated use of the whole existing electromagnetic spectrum perhaps reduces the threats and risks for organisms. Several approaches have been investigated [2] by targeting the high-quality throughput with the existing proposed technologies like Full-Duplex (FD) and Non-Orthogonal Multiple Access (NOMA). FD and NOMA both focus on the efficient utilization of the spectrum for developing a system with better Spectral Efficiency (SE) by the thought-provoking way of spectrum exploitation. The current execution of 5G is mostly based on the Orthogonal Frequency Division Multiple Access (OFDMA) due to the high cost limitation for an entirely new NOMA based system. The 4G system is also based on OFDMA, therefore, the application of 5G on the existing 4G infrastructure is comparatively easier and cost-effective. Keeping the consideration of spectrum limitation, it will be better to extend the system further by using NOMA for the 5G onward technologies.

1.1. Related Work

The incorporation of NOMA with FD is a challenging yet promising approach for the 6*G* technology. The idea of combining NOMA with FD can improve the SE and the combination will also help in managing the drawbacks of each technology. Regarding the hardware progression in the propagation and digital and analogue domains [3], several studies have been put forward for the combination of both promising techniques. Table 1 shows the comparative study of the existing FD-NOMA literature.

Table 1. Comparison study of existing papers that include NOMA with OFDMA.

Citation	Theme	Discussed Technologies	Target
[4]	C-RAN-based FD-NOMA	Relay-based cooperative communication and D2D	Performance comparison and measurements
[5]	Applications of FD-NOMA	Cellular, relay and cognitive radio	Comparison and discussion
[6]	QoS with 5G spectrum	FD, massive MIMO, NOMA, SWIPT	Performance evaluation and comparison between the technologies
[7]	Combination of potential technologies	massive MIMO, mmWave, FD, NOMA, carrier aggregation, CR, and network ultra-densification	Combined coupling factors, problems and possible solutions for the existing literature combination
[3]	Spectrum Sharing in 5G	D2D, in-band FD, NOMA, and LTE	Discussion of research methodologies and challenges in 5G networks

The existing literature explores the advantages of FD and NOMA. For maintaining a balance between FD and Half-Duplex (HD) [8], the transmission switching mode from HD to FD and vice versa is one of the common approaches of communication. Beamforming is another successful approach for NOMA and FD. It can improve the data rate of a particular user with power allocation management [9]. It also provides a better ergodic sum-rate than HD [10]. However, the HD outperforms FD at high Signal-to-Noise-Ratio (SNR) in terms of outage probability and in the delay-tolerant transmission [8,10]. There are several approaches for successful implementation for NOMA and FD with high data rate [9] and ergodic sum-rate [10] including beamforming. Cognitive Radio-based NOMA (CR-NOMA) with femtocells is a good strategy for the deployment of NOMA using pairing techniques of the near and far users [11] and for the improvement of system overall performance.

A communication system is based on several layers, each layer has different requirements of security due to multiple connected objects in the beyond 5G [12]. Physical Layer Security (PLS) is one of the main concerns in a smart system. This literature focuses on the PLS. For PLS there are two types of eavesdropper/s (Eve) that cause threats to security; active and passive. It can be amongst the trusted intended user or an outsider. Several existing algorithms are obliging for tackling the issues of PLS, however, due to the advancement of technology, the security threats are also getting advanced. The enactment of technology everywhere including; banks, buildings, security systems, houses, schools, accounts, industries and transportation makes everything vulnerable. One of the possible ways of handling security issues of jamming and eavesdropping for a hybrid eavesdropping (passive eavesdropping on the transmission source and the reactive jamming on legitimate users) of FD-NOMA is by exhausting eavesdropper by increasing its decoding complexity [13]. After the development of a numerous algorithms [12–14], the security of a wireless communication system still needs improvement.

In the traditional communication system, each device is capable of dual communication with a transmission and a reception task called HD communication. In HD, the channel is shared between the dual tasks, with orthogonal (different) time slots or orthogonal frequency bands (out-of-band FD mode). FD allows a device to broadcasts and receives the signals in the same frequency band and time slot [15]. There are two types of FD: the Out-of-Band FD (OBFD) (which is a kind of HD) and the In-Band FD (IBFD) where the transmission and reception of the signal take place at the same time slot and frequency band. In terms of network capacity, system reliability, sum rate and other theoretical aspects IBFD is superior to conventional HD [3].

Three ways for the deployment of the IBFD are shown in Figure 1: (a) shows the combined NOMA downlink and uplink system where the transmitter and the recipient can simultaneously transmit and receive the signals, (b) shows the Device-to-Device (D2D) NOMA communication system, where the near user forwards the signal to the far user with and without a direct link between the near and far user, (c) shows the Two-Way Relay (TWR) NOMA communication system, where a relay assists the far user by receiving its signals from the transmitter. The relay forwards the previously received signal in the FD mode along with the reception of a new signal in the same time slot.

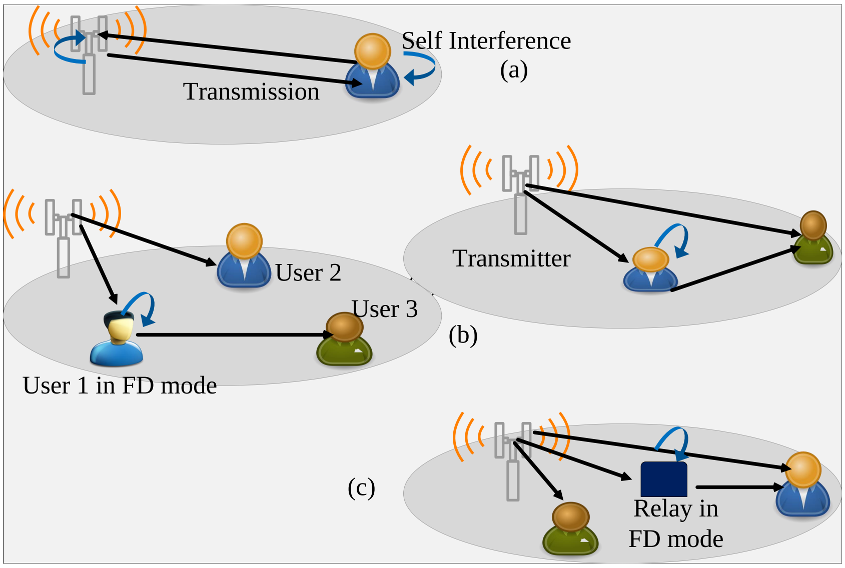

Figure 1. Three different ways of combining FD with NOMA. (**a**) When transmission is in both downlink and uplink. (**b**) D2D communication with a direct and no direct link between transmitter and the distant user. (**c**) The use of a FD mode relay for assisting the distant user.

IBFD and D2D communication have common characteristics including better performance at short distances and reduced self-interference at low power transmit signals [3]. IBFD seems to be more spectrally efficient. Therefore, this literature focuses on the important problems, solutions, benefits, challenges and exploration in the proposed system with IBFD.

In IBFD mode, the wireless nodes cannot decode the signals easily. Characteristically, the transmitted signal is approximately 100 dB higher than the received signal which causes eroded Signal Interference (SI). This reduces its capacity below HD. According to consensus by both academia and industry, it is very difficult to achieve SI cancellation/suppression for IBFD integration [16]. The increasing interference cumulatively reduces the data rate, latency, secrecy capacity and throughput.

RF digital interference cancellation [3], advance antennas cancellation and digital base band, channel estimation and power allocation [4] offers the possible solutions for IBFD. Hybrid resources [17] that switch between FD and HD have been invented for developing the radio resources and simultaneously improving the SE. Separated resources are needed like antennas for the separate transmission with the minimum possible interference. The use of FD with NOMA is also helpful to prevent the spectral resources and the use of other existing devices to avoid system complexity. One solution is proposed in this article with R-IBFD. R-IBFD not only tackles the interference involved but also provide security due to inaccessible information to the Eve.

