Taylor & Francis
Taylor & Francis Group

Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

Physical layer security based on full duplex and half-duplex multi relay assisted OFDM system

K. Ragini, K. Gunaseelan & R. Dhanusuya

To cite this article: K. Ragini, K. Gunaseelan & R. Dhanusuya (2023) Physical layer security based on full duplex and half-duplex multi relay assisted OFDM system, Automatika, 64:4, 1158-1170, DOI: 10.1080/00051144.2023.2250639

To link to this article: https://doi.org/10.1080/00051144.2023.2250639

Published online: 31 Aug 2023.

AUTOMATIKA
2023, VOL. 64, NO. 4, 1158–1170
https://doi.org/10.1080/00051144.2023.2250639

Physical layer security based on full duplex and half-duplex multi relay assisted OFDM system

K. Ragini, K. Gunaseelan and R. Dhanusuya

DECE, CEG Campus, Anna University, Chennai, India

ABSTRACT

Broadcasting in wireless channels causes security vulnerabilities since both the intended receiver and the eavesdropper may receive the information. Physical layer security (PLS) ensures the confidentiality of information transmitted wireless medium, even in the presence of eavesdroppers, without relying on cryptographic techniques implemented at higher layers. A PLS method for cooperative relay based Orthogonal Frequency Division Multiplexing (OFDM) with optimal relay selection and power optimization is proposed. In order to increase the overall system's secrecy rate, a hybrid relaying and water filling based optimal power allocation is performed for multi-relay assisted OFDM-based wireless networks. By changing the eavesdroppers' distances, the performance efficiency of the proposed system is verified. The analysis is carried out for both Full Duplex (FD) and Half Duplex (HD) systems and their performances are compared with existing equal power allocation technique. The proposed method combines relay selection and novel power optimization process to improve secrecy rate than the existing power allocation methods for both HD and FD systems.

ARTICLE HISTORY
Received 13 June 2023
Accepted 14 August 2023

KEYWORDS
Orthogonal frequency division multiplexing (OFDM); physical layer security (PLS); full duplex (FD); half duplex (HD); received signal strength (RSS)

1. Introduction

Future 5G networks are expected to support billions of devices, higher data rates and universal connectivity with the assistance of a wide range of technologies. It includes full duplex radios, mm-Wave, MIMO and so on. OFDM is another efficient technique, which has emerged as powerful and innovative method for data transmission in communication systems. This technique involves the partitioning of single information stream into multiple parallel data streams, which is subsequently transmitted over several closely spaced narrowband sub channels instead of a conventional wideband channel frequency. By exploiting the Orthogonality between subcarrier frequencies, OFDM ensures minimal interference, enabling each sub channel to independently carry its unique payload. Both CDMA and various forms of OFDM have their advantages. However, in recent implementations, there is a growing preference for OFDMA. The availability of enhanced processing power has made it relatively easy to generate and demodulate OFDM signals. Moreover, as the demand for wider bandwidth increases, OFDM proves to be a suitable choice due to its scalability and ability to support high data rates required by many applications. The 5G networks are prone to threats related to privacy due to heterogeneous devices and technologies. Since both legitimate users and eavesdroppers can access wireless signals, security is challenging. Generally, the security requirements are met using conventional cryptographic methods, which rely on complex mathematical operations. Unlike the cryptographic approaches, the physical layer security (PLS) exploits physical layer properties of the channel like Received Signal Strength (RSS) and Channel Impulse Response (CIR) to provide effective secured communication. One aspect of physical layer security is the utilization of received signal strength (RSS) to improve the confidentiality and integrity of transmitted data. RSS can be used to estimate the channel characteristics between the transmitter and the receiver. By analyzing the received signal strength, it is possible to estimate the distance between the communicating devices and determine the path loss and fading effects. This information can help in optimizing the transmission power and designing appropriate security mechanisms. RSS can also be used to detect eavesdropping attempts. When an eavesdropper tries to intercept the wireless communication, it introduces additional path loss and attenuation to the signal. By comparing the expected RSS based on the estimated channel characteristics with the actual received RSS, it is possible to detect the presence of an eavesdropper. This detection mechanism can trigger countermeasures, such as changing the transmission frequency or implementing encryption. RSS variations caused by channel characteristics can be exploited for physical layer key generation. Random fluctuations in the received signal strength can be used to generate shared secret keys between communicating

CONTACT K. Ragini skragini@gmail.com Department of ECE, CEG Campus, Anna University, Chennai, India

devices. These keys can be employed for encryption and decryption purposes, ensuring secure communication even without relying solely on higher-layer cryptographic algorithms. It is important to note that while RSS can enhance physical layer security, it should be used in conjunction with other security measures, such as encryption, authentication protocols and higher-layer security mechanisms, to provide comprehensive protection against various types of attacks. The performance of PLS is quantified in terms of secrecy capacity. If the capacity of the legitimate data transmission channel is greater than that of the eavesdropper's channel, then the secrecy of the user information is high. As result, the data is transferred at a speed that is closer to the legitimate channel capacity, making it difficult for an eavesdropper to decode the data. Efficient data transmission with resource constraints is a great challenge in wireless communication. Under such resource constraint environment, cooperative relaying methods can be used to improve the range and reliability of wireless networks. Generally, in such cooperative networks, the source requests one or more relay nodes for assistance in relaying the information. At the same time, the source-destination pair desires to keep the information confidential from these nodes. In multi-hop wireless networks, relay systems play an important role when transmitters have limited power for transmission. Relaying can be performed both in half-duplex (HD) and full duplex (FD) systems where the relaying time slots are different for the systems. In full-duplex mode, the relay is able to receive and transmit simultaneously, as opposed to half-duplex mode, when it is limited to either transmit or receive at the time. Half duplex relay needs two-time slots whereas full duplex relay needs one-time slot to exchange the information between the source and destination.

The paper referenced in ref. [1] focuses on optimizing the secrecy rate by considering power allocation at forwarding relay node, in addition to subcarrier mapping, to minimize the leakage of information to eavesdropper. It also introduces the deployment of physical layer security (PLS) in a wireless *ad hoc* network for hybrid full-/half-duplex systems. In this approach, the legitimate receiver operates in full duplex (FD) mode during a fraction of time, simultaneously receiving desired signals and transmitting jamming signals to thwart eavesdroppers. During the remaining time, the receiver operates exclusively in half-duplex (HD) mode, dedicating its resources only to receiving the desired signals. The proposed hybrid full-duplex/half-duplex receiver deployment strategy is to secure legitimate transmissions in a wireless *ad hoc* network with numerous legitimate transmitter-receiver pairs and eavesdroppers. This paper [2] studies physical layer security and derives accurate expressions and tractable approximations for the connection outage probability and the secrecy outage probability of an arbitrary legitimate link. The paper optimizes the area secure link number, network-wide secrecy throughput and network-wide secrecy energy efficiency. The paper concludes that the proposed strategy can significantly enhance the network security performance. The paper [3] discusses a physical layer security scheme for full-duplex communication systems with residual self-interference and non-eavesdropping Channel State Information (CSI). The Ergodic secrecy rate of cooperative jamming and relaying, examining its performance in both low and high signal-to-noise ratio regimes, while considering various eavesdropper positions. Since the half-duplex relay takes two time slots per data transmission, the secrecy rate is half as that of direct transmission. This loss in secrecy rate is recovered by full-duplex relaying, where the relay node receives and transmits simultaneously in single time slot for data transmission [4]. A joint relay selection and jammer selection along with power allocation scheme to maximize the secrecy rate of the legitimate transmission is proposed in For each relay, an optimal power allocation solution has been derived to obtain secrecy rate and, on this basis, the relay, which maximizes the secrecy rate, is selected for transmission [5]. This paper [6] investigates the physical layer security of a full-duplex wireless relaying network using orthogonal frequency division multiplexing (OFDM). Results show that the system model that contains a large number of user pairs achieves better secrecy performance in comparison to a small number of users, and the physical layer security of the orthogonal frequency division multiplexing based wireless relaying network is investigated. The authors [7] proposed an artificial noise-aided cooperative transmission scheme, in which the relay emits a jamming signal to confuse the eavesdropper while receiving the signal from the source. Proposed AN aided scheme achieves better secrecy performance. Numerical results verify accuracy of theoretical analysis. In ref. [8] the proposed hybrid cooperative beamforming and jamming scheme can effectively enhance the physical-layer security of a single-antenna-equipped two-way relay network in the presence of an eavesdropper. The penalty function method incorporating the rank-1 constraint into the objective function is an efficient iterative algorithm to solve the semi-definite programming (SDP) problem. The proposed optimization algorithms outperform the semi-definite relaxation (SDR) technique. The idea can be generalized to the more than one jammer case, and if there are more jammers, they can cooperatively transmit their jamming signals to achieve a better performance than that when they independently transmit. The proposed scheme and optimization algorithms can be applied to other wireless communication systems to enhance their physical-layer security. The paper [9] focuses on improving the physical-layer security of wireless communications against eavesdropping attacks by exploiting the physical

