 doi:10.20944/preprints201912.0003.v1

*Article*

# Machine Learning-Based Node Selection for Cooperative Non-Orthogonal Multi-Access System Under Physical Layer Security

**Mohammed Ahmed Salem [1], Azlan Bin Abd.Aziz [1], Hatem Fahd Al-Selwi [2], Mohamad Yusoff Bin Alias [3], Tan Kim Geok [1], Azwan Mahmud [3], and Ahmed Salem Bin-Ghooth [1]**

1 Faculty of Engineering and Technology (FET), Multimedia University, Malacca, Malaysia
2 Faculty of Electrical Engineering (FKE), Universiti Teknikal Malaysia Melaka, Malacca, Malaysia
3 Faculty of Engineering (FOE), Multimedia University, Selangor, Malaysia

* Correspondence: mohammedmmu94@gmail.com; Tel.: +60-11-2828-0720

**Abstract:** Cooperative non-orthogonal multi access communication is a promising paradigm for the future wireless networks because of its advantages in terms of energy efficiency, wider coverage, and interference mitigating. In this paper, we study the secrecy performance of a downlink cooperative non-orthogonal multi access (NOMA) communication system under the presence of an eavesdropper node. Smart node selection based on feed forward neural networks (FFNN) is proposed in order to improve the physical layer security (PLS) of a cooperative NOMA network. The selected cooperative relay node is employed to enhance the channel capacity of the legal users, where the selected cooperative jammer is employed to degrade the capacity of the wiretapped channel. Simulations of the secrecy performance metric namely the secrecy capacity ($C_S$) are presented and compared with the conventional technique based on fuzzy logic node selection technique. Based on our simulations and discussions the proposed technique outperforms the existing technique in terms of the secrecy performance.

**Keywords:** Physical layer security (PLS), cooperative relay transmission, non-orthogonal multiple access (NOMA), fuzzy logic, feed forward neural networks (FFNN) secrecy capacity.

---

## 1. INTRODUCTION

The increasing growth of wireless communication systems has led to eavesdropping attacks. In order to overcome this issue, the enhancement of security in wireless networks becomes an essential factor.

### *1.1. MOTIVATION AND RELATED LITERATURE*

The concept of physical layer security (PLS) has been proposed to complement the traditional security solutions such as the cryptographic techniques [1], by exploiting the physical layer properties of the wireless communication network. The baseline of Shannon's cipher system [2] and the developments of Aaron Wyner's Wiretap channel [3] introduce the interests of using the physical wireless characterization to enhance the security of data transmission [4].

Cooperative relay communication is a promising concept for wireless networks due to the advantages of energy efficiency, increasing the coverage and mitigating the interference [5]. The authors of [6] suggest the use of jamming signals generated from the destination node to attack an un-trusted relay that is assumed to be the eavesdropper node. The secrecy performance of this strategy is analyzed in terms of the secrecy outage probability (SOP) metric. The authors of [7] illustrate the benefits and uses of the untrusted relay node in cooperative networks. Moreover, several strategies have been considered in the literature in order to improve the PLS such as cooperative jamming [8]-[9], cognitive radio [10], and energy harvesting [11].

NOMA is an essential enabling technology for the fifth generation (5G) wireless networks to meet the heterogeneous demands on low latency, high reliability, massive connectivity, improved fairness, and high throughput [12]. The key idea behind NOMA is to serve multiple users in the same resource block, such as a

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 December 2019 doi:10.20944/preprints201912.0003.v1



time slot, subcarrier, or spreading code. The NOMA principle is a general framework, and several recently proposed 5G multiple access schemes can be viewed as special cases. In [13], the authors consider the use of a relay node with two protocols (amplify-and-forward, and decode-and-forward) in a cooperative NOMA system. The authors of [14] investigate the optimal designs of a NOMA system in terms of the transmission rates, power allocation for each user, and the decoding factor. In [15], NOMA system is considered in large scale communication system. In this strategy, the PLS is implemented by using artificial noise generated from each user node.

Smart node selection is an essential and useful strategy in cooperative NOMA communication networks in terms of enhancing the secrecy performance, saving power and expanding the coverage area. In [16], the authors consider the combination of cooperative relay and jammer selection based on the buffer-aided cooperative node selection scheme. The secrecy performance of this strategy is analyzed in terms of SOP metric. Recently, the integration of cooperative node selection with the artificial intelligence based on fuzzy logic controller strategy has been proposed to enhance the accuracy of the cooperative node selection strategy. Motivated by this integration, the authors of [17] propose a relay selection algorithm for a cooperative wireless sensor networks using fuzzy logic in order to enhance the lifetime and throughput of the network. In [18], the authors propose a relay selection scheme for multi-user cooperative network, where the cooperative relay node is selected based on fuzzy logic employed at the base station node. The authors consider four criteria (SNR, social norm, distance and relays protocol) in the relay selection process based on the channel state information (CSI) available at the base station. Authors of [19] use a relay selection strategy based on fuzzy logic with optimal power allocation and adaptive data rate. The authors considered two cases based on the geographical location of the nodes, where in the first case the distance between the source, relay and the destination are unknown. However, in the second case each node is assumed to know the geographical location of the other nodes.

Machine learning is a widely growing field in recent modern technologies. This technology has been integrated with various fields such as, security [20], signal and image processing [21], and wireless communication networks [22]. In security, machine learning techniques such as neural networks have been investigated and illustrated in considerable researches. In [23], the authors use the artificial neural networks (ANNs) technique as a relay selection method in a detect-and-forward multi-relaying network. The aim of using this method is to enhance the physical layer security of the network. Thus, the transmission between a source and a destination is secure in the presence of an eavesdropper node. Authors of [24] exploit two machine learning based physical layer security techniques namely, Naïve Bayes (NB) and support vector machine (SVM). The authors investigate the benefits of machine learning approach in order to improve the physical layer security in the presence of MIMO-Multi-antenna eavesdropper nodes. In wireless communication networks, machine learning approach has been used in several researches such as channel estimation [25], power allocation [26], and best antenna selection [27].

Based on [17], the network lifetime and end-to-end throughput is enhanced by using node selection based on artificial intelligence strategies. To the best of the authors' knowledge, applying the smart node selection based on neural network methods in cooperative NOMA system under the physical layer security has not been adequately investigated in the literature. In this paper, the smart node selection based on feed forward neural networks integrated with the null-steering jamming strategy in a cooperative NOMA network is analysed to select the best cooperative relay or jammer nodes in the presence of an eavesdropper node.

### *1.2. MAIN CONTRIBUTIONS*

Unlike the summarized papers above, this paper investigates the secrecy capacity of a cooperative NOMA communication network integrated with a smart node selection strategy based on feed forward neural networks. The main contributions of this paper are summarized as follows.

- We integrate the use of jammer and relay nodes to degrade the capacity of the eavesdropper node and enhance the capacity of the user node respectively. We use the null-steering beamforming technique to direct the shared jamming signal towards the eavesdropper node.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 December 2019 doi:10.20944/preprints201912.0003.v1



- We employ the feed forward neural network (FFNN) strategy in order to select the best cooperative node for the relaying or jamming techniques. This approach is compared with another selection approach based on fuzzy logic strategy.

The rest of this paper is organized as follows. Section 2 demonstrates the system model and the signal transmission. Section 3 presents the node selection strategies. Section 4 explains the secrecy performance analysis of the system model. Section 5 shows the results and discussions of the paper. Finally, section 6 presents the conclusion of this paper.

## 2. SYSTEM MODEL

We consider a secure non-orthogonal multi access (NOMA) system, where a base station ($B_s$) communicates with a strong user ($User_1$) (good channel conditions) and a weak user ($User_2$) (poor channel conditions) in the presence of a passive eavesdropper node which is able to monitor the main channel, as shown in Figure 1. The cooperative helper nodes ($R_1, R_2, ..., R_N$) are employed to enhance the secrecy performance of the communication scenario. In this system model, the users and the eavesdropper nodes are equipped with a single antenna. However, the helper nodes are equipped with M antennas. Moreover, the transmission time is divided to time frames in which each time frame is divided into two time slots (phases).

In this system model, we assumed that the eavesdropper node is a passive communication node which has no access to the information signal transmitted to the receiver node. Moreover, we assumed that the eavesdropper node has the ability of differentiating and detecting the superimposed data transmitted from the base station to the users [28]. This assumption provides the lower bounds for the practical scenario, where the eavesdropper node is given a strong decoding capabilities.