For the security improvement and confound the eavesdropper, a cooperative jammer [18] is used to analyse the outage performance of the system. A multi-point cooperative relay selection scheme [19], is atypical to the conventional cooperative communication, where each user assists the next further user for downloading its signal until the furthest user downloads its signal successfully. Authors used Channel State Information

(CSI), Rayleigh fading and Nakagami-m fading channel for concluding the proposed approach. For reliability and security of a system with multi-antenna users and eavesdropper, single antenna source and Nakagami-m fading channel, an imbalance in-phase and quadrature component [20] is explored for its influence on the system. An Artificial Noise (AN)-aided cooperative communication scheme with relay firing the jamming signal [21] is proposed, where the ergodic secrecy sum-rate (ESSR) is used to evaluate the system secrecy performance.

For improving sum data rate, an opportunistic relay selection scheme [22] is employed and several wireless communication techniques are used to support the system. A resource allocation problem [23] for an interplay of NOMA, FD and D2D are proposed for sum-rate optimization where a group of strong users assist weak legitimate users.

IBFD can improve conventional wireless communication in terms of time delay, loss of data due to high congestion, hidden terminals and SE. This is to develop a heterogeneous dense network with high capacity and flexible relaying nodes. The quantitative analysis of theoretical and practical deployment shows that at the cost of increased complexity, FD shows high throughput, diversity, low symbol error rate and reduce the use of conventional HD. Alongside interference and security management, the proposed R-IBFD poses the above benefits. The large buffer size for FD devices can additionally reduce the Packet-Loss-Ratio (PLR) [24]. The D2D FD communication performance increases with the increase of in-cell communication ratio that leads to bandwidth efficiency [25]. The IBFD deployment needs new algorithms for the deployment of 6G. It aims to use high-frequency bands like millimetre waves (mmWaves). This is because the low-frequency spectrum is fully utilized with the existing below 5G systems.

To prevent the use of high frequencies, harmful for the health, it is better to reuse the spectrum with FD or NOMA for higher SE and better utilization of lower frequency bands.

NOMA offers a high bandwidth efficiency when implemented with IBFD. There are several types of NOMA. Categorically, power domain NOMA and code domain NOMA are the two major divisions. This paper focuses on the power domain NOMA with IBFD. This paper elaborates the problems, solutions, benefits and challenges offered for power domain NOMA.

In NOMA, the power is allocated with respect to the distance and the channel condition of the individual user, in the same frequency band. The user far from the transmitter needs the highest power allocation. The power allocation decreases with the distance and the improvement of the channel condition. The transmitter superposes signals of all users before transmission. The sum of all user's power coefficients is always equal to 1. $\alpha_1 + \cdots + \alpha_N = 1$, where α is the coefficient of power allocation and N is the total number of user/s. At each receiving node, the nearest strong users need to do Successive Interference Cancellation (SIC) for all users' signals that have power higher than its own signal. Similarly, other users decode their signals. The furthest weak user does not receive the high power signals of other users; therefore, it considers the power of others users with the better channel conditions as noise to decode its own signal [26].

Amongst many problems of NOMA, strong interference, SIC complexity and the use of high-power allocation are the major problems. Installation of the NOMA algorithm requires high computational power for both real-time power allocation and successive interference cancellation. The new technologies such as IoT, Multiple Input and Multiple Output (MIMO), high-speed web, interactive multimedia processing and TV streaming also require energy consumption. Normal battery life for integrating the technologies in 6G will not be sufficient.

There are a number of possible proposed solutions to overcome the interference and to maintain the balance in the system in terms of high-power allocation requirements. FD Cooperative NOMA (FD-CNOMA) shows better system fairness as compared to HD Cooperative NOMA (HD-CNOMA). However, the hybrid combination of switching between HD and FD communication is also a suitable way to maintain a balance between the interference problems [5]. Space-Time Block Coding NOMA (STBC-NOMA) is one of the approaches that are helpful for reducing SIC complexity in the system using Alamouti distributed STBC [27]. Modulation based NOMA (M-NOMA) is one of the techniques that offer reduced interference, less SIC complexity and is also energy efficient [28].

Depending on the available CSI, a singular value decomposition scheme [29] is proposed for solving security issues that arise using NOMA-MIMO implementation and secrecy rate analysis. The system analysis of a two-way cooperative relay NOMA communication [30] is observed with the joint effect of imperfect SIC and quadrature and in-phase imbalance and Rician fading channel. Performance degradation with an increased number of users is caused due to high SIC on each user's end [31], to analyse the system symbol error probability is derived and simulated for imperfect SIC and Space-Time Block Code (STBC) aided NOMA with timing offsets.

A Matlab platform is designed [32] for system and link-level analysis and Long-Term Evolution (LTE) is used as a baseline technique for Bit Error Rate (BER) and capacity comparison. A two-hop relay selection NOMA for IoT communication system [33] is considered to enhance secrecy performance. Using a Tchebycheff approach [34], a system for a secure FD NOMA and SWIPT is studied with power minimization and multi-objective optimization problems.

To permit an effective Dynamic Power and Channel Allocation (DPCA) in the DL multi-channel NOMA (MC-NOMA) systems [26], the optimization as the combinative problem, and offers three investigative solutions, i.e., two-stage Greedy Randomized Adaptive Search (GRASP), stochastic algorithm, and two-stage Stochastic Sample greeDy (SSD). For shortage of frequency band resources, a Terrestrial-Satellite Integrated Network (TSIN) for ground users in [35] is evaluated with NOMA.

NOMA is an essential component for the upcoming 5G technology which will provide a promising SE. The allocation of subcarriers to the users of poor channel conditions affects the SE of the system in OMA. NOMA allows the use of the channel by all users together and offers user fairness, massive connectivity, low latency and diverse QoS. However, interference, system computational complexity and the required energy in NOMA still need thoughtful consideration. IoT requires the connection of everything, which seems very interesting but demands a lot. AI and ML together with FD and NOMA seem promising but challenging. Alongside, security is the biggest all-time issue. The security issue needs to be resolved more than the advancement of technology. The more connections amongst objects open, the more loopholes for security and privacy issues.

1.2. Motivation and Contributions

The requirement for innovative spectrum consumption, minimum interference and high security in a 6G wireless communication system motivated us to propose the R-IBFD algorithm. After a thorough study, it has been observed that co-channel interference is the main problem for enabling FD and NOMA in a communication system. A number of algorithms are given by different authors, however, due to the high connectivity of multiple devices, the security problem is not completely resolved. Keeping that in mind, the following are the contributions of this literature:

- A brief literature review for IBFD, NOMA and their system requirements in 6G technology for developing a background for the reader.
- Propose and discuss a novel Reflective In-Band Full-Duplex (R-IBFD) algorithm.
- Use R-IBFD for interference management and security enhancement.
- Derive secrecy outage probability for R-IBFD, for selection of a relay amongst K relays.
- Show the usefulness of the proposed R-IBFD with ML for the forthcoming 6G system with numerous devices and large data.
- Simulate R-IBFD for N-number of users to show minimal interference and security management as compared to baseline NOMA and HD.

This paper is an extension of a published paper in a conference [36] where the proposed algorithm is explored for a two-user system and verified the novelty using secrecy outage probability and throughput of the system.

