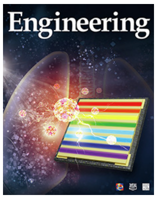
Engineering 17 (2022) 220–231

Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng



Research
Cyber Technology—Article

Dynamic Spectrum Control-Assisted Secure and Efficient Transmission Scheme in Heterogeneous Cellular Networks

Chenxi Li [a], Lei Guan [a,*], Huaqing Wu [b], Nan Cheng [a], Zan Li [a,c,*], Xuemin (Sherman) Shen [b]

[a] State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China
[b] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada
[c] Collaborative Innovation Center of Information Sensing and Understanding, Xi'an 710071, China

ARTICLE INFO

Article history:
Received 10 November 2020
Revised 27 February 2021
Accepted 14 April 2021
Available online 30 June 2021

Keywords:
Heterogeneous cellular networks
Dynamic spectrum control
Transmission security
Efficient data transmission

ABSTRACT

Heterogeneous cellular networks (HCNs) are envisioned as a promising architecture to provide seamless wireless coverage and increase network capacity. However, the densified multi-tier network architecture introduces excessive intra- and cross-tier interference and makes HCNs vulnerable to eavesdropping attacks. In this article, a dynamic spectrum control (DSC)-assisted transmission scheme is proposed for HCNs to strengthen network security and increase the network capacity. Specifically, the proposed DSC-assisted transmission scheme leverages the idea of block cryptography to generate sequence families, which represent the transmission decisions, by performing iterative and orthogonal sequence transformations. Based on the sequence families, multiple users can dynamically occupy different frequency slots for data transmission simultaneously. In addition, the collision probability of the data transmission is analyzed, which results in closed-form expressions of the reliable transmission probability and the secrecy probability. Then, the upper and lower bounds of network capacity are further derived with given requirements on the reliable and secure transmission probabilities. Simulation results demonstrate that the proposed DSC-assisted scheme can outperform the benchmark scheme in terms of security performance. Finally, the impacts of key factors in the proposed DSC-assisted scheme on the network capacity and security are evaluated and discussed.

1. Introduction

To support the surging growth of wireless data traffic while meeting the requirements for high data rates in next-generation cellular networks, heterogeneous cellular networks (HCNs) are emerging as a promising solution to enable a significant leap in network performance [1–4]. By densely deploying hierarchical infrastructure in different tiers (i.e., macro base stations (MBSs), micro base stations (mBSs), pico base stations (BSs), femto base stations, and relays) and permitting them to transmit information simultaneously over the same spectrum band, the HCNs are capable of achieving seamless coverage and accommodating more users. Motivated by the great potential, the investigation of the HCNs has received substantial interest [5–7].

Despite the benefits brought by HCNs, there are some challenging issues that should be further investigated. On the one hand, there are massive communication terminals coexisting in different tiers of HCNs and sharing limited spectrum resources. Therefore, unlike conventional single-tier cellular networks where data transmission is hampered mainly by malicious jamming, substantial intra- and inter-tier interference exists in HCNs, which reduces the success probability and reliability of data transmission. On the other hand, due to the open system architecture and the broadcast nature of radio propagation, confidential messages intended for authorized users are vulnerable to eavesdropping attacks.

Recent advances in interference and eavesdropping technologies in communication networks [8–12] further exacerbate the security risks in HCNs. Based on the report of risk-based security (RBS) in the third quarter of 2019 [13], there were 5183 data leakage events around the world in the first nine months of 2019. In view of the fact that wireless networks have been introduced into many fields (such as intelligent manufacturing [14], smart healthcare [15], and the Internet of Things [16,17]), the negative impact of data leakage on wireless network security has captured both industry and academia attention. When private information cannot

[*] Corresponding authors.
E-mail addresses: lguan@xidian.edu.cn (L. Guan), zanli@xidian.edu.cn (Z. Li).

https://doi.org/10.1016/j.eng.2021.04.019

be transmitted reliably and securely, serious consequences can occur, including property damage (e.g., disruption of industrial production chains, traffic congestion) and even personnel casualties (e.g., medical malpractice, traffic collisions).

Therefore, it is crucial to guarantee reliable and successful data transmission in HCNs while addressing interference and eavesdropping threats. However, the design of the transmission scheme is a daunting task in HCNs for the following reasons. First, the transmission scheme design should not only address the interference and eavesdropping threats but also improve the network capacity in HCNs. Considering the limited spectrum resources, dynamic spectrum control (DSC) is required to enable more authorized users to access HCNs without causing harmful interference. Second, to improve the security performance, authorized data transmission should occupy different frequency slots during the transmission period to make it intractable for eavesdroppers to intercept the transmitted information. Furthermore, reliable transmission and secure transmission probabilities should be analyzed and provided to evaluate the performance of the transmission scheme in HCNs.

1.1. Related work

In the literature, there are many studies on interference management and security enhancement [18–22]. Lv et al. [18] pioneered the study of physical layer security in downlink two-tier heterogeneous networks (HetNets) and optimized the secrecy rate performance by designing a beamforming scheme. Subsequently, Wang et al. [19] considered the randomness of the spatial location of network nodes and proposed a secrecy mobile association policy based on the access threshold, which provided a basic analytical framework to evaluate the secrecy performance of HCNs. Xu et al. [20] introduced cooperative multipoint transmission (CoMP) into the construction of HetNets to enhance the secured coverage probability. Inspired by the aforementioned methods, an interference-canceled opportunistic antenna selection (IC-OAS) scheme was proposed in Ref. [21] to improve the potential of the security–reliability tradeoff of macrocells and microcells. In Ref. [22], the secrecy energy efficiency (EE) was optimized by introducing artificial noise into orthogonal frequency division multiplexing (OFDM)-based cognitive radio networks with different base stations.

However, the aforementioned methods mainly focus on the security and interference issues of HCNs, while ignoring the ever-increasing wireless network traffic that should be handled by limited spectrum resources. In fact, the scarce spectrum resources available to support wireless communications services are underutilized. Therefore, it is essential to design an effective transmission scheme to improve the spectrum utilization efficiency and increase the network capacity of HCNs.

To mitigate spectrum scarcity in HCNs, some initiatives have been investigated in the past decade [23–26]. To improve the spectrum efficiency (SE) and EE under quality-of-service (QoS) constraints in multi-tier HetNets simultaneously, Rao and Fapojuwo [23] and Al Masri and Sesay [24] verified that traffic offloading is an effective approach. However, the performance gain brought by offloading is strongly affected by intra- and inter-tier interference. Yang et al. [25] pointed out that inter-tier interference is the main bottleneck for increasing network capacity in HetNets and proposed an F-ALOHA based cognitive spectrum access scheme for macro–femto HetNets. This scheme incorporated the idea of cross-tier spectrum access to offload traffic, thereby achieving interference management and optimization of SE. In addition, another spectrum flowing scheme that can trade or lease the licensed spectrum among tiers or network nodes to minimize spectrum holes was proposed in Ref. [26].

In summary, network capacity improvement and security enhancement have attracted substantial research interest. Although HCNs can effectively increase network capacity, the densified network architecture introduces cross-tier interference, which might further aggravate the threats to network security. The existing works focus either on network capacity improvement or transmission security enhancement in HCNs, failing to address both issues in HCNs. On the one hand, the aforementioned endeavors to cope with transmission security threats consume additional power and signal overhead, which might introduce extra interferences and hamper the network capacity performance. On the other hand, the existing approaches for increasing network capacity can effectively address the interferences in HCNs, but cannot overcome the threats of eavesdropping. To the best of our knowledge, there is no existing analysis of HCNs by jointly considering security and network performance. However, only by jointly considering the two performances together can HCNs meet the requirements of authorized users in real-world applications. This has motivated our work. In this work, we focus on the transmission scheme design in HCNs to effectively improve network capacity while guaranteeing security performance.

1.2. Main contributions

In this article, we propose a transmission scheme based on DSC for HCNs. By sensing the occupation status of the spectrum resources, the proposed scheme can generate a set of decisions by leveraging the idea of block cryptography and performing iterative and orthogonal operations. Based on these decisions, the data transmission can effectively occupy the idle frequency slots in each time slot. In addition, based on the analysis of the collision probability caused by multiple data packets occupying the same frequency slot in a time slot, the closed-form expressions of the reliable transmission probability (i.e., the data packets can be completely transmitted to authorized receivers) and secrecy probability (i.e., the data packets cannot be acquired by eavesdroppers) are derived from the idea of information-theoretic security [27]. Furthermore, under the constraints of reliable transmission probability and secrecy probability, the upper and lower bounds of network capacity can be determined. Therefore, by employing the DSC-assisted transmission scheme, the goal of strengthening the security and improving the network capacity of HCNs can be achieved. The main contributions of this article can be summarized as follows:

- We propose a DSC-assisted transmission scheme, which can guide the data packets to occupy the frequency slots in each time slot by generating orthogonal sequences. By scheduling communication links in an orderly manner, the proposed scheme can effectively reduce interference and make it more intractable for eavesdroppers to intercept transmitted privacy information.
- We theoretically analyze the collision probability of multiple data packets occupying the same frequency slot in a time slot, which provides the theoretical foundation for security and network capacity analysis in HCNs.
- We define the reliable transmission probability and secrecy probability of the proposed transmission scheme in HCNs and derive their closed-form expressions, which provides an analytical framework for evaluating the security performance of HCNs. Based on these two probabilities, the network capacity of HCNs under security constraints can be determined.
- We verify that the proposed DSC-assisted scheme can outperform the conventional secure transmission scheme in terms of security performance, which can be further improved by adjusting the network parameters. In addition, the maximum

number of users allowed to associate with HCNs can be adjusted according to the actual security requirements.

The remainder of this article is organized as follows. Section 2 depicts the system model. Then, the proposed DSC-assisted transmission scheme is presented in Section 3. Based on the proposed scheme, the security analysis in HCNs (including reliable transmission probability and secrecy probability) is conducted in Section 4. In Section 5, we evaluate the network capacity. After that, the simulation results are shown in Section 6, followed by the conclusion and future work in Section 7.

2. System model

Based on real-world application scenarios and the existing HCNs models [28–32], a typical multi-tier HCNs scenario is considered in this work as shown in Fig. 1. The HCNs consist of one MBS, multiple mBSs, several authorized users, and randomly located passive eavesdroppers. Let $\{\mathrm{BS}^{\varphi} \mid \varphi = (1, 2, \ldots, m, \mathrm{M})\}$ denote the base stations in the scenario with different clocks, where m is a positive integer representing the number of mBSs and M is a symbol representing the MBS. In addition, $\varphi \in \{1, 2, \ldots, m\}$ represents the mBS and φ = M refers to the MBS. These base stations are equipped with multiple antennas to support the communication of multiple authorized users simultaneously. In the considered HCNs scenario, the BS^{M} covers the entire network to form a macrocell and can serve authorized users with a high transmission power P_{BS} (from 5 to 40 W), where P_{BS} is the power of the BS^{M}. To handle the ever-growing traffic requirement and achieve seamless coverage, several BS^{m}s can be deployed within the macrocell. Different from the BS^{M}, BS^{m}s have smaller coverage radii and form multiple microcells that do not overlap with each other thus they can only serve the authorized users within their coverage areas with a lower transmission power P_{bs} (from 250 mW to 2 W), where P_{bs} is the power of the BS^{m}. Since it is almost impossible to accurately determine the instantaneous channel state information (CSI) of passive eavesdroppers in practice, only statistical CSI of the channels is available in our work, as assumed in many previous works [33–35]. Without loss of generality, we assume that each communication link in our constructed HCNs experiences independent flat Rayleigh fading such that the channel power gains are exponentially distributed. Specifically, the mean value of the channel power gain is $|h_{\mathrm{u}}|^2$ between the BS^{M} and authorized users, $|h_{\mathrm{e}}|^2$ between the BS^{M} and eavesdroppers, $|h_{\mathrm{mu}}|^2$ between the BS^{m} and authorized users, and $|h_{\mathrm{me}}|^2$ between the BS^{m} and eavesdroppers.