characteristics of wireless channels. The work investigates several diversity approaches, including multiple-input multiple-output (MIMO), multiuser diversity and cooperative diversity, to increase the secrecy capacity of wireless transmission. They present a case study of exploiting cooperative relays to assist the signal transmission from source to destination while defending against eavesdropping attacks. They also evaluate the security performance of cooperative relay transmission in Rayleigh fading environments in terms of secrecy capacity and intercept probability. In this paper [10], an adaptive FD/HD transmission scheme for a cooperative device-to-device (C-D2D) communications system wherein cellular uplink data is relayed through a D2D transmitter was proposed. FD transmission performs better than HD transmission for a maximum of two D2D users mapped to a cellular user. A trade-off between FD and HD transmission is observed for a large number of D2D users, depending on the cellular outage constraint. The paper proposes a joint consideration of full duplex and security to improve both spectrum efficiency and security of conventional wireless systems at the same time. In the paper [11] constructs a cross-layer secrecy rate model based on full duplex constraints, secrecy capacity constraints and secrecy flow balance. The proposed method formulates the model into a mixed integer and non-linear programming problem and reformulates it with reformulation-linearization technique and convex hull relaxation into the linear form. This paper validates the proposed optimization method and algorithm through comparing it with half duplex and jamming to demonstrate that the proposed combination of security and full duplex achieve the significant improvement of spectrum efficiency and security. The paper utilizes full-duplex in physical layer security communication to maximize secrecy rate for cross-layer optimization of multi-hop networks. The paper [12] proposes a new cooperative jamming technique for a two-hop amplify-and-forward relay network with an eavesdropper. A joint power allocation and relay selection scheme is proposed for the network with the proposed technique. The secrecy outage probability of the network is derived and joint power allocation and relay selection problem is proposed to minimize the secrecy outage probability and primal decomposition method is used to divide the problem into a master problem and a sub problem. Simulation results are presented to show that the proposed scheme for the network with the proposed technique provides lower secrecy outage probability than a conventional scheme for the network with a conventional technique. In the paper [13] provides a survey of physical layer security research on various promising 5G technologies, including physical layer security coding, massive multiple-input multiple-output, millimetre wave communications, heterogeneous networks, non-orthogonal multiple access, full duplex technology and so on. It also discusses the technical challenges which remain unresolved at the time of writing and the future trends of physical layer security in 5G and beyond. This paper [14] discusses the methods used in physical layer security (PLS) to provide node authentication, message authentication and message confidentiality. The authors review three different PLS methods of node authentication: physical unclonable functions (PUFs), biometric-based authentication and RF fingerprinting. They also review information theoretic bounds on the achievable rates when message integrity is required, both for noiseless and noisy transmission channels. Additionally, two alternative approaches to achieve message confidentiality are reviewed: keyless secrecy encoding in wiretap channels and channel-based secret key generation (SKG), used in conjunction with symmetric encryption in hybrid schemes.

The paper [15] compares the performance of a perfect full-duplex diamond network to a prevalent half-duplex diamond network and identifies conditions for achieving similar performance. It is demonstrated that for the same network but with half-duplex relays, when the number of antennas in relays satisfies a specific condition, there exists a fixed listen-transmit schedule combined with quantize-map-and-forward (QMF) relaying to achieve the optimal DMT. The perfect full-duplex diamond network outperforms the half-duplex case. A specific condition for the number of antennas in relays achieves optimal DMT. In this paper [16], the authors proposed a new practical pilot design method for OFDM-based full duplex (FD) systems and its performance is analysed in terms of the self-interference cancellation capability. Proposed pilot design method for OFDM-based FD system Efficient performance in terms of self-interference cancellation capability. The paper proposes the use of energy-harvesting (EH) from natural and man-made sources, particularly wireless power transfer, to prolong the life of energy-constrained wireless devices. The contributions of this paper are [17] performance of relaying simultaneous wireless information and power transfer (SWIPT) systems over indoor log-normal channels with half-duplex (HD) and full-duplex (FD) relaying schemes. The paper evaluates the system performance in terms of the ergodic outage probability. The paper presents a comprehensive analysis of the proposed scheme and compares it with existing schemes in terms of energy efficiency and outage probability. This work provides insights into the design and optimization of energy-harvesting wireless networks. The consequences of channel estimation in PLC systems employing an OFDM technique have been investigated in this work. Consideration has been given to one frequency (LS) and one time (LMMSE) domain channel estimation technique. There is another proposed frequency domain-based channel estimation

technique. Block and comb-type pilot arrangements are combined in the proposed technique for LS channel estimation. It obtains the real-time channel condition using comb-type estimation and the block-type estimation approach to average the long-term channel condition [18]. In order to increase the overall system's secrecy rate, new hybrid relay selection and power allocation methods are proposed which includes hybrid relaying during the transmission. The remaining sections of the paper are organized as follows. Section 2 discusses System model. Section 3 describes the proposed relay selection and power allocation techniques. In Section 4, results and analysis of the proposed scheme are discussed and Section 5 concludes the paper.

2. System model

The system model comprises a relay network based on orthogonal frequency division multiplexing (OFDM), consisting of a single source node (SN), a destination node (DN), R_i relay nodes, and two eavesdroppers is shown in Figure 1. It is assumed that the destination is outside the source's transmission range and hence the source and destination cannot communicate directly. Thus, a relay is used in between to receive the signal from the SN and transmit it to the DN. Let R_i be the set of relays available for transmission. From the set of R_i relays, one optimal relay, R∗ is selected. The physical medium is accessed through an OFDM System containing N subcarriers. Let p_n^s and p_n^r denote the transmitted power at the source and relay node respectively. The eavesdropper located near the source node is Eavesdropper 1 (Eve-n-SN) and near the destination node is Eavesdropper 2 (Eve-n-DN). The channels between the source–relay, relay–destination, source-eavesdropper, relay-eavesdropper1 and relay-eavesdropper 2 are assumed to have independent Rayleigh fading, characterized by coefficients are as follows h_n^{sr}, h_n^{rd}, h_n^{se1}, h_n^{re1} and h_n^{re2}.

Consider the distance between source and Eavesdropper 1 as d_1 and the distance between relay and Eavesdropper 2 as d_2. The system is capable of operating in both the half-duplex and full-duplex relaying modes. Hence, the proposed work is analysed in both the relaying modes. The source node and relay node transmit at odd and even time slots, respectively, in the half-duplex relaying (HDR) system. Both the source node and relay node transmit simultaneously in the full-duplex relaying (FDR) system. Power allocation is done at the source and relay nodes to efficiently utilize the available power by using the proposed power allocation method.