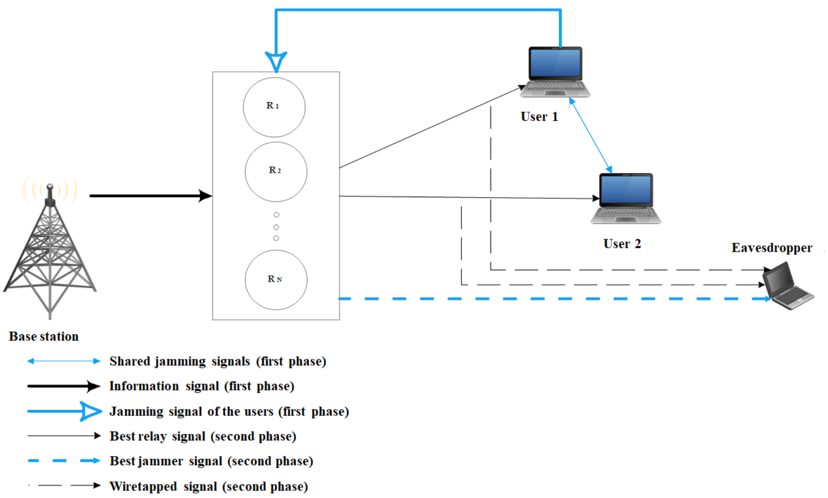



**Figure 1.** System model

### 2.1. COOPERATIVE HELPER (RELAY AND JAMMER) NODES

Cooperative communication techniques are employed either to strengthening the legal main channel of the user nodes (by using cooperative relay nodes) or to degrade the illegal wiretapped channel of the eavesdropper node (by using cooperative jammer node) [29]-[30]. The use of these techniques enhances significantly the secrecy performance of the NOMA system. In this paper, we used both techniques in order to have a secure communication between the base station and the user nodes. Moreover, the eavesdropper's channel state information (CSI) is assumed to be available at the base station and the cooperative helper nodes [32]. The cooperative helper node is selected as a cooperative relay node or a cooperative jammer by using a node selection method based on fuzzy logic and feed forward neural networks strategies.

In this paper, the relay is assumed to be a half-duplex two-way with an amplify-and-forward protocol. The relay is used as transmission node between the base station and the users with no direct channel between

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 December 2019 doi:10.20944/preprints201912.0003.v1



base station and users. Thus, the communication happens in two time slots (phases) as illustrated in Figure 1. Moreover, the cooperative relay node is used in order to enhance and improve the channel capacity of the user nodes.

In this work, the cooperative jammer node uses the CSI information to build a jamming-null-steering beamforming strategy, where the shared jamming signals generated by the users are directed to the eavesdropper node. However, the shared jamming signals are nulled in the directions of the legal user nodes. This strategy ensures that the communication channel between the friendly jammer and the legal user nodes is not available. Thus, the channel capacity of the eavesdropper node is degraded without affecting the legal user nodes. The jamming-null-steering beamforming at the jammer node is expressed as,

$$NB_E = \frac{(I_M - W)\, h_{R_j,E}}{\left\|(I_M - W)\, h_{R_j,E}\right\|} \tag{1}$$

where, $I_M$ is the identity matrix with $M * M$, $W$ is the projection matrix to the orthogonal subspace of the legal user nodes with $W = G\left(G^H G\right)^{-1} G^H$, $G = \left[h_{R_j,U_1} h_{R_j,U_2}\right]$, and $h_{R_j,U_1}$, $h_{R_j,U_2}$ and $h_{R_j,E}$ are the channel gains between the friendly jammer node and the legal user nodes $(U_1, U_2)$ and the eavesdropper node respectively.

### *2.2. CHANNEL ASSUMPTIONS*

In this model, the communication links between the nodes are assumed to be Rayleigh fading channel with exponential path loss. The coefficient of a channel link between two nodes is expressed by $h_{ab}$, where a is the node where the transmission starts and, b is the node where the transmission ends. These coefficients are modelled as constant and identically distributed at the transmission phases. Moreover, the channel state information (CSI) of the users and the eavesdropper nodes are assumed to be perfectly available at the base station and the cooperative helper nodes. However, In practice, the user nodes estimate the absolute values of the CSI from the cooperative nodes to the eavesdropper node then feed it back to the base station via the cooperative nodes. Furthermore, the noise is assumed to be a complex additive white Gaussian noise (AWGN) with zero mean and unit variance.

### *2.3. SIGNAL TRANSMISSION MODEL*

This section explains the flow of the transmitted superimposed information signal from the base station to the user nodes via the cooperative relay node and under the protection of the cooperative jammer node.

In the first phase, the base station transmits the superimposed information signals to the helper nodes. The received signal at each helper node is written as,

$$X_{BS,R_i} = \sqrt{P_{BS} a_{u_1}}\, h_{BS,R_i} B_{U_1} x_1 + \sqrt{P_{BS} a_{u_2}}\, h_{BS,R_i} B_{U_2} x_2 + \mathfrak{n}_{BS,R_i} \tag{2}$$

where, $P_{BS}$ is the power of the base station,$a_{u_1}$ and $a_{u_2}$ are the power allocation coefficient for $user_1$ and $user_2$ respectively, $x_1$ and $x_2$ are the information to $user_1$ and $user_2$ respectively, $h_{BS,R_i}$ is the channel gain between the base station and the helper node, the subscript $i$ stands for the number of the cooperative helper node, $B_{U_1}$, $B_{U_1}$ are the maximum ratio transmission beamforming vector build by the base station for the strong user and the weak user respectively, and $\mathfrak{n}_{BS,R_i}$ is the AWGN noise from the base station to the helper node. At the same phase, $user_1$ and $user_2$ generate jamming signals and share these signals. The shared jamming signals are given as,

$$J_{u_1} = \sqrt{P_{u_1}}\, h_{u_1,u_2} j_1 + \mathfrak{n}_{u_1,u_2}$$

$$J_{u_2} = \sqrt{P_{u_2}}\, h_{u_2,u_1} j_2 + \mathfrak{n}_{u_2,u_1} \tag{3}$$

where, $P_{u_1}$ and $P_{u_2}$ are the powers of the users respectively, $j_1$ and $j_2$ are the artificial jamming signals from $user_1$ and $user_2$ respectively, $h_{u_1,u_2}$ and $h_{u_2,u_1}$ are the channel gains between the users, and $\mathfrak{n}_{u_1,u_2}$ and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 December 2019 doi:10.20944/preprints201912.0003.v1



$\mathfrak{n}_{u_2,u_1}$ are the AWGN noise between the users. The shared jamming signals are transmitted by the strong user to the helper nodes. The received jamming signal at each helper node is given as,

$$J_{u_1,R_i} = \left(J_{u_1} + J_{u_2}\right) h_{u_1,R_i} + \mathfrak{n}_{u_1,R_i} \tag{4}$$

where, $h_{u_1,R_i}$ is the channel gain between the strong user and the helper node and $\mathfrak{n}_{u_1,R_i}$ is the AWGN noise from the strong user to the helper node.

At this stage each helper node is aware of the received signals from the legitimate nodes. These signals are summarised as follows.

- The superimposed information signal transmitted by the base station. Equation 2 illustrates the superimposed information signal received at the helper nodes.
- The shared jamming signal transmitted by strong user. Equations 3 and 4 demonstrate the shared jamming signal received at the helper nodes.

In the second phase, the selected cooperative relay node amplifies-and-forwards the superimposed information signal to the user nodes. The amplification factor $(A_F)$ is expressed as [33],

$$A_F = \sqrt{\frac{P_{R_s}}{P_{BS}\left|h_{BS,R_s}\right|^2 + P_{u_1}\left|h_{u_1,R_i}\right|^2 + \sigma}} \tag{5}$$

where, $P_{R_s}$ is the power of the selected cooperative relay node, the subscript $s$ stands for the selected cooperative relay node, and $\sigma$ denotes the variance of the AWGN noise.

The forwarded signal to the strong user $(user_1)$ is expressed as,

$$Y^{A_F}_{R_s,u_1} = \left[A_F h_{R_s,u_1}\left(X_{BS,R_s}\right)\right] + \mathfrak{n}_{R_s,u_1} \tag{6}$$

The forwarded signal to the weak user $(user_2)$ is expressed as,

$$Y^{A_F}_{R_s,u_2} = \left[A_F h_{R_s,u_2}\left(X_{BS,R_s}\right)\right] + \mathfrak{n}_{R_s,u_2} \tag{7}$$

At the same phase, the eavesdropper wiretaps the main channel in order to receive the transmitted signal from the cooperative relay to the user nodes. However, the selected cooperative jammer node directs the shared jamming signal towards the eavesdropper node. The received signal at the eavesdropper node under the protection of the selected cooperative jammer node is given as,

$$Y^{A_F}_{R_s,E} = A_F h_{R_s,E} X_{BS,R_s} + h_{R_j,E} J_{u_1,R_j} NB_E + \mathfrak{n}_{R_s,E} \tag{8}$$

where, $NB_E$ is the jamming-null-steering beamforming vector build by the selected cooperative jammer node, $h_{R_j,E}$ is the channel gain between the selected cooperative jammer node and the eavesdropper node, and the subscript $j$ stands for selected cooperative jammer node.

## 3. SMART NODE SELECTION STRATEGIES

In this section, we illustrate the cooperative node selection based on fuzzy logic (FL) and feed forward neural network (FFNN) strategies.

### *3.1. FUZZY LOGIC SELECTION*

Figure 2 demonstrates the general flowchart of the fuzzy logic strategy used to select the best cooperative relay and jammer node respectively.