Specifically, we focus on the downlink transmission for the authorized users, where data packets are transmitted by the base stations independently over the shared transmission channel. Without loss of generality, the authorized users U_k (k = 1, 2, …, K) can choose to associate with the BS^{M} or BS^{m}s based on the signal-to-interference-plus-noise ratio (SINR) of downlinks in HCNs [36], where K is a positive integer representing the total number of the authorized users and k represents one of them.

As shown in Fig. 1, there are many potential threats affecting the transmission performance between base stations and users (e.g., unfriendly jammers, uncooperative interference, and malicious eavesdropping). Specifically, unfriendly jammers existing in the

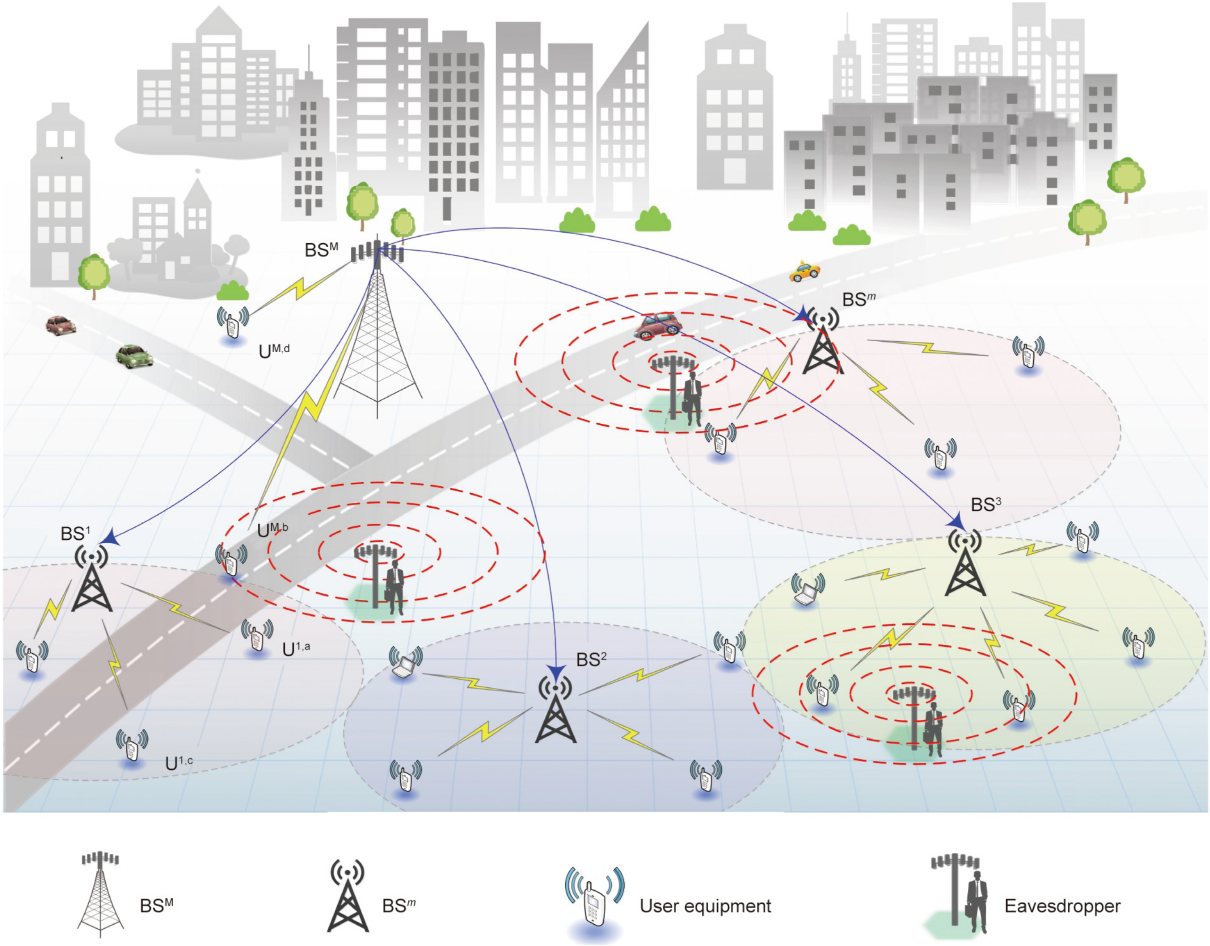


Fig. 1. Illustration of the HCNs. BS^{M}: MBS; BS^{m}: mBS; $\mathrm{U}^{\mathrm{M,d}}$: the authorized user d associated with the BS^{M}; $\mathrm{U}^{\mathrm{M,b}}$: the authorized user b associated with the BS^{M}; $\mathrm{U}^{1,\mathrm{a}}$: the authorized user a associated with the BS^{1}; $\mathrm{U}^{1,\mathrm{c}}$: the authorized user c associated with the BS^{1}.

service area might randomly send interference signals to occupy the transmission band, which reduces the quality of the communication link and even tamper with the transmitted information or interrupt communication. In addition, since the BS$^{\mathrm{M}}$ and BS^{m}s share the same frequency band, the signals transmitted by the BS$^{\mathrm{M}}$ are regarded as uncooperative interference for the authorized users in the BS^{m}s, and vice versa. Furthermore, considering the small geographical area covered by each BS^{m}, authorized users occupying the same frequency band served by the same BS^{m} can interfere with each other. However, the most malicious one is the eavesdroppers, as shown in Fig. 1, who can be randomly distributed and desire to intercept the privacy information transmitted by authorized users with the assistance of an energy detector (e.g., a radiometer).

3. DSC-assisted transmission scheme

To cope with the aforementioned threats effectively, an effective transmission scheme for assisting asynchronous networking is proposed in this section to strengthen the security of HCNs and facilitate the realization of superior network performance.

Without loss of generality, all authorized users transmit their data packets on a discrete-time channel with p time slots (t_1, t_2, ..., t_p), where p is a positive integer representing the total number of divided time slots, and t_p is the pth time slot. We assume that the transmitted data packets of authorized users in our considered HCNs need to occupy L consecutive time slots to complete their transmissions in each transmission period, where L represents the length of the transmitted data packets. Authorized users who desire to transmit information with a large data volume may require multiple transmission periods to complete the transmission of all information. In addition, to address the contradiction between the increasing number of authorized users and the limited spectrum resources, we divide the shared transmission bandwidth into q_0 non-overlapping frequency slots in advance, which constitute the set of frequency slots $F_0 = \{f_1, f_2, \ldots, f_{q_0}\}$, where q_0 is a positive integer representing the initial value of the divided frequency slots, and f_{q_0} denotes the q_0th frequency slot. Note that the frequency slots in F_0 cannot only be used by authorized users, but also be occupied by interference signals. Furthermore, considering that passive eavesdroppers can intercept data transmission, in the designed transmission scheme, every frequency slot can only be occupied by each user no more than once during a transmission period to make it intractable for eavesdroppers to decode the transmitted information. Therefore, we propose a DSC-assisted transmission scheme as follows to enhance the security of the network we are considering.

To tackle the negative impact of malicious interference, each base station leverages the spectrum sensing method within F_0 to determine the occupation status of each frequency slot in our proposed DSC-assisted transmission scheme. In recent decades, many refined spectrum sensing methods have been proposed [37–39], including spectrum sensing methods based on energy detection, eigenvalues, high-order cumulants (HOCs), and so forth. Here, we choose the HOCs-based spectrum sensing method to provide us with the occupation status of each frequency slot, since this method can extract a non-Gaussian signal from Gaussian noise even when the noise is colored and eliminate the adverse effects of noise power uncertainty in practical applications. According to the sensing results, the status of the frequency slots (P) can be expressed as $P = \{P_{f_j} \mid j = 1, 2, \ldots, q_0\}$, where j is the number of the frequency slots, the P_{f_j} represents the status of the jth frequency slot and $P_{f_j} \in\{0,1\}$. If $P_{f_j} = 1$, the jth frequency slot f_j is already occupied, otherwise frequency slot f_j can be accessed. Finally, the base station can remove the interfered frequency slots from F_0 and acquire the set of available frequency slots F_{s} with q frequency slots, where q indicates the number of idle frequency slots. Consequently, the BS$^{\varphi}$ should select and allocate frequency slots from F_{s} for the authorized users to ensure secure and reliable data transmission over a transmission period (t_1–t_p). The detailed procedure of determining F_{s} is described in Algorithm 1.

Algorithm 1. Principles of available frequency slots.

```
Input: Number of frequency slots $q_0$
1. Generate a set of frequency slots $F_0$
2. Determine the status of the entire frequency slots $P = \{P_{f1}, P_{f2}, \ldots, P_{fq_0}\}$, $P_{f_j} \in\{0,1\}$, by leveraging the spectrum sensing method
3. If $P_{f_j} = 1$, the $f_j$th frequency slot is occupied by interference, otherwise $f_j$ is available
4. Remove the set of the occupied frequency slots $F_{\mathrm{I}} = \{f_j \mid P_{f_j} = 1\}$ from $F_0$
5. Update the set of frequency slots $F_0$ and the number of frequency slots
Output: The available frequency slots $F_{\mathrm{s}}$ with $q$ frequency slots
```

In the considered HCNs, each BS$^{\varphi}$ can provide guidance for its local users to select which frequency slots to occupy in each time slot, thus completing data packet transmission successfully in an orderly manner. Let $U^{\varphi,k}$ denote user U_k, which is served by BS$^{\varphi}$. Thus, the frequency slots occupied by $U^{\varphi,k}$ during a transmission period can be presented by a DSC sequence $\boldsymbol{x}^{\varphi,k} = \{x_i^{\varphi,k} \mid i = 1, 2, \ldots, p\}$, where $x_i^{\varphi,k} \in \{f_j \mid j = 1, 2, \ldots, q\}$ represents the user $U^{\varphi,k}$ should occupy the jth frequency slot over the ith time slot to complete the packet transmission. Fig. 2 gives an example of the transmission decisions of $\mathrm{U_a}$ associated with BS^1 ($\boldsymbol{x}^{1,\mathrm{a}}$) and $\mathrm{U_b}$ associated with BS$^{\mathrm{M}}$ ($\boldsymbol{x}^{\mathrm{M,b}}$) obtained by the proposed DSC-assisted scheme. As shown in Fig. 2, the DSC-assisted transmission scheme provides a sequence $\boldsymbol{x}^{1,\mathrm{a}} = \{f_3, f_1, f_q, f_5, f_2, \ldots, f_4\}$ for $\mathrm{U}^{1,\mathrm{a}}$ associated with BS^1, and a sequence $\boldsymbol{x}^{\mathrm{M,b}} = \{f_3, f_1, f_4, f_1, f_q, \ldots, f_5\}$ for $\mathrm{U}^{\mathrm{M,b}}$ controlled by BS$^{\mathrm{M}}$.