The secrecy capacity of the proposed method is analysed for both HD and FD systems and their mathematical expressions are derived in the following sections.

2.1. Half duplex relay model

In half-duplex (HD) relaying, the source node initiates the transmission by sending the signal to the optimal relay node during the first time slot, denoted as t. The relay node transmits the signal to the destination node at the next time slot, denoted as $t+1$. Let $x_s(t)$ be the signal transmitted by the source to relay, and y_{R*} and y_{e1} denote the received signals at the relay and the eavesdropper, Eve-n-SN respectively.

At time t, the received signals at the relay and eavesdropper are given by

$$\mathrm{y}_{R*} = \sum_{n=1}^{N} (\mathrm{p}_\mathrm{n}^\mathrm{s} \mathrm{h}_\mathrm{n}^{\mathrm{s}\,R*}(t)\mathrm{x}_\mathrm{s}(t)) + \mathrm{n}_{R*}(t) \tag{1}$$

$$\mathrm{y}_{\mathrm{e1}} = \sum_{n=1}^{N} (\mathrm{p}_\mathrm{n}^\mathrm{s} \mathrm{h}_\mathrm{n}^{\mathrm{se1}}(t)\mathrm{x}_\mathrm{s}(t)) + \mathrm{n}_{\mathrm{e1}}(t) \tag{2}$$

In second time slot $t+1$, the relay decodes and forwards the received signal to the destination node. Due to the broadcast nature of the signal, the signal is also received by both the eavesdroppers, Eve-n-SN and Eve-n-DN.

The received signals at the destination and eavesdroppers are given by

$$\mathrm{y}_\mathrm{d} = \sum_{n=1}^{N} (\mathrm{p}_\mathrm{n}^{R*} \mathrm{h}_\mathrm{n}^{R*\mathrm{d}}(t+1)\mathrm{x}_\mathrm{s}(t)) + \mathrm{n}_d(t+1) \tag{3}$$

$$\mathrm{y}_{\mathrm{e1}} = \sum_{n=1}^{N} (\mathrm{p}_\mathrm{n}^\mathrm{s} \mathrm{h}_\mathrm{n}^{R*e1}(t+1)\,\mathrm{x}_\mathrm{s}(t)) + \mathrm{n}_{\mathrm{e1}}(t+1) \tag{4}$$

$$\mathrm{y}_{\mathrm{e2}} = \sum_{n=1}^{N} (\mathrm{p}_\mathrm{n}^{R*} \mathrm{h}_\mathrm{n}^{R*e2}(t+1)\,\mathrm{x}_\mathrm{s}(t)) + \mathrm{n}_{\mathrm{e2}}(t+1) \tag{5}$$

The secrecy capacities of source–relay and relay–destination are expressed as

$$C_{sR*} = \frac{1}{2} \sum_{n=1}^{N} \left\{ \log_2 \left(1 + \frac{p_n^s |h_n^{sR*}|^2}{n_0} \right) \right\} \tag{6}$$

$$C_{R*d} = \frac{1}{2} \sum_{n=1}^{N} \left\{ \log_2 \left(1 + \frac{p_n^{R*} |h_n^{R*d}|^2}{n_0} \right) \right\} \tag{7}$$

where n_0 is the additive white Gaussian noise (AWGN). The transmission rate at destination R_d is given as

$$R_d = \min(c_{sR*}, c_{R*d}) \tag{8}$$

The capacities of the eavesdroppers Eve-n-SN and Eve-n-DN are calculated asC_{e1} and $C_{e2}$is respectively.

$$C_{e1} = \frac{1}{2} \sum_{n=1}^{N} \left\{ \log_2 \left(1 + \frac{(p_n^s |h_n^{se1}|^2 + p_n^{R*} |h_n^{R*e1}|^2)}{n_0} \right) \right\} \tag{9}$$

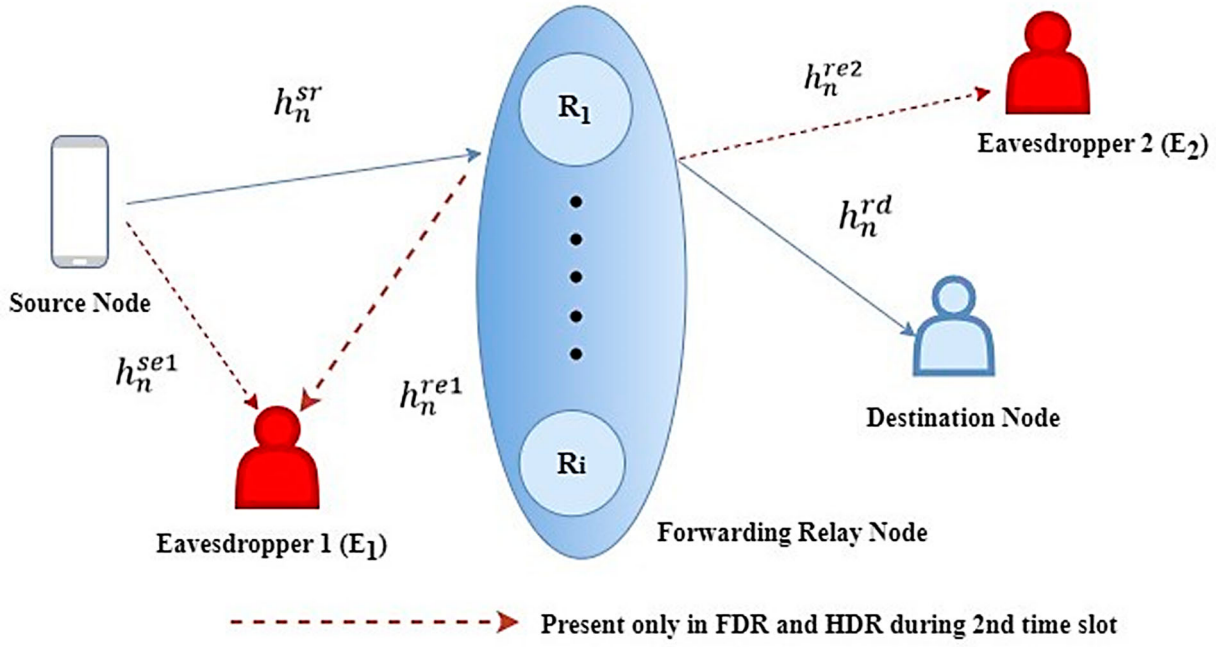

Figure 1. The system model of OFDM based HDR and FDR.

$$C_{e2} = \frac{1}{2}\sum_{n=1}^{N}\left\{\log_2\left(1+\frac{p_n^{R*}|h_n^{R*e2}|^2}{n_0}\right)\right\} \tag{10}$$

The transmission rate at the eavesdropper $R_e$is given by

$$R_e = \max(c_{e1}, c_{e2}) \tag{11}$$

The secrecy rate $R_{\text{sec,HDR}}$, which is used to analyse the system performance in ensuring secrecy, is defined as

$$R_{\text{sec,HDR}} = \max\left[R_d - R_e, 0\right]^+ \tag{12}$$

where $[.]^+$ indicates that the secrecy rate cannot be negative.

2.2. Full duplex relaying method

In FD relaying, the relay transmits and receives the message simultaneously. At time t, let $\mathrm{x_s}(t)$ be the signal transmitted by the source to the optimal relay. At the same time, the signal transmitted by the relay to destination is $\mathrm{x_s}(t\text{-}1)$.

