Contents lists available at ScienceDirect

Engineering

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

Research
Cyber Technology—Article

基于频谱动态控制的异构蜂窝网络安全高效传输方案

李晨曦[a]，关磊[a,*]，吴华清[b]，承楠[a]，李赞[a,c,*]，沈学民[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

关键词
异构蜂窝网络
频谱动态控制
传输安全
高效数据传输

摘要

异构蜂窝网络（heterogeneous cellular network, HCN）是一种具有发展前景的结构，可以提供无缝无线覆盖并提高网络容量。然而，密集化的多层网络结构引入了过多的层内和层间干扰，使HCN容易受到窃听攻击。本文提出了一种基于频谱动态控制（dynamic spectrum control, DSC）的传输方案，用于加强HCN的网络安全并提高网络容量。该DSC辅助传输方案利用了分组加密的密码学思想，通过执行迭代和正交的序列变换生成代表传输决定的序列族。基于这些序列族，多位用户可以动态地占用不同频隙进行数据传输。此外，本文还分析了数据传输的碰撞概率，从而得出可靠传输概率和保密概率的解析表达式。然后，在给定可靠传输概率和安全传输概率的要求下，进一步得出了网络容量的上下限。仿真结果表明，本研究提出的DSC辅助方案在安全性能方面能够优于基准方案。最后，本文评估并讨论了DSC辅助方案中的关键因素对网络容量和安全性的影响。

1. 引言

为了应对不断增长的无线数据通信，同时满足下一代蜂窝网络对数据传输速率的高要求，异构蜂窝网络（HCN）作为一种前景广阔的解决方案，有望实现网络性能的重大飞跃[1–4]。通过密集部署不同层级的基础设施，即宏基站（macro base station, MBS）、微基站（micro base station, mBS）、皮基站（pico base station, PBS）、飞基站和中继站，并允许它们在同一频谱带上同时传输信息，HCN能够实现无缝覆盖并容纳更多用户。由于HCN潜力巨大，研究人员对HCN进行了大量的研究[5–7]。

尽管HCN的优势明显，但仍面临着一些挑战，有待进一步研究。一方面，有大量通信终端处于HCN的不同层级，共享有限的频谱资源。因此，与主要受恶意干扰的传统单层蜂窝网络不同，HCN中存在大量的层内和层间干扰，降低了数据传输的成功率和可靠性。另一方面，由于HCN采用开放的系统结构，并且无线电传输具有广播性质，发送给授权用户的机密信息容易受到窃听攻击。

通信网络干扰和窃听技术的发展[8–12]进一步加剧了HCN的安全风险。2019年第三季度基于风险的安全管理技术（risk-based security, RBS）的报道[13]指出，在2019年的前9个月，全球共有5183起数据泄露事件。鉴于无线

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

英文原文：Engineering 2022, 17(10): 220–231
引用本文：Chenxi Li, Lei Guan, Huaqing Wu, Nan Cheng, Zan Li, Xuemin (Sherman) Shen. Dynamic Spectrum Control-Assisted Secure and Efficient Transmission Scheme in Heterogeneous Cellular Networks. *Engineering*, https://doi.org/10.1016/j.eng.2021.04.019

网络已应用于许多领域（如智能制造[14]、智慧医疗[15]、物联网[16–17]），数据泄露对无线网络安全的负面影响已经引起业界和学术界的关注。无法安全可靠地传输私人信息会导致严重的后果，包括财产损失（如工业生产链中断、交通堵塞），甚至是人员伤亡（如医疗事故、交通事故）。

因此，在解决HCN受干扰和窃听威胁的同时，保证成功可靠的数据传输至关重要。然而，出于以下原因，设计HCN的传输方案是一项艰巨的任务。首先，设计的传输方案不仅要应对干扰和窃听威胁，还要提高HCN的网络容量。考虑频谱资源有限，本文需要采用频谱动态控制（DSC），在HCN中容纳更多授权用户的同时不造成有害干扰。其次，为了提高安全性能，授权数据的传输应在传输期间占据不同的频隙，使窃听者难以截获所传输的信息。此外，应分析并提供可靠传输和安全传输的概率，以评估HCN传输方案的性能。