2. Reflective In-Band Full-Duplex with NOMA in beyond 5G

The proposed R-IBFD aims to assist the relay in forwarding the signal in the IBFD mode. The proposed algorithm is explored for NOMA for improving the SE of the system with minimal interference and better security. For obtaining the benefits of IBFD and NOMA, a reflective IBFD (R-IBFD) cooperative communication algorithm is proposed. The R-IBFD supports the IBFD mode device to forward the message with cooperative communication, ideally without interference. It is slightly different from the existing Decode-and-Forward IBFD (DF-IBFD) cooperative communication. The user in the IBFD mode decodes its own signal by using SIC (real or imaginary) and encodes the signal that needs to be forwarded to an opposite component (real or imaginary) then forwards/reflects the signal to the distant user. The trusted IBFD mode user contains the CSI of other users. Before reflecting, the IBFD mode user adds AN for preventing the security issues. The use of R-IBFD reduces the decoding complexity and co-channel interference at the IBFD mode user.

2.1. System Model

Figure 2 shows the system model for R-IBFD with a D2D cooperative communication for a Downlink (DL) communication system. The proposed system model contains a transmitter (Alice), total N users ($Bobs$) and a passive Eve. Near user/s (Bob_1, $Bob_3, \cdots$) and far users (Bob_2, $Bob_4, \cdots$, Bob_N) are considered to have similar channel conditions. Alice, Bobs and Eve contains a single antenna excluding Bob_1. Alice uses P_T as the total transmission power. Power domain NOMA is used for the allocation of power to each users' signal. α_1, α_2, α_3, α_4, $\cdot$, α_N where $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \cdots + \alpha_N = 1$. The power coefficients are allocated with respect to the distances $d_1 < d_3 < d_2 < d_4 < \cdots < d_N$ and the channel power gain $g_4 \approx g_2 < g_3 \approx g_1$ of each Bob from Alice, statistically and with machine learning. As per consideration, each Bob is facing a Rayleigh fading channel and their CSI are known by Alice and Bob_1. Eve does not have CSI information of the legitimate user/s. The Eve's channel is considered as worse than two near users conditions; therefore, Eve is unable to detect their signals. $g_4 \approx g_2 < g_e < g_3 < g_1$. Eve is capable of detecting the signal of Bob_2 and Bob_4. The other channels included in the transmission are g_{12} and g_{11} are the channels for the R-IBFD communication in the IBFD mode, from Bob_1 to Bob_2 and the SI channel from Bob_1 to itself.

Alice modulates road 1, Bobs' signal on the real component, and road 2, Bobs' signal on the quadrature component of the 16-QAM modulation constellation. This is because real and quadrature components do not interfere with each other, therefore Bobs' signals of road 1 do not interfere with Bobs' signals of road 2. It assists in reducing interference as compared to NOMA signals.

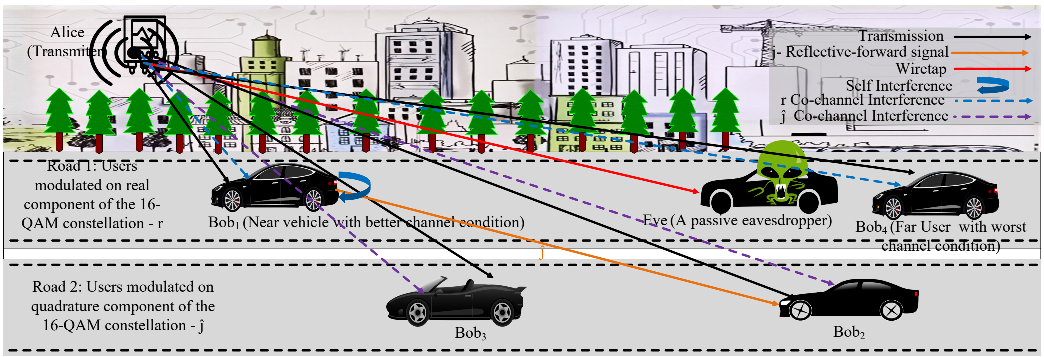
Alice
(Transmitter)
Transmission
ĵ- Reflective-forward signal
Wiretap
Self Interference
r Co-channel Interference
ĵ Co-channel Interference
Road 1: Users modulated on real component of the 16-QAM constellation - r
Bob₁ (Near vehicle with better channel condition)
Eve (A passive eavesdropper)
Bob₄ (Far User with worst channel condition)
ĵ
Road 2: Users modulated on quadrature component of the 16-QAM constellation - ĵ
Bob₃
Bob₂

Figure 2. The system model with an Alice, four Bobs and an Eve. Each Bob is modulated differently following the proposed algorithm, for the reduced NOMA interference. Bob_1 shows the IBFD nature and assists Bob_3 with an R-IBFD transmission. The given system involves self and co-channel interference.

Bob_1 and Bob_4 on road 1 are modulated on the real component and the remaining Bobs of road 2, Bob_2 and Bob_3, are modulated on the quadrature components of the modulation. Therefore, both Bobs of road 1 face the co-channel interference with each other only, as shown in Figure 2. Ideally, there is no interference between the Bobs of different roads. This is to avoid the interference between two high power signals (far users Bob_2 and Bob_4) with each other. Therefore, far users ideally do not interfere with each other, rather faces minor interference due to very low power signal, which can be considered as noise. According to the system model, the near IBFD mode user Bob_1 receives high power signals of far users therefore it can assist far user Bob_2 with R-IBFD. To decode its signal, Bob_1 performs SIC by decoding Bob_4's signal and removing the combined AN A_1 of Bob_2 and Bob_4, then subtracting it from the total received signal. Bob_1 decodes its own signal from the total received signal and adds AN A_2, null space of g_{12}, forward the signal of Bob_2 and Bob_3, using R-IBFD, like a reflector, to assist Bob_2. Bob_3 cannot decode the signal received from Bob_1 due to the addition of A_2 which is a null space of Bob_2's channel. For forwarding the signal, Bob_1 uses the power P_c. Bob_1 receives its signal, which was modulated on real component, it adds AN (A_2) for Bob_2 and forwards the signal of Bob_2 which was modulated on quadrature component as received from Alice. There is self-interference at the IBFD mode, between the complex component of the received signal by Bob_1 and the complex signal forwarded by Bob_1; however, this interference is less than the usual IBFD due to no real component interference.

2.2. Addition of Artificial Noise for Improved Security

AN is a sufficient way for the protection of transmission signals from Eve and other users. System design with AN depends on the receiver's channel but not Eve's channel. It is generated before transmission of a signal by the Alice and Bob_1 to degrade 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 [14].

3. System Analysis for a Two-User System

For the analytical insight of the proposed technique, two users are used to avoid system's complexity. For a two user system, the same situation (Figure 2) is considered with Bob_1 and Bob_2 only. 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 $s_2[t] = x_2[t]\hat{j} + A_2$.

The signal received by Bob_1 also includes the self-interference for its co-channel transmission as given in (2) of [37] :

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

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_2 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 below according to (5) in [37] :

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

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 a signal with high interference due to a lack of information about AN and the modulation alteration used.

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

3.1. Performance Evaluation

For the evaluation of a system capacity, secrecy capacity, secrecy outage probability and throughput are some of the important parameters to prove the authenticity and usefulness of any system. In R-IBFD, the 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 the far-user after adding AN for the R-IBFD cooperative communication. For the selection of relay amongst K relay, a relay selection method is used which is described later in this section.

3.2. 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:

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

and

$$\zeta_e = \zeta_{re}, \tag{5}$$

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:

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

and

$$R_{1e} = \log_2 (1 + \zeta_{1e}). \tag{7}$$

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

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

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

3.3. Relay Selection

For better secrecy performance in the presence of Eve an opportunistic relay selection scheme is used [37]. The scheme is based on the selection of the relay amongst K relays that maximize 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.

3.4. 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

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

The above expression is the conditional expression with $\mathrm{Re}[p] > 0$ and $\mathrm{Re}[1/\zeta_{1e} + 2b/\zeta_{a1}] \geq 0$ 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.