In the following, we propose a DSC-assisted transmission scheme that can be dynamically adjusted based on the spectrum sensing results with superior security performance. The DSC-assisted transmission scheme can generate a family of DSC sequences to represent the transmission decisions of the authorized users. With the proposed scheme, multiple authorized users can receive the data packets reliably during the same period and the possibility for passive eavesdroppers to decipher the transmission scheme is reduced, thereby achieving the goal of secure communication for authorized users. The procedures of generating the proposed DSC-assisted transmission scheme can be summarized in Algorithm 2.

Algorithm 2. The proposed DSC-assisted transmission scheme.

```
Input: The set of available frequency slots $F_{\mathrm{s}}$, the number of available frequency slots $q$
1. For $i = 1, 2, \ldots, p$
2.     Generate a basic sequence family ($\boldsymbol{Z}^{\varphi,k}$) for $k$ authorized users $\boldsymbol{Z}^{\varphi,k} = \{z_i^{\varphi,k} | k = 1, 2, \ldots, K\}$ based on the block cryptography
3.     Upon applying $s_i^{\varphi,k} = (s_{i-1}^{\varphi,k} + z_i^{\varphi,k} + i)\mathrm{mod}(q)$, acquire the sequence family $\boldsymbol{S}^{\varphi,k} = \{s_i^{\varphi,k}\}$
4.     If the frequency slots $s_i^{\varphi,k}$ and $s_i^{\varphi,w}$ occupied by user $U_k$ and user $U_w$ associated with BS$^{\varphi}$ in the $i$th time slot satisfies $s_i^{\varphi,k} = s_i^{\varphi,w}$ (the authorized user $w = 1, 2, \ldots, K$; $w \neq k$), let $x_i^{\varphi,k} = (s_i^{\varphi,k} + r_i)\mathrm{mod}(q)$, where the orthogonal transformation factor $r_i = \min(r | (s_i^{\varphi,k} + r)\mathrm{mod}(q) \neq s_i^{\varphi,w})$, otherwise, $x_i^{\varphi,k} = s_i^{\varphi,k}$
5. End for
Output: The DSC sequence family $\boldsymbol{X}^{\varphi,k} = \{\boldsymbol{x}^{\varphi,k}; k = 1, 2, \ldots, K\}$
```

Specifically, the detailed steps are as follows:

- **Generate a basic sequence:** A random basic sequence $\boldsymbol{Z}^{\varphi,0}$ = $\{z_i^{\varphi,0}|\ i = 1, 2, \ldots, p\}$ for an authorized user $U^{\varphi,0}$ should be generated by the time of day (TOD) series t_i ($i = 1, 2, \ldots, p$) and the identification of the user's key. $z_i^{\varphi,0} = f_j$ ($j\in\{1, 2, \ldots, q\}$) represents that $U^{\varphi,0}$ occupies the f_jth frequency slot to transmit its data packet at the ith time slot. To simultaneously provide $k\in(1, 2, \ldots, K)$ users with transmission decisions that are hard to crack by the passive eavesdroppers, this basic sequence should be extended into a group containing k sequences.
- **Expanding the basic sequence by iterative operations:** In light of the block cipher algorithm [40], the initial iteration factor $P_i^{\varphi,0}$ which generates $Z_i^{\varphi,0}$ is iterated for k rounds as $P_i^{\varphi,k} = P_i^{\varphi,k-1} \oplus \mathrm{key}_i \oplus \mathrm{box}_g(P_i^{\varphi,k-1})$, where $\oplus$ denotes the exclusive OR operation, key_i is the identification symbol of the authorized users associated with BS^{φ} in the ith time slot, and g ($g = 1, 2, 3, \ldots$) is the number of the iterative operation box. Therefore, a group of basic sequences $\boldsymbol{Z}^{\varphi,k} = \{Z_i^{\varphi,1}, Z_i^{\varphi,2}, \ldots, Z_i^{\varphi,k}|\ i = 1, 2, \ldots, p\}$ can be obtained as $Z_i^{\varphi,k} = P_{i1}^{\varphi,k} \oplus P_{i2}^{\varphi,k} \oplus \ldots \oplus P_{ij}^{\varphi,k}$. Then, comparing $Z_i^{\varphi,k} \in \boldsymbol{Z}^{\varphi,k}$ with the optimal decision threshold value can produce two different mappings. If $z_i^{\varphi,k}$ is less than the threshold value, $s_i^{\varphi,k} = z_i^{\varphi,k}$, otherwise $s_i^{\varphi,k} = (s_{i-1}^{\varphi,k} + z_i^{\varphi,k} \ + i)\mathrm{mod}(q)$. Therefore, $\boldsymbol{S}^{\varphi,k} = \{s_i^{\varphi,1}, s_i^{\varphi,2}, \ldots, s_i^{\varphi,k};\ i = 1, 2, \ldots, p\}$ can be acquired.
- **Orthogonalize the group of sequences:** When $s_i^{\varphi,k} = s_i^{\varphi,w}$ ($w = 1, 2, \ldots, K;\ w \neq k$), we can acquire $x_i^{\varphi,k} = (s_i^{\varphi,k} + r_i)\mathrm{mod}(q)$, where the orthogonal transformation factor $r_i = \min(r|(s_i^{\varphi,k} + r)\mathrm{mod}(q) \neq s_i^{\varphi,w})$, otherwise, $x_i^{\varphi,k} = s_i^{\varphi,k}$. Therefore, a DSC sequence family $\boldsymbol{X}^{\varphi,k} = \{\boldsymbol{x}^{\varphi,k};\ k = 1, 2, \ldots, K\}$ is obtained, where the sequence $\boldsymbol{x}^{\varphi,k}$ represents the frequency slots occupied by $U^{\varphi,k}$ to transmit data packets during the transmission period.

Based on the generated DSC sequence family $\boldsymbol{X}^{\varphi,k}$, authorized users can occupy idle frequency slots in each time slot. It is clear that authorized users in the same microcell can access this micronetwork synchronously under the control of the mBS. Since the clocks are different in diverse microcells, the users associated with different mBSs and the MBS access the shared spectrum resources asynchronously. As shown in Fig. 2, two authorized users in different communication cells ($\mathrm{U}^{1,\mathrm{a}}$ and $\mathrm{U}^{\mathrm{M,b}}$) transmit the data packet occupying L ($L \leq p \ll q$) consecutive time slots independently and randomly.

4. Security analysis of data transmission in HCNs

In this section, we conduct a theoretical analysis of the collision probability between two authorized users employing the DSC-assisted transmission scheme. Based on the analysis of the collision probability, we also derive the closed-form expressions of the probability that authorized users can reliably receive the transmitted data packets and the probability that the eavesdroppers cannot acquire the transmitted data packets.

4.1. Collision probability

Considering that the TODs of these communication cells are different, authorized users in the MBS and mBSs might occupy the same frequency slot simultaneously, which causes a collision and introduces transmission interference. We assume that the process

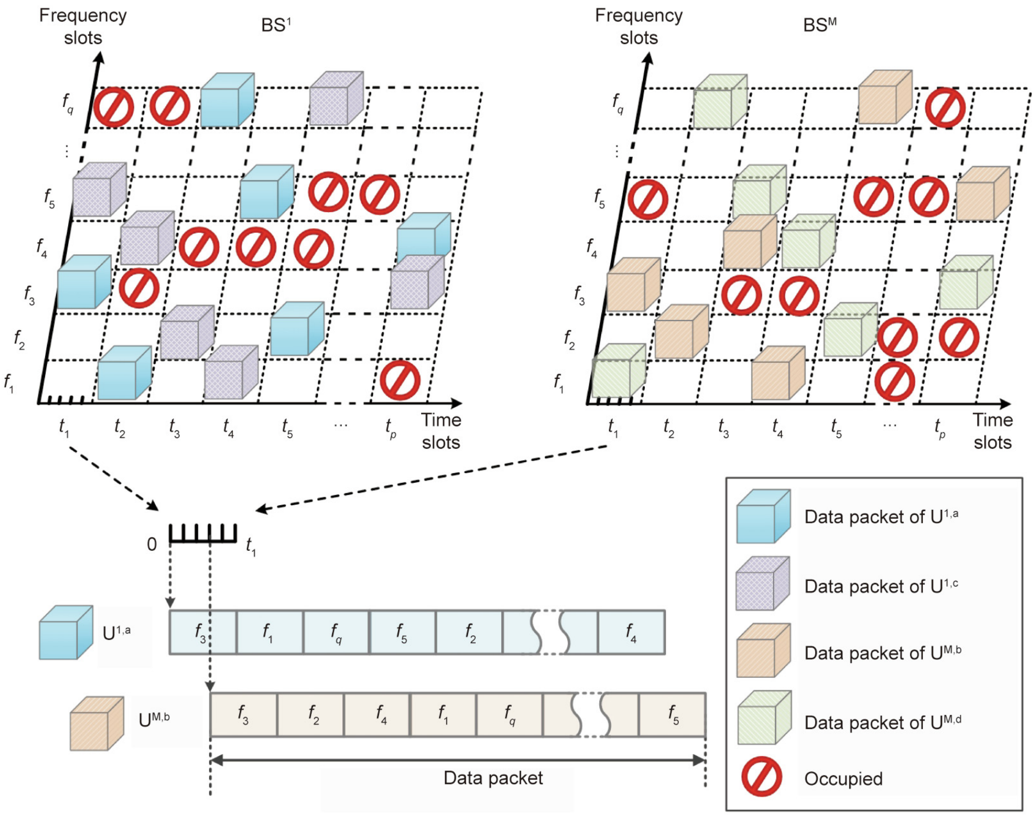


Fig. 2. Schematic diagram of the transmission scheme. f_q: the qth frequency slot.

of data packets arriving at the shared transmission channel follows a Poisson distribution with an arrival rate (G).

Consequently, the probability density function (PDF) of transmitting data packets n in L time slots can be presented by $f_{\mathrm{PDF}}(n)$.

$$f_{\mathrm{PDF}}(n) = \frac{G^n \mathrm{e}^{-G}}{n!} \tag{1}$$

Note that the interference caused by the authorized data transmission in the HCNs is much greater than the interference power of the background noise. Therefore, the collision probability of data transmission should be analyzed since it greatly affects the data transmission performance. In our constructed HCNs, the collision probability for an authorized user refers to the probability that the authorized user occupies the same frequency slot as others in the same time slot when transmitting data packets in this network. Note that with the proposed DSC-assisted transmission scheme, authorized users served by the same base station do not collide with each other following the orthogonal sequences. Therefore, the data transmitted by the MBS can only conflict with the data transmitted by the mBS. Furthermore, considering that the coverage areas of the mBSs do not overlap with each other, an authorized user served by an mBS can only conflict with the data transmission from the MBS. In the following, we analyze the collision probability between users $\mathrm{U}^{1,\mathrm{a}}$ (associated with BS^1) and $\mathrm{U}^{\mathrm{M,b}}$ (associated with the BS^{M}) when transmitting their data packets.