At time t, the received signals at the relay and destination are given by

$$\mathrm{y}_{R*} = \sum_{i=1}^{N}(\mathrm{p_n^s h_n^{sR*}}(t)\mathrm{x_s}(t) + \mathrm{p_n^{R*} h_n^{R*R*}}(t)\mathrm{x_s}(t-1)) + \mathrm{n}_{R*}(t) \tag{13}$$

The 2nd term in Equation (14) is due to self-interference

$$\mathrm{y_d} = \sum_{i=1}^{N}(\mathrm{p_n^{R*} h_n^{R*d}}(t)\ \mathrm{x_s}(t-1)) + \mathrm{n_d}(t) \tag{14}$$

Similarly, the received signals at the eavesdroppers, Eve-n-SN and Eve-n-DN are

$$\mathrm{y_{e1}} = \sum_{n=1}^{N}(\mathrm{p_n^s}(t)\ \mathrm{h_n^{se1}x_s}(t) + \mathrm{p_n^{R*}}(t)\mathrm{h_n^{R*e1}x_s}(t-1)) + \mathrm{n_{e1}}(t) \tag{15}$$

$$\mathrm{y_{e2}} = \mathrm{p_n^r h_n^{R*e2}}(t)\ \mathrm{x_s}(t-1) + \mathrm{n_{e2}}(t) \tag{16}$$

The secrecy capacities of source–relay and relay–destination are expressed as

$$C_{sR*} = \sum_{n=1}^{N}\left\{\log_2\left(1+\frac{p_n^s|h_n^{sR*}|^2}{n_0 + p_n^{R*}|h_n^{R*R*}|^2}\right)\right\} \tag{17}$$

$$C_{R*d} = \sum_{n=1}^{N}\left\{\log_2\left(1+\frac{p_n^{R*}|h_n^{R*d}|^2}{n_0}\right)\right\} \tag{18}$$

where n_0 is the additive white Gaussian noise (AWGN). The transmission rate at destination $R_d$is given as

$$R_d = \min(c_{sr}, c_{rd}) \tag{19}$$

The capacities of the eavesdroppers Eve-n-SN and Eve-n-DN are calculated asC_{e1} and $C_{e2}$is respectively.

$$C_{e1} = \sum_{n=1}^{N}\left\{\log_2\left(1+\frac{(p_n^s|h_n^{se1}|^2 + p_n^r|h_n^{R*e1}|^2)}{n_0}\right)\right\} \tag{20}$$

$$C_{e2} = \sum_{n=1}^{N}\left\{\log_2\left(1+\frac{p_n^{R*}|h_n^{R*e2}|^2}{n_0}\right)\right\} \tag{21}$$

The transmission rate at the eavesdropper R_e is given by

$$R_e = \max(c_{e1}, c_{e2}) \tag{22}$$

The secrecy rate $R_{\text{sec,FDR}}$, which is used to determine the system performance in ensuring secrecy, is defined as

$$R_{\text{sec,FDR}} = \max\left[R_d - R_e, 0\right]^+ \tag{23}$$

where $[.]^+$ indicates that the secrecy rate cannot be negative.

2.3. Secrecy outage probability

The outage probability for secrecy capacity is derived for both the HD and FD systems and the mathematical derivation is given in Equation (24) & (25)

$$P_{\text{HDR}} = (R_{\text{sec,HDR}} < R_s) \tag{24}$$

Where P_{HDR} is the secrecy outage probability, $R_{\text{sec,HDR}}$ is the secrecy rate of the HDR system from (13) and R_s is the target secrecy rate

$$P_{\text{FDR}} = (R_{\text{sec,FDR}} < R_s) \tag{25}$$

where P_{FDR} is the secrecy outage probability, $R_{\text{sec,FDR}}$ is the secrecy rate of the FDR system from (24) and R_s is the target secrecy rate.

3. Proposed hybrid relay selection and power optimization technique

Among the set of R_i relays, it is critical to choose the optimal relay to support the source signal transmission. The eavesdroppers are passive and hence it is challenging to collect their channel information. Hence, the source–relay and relay–destination channel conditions are used for selecting the optimal relay. The optimal relay is selected by modifying the already-existing equation in [9] for the case of two eavesdroppers. The mathematical expression to select the optimal relay R∗ is given in Equation (26)

$$\text{R}* = \arg max_{i\in R}\left\{\frac{\sum_{n=1}^{N}|h_n^{si}|^2\sum_{n=1}^{N}|h_n^{id}|^2}{\sum_{n=1}^{N}|h_n^{si}|^2+\sum_{n=1}^{N}|h_n^{id}|^2}\right\} \tag{26}$$

where h_n^{si} represent the nth sub-channel gain from the source to the optimal relay R* and h_n^{id} represent the nth sub-channel gain from the optimal relay R∗to destination. The proposed relay selection method only needs the main channel information, $|h_n^{si}|^2$ and $|h_n^{id}|^2$, with which the main channel capacity is maximized. In the proposed method, power allocation is performed at the source node by considering only eavesdropper near to the SN and power allocation is performed at the relay node by considering both the eavesdroppers near the SN and DN. Full duplex mode is considered in proposed method to enhance PLS security. For that, the half of the power is distributed equally among the best channels chosen by comparing the CSI of source to relay and CSI of source to eavesdropper's channels to ensure improved secrecy rate. Remaining half of the total transmit power is allocated to subcarriers using water filling algorithm by considering only CSI of source to optimal relay node. In proposed method, the full duplex mode is utilized to improve the secrecy rate.

The transmitter structure diagram of the novel OFDM-Multi relay assisted system is illustrated in Figures 2 and 3.

In Figure 2, information bits are mapped and subjected to OFDM modulation. To optimize power allocation across the OFDM subcarriers, the total power at the source node is divided into two equal halves and power allocation is performed as described in Section 4. Figure 3 highlights the receiving end of the system, where the OFDM modulated signal is received at the relay node. Here, the received signal is amplified and then forwarded to the destination. The power allocation at the relay node is same as that of the source node.

Table 1. Simulation parameters.

Parameters	Value
Wireless channel bandwidth	1 MHz
Noise spectrum density	4.14×10^{-21} W/Hz
Number of relays	4
Path loss exponent	4

4. Results and discussion

This section discusses the results of simulations that were implemented to verify the secrecy capacities of both HDR and FDR systems. Using the secrecy rate parameter, R_{sec} the system's physical layer security is evaluated. The simulations are carried out using MATLAB R2021a software, and the obtained results are analysed. For simulation, it is assumed that the wireless channels experience Rayleigh fading and the specific parameters used in the simulations are summarized in Table 1.

The position of the chosen relay is constant, whereas the eavesdropper distance is variable for all figures from Figures 3–8. The impact of transmission power on the secrecy rate at different distances d_1 and d_2 is depicted in the following Figures 3–6. Figures 7 and 8 illustrate the secrecy outage probability of HD and FD systems.

The effect of distances $d_1 = 20$ m and $d_2 = 60$ m on the secrecy rate for both half duplex and full duplex systems is analysed in Figure 4. The secrecy rate of the full duplex system with the proposed power allocation

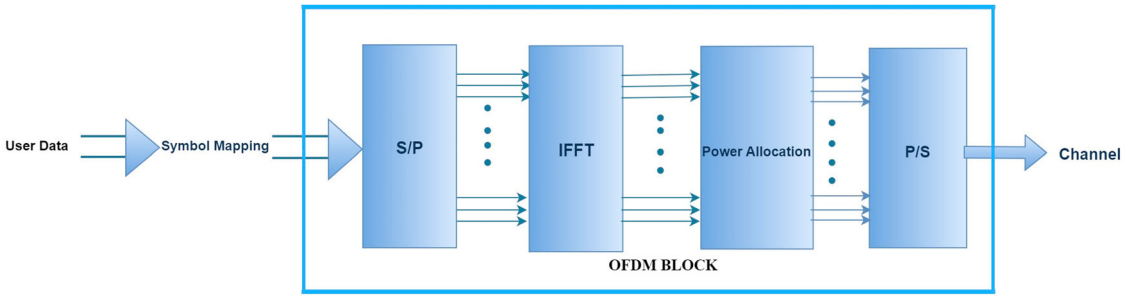

Figure 2. Block diagram of power allocation at source node.

