Dynamic power allocation scheme with clustering based on physical layer security

Tianqi Liu¹, Shuai Han², Weixiao Meng³, Cheng Li², Mugen Peng³

1 Communication Research Center, Harbin Institute of Technology, Post Box 312, No. 92, West Dazhi Street, Harbin Institute of Technology, Harbin, People’s Republic of China
2 Electrical and Computer Engineering, Memorial University, Faculty of Engineering and Applied Science Memorial University St John’s, NL, A1B 3X5, Canada
3 The Key Laboratory of Universal Wireless Communications for the Ministry of Education, Beijing University of Posts and Telecommunications, Beijing, People’s Republic of China
E-mail: hanshuai@hit.edu.cn

Abstract: Achieving large confidential capacity under the wiretap channel model is a challenge due to the narrow modulation bandwidth and total transmission power constraints. The confidential capacity of a system can be improved through a non-orthogonal multiple access technique that can obtain the highest transmission power in a downlink network. A clustering method is applied to network users who require data with similar contents. Based on the channel gain of each user, cluster heads are selected as agents for the corresponding clusters; then, the total transmission power is shared among the cluster heads. Before the power allocation process, the signal-to-interference-plus-noise ratio of the cluster heads is derived by considering clipping noise to ensure fairness. On this basis, an optimal power allocation scheme is proposed using Lagrangian dual theory. A case is presented to validate the performance of the proposed power allocation scheme. The comparison of the numerical results with those of other schemes shows that the proposed method achieves better performance regarding both secrecy sum capacity and outage probability.

1 Introduction

Due to the rapid development of wireless communication technology, emerging wireless networks have attracted increasing attention and are widely used worldwide, providing access to an enormous number of users and devices. However, the growth of applications in such networks also causes security concerns because of the openness of the wireless transmission medium, the mobility of wireless terminals and the instability of network structures [1, 2]. The above-mentioned factors pose severe challenges to the transmission reliability and security of wireless communication systems. Traditional security schemes based on cryptography at the network layer trade off high complexity for security [3, 4]. However, the high data transmission rate of the upcoming 5G standard imposes stricter demands for real-time, low complexity and low latency signal processing. Therefore, instead of traditional security approaches with cryptographic algorithms, this paper proposes a physical layer security scheme that utilises the transmission characteristics of wireless channels to maintain transmission security [5]. The theoretical basis of physical layer security is the physical layer security model established by Shannon, in which the basic idea is to exploit the uncertainty of multi-path and channel noise characteristics to encrypt data such that the amount of information received by eavesdroppers tends to zero [6]. Through proper encoding and signal processing, the physical layer security scheme guarantees data security, ensuring that confidential messages can be decoded only by legitimate receivers.

To further improve the system capacity of wireless communication networks that rely on physical layer security, the use of the non-orthogonal multiple access (NOMA) technique is widely considered to be a promising approach [7, 8]. In the downlink NOMA system, users accessing the network are differentiable in the power domain because of their discrepant power levels. Furthermore, users employ successive interference cancellation (SIC) to remove interference from other users before decoding their own messages [9].

The further improvement of the performance of the confidential communication network and the full realisation of its potential require resource management. Here, an optimal power allocation scheme is proposed based on Lagrangian duality theory that uses convex optimisation, in which the key point is that this scheme involves cluster formation in the physical layer security. By employing values collected by big data, the fundamental process in cluster formation is to share contents among clusters [10]. The proposed scheme consistently improves the sum capacity of the network and the outage probability compared to other NOMA power allocation schemes because the cluster-formation process saves power when the base station (BS) sends superposition data only to cluster heads instead of to all connected users.

The contribution of this paper is that a wiretap channel model is established based on NOMA, and then, a data-driven cluster formation scheme is applied among users in the system. Additionally, an optimal power allocation algorithm is proposed, aiming at achieving maximal secrecy sum capacity as well as ensuring fairness among users under total transmission power and secrecy transmission rate constraints. The proposed scheme can achieve good performance compared with common power allocation schemes, which verifies the superiority of the proposed scheme.