The data packet transmission processes of $\mathrm{U}^{1,\mathrm{a}}$ and $\mathrm{U}^{\mathrm{M,b}}$ that are located in the BS^1 cell are shown in Fig. 3. The symbols $x_i^{1,\mathrm{a}}$ (i = 1, 2, . . ., L) and $x_i^{\mathrm{M,b}}$ in Fig. 3 correspond to the frequency slots that are occupied by $\mathrm{U}^{1,\mathrm{a}}$ and $\mathrm{U}^{\mathrm{M,b}}$ at the ith time slot, respectively. Considering that the clocks of different cells are independent of each other, the data transmission start time of $\mathrm{U}^{\mathrm{M,b}}$ might not be aligned with that of $\mathrm{U}^{1,\mathrm{a}}$. As shown in Fig. 3, $\mathrm{U}^{\mathrm{M,b}}$ does not start transmitting until $\mathrm{U}^{1,\mathrm{a}}$ is about to complete the transmission task of the second time slot. We assume that there are l time slots overlapping between these two packets during the transmission period. In this case, during the data transmission period of $\mathrm{U}^{\mathrm{M,b}}$, every time slot t ($t_1 \le t \le t_{l-1}$) of $\mathrm{U}^{\mathrm{M,b}}$ overlaps with two consecutive time slots of $\mathrm{U}^{1,\mathrm{a}}$, the lth time slot of $\mathrm{U}^{\mathrm{M,b}}$ only overlaps with the Lth time slot of $\mathrm{U}^{1,\mathrm{a}}$, and the remaining time slots of $\mathrm{U}^{\mathrm{M,b}}$ do not overlap with $\mathrm{U}^{1,\mathrm{a}}$. It is worth noting that there is a special case where only the first time slot of $\mathrm{U}^{\mathrm{M,b}}$ overlaps with the last time slot of $\mathrm{U}^{1,\mathrm{a}}$.

Theorem 1: Given the set of available frequency slots F_s with q_s frequency slots, each available frequency slot f_j could be occupied by the authorized users with a probability of Pr ($x_i^{\varphi,k}$ = $f_j | i$ = 1, 2, . . ., L; j = 1, 2, . . ., q) If there are c time slots overlapping between two authorized users who access the HCNs asynchronously, when $P_1 = P_2 = \cdots = P_q = 1/q$, the maximum non-collision probability of these two users can be acquired, that is

$$\mathrm{Pr}_{\max}(l,q) = \left(1 - \frac{1}{q}\right)^{2l-1} \tag{2}$$

Proof: Without loss of generality, if two data packets occupy different frequency slots in each time slot, they can be regarded as not colliding. Considering that data transmission in different time slots is independent of each other, the non-collision probability of two data packets transmitted by $\mathrm{U}^{1,\mathrm{a}}$ and $\mathrm{U}^{\mathrm{M,b}}$ is

$$\begin{aligned}\mathrm{Pr}(\mathrm{U}^{1,\mathrm{a}}, \mathrm{U}^{\mathrm{M,b}}) = \prod_{r=1}^{l-1} \mathrm{Pr}\left(x_{L-l+r}^{1,\mathrm{a}} \neq x_r^{\mathrm{M,b}}, x_{L-l+r+1}^{1,\mathrm{a}} \neq x_r^{\mathrm{M,b}}\right)\cdot \\ \mathrm{Pr}\left(x_L^{1,\mathrm{a}} \neq x_l^{\mathrm{M,b}}\right)\end{aligned} \tag{3}$$

where $x_r^{\mathrm{M,b}}$ is the frequency slot occupied by the user $\mathrm{U_b}$ associated with BS^{M} in the rth time slot, and r is a real number that goes through 1 to $l - 1$. We assume that the probability of $\mathrm{U}^{\mathrm{M,b}}$ occupying the jth frequency slot in the rth time slot is $\mathrm{Pr}(x_r^{\mathrm{M,b}}$ = $f_j)$ = P_j.

Since the frequency slots occupied by $\mathrm{U}^{1,\mathrm{a}}$ in the t_{L-l+r}th time slot and the $t_{L-l+r+1}$th time slot are independent of each other, we can acquire that

$$\mathrm{Pr}\left(x_{L-l+r}^{1,\mathrm{a}} \neq f_j, x_{L-l+r+1}^{1,\mathrm{a}} \neq f_j\right) = (1 - P_j)^2 \tag{4}$$

Similarly, when $\mathrm{Pr}(x_l^{\mathrm{M,b}} = f_{\hat{j}} \big| \hat{j} = 1, 2, \ldots, q) = P_{\hat{j}}$, we can obtain that

$$\mathrm{Pr}\left(x_L^{1,\mathrm{a}} \neq x_l^{\mathrm{M,b}}\right) = 1 - P_{\hat{j}} \tag{5}$$

Considering that $\mathrm{U}^{\mathrm{M,b}}$ can randomly occupy one of the available frequency slots at the rth time slot and lth time slot, (i.e.,

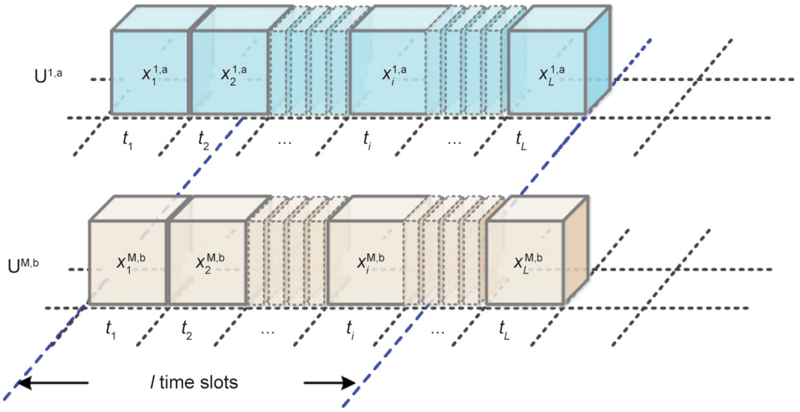


Fig. 3. Packet-transmission of $\mathrm{U}^{1,\mathrm{a}}$ and $\mathrm{U}^{\mathrm{M,b}}$. l: the number of overlapping time slots between two packets in a transmission period; $x_L^{1,\mathrm{a}}$: the frequency slot that is occupied by $\mathrm{U}^{1,\mathrm{a}}$ at the Lth time slot; $x_i^{1,\mathrm{a}}$: the frequency slot that is occupied by $\mathrm{U}^{1,\mathrm{a}}$ at the ith time slot; $x_L^{\mathrm{M,b}}$: the frequency slot that is occupied by $\mathrm{U}^{\mathrm{M,b}}$ at the Lth time slot; $x_i^{\mathrm{M,b}}$: the frequency slot that is occupied by $\mathrm{U}^{\mathrm{M,b}}$ at the ith time slot; t_L and t_i are the Lth and ith time slots, respectively.

$\sum_{j=1}^{q}\Pr(x_r^{\mathrm{M,b}}=f_j)=\sum_{\hat{j}=1}^{q}\Pr\left(x_l^{\mathrm{M,b}}=f_{\hat{j}}\right)=1$), with the aid of the condition probability formula and the classical theory of probability, we can obtain

$$\begin{aligned}&\Pr(\mathrm{U}^{1,\mathrm{a}},\mathrm{U}^{\mathrm{M,b}})\\&=\prod_{r=1}^{l-1}\sum_{j=1}^{q}\Pr\left(x_{L-l+r}^{1,\mathrm{a}}\neq f_j,x_{L-l+r+1}^{1,\mathrm{a}}\neq f_j|x_r^{\mathrm{M,b}}=f_j\right)\\&\quad\cdot\Pr(x_r^{\mathrm{M,b}}=f_j)\cdot\sum_{\widehat{j}=1}^{q}\Pr\left(x_L^{1,\mathrm{a}}\neq f_{\widehat{j}}\right)\Pr(x_l^{\mathrm{M,b}}=f_{\widehat{j}})\\&=\prod_{r=1}^{l-1}\sum_{j=1}^{q}(1-P_j)^2(P_j)\cdot\sum_{\widehat{j}=1}^{q}(1-P_{\widehat{j}})(P_{\widehat{j}})\\&=\left(\sum_{j=1}^{q}(1-P_j)^2(P_j)\right)^{l-1}\cdot\sum_{\widehat{j}=1}^{q}(1-P_{\widehat{j}})(P_{\widehat{j}})\end{aligned}\tag{6}$$

where $\sum_{j=1}^{q}P_j=\sum_{j=1}^{q}P_{\widehat{j}}=1,0\leq\{P_j,P_{\widehat{j}}\}\leq1$.

To obtain the maximum value of $\Pr(\mathrm{U}^{1,\mathrm{a}},\mathrm{U}^{\mathrm{M,b}})$, we formulate the Lagrangian multiplier expression $\mathscr{L}$.

$$\begin{aligned}&\mathscr{L}(\mathrm{U}^{1,\mathrm{a}},\mathrm{U}^{\mathrm{M,b}})\\&=\Pr(\mathrm{U}^{1,\mathrm{a}},\mathrm{U}^{\mathrm{M,b}})-\varepsilon g(q)\\&=\left(\sum_{j=1}^{q}(1-P_j)^2(P_j)\right)^{l-1}\cdot\sum_{j=1}^{q}(1-P_{\widehat{j}})(P_{\widehat{j}})-\varepsilon(1-\sum_{j=1}^{q}P_j)\end{aligned}\tag{7}$$

where ε is a real number representing the Lagrangian parameter; $g(\cdot)$ is a constraint function equal to zero.

Subsequently, we find the partial derivatives of $\mathscr{L}(\mathrm{U}^{1,\mathrm{a}},\mathrm{U}^{\mathrm{M,b}})$ with respect to P_1, P_2, …, P_q, ε, and set them equal to 0, then Eq. (8) can be acquired.

$$\begin{cases}\frac{\mathscr{L}}{\partial P_1}=(l-1)\left(\sum_{j=1}^{q}(1-P_j)^2(P_j)\right)^{l-2}\cdot\left(2(1-P_1)(P_1)+(1-P_1)^2\right)\\\quad\cdot\sum_{j=1}^{q}(1-P_j)\cdot(P_j)+\left(\sum_{j=1}^{q}(1-P_j)^2(P_j)\right)^{l-1}\cdot(1-2P_1)-\varepsilon=0\\\frac{\mathscr{L}}{\partial P_2}=(l-1)\left(\sum_{j=1}^{q}(1-P_j)^2(P_j)\right)^{l-2}\cdot\left(2(1-P_2)(P_2)+(1-P_2)^2\right)\\\quad\cdot\sum_{j=1}^{q}(1-P_j)\cdot(P_j)+\left(\sum_{j=1}^{q}(1-P_j)^2(P_j)\right)^{l-1}\cdot(1-2P_2)-\varepsilon=0\\\qquad\vdots\\\frac{\mathscr{L}}{\partial P_q}=(l-1)\left(\sum_{j=1}^{q}(1-P_j)^2(P_j)\right)^{l-2}\cdot\left(2(1-P_q)(P_q)+(1-P_q)^2\right)\\\quad\cdot\sum_{j=1}^{q}(1-P_j)\cdot(P_j)+\left(\sum_{j=1}^{q}(1-P_j)^2(P_j)\right)^{l-1}\cdot(1-2P_q)-\varepsilon=0\\\frac{\mathscr{L}}{\partial\varepsilon}=-1+\sum_{j=1}^{q}P_j=0\end{cases}\tag{8}$$

Since $0\leq\{P_j,P_{\widehat{j}}\}\leq1,\{j,\widehat{j}\}=1,2,...,q$, apparently only when $P_1=P_2=\ldots=P_q=1/q$ can $\Pr(\mathrm{U}^{1,\mathrm{a}},\ \mathrm{U}^{\mathrm{M,b}})$ obtain its maximum value. Therefore, the maximum value of the non-collision probability is Eq. (2).

