

# Multiuser-scheduling and resource allocation using max-min technique in wireless powered communication networks

Richu Mary Thomas, Malarvizhi Subramani

Department of Electronics and Communication Engineering, Faculty of Engineering, SRM Institute of Science and Technology, Kancheepuram, India

## Article Info

### Article history:

Received Mar 23, 2022

Revised Jun 1, 2022

Accepted Jun 16, 2022

### Keywords:

Hybrid relay

Max-Min fairness approach

Multiuser scheduling

Secrecy performance

Secrecy throughput

Sensor network

## ABSTRACT

Wireless powered communication network (WPCN) is a promising research area for improving network security and speed. The transmission power of the source during the uplink functions as a random variable in WPCN due to the intrinsic power transfer process, whereas it is a constant in typical cooperative networks, culminating in the signal to noise ratio of the source-access point and all the source-relay-access point being mutually correlated. As a result of the massive increase in communication devices powered by battery, the goal of prolonging their life is critical. To get the most throughput in the shortest amount of time, the best uplink and downlink time allocations were calculated. For high throughput and secrecy performance, the proportional max-min fairness algorithm was used in this paper for secure communication in hybrid relays integrated with WPCN. This method allows for multi-user scheduling with optimum targets to provide reliable hybrid outage probability, secrecy outage probability, and energy outage probability. Efficacy of the proposed system was demonstrated regarding throughput, outage probability, and confidentiality. The performance of the model was compared to that of various energy harvesting models like random user scheduling, best user scheduling, and several others, and was found to outperform them for secure transmission.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Malarvizhi Subramani

Department of Electronics and Communication Engineering, Faculty of Engineering

SRM Institute of Science and Technology

Kancheepuram, Tamilnadu, India

Email: malarvig@srmist.edu.in

## 1. INTRODUCTION

Wireless powered communication network (WPCN) eliminates the need for manual cell replacement/recharging, outperforming typical battery-powered communications systems in various ways, including increased throughput, longer device lifetime, and lower network operating costs. WPCN also offers complete control over its power transmission, with the transmit power, waveforms, and utilized frequency/time dimensions, among other things, all tuneable to guarantee a reliable energy supply under a variety of physical situations and service requirements.

The swift expansion of wireless communication technological factors has made the world move towards innovative network architecture that has been characterized by large network capacity, fast transmission power and low delay [1]. With these applications, huge devices and machines in the communication network have modified the lifestyle of people, working and learning methods considerably [2]. Further, high-speed data and increased multimedia services associated with the stipulation to ameliorate the quality of service (QoS) lead to a gradual increase in energy consumption [3]. Generally, wireless

powered communication (WPC) is termed a wireless network that comprises devices that produce energy for the exchange of information [4].

Remarkably, the wireless terminal battery in WPCN could be replenished remotely by a power beacon (PB) with the employment of energy harvesting (EH) technology in order to steer clear of the burden occurring due to frequent battery charging and wired charging for communication devices [5], [6]. Hence, WPC draws extensive attention and gradually explores several wireless communication systems like wireless sensor networks (WSN) and cognitive radio networks (CRN) [7]. Consequently, the major obstacle observed for the transmission is the short distance because of the fading and dual-path loss that results in the constrained harvested energy in the terminals [8]. Nowadays, cooperative communication techniques for achieving spatial diversity gain and improving system effectiveness without the rise of quantity and complexity of devices are considered a promising method to overcome the specified problem. Apart from several advantages, WPCN faces several more severe issues than the conventional wireless networks concerning privacy and security because of the network structure complexity and diversified nodes [9].

Verma *et al.* [10] investigated the effects of several battery models on five routing protocols using a wireless sensor network system and provided an analytical approach for analysing important performance indicators such as average jitter, first and last packet received, total bytes received, average end-to-end delay, throughput, and energy consumption. These issues make it susceptible to eavesdropping and information interception [11]. To mitigate such issues, physical layer security contributing to low complexity, latency and ability integrated with other security approaches will improve secrecy performance [12]. In terms of performance measures, [13] assessed a dense WSN architecture that includes two data distribution routing protocols: sense count, transmit count, and receive redundant count. Sharma and Verma [14], a unique energy-efficient routing strategy is proposed. Catenarian-Trim Medley routing systems extend the life of a wireless sensor network by distributing transmission loads among all nodes and saving significant energy by transmitting data with just one node in one round. An integrated exploration on internet of things (IoT) and wireless sensor networks (WSN) was done by [15]. The physical layer security (PLS) in wireless communication systems has recently acquired significant attention. Several existing articles suggested various approaches for improvising the secrecy performance of wireless systems like spatial diversity and cooperative diversity [16]. This paper provides a comprehensive review of prevailing literature in accordance with improving secrecy performance [17]. IoT models that contain relay selection have been investigated by several studies, such as implementing a multiple access technique called non-orthogonal multiple access (NOMA) [18]. This research work by Rezaei *et al.* [19] has investigated and applied a supervised machine learning technique for sensing the three well-known security attacks, namely hello flood, increased version and decreased rank.

## 2. METHOD

### 2.1. Background

This section provides comprehensive insights into existing literature corresponding to the proposed scheme. A novel technique was suggested by Do *et al.* [20], namely, relay selection NOMA (RS-NOMA), mainly considering secure performance. This study evaluated secure performance, in which a base station (BS) transfers a confidential message to critical sensors. In the suggested method, two NOMA sensors and an illegal sensor were given various levels of allocated power. Moreover, the study formulated closed-form expressions strictly positive secure capacity (SPSC) and secure outage probability (SOP) for examining secrecy performance under the parameters like threshold rates, channel gains, number of selected relay and signal to noise ratio (SNR). Finally, the study stated that NOMA has more advantages in secure performance than orthogonal multiple access (OMA). This paper concluded the impact of degree of freedom on the chisquared node distribution strategy for wireless sensor network [21]. Similarly, a new secrecy scenario of uplink NOMA with co-operative jammers has been investigated by Jiang *et al.* [22] for improvising the performance of secrecy. First, the study distinguished the performance of secrecy according to effective secrecy throughput (EST), SOP, and the closed-form expressions of individual secrecy performance was acquired from the study. From the experimental analysis, the outcomes of the study depicted an improved secrecy performance and demonstrated how every jammer impacts the secrecy performance [23]. Further, the study examined individual secrecy performance for asymptomatic behaviours. Finally, they provided an in-depth analysis in maximizing the secrecy performance by examining optimization problems such as optimal jammer selection under identical transmit power and optimal allocation of power in every transmitter with limited transmit power. Singh *et al.* [24] assessed a WSN framework that uses trust and reputation models to quantify and compare performance across multiple WSN modes, such as static, dynamic, and oscillatory.