The remainder of this paper is organised as follows. Section 2 presents the secure communication system based on NOMA, followed by the scheme for forming data-driven clusters. Section 3 introduces the details of the optimal power allocation algorithm with total transmission power and secrecy transmission rate constraints. Numerical results and the performance evaluation are presented in Section 4, and Section 5 concludes this work.

2 System model

First, the wiretap channel model is described for the NOMA-based secure communication network. Then, the cluster forming scheme and the corresponding signal-to-interference-plus-noise ratio (SINR) of each cluster head are presented.
2.1 Wiretap channel model description

Consider a downlink communication system model similar to that defined in [11], where a BS with a single antenna sends confidential content to multiple signal-antenna receivers. The main distinction between this model and the one in [12] lies in the multiple access approach. In [12], the system model adopts orthogonal multiple access, while in this study, NOMA is employed instead. All available physical resources are shared by all users, and transmission power is allocated to various users based on their channel states. Channel state information can be collected by user devices and the BS by employing big data techniques. Thus, the wireless channels between the BS and legitimate users or eavesdroppers are assumed to be perfectly known, even though in practice, it is difficult to obtain the real channel capacity of eavesdroppers. The reason is that the purpose of taking into consideration channel capacity is to qualitatively analyse the influence of eavesdroppers. Under the condition of the existence of eavesdroppers, it is important to determine how to decrease their influence and to finally obtain an optimal power allocation scheme. The purpose of our assumption of perfectly known wireless channels between the BS and the eavesdroppers is to obtain the best performance of the proposed scheme in theory. Without loss of generality, the power allocation scheme is investigated with the goal of obtaining the optimal confidential sum capacity under certain quality of service limits.

At the physical layer, NOMA technology is adopted at each orthogonal subchannel. In this system, only \( N \) users are considered with confidentiality requirements. Several active eavesdroppers exist in the network; their goal is to wiretap the transmission signals in all the data-bearing subchannels. In a NOMA-based classified network, to ensure communication security for legitimate users, the total transmission power should be allocated to users at different levels. Users near the BS are allocated small amounts of transmission power, while users at greater distances are allocated higher amounts of power [13, 14]. Based on a cluster formation algorithm (to be introduced later), users who satisfy specific conditions can be grouped into one cluster and receive confidential content cooperatively, while other individuals users who do not belong to any cluster work alone as cluster heads. Only cluster heads receive content from the BS directly. The cluster heads function as an amplify-and-forward relay between the BS and the cluster members, sharing confidential content among cluster members via short-range direct communication techniques, such as Wi-Fi and device to device [15]. However, in this paper, the information-sharing technology is not the focus. With the normalised channel gain, SIC is adopted at the receivers [16].

2.2 Description of data-driven cluster formation

2.2.1 Condition of cluster formation: Before forming clusters, the conditions the users need to satisfy are clarified. Considering the short-range communication in clusters, cluster members should be capable of co-locating or be co-located with the cluster heads, who request locations and analyse ‘encounter patterns’ collected from users to ensure that they meet certain conditions. Under this scenario, a metric \( D_{ij} \) is defined to measure the average inter-encounter time between paired users. This metric means that, after the time period \( D_{ij} \), users \( i \) and \( j \) will be capable of receiving confidential content cooperatively. \( D_{ij} \) is a binary adjacency function used to determine whether paired users can be grouped together

\[
C_{ij} = \begin{cases} 
1, & D_{ij} < D_{th} \\
0, & D_{ij} \geq D_{th}.
\end{cases}
\]  

(1)

The determining factor of \( D_{ij} \) depends on the confidentiality and similarity of the required content as well as user locations and encounter patterns. \( D_{th} \) represents a threshold for determining whether the average inter-encounter time is sufficiently short to guarantee the security of sharing confidential content. Although single-user clusters receive content directly from the BS, they still benefit from this clustering scheme because the cooperative receiving operations by cluster members save physical resources and increase the capacity of the entire network.

