SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I12P106

Volume 11 Issue 12, 56-70, December 2024

Original Article

Power Optimization Algorithms for Secure Communication via Cooperative Jamming Schemes: A Comparative Study

Shemi Panayappilly Mohammed[1], M. V. Rajesh[2], Vishnu Vasudev[3]

[1]*Department of Electronics, MES College Marampally, Aluva, Kerala, India.*
[2]*Department of Electronics Engineering, College of Engineering, Poonjar, Kerala, India.*
[3]*Department of Electronics Engineering, College of Engineering, Chengannur, Kerala, India.*

[1]*Corresponding Author : shemipm@mesmarampally.org*

Received: 11 October 2024 Revised: 15 November 2024 Accepted: 06 December 2024 Published: 30 December 2024

Abstract *- The ultimate objective of cooperative communication is to secure data transmitted from source to destination against eavesdropper attacks. The paper compares different power optimization algorithms for cooperative jamming schemes to improve the secrecy performance of a four-node Amplify and Forward (AF) relay network. The main focus of the work is on the investigation of Optimal Power Allocation (OPA) for maximizing the secrecy rate subject to a total power constraint using two cooperative jamming schemes, Source and Relay Based Jamming (SRBJ) and Source Based Jamming (SBJ). The secrecy performance of SBJ is evaluated for trusted and untrusted relaying scenarios. In the untrusted case, the situation in which an external eavesdropper and untrusted relay exist simultaneously is analyzed. The iterative algorithms such as the Nelder-Mead technique (N-M), the Broyden - Fletcher – Goldfarb - Shanno (BFGS) algorithm and the Conjugate-Gradient (CG) methods are used for power optimization and, consequently, for secrecy rate maximization. Both symmetric and asymmetric relay positions are subjected to the secrecy analysis. A comparison is conducted using the equal power Allocation (EPA) approach and the Exhaustive Search (ES) algorithm. The paper also studies the complexity of different algorithms and jamming methods based on the average number of iterations required for system convergence. It was found that the iterative algorithms provide better secrecy than the conventional methods. Experimental results reveal a trade-off between the iterative algorithms' convergence and complexity. The gradient-based BFGS and CG algorithms are less complex than the gradient-free N-M method. When assessing all jamming schemes, the N-M method is a good choice for convergence, whereas the BFGS is the best choice for lesser complexity.*

Keywords *- Broyden – Fletcher - Goldfarb - Shanno method, Conjugate - Gradient method, Cooperative jamming, Nelder Mead method, Secrecy rate.*

1. Introduction

Security has always played a critical role in the design of wireless cooperative communication systems. This study aims to bring a unique perspective on how an apt power optimization algorithm for cooperative jamming is selected for secrecy enhancement in AF relay networks. Physical Layer Security (PLS) has emerged as a cutting-edge method to dramatically enhance and supplement wireless networks' security. PLS can be used in conjunction with cryptography-based algorithms. It uses physical layer characteristics like fading or noise to establish secrecy for secure communication [1]. Two common threats to the information security of wireless networks are jamming and eavesdropping. However, a secure communication channel between the legitimate transmitter and the receiver can be established through cooperative jamming. In cooperative communication, relay nodes can use PLS to support secure transmission from a source to a destination in the presence of eavesdroppers. Unlike the non-cooperative scenario, many studies have shown that cooperation between legitimate nodes can significantly enhance their secrecy performance.

PLS provides cooperative diversity solutions, including Cooperative Relaying (CR) and Cooperative Jamming (CJ) systems, to protect the confidentiality of data being transferred. CR is a protocol where intermediate nodes called relays assist in transmitting information between the source and destination. In CJ, the nodes send jamming signals as artificial noise to degrade the eavesdropper. While CR protocol increases the main channel capacity, CJ reduces the capacity of the eavesdropper channel. In both cases, the cooperative network's confidentiality is strengthened. In

cooperative relaying, relays need system resources and power, limiting the overall energy efficiency of the CR scheme. Relay Selection (RS) approaches can overcome this energy efficiency problem [2], [3]. Node selection has been used in multi-node wireless networks to improve transmission reliability and has tremendous potential for improving wireless security [4]. Although RS increases resource efficiency, imperfect channel conditions may prevent it from always ensuring perfect secrecy. Cooperative Jamming is an alternative method to enhance PLS in wireless systems and a solution to the RS problem [5]. Thus, relay nodes can be used for relaying and jamming [6], [7]. Depending on whether jamming signals are provided by the source, destination, relay, or external jammer, CJ can be either Source Based Jamming (SBJ), Destination Based Jamming (DBJ) or friendly jammer-based jamming. In [8], a friendly interferer allocates jamming power to eavesdropping channels to increase secrecy. Sometimes, two nodes can transmit jamming signals, hence called hybrid jamming. Because the destination can cancel self-interference using its past knowledge of the jamming signal, the DBJ method, among the many CJ approaches, is the easiest to implement. However, the main drawback of the DBJ method is that the source-destination direct link cannot be considered in the case of half-duplex systems [9], [10]. Hence, the flexibility of cooperation cannot be utilised entirely without a direct link.

In the CJ design, one must pay attention to secure performance and energy efficiency for the following three reasons: wireless devices are often small, wireless portable electronics that demand frequent battery recharges. Furthermore, in some deployments, batteries may present significant safety risks. Finally, disposing of billions of used batteries in landfills is not environmentally friendly [11]. The jamming technique and the jamming signal power significantly impact the success of CJ schemes. The jamming signal power allocated should be high enough to reduce the strength of the signal at the eavesdropper. However, the signal quality at the destination may suffer if the jamming signal is subjected to excessive power. Hence, to maximize the secrecy rate, Optimal Power Allocation (OPA) is necessary for the jamming signals [12]. A survey of various optimization techniques used in wireless PLS in terms of performance parameters, PLS designs, etc., is carried out in [13]. Resource allocation, frequently used in traditional communications without taking secrecy into account, is an efficient method for increasing PLS. The primary problem of secure resource allocation is to make the best use of the limited network resources, such as bandwidth and energy, and to meet the requirements of some performance parameters, such as outage probability, secrecy rate, power consumption and secure energy efficiency. A relay power allocation scheme that maximizes the overall secrecy rate of the single-relay system is studied in [14]. The paper [15] classifies the cooperative communication system based on the number of relay nodes, transmission mode, and diversity gain. It also discusses the technologies of cooperative systems that include relay selection and power allocation. The network model, architecture and resource allocation algorithms of the 5G cooperative communication system are also discussed in the paper.

Most existing studies focus on the conventional derivative method for power optimization. In [16], the gradient-free Nelder-Mead algorithm (N-M) is used for power optimization in a hybrid SRBJ scheme in multiple AF relay networks. In the three-node scenario [17], where SBJ is used, the derivative method is used for power optimization. SRBJ uses two independent jamming signals to degrade the eavesdropper, whereas SBJ uses a single jamming signal, which makes SBJ less complex than SRBJ [18]. Inspired by these observations, this paper performs a comparative study of different power optimization algorithms among different jamming methods. The function that maximizes the achievable secrecy rate subject to a total power constraint is examined. The OPA based on the gradient-free N-M method [19] is compared with gradient-based methods, namely the Broyden–Fletcher–Goldfarb– Shanno (BFGS) algorithm [20] and the Conjugate-Gradient (CG) method [21]. Their performance is compared with the Equal Power Allocation (EPA) approach and the Exhaustive Search algorithm (ES). The work aims to find the optimal optimization strategy for solving the secrecy equations in terms of convergence and the number of iterations required to solve them. The secrecy performance and complexity of the OPA-based algorithms and jamming techniques are investigated using MATLAB and R programming simulations.

The major contributions of the work are summed up as follows:

The performance comparison of three iterative power optimization algorithms, the Nelder-Mead method, Broyden–Fletcher–Goldfarb–Shanno algorithm and Conjugate-Gradient method for secrecy enhancement in a two-hop four-node AF relay network, is formulated. The power allocation approach employed in the work optimally determines the power of the source and relay and the power of the information and jamming signals, considering the total power budget. Two cooperative jamming schemes — Source and Relay-Based Jamming (SRBJ) with a trusted relaying scheme and Source Based Jamming (SBJ) with both trusted and untrusted relaying schemes — are used for secrecy enhancement. The schemes without power allocation, the EPA approach, and a three/two-dimensional exhaustive search algorithm are used as the conventional schemes for comparison. Additionally, a complexity analysis is carried out for all the optimization techniques and jamming schemes by examining the average number of iterations taken to produce an optimal solution. Thus, the selection of an algorithm is validated by its theoretical efficiency and fast convergence towards an optimal output. The paper concludes by finding the best suited optimization method in terms of convergence and complexity.