The performance of secrecy for Multiple input single output (MISO) with secret messages for visible light communication channel was investigated by Arfaoui *et al.* [25]. This model included  $K+1$  nodes that had a transmitter which had  $N$  attachments of light-emitting diode (LED) and users ( $K$ ) who were

dispersed spatially. Further, the study modelled the MU channel as real-valued and deterministic and assumed active. The study considered the measures of secrecy performance like weighted fairness, proportional fairness, harmonic mean and max-min fairness for deriving a satisfactory secrecy rate. Additionally, the study suggested algorithms which produce the finest secrecy rate pre-coding matrix, in which the study analyzed its computational complexities and convergence. Finally, the study presented various numerical examples by utilizing the suggested method, from which it has achieved better secrecy performance [26]. Similarly, the performance of secrecy of intelligent reflecting surface (IRS) based indoor wireless communication was examined in [27]. The intelligent reflecting surface can adjust the phase shift and direction of a reflected signal and assists a source for communicating with authorized users when there are numerous unauthorized users. Further, this study designs a tile allocation and phase shift adjustment (TAaPSA) method to optimize average secrecy rate (ASR) and to evaluate SOP. To accomplish this, the study adopted the rice distribution and ray model for describing the IRS reflected signal propagation and fading process. Besides, the study also obtained the analytical closed-form expressions for mean secrecy rate and SOP [28].

An opportunistic secure multi-user scheduling was examined by [29] in un-trusted energy harvesting networks, in which a power-deprived amplify and forward (AF) relay yields power from radio frequency (RF) signals received by utilizing a power splitting (PS) protocol. Further, the study investigated three opportunistic user-scheduling methods like minimum scheduling, maximum scheduling, and optimal scheduling methods for exploiting benefits like direct link and multi-user diversity. In particular, the user selection has been performed by the optimal scheduling method by maximizing SNR. For these methods, the study examined the satisfactory secrecy performance such as SOP, secrecy throughput (ST), asymptomatic SOP and secure energy efficiency (SEE) for facilitating an efficient transmission design. Finally, the study performed simulation analysis, and from the outcomes, it was stated that the maximal scheduling method outshines the minimal scheduling method in accordance to SOP at lower target secrecy rates and SNRs.

The influence of rogue servers on various trust and reputation models in WSN is discussed in [30]. First, we looked at the bioinspired trust and reputation model WSN (BTRM-WSN), peer trust, power trust, Eigen trust, and linguistic fuzzy trust model, which are all trust and reputation models. They also developed a wireless sensor network concept for the optimization of their models. A multi-user uplink network was investigated by Li *et al.* [31] that incorporates one base station (BS), eavesdropper (E) and multiple users, in which the users transmit confidential messages to the base station, whereas the eavesdropper attempted to tap their transmissions. In order to improve the secrecy in transmission, this study recommended two jammer selection based multi-user scheduling methods such as random jammer selection based multi-user scheduling (RJS MUS), where the channel state information (CSI) of the eavesdropper are unavailable and optimal jammer selection based multi-user scheduling (OJS-MUS), where the CSI of eavesdropper are available. The experimental analysis found that the suggested method has better secrecy performance, and it outshined other conventional non-jammer selection-aided multiuser scheduling (NJS MUS) methods in terms of SOP. The transmission performance of multi-user downlink asymmetric free-space optical/radiofrequency link (FSO/RF) was examined in reference [32]. With the help of derived ergodic capacity and available statistical channel state information, the study suggested a new proportional fair scheduling (PFS) method. Finally, the numerical results deliberated the superiority of the suggested method.

Ding *et al.* [33] examined the security of the physical-layer security (PLS) of cognitive radio system (CRS) in numerous eavesdroppers (EDs) scenario, that incorporates secondary base station (SBS), several secondary users (SUs) and primary transmitter and primary receiver (PT&PR). Further, the study considered two user-scheduling methods: channel aware user scheduling (CAUS) and energy-aware user scheduling (EAUS) methods. The study analyzed the security reliability trade-off (SRT) of EAUS and CAUS methods according to the outage probability and intercept. Finally, the study demonstrated that the EAUS method had accomplished better secrecy performance [34].

## 2.2. The problem

There exist various limitations in prevailing works of literature, in which from [35], it was stated that users who have poor channels might lose access to channels. Further, the conventional max-min scheduling scheme has disadvantages like limited throughput since relay nodes are not equipped with a buffer. Additionally, there is very little probability of scheduling for users with inferior channel quality [36]. In addition, the user pairs, who have poor channel quality, are segregated into two batches. In the first batch, every user pair has poor channel quality for relay-destination and source-relay links. In the second batch, every pair has superior quality of channel for relay-destination and source-Relay links and inferior channel quality for every other link. This results in a limited selection of users since the worse links restrict the probability of selection. In such scenarios, channel resources of superior links will be wasted.

Even though the Max-max scheduling method could fully use wireless channel diversity, it does not solve channel imbalance issues. However, this method also has similar disadvantages to the Max-min scheme. To overcome these problems, the presented proportional Max-min scheduling scheme allocates the users to have maximum SNR, thereby maximizing the rate of users while assuring every user rate is proportional to the channel quality of users. This also results in accomplishing better secrecy performance.