3.5. Secrecy Throughput Evaluation

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

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

4. System Analysis for a Four User System and Machine Learning

The current and forthcoming demand of high data and large number of systems will increase the processing power and system complexity. For such situation, an MLGA is used for the optimization instead of an statistical optimization technique. The superposed signal by the Alice for the broadcast can be given as:

$$s[t] = s_1[t] + s_2[t], \tag{15}$$

where $s_1[t] = \sqrt{P_T}(\sqrt{\alpha_1}x_1[t] + \hat{j}\sqrt{\alpha_2}x_2[t])$ and $s_2[t] = \sqrt{P_T}(\sqrt{\alpha_3}x_3[t] + \hat{j}\sqrt{\alpha_4}x_4[t]) + A_1$.

In this article, each user individually does not have a complex nature. However, it is combined with the signal of another user or/and AN to make the total complex signal. Here, two users are considered to have the same channel conditions, so that we can collectively add the same AN for two users, it will save the bandwidth and the data rate will remain higher. Since the allocation of AN to each user separately needs more bandwidth. Additionally, in this case, adding AN for the near users is not necessary as the Eve cannot decode their signal.

Bob_3 performs SIC to remove Bob_2's high power signal as they are encoded on the same component. Bob_4 decodes the signal by considering Bob_1's low power signal as noise. Bob_3 cannot decode the signal received from Bob_1, as Bob_1 has added A_2, that is the null space of the channel g_{12} of Bob_2 only. The signal received by the Bob_1 also includes the self-interference for its co-channel transmission according to (2) in [37]:

$$\begin{aligned} y_1[t] = K_1 {d_0}^{\gamma} {d_1}^{-\gamma} \Big[& \sqrt{g_1 P_T}\Big(\sqrt{\alpha_1}x_1[t] + \hat{j}\sqrt{\alpha_2}x_2[t]\Big) \\ & + \sqrt{g_1 P_T}\Big(\sqrt{\alpha_4}x_4[t] + \hat{j}\sqrt{\alpha_3}x_3[t]\Big)\Big] + A_1 \\ & + \sqrt{g_{11}[t]P_1 s[t]} + w_1[t], \end{aligned} \tag{16}$$

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_2 in the FD mode, which causes self-interference.

The data rate for the Bob_2 received by Bob_1 is given as:

$$R_{12} = \log_2\left(1 + \frac{G_1 P_T \alpha_2}{G_1 \alpha_3 P_T + 1}\right), \tag{17}$$

where $G_n = K_n {d_0}^{\gamma} {d_n}^{-\gamma} g_n / {\sigma_n}^2$, K_n is the path loss constant, d_0 is the reference distance, d_n is the respective distance of the Bob from Alice and ${\sigma_n}^2$ is the noise variance. For G_2, g_2 is the channel power gain, for G_{12}, g_{12} is the channel power gain between Bob_1 and Bob_2 and so on. The second term of the data rate is the SINR. The data rate of Bob_1 for detecting its own signal is given as:

$$R_1 = \log_2\left(1 + \frac{G_1 P_T \alpha_1}{G_1 \alpha_4 P_T + 1}\right). \tag{18}$$

Similarly, we can write the data rate for Bob_4 received by Bob_3 and the data rate at Bob_3 of its own signal. The IBFD communication is used only for the priority user Bob_2; therefore, without the loss of generality a delay τ has been introduced. The total DL received signal by Bob_2 from Alice and Bob_1 is given below according to (5) of [37]:

$$\begin{aligned} y_2[t] = & \sqrt{g_2 P_T}(\sqrt{\alpha_1}x_1[t] + \hat{j}\sqrt{\alpha_2}x_2[t]) + \sqrt{g_2 P_T}(\sqrt{\alpha_3}x_3[t] \\ & + \hat{j}\sqrt{\alpha_4}x_4[t]) + \sqrt{g_{12}P_c}\hat{j}(x_2 + x_3)[t-\tau] + w_2[t]. \end{aligned} \tag{19}$$

In the above equation, the signal received from Bob_1 contains only the imaginary part, as $g_{12}A_2 = 0$.

Eve's received signal can be determined by adding AN [14] A_1 in the second and A_2 in the third term of (19). Eve receives signals with high interference due to lack of information about AN, the component and R-IBFD. Due to high interference Eve receives a signal with very low SINR and it includes the factor of AN which greatly reduces its achievable data rate/capacity R_{Eve} as given in the following equations:

$$\begin{aligned} y_e[t] = {} & K_e {d_0}^{\gamma} {d_e}^{-\gamma} \Big[g_e \Big(\sqrt{P_T}(\sqrt{\alpha_1} x_1[t] + \hat{j}\sqrt{\alpha_2} x_2[t]) \Big) \\ & + g_e \Big(\sqrt{P_T}(\sqrt{\alpha_4} x_4[t] + \hat{j}\sqrt{\alpha_3} x_3[t]) + A_1 \Big) \Big] + \\ & K_{1e} {d_0}^{\gamma} {d_{1e}}^{-\gamma} g_{1e}[t] \Big(\sqrt{P_c}(x_2 + x_3)[t-\tau]\hat{j} + A_2 \Big) + w_e[t] \end{aligned} \tag{20}$$

and

$$\begin{aligned} R_{\text{Eve}} = {} & \log_2 \Big(1 + \frac{G_{1e} P_1}{G_{1e}|A_2|^2 + 1} + \\ & \frac{G_e P_T \alpha_3}{G_e P_T(\alpha_1 + \alpha_2 + \alpha_4) + G_e |A_1|^2 + 1} \Big), \end{aligned} \tag{21}$$

where G_n is the total Rayleigh flat fading channel including path loss. Eve is facing interference due to all other signals as shown by α_n in the denominator due to absence of component information. The data rate of Bob_2 and Bob_4 is sufficiently high, because of no interference of the other road's users and no A_n in the denominator in the equation. Above are the equations for R-IBFD. For other baseline techniques, equations can be written accordingly.

4.1. Optimization of Reflective IBFD with ML

The increasing demand for the execution of smart systems in the modern B5G necessitates the use of Machine Learning (ML). It seems with the name that ML is cumbersome and needs intelligence. However, the fact is it needs the intelligence of a machine, not a human. ML is generally helpful for a system with big data and more connected devices. Smart transportation systems also need suitable algorithms for optimization. However, the mathematical techniques may not be suitable for system automation where the machines have to make decisions in a limited period of time with the flexibility of variable data and relevant setup. There are several possible ML algorithms that can be useful, in this paper, MLGA is for the optimization of parameters in the proposed system model.

4.1.1. Machine Learning-Based Genetic Algorithm

MLGA is based on the principles of natural collection and genetics. The problems with mixed continuous-discrete variables, discontinuous variables and non-convex spaces entail optimization for the system design. On-line linear programming methods of optimization can also be useful for the aforementioned problems; though, they will lead to computational expenses and inefficiency. Consequently, the usage of MLGA will be productive. Similar to natural genetic progressions, MLGA is also founded on reproduction, crossover and mutation. Figure 3 characterizes the whole technique that is required for the employment of an MLGA in the corresponding optimization problem [28]. The opted randomly generated parameters are used to obtain the fitness function which is the secrecy capacity in this article. If the fitness function does not achieve the required maximum possible value then the algorithm selects the randomly generated parameters, responsible for the current highest fitness function. The selected parameters are mixed together and exploited to obtain better parameters with crossover. The new parameters are being mutated with some of the old parameters to obtain the best possible fitness function. The process goes on until the best fitness function has been obtained.