1.1. 相关研究

文献中有许多解扰处理和增强安全性能的研究[18–22]。Lv等[18]率先研究了双层异构网络（heterogeneous network, HetNet）的下行链路的物理层安全，并通过设计波束成形方案优化了保密率。之后，Wang等[19]考虑网络节点空间位置的随机性，提出了基于接入阈值的保密移动关联策略，为评估HCN的保密性能提供了一个基本的分析框架。Xu等[20]在异构网络的构建中引入了多点协作传输（cooperative multipoint transmission, CoMP）的概念，以提高安全覆盖率。在上述方法的启发下，参考文献[21]提出了干扰消除机会天线选择（interference-canceled opportunistic antenna selection, IC-OAS）方案，从而提高宏基站和微基站在平衡安全与可靠性方面的潜力。参考文献[22]在不同基站的基于正交频分复用（orthogonal frequency division multiplexing, OFDM）的认知无线电网络中引入了人工噪声，以此优化能量效率（energy efficiency, EE）。

然而，上述方法主要聚焦于HCN面临的安全和干扰问题，却忽略了有限频谱资源需应对不断增长的无线网络流量。事实上，可支持无线通信服务的稀缺频谱资源并未得到充分利用。因此，为提高HCN中的频谱利用效率和网络容量，有必要设计一个有效的传输方案。

为了缓解HCN的频谱稀缺性，研究人员在过去十年间已经研究了一些方案[23–26]。为了在服务质量（quality-of-service, QoS）的约束下同时提高多层异构网络的频谱效率（spectrum efficiency, SE）和能效，Rao和Fapojuwo [23]以及Al Masri和Sesay [24]验证了流量卸载的有效性。然而，卸载带来的性能提升受到层内和层间干扰的强烈影响。Yang等[25]指出，层间干扰是提高异构网络容量的主要瓶颈，并基于F-ALOHA的认知频谱，提出了一个适用于宏-飞异构网络的接入方案。该方案采用跨层频谱接入的方式来卸载流量，以此抑制干扰并优化SE。此外，参考文献[26]还提出了另一种频谱流动方案，通过在各层或各网络节点之间交易或出租授权频谱以尽量减少频谱空洞。

综上所述，提高网络容量和安全性能已经引起了大量研究者的兴趣。尽管HCN可以有效提高网络容量，但密集的网络结构会引入跨层干扰，可能会进一步加剧网络安全面临的威胁。现有研究要么致力于提高HCN的网络容量，要么致力于加强HCN的传输安全，但未同时研究这两个问题。一方面，上述应对传输安全威胁的方法会造成额外的功率消耗和信号开销，还可能会引入额外干扰并影响网络容量性能。另一方面，用于提高网络容量的现有方法可以有效应对HCN中的干扰，但无法消除窃听威胁。目前还没有关于同时考虑安全性能和网络性能的HCN分析。只有同时考虑这两种性能，HCN才能在现实应用中满足授权用户的要求。本文重点研究了能够有效提高网络容量，同时保证安全性能的HCN传输方案设计。

1.2. 主要贡献

本文提出了一种基于DSC的HCN传输方案。通过检测频谱资源的占用状态，利用分块加密思想，通过迭代和正交序列来产生一组决策序列族。基于这些决策，数据传输可以有效占用每个时隙中的空闲频隙。而且，通过分析一个时隙中多个数据包占用同一频隙所造成的碰撞概率，该方案根据信息论安全的思想得出了可靠传输概率（即数据包能完整传输给授权接收者）和保密概率（即窃听者无法获取数据包）的解析表达式[27]。此外，在设定的可靠传输概率和保密概率下，可以确定网络容量的上限和下限。因此，采用该DSC辅助传输方案可以实现加强HCN安全性和提高网络容量的目标。本文的主要贡献可以概括为以下几点：

• 本研究提出了一种基于DSC的辅助传输方案，可以通过生成正交序列引导数据包占用每个时隙中的频隙。该方案通过有序调度通信链路来有效减少干扰，使窃听者较难截获所传输的隐私信息。

• 本研究从理论上分析了在一个时隙中占据同一频隙的多个数据包的碰撞概率，为HCN的安全性和网络容量分析提供了理论基础。

• 本研究定义了该HCN传输方案中的可靠传输概率和保密概率，并推导出两者的解析表达式，为HCN的安全性能评估提供了分析框架。根据这两个概率，可以确定在安全约束下的HCN网络容量。

• 本研究验证了该DSC辅助方案在安全性能方面胜过传统的安全传输方案，且安全性能可以通过调整网络参数进一步提高。此外，可以根据实际安全要求调整允许与HCN关联的最大用户数。