Based on Figure 2, three main steps are required to select the best cooperative relay or jammer nodes based on the fuzzy logic controller strategy.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 December 2019 doi:10.20944/preprints201912.0003.v1



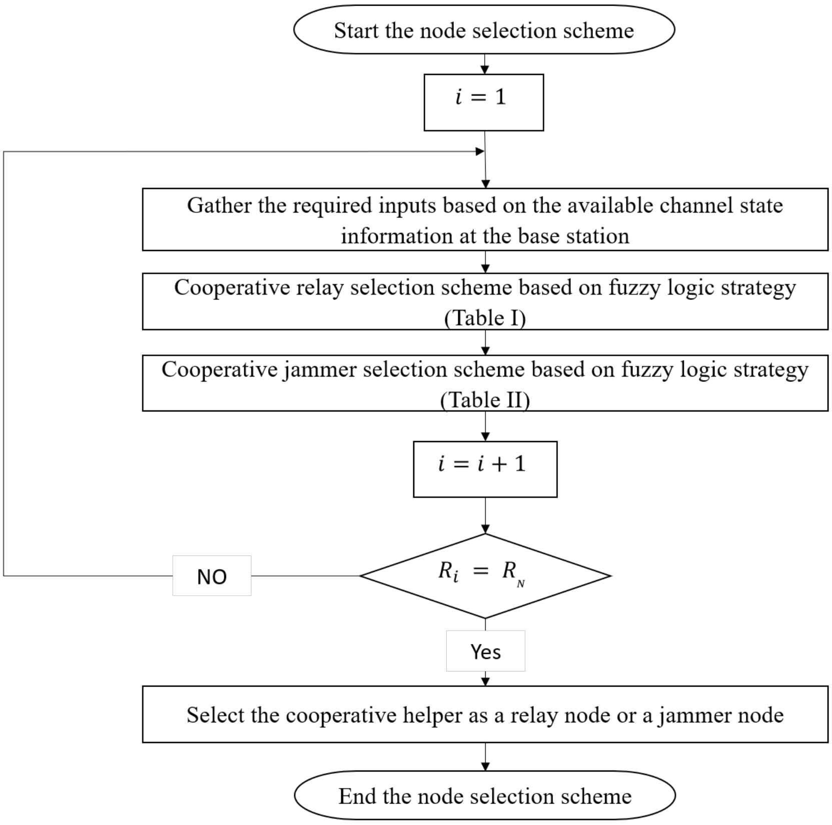



**Figure 2.** Flowchart of cooperative node selection based on fuzzy logic

3.1.1. Required input gathering

At the end of each time frame the base station gathers the estimated information of network users, and at the beginning of each time frame the base station selects the best cooperative relay enhance the legal channel capacity and the best cooperative jammer to degrade the wiretapped channel capacity. To this end, the base station should estimate five parameters namely, signal to noise ratio for the legal users ($SNR_U$), power amplification factor ($PAF$), the distance between the cooperative helper and legal user nodes ($D_U$), signal to noise ratio for the eavesdropper ($SNR_E$),and the distance between the cooperative helper and the eavesdropper ($D_E$). These parameters are gathered with the help of the channel state information (CSI) available at the base station. In order to use these parameters in the fuzzy logic model, we normalized the each parameter value to the interval [0,1].

- Signal to noise ratio (for the legal users $SNR_U$)

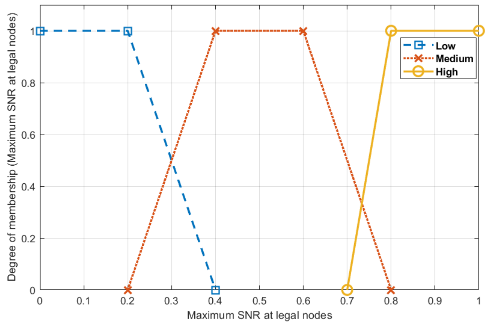
Signal-to-noise ratio is the main criterion in the process of helper selection. The SNR values for the system model shown in Fig 1 are calculated as,

$$\xi_{u_1} = \frac{A_F^2 P_{BS} a_{u_1} \left|h_{R_i u_1}\right|^2 \left|h_{BS,R_i}\right|^2}{\left(A_F^2 \left|h_{R_i u_1}\right|^2 + 1\right)\sigma^2} \tag{9}$$

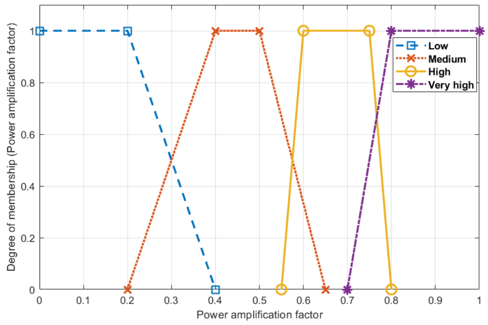
$$\xi_{u_2} = \frac{A_F^2 P_{BS} a_{u_2} \left|h_{R_i,u_2}\right|^2 \left|h_{BS,R_i}\right|^2}{A_F^2 P_{BS} a_{u_1} \left|h_{R_i,u_2}\right|^2 \left|h_{BS,R_i}\right|^2 + \left(A_F^2 \left|h_{R_i,u_2}\right|^2 + 1\right)\sigma^2} \tag{10}$$

We mapped the maximum normalized $SNR_U$ into low, medium and high as shown in Figure 3 (a). The maximum SNR is chosen as,

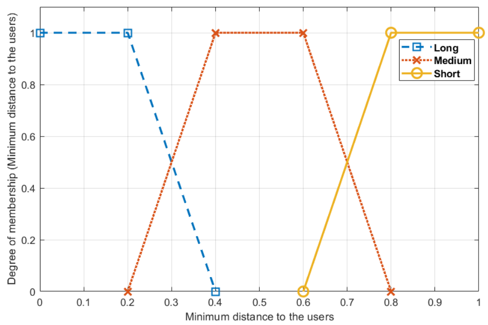
$$\mathrm{SNR_U} = \max\left\{\xi_{u_1}, \xi_{u_2}\right\} \tag{11}$$




**(a)** Membership function for $SNR_U$




**(b)** Membership function for $PAF$




**(c)** Membership function for $D_U$

**Figure 3.** Membership function for cooperative relay input fuzzy sets

- Power amplification factor ($PAF$)

Power amplification factor is a direct aspect to enhance the capacity of the main communication channels between the selected cooperative relay node and the legal user nodes. Equation (5) is used in order to calculate the power amplification factor. We mapped the normalized power amplification factor into low, medium, high and very high as shown in Figure 3 (b).

- Distance between the cooperative helper and legal user nodes ($D_U$)

The helper location has significant impact on average achievable rate at the receiver nodes. The distances between the helper nodes and the legal user nodes are calculated as,

$$\begin{aligned} D_{U_1} &= \sqrt{\left(X_{U_1} - X_{R_i}\right)^2 + \left(Y_{U_1} - Y_{R_i}\right)^2} \\ D_{U_2} &= \sqrt{\left(X_{U_2} - X_{R_i}\right)^2 + \left(Y_{U_2} - Y_{R_i}\right)^2} \end{aligned} \tag{12}$$

where, $X_{U_1}$, $X_{U_2}$ and $X_{R_i}$ are the coordinates of the horizontal axis for $user_1$, $user_2$ and the cooperative helper node $i$, and $Y_{U_1}$, $Y_{U_2}$ and $Y_{R_i}$ are the coordinates of the vertical axis for $user_1$, $user_2$ and the cooperative helper node $i$. In this work, we choose the minimum distance between the cooperative helper and legal nodes. The minimum distance is given as,

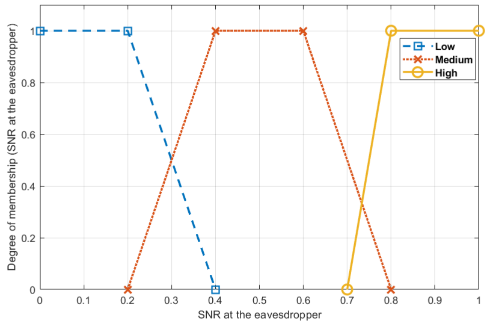
$$D_U = \min\left\{D_{U_1}, D_{U_2}\right\} \tag{13}$$

We mapped the normalized minimum distance ($D_U$) into long, medium and short as shown in Figure 3 (c).