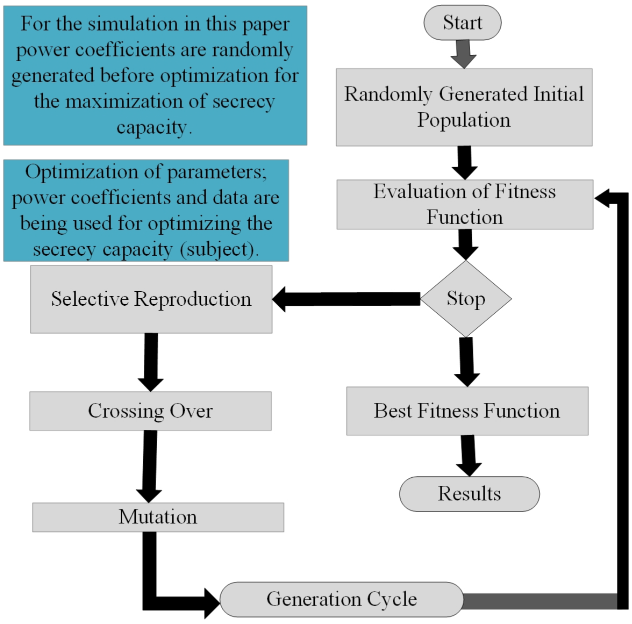
For the simulation in this paper power coefficients are randomly generated before optimization for the maximization of secrecy capacity.
Optimization of parameters; power coefficients and data are being used for optimizing the secrecy capacity (subject).
Start
Randomly Generated Initial Population
Evaluation of Fitness Function
Stop
Selective Reproduction
Crossing Over
Mutation
Best Fitness Function
Results
Generation Cycle

Figure 3. Flow chart description of genetic algorithm based ML.

The MLGA is a suitable ML technique for an optimization problem. It uses the survival-of-the-fittest principle of nature to maximize the fitness function of the offered problem [38]. In this paper, we used the secrecy capacity as the fitness function of the problem.

4.1.2. Sum Secrecy Capacity Optimization Problems

There are several techniques for system optimization; however, the computation efficiency of using unlimited data leads towards the use of MLGA. The optimization of the sum secrecy capacity requires the secrecy capacity of the individual users affected by the Eve. In this system, we have considered Bob_3 and Bob_4 as the affected users.

To make the secrecy capacity better, we optimize it by using MLGA. We deal here with the optimization of the data rate and power coefficients of the system. For optimization of sum secrecy capacity S_T of the system, it is considered as the fitness function of the algorithm as shown in Figure 3.

The individual secrecy capacities of each affected vehicle can be calculated as: $S_n = R_n - R_{ne}$, where $n = \{3, 4\}$. The problem formulation for the secrecy capacity maximization is given as:

$$\text{P1: max:} S_T = \left(R_{Bob_2} - R_{Eve}\right) + \left(R_{Bob_4} - R_{Eve}\right). \tag{22}$$

The constraints on the power coefficient are:

$$\text{C1: } A(\alpha_1, \cdots, \alpha_4) = \textstyle\sum_{n=1}^{4} \alpha_n = 1,$$

$$\text{C2: } \alpha_n > 0, n = \{1, \cdots, 4\}$$

and the SINR ζ_n

$$\text{C3: } \zeta_n > \zeta_T, n = \{1, \cdots, 4\}$$

where ζ_T is the threshold for the received SINR. In the left hand side of the above equation, there are two round brackets that shows the secrecy capacity of Bob_3 with the difference between the capacity of Bob_2 and Eve and Bob_4.

In the secrecy capacity expression, each term shows the received SINR of the respective Bob_n and Eve.

To make the secrecy capacity highly positive we have used the modulation orthogonality and the *AN*. Since Eve does not have the information of the modulation component, therefore it will face more interference and can not decode the information properly. Additionally, the AN increases interference of the Eve. A legitimate user is not affected by AN because it is the null space of the offered channel. The sum secrecy capacity of the system is given as:

$$S_T = R_2 - R_{Eve} + R_4 - R_{Eve}. \tag{23}$$

The above equation clearly shows the dependence on the capacity of Eve and the affected Bobs. Hence, it is highly subjected to the individual's received SINR, channel, power, power coefficient and interference. Eve has lower received SINR and hence low R_{Eve} due to high interference as shown in (21). R_2 and R_4 are higher due to less interference for R-IBFD. Therefore, The secrecy capacity will be highly positive.

5. Use-Cases of Reflective IBFD

There are a number of use-cases for the proposed R-IBFD communication system. In recent years, exponential growth is observed for dense IoT networks for monitoring critical data that need efficient bandwidth and resource allocation. Internet-of-Energy is an upcoming field including digital smart grids, renewable energy resources, electric vehicle infrastructure, smart metering, smart water system, IoT security and privacy, IoT sensing, data analytic, Software-Defined Networking (SDN)-based IoT fog, industrial mobile IoT, etc. Figure 4 shows the IoT communication system that involves the connected world, home IoT system, smartphones and back-end network systems. Figure also lists several latest offered attacks for an IoT system that need serious consideration. Enabling IoT will increase the number of connected devices which requires the better utilization of the spectrum. IBFD communication can improve the spectral efficiency of the IoT system as compared to HD. R-IBFD is an efficient algorithm that can support the IBFD with minimum interference and prevent the system from security threats like eavesdropping, spyware and man-in-the-middle attacks, as the attacker or eavesdropper cannot download the transmitted signals due to offered system limitations.

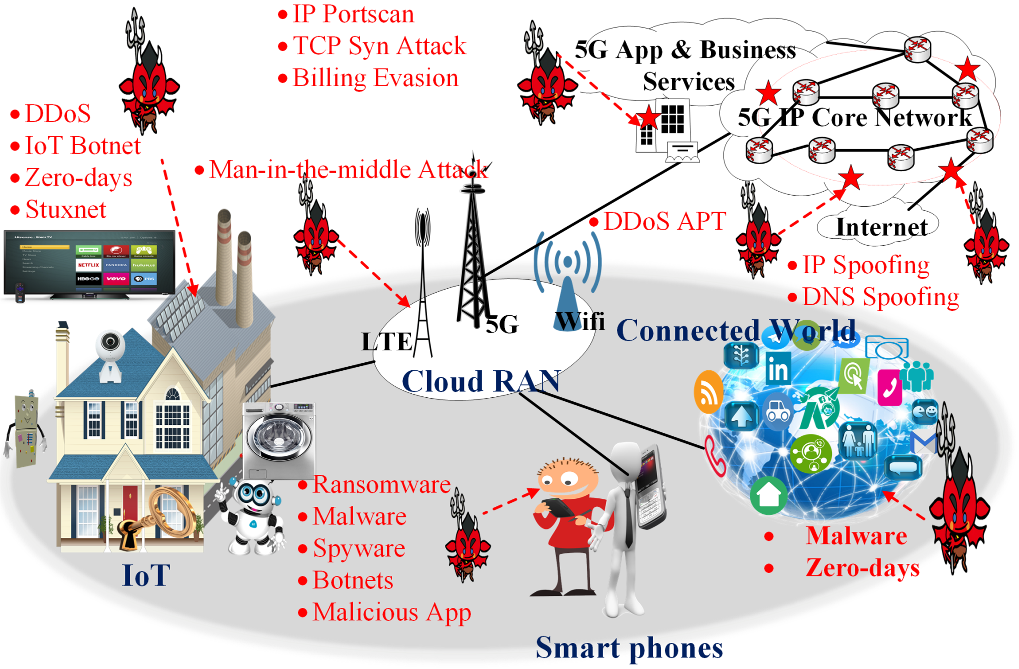

Figure 4. Possible cyber-security attacks in a 5G wireless communication system.