2.2.2 Selection of cluster heads: Cluster heads work as relays connecting the BS and cluster members; therefore, cluster heads must have a good wireless channel state so that they receive confidential content reliably and efficiently. Additionally, cluster heads should have non-zero adjacency to as many users as possible for content-sharing purposes. Hence, a utility function is defined, \( U_i (1 \leq i \leq N) \), to evaluate the suitability of a user to be selected as a cluster head

\[
U_i = C_i^j \sum_{j=1, j \neq i}^{N} C_{ij} = C_i^j \| C_i \|.
\]  

(2)

where \( C_i^j \) denotes the secrecy capacity per transmission of user \( i \) when receiving data from the BS, and \( \sum_{j=1, j \neq i}^{N} C_{ij} = \| C_i \| \) indicates the number of cluster members (including the cluster head itself) when user \( i \) is chosen as a cluster head. In the following section, the derivation process of \( C_i^j \) is explained in detail.

2.2.3 Process of cluster formation: The cluster formation process involves two steps; first, a user satisfying certain rules (such as the channel gain) is selected, forming a single-user initial cluster. Then, based on the adjacency function, those closer than a non-zero value to the cluster head can be added to the initial cluster. Individual users not added to any clusters form independent single-user clusters.

2.3 SINR of NOMA with cluster formation

For the Gaussian wiretap channel mode, the secrecy capacity of the entire system can be expressed as follows:

\[
C_i = \max \{ I(X;Y) - I(X;Z) \},
\]  

(3)

where \( X \) is the encoded original information from the BS, \( Y \) is the message received by a legitimate user, and \( Z \) is the message received by an eavesdropper through a wiretap channel. \( I(X;Y) \) and \( I(X;Z) \) represent the mutual information between \( X \) and \( Y \) and between \( X \) and \( Z \), respectively. The channel capacity of legal users and eavesdropper is denoted by \( C_M \) and \( C_W \), respectively. Therefore, the secrecy capacity is

\[
C_i = C_M - C_W, \quad C_M > C_W; \quad 0, \quad C_M \leq C_W.
\]  

(4)

Next, the SINR of cluster heads is discussed. Under the Gaussian wiretap channel with NOMA system model, cluster heads are given the same status during the SIC process because they are uniformly distributed in one micro-cell. The performance of NOMA increases when the channel gains of multiple users vary greatly. We assume that there are \( N \) mobile users in the cellular network forming \( K \) generalised clusters, including \( m \) cluster heads and \( n \) individual users. The object of discussion is the \( K (K = m + n) \) cluster heads (CHs); their distribution of confidential content among cluster members is immaterial in this study. The BS transmits superimposed signals, denoted as \( x \), to the \( i \)th cluster head \( CH_i \), \( (i = 1, 2, \ldots, K) \), where \( E \{ |x|^2 \} = 1, (i = 1, 2, \ldots, K) \) represents the average strength of the single user \( i \) normalised to 1. The total transmission power to cluster heads is restricted to \( P_{\text{max}} \). Hence, the superimposed code transmitted downlink via the wireless channel is as follows:

\[
x = \sum_{i=1}^{K} P_i x_i.
\]  

(5)

Therefore, the received signal at \( CH_i \) is
where $h_i$ is the complex channel coefficient collected from network data, and $w_i$ is the inter-cell interference plus additive zero-mean Gaussian noise with variance $\sigma_i^2$. SIC is implemented in NOMA downlinks to reduce interference by eliminating the influence of other users who have been allocated high power levels. Users are decoded based on channel gain order of not only the target user but also other users due to inter-user interference.