The paper is organized as follows. The proposed method with the theoretical background is explained in Section 2. The different power optimization methods are presented in Section 3. The performance analysis and the simulation results are presented in 4 and 5, respectively. Finally, the conclusion and future directions are given in Section 6.

2. Proposed Method

The network model used, the cooperative jamming schemes employed and the methodology, including the flow diagram, are explained in this section.

2.1. Network Description

A source (S), a destination (D), a trusted/untrusted relay (R) running in half-duplex mode, and a passive eavesdropper (E) make up the four-node AF relay network shown in Fig 1. The eavesdropper wiretaps the channels during both transmission phases. A direct link between the source and the destination is utilized to fully exploit the benefits of cooperation. Each of the four nodes is equipped with an omnidirectional antenna. All Channel State Information (CSI) is assumed to be available despite the channel experiencing Rayleigh flat fading.

2.2. Transmission Schemes

The two jamming schemes employed to degrade the eavesdropper are the source-and-relay-based jamming scheme (SRBJ) and the source-based jamming scheme (SBJ). In SRBJ, two independent jamming signals, one at the source and another at the relay, are used along with the information, whereas in SBJ, a single jamming signal is used at the source. This is done under the presumption that a legitimate receiver has prior knowledge of the jamming signals, which can be practically implemented with minimal overhead [12]. This assumption is made by taking advantage of the channel reciprocity between the source and the legitimate destination [17]. The jamming signals can be totally eliminated from the signal at the legitimate receivers since the channels are assumed to be quasi-static and the CSI is available.

The two phases of transmission are the broadcast and the relaying phases. During the broadcast phase, the source broadcasts the information with a jamming signal, which reaches the relay, eavesdropper and destination. Depending on the transmission scheme, the relay amplifies and broadcasts the signal received, reaching the eavesdropper and destination.

While in SBJ, the relay amplifies the received signal and transmits as such during the relaying phase, in SRBJ, the trusted relay eliminates the jamming signal and adds another jamming signal for transmission.

During the first phase, the SNRs at the destination D and eavesdropper E are the same for both transmission schemes.

$$\gamma_D{}^{(1)} = a a_s \gamma_{SD} \tag{1}$$

$$\gamma_E{}^{(1)} = \frac{a a_s \gamma_{SE}}{1+a(1-a_s)\gamma_{SE}} \tag{2}$$

Where a, a_s such that $0 < a, a_s \leq 1$, are the power allocation factors, one between S and R and the other between the information signal and jamming signal at the source. The received SNR, γ_{ij} of any arbitrary *i-j* link is mathematically expressed as

$$\gamma_{ij} = P\frac{|h_{ij}|^2}{\sigma_j{}^2} \tag{3}$$

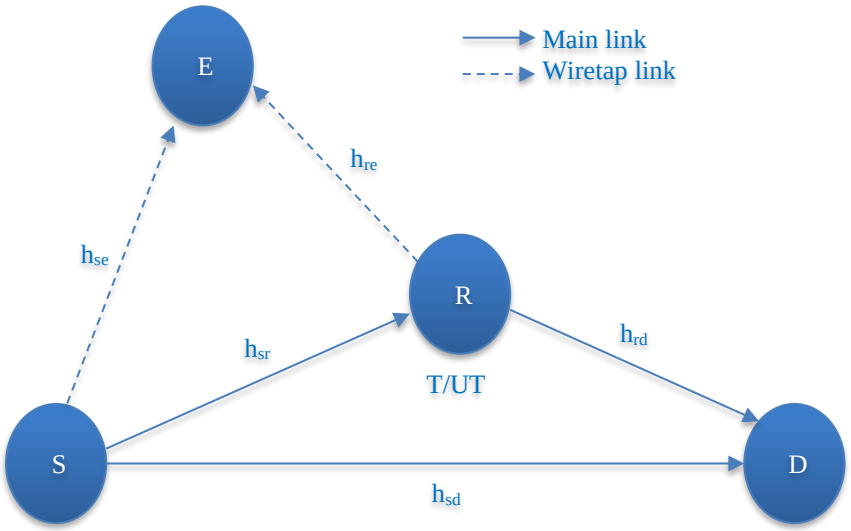

Fig. 1 Network model with channel coefficients

The noise variance at node j is σ_j^2, the channel coefficient between the nodes i and j is h_{ij}, and P is the total transmit power. Rayleigh's fading channel with a path loss is considered. Hence, h_{ij} = CN (0, $d_{i,j}^{-L}$) where $d_{i,j}$ is the distance between the nodes and L is the path-loss coefficient. The power allocation used in the work ideally determines the power of the source and the relay, and also the power of the information and jamming signals, taking into account the total power budget. The power allocation in the SRBJ and SBJ schemes are illustrated in Figs. 2 and 3, respectively.

The work thus aims at obtaining better secrecy for secure data transmissions by allocating maximum power to the information signal and minimum power to the jamming signal with minimal complexity possible.

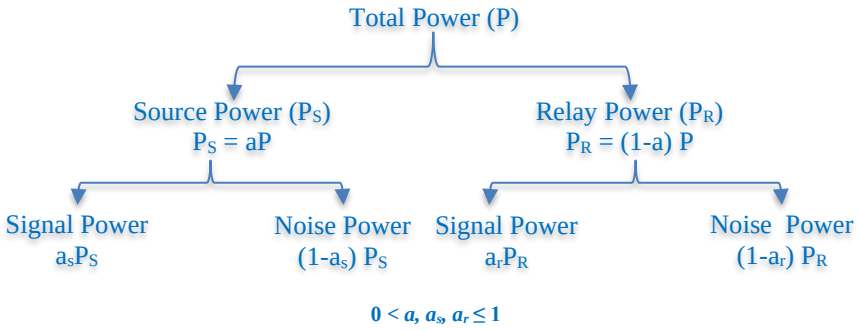

Fig. 2 Power allocation in SRBJ

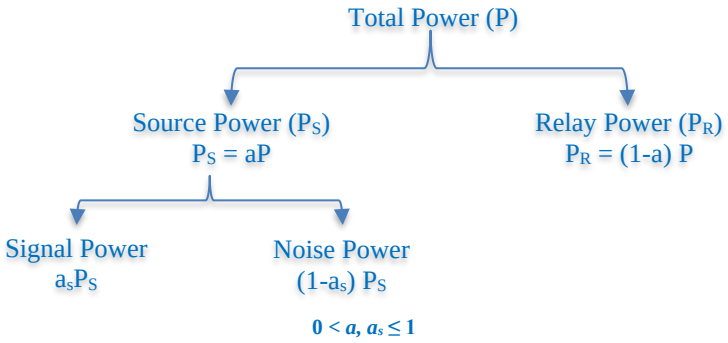

Fig. 3 Power allocation in SBJ

2.2.1. Analysis of the SRBJ Scheme

The SNR at the relay after jamming signal cancellation is

$$\gamma_{R_{SRBJ}} = aa_s\gamma_{SR} \quad (4)$$

During the relaying phase, the relay transmits the scaled version of the received signal with another jamming signal by keeping the power constraint P. As a result, the SNR at the destination D and eavesdropper E are,

$$\gamma_{D_{SRBJ}}^{(2)} = \frac{a(1-a)a_s a_r\gamma_{SR}\gamma_{RD}}{1+aa_s\gamma_{SR}+(1-a)a_r\gamma_{RD}} \quad (5)$$

$$\gamma_{E_{SRBJ}}^{(2)} = \frac{a(1-a)a_s a_r\gamma_{SR}\gamma_{RE}}{1+aa_s\gamma_{SR}+(1-a)\gamma_{RE}+a(1-a)a_s(1-a_r)\gamma_{SR}\gamma_{RE}} \quad (6)$$

where a_r, such that $0 < a_r \leq 1$; is the relay power allocation factor.