R-IBFD is a reliable system and gives a better data rate and therefore can be explored as an Ultra-Reliable and Low Latency Communication (URLLC) in 5G communication. URLLC is needed for the overall IoT system, especially in emergency situations, like natural disasters. Another use-case of R-IBFD communications is in the IoT in health sectors. Health sectors are sensitive areas that need high security and low interference. R-IBFD can provide ideally no interference if a smaller number of users are connected to a certain bandwidth. It will be reliable, secure and safe for the patients exposed to IoT health devices. It is also beneficial for operations for its reliability and speed.

Other use-cases include the use of helicopters and drones in natural disaster situations. A number of natural disasters lead to the destruction of whole cities and villages. In such cases, 5G wireless communication with R-IBFD can help save lives. It can be used for the indication of lives, rescue, provision of food and resources, etc.

In energy sectors, industry 4.0 is moving towards the deployment of the 5G communication system, particularly where the implementation of fibre is not possible. It includes the rural and mountain areas. R-IBFD can fulfil the requirement of fast, reliable and secure communication for remote areas. Such renewable energy resource sites need constant monitoring; however, it is nearly impossible to deploy staff 24 h a day. Security is another important factor that needs to be considered, not only in the energy sectors to prevent power breakdowns but also for communications where life, fraud, destruction risk and confidentiality is involved.

In this paper, a basic communication system is used as an application for the implementation of the proposed R-IBFD. A brief description of how R-IBDF can be implemented for reliable, fast and secure communication is given in the following sections.

6. Performance Evaluation

6.1. Two-User System

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 the same including AN. The only difference is the interference level during the IBFD mode in both techniques.

Figure 5 shows the comparison for the secrecy outage probability offered by DF-IBFD and R-IBFD. In Figure 5 the transmitted powers of Alice P_1 and the relay P_2 are chosen according to the NOMA power allocation strategy. To show the different responses 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 the 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.

Figure 6 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 the figures that with $K = 4$ the throughput is optimum. The level of throughput depends on the relay(s) selection. Additionally, 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 R-IBFD, the message signal uses half bandwidth for the transmission comparatively.

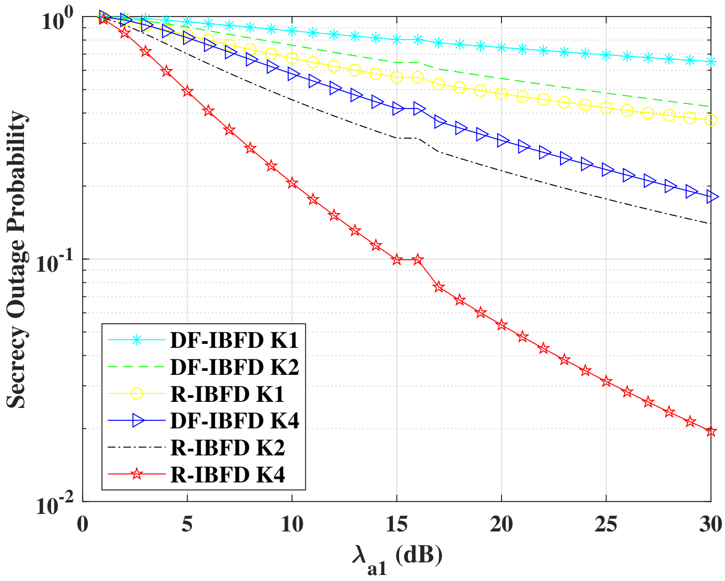

Figure 5. Secrecy outage probability comparison for Reflective In-Band Full-Duplex (R-IBFD) and Decode-and-Forward In-Band Full-Duplex (DF-IBFD) with $C_{th} = 1$, $\zeta_{12} = \zeta_{11} = 12$ dB, K = 1, 2 and 4 and ζ_{1e} is calculated with respect to Rayleigh flat fading and respective interference.

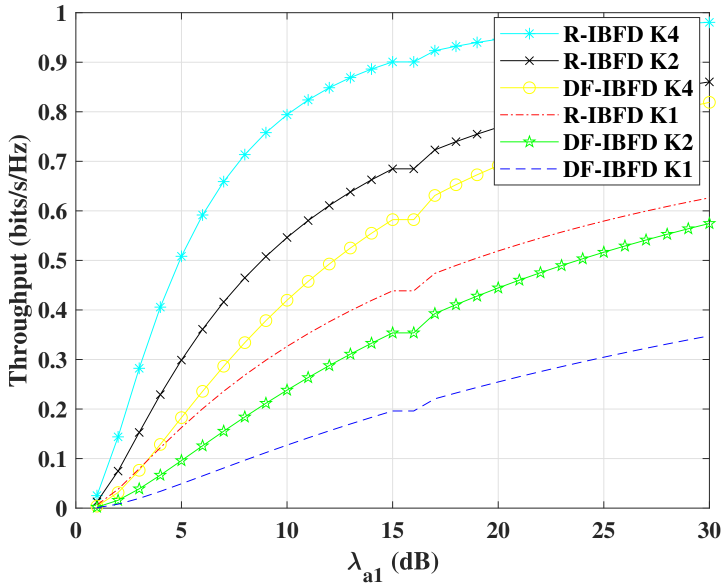

Figure 6. Throughput comparison for Reflective In-Band Full-Duplex (R-IBFD) and Decode-and-Forward IBFD (DF-IBFD) with $C_{th} = 1$, $\zeta_{12} = \zeta_{11} = 12$ dB, K = 1, 2 and 4 and ζ_{1e} is calculated with respect to Rayleigh flat fading and respective interference.

6.2. Four-User System

This section evaluates the proposed R-IBFD system performance. For the simulation 16-QAM modulation, Rayleigh fading channel is used and total transmission power P_T = 1 W is used. Secrecy capacity comparison with baseline techniques is evaluated, MLGA is also used for the optimization of secrecy capacity.

The baseline comparative schemes are NOMA R-IBFD without *AN*, Reflective HD (R-HD), R-HD with *AN* (RA-HD) and R-IBFD with *AN* (RA-IBFD).

Figure 7 shows the simulated result for secrecy capacity with a four-user system and a passive Eve. The comparison of RA-IBFD and R-IBFD with R-HD, RA-HD, and NOMA shows that the proposed RA-IBFD outperforms all other implementations. It is due to the fact (21) that the Eve faces a high amount of interference due to the addition of *AN*, no

CSI information of the Bobs and the desired component of the particular Bob. Therefore, it leads to a significant gain of RA-IBFD.

The high interference on the Eve node increases the difference between the capacities of the respective Bob and the Eve, which leads to the increase of secrecy capacity. Figure 8 shows the simulated result of RA-IBFD with and without MLGA. For MLGA, the power coefficients are generated randomly. For each Bob_i, four random numbers have been generated as the initialized population with respect to distance and with the sum equal to 1. The secrecy capacity is used as the fitness function of the MLGA. The optimized secrecy capacity has been simulated using the MLGA method as shown in Figure 3. The result shows that MLGA further enhances the performance of RA-IBFD due to the optimized parameters subjected to the optimized level of RA-IBFD secrecy capacity. Therefore, the use of MLGA makes improves the secrecy capacity. For a limited number of users as chosen in this article, it is easy to measure system parameters statistically. However, in a system with a high number of users, machine learning is a necessity for a wireless communication system with high data.