Therefore, only when all the available frequency slots can be occupied by authorized users with equal probability, the maximum value of non-collision probability can be obtained.

Based on the Theorem 1, we analyze the probability that n data packets can be transmitted without collision in HCNs.

Theorem 2: Suppose that the authorized users in our constructed HCNs can occupy the frequency slots in F_s with equal probability $1/q$. When user $U^{\varphi,\tau}$ ($\tau\in\{1, 2, \ldots, K\}$) is transmitting a data packet, there are k ($k\leq K$) users that might collide with $U^{\varphi,\tau}$ (when φ = M, these k authorized users served by all the mBSs, when φ = 1, 2, …, m, these k authorized users served by the MBS). Hence, the probability that $U^{\varphi,\tau}$ transmits a data packet without collision during the L data transmission time slots is

$$\Pr(L,k,q)=\left(1-\frac{L}{q}\right)^k\tag{9}$$

Proof: Assume that the data transmission of authorized users $\mathrm{U}^{1,\mathrm{a}}$ and $\mathrm{U}^{\mathrm{M,b}}$ overlaps by l time slots. Since the process of the data packet arriving at the transmission channel follows the Poisson distribution, the probability for the authorized users transmitting the information at any time slot is equal. Accordingly, we can obtain that the probability of two data packets overlapping l time slots is

$$\Pr(l)=\Pr(l=1)=\Pr(l=2)=\ldots=\Pr(l=L)=\frac{1}{L}\tag{10}$$

Consequently, the probability of two authorized users transmitting data packets without collision is

$$P_1(L,q)=\sum_{l=1}^{L}\Pr_{\max}(l,q)\Pr(l)=\sum_{l=1}^{L}\left(1-\tfrac{1}{q}\right)^{2l-1}\cdot\tfrac{1}{L}\tag{11}$$

In our proposed DSC-assisted transmission scheme, the number of divided frequency slots should be controlled to be much larger than the number of time slots occupied for a data transmission, (i.e., $q\gg L$). By leveraging a Taylor series and ignoring the high-order term, the above Eq. (11) can be further expressed as

$$\begin{aligned}P_1(L,q)&=\tfrac{1}{L}\cdot\left(\left(1-\tfrac{1}{q}\right)+\left(1-\tfrac{1}{q}\right)^3+\ldots+\left(1-\tfrac{1}{q}\right)^{2L-1}\right)\\&\approx\tfrac{1}{L}\cdot\left(L-\tfrac{1}{q}-\tfrac{3}{q}-\cdots-\tfrac{2L-1}{q}\right)=1-\tfrac{L}{q}\end{aligned}\tag{12}$$

Hence, the non-collision probability between this data packet and all other k data packets is given by Eq. (9).

Two remarks can be derived from Theorem 2.

Remark 1: For a fixed k, $\Pr(L,k,q)$ is a power function of the ratio L/q, and this function monotonically decreases with increasing value of L/q.

Remark 2: For a fixed L/q, $\Pr(L,k,q)$ is an exponential function of k. In addition, since 0 < 1 − (L/q) < 1, $\Pr(L,k,q)$ decreases as k increases.

Corollary 1: Based on Theorem 2, the collision probability between $U^{\varphi,\tau}$ and k users in other base stations can be given by

$$\Pr_l=1-\Pr(L,k,q)=1-\left(1-\frac{L}{q}\right)^k\tag{13}$$

where $L\ll q$. With the aid of the Taylor series, Eq. (13) can be further expressed as

$$\Pr_l\approx1-\left(1-\frac{L\cdot k}{q}\right)=\frac{L\cdot k}{q}\tag{14}$$

4.2. Reliable transmission probability

In HCNs, the interference to the transmitted information mainly comes from three aspects: background noise (N_0), unauthorized malicious interference devices (I_{un}), and collisions between authorized users during data transmission (I_{c}). Therefore, the SINR of the authorized user ($\mathrm{SINR}_{\mathrm{u}}$) can be expressed as

$$\mathrm{SINR}_{\mathrm{u}} = \frac{P_{\mathrm{u}}}{I_{\mathrm{un,u}} + I_{\mathrm{c,u}} + N_0} \tag{15}$$

where P_{u} represents the power received by the authorized user from the associated BS, and $I_{\mathrm{c,u}}$ is the interference from other authorized users due to transmission collision. Note that the influence of unauthorized malicious interference devices on data packets transmitted by authorized users $I_{\mathrm{un,u}}$ can be avoided by Algorithm 1 (i.e., $I_{\mathrm{un,u}}$ = 0). Moreover, N_0 is characterized by a zero-mean, complex Gaussian random variable. Similarly, the SINR of the eavesdropper ($\mathrm{SINR}_{\mathrm{e}}$) can be presented by

$$\mathrm{SINR}_{\mathrm{e}} = \frac{P_{\mathrm{e}}}{I_{\mathrm{un,e}} + I_{\mathrm{c,e}} + N_0} \tag{16}$$

where P_{e} is the power of the data packet received by the eavesdropper, and $I_{\mathrm{c,e}}$ denotes the collisions between data packets transmitted within the observed frequency slots of the eavesdropper and other authorized transmitted data packets. The interference of unauthorized signals to the frequency slots observed by eavesdropper $I_{\mathrm{un,e}}$ = 0.

As Wyner demonstrated in pioneering work [27], to decode the received data packet, the SINR of the authorized user should be greater than the decoding threshold (δ_{u}). We define the probability that all transmitted information can be received by authorized users as the reliable transmission probability, which can be expressed as

$$P(\delta_{\mathrm{u}}) = \Pr(\min(\mathrm{SINR}_{\mathrm{u,BS}}) \geq \delta_{\mathrm{u}}) \tag{17}$$

where $\mathrm{SINR}_{\mathrm{u,BS}}$ is the SINR of the authorized user associated with the BS^{M}.

In the DSC-assisted scheme, the probability of the MBS occupying an available frequency slot ($f_j \in F_{\mathrm{s}};\ j = 1, 2, ..., q$) is $\Pr(f_j)$. Then, the power of desired data transmission received by the authorized user ($P_{\mathrm{u,BS}}$) can be expressed as

$$P_{\mathrm{u,BS}} = \frac{P_{\mathrm{BS}}}{\theta \cdot L} \sum_{l=1}^{L} \sum_{j=1}^{q} \Pr(f_j) g(\mathrm{u}, \mathrm{BS}) \tag{18}$$

where P_{BS} is the power of the BS^{M}, θ is the number of authorized users associated with the BS^{M}; $g(\mathrm{u,BS}) = |h_{\mathrm{u}\cdot f_j \cdot l}|^2$ denotes the channel gain between the BS^{M} and the authorized user at the lth time slot, which follows an exponential distribution with parameter α^2; u indicates the authorized users. In addition, the interference power caused by other authorized users occupying the same frequency slot is

$$I_{\mathrm{c,u}} = \sum_{\varphi=1}^{m} \frac{P_{\mathrm{BS}^{\varphi}}}{k \cdot L} \sum_{l=1}^{L} \sum_{f=1}^{q} \Pr_l \Pr(f_j) g(\mathrm{u}, \mathrm{BS}^{\varphi}) \tag{19}$$

where $P_{\mathrm{BS}^{\varphi}}$ ($\varphi = 1, 2, \ldots, m$) refers to the power of the mBSs. In addition, we assume g(u,bs)= $|h_{\mathrm{m_u} \cdot f_j \cdot l}|^2$ is the channel gain between the BS^{φ} and authorized user, which follows exponential distribution with parameter β_{φ}^2.

Upon substituting Eqs. (14), (18), and (19) into Eq. (15), the SINR of the authorized user can be rewritten as

$$\mathrm{SINR}_{\mathrm{u,BS}} = \frac{\frac{P_{\mathrm{BS}}}{\theta \cdot L} \sum_{l=1}^{L} \sum_{j=1}^{q} \Pr(f_j) \left| h_{\mathrm{u} \cdot f_j \cdot l} \right|^2}{\sum_{\varphi=1}^{m} P_{\mathrm{BS}^{\varphi}} \sum_{l=1}^{L} \sum_{j=1}^{q} \frac{1}{q} \Pr(f_j) \left| h_{\mathrm{m_u} \cdot f_j \cdot l} \right|^2 + N_0} \tag{20}$$

Based on Eq. (20), we can now derive the following proposition.

Proposition 1: The reliable transmission probability for an authorized user receiving the data packet from the MBS given by

$$P(\delta_{\mathrm{u}})_{\mathrm{BS}} = \left(\frac{(P_{\mathrm{BS}}/L)\alpha^2}{(P_{\mathrm{BS}}/L)\alpha^2 + P_{\mathrm{bs}} \theta \beta^2 \delta_{\mathrm{u}}/q} \right)^m \exp\left(-\frac{\delta_{\mathrm{u}} N_0 \theta L}{P_{\mathrm{BS}} \alpha^2} \right) \tag{21}$$

where P_{bs} indicates the power of the mBSs.

Proof: Please refer to the Appendix A.

Similarly, for an authorized user associated with mBS (BS^{φ}, φ = 1, 2, …, m), the reliable transmission probability can be expressed as

$$P(\delta_{\mathrm{u}})_{\mathrm{bs}} = \left(\frac{(P_{\mathrm{bs}}/L)\beta^2}{(P_{\mathrm{bs}}/L)\beta^2 + P_{\mathrm{BS}} \rho \alpha^2 \delta_{\mathrm{u}}/q} \right) \exp\left(-\frac{\delta_{\mathrm{u}} N_0 \rho L}{P_{\mathrm{bs}} \beta^2} \right) \tag{22}$$

where ρ refers to the number of users served by the mBSs.

4.3. Secrecy probability

To prevent passive eavesdroppers from decoding the information transmitted between authorized devices, the SINR of any eavesdroppers should be lower than the decoding threshold δ_{e}.

Accordingly, we define the probability that valid information cannot be obtained by any eavesdropper as the secrecy probability, for example,

$$P(\delta_{\mathrm{e}}) = \Pr(\max(\mathrm{SINR}_{\mathrm{e,BS}}) \leq \delta_{\mathrm{e}}) \tag{23}$$

where $\mathrm{SINR}_{\mathrm{e,BS}}$ is the SINR of the eavesdropper observing the signal transmitted by the BS^{M}.