Applying maximal ratio combining (MRC), the overall SNR at D and E is given by

$$\gamma_{D_{SRBJ}} = aa_s\gamma_{SD}\frac{a(1-a)a_s a_r\gamma_{SR}\gamma_{RD}}{1+aa_s\gamma_{SR}+(1-a)a_r\gamma_{RD}} \quad (7)$$

$$\gamma_{E_{SRBJ}} = \frac{aa_s\gamma_{SE}}{1+a(1-a_s)\gamma_{SE}} + \frac{a(1-a)a_s a_r\gamma_{SR}\gamma_{RE}}{1+aa_s\gamma_{SR}+(1-a)\gamma_{RE}+a(1-a)a_s(1-a_r)\gamma_{SR}\gamma_{RE}} \quad (8)$$

2.2.2. Analysis of the SBJ Scheme

The SNR at the relay R after the first transmission phase is

$$\gamma_{R_{SBJ}} = \frac{aa_s\gamma_{SR}}{1+a(1-a_s)\gamma_{SR}} \quad (9)$$

Following the second transmission phase, the SNR at the destination D and eavesdropper E is

$$\gamma_{D_{SBJ}}^{(2)} = \frac{a(1-a)a_s\gamma_{SR}\gamma_{RD}}{1+a\gamma_{SR}+(1-a)\gamma_{RD}} \quad (10)$$

$$\gamma_{E_{SBJ}}^{(2)} = \frac{a(1-a)a_s\gamma_{SR}\gamma_{RE}}{1+a(1-a)(1-a_s)\gamma_{SR}\gamma_{RE}+a\gamma_{SR}+(1-a)\gamma_{RE}} \quad (11)$$

For the trusted and untrusted SBJ schemes, the overall SNR at destination D is the same as given by

$$\gamma_{D_{SBJ}} = aa_s\gamma_{SD} + \frac{a(1-a)a_s\gamma_{SR}\gamma_{RD}}{1+a\gamma_{SR}+(1-a)\gamma_{RD}} \quad (12)$$

The overall signal-to-interference noise ratio (SINR) at the eavesdropper E differs for trusted/ untrusted cases. The SINR at E for the trusted case applying MRC, assuming equal noise variances, is

$$\gamma_{E_{SBJ-T}} = \frac{aa_s\gamma_{SE}}{1+a(1-a_s)\gamma_{SE}} + \frac{a(1-a)a_s\gamma_{SR}\gamma_{RE}}{1+a(1-a)(1-a_s)\gamma_{SR}\gamma_{RE}+a\gamma_{SR}+(1-a)\gamma_{RE}} \quad (13)$$

For the untrusted case, both the untrusted relay (R) and the external eavesdropper (E) are malicious nodes. Here, the signals received during the first and second phases by the relay and external eavesdropper are considered separately. The maximum leakage to R and E is the amount of information leakage represented by γ_E [22].

$$\gamma_{E_{SBJ-UT}} = max\left\{\gamma_{R_{SBJ}}, \gamma_E^{(1)}, \gamma_{E_{SBJ}}^{(2)}\right\} \quad (14)$$

2.3. Methodology

The jamming schemes and the performance parameters for the power optimization employed in the work are summarized in Table 1. The symmetric and asymmetric relay positions for the evaluation are also indicated in the table.

Table 1. Summary of the work

Methodology		
Jamming Schemes used	**Relay Positions**	**Performance Parameters**
i) SRBJSBJ-T ii) SBJ-UT iii) SBJ-UT	i) Symmetric at the centre ii)Asymmetric 1-near the source iii)Asymmetric 2- near the destination	i) Secrecy Rate – convergence ii) Average number of iterations complexity

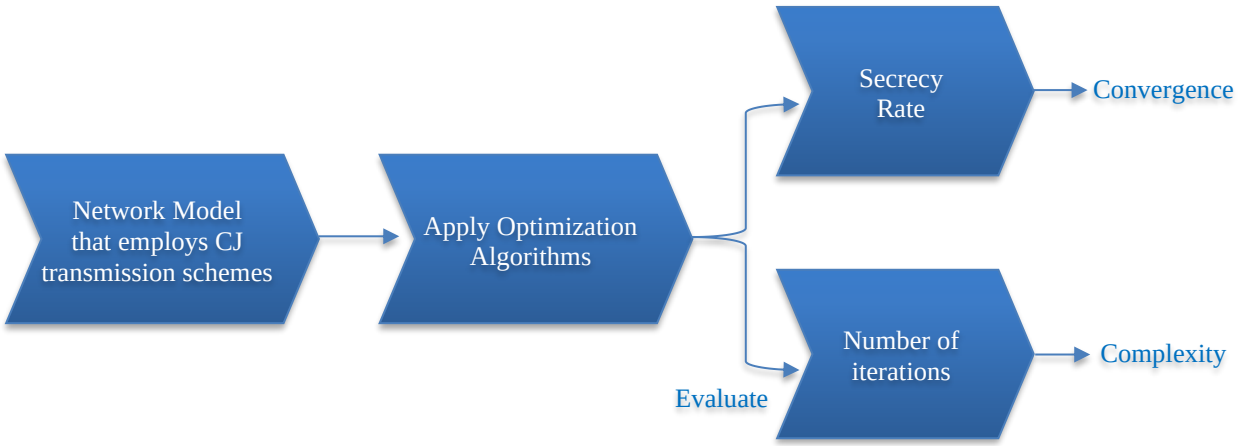

Fig. 4 Workflow diagram

Figure 4 illustrates the workflow diagram. Since a cooperating jamming scenario is used, there is a need to optimise source and relay powers as well as information and jamming signal powers. For that, it would be a great choice to apply optimization algorithms. Once the network model is defined, an optimization algorithm is applied. The secrecy performance of the network is evaluated using the performance parameter named secrecy rate. Depending upon the evaluation criteria and complexity, the system may or may not converge during optimization. The algorithms that do not cause system convergence are not suitable for optimization. The system complexity is evaluated based on the number of iterations needed for convergence. The algorithm that takes less number of iterations to converge is the best-suited one. It is experimentally found that a trade-off exists between the convergence and complexity of the algorithms.

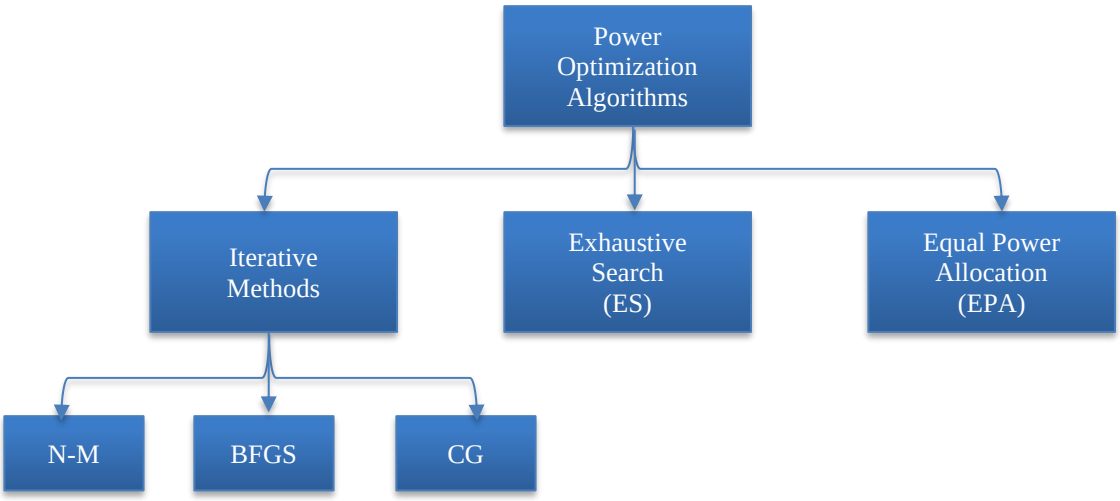

Fig. 5 Power optimization algorithms

3. Power Optimization Methods

The iterative algorithms used for power optimization are N-M, BFGS, and CG methods. The performance of these methods is compared with the conventional exhaustive search algorithm and the algorithm without power optimization – i.e., the Equal Power Allocation (EPA) strategy. The different optimization algorithms employed in this work are given in Figure 5. The selection of an algorithm is validated by its theoretical efficiency and its fast convergence in attaining an ideal outcome.

3.1. Nelder-Mead (N-M) Method

The N-M method formulated by Nelder and Mead is a gradient-free optimization method widely used for unconstrained optimization of non-linear functions [19]. This approach minimizes a function with '*n*' variables using the function values at a generic simplex's (n+1) vertices. Depending on the function's value, the simplex is modified by any of the four operations: reflection, expansion, contraction, and shrinking. Since the worst vertex with the highest function value is replaced with a new vertex, a new simplex is produced after each iteration, and the search is continued. Finally, the simplex with optimal value is found [23]. The N-M algorithm's iterative process is described in [16].

For a given $x \in R_n$, if $h(n)$ denotes the number of operations required to compute the function $f(x)$, then the computational complexity of the N-M method is given as [24]
i) Max {O (n log n), O (h (n))}, if no shrinking step is used;
ii) O (n h (n)), otherwise.

3.2. Broyden – Fletcher – Goldfarb – Shanno (BFGS) Algorithm

The BFGS algorithm is a second-order optimization algorithm intended to solve unconstrained nonlinear optimization problems [20]. This is referred to as the Quasi-Newton method, an extension of Newton's optimisation method. Newton's method involves the calculation of the inverse of the Hessian matrix, which is computationally expensive. Quasi-Newton algorithms differ in how the inverse Hessian approximation is done. Instead of recalculating the inverse Hessian after each iteration, the BFGS algorithm uses gradient evaluations and a generalized secant approach to estimate it [25]. The computational complexity of BFGS is only O (n^2), compared to O (n^3) in Newton's method.