**2.3. The proposed solution**

In this work, a novel proportional max-min fairness approach for improvising the secrecy performance of multiuser wireless powered cooperative communication network. Further, this study scheduled the multi-users based on scheduling rules, which rely on user data rate, bandwidth, and availability of resource blocks. By optimizing the targets, the study achieved satisfactory results. Finally, the performance analysis of the study revealed that the proposed method had improvised the secrecy performance. For high throughput and secrecy performance, the proportional max-min fairness algorithm was used to secure communication in hybrid relays integrated with WPCN. This suggested method allows for multi-user scheduling with optimum targets in order to provide reliable hybrid outage probability, SOP (security outage probability), and energy outage probability. The proposed system's usefulness was demonstrated in terms of throughput, outage probability, and confidentiality. The performance of the proposed model was compared to that of existing methods like random user scheduling, best user scheduling, and a variety of other energy harvesting models, and it was found to outperform them in terms of secure transmission. The various objectives of this method are as shown in. i) To enable multiuser scheduling with predicting optimizing targets and accomplish hybrid outage probability, secrecy outage probability as well as energy outage probability by utilizing relay-based scheduling rules; ii) To improvise the secrecy throughput of the targeted WPCN by employing novel proportional Max min fairness scheme; iii) To solve the maximization issue of secrecy throughput by implementing the presented model.

The study considered WPCCN, where the orthogonal subcarriers were clustered in frequency and time as Resource blocks ( $RB_{s0}$ ) with  $T_{ib}$  seconds (duration) as well as  $W_{ib}$  Hertz as the frequency span. Further, there are  $T_i$  resource blocks by the frame and  $N_i$  sub-channels available that are scheduled to  $M$  users. Subsequently, the study assumed that, the users are linked to base station (BS)  $B_{s0}$  via a relay node  $R_{s0}$  at a given time period. The  $M$  users connected to the base station via relay node are determined by a high layer process. The outcomes could be extended to multiple relay node scenarios.

The relay node is said to be a wireless powered cooperative communication network-based hybrid relay that multiplexes the data of the user after obtaining from  $B_{s0}$ . Further, the relay node might remap the  $RB_{s0}$  from one sub-channel to another sub-channel. The study noted that, in the case of switching, a better sub-channel could be a hindrance by a deeply faded sub-channel. The relay node  $R_{s0}$  has majority of  $T_i/2$  resource blocks ( $RB_{s0}$ ) on every sub-channel prior to re-transmitting it to the users as resource blocks must be allocated in sets. Multi-users might have resource blocks on similar channels in the selfsame frame. The quantity of bits carried across in the resource block relies on coding and adaptive modulation in integrated transmission in two hops.

**2.4. System model**

Figure 1 represents the system model that represents an uplink transmission in a multi-user wireless powered sensor network, which incorporated power beacon (PB), Eavesdropper (Eve), intended destination (D) as well as multiple sensors  $S_n$ . Due to terminal device limitations,  $S_n$  must acquire energy through wireless power transfer (WPT) from a dedicated power beacon for supporting information transformation. On the contrary, the destination acquires energy through on-grid power. In addition, it is assumed that, at every sensor  $S_n$ , the Eve and D are half-duplex devices and have a single antenna.

The number of bits that a  $RB_{s0}$  (resource block) carries is dependent on the modulation and the transmission in two hops combined. In the study, we denoted the number of transmitted bits in the resource block with  $b_{a,b}^{(M_0)}$ , which is assigned for the user  $M_0$  on sub channel a by base station  $B_{s0}$  and re-transmitted on channel b by the resource block. Subsequently,  $b_{a,b}^{(M_0)}$  is said to be the sub-channel coupling rate for user  $M_0$ , in which  $(a, b)$  indicates ‘coupled’ transmission from the BS to the relay node, on sub-channel a with transmission from the relay node to the user  $M_0$  on sub-channel b.

The harvested energy could be represented as shown in (1).

$$y_D = \sqrt{P_{a,b}} b_{a,b}^{(M_0)} * x_{a,b}^{(M_0)} + n_D \tag{1}$$

And the received signals at destination can be depicted as (2).

$$E_{a,b} = \eta P_B \alpha T |b_{a,b}^{(M_o)}| \tag{2}$$

From (1) and (2),  $P_{a,b}$  indicates the users' transmit power,  $E_{a,b}$  is the harvested energy from the users,  $\eta$  denotes energy harvest efficacy factor,  $\alpha$  is said to be the time switching factor,  $P_B$  indicates the transmit power of the power beacon (PB),  $T$  is the time slot,  $y_D$  is said to be the received signal at destination D as well as  $n_D$  indicates the noise variance at destination D.

Moreover, the end-to-end user rate rely on allocation of the resource blocks in the frame.

$$rm_i = \frac{1}{T_{bi}} \sum_{a=1}^{N_i} \sum_{b=1}^{N_i} b_{a,b}^{(M_o)} x_{a,b}^{(M_o)} \tag{3}$$

From (3),  $rm_i$  is said to be the rate of user  $M_o$  in bits per second, and the term  $x_{a,b}^{(M_o)}$  are unknowns that are searched by the radio resource management (RRM) algorithm.