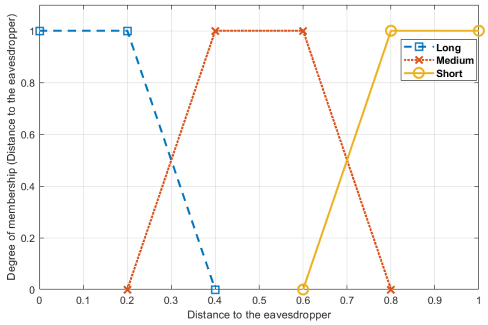
- Signal to noise ratio (for the eavesdropper $SNR_E$)

doi:10.20944/preprints201912.0003.v1

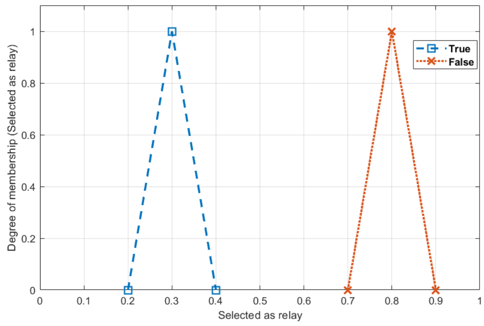





**(a)** Membership function for $SNR_E$




**(b)** Membership function for $D_E$




**(c)** Membership function for $R_S$

**Figure 4.** Membership function for cooperative jammer input fuzzy sets

The SNR values for the eavesdropper node is expressed as,

$$\xi_E = \frac{A_F^2 P_{BS} a_m \left|h_{R_i,E}\right|^2 \left|h_{BS,R_i}\right|^2}{A_F^2 \left|h_{R_i,E}\right|^2 J_{u_1,R_i} \left|NB_E\right|^2 + \left(A_F^2 \left|h_{R_i,E}\right|^2 + 1\right)\sigma^2} \quad (14)$$

where, $m \in (U_1, U_2)$. We mapped the normalized $SNR_E$ into low, medium and high as shown in Figure 4 (a).

- Distance between the cooperative helper and the eavesdropper ($D_E$)

The distances between the helper nodes and the eavesdropper node are calculated as,

$$D_E = \sqrt{\left(X_E - X_{R_i}\right)^2 + \left(Y_E - Y_{R_i}\right)^2} \quad (15)$$

We mapped the normalized distance ($D_E$) into long, medium and short as shown in Figure 4 (b).

- The cooperative helper node is selected as the best relay ($R_S$)

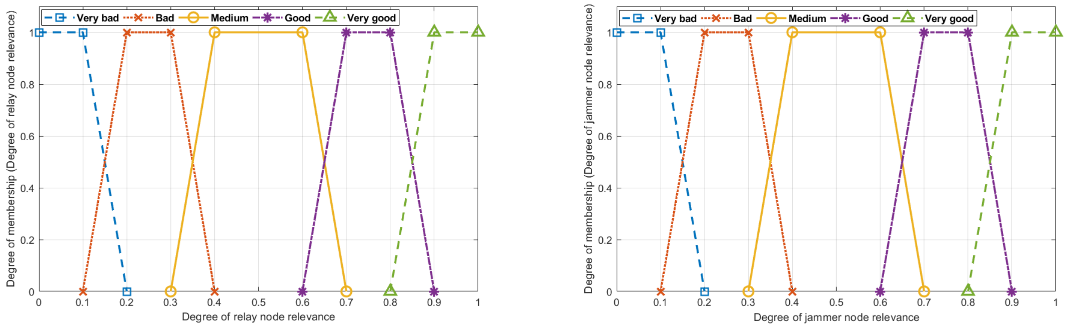
In this work, the priority is given to the relay selection. In other words, the output for the degree of relay node relevance is fed as an input for the jammer node selection. Hence, if the cooperative helper node is selected as a relay then the degree of jammer relevance for that node is very bad. We mapped the relay node selection into true and false as shown in Figure 4 (c).

This step is summarized as follows.

- The required parameters are gathered based on the available channel state information (CSI) at the base station node.
- Each parameter is mapped in a fuzzy set. the fuzzy sets are as follows.

*Preprints* (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 December 2019 doi:10.20944/preprints201912.0003.v1






**(a)** Cooperative relay

**(b)** Cooperative jammer

**Figure 5.** Membership function for degree of cooperative node relevance

- $SNR_U \in$ { Low, Medium, High }
- PAF $\in$ { Low, Medium, High, Very high }
- $D_U \in$ { Long, Medium, Short }
- $SNR_E \in$ { Low, Medium, High }
- $D_E \in$ { Long, Medium, Short }
- $R_S \in$ { True, False }

#### 3.1.2. Process of Fuzzification

In this step, we use the fuzzy inference system (FIS) to obtain the fuzzy sets $Z_r$ and $Z_j$ that maps the degree of relevance for relay and jammer respectively. However, these fuzzy sets are a description of $f_r(SNR_U, PAF, D_U)$ and $f_j(SNR_E, D_U, R_S)$ functions. The relevance fuzzy sets are given as.

$$\begin{aligned} Z_r &\in \{\text{ Very bad, Bad, Medium, Good, Very good }\} \\ Z_j &\in \{\text{ Very bad, Bad, Medium, Good, Very good}\} \end{aligned} \tag{16}$$

where, very bad, bad, medium, good, and very good are the degree of relevance for each cooperative node. In other word, if the degree of relaying relevance for any cooperative node is very good, then the probability of selecting this node as a relay is high. Figure 5 shows the membership function for the relay and jammer nodes relevance fuzzy sets respectively. In this work, we use AND logic in determining the fuzzy rules and in order to map the input fuzzy sets $(SNR_U, PAF, D_U, SNR_E, D_U, R_S)$ into the relevance fuzzy sets $(Z_r, Z_j)$. Table 1 summarizes the fuzzy rules for the cooperative relay selection scheme.

**Table 1.** Rules for relay selection scheme

| | | Power amplification factor | | | |
|---|---|---|---|---|---|
| **SNR** | **Distance** | **Low** | **Medium** | **High** | **Very High** |
| Low | long | Very bad | Bad | Bad | Medium |
| Low | Medium | Very bad | Bad | Bad | Medium |
| Low | Short | Very bad | Medium | Medium | Medium |
| Medium | long | Very bad | Medium | Medium | Medium |
| Medium | Medium | Bad | Medium | Good | Good |
| Medium | Short | Bad | Medium | Good | Good |
| High | long | Bad | Medium | Medium | Good |
| High | Medium | Medium | Good | Good | Very Good |
| High | Short | Medium | Good | Very Good | Very Good |

In this paper, we have 36 fuzzy rules for the cooperative relay selection scheme and 18 fuzzy rules for the cooperative jammer selection scheme. Note that the priority is for the cooperative relay selection scheme, so

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 December 2019 doi:10.20944/preprints201912.0003.v1



the cooperative relay node is selected first, then the cooperative jammer node is selected. Table 2 summarizes the fuzzy rules for the cooperative jammer selection scheme.

**Table 2.** Rules for jammer selection scheme

| SNR | Distance | The node is selected as relay: True | The node is selected as relay: False |
|---|---|---|---|
| Low | long | Very bad | Medium |
| Low | Medium | Very bad | Good |
| Low | Short | Very bad | Very good |
| Medium | long | Very bad | Bad |
| Medium | Medium | Very bad | Medium |
| Medium | Short | Very bad | Medium |
| High | long | Very bad | Very bad |
| High | Medium | Very bad | Bad |
| High | Short | Very bad | Bad |

3.1.3. Process of defuzzification

This section illustrates the process of obtaining the output (degree of (relay or jammer) relevance). In order to obtain the outputs of the fuzzy logic system we used the process of crisp output center of sum defuzzification method denoted as $z_{crisp}$. Firstly, the fuzzy logic controller calculates the geometric centre of area defined as $COA$ for all the membership function of the relay and jammer degree of relevance [34]. The geometric centre of area is given as,

$$\mathrm{COA}_{\mathrm{Z_r}} = \frac{\int \mu_{Z_r}(Z_r) Z_r \mathrm{d}Z_r}{\int \mu_{Z_r}(Z_r) \mathrm{d}Z_r}$$

$$\mathrm{COA}_{\mathrm{Z_j}} = \frac{\int \mu_{Z_j}(Z_j) Z_j \mathrm{d}Z_j}{\int \mu_{Z_j}(Z_j) \mathrm{d}Z_j} \quad (17)$$

Finally, the controller calculates weighted average for the geometric centre of area for all the membership function of the relay and jammer degree of relevance. The weighted average for the geometric centre of area is given as,

$$z_{\mathrm{crisp_r}} = \frac{\sum_{i=1}^{N} \mathrm{COA}_{z_{r_i}} \cdot \mathrm{A}_{z_{r_i}}}{\sum_{i=1}^{N} \mathrm{A}_{z_{r_i}}}$$

$$z_{\mathrm{crisp_j}} = \frac{\sum_{i=1}^{N} \mathrm{COA}_{z_{j_i}} \cdot \mathrm{A}_{z_{j_i}}}{\sum_{i=1}^{N} \mathrm{A}_{z_{j_i}}} \quad (18)$$

where, $A$ is the area under the scaled membership functions for the relay $(A_{z_{r_i}})$ and jammer $(A_{z_{j_i}})$ degree of relevance and within the range of the output variable.

### *3.2. MACHINE LEARNING-BASED FEED FORWARD NEURAL NETWORK SELECTION*

In this paper, a machine learning FFNN-based algorithm is proposed in order to select the best cooperative relay and jammer nodes respectively. In this section, the main steps for the proposed strategy are explained in detail.