3.3. Conjugate-Gradient (CG) Method

The CG method developed by Magnus Hestenes and Eduard Stiefel [21] is an iterative approach used for both linear and non-linear system optimization. Its performance is between the steepest descent and the Newton methods. Adding a positive multiple of the direction utilized in the previous stage distorts the direction of the steepest descent method. In [26], a comparison of the steepest descent and the CG methods for solving systems of linear equations is explained. Usually, this strategy is applied to solve very large systems that are too complex to solve directly. Restarting and preconditioning are crucial for CG technique improvement [27]. The CG approach is more fragile than the BFGS method, but it works better on much bigger optimization problems because it does not store a matrix.

The time complexity of the CG method is O ($m\sqrt{K}$) compared to O (n^3) in Newton's method. The coefficient matrix A's dimension, condition number, and the number of non-zero terms are denoted by the letters m, K, and n, respectively. Knowing A-1 is essential to calculate the condition number; it is necessary to estimate through alternate means. Yet, it has the result of decreasing the value of K by preconditioning a matrix. K should ideally be as near to 1 as possible so that it does not affect the time complexity of the CG method. Most numerical analysts concur that a preconditioner should always be used for the CG method.

N-M uses the simplex algorithm and is robust in many applications. As the numerical computations of derivatives can be trusted, other algorithms that use the first and/or second derivatives may be preferred for their better performance.

N-M generally addresses parameter estimation and related statistical issues when the function values are subjected to noise. BFGS will converge in fewer steps than CG as a quasi-Newton approach and need minor algorithmic adjustments. Even with non-smooth optimizations, BFGS has proven to perform strongly.

3.4 Exhaustive Search (ES) Method

ES is the algorithm that tries every possible solution of an objective function where the objective function is evaluated at a predetermined number of equally spaced points δ. After evaluation, the maximum function value is obtained. The power allocation factors - a, a_s, and a_r that provide the maximum function value are taken as the optimal values. Although conceptually simple and frequently effective, ES is viewed as an inappropriate method of problem-solving [28].

3.4. Equal Power Allocation (EPA) Method

The method that allocates equal power to the source and relay is the EPA method. Here, power at the source and at the relay is 0.5 times the total system power P, i.e., $P_s = P_r = 0.5P$.

4. Secrecy Rate

The secrecy rate (R_S) is the parameter used for performance study, and the system that gives a higher secrecy rate with less power allocation to jamming signals is preferred.

The secrecy rate is defined as the transmission rate at which an untrusted intermediate node cannot extract source information. The instantaneous secrecy rate is given by [29].

$$R_S = \left(R_D - R_E\right)^+ = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right)\right]^+ \tag{15}$$

Where $(x)^+ = \max\{0, x\}$; R_D and R_E represent the destination and untrusted node transmission rates, respectively. If proper power allocation can guarantee a positive secrecy rate [9], then it becomes

$$R_S = R_D - R_E = \frac{1}{2}\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right) \tag{16}$$

Substituting the values, the secrecy rate of different schemes are

$$R_{s_{SRBJ}}(a, a_s, a_r) = \left[\frac{1}{2} log_2\left(\frac{1+aa_s\gamma_{SD}+\frac{a(1-a)a_s a_r\gamma_{SR}\gamma_{RD}}{1+aa_s\gamma_{SR}+(1-a)a_r\gamma_{RD}}}{1+\frac{aa_s\gamma_{SE}}{1+a(1-a_s)\gamma_{SE}}+\frac{a(1-a)a_s a_r\gamma_{SR}\gamma_{RE}}{1+aa_s\gamma_{SR}+(1-a)\gamma_{RE}+a(1-a)a_s(1-a_r)\gamma_{SR}\gamma_{RE}}}\right)\right]^+ \tag{17a}$$

Using [17], (17 *a*) can be written as

$$\overline{R_{s_{SRBJ}}}(a, a_s, a_r) = \max_{a,a_s,a_r\in(0,1)} E\left[\frac{1}{2} log_2\left(\frac{1+aa_s\gamma_{SD}+\frac{a(1-a)a_s a_r\gamma_{SR}\gamma_{RD}}{1+aa_s\gamma_{SR}+(1-a)a_r\gamma_{RD}}}{1+\frac{aa_s\gamma_{SE}}{1+a(1-a_s)\gamma_{SE}}+\frac{a(1-a)a_s a_r\gamma_{SR}\gamma_{RE}}{1+aa_s\gamma_{SR}+(1-a)\gamma_{RE}+a(1-a)a_s(1-a_r)\gamma_{SR}\gamma_{RE}}}\right)\right] \tag{17b}$$

$$R_{s_{SBJ-T}}(a, a_s) = \left[\frac{1}{2} log_2\left(\frac{1+aa_s\gamma_{SD}+\frac{a(1-a)a_s\gamma_{SR}\gamma_{RD}}{1+a\gamma_{SR}+(1-a)\gamma_{RD}}}{1+\frac{aa_s\gamma_{SE}}{1+a(1-a_s)\gamma_{SE}}+\frac{a(1-a)a_s\gamma_{SR}\gamma_{RE}}{1+a(1-a)(1-a_s)\gamma_{SR}\gamma_{RE}+a\gamma_{SR}(1-a)\gamma_{RE}}}\right)\right]^+ \tag{18a}$$

$$\overline{R_{s_{SBJ-T}}}(a, a_s) = \max_{a,a_s\in(0,1)} E\left[\frac{1+aa_s\gamma_{SD}+\frac{a(1-a)a_s\gamma_{SR}\gamma_{RD}}{1+a\gamma_{SR}+(1-a)\gamma_{RD}}}{1+\frac{aa_s\gamma_{SE}}{1+a(1-a_s)\gamma_{SE}}+\frac{a(1-a)a_s\gamma_{SR}\gamma_{RE}}{1+a(1-a)(1-a_s)\gamma_{SR}\gamma_{RE}+a\gamma_{SR}(1-a)\gamma_{RE}}}\right] \tag{18b}$$

$$R_{s_{SBJ-UT}}(a, a_s) = \left\{\frac{1}{2} log_2 \quad \left(1 + aa_s\gamma_{sD} + \frac{a(1-a)a_s\gamma_{sR}\gamma_{RD}}{1+a\gamma_{sR}+(1-a)\gamma_{RD}}\right) - \frac{1}{2} log_2\left(1 + max\left\{\gamma_{R_{SBJ}}, {\gamma_E}^1, {\gamma_E}^2_{SBJ}\right\}\right)\right\}^+ \tag{19}$$

The different optimization methods are applied to the functions in (17b), (18b), and (19) to estimate the OPA factors a, a_s, and a_r and secrecy rate. The function is inverted to obtain the maximum value since the N-M approach finds the minimum of a function. A positive secrecy can be ensured by using multiple relay scenarios. With the EPA system, secrecy is obtained by taking 0.5 for the power allocation factors.

5. Simulation and Discussion

This section investigates the performance of three power optimization algorithms on different jamming schemes via numerical experiments and simulations. A two-dimensional system model is examined, and the source and destination locations are fixed at coordinates (0, 0) and (10, 0), respectively. The analysis is done for three relay positions.

The central relay is symmetric, whereas the other relay positions are asymmetric. For the analysis, the relay near the source and the destination are taken as asymmetric cases 1 and 2, respectively. The worst-case scenario of an eavesdropper appearing near the source node is considered. The network topology is shown in Fig 6. The total transmit power P of 30 dBm and SNR of 10dB are used. Monte-Carlo simulations with 10^5 independent trials are performed for secrecy rate maximization. The OPA that maximizes the secrecy rate is found analytically. Finally, the simulations were presented to validate the analytical results. In the study of wireless communications, the path-loss coefficient varies in the range of 2 to 4, where 2 is for free space and 4 is for relatively lossy environments [30]. The scenario considered in this work falls between these limits, so a path-loss coefficient (L) of 3 is selected. Power allocation factors of 0.5 are used for the EPA strategy. The simulation parameters used are summarised in Table 2. Tables 3, 4 and 5 present the results of SRBJ, SBJ-T, and SBJ-UT jamming schemes, respectively, in terms of power allocation factors. The powers allocated to information and jamming signals at the source and relay are tabulated based on the power allocation factors, as illustrated in Figures 2 and 3. Each table compares the iterative algorithms with the ES method and EPA strategy for symmetric and asymmetric relay positions. For the analysis, more source power is required as the distance between the source and the relay increases, and more jamming power is required in cases where the eavesdropper appears near the source. Optimization, which allocates more signal and less jamming power, is considered the best method.