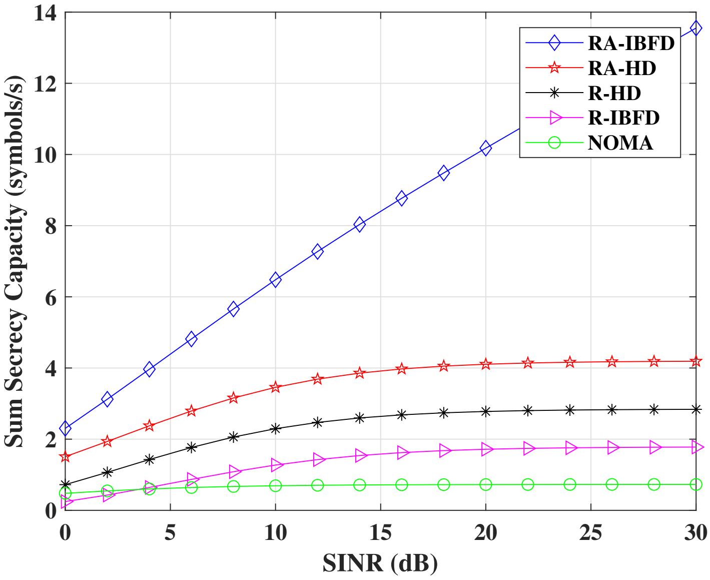

Figure 7. Sum secrecy capacity comparison for Proposed RA-IBFD and R-IBFD with R-HD, RA-HD and NOMA.

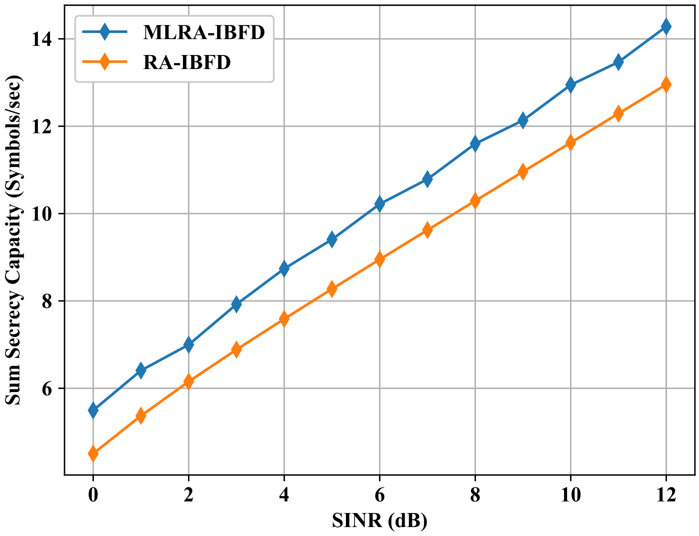

Figure 8. Sum secrecy capacity comparison for Proposed RA-IBFD with and without MLGA.

7. Conclusions

IBFD is a SE technology that can meet the target of the high data demand in the 6G era, where a relay or an existing user assists a far user in an IBFD mode. The exploration of proposed R-IBFD and RA-IBFD has shown the enhancement of the secrecy capacity, along with the SE and reduced interference.

The system fulfils the requirement of high data rate using proposed R-IBFD and RA-IBFD. The high data rate or high capacity will lead towards the management of big data and high secrecy capacity. The ML is a part of the modern systems of wireless communication, it can be used for multiple purposes where it improved the system's performance without altering and disturbing its surrounding. This paper is an extension of a conference paper [36]. In this paper, an SOP equation is derived for a selection of relay in R-IBFD, MLGA is used for the optimization of power coefficients subjected to secrecy capacity of the given system, this will be particularly helpful for dealing with larger number of users and data. Overall, R-IBFD is an efficient system that provides a better transmission data rate and enhances security. Other ML and statistical algorithms can also be used to improve the performance of the proposed algorithm [39], which will be further explored as a part of future research of the proposed algorithm. Alongside the simulation results, use cases of the proposed algorithm are also given in this paper. Further research is highly required for the flexibility of systems with several real-life 6G communication environment that needs to be explored for other security reasons including active attacks during public holidays.

Author Contributions: Conceptualization, R.K.; methodology, R.K.; software, R.K. and N.T.; validation, R.K. and R.A.; formal analysis, R.K.; investigation, R.K.; resources, R.K. and N.T.; writing—original draft preparation, R.K.; writing—review and editing, R.K., N.T. and R.A.; visualization, R.K. All authors have read and agreed to the published version of the manuscript.

Funding: The author acknowledge the internal research start-up funding, reference: 1012606FA1, from University of East Anglia (UEA), Norwich.

Data Availability Statement: This article used randomly generated data for MLGA. Python is used as a tool for the simulation of MLGA, the basic command for randomly generated sequence of Python is used to generate data.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

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

$$\begin{aligned} F_Z(z) &= Pr[min(L,M) < z] \\ &= 1 - Pr[min(L,M) < z] \\ &= 1 - Pr[L > z]Pr[M > z] \\ &= 1 - (1 - F_L(z))(1 - F_M(z)). \end{aligned} \tag{A1}$$

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

$$\begin{aligned} F_L &= Pr\left[\frac{\zeta_{a1}}{\zeta_{11}+1} < z\right] \\ &= \int_{-0}^{\infty} F_{\zeta_{a1}}(l(m+1)) f_{\zeta_{11}}(m)dm \end{aligned} \tag{A2}$$

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

$$F_L = 1 - \frac{\lambda_{a1}}{\lambda_{ar} + \lambda_{11} l} e^{-\frac{l}{\lambda_{a1}}} \tag{A3}$$

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

$$F_Z(z) = 1 - \frac{\lambda_{a1}}{\lambda_{a1} + \lambda_{11} z} e^{-z\left(\frac{1}{\lambda_{a1}} + \frac{1}{\lambda_{12}}\right)}. \tag{A4}$$