3.2.1. Input Data Generation

For training the FFNN model, cooperative relay and jammer data are generated containing $L$ samples. The generated data is extracted from the known CSI at the base-station node. The generated relay data denoted as $GD_R$ consists of three parameters, namely $SNR_U$, $PAF$, and $D_U$. Similarly, the generated jammer

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 December 2019 doi:10.20944/preprints201912.0003.v1



data denoted as $GD_J$ consist of three parameters, namely $SNR_E$, $D_E$, and $R_S$. These parameters are expressed as,

$$GD_R = [SNR_U, PAF, D_U]^L \tag{19}$$

$$GD_J = [SNR_E, R_S, D_E]^L \tag{20}$$

where, $SNR_U$,PAF, $D_U$, $SNR_E$, $R_S$ and $D_E$ are the estimated information of the network users gathered by the base-station at the end of each frame. We normalized the generated data to the interval [0,1].

#### 3.2.2. Output Labelling

In the data generated, the degree of relay node relevance and the degree of jammer relevance are chosen as the performance indicators for relay and jammer respectively. Each training data sample is associated with a performance indicator corresponding to the current sample. Table 3 illustrates the labelling of cooperative nodes relevance.

**Table 3.** Labelling the relevance of the cooperative nodes

| **Cooperative (relay or jammer) relevance** | **Label (t)** |
|---|---|
| Very bad | 0 |
| Bad | 1 |
| Medium | 2 |
| Good | 3 |
| Very good | 4 |

Based on Table 3, the training data samples are labelled according to the performance of each relay and jammer nodes respectively.

#### 3.2.3. Data Set Training

After generating the input samples and output labels, the input-output pairs are concatenated to create two full data sets for relay and jammer respectively.

$$D_{relay\ train} = \{([GD_R]^1, t^1), ([GD_R]^2, t^2), \ldots, ([GD_R]^L, t^L)\} \tag{21}$$

$$D_{jammer\ train} = \left\{\left([GD_J]^1, t^1\right), \left([GD_J]^2, t^2\right), \ldots, \left([GD_J]^L, t^L\right)\right\} \tag{22}$$

where, $t^L$ is the Lth class label.

#### 3.2.4. FFNN structure

The labelled training data sets is used to train the FFNN model. The input of the models are absolute values of the generated data $(GD_R, GD_J)$ and the output is the performance of the relay or jammer. The output of the model indicates the degree of relevance for relay and jammer respectively. Here, the basics of the neural network is described briefly. The structure of the FFNN model consists of multiple hidden layers, each hidden layer contains multiple neutral nodes. After each layer a nonlinear function (activation function) is implemented. Due to their efficiency in generalizing the trained model ,the nonlinear activation functions are the most used activation functions, the most common choices of these functions is the rectified linear unit ($ReLU$) function expressed by,

$$f_{ReLU}(x) = \max(0, x) \tag{23}$$

where, x is the argument of the function. Choosing an activation function is a vital step when building a neural network model and ensures a good performance model . In this experiment, the ReLU function is applied to all hidden layers where it enables the model to learn more complex structures and generalize to variety of data. Our experiment is a multi-class classification case. Thus, an activation function is used at the output layer expressed by,

$$f_{Softmax}(x_i) = \frac{\exp(x_i)}{\sum_{j=i}^{C} \exp(x_j)'} \tag{24}$$

where, C is the number of classes, $i, j \in 1,2,\ldots,C$, and $x_i, x_j$ are scores of the ith class and jth class, respectively. The network model consists of four layers namely, input, two hidden and output layers. The input layer takes input parameters $(GD_R, GD_J)$ for relay or jammer nodes receptively. Figure 6 shows the feed forward neural networks design model.

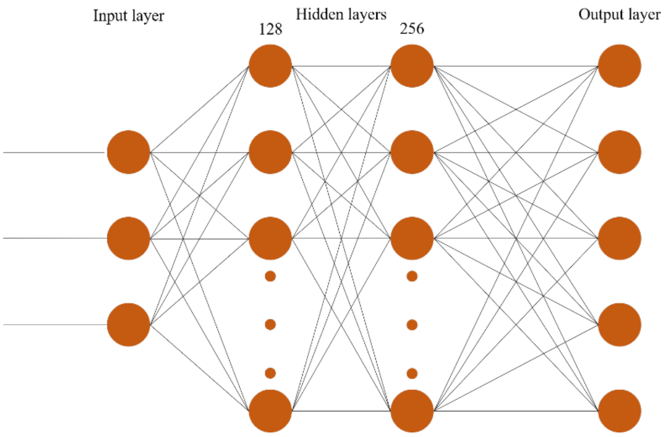



**Figure 6.** FFNN design model

Based on Figure 6, the first and the second hidden layers consist of 128, 256 neurons, respectively. The output layer consists of five neurons corresponding to the classes of the cooperative (relay or jammer) relevance. Softmax function is applied to this layer which gives us the probability distribution over all classes. The final output of the network is the class with the maximum probability value.

3.2.5. FFNN training

In this section, the process of setting the training parameters of our FFNN model is described. In total, two data sets were generated using two groups of data samples, 60000 samples of relay data $(GD_R)$ and 60000 samples of jammer data $(GD_J)$. Two models were trained using the two data sets of relay and jammer respectively. The training data sets were split into the training set and the testing set. The training set was used to train the model parameters and the testing set was used to evaluate the trained model. In this FFNN model, cross entropy is applied as the loss function for our FFNN model. Therefore, the loss function for each ith sample of input $GD_R$ of relay data and each jth sample of input $GD_J$ of jammer data is formulated as,

$$Loss_R\left(t^i, o\left(GD_R^i, W, b\right)\right) = -\log\left(o\left(GD_R^i, W, b\right)\right)$$

$$Loss_J\left(t^j, o\left(GD_J^j, W, b\right)\right) = -\log\left(o\left(GD_J^j, W, b\right)\right) \tag{25}$$

where, $o\left(GD_R^i, W, b\right)$ is the output that is predicted by the model for the best cooperative relay node. The target of the training process is to find the suitable parameters W and b that minimize the average loss “cost function” of entry training data sets, the cost function is defined as,

$$L_R(\Theta) = \frac{1}{M}\sum_{i=1}^{M} Loss\left(t^i, o\left(GD_R^i, W, b\right)\right)$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 December 2019 doi:10.20944/preprints201912.0003.v1



$$L_J(\Theta) = \frac{1}{M}\sum_{j=1}^{M} Loss\left(t^j, o\left(GD_J^j, W, b\right)\right) \tag{26}$$

where the set $\Theta = \{W, b\}$ contains every training parameter of the FFNN model. Every parameter is generally adjusted iteratively using the gradient descent methods. At each iteration, every parameter is adjusted simultaneously as,

$$\Theta^{m+1} = \Theta^m - \eta^{\nabla_\Theta} L(\Theta), \tag{27}$$

where $\nabla_\Theta$ represents as the gradient operator with respect to $\Theta$, $\eta$ is the learning rate, and $m$ is the iteration number (250 iterations). Backpropagation is used to update the weights W and biases b of the neural network using the local error of the network. During training the network, when a prediction is made for the input values, the actual output values are compared to the predicted values and an error is calculated. The calculated error is then used to update the weights W and biases b of the network starting at the layers connected directly to the output nodes and then proceeding further backward toward the binput layer. In other words, the backpropagation is used to calculate the gradients efficiently which is then used to train the network, by adjusting the weights W and biases b throughout the network to get the desired output.

In this experiment , Adam optimization algorithm was applied to the FFNN model because it is a first-order gradient-based optimization algorithm, thus reducing computational complexity [17]. In addition, the dropout technique is applied in this FFNN model in order to reduce the overfit in training and improve generalization of the model (0.5 dropout was chosen), for which the proposed FFNN model performs well. Finally, after training and testing the two models of relay and jammer respectively , the FFNN models are frozen and can be used to select the best cooperative helper node as a relay or jammer.

## 4. SECRECY PERFORMANCE ANALYSIS

In this section, we illustrate the secrecy performance metric in terms of the secrecy capacity for the system model shown in Figure 1 assisted with the fuzzy logic and the feed forward neural network strategies. The secrecy capacity metric is defined as the maximum capacity rate difference between the channel capacity of the legitimate users and the channel capacity of the eavesdropper node. The channel capacity of the strong user ($user_1$) is given as,

$$\zeta_{u_1} = \frac{1}{2}\log_2\left(1 + \xi_{u_1}\right) \tag{28}$$

where, $\xi_{u_1}$ is the signal to noise ratio (SNR) at the strong user expressed in equation (9). The strong user is able to decode the weak user's information signal and suppressed it by using the successive interference cancellation (SIC) strategy. The channel capacity of the weak user ($user_2$) is given as,

$$\zeta_{u_2} = \frac{1}{2}\log_2\left(1 + \xi_{u_2}\right) \tag{29}$$

where, $\xi_{u_2}$ is the signal to interference plus noise ratio (SINR) at the weak user expressed in equation (10). The weak user is not able to decode the strong user's information signal, so the strong user's information signal is an interference to the weak user. The channel capacity of the eavesdropper node is given as,

$$\zeta_E = \frac{1}{2}\log_2\left(1 + \xi_E\right) \tag{30}$$

where, $\xi_E$ is the signal to jamming plus noise ratio (SJNR) at the eavesdropper node expressed in equation (14). We assume that the eavesdropper node is able to distinguish the superimposed mixture signal by using the parallel interference cancellation (PIC) strategy.The secrecy capacity for each user is formulated as,

$$[\zeta_{u_1}^E]^+ = \max\{[\zeta_{u_1} - \zeta_E], 0\}$$

$$[\zeta^{E}_{u_2}]^+ = \max\{[\zeta_{u_2} - \zeta_E], 0\} \tag{31}$$

In order to evaluate the accuracy of the proposed cooperative node selection strategy, the error analysis is carried on by comparing the secrecy capacity achieved based on the fuzzy logic and the FFNN strategies with maximum secrecy capacity of the system model.