Assume that eavesdroppers do not know the sequence family $\boldsymbol{X}^{\varphi,k}$, which is also the common case for most practical systems. Therefore, each eavesdropper associates a random frequency slot to intercept the transmitted data packet. Hence, when eavesdropping on the BS^{M} transmission, the total power of intercepted data packets by the eavesdropper U_{e} (P_{e}) and the inter-cell interference to U_{e} ($I_{\mathrm{c,e}}$) can be expressed as

$$\begin{aligned} P_{\mathrm{e}} &= \frac{P_{\mathrm{BS}}}{q \cdot \theta \cdot L} \sum_{l=1}^{L} g(\mathrm{e}, \mathrm{BS}) \\ I_{\mathrm{c,e}} &= \sum_{\varphi=1}^{m} \frac{P_{\mathrm{BS}\varphi}}{q \cdot k \cdot L} \sum_{l=1}^{L} \Pr_l g(\mathrm{e}, \mathrm{bs}) \end{aligned} \tag{24}$$

where e refers to the eavesdropper, the channel gain g(e,BS) = $|h_{\mathrm{e} \cdot f_j \cdot l}|^2$ between the eavesdropper and the MBS follows an exponential distribution with parameter λ^2. Similarly, the channel gain g(e,bs) = $|h_{\mathrm{m_e} \cdot f_j \cdot l}|^2$ between the eavesdropper and an mBS obeys an exponential distribution with parameter ω^2.

Substituting Eqs. (14) and (24) into Eq. (16), the SINR of eavesdropper can be rewritten as

$$\mathrm{SINR}_{\mathrm{e,BS}} = \frac{\frac{P_{\mathrm{BS}}}{q \cdot \theta \cdot L} \sum_{l=1}^{L} \left| h_{\mathrm{e} \cdot f_j \cdot l} \right|^2}{\sum_{\varphi=1}^{m} P_{\mathrm{bs}^{\varphi}} \sum_{l=1}^{L} \frac{1}{q^2} \left| h_{\mathrm{m_e} \cdot f_j \cdot l} \right|^2 + N_0} \tag{25}$$

With Eq. (25), we can derive the following proposition.

Proposition 2: The secrecy probability can be expressed as

$$P(\delta_{\mathrm{e}})_{\mathrm{BS}} = 1 - \left(\frac{(P_{\mathrm{BS}}/L)\lambda^2}{(P_{\mathrm{BS}}/L)\lambda^2 + P_{\mathrm{bs}} \theta \omega^2 \delta_{\mathrm{e}}/q} \right)^m \cdot \exp\left(-\frac{\delta_{\mathrm{e}} N_0 q \theta L}{P_{\mathrm{BS}} \lambda^2} \right) \tag{26}$$

Proof: Proposition 2 can be verified in a similar manner as Proposition 1, so that the detailed proof is omitted here.

For an authorized user associated with the MBS, the secrecy probability can be expressed as

$$P(\delta_{\mathrm{e}})_{\mathrm{bs}} = 1-\left(\frac{(P_{\mathrm{bs}}/L)\omega^2}{(P_{\mathrm{bs}}/L)\omega^2+P_{\mathrm{BS}}\rho\lambda^2\delta_{\mathrm{e}}/q}\right)\cdot\exp\left(-\frac{\delta_{\mathrm{e}}N_0q\rho L}{P_{\mathrm{bs}}\omega^2}\right) \tag{27}$$

5. Network capacity analysis

According to the analysis in Section 4, we can find that the reliable transmission probability and secrecy probability are both dependent on the number of users in the HCNs. Therefore, the upper and lower bounds on network capacity (i.e., the number of users that can be supported in the network) are derived in this section to guarantee reliable and secure data transmission probabilities.

5.1. Network capacity of the MBS

Assuming that $P_{\mathrm{r,min}}$ is the minimum required reliable transmission probability in HCNs, the following relationship can be obtained according to Proposition 1.

$$P_{\mathrm{r,min}} \le \left(\frac{(P_{\mathrm{BS}}/L)\alpha^2}{(P_{\mathrm{BS}}/L)\alpha^2+P_{\mathrm{bs}}\theta\beta^2\delta_{\mathrm{u}}/q}\right)^m\exp\left(-\frac{\delta_{\mathrm{u}}N_0\theta L}{P_{\mathrm{BS}}\alpha^2}\right) \tag{28}$$

that is

$$\ln\frac{P_{\mathrm{r,min}}}{\exp\left(-\frac{\delta_{\mathrm{u}}N_0\theta L}{P_{\mathrm{BS}}\alpha^2}\right)} \le m\cdot\ln\left(\frac{(P_{\mathrm{BS}}/L)\alpha^2}{(P_{\mathrm{BS}}/L)\alpha^2+P_{\mathrm{bs}}\theta\beta^2\delta_{\mathrm{u}}/q}\right)$$

$$\begin{aligned}
&\ln P_{\mathrm{r,min}}+\tfrac{\delta_{\mathrm{u}}N_0\theta L}{P_{\mathrm{BS}}\alpha^2}+m\cdot\ln\left(\tfrac{(P_{\mathrm{BS}}/L)\alpha^2+P_{\mathrm{bs}}\theta\beta^2\delta_{\mathrm{u}}/q}{(P_{\mathrm{BS}}/L)\alpha^2}\right)\le 0\\
&\tfrac{qN_0L}{P_{\mathrm{bs}}\beta^2P_{\mathrm{BS}}\alpha^2}\left(\tfrac{P_{\mathrm{BS}}}{L}\alpha^2+\tfrac{P_{\mathrm{bs}}\beta^2\delta_{\mathrm{u}}}{q}\cdot\theta\right)+m\cdot\ln(\tfrac{P_{\mathrm{BS}}}{L}\alpha^2+\tfrac{P_{\mathrm{bs}}\beta^2\delta_{\mathrm{u}}}{q}\cdot\theta)\\
&\quad+\ln\tfrac{P_{\mathrm{r,min}}}{\left((P_{\mathrm{BS}}/L)\alpha^2\right)^m}-\tfrac{qN_0}{P_{\mathrm{bs}}\beta^2}\le 0
\end{aligned} \tag{29}$$

By leveraging the Lambert-W function, which is the inverse of xe^x, we can obtain that the upper bound of the network capacity of the BS$^{\mathrm{M}}$ in HCNs is

$$\theta \le \frac{mP_{\mathrm{BS}}\alpha^2}{LN_0\delta_{\mathrm{u}}}W\left(\frac{qN_0L}{mP_{\mathrm{bs}}\beta^2P_{\mathrm{BS}}\alpha^2}\cdot\exp(-(\frac{\ln\frac{P_{\mathrm{r,min}}\cdot L^m}{(P_{\mathrm{BS}}\alpha^2)^m}-\frac{qN_0}{P_{\mathrm{bs}}\beta^2}}{m}))\right)-\frac{qP_{\mathrm{BS}}\alpha^2}{LP_{\mathrm{bs}}\beta^2\delta_{\mathrm{u}}} \tag{30}$$

where W is the Lambert-W function.

As long as the number of authorized users associated with the BS$^{\mathrm{M}}$ does not exceed the maximum capacity of this network, the data transmission can be successfully completed.

Similarly, when the HCNs are constrained by the minimum secrecy probability ($P_{\mathrm{s,min}}$), we can acquire the following relationship

$$P_{\mathrm{s,min}} \le P(\delta_{\mathrm{e}})_{\mathrm{BS}} = 1-\left(\tfrac{(P_{\mathrm{BS}}/L)\lambda^2}{(P_{\mathrm{BS}}/L)\lambda^2+P_{\mathrm{bs}}\theta\omega^2\delta_{\mathrm{e}}/q}\right)^m\cdot\exp\left(-\tfrac{\delta_{\mathrm{e}}N_0q\theta L}{P_{\mathrm{BS}}\lambda^2}\right) \tag{31}$$

that is

$$\begin{aligned}
&\ln(1-P_{\mathrm{s,min}})+\frac{\delta_{\mathrm{e}}N_0q\theta L}{P_{\mathrm{BS}}\lambda^2}+m\cdot\ln\left(\frac{(P_{\mathrm{BS}}/L)\lambda^2+P_{\mathrm{bs}}\theta\omega^2\delta_{\mathrm{e}}/q}{(P_{\mathrm{BS}}/L)\lambda^2}\right)\ge 0\\
&\frac{\delta_{\mathrm{e}}N_0qL}{P_{\mathrm{BS}}\lambda^2}\cdot\theta+m\cdot\ln\left(\frac{P_{\mathrm{BS}}\lambda^2}{L}+\frac{P_{\mathrm{bs}}\omega^2\delta_{\mathrm{e}}}{q}\cdot\theta\right)+\ln\left(\frac{1-P_{\mathrm{s,min}}}{\left((P_{\mathrm{BS}}/L)\lambda^2\right)^m}\right)\ge 0\\
&\frac{N_0q^2L}{P_{\mathrm{bs}}\omega^2P_{\mathrm{BS}}\lambda^2}\left(\frac{P_{\mathrm{BS}}\lambda^2}{L}+\frac{P_{\mathrm{bs}}\omega^2\delta_{\mathrm{e}}}{q}\cdot\theta\right)+m\cdot\ln(\frac{P_{\mathrm{BS}}\lambda^2}{L}+\frac{P_{\mathrm{bs}}\omega^2\delta_{\mathrm{e}}}{q}\cdot\theta)\\
&\quad+\ln\left(\frac{1-P_{\mathrm{s,min}}}{\left((P_{\mathrm{BS}}/L)\lambda^2\right)^m}\right)-\frac{N_0q^2}{P_{\mathrm{bs}}\omega^2}\ge 0
\end{aligned} \tag{32}$$

With the aid of the Lambert-W function, we can derive the lower bound of this macrocell network capacity in HCNs under the constraints of $P_{\mathrm{s,min}}$.

$$\begin{aligned}
\theta \ge{}& \frac{mP_{\mathrm{BS}}\lambda^2}{LN_0\delta_{\mathrm{e}}q}W\left(\frac{q^2N_0L}{mP_{\mathrm{BS}}\lambda^2P_{\mathrm{bs}}\omega^2}\cdot\exp\left(-\left(\frac{\ln\frac{1-P_{\mathrm{s,min}}}{\left((P_{\mathrm{BS}}/L)\lambda^2\right)^m}-\frac{N_0q^2}{P_{\mathrm{bs}}\omega^2}}{m}\right)\right)\right)\\
&-\frac{qP_{\mathrm{BS}}\lambda^2}{LP_{\mathrm{bs}}\omega^2\delta_{\mathrm{e}}}
\end{aligned} \tag{33}$$

Therefore, the number of authorized users associated with the BS$^{\mathrm{M}}$ should exceed the lower bound of the capacity to ensure that the data packets transmitted in the BS$^{\mathrm{M}}$ cannot be decrypted by the eavesdropper.