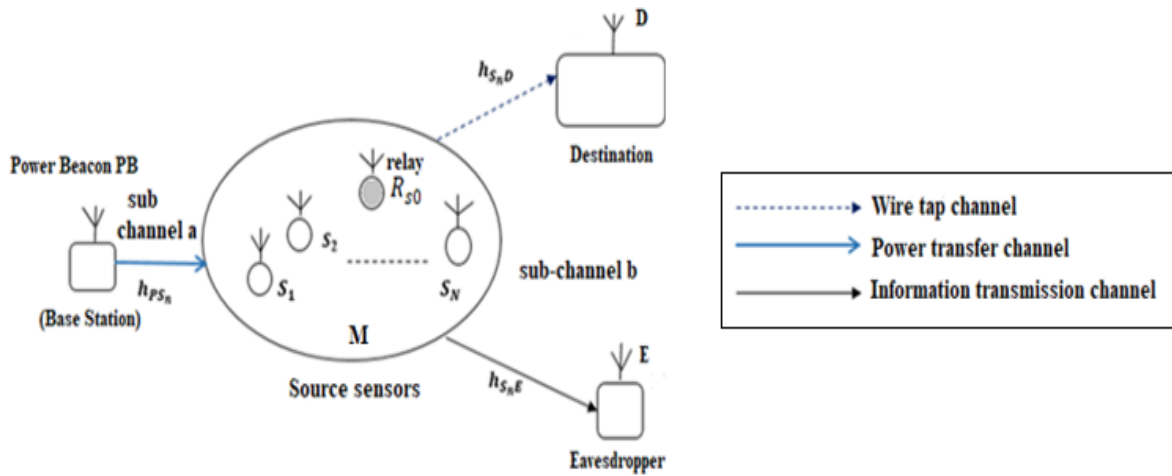


Figure 1. System model

**2.5. Max-min scheduling scheme for hybrid relay networks**

The study formulated the rate of allocation of max-min sub-channels for WPCCN based hybrid relay-assisted networks and solved it with an algorithm that was gradient-based, such that, an optimization was formulated that asymptotically gives max-min fair rates, and has convex related counterparts.

$$\max_{x_{a,b}^{M_o}} \sum_{M_o=1}^M \frac{1}{1-\gamma} \left( \frac{1}{T_{bi}} \sum_{a=1}^{N_i} \sum_{b=1}^{N_i} b_{a,b}^{(M_o)} x_{a,b}^{(M_o)} \right)^{1-\gamma} \tag{4}$$

$$\text{Subject to } \sum_{M_o=1}^M \sum_{b=1}^{N_i} b_{a,b}^{(M_o)} \leq \frac{T_i}{2}, 1 \leq a \leq N_i \tag{5}$$

$$\sum_{M_o=1}^M \sum_{a=1}^{N_i} b_{a,b}^{(M_o)} \leq \frac{T_i}{2}, 1 \leq b \leq N_i \tag{6}$$

$$x_{a,b}^{(M_o)} \in \left\{ 0, \dots, \dots, \frac{T_i}{2} \right\} 1 \leq a, b \leq N_i, 1 \leq M_o \leq M \tag{7}$$

From (4)-(7), it is observed that, M indicates the number of users,  $T_{bi}$  is said to be the time duration of the resource block, the number of sub channels are indicated by  $N_i$  and  $b_{a,b}^{(M_o)}$  denotes the number of bits, which are carried in resource block for sub channel coupling (a, b) of the user  $M_o$ , whereas  $x_{a,b}^{(M_o)}$  is said to be the amount of resource blocks allocated to the user  $M_o$ . Finally,  $\gamma$  denotes the parameter that gives rates of max-min fairness asymptotically.

$$U_{N_i}(\dots, x_{a,b}^{(M_o)}, \dots) = \sum_{M_o=1}^M \frac{1}{1-\gamma} \left( \frac{1}{T_{bi}} \sum_{a=1}^{N_i} \sum_{b=1}^{N_i} b_{a,b}^{(M_o)} x_{a,b}^{(M_o)} \right)^{1-\gamma} \tag{8}$$

From (8), it is perceived that the objective function called the fairness utility function is represented by  $\gamma$  that was previously utilized for obtaining generalized fair rates for  $0 \leq \gamma \leq 1$ . As  $\gamma \rightarrow \infty$ , the optimal rates obtained from the objective function are said to be max-min fairs. Further, the (5) and (6) guarantee that the total quantity of scheduled blocks doesn't surpass the number of blocks present in the frame. Whereas (7) assures that the scheduling is integral. The time allocation integrality demonstrated by (7) leads to computation complexities. Nevertheless, replacing (5) with optimization becomes a convex issue if time allocation integrality is relaxed.

$$0 \leq x_{a,b}^{(M_o)} \leq \frac{T_i}{2}, 1 \leq a, b \leq N_i, 1 \leq M_o \leq M \tag{9}$$

As this study deals with the asymptomatic value of  $\gamma \rightarrow \infty$ , utilizing a pre-fabricated convex solver is impossible. However, it could be rectified by returning the objective function with a conventional max-min objective and using an off-the-rack linear program.

$$\max_{x_{a,b}^{(M_o)}} \min_{M_o} \frac{1}{T_{bi}} \sum_{a=1}^{N_i} \sum_{b=1}^{N_i} b_{a,b}^{(M_o)} x_{a,b}^{(M_o)} \tag{10}$$

The performance of the max-min linear optimization solutions are upper bound on the integer solution due to the absolute number relaxation. Nevertheless, a relaxed issue solution is utilized to calculate optimum as it incorporates real numbers that dominate the integrality of the actual issue. Thus, this study developed a sub-optimal algorithm with lesser complexities. The relaxed optimization is fathomed by using this algorithm. The Taylor's expansion of objective function is represented as (11), (12).

$$U_{ni}(\dots, x_{a,b}^{(M_o)} + 1, \dots) \approx U_{ni}(\dots, x_{a,b}^{(M_o)}, \dots) + \frac{\partial}{\partial x_{a,b}^{(M_o)}} U_{ni}(\dots, x_{a,b}^{(M_o)}, \dots) \tag{11}$$

$$\frac{\partial}{\partial x_{a,b}^{(M_o)}} U_{ni}(\dots, x_{a,b}^{(M_o)}, \dots) = \frac{b_{a,b}^{(M_o)}}{(\sum_{a=1}^{N_i} \sum_{b=1}^{N_i} b_{a,b}^{(M_o)} x_{a,b}^{(M_o)})} \tag{12}$$

By utilizing the previous equation, the study developed an iterative algorithm for solving GPF (generalized proportionally fair) optimization. The user with a higher partial derivative was scheduled a resource block in every iteration.

$$(a^*, b^*, M_o^*) \leftarrow \underset{\substack{1 \leq M_o \leq m_o \\ 1 \leq a, b \leq N_i}}{\operatorname{argmax}} \frac{b_{a,b}^{(M_o)}}{(\sum_{a=1}^{N_i} \sum_{b=1}^{N_i} b_{a,b}^{(M_o)} x_{a,b}^{(M_o)})} \tag{13}$$

From (13), the study devised a gradient-based algorithm for solving the issue  $\gamma \rightarrow \infty$  that correlate with max-min rate scheduling. The study used a gradient-based algorithm for identifying max-min fair (algorithm MM) scheduling of the user rates. The devised algorithm is as given in Table 1.