下文结构如下：第2节描述系统模型。第3节介绍DSC辅助传输方案。基于该方案，第4节开展了HCN的安全性分析（包括可靠传输概率和保密概率）。第5节评估了网络容量。第6节展示了仿真结果。最后，第7节进行了结论和未来研究展望。

2. 系统模型

基于现实中的应用场景和现有HCN模型[28–32]，本研究使用的是一个典型的多层HCN场景，如图1所示。该HCN由一个MBS、多个mBS、多位授权用户和随机分布的被动窃听者组成。$\{BS^{\varphi} \mid \varphi = (1, 2, \cdots, m, M)\}$代表在此场景中具有不同时钟的基站，其中$m$是代表mBS数量的正整数，M代表MBS。此外，$\varphi \in \{1, 2, \cdots, m\}$代表mBS，当$\varphi = M$时表示MBS。这些基站配备了多个天线，以支持多位授权用户同时通信。在此HCN场景中，BS^M覆盖整个网络，形成一个宏蜂窝小区，并能以高传输功率P_{BS}（5~40 W）服务授权用户，其中P_{BS}表示BS^M的功率。为了满足不断增长的流量需求并实现无缝覆盖，可以在宏蜂窝小区内部署多个BS^m。与BS^M不同的是，BS^m的覆盖半径较小，从而形成多个互不重叠的微蜂窝小区，因此它们只能以较低的发射功率P_{bs}（250 mW~2 W）为其覆盖范围内的授权用户服务，其中P_{bs}表示BS^m的功率。由于在实际情况下几乎不可能准确地确定被动窃听者的瞬时信道状态信息（CSI），因此和许多先前的研究[33–35]所假设的一样，本研究只有信道的统计CSI。在不失一般性的情况下，假设本文所构建的HCN中的每条通信链路都经历了独立的平坦瑞利衰落（flat Rayleigh fading），使信道功率增益呈指数分布。具体而言，BS^M和授权用户之间的信道功率增益平均值是$|h_u|^2$，BS^M和窃听者之间是$|h_e|^2$，BS^m和授权用户之间是$|h_{mu}|^2$，BS^m和窃听者之间是$|h_{me}|^2$。

本文关注授权用户的下行链路传输，其中数据包由基站在共享传输信道上独立传输。在不失一般性的情况下，授权用户U_k $(k = 1, 2, \cdots, K)$可以根据HCN中下行链路的信号与干扰加噪声比（signal-to-interference-plus-noise ratio, SINR）选择与BS^M或BS^m关联[36]，其中K代表授权用户的总数，k代表其中一位授权用户。

如图1所示，存在许多潜在威胁影响基站和用户之间传输性能（如恶意干扰器、无益干扰、恶意窃听）。服务区域内的恶意干扰器会随机发送干扰信号以占用传输频段，从而降低通信链路的质量，有时甚至会篡改传输信息或中断通信。此外，由于BS^M和BS^m共享同一频段，因此BS^M发射的信号对BS^m中的授权用户而言是无益干扰，反之亦然。再者，考虑每个BS^m覆盖的地理区域较小，同一BS^m中占用同一频段的授权用户会相互干扰。恶意最大的是窃听者。如图1所示，这些窃听者可以随机分布，在能量探测器（如辐射计）的帮助下截获授权用户传输的隐私信息。

3. DSC辅助传输方案

为了有效应对上述威胁，本节提出了一种辅助异步联网的有效传输方案，以加强HCN的安全性，加速实现卓越的网络性能。

在不失一般性的情况下，所有授权用户在一个具有p个时隙（$t_1, t_2, \cdots, t_p$）的离散时间信道上传输数据包，其中p代表所划分时隙的总数，是一个正整数，t_p表示第p个时隙。假设在所考虑的HCN中，授权用户所传输的数据包在每个传输期内需要占用L个连续的时隙来完成传输，其中L代表传输数据包的长度。想要传输大量数据信息的授权用户可能需要多个传输期才能完成所有信息的传输。此外，为了解决授权用户数量日益增加与有限频谱资源之间的矛盾，本文事先将共享的传输带宽划分为q_0个不重叠的频隙，构成频隙集（$F_0 = \{f_1, f_2, \cdots, f_{q_0}\}$）。其中$q_0$是代表所划分频隙初始值的正整数，$f_{q_0}$表示第$q_0$个频隙。注意，$F_0$中的频隙不能只限授权用户使用，它也会被干扰信号占据。此外，考虑被动窃听者可以拦截数据传输，在所设计的传输方案中，每位用户在每个传输期内占用一个频隙的次数不能超过一次，从而使窃听者难以破译所传输的信息。因此，本文提出了如下DSC辅助传输方案来增强此网络的安全性。