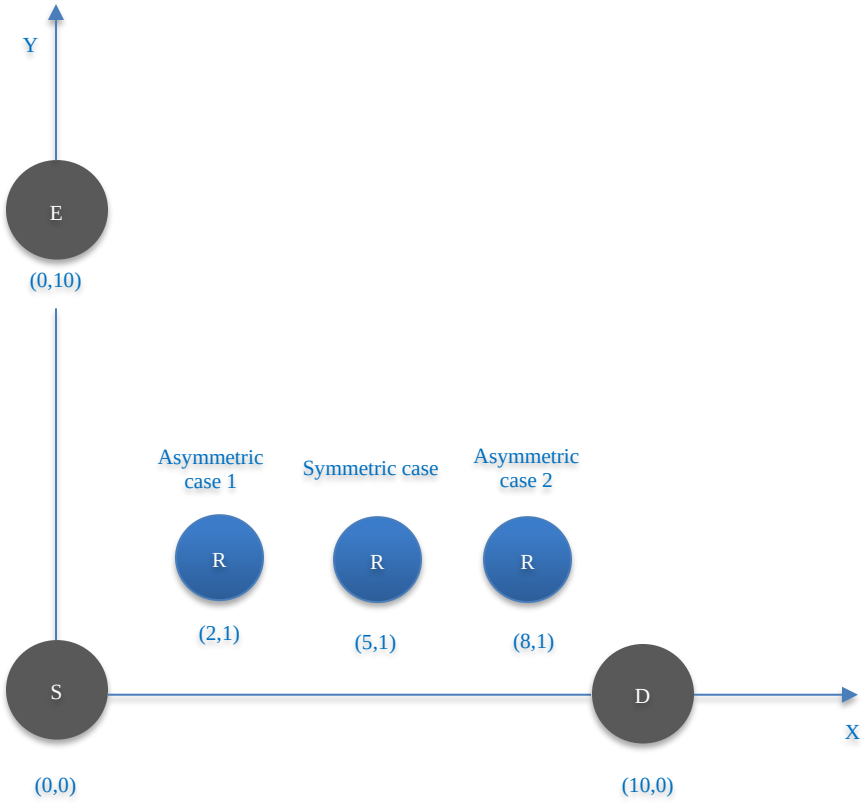

Fig. 6 Network topology

Table 2. Simulation parameters

Parameters	Specification
Total Power (P)	30 dBm
Path loss coefficient (L)	3
SNR	10 dB
Power optimization factors:	0.5 for EPA
Step size for ES algorithm	0.05

Table 3. Comparison table of SRBJ scheme

Relay Position	Optimization methods	Power allocation factors			P_S		P_R	
		a	a_s	a_r	Signal power	Noise power	Signal power	Noise power
Symmetric case	N-M	0.5740229	0.4792337	0.4848957	0.27509	0.29893	0.20656	0.21942
	BFGS	0.5739846	0.4792757	0.4849550	0.27510	0.29889	0.20660	0.21941
	CG	0.5739837	0.4792762	0.4849537	0.27510	0.29888	0.20660	0.21942
	ES (δ = 0.05)	0.55	0.5	0.5	0.275	0.275	0.225	0.225
	EPA	0.5	0.5	0.5	0.25	0.25	0.25	0.25
Asymmetric case 1	N-M	0.1401137	0.3882902	0.5001550	0.05440	0.08570	0.43010	0.42980
	BFGS	0.1400652	0.3883303	0.5001297	0.05439	0.08567	0.43008	0.42986
	CG	0.1400975	0.3883019	0.5001165	0.05436	0.08564	0.43010	0.42990
	ES (δ = 0.05)	0.15	0.4	0.5	0.06	0.09	0.425	0.425
	EPA	0.5	0.5	0.5	0.25	0.25	0.25	0.25
Asymmetric case 2	N-M	0.9849943	0.5184048	0.4864313	0.51063	0.47437	0.0073	0.0077
	BFGS	**No Convergence**						
	CG	**No Convergence**						
	ES (δ = 0.05)	0.95	0.5	0.55	0.475	0.475	0.0275	0.0225
	EPA	0.5	0.5	0.5	0.25	0.25	0.25	0.25

Table 4. Comparison table of SBJ-T scheme

Relay Position	Optimization methods	Power allocation factors		P_S		
		a	a_s	Signal power	Noise power	P_R
Symmetric case	N-M	0.5769554	0.4770439	0.27523	0.30172	0.42304
	BFGS	0.5769180	0.4770811	0.27524	0.30168	0.42308
	CG	0.5769177	0.4770811	0.27524	0.30168	0.42308
	ES (δ=0.05)	0.6	0.5	0.3	0.3	0.4
	EPA	0.5	0.5	0.25	0.25	0.5
Asymmetric case 1	N-M	0.1104253	0.4858369	0.05364	0.05678	0.88958
	BFGS	0.1104270	0.4858781	0.05366	0.05677	0.88957
	CG	**No Convergence**				
	ES (δ = 0.05)	0.1	0.5	0.05	0.05	0.9
	EPA	0.5	0.5	0.25	0.25	0.5
Asymmetric case 2	N-M	0.928745	0.5247478	1.3295		
	BFGS	**No Convergence**				
	CG	**No Convergence**				
	ES (δ = 0.05)	0.9	0.5	0.45	0.45	0.1
	EPA	0.5	0.5	0.25	0.25	0.5

The best relay position is at the centre of the network model as it has the same source-relay SNR (γ_{sr}) and relay-destination SNR (γ_{rd}) and is thus named symmetric [16]. Asymmetric case is the case where $\gamma_{sr} > > \gamma_{rd}$ or $\gamma_{sr} < < \gamma_{rd}$. In a symmetric case, the system allocates more or less the same power to source and relay; it converges after the required number of iterations, as seen in Tables 3, 4 and 5.

Since the worst case of an eavesdropper near the source is assumed, the source has to allocate more power to the jamming signal. For the SRBJ symmetric case employing the N-M method, the power allocation to information and jamming signals at the source is 0.27509W and 0.29893W, respectively. Similar is the case with other jamming schemes. For the asymmetric case, the gradient-based optimization algorithms – BFGS and CG methods- are complicated and may fail to converge. A great variation among the source and relay powers can be seen in asymmetric cases.

From the tables, it is seen that all the iterative algorithms converge in a symmetric relay position. Even though BFGS and CG methods allocate less jamming power for the symmetric case, they may not converge in asymmetric cases.

Hence, the N-M method is considered a good choice for optimization since it converges at all times, irrespective of the relay position.

Table 5. Comparison table of SBJ-UT Scheme

Relay Position	Optimization methods	Power allocation factors		P_S		P_R
		a	a_s	Signal power	Noise power	
Symmetric case	N-M	0.5430821	0.3372396	0.18315	0.35993	0.45692
	BFGS	0.5430125	0.3373360	0.18318	0.35984	0.45698
	CG	0.5430136	0.3373357	0.18318	0.35984	0.45698
	ES (δ = 0.05)	0.55	0.35	0.1925	0.3575	0.45
	EPA	0.5	0.5	0.25	0.25	0.5
Asymmetric case 1	N-M	0.2007138	0.3088237	0.06199	0.13872	0.79929
	BFGS	0.2007821	0.3088283	0.06200	0.13878	0.79922
	CG	0.2015353	0.3088287	0.06223	0.13930	0.79847
	ES (δ = 0.05)	0.2	0.3	0.06	0.14	0.8
	EPA	0.5	0.5	0.25	0.25	0.5
Asymmetric case 2	N-M	0.8941012	0.3327613	0.29752	0.59658	0.1059
	BFGS	**No Convergence**				
	CG	0.8941001	0.332768	0.29753	0.59657	0.1959
	ES (δ=0.05)	0.9	0.35	0.315	0.585	0.1
	EPA	0.5	0.5	0.25	0.25	0.5