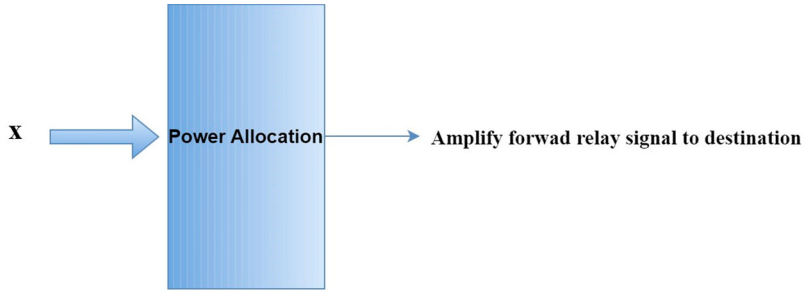

Figure 3. Block diagram of power allocation at relay node.

is 43 bits/sec/Hz for 30 W, which is higher than that of existing equal power allocation by 3 bits/sec/Hz. For HD system, the secrecy rate is 23 bits/sec/Hz for 30 W, which is higher than that of existing method by 2 bits/sec/Hz and it is shown in Table 1.

Figure 5 shows the impact of distances $d_1 = 20$ m and $d_2 = 100$ m on the secrecy rate for both half duplex and full duplex systems. The full duplex system with the proposed power allocation has 5 bits/sec/Hz higher secrecy rate compared to that of existing equal power allocation [1]. For HD system, the secrecy rate is 25 bits/sec/Hz for 30 W, which is higher than that of existing method by 3 bits/sec/Hz. The results of these analyses show that the proximity of the eavesdropper to the source node has a significant impact on the secrecy rate performance. There is no optimal relay selection and power allocation in [1]. Hence, secrecy rate performance is always less than that of the proposed method. The proposed algorithm aims to optimize the secrecy rate and minimize information leakage to eavesdroppers by considering the distance. It is also compared with existing method in Table 1.

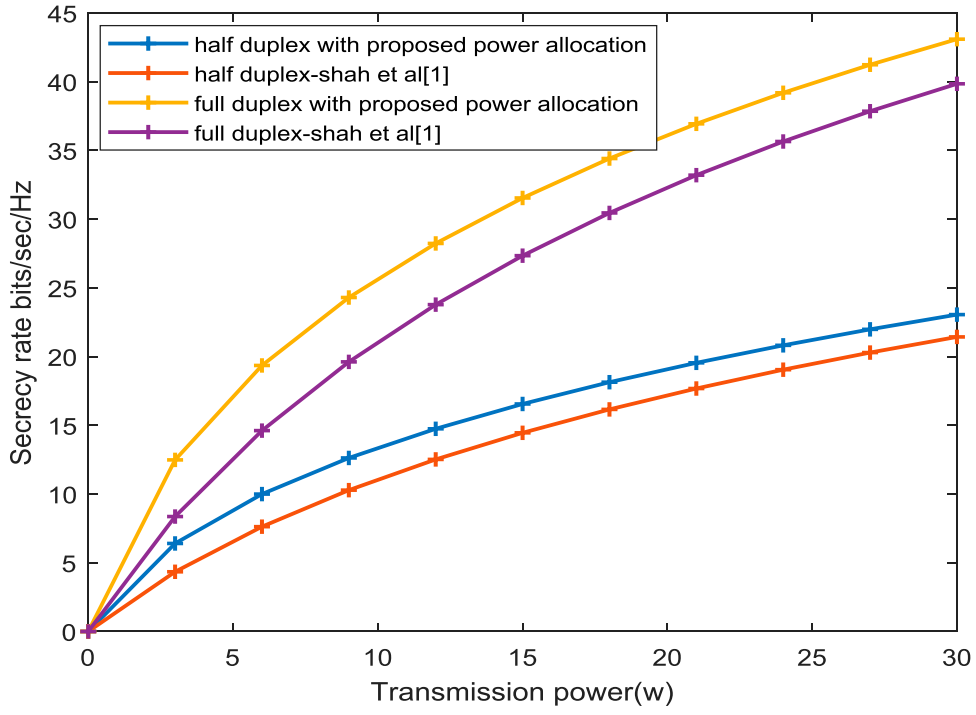

Figure 4. Secrecy rate versus transmission power for distance $d_1 = 20$ m and $d_2 = 60$ m from Relay.

Algorithm of proposed relay selection and power allocation method

Input: Channel response coefficients

$|h_n^{SR_i}| = \{h_1^{SR_i}, h_2^{SR_i} \ldots..h_N^{SR_i}\}$, $|h_n^{R_id}| = \{h_1^{R_id}, h_2^{R_id} \ldots..h_N^{R_id}\}$, $|h_n^{se1}| = \{h_1^{se1}, h_2^{se1} \ldots..h_N^{se1}\}$

$|h_n^{R_ie1}| = \{h_1^{R_ie1}, h_2^{R_ie1} \ldots..h_N^{R_ie1}\}$, $|h_n^{R_ie2}| = \{h_1^{R_ie2}, h_2^{R_ie2} \ldots..h_N^{R_ie2}\}$

Output: Secrecy rate of the HD/FD relay system, $R_{\text{sec,HDR}}$ and $R_{\text{sec,FDR}}$

Step 1: Optimal Relay is Selected using (26) $\mathrm{R}^* = \text{argmax}_{i\in R}\left\{\frac{\sum_{n=1}^{N}|h_n^{si}|^2\sum_{n=1}^{N}|h_n^{id}|^2}{\sum_{n=1}^{N}|h_n^{si}|^2+\sum_{n=1}^{N}|h_n^{id}|^2}\right\}$

Step 2: The total power at the source and relay are divided into two equal halves for power allocation as

$p_{1s} = p_{2s} = \frac{p_s}{2}$ subject to $p_s = p_{1s} + p_{1r}$ and $p_{1r} = p_{2r} = \frac{p_r}{2}$ subject to $p_r = p_{1r} + p_{2r}$

Step 3: Half Duplex relaying

i. Power allocation at source node

Let s_1 contain the sub-carriers whose channel coefficients satisfy the following condition

$s_1 = []$

for $n = 1 : N$

if $h_n^{sR*} \geq h_n^{se1}$

$s_1[n] = h_n^{sR*}$

else

$s_1[n] = 0$

end

end

p_{1s} power is equally allocated to all the channels of s_1

Remaining Half power p_{2s} is allocated to the non-zero channels of s_1 using water-filling algorithm [19]

$$\sum_{n=0}^{N-1}\left(\frac{1}{\lambda} - \frac{N_o}{|h_n^{sR*}|2}\right) = p_{2s}$$

ii. Power allocation at relay node

Let s_2 contain the sub-carriers whose channel coefficients satisfy the following condition

$s_2 = []$

for $n = 1 : N$

if $(h_n^{R*d} \geq h_n^{R*e1})$ and $(h_n^{R*d} \geq h_n^{R*e2})$

$s_2[n] = h_n^{R*d}$

else

$s_2[n] = 0$

end

end

p_{1r} power is equally allocated to all the channels of s_2

Remaining half power is allocated to the non-zero channels of s_2 using water filling

$$\sum_{n=0}^{N-1}\left(\frac{1}{\lambda} - \frac{N_o}{|h_n^{sR*}|2}\right) = p_{2r}$$

Where λ is the Lagrange multiplier satisfies the condition [16] as given in equation relay, and N_o is the noise variance.

iii. Secrecy Rate calculation for HD Relaying

1. Calculate the secrecy capacities of source–relay, C_{sr} and relay–destination, C_{rd} using Equations (6) and (7).
2. The transmission rate at the destination node, R_d is given by the minimum of C_{sr} and C_{rd}.
3. The capacities of the eavesdroppers, C_{e1} and C_{e2} are calculated from Equations (9) and (10).
4. The maximum transmission rate of the eavesdropper, R_e is given by the maximum of c_{e1} and c_{e2}.
5. Finally, the secrecy rate of the HD system, $R_{\text{sec,HDR}}$ is calculated from Equation (12).