Without loss of generality, the index of the $K$ users is rearranged according to their channel gains by sorting them as $\pi_1 \leq \cdots \leq \pi_i \leq \cdots \leq \pi_K$. When addressing $\mathcal{CH}_i$, $\mathcal{CH}_i(\forall i \in \{1, 2, \ldots, i-1\})$ whose order is smaller than the target $\mathcal{CH}_i$ should be decoded in advance and subtracted from the received signal [16] because the influences of users with larger indexes are regarded as interference that cannot be eliminated. Thus, the SINR of $\mathcal{CH}_i$ is

$$r'_M = \frac{\pi_i P_i}{\pi_i \sum_{j \neq i} P_j} + 1.$$  \hspace{1cm} (8)

The channel capacity of $\mathcal{CH}_i$ through the legitimate link is represented by

$$C_M = \log(1 + r'_M).$$  \hspace{1cm} (9)

Assuming that each cluster has only one eavesdropper, the channel capacity of the eavesdropping link is as follows:

$$C_W = \log\left(1 + \frac{P_w^i}{\sigma_w^2}\right).$$  \hspace{1cm} (10)

where $P_w^i/\sigma_w^2$ is the SNR of the illegal channel. The secrecy capacity of the Gaussian wiretap channel for user $i$ is as follows:

$$C_i^* = (C_M - C_W)^* = \max \left\{ C_M - C_W, 0 \right\}. $$  \hspace{1cm} (11)

To consider the confidential transmission rate $R_c$ that must be satisfied in the case of transmission interruption, the secrecy capacity of user $i$ is written as follows:

$$C_i' = \begin{cases} (|| C_i || \cdot C_M - C_W): & C_M - C_W \geq R_c; \\ 0: & C_M - C_W < R_c. \end{cases}$$  \hspace{1cm} (12)

3 Power allocation schemes

In this section, the proposed optimal power allocation scheme is analysed based on Lagrangian dual theory. Then, other power allocation schemes are briefly introduced for comparison. Based on the clustering result, $C_i$ is obviously related to the power allocation for cluster heads. This allocation affects the achievable throughput of not only the target user but also other users due to inter-user interference. Therefore, the next step is to optimise the power allocation to maximise the secrecy sum capacity of the entire system under certain constraint conditions, which can be represented as follows:

$$\text{Prob1} : \max_p \sum_{i=1}^{K} \| C_i \| = \min \sum_{i=1}^{K} \| C_i \| C_M + C_W$$

s.t. $C_i : C_M \geq C_W + R_c, \; \forall i$;

$$C_i : \sum_{j \neq i} P_j \leq P_{\text{max}};$$

$$C_i : P \geq 0,$$  \hspace{1cm} (13)

where $P = (P_1, P_2, \ldots, P_K)^T$ is the power allocation vector of the cluster heads. In (13), $C_i$ is imposed to guarantee that each cluster head is allocated sufficient power to transmit data effectively; $C_i$ is a power constraint for the BS, which has maximum transmission power limit $P_{\text{max}}$; and $C_i$ is the non-negative transmission power constraint for each cluster head. Obviously, Prob1 is a combinatorial non-convex problem due to the non-convexity of the target function and $C_i$. Full-search power allocation would achieve optimal performance by exhaustively considering all possible combinations of power allocations for each candidate user set [17]. However, this method involves unacceptably high computational complexity - especially with large numbers of users. Consequently, a suboptimal solution is considered by transforming the original problem into a convex problem. In the following, we first show that non-convex problem Prob1 can be transformed into an equivalent convex one.