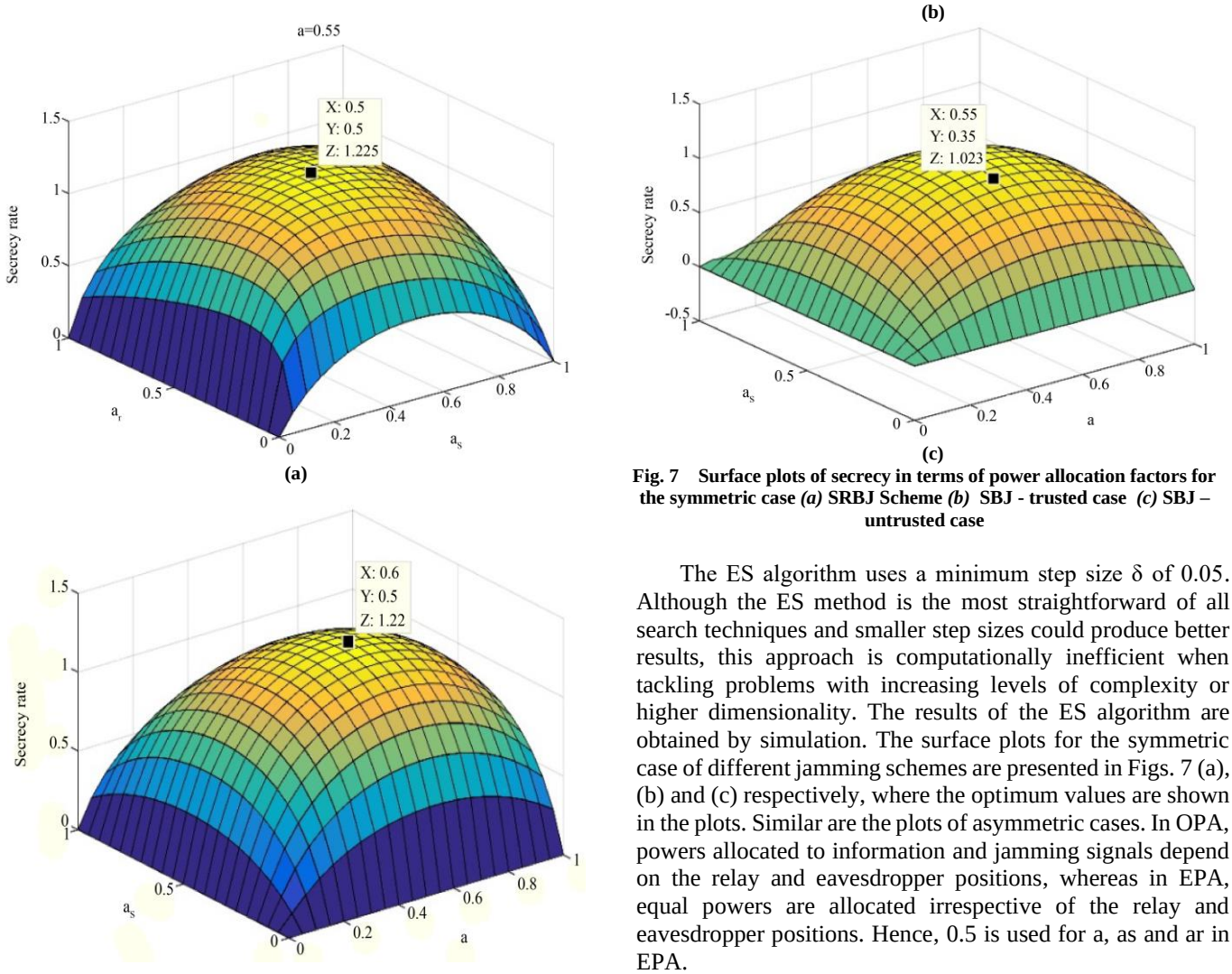

Fig. 7 Surface plots of secrecy in terms of power allocation factors for the symmetric case *(a)* SRBJ Scheme *(b)* SBJ - trusted case *(c)* SBJ – untrusted case

The ES algorithm uses a minimum step size δ of 0.05. Although the ES method is the most straightforward of all search techniques and smaller step sizes could produce better results, this approach is computationally inefficient when tackling problems with increasing levels of complexity or higher dimensionality. The results of the ES algorithm are obtained by simulation. The surface plots for the symmetric case of different jamming schemes are presented in Figs. 7 (a), (b) and (c) respectively, where the optimum values are shown in the plots. Similar are the plots of asymmetric cases. In OPA, powers allocated to information and jamming signals depend on the relay and eavesdropper positions, whereas in EPA, equal powers are allocated irrespective of the relay and eavesdropper positions. Hence, 0.5 is used for a, as and ar in EPA.

Table 6. Complexity analysis of different optimization algorithms in terms of the average number of iterations

SNR (dB)	The average number of iterations (Symmetric case)								
	SRBJ			SBJ-T			SBJ-UT		
	N-M	BFGS	CG	N-M	BFGS	CG	N-M	BFGS	CG
2	162	15	233	49	11	37	55	9	36
4	106	10	115	53	8	44	55	10	31
6	74	12	50	43	19	34	49	19	55
8	74	16	41	43	26	29	49	15	30
10	60	17	41	41	19	26	45	18	40
12	76	20	33	45	14	24	51	26	42
14	86	22	38	43	10	21	53	26	49
16	82	22	36	43	12	21	53	10	99
18	82	16	40	45	18	19	51	10	87
20	86	15	40	41	13	19	51	10	64

The complexity of the optimization algorithms can be studied from the average number of iterations needed for the function convergence. The average number of iterations at various SNR values for different optimization techniques in the symmetric case is shown in Table 6. Although the gradient-based approach appears to have a lower level of complexity, sometimes, the non-linear function may fail to converge or produce results. The gradient-free method is the alternative solution in such cases.

From the perspective of the number of iterations for system convergence, the N-M method is the most complex as it requires more iterations, and BFGS is the least complex. The complexity of the CG method falls somewhere in the middle of the other two algorithms. The increased number of iterations shows the complexity of the method. More memory and processing time are required for sophisticated algorithms. SRBJ is a more complex jamming strategy than SBJ due to the increased number of computations involved. Table 6 illustrates how the average number of iterations drops with SNR, showing less variation across all situations over 10 dB. Therefore, the minimum SNR needed for acceptable performance is set at 10 dB. Similar is the case with asymmetric relay positions. Sometimes, the system will not converge at a very low SNR for the asymmetric cases.

Table 7 compares the secrecy rate of different jamming schemes for different relay positions. The iterative algorithms produce better secrecy than conventional ES and EPA strategies. The system that does not converge is also mentioned in the table. Though SRBJ gives better secrecy performance than SBJ, it is complex. SBJ schemes, both trusted and untrusted, require only one jamming signal; hence, they are less secure and less complex than SRBJ. The untrusted scheme is always less secure than the trusted scheme. For the ES algorithm, the maximum secrecy rate is obtained by simulation. The secrecy rate for the symmetric case is shown in the surface plots of Figure 7. EPA shows fairly good performance only for the symmetric case. In asymmetric cases, the secrecy performance of the EPA is poor. From the table, it is seen that the variation of EPA with the iterative algorithm for the SRBJ case is 0.01229 bits/sec/Hz only for the symmetric case, 0.13963 bits/sec/Hz for the asymmetric case 1 and 0.37955 bits/sec/Hz for the asymmetric case 2. Similar is the case with other jamming schemes.

Table 8 presents the statistical explanation of the trade-off between the convergence and complexity of iterative algorithms subjected to symmetric and asymmetric relay positions for SNR =10dB. The table shows that all the algorithms converge for symmetric relay positions, and only the N-M method works for asymmetric relay positions. All the algorithms tried and tested do not promise 100% convergence, nor do they ensure lesser complexity. If pursued based on convergence, N-M is the better algorithm but is substantially complex. Paradoxically, if pursued for a lesser complex algorithm, BFGS presents a superior option but does not ensure 100% convergence. In principle, there is a trade-off between convergence and complexity when considering different algorithms.

Figures 8, 9, and 10 show the variation of power allocation factors regarding SNR for different jamming schemes. It is obvious that the power allocation factors - a, a_s, and a_r depends on the relay and eavesdropper position. The figures show that the N-M method exhibits more a, whereas the CG and BFGS gradient methods exhibit more a_s and a_r for all the jamming schemes. The CG and BFGS methods show more or less the same performance. Although the variation of optimization parameters is much less, they considerably change the secrecy performance.

Table 7. Comparison of the secrecy rate of different jamming schemes

Relay positions	Optimization methods	Secrecy rate (bits/s/Hz)			Inference
		SRBJ	SBJ-T	SBJ-UT	
Symmetric case	Iterative algorithms	1.22609	1.22183	1.05721	All converge
	ES	1.225	1.2204	1.023	
	EPA	1.2138	1.2122	0.9675	
Asymmetric case 1	Iterative algorithms	1.00673	0.99631	0.78319	No convergence for CG in the SBJ-T scheme
	ES	1.0024	0.9933	0.7823	
	EPA	0.8671	0.8612	0.6089	
Asymmetric case 2	Iterative algorithms	1.33795	1.3295	1.03375	No convergence for BFGS & CG in the SRBJ and SBJ-T schemes, and BFGS in the SBJ-UT scheme
	ES	1.3345	1.3214	1.0334	
	EPA	0.9584	0.9385	0.6896	

Table 8. Convergence vs. Complexity

Jamming Schemes	Optimization methods	Convergence (Yes/No)			Complexity (Average number of iterations)		
		Symmetric case	Asymmetric case 1	Asymmetric case 1	Symmetric case	Asymmetric case 1	Asymmetric case 1
SRBJ	N-M	Yes	Yes	Yes	60	56	68
	BFGS	Yes	Yes	No	17	18	---
	CG	Yes	Yes	No	41	49	---
SBJ-T	N-M	Yes	Yes	Yes	41	51	53
	BFGS	Yes	Yes	No	19	21	---
	CG	Yes	No	No	26	---	---
SBJ-UT	N-M	Yes	Yes	Yes	45	47	57
	BFGS	Yes	Yes	No	18	10	---
	CG	Yes	Yes	Yes	40	59	102