5.2. Network capacity of the mBSs

Similar to the analysis in Section 5.1, the network capacity of the mBSs can be obtained. The upper bound of the mBS network capacity is

$$\rho \le \frac{P_{\mathrm{bs}}\beta^2}{LN_0\delta_{\mathrm{u}}}W\left(\frac{qN_0L}{P_{\mathrm{BS}}\alpha^2P_{\mathrm{bs}}\beta^2}\cdot\exp(-(\ln\frac{P_{\mathrm{r,min}}\cdot L}{(P_{\mathrm{bs}}\beta^2)}-\frac{qN_0}{P_{\mathrm{BS}}\alpha^2}))\right)-\frac{qP_{\mathrm{bs}}\beta^2}{LP_{\mathrm{BS}}\alpha^2\delta_{\mathrm{u}}} \tag{34}$$

and the lower bound of the micro cell network capacity is

$$\rho \ge \tfrac{P_{\mathrm{bs}}\omega^2}{LN_0\delta_{\mathrm{e}}q}W\left(\tfrac{q^2N_0L}{P_{\mathrm{bs}}\omega^2P_{\mathrm{BS}}\lambda^2}\cdot\exp(-(\ln\tfrac{1-P_{\mathrm{s,min}}}{\left((P_{\mathrm{bs}}/L)\omega^2\right)}-\tfrac{N_0q^2}{P_{\mathrm{BS}}\lambda^2}))\right)-\tfrac{qP_{\mathrm{bs}}\omega^2}{LP_{\mathrm{BS}}\lambda^2\delta_{\mathrm{e}}} \tag{35}$$

To this end, the upper and lower bounds of the number of authorized users allowed to access the network can be obtained according to the requirements of the actual application scenarios for the reliable transmission probability $P_{\mathrm{r,min}}$ and secrecy probability $P_{\mathrm{s,min}}$ of the HCNs. Therefore, by reasonably limiting the number of users accessing the network, the goal of effectively increasing the possibility of multiple users successfully transmitting data packets in the same transmission period while reducing the possibility of eavesdropping can be achieved.

6. Numerical results

In this section, we present simulation results to validate our theoretical analysis of the security and network capacity of HCNs. Moreover, we compare the proposed DSC-assisted transmission scheme with a benchmark scheme to demonstrate the effectiveness of the proposed scheme.

6.1. Simulation configurations

We consider a two-tier HCNs scenario, which consists of one MBS, and ten mBSs. Additionally, there are ten passive eavesdroppers were randomly distributed in our constructed HCNs. The powers of the MBS and the mBS are P_{BS} = 43 decibel relative to one milliwatt (dBm)) and P_{bs} = 30 dBm, respectively. The parameter of average channel gain between the MBS and the authorized user is α^2 = 5, for the channel between the MBS and the eavesdropper, it is λ^2 = 3. Similarly, for the mBSs, the parameter of average channel gain for the authorized user is β^2 = 2, and for the eavesdropper is ω^2 = 1. In addition, the bandwidth of the shared transmission channel is set to 300 MHz. Unless otherwise specified, all of the results in this section are obtained with the above parameter settings.

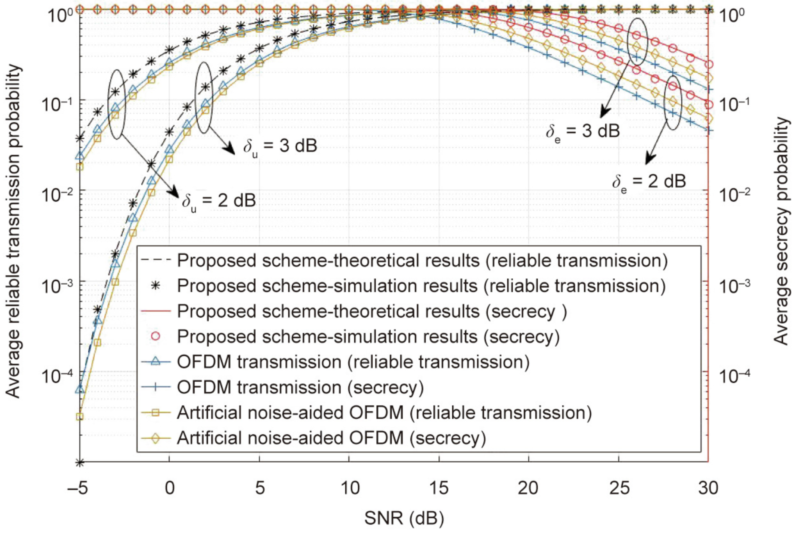


Fig. 4. Average reliable transmission and average secrecy probabilities vary with the SNR when q = 128 and L = 8. dB: decibel.

6.2. Security performance evaluation

(1) **Different SINR thresholds δ_u and δ_e:** Fig. 4 shows the average reliable transmission probability and the secrecy probability with different signal-to-noise ratios (SNRs) when q and L are equal to 128 and 8, respectively. From the figure, we can find that

- The probability of reliable transmission increases with increasing SNR, while the secrecy probability decreases approximately linearly. This phenomenon is especially obvious when the SNR is in the range from −5 to 10 decibel (dB). This demonstrates that with the assistance of our proposed DSC-assisted transmission scheme, when the communication environment improves, the possibility of reliable transmission can increase rapidly, while the possibility of eavesdroppers intercepting the information also slightly increases.
- When the decoding thresholds δ_u and δ_e increase from 2 to 3, the probability of reliable transmission decreases, while the secrecy probability increases. This shows that with stricter requirements on the channel conditions for successful data transmission, HCNs become more vulnerable to security threats.
- We compare our proposed scheme with a conventional OFDM transmission method and an artificial noise-aided OFDM method [22]. The conventional OFDM transmission scheme aims to improve the resource utilization efficiency and achieve better network performance. Based on the conventional OFDM transmission scheme, the artificial noise-aided OFDM scheme introduces artificial noise to combat eavesdropping and enhance network security. We can find from the simulation results that the proposed DSC-assisted scheme can obtain the highest reliable transmission probability and secrecy probability. Furthermore, the proposed scheme does not introduce additional signal sources or require knowledge of the location of authorized users in advance. Therefore, it consumes less transmission power than the artificial noise-aided OFDM method and has a lower implementation complexity than the other two schemes.
- The theoretical results match well with the simulation results as shown in Fig. 4, which confirms the correctness of our theoretical analysis. In the following, we use theoretical results to evaluate the impact of different parameters on the performance of the proposed scheme.

(2) **Impacts of L and q on the reliable transmission probability:** Fig. 5 demonstrates the influence of the time slot number L and the frequency slot number q on the average reliable transmission probability of the HCNs. The decoding threshold of the transmission link between the BSs and authorized users δ_u is 3. When each data transmission occupies L = 8 time slots, the reliable transmission probability increases as q increases. This is because dividing more frequency slots can effectively reduce the collision possibility among the data transmissions, leading to less co-channel interference among authorized users. In other words, it enhances the probability that the data packets can be successfully transmitted. However, when the available frequency slots number q is 128, as L increases, the reliable transmission probability decreases. The reason is that, with more time slots required for one data transmission, the collision probability increases with more co-channel interference.

(3) **Impacts of L and q on the secrecy probability:** We obtain the average secrecy probability curves in Fig. 6 with δ_e = 3. Different from the results in Fig. 5, the secrecy probability decreases with increasing SNR. Moreover, from Fig. 6, it is clear that the secrecy probability increases with a large L, when q is fixed. Once L is determined, the secrecy probability also increases as q increases. By utilizing the DSC-assisted transmission scheme, the eavesdropper has no idea which frequency slot is occupied for target data transmission in each time slot. If the eavesdropper always monitors one or several available frequency slots, it can only receive data fragments from different data packet transmissions. Since each data packet transmission occupies different frequency slots at different time slots, the eavesdropper has to successfully intercept all the data fragments to decode and obtain the entire data packet. With larger L and q, the eavesdropper needs to monitor more frequency slots for a longer time to obtain the complete data packet transmitted by the target authorized user. Therefore, with large L and q in the proposed DSC-assisted transmission scheme, it is difficult for the eavesdropper to decipher the transmitted data packets, leading to a high network security performance.

6.3. Network capacity evaluation

We examine the impacts of different parameter settings on the network capacity of the proposed scheme. Fig. 7 shows the

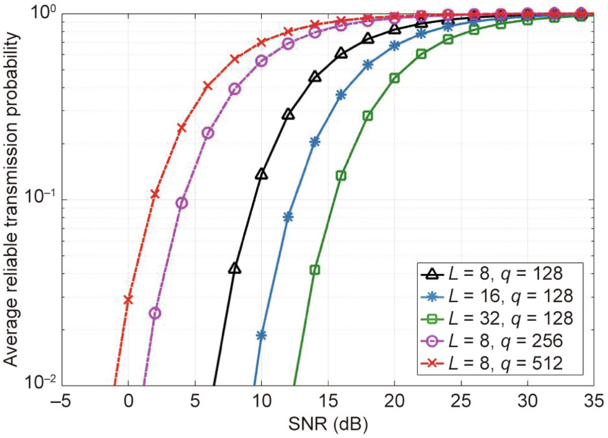


Fig. 5. Average reliable transmission probability variation with SNR under different L and q when $\delta_u = 3$.

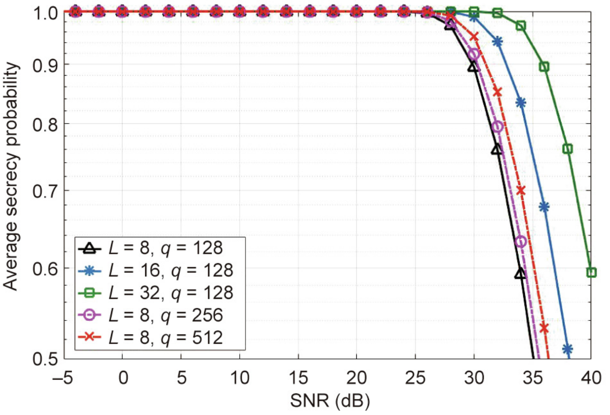


Fig. 6. Average secrecy transmission probability variation with SNR under different L and q when $\delta_e = 3$.

network capacity of the HCNs when $L = 8$, and $\delta_u = \delta_e = 2$. Fig. 7(a) shows that as the minimum required value of the reliable transmission probability increases, the upper bound of the network capacity slightly decreases. This is because when the requirement for the successful transmission of data packets becomes stricter, fewer users are allowed to access the network to reduce the collision probability between data packets transmitted over the limited spectrum resources. Fig. 7(b) reflects that as the minimum required value of secrecy probability increases, the lower bound of network capacity increases. To make it more difficult for eavesdroppers to obtain data packets in HCNs, the number of users accessing the network should increase to introduce more possibilities of frequency slot occupation at different time slots.

We can also find from Figs. 7(a) and (b) that, with a fixed $P_{r,\min}$ or $P_{s,\min}$, a larger q indicates that more authorized users can be allowed to access the network. Furthermore, according to our simulation, for the cases with q greater than 128, the lower bound of the network capacity falls below 0, which means that the secrecy requirements of the HCNs can always be guaranteed regardless of the number of users in the networks. The above observations allow us to conclude that with fixed requirements on reliable transmission probability and secrecy probability, the parameters of the DSC-assisted transmission scheme can be adjusted to accommodate more users for reliable and secure transmission.