This algorithm is performed in iterations for scheduling time to accomplish the max-min fairness for the user rates. Step 3 and step 4 execute the search in accordance with preposition. Step 3 finds the minimum rate user, whereas step 4 finds the best channel coupling. Further, the variables such as  $T_{b_i}(RS_o)$  and  $T_{b_i}(BS_o)$  track the obtainable slots on every sub-channel for relay node and base station transmissions. After every iteration,  $T_{b_i}(RS_o)$  and  $T_{b_i}(BS_o)$  are updated in step 6 and step 7 if any slots were scheduled on channels. Also, the  $\hat{b}_{a,b}^{M_o}$  bits per slot values were updated according to the resource block availability, assuring that the scheduled slots weren't considered in the next iteration, i.e. from steps 8 to 12.

It is crucial to note that, as the algorithm runs and when  $\hat{b}_{a,b}^{M_o}$  doesn't change, it is utilized for identifying user rates, whereas when  $\hat{b}_{a,b}^{M_o}$  changes, it is utilized to identify better coupling for selected user in every iteration. In addition to that,  $\hat{b}_{a,b}^{M_o}$  reflects the scheduling in the previous steps.

Table 1. Steps for the proportional max-min algorithm

Steps	Algorithm: Proportional Max-min
Input	$(b_{a,b}^{(M_0)}, M_0, N_o, T_b)$
Step 1	$\forall a, b, M_0: b_{a,b}^{(M_0)} \leftarrow b_{a,b}^{(M_0)}$ Initialize $1 \leq a, b \leq N_o; T_{b_i}^{BS} = \frac{T_b}{2}, T_{b_j}^{RS} = \frac{T_b}{2}$
Step 2	While $\exists T_{b_i}^{BS} > 0$ and $\exists T_{b_i}^{RS} > 0$ do
Step 3	$M_0^* \leftarrow \arg \min_{1 \leq a, b \leq M_0} \sum_{a=1}^{N_i} \sum_{b=1}^{N_i} b_{a,b}^{(M_0)} x_{a,b}^{(M_0)}$
Step 4	$(a^*, b^*) \leftarrow \arg \min_{1 \leq a, b \leq M_0} b_{a,b}^{(M_0)}$
Step 5	$x_i(M_0^*) \leftarrow x_i(M_0^*) + 1$
Step 6	$T_{b_i}(BS_o) \leftarrow T_{b_i}(BS_o) - 1$
Step 7	$T_{b_j}(RS_o) \leftarrow T_{b_j}^{RS_o} - 1$
Step 8	if $T_{b_i}(BS_o) = 0$ then, $b_{a,b}^{(M_0)} \leftarrow 0, 1 \leq M_0 \leq M, 1 \leq b \leq N_o$
Step 9	if $T_{b_i}(RS_o) = 0$ then, $b_{a,b}^{(M_0)} \leftarrow 0, 1 \leq M_0 \leq M, 1 \leq a \leq N_c$
Step 10	End if
Step 11	End if
Step 12	End while

### 3. RESULTS AND DISCUSSION

The following section illustrates that the proposed model is based on secured communication in hybrid relay integrated with WPCC has been adopted with the proportional Max-Min fairness algorithm for obtaining high throughput and secrecy performance. The input is the randomly created network topology. The following section illustrates the comparative analysis of the proposed model with other existing models.

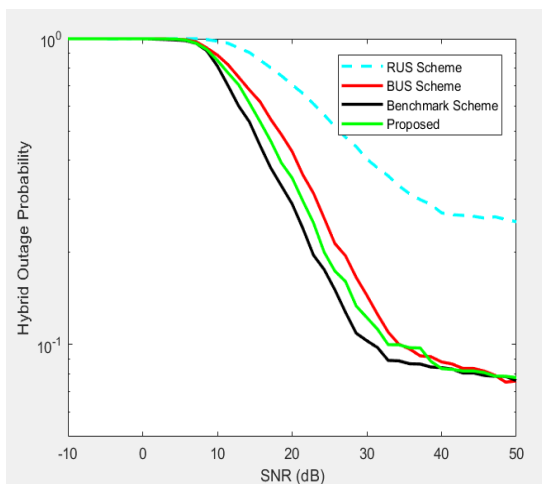


Figure 2. Hybrid outage probability vs SNR

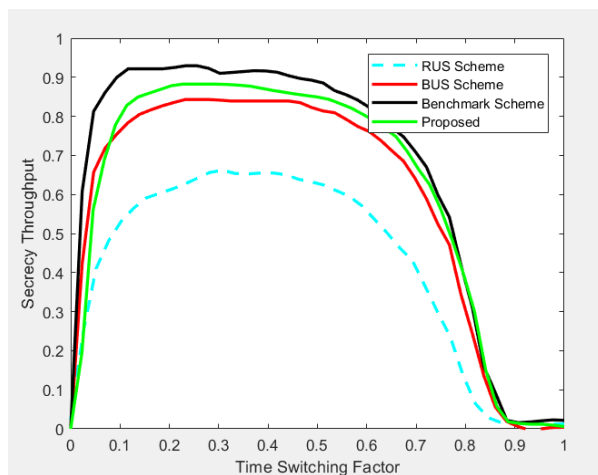


Figure 3. Secrecy throughput vs Time switching factor

Figure 2 depicts the hybrid outage probability versus transmit SNR. This graph compares the proposed method to other prevailing approaches such as random user scheduling (RUS) scheme and best user scheduling (BUS) scheme [37]. It is observed that the proposed proportional max-min fairness (PMMF) method has obtained netter secrecy performance when compared to BUS and RUS schemes. On the opposite, the secrecy performance of the benchmark scheme was slightly better than the proposed method. Nevertheless, it is noticed that achieving benchmarks scores are considerably hard to obtain because the source users and hybrid relay are challenging to get the channel state information to an eavesdropper. Therefore, the proposed method is considered effective for accomplishing a secure transmission.