In this paper, the maximum secrecy capacity is achieved when the eavesdropper node does not exist. The maximum secrecy capacity at each user is respectively formulated as,

$$[\zeta^{max}_{u_1}]^+ = \max\{[\zeta_{u_1}], 0\}$$

$$[\zeta^{max}_{u_2}]^+ = \max\{[\zeta_{u_2}], 0\} \tag{32}$$

In this section, the accuracy percentage ($A_p$), and the root mean square error ($RMSe$) equations for both users are respectively given as,

$$A_{p_{u_m}} = \left(1 - \left|\frac{\left|[\zeta^{max}_{u_1}]^+ - [\zeta^{E}_{u_m}]^+\right|}{[\zeta^{max}_{u_m}]^+}\right|\right) \times 100\% \tag{33}$$

$$\mathrm{RMSe}_{\mathrm{u}_m} = \sqrt{\frac{\sum_{\mathrm{k}=1}^{\mathrm{K}}\left([\zeta^{\mathrm{max}}_{\mathrm{u}_m}]^+ - [\zeta^{\mathrm{E}}_{\mathrm{u}_m}]^+\right)^2}{\mathrm{K}}} \tag{34}$$

where, K is the maximum repetition based on the maximum transmit power.

## 5. RESULTS AND DISCUSSION

In this section, the numerical results are obtained and discussed to evaluate the secrecy performance of the proposed cooperative NOMA assisted with null-steering beamforming jamming and node selection based on FFNN technique. The simulation setup parameters of the proposed technique are summarized in Table 4.

**Table 4.** SIMULATION SET UP PARAMETERS

| PARAMETER | DETAILS |
|---|---|
| Cooperative nodes | Five cooperative nodes |
| Nodes locations | Illustrated in Figure 7 |
| Power allocation for the strong user | 0.2 |
| Power allocation for the weak user | 0.8 |
| Total transmission power | 30 dBm |
| Path loss coefficient | 3.5 |
| Noise density | -60 dBm |
| Channel model | Slow fading Rayleigh channel |
| Defuzzification process | Crisp output center of sum |

Figure 7 shows the geographical locations of the cooperative NOMA system for all the nodes. These locations are used in order to simulate the experiments (1 and 2).

Table 4 and Figure 7 illustrate that five cooperative helper nodes are used in order to complete the relaying and jamming processes. However, the data relaying process is done by a single cooperative relay node selected by using a smart node selection strategy discussed in section 4. Similarly, jamming the eavesdropper node is done by a selected cooperative jammer node.

The distances between the base station and the cooperative helper nodes are assumed to be non-equidistant to the distances between the relay nodes and the legal users. The eavesdropper is positioned at a fixed coordinates (1500, -200) about 1513.28 meters away from the base station.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 December 2019 doi:10.20944/preprints201912.0003.v1



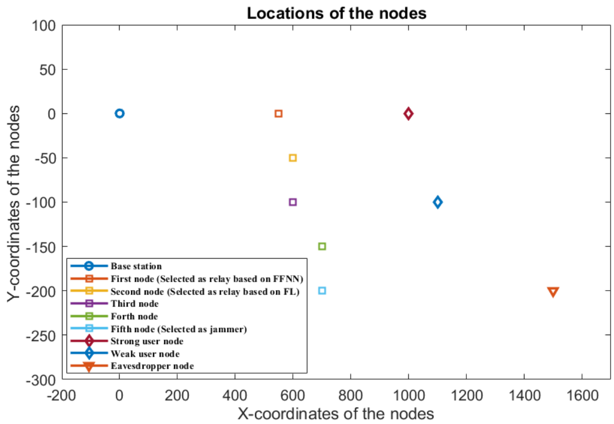



**Figure 7.** Locations of the nodes for the experiments

In this section, we evaluate the smart node selection by two experiments. Each experiment discusses smart node selection based on FFNN and fuzzy logic strategies.

### *5.1. EXPERIMENT 1 (PROPOSED SMART NODE SELECTION BASED ON FFNN STRATEGY)*

In this experiment, we propose a machine learning based on FFNN strategy to select the best cooperative (relay, jammer) node. This strategy is proposed in order to enhance the physical layer security of the cooperative NOMA system shown in Figure 1.

Table 5 illustrates the cooperative relay selection based on FFNN strategy. The relay selection criteria are extracted based on the known CSI at the base-station.

**Table 5.** Cooperative relay selection based on feed forward neural networks

| Node | Relay selection criteria | | | Relevance | Selection |
|---|---|---|---|---|---|
| | $SNR_U$ | $PAF$ | $D_U$ | | |
| 1 | 0.8684 | 0.7213 | 0.7284 | Very good | Selected |
| 2 | 0.8522 | 0.6953 | 0.6429 | Good | |
| 3 | 0.4855 | 0.6844 | 0.5890 | Medium | |
| 4 | 0.3010 | 0.6920 | 0.5759 | Medium | |
| 5 | 0.1717 | 0.5429 | 0.6061 | Bad | |

Based on Table 5, we observe that the first cooperative node gives the best relay relevance (very good) in comparison with the other cooperative nodes, hence it is selected by the base-station as the best cooperative relay node. Table 6 illustrates the cooperative jammer selection based on FFNN strategy.

**Table 6.** Cooperative jammer selection based on feed forward neural networks

| Node | Jammer selection criteria | | | Relevance | Selection |
|---|---|---|---|---|---|
| | $SNR_E$ | $D_E$ | $R_S$ | | |
| 1 | 0.8981 | 0.6960 | True | Very bad | |
| 2 | 0.4372 | 0.6472 | False | Bad | |
| 3 | 0.2122 | 0.6037 | False | Medium | |
| 4 | 0.1197 | 0.5667 | False | Medium | |
| 5 | 0.0860 | 0.5375 | False | Very good | Selected |

In this paper, the priority is given to the relay selection. Hence, the first cooperative node is not selected as the best jammer node. However, we observe that the fifth node provides the best jammer relevance

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 December 2019 doi:10.20944/preprints201912.0003.v1



compared to the other cooperative nodes. Thus, it is selected as by the base-station the best cooperative jammer node.

### 5.2. EXPERIMENT 2 (SMART NODE SELECTION BASED ON FUZZY LOGIC SCHEME)

In this experiment, we use a smart node selection based on the fuzzy logic strategy to select the best cooperative (relay, jammer) node. Table 7 illustrates the cooperative relay selection based on fuzzy logic strategy. The relay selection criteria are the same as the criteria used in Table 5.

**Table 7.** Cooperative relay selection based on fuzzy logic selection scheme

| Node | Relay selection criteria | | | Relevance | Selection |
|---|---|---|---|---|---|
| | $SNR_U$ | $PAF$ | $D_U$ | | |
| 1 | 0.8684 | 0.7213 | 0.7284 | Good | |
| 2 | 0.8522 | 0.6953 | 0.6429 | Good | Selected |
| 3 | 0.4855 | 0.6844 | 0.5890 | Medium | |
| 4 | 0.3010 | 0.6920 | 0.5759 | Bad | |
| 5 | 0.1717 | 0.5429 | 0.6061 | Very bad | |

Based on Table 7, we observe that the first and second cooperative nodes give the best relay relevance (good) in comparison with the other cooperative nodes. However, fuzzy logic controller selects the second node as the best cooperative relay node. This is due to the distance significance compared to the first node. Table 8 illustrates the cooperative jammer selection based on the fuzzy logic strategy.

**Table 8.** Cooperative jammer selection based on fuzzy logic selection scheme

| Node | Jammer selection criteria | | | Relevance | Selection |
|---|---|---|---|---|---|
| | $SNR_E$ | $D_E$ | $R_S$ | | |
| 1 | 0.8981 | 0.6960 | False | Bad | |
| 2 | 0.4372 | 0.6472 | True | Very bad | |
| 3 | 0.2122 | 0.6037 | False | Medium | |
| 4 | 0.1197 | 0.5667 | False | Good | |
| 5 | 0.0860 | 0.5375 | False | Very good | Selected |

Based on Table 8, we observe that the fuzzy logic controller selects the same cooperative jammer node selected by the proposed FFNN strategy.