iv. Secrecy outage probability

Calculate the secrecy outage probability for P_{HDR} using (24)

Step 4: Full Duplex relaying

i. Power allocation at source node

Let s_1 contain the sub-carriers whose channel coefficients satisfy the following condition

$s_1 = []$

for $n = 1 : N$

if $(h_n^{sR*} \geq h_n^{se1})$ and $(h_n^{sR*} \geq h_n^{R*e1})$

$s_1[n] = h_n^{sR*}$

else

$s_1[n] = 0$

end

end

p_{1s} power is equally allocated to all the channels of s_1

Algorithm of proposed relay selection and power allocation method

Remaining Half power p_{2s} is allocated to the non-zero channels of s_1 using water-filling algorithm [19]

$$\sum_{n=0}^{N-1}\left(\frac{1}{\lambda}-\frac{N_o}{|h_n^{R*d}|2}\right)=p_{2R*}$$

ii. Power allocation at relay node

Let s_2 contain the sub-carriers whose channel coefficients satisfy the following condition

$s_2 = []$

forn $= 1 : N$

if $(h_n^{R*d} \geq h_n^{R*e1})$ and $(h_n^{R*d} \geq h_n^{R*e2})$

$s_2[n] = h_n^{R*d}$

else

$s_2[n] = 0$

end

end

p_{1r} power is equally allocated to all the channels of s_2

Remaining half power is allocated to the non-zero channels of s_2 using water filling [19]

$$\sum_{n=0}^{N-1}\left(\frac{1}{\lambda}-\frac{N_o}{|h_n^{R*}|2}\right)=p_{2R*}$$

iii. Secrecy Rate calculation for FD Relaying

1. Calculate the secrecy capacities of source–relay, C_{sr} and relay–destination, C_{rd} using Equations (17) and (18).
2. The transmission rate at the destination node, R_d is given by the minimum of C_{sr} and C_{rd}.
3. The capacities of the eavesdroppers, C_{e1} and C_{e2} are calculated from Equations (20) and (21).
4. The maximum transmission rate of the eavesdropper, R_e is given by the maximum of c_{e1} and c_{e2}.
5. Finally, the secrecy rate of the FD system, $R_{\text{sec,FDR}}$ is calculated from Equation (23).

iv. Secrecy outage probability

Calculate the secrecy outage probability for P_{FDR} using (25)

Step 5: End

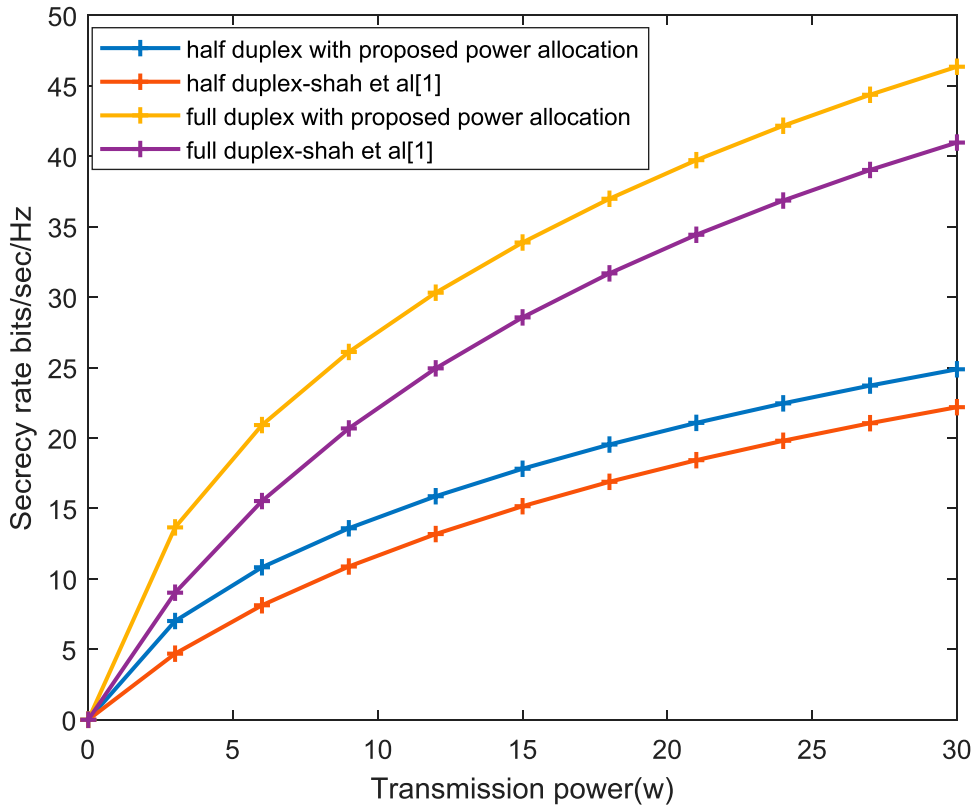

Figure 5. Secrecy rate versus transmission power for distance $d_1 = 20$ m & $d_2 = 100$ m from Relay.

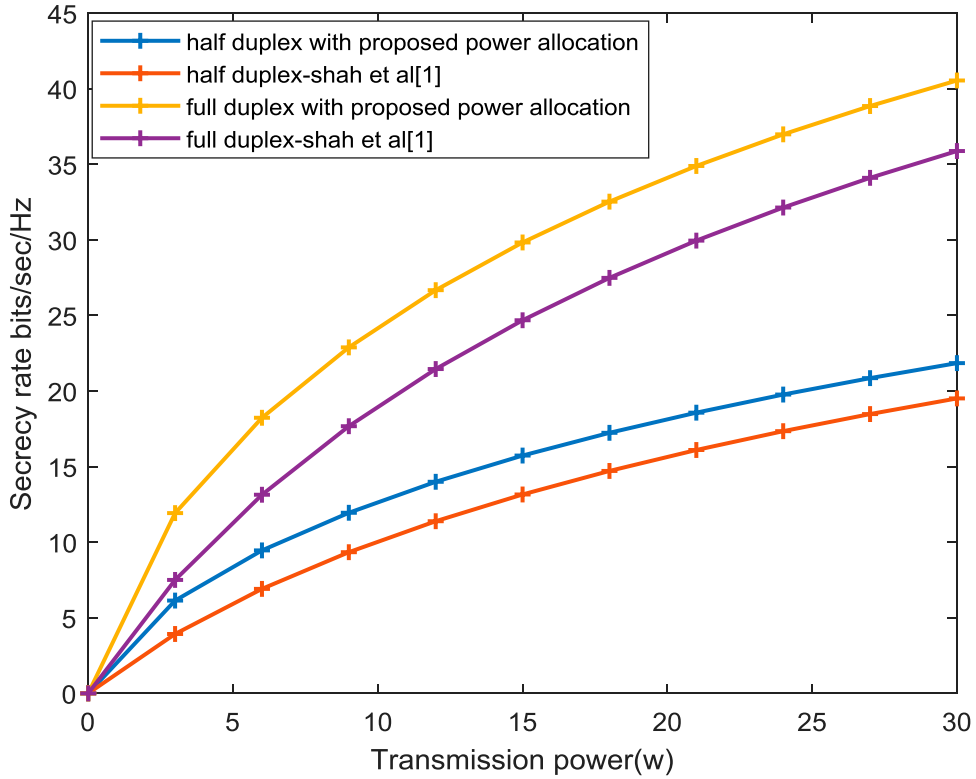

Figure 6. Secrecy rate versus transmission power for distance $d_1 = 60$ m &$d_2 = 20$ m from Relay.