Figure 3 demonstrates secrecy throughput (ST) versus time switching factor for which the proposed PMMF scheme is compared to BUS and RUS schemes [37]. In general, the source users cannot yield sufficient energy when the time switching factor is negligible. On the contrary, when the time switching factor is significantly higher, the transmission time will be considerably less, thus resulting in a higher hybrid outage probability. This results in a small value of secrecy throughput.

Figure 4 illustrates the secrecy throughput versus the transmission rate. This figure shows that the suggested method is collated with prevailing methods like the BUS scheme and RUS scheme [37]. Further, it is identified that the function of secrecy throughput in accordance to the transmission rate is said to be a uni-model function. This has proved that there prevails an optimal transmission rate to the maximum secrecy throughput.

Figure 5 deliberates the secrecy outage probability (SOP) against the transmit power. From this figure, it is observed that the proposed scheme is compared to other energy harvesting (EH) models such as saturation non-linear EH with activation threshold (SNAT) simulations, saturation non-linear EH (SNEH) simulations as well as linear energy harvesting (LEH) simulations. The low transmit power of the power beacon in other existing models makes it difficult to achieve a saturation threshold. But, the proposed model has accomplished a saturation threshold as it had a higher transmit power of power beacon.

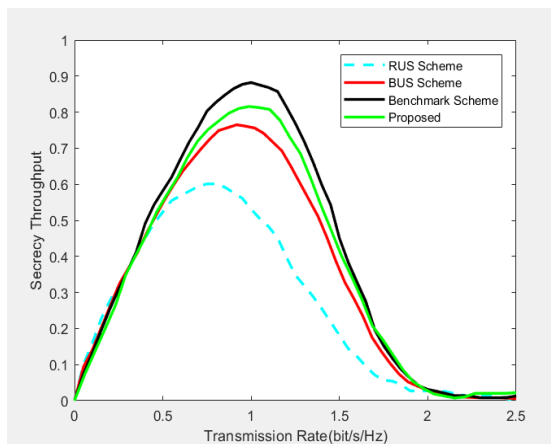


Figure 4. Secrecy throughput vs Transmission rate

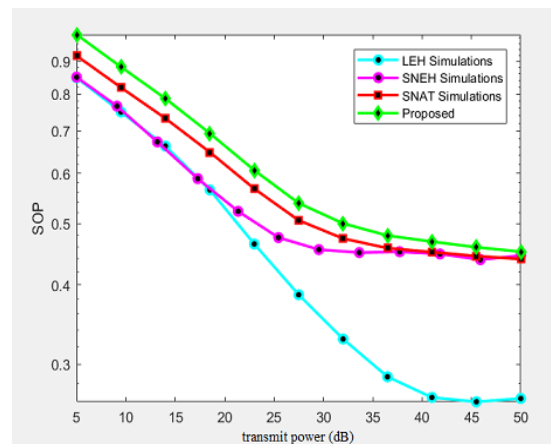


Figure 5. SOP vs transmit power

#### 4. CONCLUSION

Battery-powered energy-constrained wireless systems, such as sensor and machine-type networks, have a limited lifetime. WPT is a potential technology for energy-efficient networks, in which terminals gather energy from ambient or dedicated electromagnetic radiation using electronic circuits. When WPT technology is integrated into communication networks, it allows for the fundamental coexistence of information and energy flows; radio-frequency signals can be utilised to transmit information and/or energy. Wireless powered communications is a new communication paradigm that arises from the efficient control of these two sources through complex networking protocols, signal processing/communication techniques, and network topologies. WPC is a key enabler for global connectivity and energy conservation in emerging communication networks that will include a large number of low-power, low-rate devices.

In recent years, wireless powered communication networks have shown to be a new and exciting study subject. In this study, we designed a novel proportional max-min fairness scheme for focusing on three main directions. Firstly, for scheduling the multi-users with optimizing targets to achieve hybrid outage probability, energy outage probability and secrecy outage probability. Secondly, we exploited the proposed proportional Max-min fairness approach to improve the performance of secrecy for a relay-assisted multi-user wireless powered cooperative communication network (WPCCN). Thirdly, this method solved the maximization problem of secrecy throughput (ST). Finally, we have compared the proposed scheme with other existing schemes such as RUS and BUS schemes, and the outcomes proved that the proposed model had achieved better performance in terms of transmission power, SNR and secrecy throughput. The study showed that the time-switching factor has a significant impact on secrecy performance and should be carefully examined. Therefore, the proposed method is considered effective for accomplishing a secure transmission.



In the future research, the following are the two main research directions that we aim at. First, to make optimum use of the stored energy, ideal long-term strategies for the wireless energy transfer mechanism, such as transmission powers, transmission duration, and amount of transferred energy, should be established rather than the existing slot-oriented one. Second, cross-layer techniques should be prioritised, taking into consideration parameters and information available at the physical, MAC, and network layers. This could likely make it possible to find effective data scheduling/transmission and energy transfer solutions, both system-wide and per-user.