References

1. Moradi, M.; Naghdi, N.; Hemmati, H.; Asadi-Samani, M.; Bahmani, M. Effect of Ultra High Frequency Mobile Phone Radiation on Human Health. *Electron. Physician* **2016**, *8*, 2452–2457; Erratum in *Electron. Physician* **2017**, *9*, 4473. [CrossRef] [PubMed]
2. Khan, R.; Jayakody, D.N.K. Full Duplex Component-Forward Cooperative Communication for a Secure Wireless Communication System. *Electronics* **2020**, *9*, 2102. [CrossRef]
3. Zhang, L.; Xiao, M.; Wu, G.; Alam, M.; Liang, Y.; Li, S. A Survey of Advanced Techniques for Spectrum Sharing in 5G Networks. *IEEE Wirel. Commun.* **2017**, *24*, 44–51. [CrossRef]
4. Chen, X.; Liu, G.; Ma, Z.; Zhang, X.; Fan, P.; Chen, S.; Yu, F.R. When Full Duplex Wireless Meets Non-Orthogonal Multiple Access: Opportunities and Challenges. *IEEE Wirel. Commun.* **2019**, *26*, 148–155. [CrossRef]
5. Mohammadi, M.; Shi, X.; Chalise, B.K.; Ding, Z.; Suraweera, H.A.; Zhong, C.; Thompson, J.S. Full-Duplex Non-Orthogonal Multiple Access for Next Generation Wireless Systems. *IEEE Commun. Mag.* **2019**, *57*, 110–116. [CrossRef]
6. Nasir, A.A.; Tuan, H.D.; Duong, T.Q. Fractional Time Exploitation for Serving IoT Users with Guaranteed QoS by 5G Spectrum. *IEEE Commun. Mag.* **2018**, *56*, 128–133. [CrossRef]
7. Yadav, A.; Dobre, O.A. All Technologies Work Together for Good: A Glance at Future Mobile Networks. *IEEE Wirel. Commun.* **2018**, *25*, 10–16. [CrossRef]
8. Yue, X.; Liu, Y.; Kang, S.; Nallanathan, A.; Ding, Z. Exploiting Full/Half-Duplex User Relaying in NOMA Systems. *IEEE Trans. Commun.* **2018**, *66*, 560–575. [CrossRef]
9. Mohammadi, M.; Chalise, B.K.; Hakimi, A.; Mobini, Z.; Suraweera, H.A.; Ding, Z. Beamforming Design and Power Allocation for Full-Duplex Non-Orthogonal Multiple Access Cognitive Relaying. *IEEE Trans. Commun.* **2018**, *66*, 5952–5965. [CrossRef]
10. Li, X.; Liu, M.; Deng, C.; Mathiopoulos, P.T.; Ding, Z.; Liu, Y. Full-Duplex Cooperative NOMA Relaying Systems With I/Q Imbalance and Imperfect SIC. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 17–20. [CrossRef]
11. Budhiraja, I.; Tyagi, S.; Tanwar, S.; Kumar, N.; Guizani, M. Cross Layer NOMA Interference Mitigation for Femtocell Users in 5G Environment. *IEEE Trans. Veh. Technol.* **2019**, *68*, 4721–4733. [CrossRef]
12. Khan, R.; Kumar, P.; Jayakody, D.N.K.; Liyanage, M. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 196–248. [CrossRef]
13. Xu, D.; Ren, P.; Lin, H. Combat Hybrid Eavesdropping in Power-Domain NOMA: Joint Design of Timing Channel and Symbol Transformation. *IEEE Trans. Veh. Technol.* **2018**, *67*, 4998–5012. [CrossRef]
14. Goel, S.; Negi, R.; Guaranteeing Secrecy using Artificial Noise. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2180–2189. [CrossRef]
15. Sergey, S.; Elsayed, A.; Alireza, S.B.; Waleed, Y.; Ahmed, M.E. Frequency and Timing Synchronization for In-Band Full-Duplex OFDM System. In Proceedings of the 2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–7. [CrossRef]
16. Panse, V.; Jain, T.K.; Sharma, P.K.; Kothari, A. Digital Self-interference cancellation in the era of machine learning:A comprehensive review. *Phys. Commun.* **2021**, *50*, 101526. [CrossRef]
17. Firouzabadi, A.D.; Rabiei, A.M.; Vehkaperä, M. Fractional Frequency Reuse in Random Hybrid FD/HD Small Cell Networks With Fractional Power Control. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 6691–6705. [CrossRef]
18. Chen, Y.; Zhang, Z.; Li, B. Cooperative Secure Transmission in MISO-NOMA Networks. *Electronics* **2020**, *9*, 352. [CrossRef]
19. Tran, T.-N.; Voznak, M. Multi-Points Cooperative Relay in NOMA System with N-1 DF Relaying Nodes in HD/FD Mode for N User Equipments with Energy Harvesting. *Electronics* **2019**, *8*, 167. [CrossRef]
20. Li, X.; Zhao, M.; Zhang, C.; Khan, W.U.; Wu, J.; Rabie, K.M.; Kharel, R. Security Analysis of Multi-Antenna NOMA Networks Under I/Q Imbalance. *Electronics* **2019**, *8*, 1327. [CrossRef]
21. Ren, Y.; Tan, Y.; Makhanbet, M.; Zhang, X. Improving Physical Layer Security of Cooperative NOMA System with Wireless-Powered Full-Duplex Relaying. *Information* **2021**, *12*, 279. [CrossRef]
22. Nomikos, N.; Trakadas, P.; Hatziefremidis, A.; Voliotis, S. Full-Duplex NOMA Transmission with Single-Antenna Buffer-Aided Relays. *Electronics* **2019**, *8*, 1482. [CrossRef]
23. Amer, A.; Ahmad, A.-M.; Hoteit, S. Resource Allocation for Downlink Full-Duplex Cooperative NOMA-Based Cellular System with Imperfect SI Cancellation and Underlaying D2D Communications. *Sensors* **2021**, *21*, 2768. [CrossRef]
24. Zhang, Z.; Long, K.; Vasilakos, A.V.; Hanzo, L. Full-Duplex Wireless Communications: Challenges, Solutions, and Future Research Directions. *Proc. IEEE* **2016**, *104*, 1369–1409. [CrossRef]

25. Kim, S.; Stark, W. Full duplex device to device communication in cellular networks. In Proceedings of the International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 3–6 February 2014; pp. 721–725. [CrossRef]
26. Xu, Z.; Petrunin, I.; Li, T.; Tsourdos, A. Efficient Allocation for Downlink Multi-Channel NOMA Systems Considering Complex Constraints. *Sensors* **2021**, *21*, 1833. [CrossRef]
27. Khan, R.; Jayakody, D.N.K.; Pervaiz, H.; Tafazolli, R. Modulation Based Non-Orthogonal Multiple Access for 5G Resilient Networks. In Proceedings of the IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
28. Khan, R.; Jayakody, D.N.K.; Sharma, V.; Kumar, V.; Kaur, K.; Chang, Z. A Machine Learning Based Energy-Efficient Non-Orthogonal Multiple Access Scheme. In Proceedings of the International Forum on Strategic Technology, Tomsk, Russia, 14–17 October 2019; pp. 1–6.
29. Madeira, J.; Guerreiro, J.; Serra, H.; Dinis, R.; Montezuma, P.; Campos, L.M. A Physical Layer Security Technique for NOMA Systems with MIMO SC-FDE Schemes. *Electronics* **2020**, *9*, 240. [CrossRef]
30. Tian, X.; Li, Q.; Li, X.; Peng, H.; Zhang, C.; Rabie, K.M.; Kharel, R. I/Q Imbalance and Imperfect SIC on Two-Way Relay NOMA Systems. *Electronics* **2020**, *9*, 249. [CrossRef]
31. Akhtar, M.W.; Hassan, S.A.; Jung, H. On the Symbol Error Probability of STBC-NOMA with Timing Offsets and Imperfect Successive Interference Cancellation. *Electronics* **2021**, *10*, 1386. [CrossRef]
32. Khan, A.; Usman, M.A.; Usman, M.R.; Ahmad, M.; Shin, S.-Y. Link and System-Level NOMA Simulator: The Reproducibility of Research. *Electronics* **2021**, *10*, 2388. [CrossRef]
33. Do, D.-T.; Van Nguyen, M.-S.; Hoang, T.-A.; Voznak, M. NOMA-Assisted Multiple Access Scheme for IoT Deployment: Relay Selection Model and Secrecy Performance Improvement. *Sensors* **2019**, *19*, 736. [CrossRef] [PubMed]
34. Wang, J.; Song, X.; Ma, Y.; Xie, Z. Power Efficient Secure Full-Duplex SWIPT Using NOMA and D2D with Imperfect CSI. *Sensors* **2020**, *20*, 5395. [CrossRef]
35. Yan, Y.; Xu, H.; Zhang, N.; Han, G.; Liu, M. Dynamic Divide Grouping Non-Orthogonal Multiple Access in Terrestrial-Satellite Integrated Network. *Sensors* **2021**, *21*, 6199. [CrossRef] [PubMed]
36. Khan, R.; Asif, R. Reflective In-Band Full Duplex NOMA Communications for Secure 5G Networks. In Proceedings of the 2021 International Conference on Smart Applications, Communications and Networking (SmartNets), Glasgow, UK, 22–24 September 2021; pp. 1–6. [CrossRef]
37. Zhang, Z.; Ma, Z.; Xiao, M.; Ding, Z.; Fan, P. Full-Duplex Device-to-Device-Aided Cooperative Non-orthogonal Multiple Access. *IEEE Trans. Veh. Technol.* **2017**, *66*, 4467–4471. [CrossRef]
38. Yin, L.; Chenggong, W.; Kai, M.; Kuanxin, B. A NOMA Power Allocation Strategy Based on Genetic Algorithm. *Commun. Signal Process. Syst.* **2019**, *571*, 2182–2190.
39. Khan, R.; Jayakody, D.N.K. An Ultra-Reliable and Low Latency Communications Assisted Modulation based Non-Orthogonal Multiple Access Scheme. *Phys. Commun.* **2020**, *43*, 101035. [CrossRef]