3.1 Optimal power allocation scheme

In this subsection, the Lagrangian dual method is used to solve Prob1 with low complexity. First, the constraint condition $C_i$ is rewritten as follows:

$$\log\left(1 + \frac{\pi_i P_i}{\pi_i \sum_{j \neq i} P_j + 1}\right) \geq C_W + R_c$$

$$\Rightarrow \pi_i \sum_{j \neq i} P_j + 1 \geq 2^{C_W + R_c} \left(\pi_i \sum_{j \neq i} P_j + 1\right).$$  \hspace{1cm} (14)

By replacing $C_i$ in (13) with (14), the Lagrangian function of the optimal solution of Prob1 can be written as follows:

$$L(p, \lambda, \mu) = - C_M - C_W \log\left(1 + \frac{\pi_i P_i}{\pi_i \sum_{j \neq i} P_j + 1}\right)$$

$$- \lambda \left(\sum_{i=1}^{K} P_i - P_{\text{max}}\right)$$

$$- \sum_{i=1}^{K} \mu_i \left(\sum_{j \neq i} P_j + 1 - 2^{C_W + R_c} \left(\pi_i \sum_{j \neq i} P_j + 1\right)\right)$$

where $\lambda = (\lambda_1, \ldots, \lambda_K)$ and $\mu$ are Lagrange multipliers, which are non-negative dual variables associated with the corresponding constraints of Prob1. Based on the conclusions presented in [11], if and only if the wiretap channel capacity satisfies (16) is Prob1 proved convex with at least one feasible solution

$$\sum_{i=1}^{K} \left(\pi_i \sum_{j \neq i} \left(2^{C_i} - C_M - C_W - 1\right)\right) \leq P_{\text{max}}.$$  \hspace{1cm} (16)

Under this constraint, because Prob1 is convex, the globally optimal solution can be obtained by solving the following Kraus–Kuhn–Tucker (KKT) conditions. The KKT conditions of Prob1 are (see (17a))

$$\mu \left(\sum_{i=1}^{K} P_i - P_{\text{max}}\right) = 0;$$  \hspace{1cm} (17b)
\[ \lambda \left( \pi \sum_{j=1}^{K} p_j + 1 - 2^{C_{i} + R_i} \right) = 0, \quad \forall i; \quad (17c) \]

\[ \lambda, \mu \geq 0. \quad (17d) \]

Furthermore, based on (17), a reasonable addition is assumed that \( C_{i-1} \leq C_i \) which means that cluster heads who experience better channel gain can include more users in their clusters. Then, by considering \( \pi_{i-1} \leq \pi_i \) and calculating \( (\partial L(p, \lambda, \mu)/\partial p_i) - (\partial L(p, \lambda, \mu)/\partial p) \), we can obtain (see (18)).

Without considering the special case where \( \pi_{i-1} = \pi_i \), the equals sign can be omitted, and only the situation involving the greater-than sign is addressed. As \( \lambda_i \geq 0, \) it is obvious that \( \lambda_{i-1} 2^{C_{i-1} + R_{i-1}} - \lambda_i \pi_i > 0. \) Then, we obtain

\[ \pi \sum_{j=1}^{K} p_j + 1 - 2^{C_{i} + R_i} \left( \pi \sum_{j=1}^{K} p_j + 1 \right) = 0, \quad \forall i. \quad (19) \]

Thus, the optimum confidential capability of the entire system is \( \sum_{i=1}^{K} C_i + R_i \), which can be easily solved. The case in which \( \lambda_i = 0 \) is also considered, which means that redundant power has been allocated to the cluster head with the best channel gain. Other cluster heads are allocated the minimum transmission power necessary to reach the minimum required rate \( R_i \). From (17c), for \( \forall 1 \leq i \leq K - 1, \) we obtain

\[ \sum_{j=1}^{K} p_j = \frac{\sum_{j=1}^{K} p_j \left( 1 - 2^{C_{i} + R_i} \right)}{2^{C_{i} + R_i} \pi_i}. \quad (20) \]

Then, the expression of \( P_i \) can be deduced as follows:

\[ P_i = \sum_{j=1}^{K} p_j - \sum_{j=1}^{K} p_j = \frac{\sum_{j=1}^{K} p_j \left( 1 - 2^{C_{i} + R_i} \right)}{2^{C_{i} + R_i} \pi_i} \quad (21) \]

\[ = \frac{1}{2^{C_{i} + R_i}} \left( 1 - 2^{C_{i} + R_i} \pi_i \right). \]