## REFERENCES

- [1] D. Niyato, D. I. Kim, M. Maso, and Z. Han, "Wireless powered communication networks: Research directions and technological approaches," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 88–97, Dec. 2017, doi: 10.1109/MWC.2017.1600116.
- [2] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: applications, requirements, technologies, challenges, and research directions," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 957–975, 2020, doi: 10.1109/ojcoms.2020.3010270.
- [3] D. Wang, J. Liu, and D. Yao, "An energy-efficient distributed adaptive cooperative routing based on reinforcement learning in wireless multimedia sensor networks," *Computer Networks*, vol. 178, p. 107313, Sep. 2020, doi: 10.1016/j.comnet.2020.107313.
- [4] A. M. Jawad, R. Nordin, S. K. Gharghan, H. M. Jawad, and M. Ismail, "Opportunities and challenges for near-field wireless power transfer: A review," *Energies*, vol. 10, no. 7, p. 1022, Jul. 2017, doi: 10.3390/en10071022.
- [5] A. Jamalipour and Y. Bi, "Introduction to wireless powered communication network," in *Wireless Powered Communication Networks*, Cham: Springer International Publishing, 2019, pp. 1–23, doi: 10.1007/978-3-319-98174-1\_1.
- [6] J. Kang *et al.*, "Toward secure energy harvesting cooperative networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 114–121, Aug. 2015, doi: 10.1109/MCOM.2015.7180517.
- [7] M. F. Zia and J. M. Hamamreh, "An advanced non-orthogonal multiple access security technique for future wireless communication networks," *RS Open Journal on Innovative Communication Technologies*, vol. 1, no. 2, Dec. 2020, doi: 10.46470/03d8ffbd.19888ce7.
- [8] S. Wang, M. Xia, K. Huang, and Y. C. Wu, "Wirelessly powered two-way communication with nonlinear energy harvesting model: Rate regions under fixed and mobile relay," *IEEE Transactions on Wireless Communications*, vol. 16, no. 12, pp. 8190–8204, Dec. 2017, doi: 10.1109/TWC.2017.2758767.
- [9] F. Zhou, Y. Wu, Y. C. Liang, Z. Li, Y. Wang, and K. K. Wong, "State of the art, taxonomy, and open issues on cognitive radio networks with NOMA," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 100–108, Apr. 2018, doi: 10.1109/MWC.2018.1700113.
- [10] V. K. Verma, A. Sharma, K. Ntalianis, and K. Verma, "CTMRS: catenarian-trim medley routing system for energy balancing in dispensed computing networks," *IEEE Transactions on Network Science and Engineering*, pp. 1–1, 2022, doi: 10.1109/TNSE.2021.3140139.
- [11] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 40–47, Oct. 2019, doi: 10.1109/MWC.001.1900028.
- [12] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Physical layer security for NOMA: requirements, merits, challenges, and recommendations," *arXiv preprint*, arXiv: 1905.05064, May 2019, [Online]. Available: <http://arxiv.org/abs/1905.05064>.
- [13] S. Sharma and V. K. Verma, "An integrated exploration on internet of things and wireless sensor networks," *Wireless Personal Communications*, vol. 124, no. 3, pp. 2735–2770, Jun. 2022, doi: 10.1007/s11277-022-09487-3.
- [14] S. Sharma and V. K. Verma, "AIEMLA: artificial intelligence enabled machine learning approach for routing attacks on internet of things," *Journal of Supercomputing*, vol. 77, no. 12, pp. 13757–13787, Dec. 2021, doi: 10.1007/s11227-021-03833-1.
- [15] V. K. Verma, K. Ntalianis, S. Singh, and N. P. Pathak, "Data proliferation based estimations over distribution factor in heterogeneous wireless sensor networks," *Computer Communications*, vol. 124, pp. 111–118, Jun. 2018, doi: 10.1016/j.comcom.2017.09.017.
- [16] V. K. Verma, S. Singh, and N. P. Pathak, "Towards comparative evaluation of trust and reputation models over static, dynamic and oscillating wireless sensor networks," *Wireless Networks*, vol. 23, no. 2, pp. 335–343, Feb. 2017, doi: 10.1007/s11276-015-1144-4.
- [17] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. D. Renzo, "Secrecy performance analysis of RIS-Aided wireless communication systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12296–12300, Oct. 2020, doi: 10.1109/TVT.2020.3007521.
- [18] C. Guo, B. Liao, D. Feng, C. He, and X. Ma, "Minimum secrecy throughput maximization in wireless powered secure communications," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 3, pp. 2571–2581, Mar. 2018, doi: 10.1109/TVT.2017.2767633.
- [19] R. Rezaei, S. Sun, X. Kang, Y. L. Guan, and M. R. Pakravan, "Secrecy throughput maximization for full-duplex wireless powered IoT networks under fairness constraints," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6964–6976, Aug. 2019, doi: 10.1109/JIOT.2019.2913219.
- [20] D. T. Do, M. S. Van Nguyen, T. A. Hoang, and M. Voznak, "NOMA-assisted multiple access scheme for IoT deployment: Relay selection model and secrecy performance improvement," *Sensors (Switzerland)*, vol. 19, no. 3, p. 736, Feb. 2019, doi: 10.3390/s19030736.
- [21] V. K. Verma, S. Singh, and N. P. Pathak, "Analytical event-based investigations over delphi random generator distributions for data dissemination routing protocols in highly dense wireless sensor network," *Wireless Personal Communications*, vol. 87, no. 4, pp. 1209–1222, Apr. 2016, doi: 10.1007/s11277-015-3049-z.
- [22] K. Jiang, W. Zhou, and L. Sun, "Jamming-aided secrecy performance in secure uplink NOMa System," *IEEE Access*, vol. 8, pp. 15072–15084, 2020, doi: 10.1109/ACCESS.2020.2966822.
- [23] L. T. Anh and H. Y. Kong, "Secrecy performance of an uplink-downlink cooperative PD-NOMA DF network in PLS," *International Journal of Electronics*, vol. 107, no. 11, pp. 1861–1886, Nov. 2020, doi: 10.1080/00207217.2020.1756440.
- [24] S. Singh, V. K. Verma, and N. P. Pathak, "Sensors augmentation influence over trust and reputation models realization for dense wireless sensor networks," *IEEE Sensors Journal*, vol. 15, no. 11, pp. 6248–6254, Nov. 2015, doi: 10.1109/JSEN.2015.2448642.