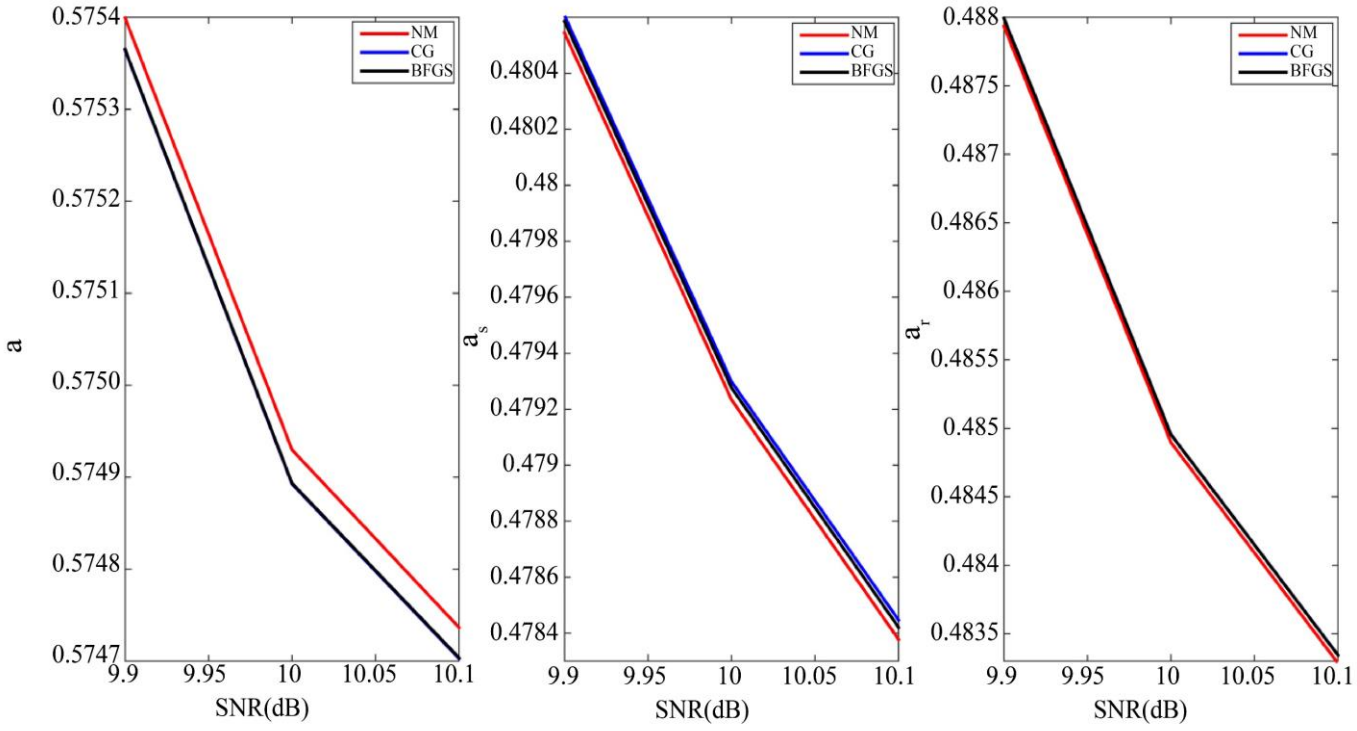

Fig. 8 Variation of power allocation factors in terms of SNR for the SRBJ scheme.

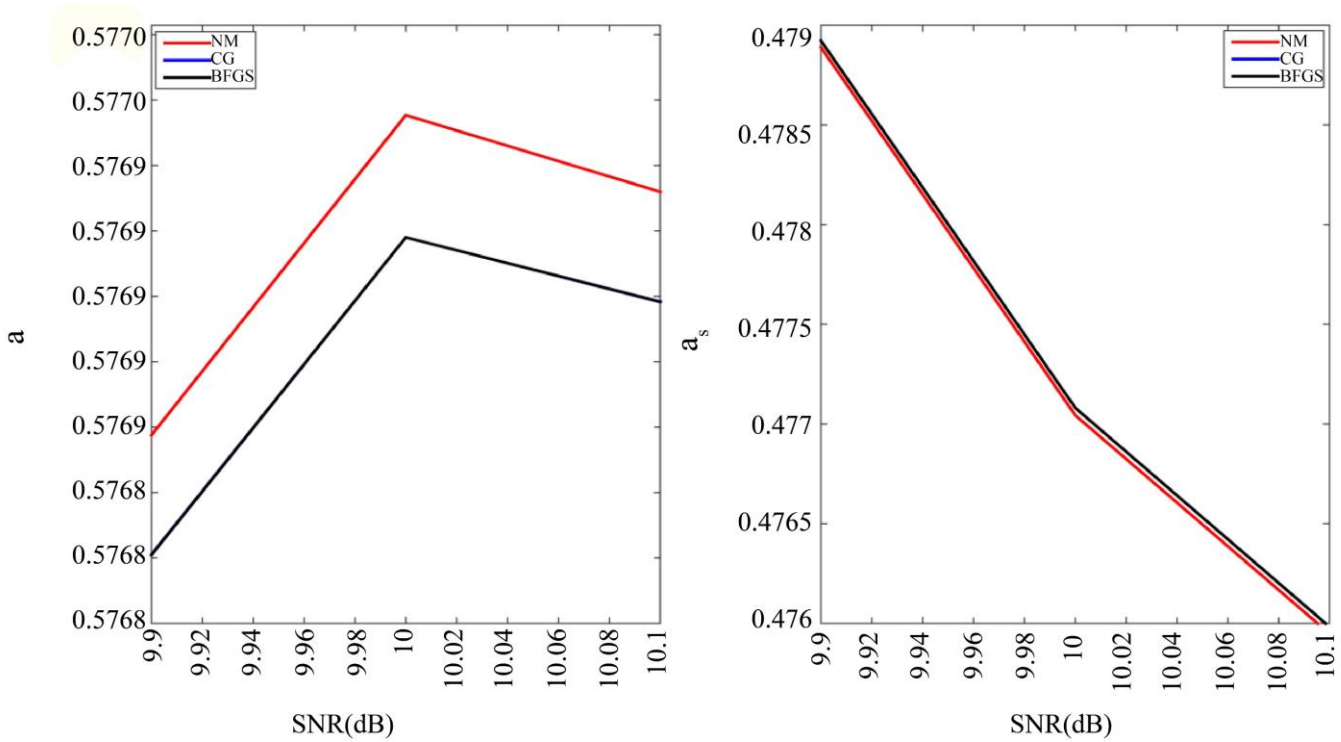

Fig. 9 Variation of power allocation factors in terms of SNR for the SBJ-T scheme

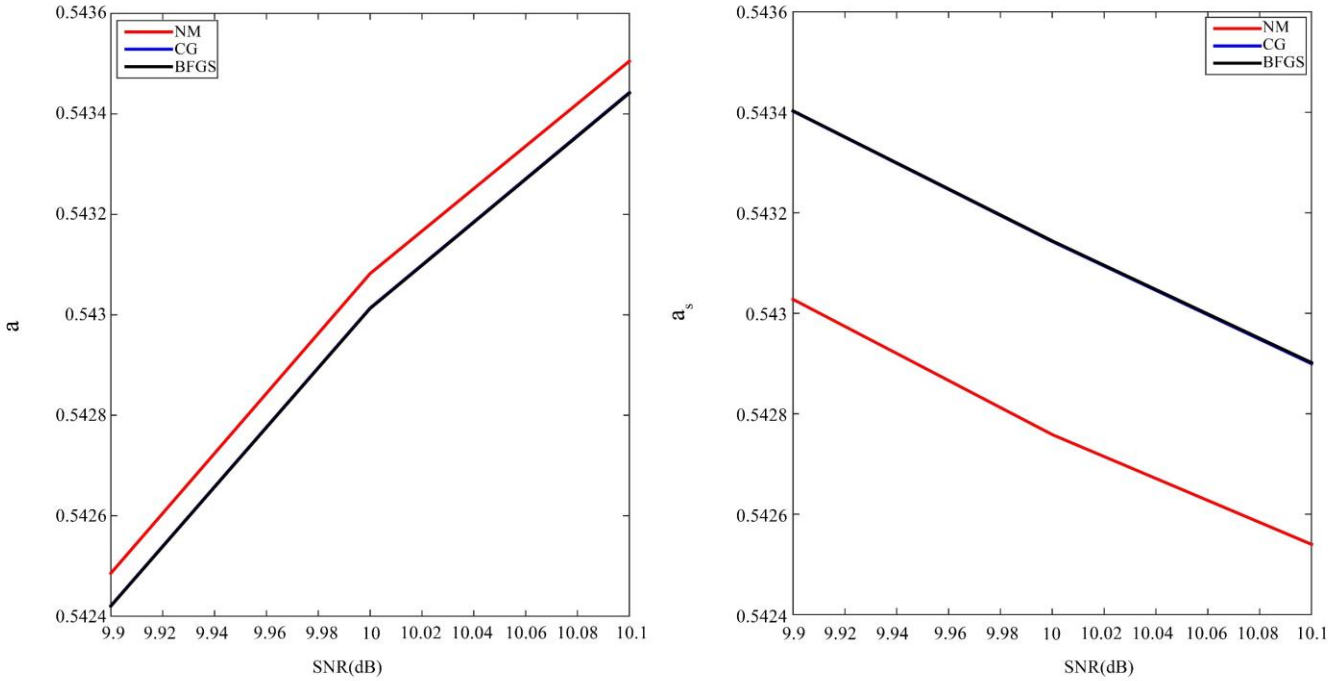

Fig. 10 Variation of power allocation factors in terms of SNR for the SBJ-UT scheme