The preceding formula is not the final expression of \( P_i \); additional conditions are necessary. As \( \lambda_i > 0, \) it can be proved that \( \mu \) is positive using the following formula:

\[ \mu = \frac{\| C_i \| \pi_i}{\ln 2 (\pi_i \sum_{j=1}^{K} p_j + 1)} + \sum_{j=1}^{K} p_j + 1 \quad (22) \]

Then, considering the constraint condition in (17b), we have \( \sum_{j=1}^{K} p_j = P_{\text{max}} \), and obtain

\[ P_i = \left( P_{\text{max}} - \sum_{j=1}^{K} p_j + \frac{1}{\pi_i} \right) \frac{1}{2^{C_{i} + R_i}}, \quad \forall 1 \leq i < K - 1. \quad (23) \]

Hence, the optimal \( p_i^* \) can be expressed as follows:

\[ P_i = \left( P_{\text{max}} - \sum_{j=1}^{K} p_j + \frac{1}{\pi_i} \right) \frac{(2^{C_i + R_i} - 1)}{2^{C_i + R_i}}, \quad 1 \leq i < K; \]

\[ P_i = \sum_{j=1}^{K-1} p_j, \quad i = K. \quad (24) \]

Substituting the expression for \( P_K \) into the optimal secrecy sum capacity, we obtain the following:

\[ \sum_{i=1}^{K} (\| C_i \| - \| C_{i+1} \| + \| C_K \| (\log_2(1 + P_K)) - \sum_{i=1}^{K} \| C_i \| - \| C_{i+1} \| + \| C_K \| - \sum_{i=1}^{K} C_i). \quad (25) \]

Note that this optimal power allocation scheme not only meets the minimum required rate for confidential transmission but also maximises the sum secrecy capacity. This optimal power allocation scheme focuses on reducing the outage probability of the downlink with the goal of allowing more users to transmit data without interruption.

### 3.2 Power allocation schemes for comparison

Static power allocation (SPA) based on normalised noise and interference \( \pi_i \), sorted in ascending order [18]. SPA is related only to the index of CHs

\[ P_i = \alpha_{SPA} P_{i-1}, \quad (0 \leq \alpha_{SPA} \leq 1), \quad (26) \]

where \( \alpha_{SPA} \) is the SPA coefficient. In SPA, CHs with larger indexes, which indicate better channel state and higher channel gains, will be allocated more transmission power.

Gain ratio power allocation (GRPA) adds into consideration the channel gain of each cluster head [19]. The GRPA coefficient is calculated as follows:

\[ \alpha_{GRPA} = \left( \frac{\pi_i}{\pi_j} \right)^{\mu}, \quad \forall 2 \leq i \leq K. \quad (27) \]

GRPA depends on the relative values of the channel gains and the index. Then, the power allocated to each CH is

\[ P_i = \alpha_{GRPA} P_{i-1}. \quad (28) \]

The power assigned to cluster heads decreases based on their order because for CHs with good channel conditions, lower power levels are sufficient for signal decoding after subtracting signals under worse channel conditions. GRPA achieves greater fairness among cluster heads because it includes the ratio \( \left( \pi_i / \pi_j \right) \).