- [25] M. A. Arfaoui, A. Ghayeb, and C. M. Assi, "Secrecy performance of multi-user MISO VLC broadcast channels with confidential messages," *IEEE Transactions on Wireless Communications*, vol. 17, no. 11, pp. 7789–7800, Nov. 2018, doi: 10.1109/TWC.2018.2871055.
- [26] M. Yang, B. Zhang, Y. Huang, N. Yang, D. B. Da Costa, and D. Guo, "Secrecy enhancement of multiuser MISO networks using OSTBC and artificial noise," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 11394–11398, Dec. 2017, doi: 10.1109/TVT.2017.2725643.
- [27] V. P. Tuan and I. P. Hong, "Secrecy performance analysis and optimization of intelligent reflecting surface-aided indoor wireless communications," *IEEE Access*, vol. 8, pp. 109440–109452, 2020, doi: 10.1109/ACCESS.2020.3002382.
- [28] R. Zhao, H. Lin, Y. C. He, D. H. Chen, Y. Huang, and L. Yang, "Secrecy performance of transmit antenna selection for MIMO relay systems with outdated CSI," *IEEE Transactions on Communications*, vol. 66, no. 2, pp. 546–559, Feb. 2018, doi: 10.1109/TCOMM.2017.2747554.
- [29] D. Chen, Y. Cheng, X. Wang, W. Yang, J. Hu, and Y. Cai, "Energy-efficient secure multiuser scheduling in energy harvesting untrusted relay networks," *Journal of Communications and Networks*, vol. 21, no. 4, pp. 365–375, Aug. 2019, doi: 10.1109/JCN.2019.000025.
- [30] V. K. Verma, S. Singh, and N. P. Pathak, "Impact of malicious servers over trust and reputation models in wireless sensor networks," *International Journal of Electronics*, vol. 103, no. 3, pp. 530–540, Mar. 2016, doi: 10.1080/00207217.2015.1036803.
- [31] B. Li, Y. Zou, J. Zhou, F. Wang, W. Cao, and Y. D. Yao, "Secrecy outage probability analysis of friendly jammer selection aided multiuser scheduling for wireless networks," *IEEE Transactions on Communications*, vol. 67, no. 5, pp. 3482–3495, May 2019, doi: 10.1109/TCOMM.2019.2894824.
- [32] H. Kong, M. Lin, W. P. Zhu, H. Amindavar, and M. S. Alouini, "Multiuser Scheduling for Asymmetric FSO/RF Links in Satellite-UAV-Terrestrial Networks," *IEEE Wireless Communications Letters*, vol. 9, no. 8, pp. 1235–1239, Aug. 2020, doi: 10.1109/LWC.2020.2986750.
- [33] X. Ding, Y. Zou, G. Zhang, X. Chen, X. Wang, and L. Hanzo, "The security-reliability tradeoff of multiuser scheduling-aided energy harvesting cognitive radio networks," *IEEE Transactions on Communications*, vol. 67, no. 6, pp. 3890–3904, Jun. 2019, doi: 10.1109/TCOMM.2019.2904258.
- [34] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, "Secure multiuser scheduling in downlink dual-hop regenerative relay networks over Nakagami- m fading channels," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8009–8024, Dec. 2016, doi: 10.1109/TWC.2016.2610965.
- [35] S. M. Hosseini, S. Shahsavari, and C. Rosenberg, "Multi-user scheduling in hybrid millimeter wave massive MIMO systems," *arXiv e-prints*, pp. 1617–1622, Sep. 2022, doi: 10.1109/wcnc51071.2022.9771680.
- [36] X. Shang, H. Yin, Y. Wang, M. Li, and Y. Wang, "Secure multiuser scheduling for hybrid relay-assisted wireless powered cooperative communication networks with full-duplex destination-based jamming," *IEEE Access*, vol. 9, pp. 49774–49787, 2021, doi: 10.1109/ACCESS.2021.3067472.
- [37] X. Shang, H. Yin, Y. Wang, M. Li, and Y. Wang, "Secrecy performance analysis of wireless powered sensor networks under saturation nonlinear energy harvesting and activation threshold," *Sensors (Switzerland)*, vol. 20, no. 6, p. 1632, Mar. 2020, doi: 10.3390/s20061632.

## BIOGRAPHIES OF AUTHORS



**Richu Mary Thomas**    secured her Bachelor of Engineering (B. E.) degree in Electronics and Communication Engineering from Anna University in 2011. She received her post-graduate degree in Engineering (M. Tech) in Applied Electronics and Communication Systems from the University of Calicut in 2013. From 2014–2016, she had worked as a lecturer at P. A. College of Engineering, Mangalore and is at present, a research scholar in the field of Wireless Communication, in the department of Electronics and Communication Engineering at SRM Institute of Science and Technology, Kattankulathur. Her current research interests include wireless communication and sensor networks. She can be contacted at email: rm6474@srmist.edu.in.



**Prof. Dr. Malarvizhi Subramani**    was awarded her Ph.D. degree in Wireless Communication in 2006 from Anna University after receiving her M.Tech degree in Applied Electronics in 1991. She is currently a Professor in the department of Electronics and Communication Engineering at SRM Institute of Science and Technology, Kattankulathur and was the 'Head of the Department' for many years. Having more than two decades of teaching experience, she has published in all reputed journals and conferences and is the recipient of several teaching awards for her excellence in research. She has also guided and also been the principal investigator for several projects funded by various organizations and also holds two patents. Dr. Malarvizhi has got memberships in various professional organizations such as IEEE, IETE, ISC, ISTE, IET and is a reviewer for numerous journals and conferences. Her research interests include wireless communication, VLSI signal processing, image processing, and sensor communication. She can be contacted at email: malarvig@srmist.edu.in.