6. Conclusion and Future Directions

Resource allocation is one of the most important issues in communication networks. This paper studied a performance comparison of different power optimization algorithms for cooperative jamming schemes to improve the secrecy performance of an AF relaying network with an external eavesdropper. The results show that the iterative algorithms offer greater secrecy than conventional methods, and EPA performs well only in symmetric relay positions. The iterative algorithms are evaluated in terms of convergence and

complexity. Further, it is observed that a trade-off exists between the convergence and complexity of the optimization algorithms. It is found that the gradient-based optimization methods are less complex than the gradient-free optimization methods. The method that allocates less power to the jamming signal and the one that requires fewer iterations for convergence is considered the best choice.

Hence, from the experimental results, it can be concluded that the Nelder-Mead method is the best option for convergence, whereas BFGS is the better choice for lesser complexity. The drawback of the BFGS algorithm is that it converges only for the symmetric relay position and may or may not converge for asymmetric relay positions. The performance of the CG method is somewhat mid-way between the two methods. So, it can be concluded that if the relay position is known, BFGS is a good option for symmetric cases, and N-M can be used for asymmetric cases. The different optimization methods used in the network can be applied to any cooperative network where the power allocation problem is a concern.

The four-node system model can be extended to the generalized case of a network scenario with multiple relays. The case of various eavesdroppers that can wiretap communication and the scenarios of colluding and non-colluding eavesdropper cases can also be considered. Also, the algorithms can be used with other transmission protocols as well in cooperative communication. Although passive eavesdropping attacks are the main focus of current PLS research, active attack instances may be considered for further study. Also, analysis and implementation in real-world scenarios with varying noise levels, mobility of nodes, etc., can be considered for future work.

References

[1] Raef Bassily et al., "Cooperative Security at the Physical Layer: A Summary of Recent Advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16-28, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[2] A. Bletsas et al., "A Simple Cooperative Diversity Method Based on Network Path Selection," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 659-672, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[3] Xu Chen et al., "Asymptotic Analysis of Opportunistic Relaying Based on the Max-Generalized-Mean Selection Criterion," *IEEE Transactions on Wireless Communication*, vol. 10, no. 4, pp. 1050-1057, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[4] Yulong Zou et al., "Improving Physical Layer Security in Wireless Communications Using Diversity Techniques," *IEEE Network*, vol. 29, no. 1, pp. 42-48, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ruoheng Liu, and Wade Trappe, *Securing Wireless Communications at the Physical Layer*, Springer, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[6] Amitav Mukherjee et al., "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550-1573, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[7] Aylin Yener, and Sennur Ulukus, "Wireless Physical-Layer Security: Lessons Learned From Information Theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814-1825, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[8] Zhifan Xu, and Melike Baykal-Gürsoy, "Power Allocation for Cooperative Jamming Against a Strategic Eavesdropper Over Parallel Channels," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 846-858, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Ali Kuhestani, and Abbas Mohammadi, "Destination-Based Cooperative Jamming in Untrusted Amplify-and-Forward Relay Networks: Resource Allocation and Performance Study," *IET Communications*, vol. 10, no. 1, pp. 17-23, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[10] Wei Wang, Kah Chan The, and Kwok Hung Li, "Relay Selection for Secure Successive AF Relaying Networks with Untrusted Nodes," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2466-2476, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[11] Yuandong Wu, and Yan Huo, "A Survey of Cooperative Jamming-Based Secure Transmission for Energy-Limited Systems," *Hindawi Wireless Communications and Mobile Computing*, vol. 2021, no. 1, pp. 1-11, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Lun Dong et al., "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875-1888, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[13] Dong Wang et al., "A Survey of Optimization Approaches for Wireless Physical Layer Security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1878-1911, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] Zonghao Ma et al., "Relay Power Allocation for Security Enhancement in Three-Phase AF Two-Way Relaying Systems," *2017 9th International Conference on Wireless Communications and Signal Processing*, Nanjing, China, pp. 1-6, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[15] Wanying Guo et al., "Cooperative Communication Resource Allocation Strategies for 5G and Beyond Networks: A Review of Architecture, Challenges and Opportunities," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8054-8078, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] P.M. Shemi, M.G. Jibukumar, and M.A. Ali, "Nelder-Mead-Based Power Optimization for Secrecy Enhancement in Amplify-and-Forward Cooperative Relay Networks," *International Journal of Communication Systems*, vol. 32, no. 11, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[17] Lu Lv et al., "Improving Physical Layer Security in Untrusted Relay Networks: Cooperative Jamming and Power Allocation," *IET Communications*, vol. 11, no. 3, pp. 393-399, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[18] P.M. Shemi, M.G. Jibukumar, and M.A. Ali, "Enhancing Secrecy in Cooperative Networks via Power Optimized Source Based Jamming," *2019 2nd IEEE Middle East and North Africa Communications Conference (MENACOMM)*, Manama, Bahrain, pp. 1-6, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[19] J.A. Nelder, and R. Mead, "A Simplex Method for Function Minimization," *The Computer Journal*, vol. 7, no. 4, pp. 308-313, 1965. [CrossRef] [Google Scholar] [Publisher Link]

[20] R. Fletcher, *Practical Methods of Optimization*, Wiley, pp. 1-464, 1987. [Google Scholar] [Publisher Link]

[21] Terry Anthony Straeter, "*On the Extension of the Davidon-Broyden Class of Rank One, Quasi-Newton Minimization Methods to an Infinite Dimensional Hilbert Space with Applications to Optimal Control Problems*," Thesis, North Carolina State University at Raleigh, 2011. [Google Scholar] [Publisher Link]

[22] Ali Kuhestani, Abbas Mohammadi, and Mohammadali Mohammadi, "Joint Relay Selection and Power Allocation in Large-Scale MIMO Systems with Untrusted Relays and Passive Eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 341-355, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[23] John H. Mathews, and Kurtis D. Fink, *Numerical Methods: Using Matlab*, Pearson, pp. 1-680, 2004. [Google Scholar] [Publisher Link]

[24] Qiu Hong Zhao et al., "A Restarted and Modified Simplex Search for Unconstrained Optimization," *Computers & Operations Research*, vol. 36, no. 12, pp. 3263-3271, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[25] Jr. J.E. Dennis, and Robert B. Schnabel, *Secant Methods for Unconstrained Minimization*, Numerical Methods for Unconstrained Optimization and Nonlinear Equations, Englewood Cliffs, NJ: Prentice-Hall, pp. 194-215, 1983. [CrossRef] [Google Scholar] [Publisher Link]

[26] Oleksandra Osadcha, and Zbigniew Marszaek, "Comparison of Steepest Descent Method and Conjugate Gradient Method," *CEUR Workshop Proceedings, SYSTEM 2017 - Proceedings of the Symposium for Young Scientists in Technology, Engineering and Mathematics*, pp. 1-6, 2017. [Google Scholar] [Publisher Link]

[27] Wenyu Sun, and Ya-Xiang Yuan, *Optimization Theory and Methods: Nonlinear Programming*, Springer US, pp. 1-687, 2006. [Google Scholar] [Publisher Link]

[28] Jürg Nievergelt, "Exhaustive Search, Combinatorial Optimization and Enumeration: Exploring the Potential of Raw Computing Power," *SOFSEM 2000 - Theory and Practice of Informatics*, pp. 18-35, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[29] Matthieu Bloch et al., "Wireless Information-Theoretic Security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515-2534, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[30] Mischa Dohler, and Yonghui Li, *Cooperative Communications: Hardware, Channel and PHY*, Wiley, pp. 1-464, 2010. [Google Scholar] [Publisher Link]