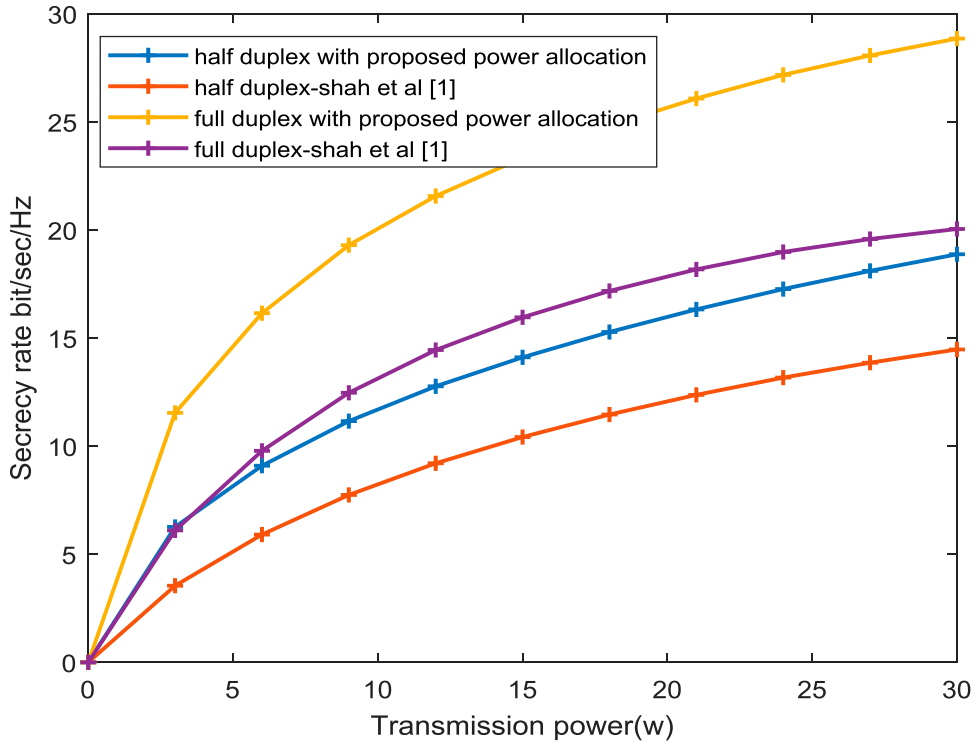

Figure 7. Secrecy rate versus transmission power for distance $d_1 = 100$ m &$d_2 = 20$ m from Relay.

Figure 6 depicts the effect of the distances $d_1 = 60$ m and $d_2 = 20$ m on the secrecy rate for both half-duplex and full-duplex systems. The secrecy rate of the full duplex system with the proposed power allocation is 40 bits/sec/Hz for 30 W, which is higher than that of existing equal power allocation by 4 bits/sec/Hz. It is compared in Table 1. For HD system, the secrecy rate is 21 bits/sec/Hz for 30 W, which is higher than that of existing method by 2 bits/sec/Hz.

The distance $d_1 = 100$ m and $d_2 = 20$ m affect the secrecy rate of HD and FD systems as shown in Figure 6. The secrecy rate of the full duplex system with the proposed power allocation is 29 bits/sec/Hz for 30 W which is 9 bits/sec/Hz higher than the existing equal

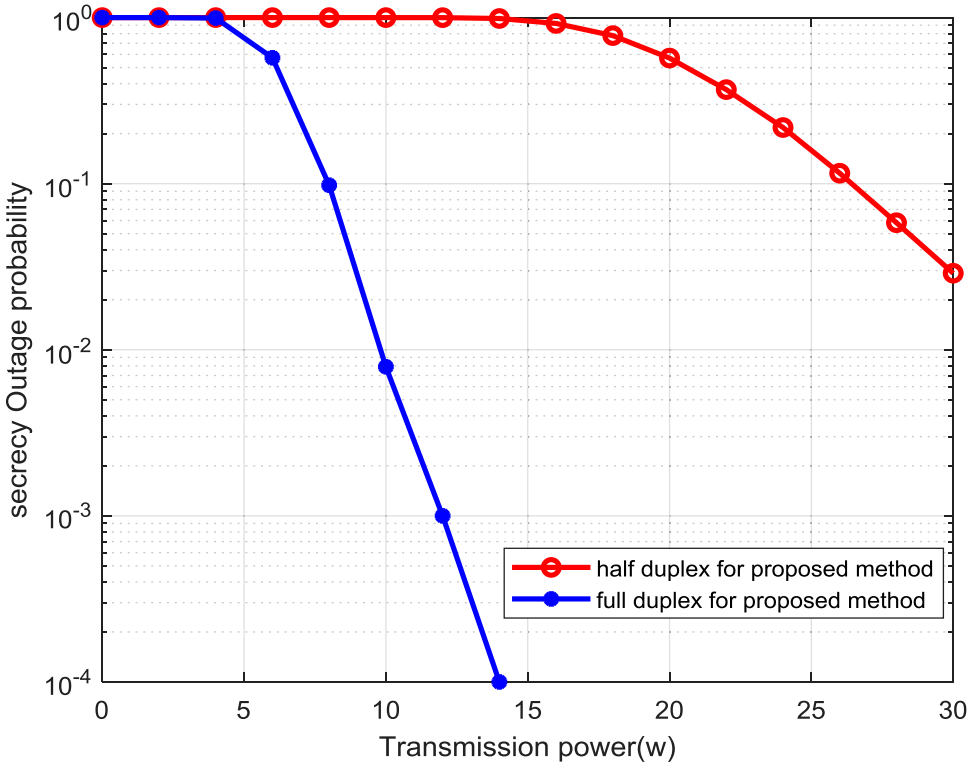

Figure 8. Secrecy outage probability versus Transmission power [FD and HD proposed method].

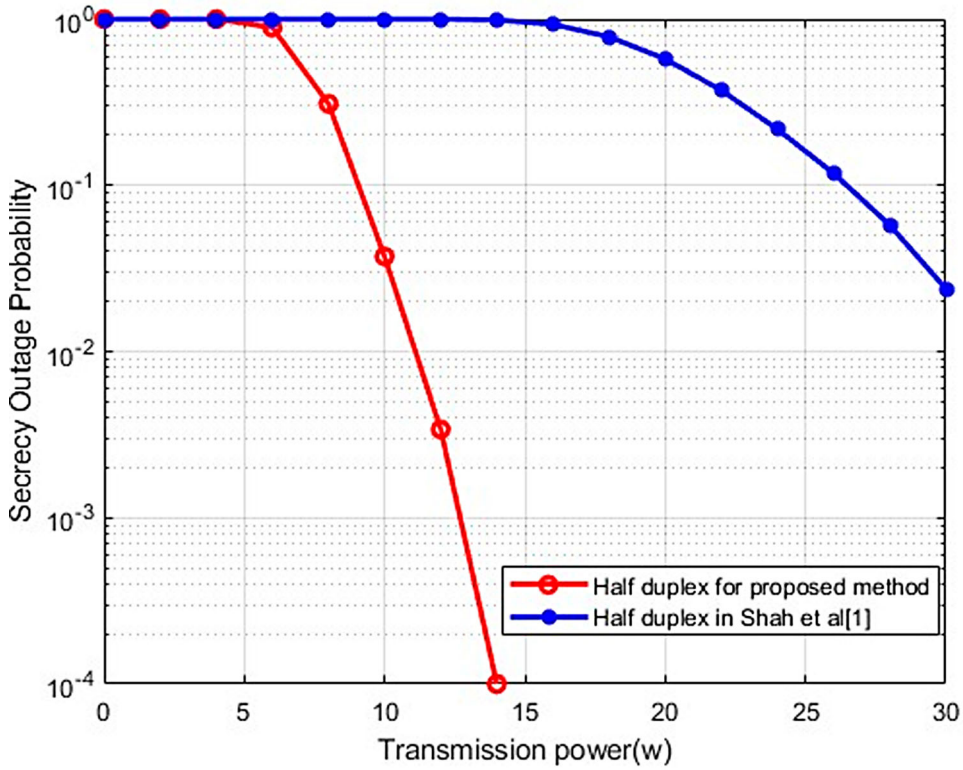

Figure 9. Secrecy outage probability versus transmission power [HD proposed method and HD in shah et al. [1]].

power allocation [1]. For HD system, the secrecy rate is 20 bits/sec/Hz for 30 W, which is higher than the existing method by 2 bits/sec/Hz. In Comparing the effect of varying distances d_1 and d_2 from the relay, increasing distance d1 from relay shows improvement in secrecy rate performance. Also shown in Table 1. It is more difficult for the eavesdropper to decode the data in a FD system because they simultaneously receive signals from the source and relay at the same time, which interfere with each other. This decreases the secrecy rate of the eavesdroppers, and hence improves the secrecy performance of FD system compared to HD systems.