Fractional transmission power allocation (FTPAP) is motivated by the fractional transmission power control used in the LTE uplink [20], which fully considers the decoding complexity at the receiving terminals as well as the fairness of cluster heads. The power allocation of each CH is as follows:

\[ \frac{\partial L(p, \lambda, \mu)}{\partial p_i} - \ln 2 \sum_{k=i}^{K} \frac{\| C_k \| \pi_k}{\left( \sum_{j=1}^{K} p_j + 1 \right)} - \frac{\| C_k \| \pi_k}{\left( \sum_{j=1}^{K} p_j + 1 \right)} = 0, \quad \forall i; \quad (17a) \]

\[ \lambda_{i-1} 2^{C_{i-1} + R_{i-1}} - \lambda_i \pi_i = \frac{1}{\ln 2} \left( \frac{\| C_i \| \pi_i}{\left( \sum_{j=1}^{K} p_j + 1 \right)} - \frac{\| C_{i-1} \| \pi_{i-1}}{\left( \sum_{j=1}^{K} p_j + 1 \right)} \right) \geq 0. \quad (18) \]
where $\alpha_{ftpa}$ is the decay factor of FTPA. This algorithm considers the influence of each CH's channel state, which in turn influences the power allocated to each cluster head.

4 Numerical results and performance evaluation

In this section, the performance of the proposed optimal power allocation scheme is compared with those of three other schemes, including SPA, GRPA and FTPA. The case of power allocation to 20 users in one cell is taken as an example. The clustering process is based on user adjacency and employs data collected by the BS and user devices. We assume that clusters are already formed and consist of three large clusters and seven individual users. The emphasis is on allocating power to maximise the secrecy sum capacity of the entire system under some constraint conditions. Hence, to validate the power allocation scheme performance, it is applied to a specific scenario. The bandwidth of the considered subcarrier is $W_{sc} = 30$ kHz. As legitimate users experience better channels than do eavesdropping users, in this scenario, the equivalent channel gain of a legitimate link is set to vary between 0 and 10 dB, while that of an eavesdropping link varies between $-10$ and $-5$ dB. In this simulation, the power allocation factors of SPA and FTPA are $\alpha_{spa} = 0.5$ and $\alpha_{ftpa} = 0.5$, respectively, which correspond to the best performances of the two schemes.

Fig. 1 shows a comparison among the secrecy sum capacities of different power allocation schemes within the entire network. The required transmission rates $R_0$ with the outage probability of the tested schemes are depicted in Fig. 2. It is reiterated that to guarantee that the target problem is convex, the value range of $R_0$ must satisfy (17b). Hence, the range of $R_0$ is limited to $0 < R_0 < 0.46$ (bits/s/Hz). From Figs. 1 and 2, it can be seen that the performance of the optimal power allocation scheme is competitive. Even though its averaged secrecy sum capacity is no better than that of FTPA, compared to the other two schemes, the proposed scheme achieves a sufficiently high secrecy sum capacity. Additionally, concerning the outage probability performance, the proposed optimal scheme has excellent performance compared to the other schemes under all $R_0$ constraints, which means that the proposed scheme meets the $R_0$ requirement of each legal confidential user when operating at full speed.

Fig. 3 shows the secrecy capacity of each user in the system obtained using the various power allocation schemes. As the figure shows, the power allocation process of the proposed scheme leads to a flatter capacity, eliminating the differences in channel quality experienced by users, which increases the fairness among users. By contrast, the FTPA scheme provides excellent performance to only a few users with relatively good channel conditions and neglects the users with poor channel states. In Fig. 4, the secrecy capacity of each user is given in a single histogram to provide a more intuitive comparison among the performances of the various power allocation schemes. As shown, the proposed optimal power allocation scheme achieves better performance with regard to capacity as well as fairness. The excellent performance of the proposed scheme is ascribed to the cluster formation scheme. Transmission power is only allocated to cluster heads with relatively better channel state directly. Then, the equivalent number of users in the system that are allocated power directly is decreased. Hence, each cluster head will benefit from better secrecy capacity. As for the fairness among clusters, the insight into the proposed power allocation scheme reveals that the system gives priority to guarantee the secrecy communication of every user.
cluster head. Additionally, if one of the channel states of one cluster head is too poor to communicate securely, then the cluster
will not be allocated any power to avoid a waste of power, and this
scheme is fair to the other clusters in the system.