The outputs of these experiments are summarized as follows.

- The proposed FFNN strategy selects the first cooperative helper node as the relay node.
- The fuzzy logic scheme selects the second cooperative helper node as the relay node.
- Fifth cooperative helper node is selected as the jammer node by both approaches.

Figure 8 depicts the secrecy performance in terms of secrecy capacity within a range of total transmission power from 0 dBm to 30 dBm. The secrecy performance of the cooperative NOMA system is analysed for the proposed FFNN based node selection strategy and the fuzzy logic based node selection scheme.

Based on Figure 8, we observe that the secrecy capacity for each legal user is affected by several factors namely, the total transmission power, decoding abilities i.e., SIC, and strategy used for the cooperative node selection. Firstly, the secrecy capacity performance for each legal user is enhanced as the total transmission power and the shared-jamming power increased.

Based on Figure 8, we observe that the secrecy capacity of the strong user ($\zeta_{u_1}$) is better than the secrecy performance of the weak user ($\zeta_{u_2}$). The reason behind this is the successive interference cancellation technique used by the strong user. This technique enables the strong user to decode the information signal aimed to be sent to the weak user node. Thus, the strong user is not affected by the signal interference.

 doi:10.20944/preprints201912.0003.v1



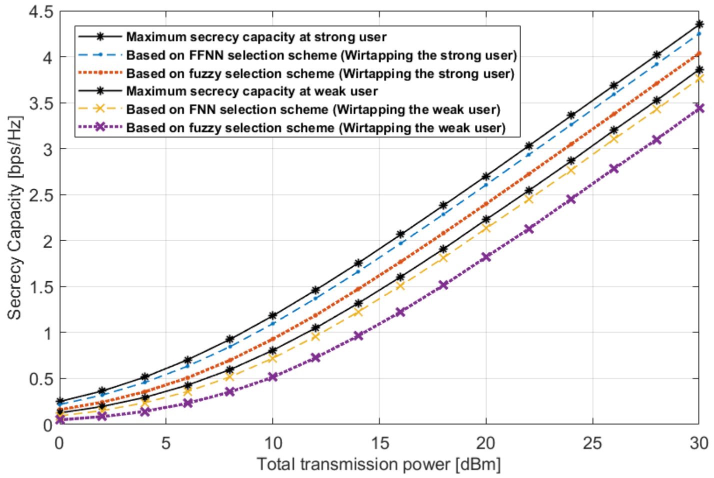



**Figure 8.** Secrecy capacity of the cooperative NOMA system assisted with smart node selection scheme

However, the weak user is affected by the strong user signal as the interference signal. Thus, the secrecy capacity performance is decreased at the weak user.

Lastly, we observe that the proposed FFNN based node selection strategy provides high secrecy capacity performance in comparison with the fuzzy logic scheme, This is due to the high estimation accuracy established by the machine learning based on the feed forward neural network (FFNN) compared with the fuzzy logic based selection scheme. The accuracy analysis of the cooperative node selection based on FFNN strategy and fuzzy logic scheme is illustrated in Figure 9.

The accuracy analysis shown in Figure 9 is carried on by comparing the maximum secrecy capacity performance of the cooperative NOMA system shown in Figure 1 (without considering the eavesdropper) with the resulted secrecy capacity for the proposed node selection based on FFNN and the fuzzy logic based node selection.

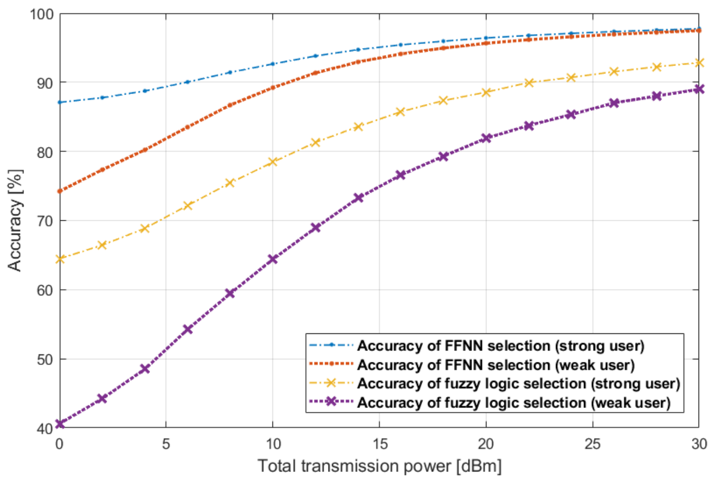



**Figure 9.** The cooperative node selection accuracy based on fuzzy logic and FFNN

Based on Figure 9, we observe that the accuracy of using the proposed strategy (FFNN based node selection) in order to approach the maximum secrecy capacity (without eavesdropping) is higher than accuracy of the fuzzy logic based scheme. In other words, the physical layer security of the cooperative NOMA system model shown in Figure 1 using the proposed strategy is high in comparison with the fuzzy logic scheme.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 December 2019 doi:10.20944/preprints201912.0003.v1



Table 9 illustrates the RMSe analysis for the smart node selection based on FFNN strategy and fuzzy logic scheme.

**Table 9.** Root mean square error ($RMSe$)

| User nodes | Cooperative node selection strategy | |
|---|---|---|
| | **Fuzzy logic** | **FFNN** |
| Wiretapping strong user | 0.2639 | 0.0846 |
| Wiretapping weak user | 0.3343 | 0.0859 |

Based on Table 9, we observe that the standard deviation (prediction errors) of the proposed strategy is lower than the fuzzy logic scheme for both legal user nodes. As summary of the comparison, the results obtained emphases that it is beneficial to use the proposed node selection based on FFNN strategy instead of the node selection based on fuzzy logic scheme.

## 6. Conclusion

In this paper, we proposed a strategy to enhance the physical layer security for a cooperative non-orthogonal multi access system. The proposed node selection strategy is integrated with a jamming null-steering beamforming technique in order to degrade the channel capacity of the eavesdropper node. Thus, enhancing the secrecy performance of the cooperative NOMA system. In conclusion, the results illustrate that the proposed cooperative node selection based on FFNN strategy outperforms the cooperative node selection based on fuzzy logic scheme due to the high estimation accuracy established by FFNN strategy.

For future work, we will consider the assumption of unknown CSI of the eavesdropper node at the base-station. Moreover, we will study the effect of relay protocols (detect-and-forward, and compress-and-forward) on the secrecy performance analysis. Furthermore, we will apply the proposed strategy on large cooperative NOMA scale where multi-eavesdropper nodes are considered.

## Appendix A Trapezoidal function

In section 3 we mapped each parameter ($SNR_U$, PAF, $D_U$, $SNR_E$, $D_E$ and $R_S$) into a linguistic fuzzy sets functions. In order to describe these functions mathematically, we used the trapezoidal function. The trapezoidal function for the first parameter is given as [18],

$$\text{trapezoidal}\left(snr_u; v_1, c_1, c_2, v_1\right) = \begin{cases} \frac{x-v_1}{c_1-v_1}, & \text{if } snr_u \in [v_1, c_1] \\ 1, & \text{if } snr_u \in [c_1, c_2] \\ \frac{b-snr_u}{v_2-c_2}, & \text{if } snr_u \in [c_2, v_2] \\ 0, & \text{otherwise} \end{cases} \tag{A1}$$

where, ($v_1$, $v_2$) are the valleys and ($c_1$, $c_2$) are the climaxes of the trapezoidal function, such that $v_1 < c_1 \leq c_2 < v_2$. The particular case when $c_1 = c_2$, the function is not a trapezoidal function anymore, in fact it is a triangular function. In equation (A.1), the trapezoidal function maps the input parameter into a value between the interval [0,1] with degree of membership called $\mu(snr_u)$. Similarly, the degree of membership of the other input parameters are $\mu(snr_u)$, $\mu(paf)$, $\mu(D_u)$, $\mu(snr_e)$, $\mu(d_e)$ and $\mu(r_s)$, $\mu_(Z_r)$, and $\mu_(Z_j)$ are the degree of membership for the (relay, jammer) relevance parameters. We distributed the trapezoidal function for the first parameter ($SNR_U$) as,

$$\begin{aligned} Low &= \text{trapezoidal}\left(snr_u; -0.4, 0, 0.2, 0.4\right), \\ Medium &= \text{trapezoidal}\left(snr_u; 0.2, 0.4, 0.6, 0.8\right), \\ High &= \text{trapezoidal}\left(snr_u; 0.7, 0.8, 1, 1.1\right). \end{aligned} \tag{A2}$$

Similarly, this relation can be rewritten for the other input and relevance parameters.

 doi:10.20944/preprints201912.0003.v1



## Appendix B Fuzzy logic block diagram for cooperative node selection

Figure 10 shows the block diagram of the fuzzy logic strategy used to select the best cooperative (relay, jammer) node.