Table 2. Comparison chart for secrecy rate versus distance with respect to relaying modes.

Relaying Modes	Distance from relay node d_1 (m)	d_2 (m)	Secrecy rate Existing method [Shat et al.] (bits/sec/Hz)	Proposed method (bits/sec/Hz)
HDR	20	60	21	23
	20	100	22	25
	60	20	19	20
	100	20	14	18
FDR	20	60	40	43
	20	100	41	46
	60	20	34	40
	100	20	20	29

Table 3. Comparison chart for secrecy outage probability versus transmission power with HD relaying mode.

Relaying mode	Transmission power [W]	Secrecy outage probability Existing method [Shat et al.]	Proposed method
HDR	**14**	**1**	**10^{-4}**

In Figure 8, the HD system with the proposed power allocation method has higher secrecy outage probability compared to that of the FD system. When compared to HD,FD system provides better secrecy for data transmission. For $R_s = 18$ and for transmission power less than 14 W, the outage probability is equal to 1 for HD systems whereas the outage of FD system is 10^{-3} resulting in superior secrecy outage probability performance.

Figure 9 presents a comparative analysis of outage probabilities for a full duplex (HD) system using both the proposed method and the existing method introduced by Shah et al. [1]. The target of this comparison is to assess the performance differences in terms of secrecy outage probability between the two methods. For $R_s = 18$ and transmission power less than 14 W, the proposed HD system has a very low outage probability $10^{-4.}$ Our proposed method showcases a notable advantage, achieving a significantly lower secrecy outage probability than the existing method. It is shown in Table 2.

5. Conclusion

A comprehensive analysis of the secrecy performance in both half-duplex and full duplex systems using OFDM in the presence of eavesdroppers near the source and destination nodes is performed. To enhance the PLS and ensure better confidentiality of transmitted information, the proposed method introduces relay selection schemes along with optimal power allocation techniques at the source and relay nodes. The proposed method significantly improves confidentiality and mitigates information leakage to eavesdroppers. To increase the overall system's secrecy rate, a hybrid relaying and water-filling-based optimal power allocation scheme is employed for multi-relay assisted OFDM-based wireless networks. Through simulations that consider varying eavesdropper distances, the proposed system's performance is verified. The analysis encompasses both FD and HD systems, and their performances are compared against an existing equal power allocation technique and the quantitative results are presented in Tables 2 and 3. The proposed approach represents a significant improvement in securing wireless communication, ensuring that sensitive information remains protected from potential eavesdroppers without relying on higher-layer cryptographic methods. Overall, the proposed PLS method provides a solution for enhancing wireless communication security and confidentiality.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

[1] Shah H, Koo I (member, IEEE). A novel physical layer security scheme in OFDM-based cognitive radio networks. IEEE Access Sel Areas Commun. Nov 2018;6:29486–29498.

[2] Zheng T-X, Wang H-M, Yuan J, et al. Physical layer security in wireless ad hoc network under a hybrid full/half-duplex receiver deployment strategy. IEEE Trans Wireless Commun. Jun 2017;16(6):3827–3839.

[3] Lei W, Zhou Y, Lin X. A physical layer security scheme for full-duplex communication systems with residual self-interference and non-eavesdropping CSI. Dig Commun Netw. Aug 2021;7(3):352–361. doi: 10.1016/j.can.2020.07.004

[4] Zhong C, Suraweera HA, et al. Wireless information and power transfer with full duplex relaying. IEEE Trans Commun. Oct 2014;62(10). doi:10.1109/TCOMM.2014.2357423

[5] Guo H, Yang Z, Zhang J, et al. Power-constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks. IEEE Trans Wireless Commun. May 2017;65(5):2180–2193. doi: 10.1109/TCOMM.2017.2651066.

[6] Ozduran V. Physical layer security of multi-user full-duplex one-way wireless relaying network. In: 2018 Advances in Wireless and Optical Communications (RTUWO). Nov 2018:17–22. doi:10.1109/RTUWO.2018.8587910.

[7] Ren Y, Tan Y, Makhanbet M, et al. Improving physical layer security of cooperative NOMA system with wireless-powered full-duplex relaying. Information. Jul 2021;12(7):279–286. doi:10.3390/info12070279.

[8] H Wang, M Luo, Q Yin, et al. Hybrid cooperative beam forming and jamming for physical-layer security of two-way relay networks. IEEE Trans Inf Forensics Secur. Dec 2013;8(12):2007–2020. doi: 10.1109/TIFS.2013.2287046.

[9] Zou Y, Zhu J, Wang X, et al. Improving physical-layer security in wireless communications using diversity techniques. IEEE Network. Feb 2015;29(1):42–48. doi: 10.1109/MNET.2015.7018202.

[10] Bajpai R, Gupta N, Ashok V. An adaptive full-duplex/half-duplex multiuser cooperative D2D communications system with best user selection. IEEE Open

J Commun Soc. 2021;2:1445–1457. doi:10.1109/OJCOMS.2021.3091905
[11] Tian F, Chen X, Liu S, et al. Secrecy rate optimization in wireless multi-hop full duplex networks. IEEE Access. Mar 2018;6:5695–5704. doi: 10.1109/ACCESS.2018.2794739.
[12] Choi Y, Lee JH. A new cooperative jamming technique for a two-hopamplify-and-forward relay network with an eavesdropper. IEEE Trans Veh Technol. Dec 2018;67(12). doi:10.1109/TVT.2018.2878236
[13] Wu Y, Khist A, Xiao C, et al. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE J Sel Areas Commun. Apr 2018;36(4):679–695. doi: 10.1109/JSAC.2018.2825560.
[14] Shakiba-Herfeh M, Chorti A, Vincent H. Physical layer security: authentication, integrity, and confidentiality. Information Theory. Jan 2021;arXiv:2001.07153. doi: 10.48550/arXiv.2001.07153.
[15] Jafarian F, Parvaresh F, Jafarian F. Half-duplex multiple-relay multiple-antenna diamond networks with perfect full-duplex performance. AEU-Int J Electron Commun. Oct 2020;125(3):1–9. doi: 10.1016/j.aeue.2020.153369.
[16] Zhou J, Shen Y, Li L, et al. Efficient pilot design scheme for OFDM-based full-duplex systems. IET Commun. Nov 2020;14:3340–3349. doi: 10.1049/iet-com.2020.0263.
[17] Rabie KM, Adebisi B, Alouini M-S. Half-duplex and full-duplex AF and DF relaying with energy-harvesting in log-normal fading. IEEE Trans Green Commun Netw. December 2017;1(4):468–480. doi: 10.1109/TGCN.2017.2740258.
[18] Bogdanović M. Frequency domain based LS channel estimation in OFDM based power line communications. AUTOMATIKA. Jan 2017;55:487–494. doi:10.7305/automatika.2014.12.639
[19] Goldsmith A. Wireless communications. 2nd ed. Cambridge: Cambridge University Press; 2005.