7. Conclusions and future work

In this article, we have investigated the reliable and secure transmission problem in HCNs. Specifically, we have proposed a DSC-assisted transmission scheme to flexibly schedule the spectrum occupation for authorized data transmissions at different time slots. Moreover, we have also analyzed and derived closed-form expressions of the collision probability, reliable transmission probability, secrecy probability, and network capacity. By adopting the proposed scheme, limited spectrum resources can be efficiently utilized, and the parameters of the DSC-assisted scheme (e.g., L and q) can be flexibly adjusted to enhance network capacity while guaranteeing secure transmission. The scheme design and theoretical analysis in this work can provide useful guidance for future research on security enhancement of wireless networks. For our future work, we will introduce friendly interference sources and investigate source selection and power allocation to further improve the reliable and secure transmission probabilities.

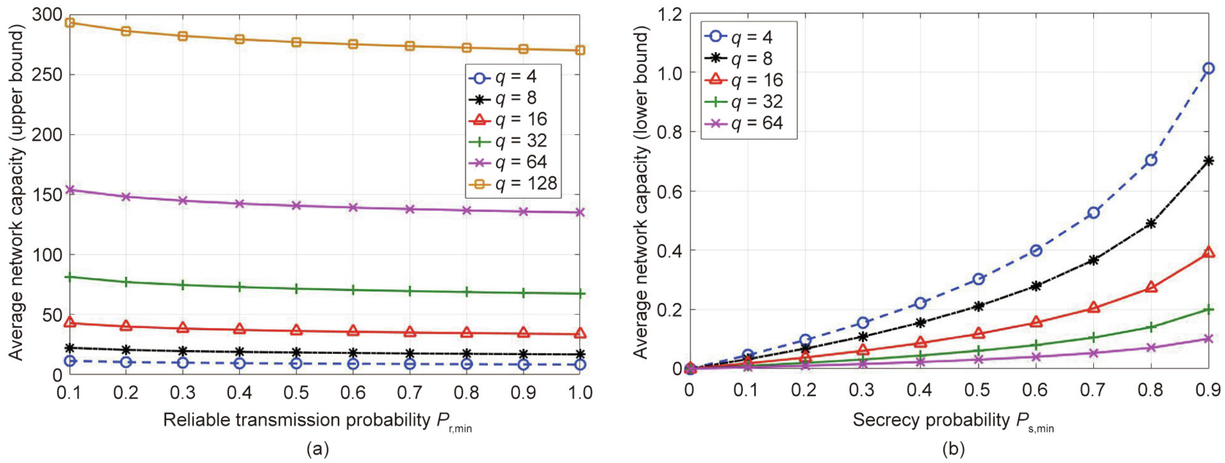


Fig. 7. Average network capacity variation with different requirements on reliable transmission probability and secrecy probability for $P_{BS} = 43$ dBm, $P_{bs} = 30$ dBm, $L = 8$, and $\delta_u = \delta_e = 2$. (a) The impact of the reliable transmission probability requirement on the upper bound of average network capacity with different values of q; (b) the impact of the secrecy probability requirement on the lower bound of average network capacity with different values of q.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61825104 and 91638204), the China Scholarship Council (CSC), the Natural Sciences and Engineering Research Council (NSERC) of Canada, and University Innovation Platform Project (2019921815KYPT009JC011).

Compliance with ethics guidelines

Chenxi Li, Lei Guan, Huaqing Wu, Nan Cheng, Zan Li, and Xuemin (Sherman) Shen declare that they have no conflicts of interest or financial conflicts to disclose.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.eng.2021.04.019.

References

[1] Giordani M, Polese M, Mezzavilla M, Rangan S, Zorzi M. Toward 6G networks: use cases and technologies. IEEE Commun Mag 2020;58(3):55–61.

[2] Chen S, Liang YC, Sun S, Kang S, Cheng W, Peng M. Vision, requirements, and technology trend of 6G: how to tackle the challenges of system coverage, capacity, user data-rate and movement speed. IEEE Wirel Commun 2020;27(2): 218–28.

[3] Zhuang W, Ye Q, Lyu F, Cheng N, Ren J. SDN/NFV-empowered future IoV with enhanced communication, computing, and caching. Proc IEEE 2020;108(2): 274–91.

[4] Wu H, Chen J, Xu W, Cheng N, Shi W, Wang L, et al. Delay-minimized edge caching in heterogeneous vehicular networks: a matching-based approach. IEEE Trans Wirel Commun 2020;19(10):6409–24.

[5] Zhou Z, Chen X, Zhang Y, Mumtaz S. Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks. IEEE Netw 2020;34(1):24–31.

[6] Tang W, Feng S, Ding Y, Liu Y. Physical layer security in heterogeneous networks with jammer selection and full-duplex users. IEEE Trans Wirel Commun 2017;16(12):7982–95.

[7] Zhou H, Cheng N, Yu Q, Shen XS, Shan D, Bai F. Toward multi-radio vehicular data piping for dynamic DSRC/TVWS spectrum sharing. IEEE J Sel Areas Commun 2016;34(10):2575–88.

[8] Zhang L, Ding G, Wu Q, Zou Y, Han Z, Wang J. Byzantine attack and defense in cognitive radio networks: a survey. IEEE Commun Surv Tutor 2015;17(3): 1342–63.

[9] Yang XN, Wang W, Xu XF, Pang GR, Zhang CL. Research on the construction of a novel cyberspace security ecosystem. Engineering 2018;4(1):47–52.

[10] Chen H, Hua J, Li F, Chen F, Wang D. Interference analysis in the asynchronous f-OFDM systems. IEEE Trans Commun 2019;67(5):3580–96.

[11] Xu G, Li H, Ren H, Yang K, Deng RH. Data security issues in deep learning: attacks, countermeasures, and opportunities. IEEE Commun Mag 2019;57(11): 116–22.

[12] Ren K, Zheng T, Qin Z, Liu X. Adversarial attacks and defenses in deep learning. Engineering 2020;6(3):346–60.

[13] Goddijn I, Kouns J. Data breach QuickView report 2019 Q3 trends. Technical report. Richmond: Risk Based Security, Inc.; 2019 Nov.

[14] Tao F, Qi Q, Wang L, Nee AYC. Digital twins and cyber–physical systems toward smart manufacturing and Industry 4.0: correlation and comparison. Engineering 2019;5(4):653–61.

[15] Cook DJ, Duncan G, Sprint G, Fritz RL. Using smart city technology to make healthcare smarter. Proc IEEE 2018;106(4):708–22.

[16] O'Neill M. Insecurity by design: today's IoT device security problem. Engineering 2016;2(1):48–9.

[17] Afzal MK, Zikria YB, Mumtaz S, Rayes A, Al-Dulaimi A, Guizani M. Unlocking 5G spectrum potential for intelligent IoT: opportunities, challenges, and solutions. IEEE Commun Mag 2018;56(10):92–3.

[18] Lv T, Gao H, Yang S. Secrecy transmit beamforming for heterogeneous networks. IEEE J Sel Areas Commun 2015;33(6):1154–70.

[19] Wang HM, Zheng TX, Yuan J, Towsley D, Lee MH. Physical layer security in heterogeneous cellular networks. IEEE Trans Commun 2016;64(3): 1204–19.

[20] Xu M, Tao X, Yang F, Wu H. Enhancing secured coverage with CoMP transmission in heterogeneous cellular networks. IEEE Commun Lett 2016;20(11):2272–5.

[21] Zou Y, Sun M, Zhu J, Guo H. Security–reliability tradeoff for distributed antenna systems in heterogeneous cellular networks. IEEE Trans Wirel Commun 2018;17(12):8444–56.

[22] Jiang Y, Zou Y, Ouyang J, Zhu J. Secrecy energy efficiency optimization for artificial noise aided physical-layer security in OFDM-based cognitive radio networks. IEEE Trans Veh Technol 2018;67(12):11858–72.

[23] Rao JB, Fapojuwo AO. Analysis of spectrum efficiency and energy efficiency of heterogeneous wireless networks with intra-/inter-RAT offloading. IEEE Trans Veh Technol 2015;64(7):3120–39.

[24] Al Masri MA, Sesay AB. Mobility-aware performance evaluation of heterogeneous wireless networks with traffic offloading. IEEE Trans Veh Technol 2016;65(10):8371–87.

[25] Yang L, Song SH, Letaief KB. Optimal overlay cognitive spectrum access with F-ALOHA in macro–femto heterogeneous networks. IEEE Trans Wirel Commun 2016;15(2):1323–35.

[26] Yang C, Li J, Guizani M, Anpalagan A, Elkashlan M. Advanced spectrum sharing in 5G cognitive heterogeneous networks. IEEE Wirel Commun 2016;23(2): 94–101.

[27] Wyner AD. The wire-tap channel. Bell Syst Tech J 1975;54(8):1355–87.

[28] Cheng N, Zhang N, Lu N, Shen X, Mark JW, Liu F. Opportunistic spectrum access for CR-VANETs: a game-theoretic approach. IEEE Trans Veh Technol 2014;63(1): 237–51.

[29] Li Z, Guan L, Li C, Radwan A. A secure intelligent spectrum control strategy for future THz mobile heterogeneous networks. IEEE Commun Mag 2018;56(6): 116–23.

[30] Jiang C, Chen Y, Liu KJR, Ren Y. Renewal-theoretical dynamic spectrum access in cognitive radio network with unknown primary behavior. IEEE J Sel Areas Commun 2013;31(3):406–16.

[31] Li X, Wang X, Li K, Han Z, Leung VCM. Collaborative multi-tier caching in heterogeneous networks: modeling, analysis, and design. IEEE Trans Wirel Commun 2017;16(10):6926–39.

[32] Li C, Li Z, Shi J, Guan L, Zhang L. Intelligent spectrum control in heterogeneous networks with high security capability. IEEE Wirel Commun Lett 2020;9(6): 830–3.

[33] Hu L, Wen H, Wu B, Tang J, Pan F, Liao RF. Cooperative jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers. IEEE Trans Veh Technol 2018;67(3):2108–17.

[34] Si J, Cheng Z, Li Z, Cheng J, Wang HM, Al-Dhahir N. Cooperative jamming for secure transmission with both active and passive eavesdroppers. IEEE Trans Commun 2020;68(9):5764–77.

[35] Kim KJ, Liu H, Wen M, Orlik PV, Poor HV. Secrecy performance analysis of distributed asynchronous cyclic delay diversity-based cooperative single carrier systems. IEEE Trans Commun 2020;68(5):2680–94.

[36] Jo HS, Sang YJ, Xia P, Andrews JG. Heterogeneous cellular networks with flexible cell association: a comprehensive downlink SINR analysis. IEEE Trans Wirel Commun 2012;11(10):3484–95.

[37] Yuan Q, Zhou H, Liu Z, Li J, Yang F, Shen X. CESense: cost-effective urban environment sensing in vehicular sensor networks. IEEE Trans Intell Transp Syst 2019;20(9):3235–46.

[38] Jiang C, Chen Y, Gao Y, Liu KJR. Joint spectrum sensing and access evolutionary game in cognitive radio networks. IEEE Trans Wirel Commun 2013;12(5): 2470–83.

[39] Wang D, Zhang N, Li Z, Gao F, Shen X. Leveraging high order cumulants for spectrum sensing and power recognition in cognitive radio networks. IEEE Trans Wirel Commun 2018;17(2):1298–310.

[40] Li Z, Chang Y, Jin L. A novel family of frequency hopping sequences for multi-hop bluetooth networks. IEEE Trans Consum Electron 2003;49 (4):1084–9.