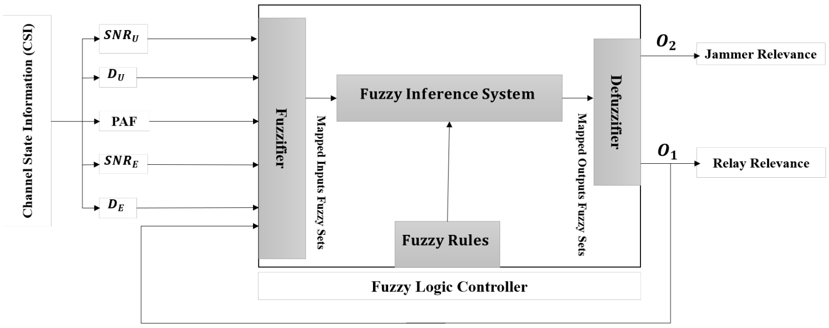



**Figure A1.** block diagram for cooperative node (relay, jammer) selection based on fuzzy logic

## Acknowledgment

The supporter of this research is the TM Research and Development centre (TMRND).

## References

1. M. A. Salem, A. B. Abd. Aziz, M. Y. Bin Alias and A. A. Abdul Rahman, "Secrecy Performance on Half-Duplex Two-Way Multi-Relay Transmission Technique Under Wireless Physical Layer Security," International Symposium on Information Theory and Its Applications (ISITA), Singapore, 2018, pp. 668-672.
2. C. E. Shannon, "Communication Theory of Secrecy Systems," in The Bell System Technical Journal, vol. 28, no. 4, pp. 656-715, Oct. 1949.
3. A. D. Wyner, "The wire-tap channel," in The Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.
4. T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura, and H. V. Poor, "Cooperative Beamforming and User Selection for Physical Layer Security in Relay Systems."
5. E. Nosrati, X. Wang, A. Khabbazibasmenj, and A. M. Akhtar, "Secrecy Enhancement Via Cooperative Relays in Multi-Hop Communication Systems," IEEE Veh. Technol. Conf., vol. 2016–July, no. iv, 2016.
6. A. Kumar and S. Sharma, "Secrecy Outage Probability with Destination Assisted Jamming in Presence of an Untrusted Relay," 2016.
7. A. Yener and S. Ulukus, "Wireless Physical-Layer Security: Lessons Learned from Information Theory," Proc. IEEE, vol. 103, no. 10, pp. 1814–1825, 2015.
8. M. A. Salem, A. B. Abd.Aziz, M. Y. B. Alias, A. A. A. Rahman and A. Mahmud, "Secrecy Analysis on Half-Duplex Two-Way Relay Transmission Using Various Transmission Channels and Jamming Strategies," 7th International Conference on Computer and Communication Engineering (ICCCE), Kuala Lumpur, 2018, pp. 432-436.
9. M. A. Salem, A. AbdAziz, M. Y. Alias and A. A. A. Rahman,"Jamming Power Estimation Technique under Wireless Physical Layer Security in Presence of an Eavesdropper", accepted by the 7th International Conference on Smart Computing Communications, 2019, Malaysia.
10. Y. Zou, X. Wang and W. Shen, "Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks," in IEEE Transactions on Communications, vol. 61, no. 12, pp. 5103-5113, December 2013.
11. M. Zhang and Y. Liu, "Energy Harvesting for Physical-Layer Security in OFDMA Networks," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 1, pp. 154-162, Jan. 2016.
12. Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan and V. K. Bhargava, "A Survey on Non-Orthogonal Multiple Access for 5G Networks: Research Challenges and Future Trends," in IEEE Journal on Selected Areas in Communications, vol. 35, no. 10, pp. 2181-2195, Oct. 2017.
13. J. Chen, L. Yang and M. Alouini, "Physical Layer Security for Cooperative NOMA Systems," in IEEE Transactions on Vehicular Technology, vol. 67, no. 5, pp. 4645-4649, May 2018.

 doi:10.20944/preprints201912.0003.v1



14. B. He, A. Liu, N. Yang and V. K. N. Lau, "On the Design of Secure Non-Orthogonal Multiple Access Systems," in IEEE Journal on Selected Areas in Communications, vol. 35, no. 10, pp. 2196-2206, Oct. 2017.
15. Y. Liu, Z. Qin, M. Elkashlan, Y. Gao and L. Hanzo, "Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks," in IEEE Transactions on Wireless Communications, vol. 16, no. 3, pp. 1656-1672, March 2017.
16. K. Sasaki, X. Liao and X. Jiang, "Cooperative Jamming in a Two-Hop Relay Wireless Network with Buffer-Aided Relays," 2017 Fifth International Symposium on Computing and Networking (CANDAR), Aomori, 2017, pp. 565-569.
17. G. Brante, G. de Santi Peron, R. D. Souza and T. Abrão, "Distributed Fuzzy Logic-Based Relay Selection Algorithm for Cooperative Wireless Sensor Networks," in IEEE Sensors Journal, vol. 13, no. 11, pp. 4375-4386, Nov. 2013.
18. B. Razeghi, M. Hatamian, A. Naghizadeh, S. Sabeti and G. A. Hodtani, "A Novel Relay Selection Scheme For Multi-User Cooperation Communications Using Fuzzy Logic," 2015 IEEE 12th International Conference on Networking, Sensing and Control, Taipei, 2015, pp. 241-246.
19. N. Taj, M. H. Zafar, S. A. Waqas, H. Rehman, M. O. Alassafi and I. Khan, "Smart Relay Selection Scheme Based on Fuzzy Logic with Optimal Power Allocation and Adaptive Data Rate Assignment" International Journal of Communication Networks and Information Security (IJCNIS), vol. 11, no. 1, pp. 239-247, April 2019.
20. J. Ahmad, H. Larijani, R. Emmanuel, M. Mannion and A. Qureshi, "Secure Occupancy Monitoring System for IoT Using Lightweight Intertwining Logistic Map," 2018 10th Computer Science and Electronic Engineering (CEEC), Colchester, United Kingdom, 2018, pp. 208-213.
21. L. Lei, T. X. Vu, L. You, S. Fowler and D. Yuan, "Efficient Minimum-Energy Scheduling with Machine-Learning Based Predictions for Multiuser MISO Systems," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, 2018, pp. 1-6.
22. Y. Sun, M. Peng, Y. Zhou, Y. Huang and S. Mao, "Application of Machine Learning in Wireless Networks: Key Techniques and Open Issues," in IEEE Communications Surveys and Tutorials.
23. T. T. Nguyen, J. H. Lee, M. T. Nguyen, Y. H. Kim, "Machine Learning-Based Relay Selection for Secure Transmission in Multi-Hop DF Relay Networks" Multidisciplinary Digital Publishing Institute (MDPI) on Electronics, vol. 11, no. 1, pp. 239-247, August 2019.
24. D. He, C. Liu, T. Q. S. Quek and H. Wang, "Transmit Antenna Selection in MIMO Wiretap Channels: A Machine Learning Approach," in IEEE Wireless Communications Letters, vol. 7, no. 4, pp. 634-637, Aug. 2018.
25. C. Wen, S. Jin, K. Wong, J. Chen and P. Ting, "Channel Estimation for Massive MIMO Using Gaussian-Mixture Bayesian Learning," in IEEE Transactions on Wireless Communications, vol. 14, no. 3, pp. 1356-1368, March 2015.
26. R. Amiri, H. Mehrpouyan, L. Fridman, R. K. Mallik, A. Nallanathan and D. Matolak, "A Machine Learning Approach for Power Allocation in HetNets Considering QoS," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, 2018, pp. 1-7.
27. J. Joung, "Machine Learning-Based Antenna Selection in Wireless Communications," in IEEE Communications Letters, vol. 20, no. 11, pp. 2241-2244, Nov. 2016.
28. Y. Zhang, H. Wang, Q. Yang and Z. Ding, "Secrecy Sum Rate Maximization in Non-orthogonal Multiple Access," in IEEE Communications Letters, vol. 20, no. 5, pp. 930-933, May 2016.
29. H. Deng, H. Wang, W. Guo and W. Wang, "Secrecy Transmission With a Helper: To Relay or to Jam," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 293-307, Feb. 2015.
30. T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura and H. V. Poor, "Cooperative Beamforming and User Selection for Improving the Security of Relay-Aided Systems," in IEEE Transactions on Communications, vol. 63, no. 12, pp. 5039-5051, Dec. 2015.
31. Z. Mobini, M. Mohammadi and C. Tellambura, "Wireless-Powered Full-Duplex Relay and Friendly Jamming for Secure Cooperative Communications," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 621-634, March 2019.
32. Y. Alsaba, C. Y. Leow and S. K. Abdul Rahim, "A Game-Theoretical Modelling Approach for Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access System," in IEEE Access, vol. 7, pp. 5896-5904, 2019.
33. J. Chen, L. Yang and M. Alouini, "Physical Layer Security for Cooperative NOMA Systems," in IEEE Transactions on Vehicular Technology, vol. 67, no. 5, pp. 4645-4649, May 2018.
34. G. Chen and T. T. Pham, Introduction to Fuzzy Sets, Fuzzy Logic, and Fuzzy Control Systems. CRC press, 2001.