5 Conclusion
In this paper, the power allocation for a downlink wiretap channel
model is analysed using NOMA to maximise the security sum
capacity under a required transmission rate constraint. An optimal
power allocation algorithm is proposed based on clustering. An
expression to calculate the SINR of each cluster head is first
provided, and then, the secrecy sum capacity of the entire system is
given. Subsequently, both the basic idea and the closed-form
solution of the proposed power allocation scheme are provided.
Finally, the proposed scheme is compared with SPA, GRPA and
FTPA to validate its performance.

6 Acknowledgments
This work is supported by the National Natural Science Foundation
of China (no. 61771169).

7 References
layer security in the presence of interference’, IEEE Wir. Commun. Lett.,
2017, 6, (6), pp. 802–805
networks for efficient and secure transmission’, IEEE Netw., 2018, 32, (2),
pp. 100–106
2017, 66, (11), pp. 10259–10270
(iTo): models, schemes, and implementations’. 2016 8th IFIP Int. Conf. on
New Technologies, Mobility and Security (NTMS), Larnaca, Cyprus,
November 2016, pp. 1–2
physical layer security in cognitive radio networks’, IET Commun., 2012, 6,
(16), pp. 2676–2687
orthogonal multiple access in large-scale networks’. 2016 IEEE Int. Conf. on
Communications (ICC), Kuala Lumpur, May 2016, pp. 1–6
access (NOMA) for cellular future radio access’, 2013 IEEE 77th Vehicular
Technology Conf. (VTC Spring), Dresden, Germany, June 2013, pp. 1–5
Mag., 2015, 53, (9), pp. 74–81
multiple access in 5G systems with randomly deployed users’, IEEE Signal
allocation strategy with secrecy constraints’, 2017 IEEE Int. Conf. on
Communications (ICC), Paris, France, May 2017, pp. 1–6
NOMA downlinks with individual QoS constraints’, IEEE Commun. Lett.,
2017, 21, (7), pp. 1649–1652
mobile networks with big data of users and networks’, IEEE Netw., 2016, 30,
(1), pp. 6–10
ordering SIC receiver for uplink NOMA systems’, IEEE Commun. Lett.,
2017, 21, (10), pp. 2246–2249
multiple access for visible light communications’, IEEE Photonics Technol.
as an underlay to LTE-advanced networks’, IEEE Commun. Mag., 2009, 47,
(12), pp. 42–49
[16] Tomita, S., Higuchi, K.: ‘Non-orthogonal access with SIC in cellular
downlink for user fairness enhancement’. 2011 Int. Symp. on Intell Signal
Processing and Communications Systems (ISPACS), Chiang Mai, Thailand,
December 2011, pp. 1–6
evaluation of downlink-non orthogonal multiple access (NOMA)’. 2013 IEEE
24th Annual Int. Symp. on Personal, Indoor, and Mobile Radio Communications
(PIMRC), London, UK, September 2013, pp. 611–615
amplify-and-forward relay systems’. VTC Spring 2009 - IEEE 69th Vehicular
Technology Conf., Barcelona, Spain, April 2009, pp. 1–5
downlink NOMA combined with SU-MIMO for future LTE enhancements’.
2014 IEEE Globecom Workshops (GC Wkshps), Austin, TX, USA,
December 2014, pp. 706–710
access with SIC in cellular downlink using proportional fair-based resource
allocation’. 2012 Int. Symp. on Wireless Communication Systems (ISWCS),
Paris, France, August 2012, pp. 476–480
学霸图书馆
www.xuebalib.com

本文献由“学霸图书馆·文献云下载”收集自网络，仅供学习交流使用。

学霸图书馆（www.xuebalib.com）是一个“整合众多图书馆数据库资源，
提供一站式文献检索和下载服务”的24小时在线不限IP图书馆。
图书馆致力于便利、促进学习与科研，提供最强文献下载服务。

图书馆导航：
图书馆首页  文献云下载  图书馆入口  外文数据库大全  疑难文献辅助工具