为了应对恶意干扰的负面影响，在提出的DSC辅助传输方案中，每个基站利用F_0内的频谱感知方法来确定每个频隙的占用情况。近几十年来，研究者提出了多种频谱感知方法[37–39]，包括基于能量检测、特征值、高阶累积量（high-order cumulant, HOC）的频谱感知方法。本文选择基于HOC的频谱感知方法来确定每个频隙的占用情况，因为即使是有色噪声，该方法也可以从高斯噪声中

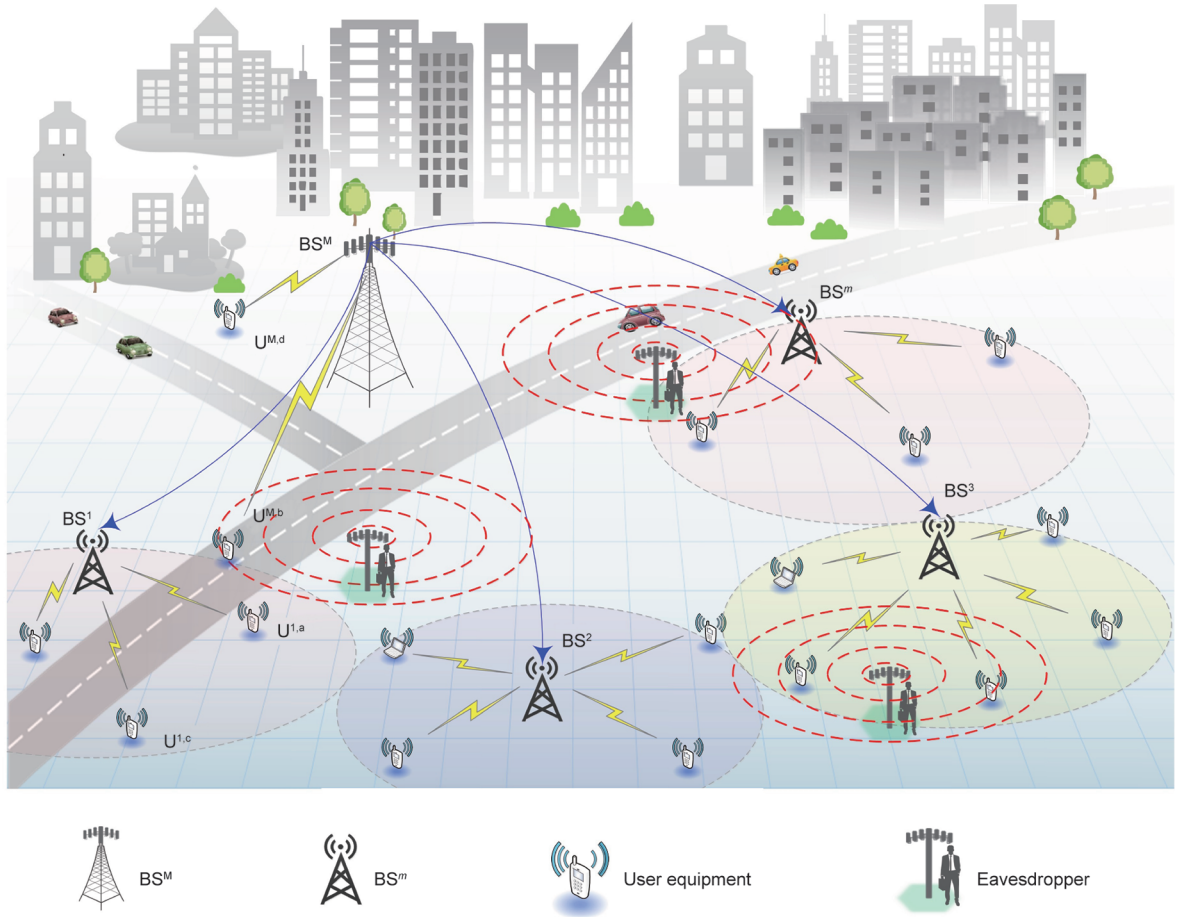

图1. HCN的图示。BS^M：MBS；BS^m：mBS；$U^{M,d}$：与BS^M关联的授权用户d；$U^{M,b}$：与BS^M关联的授权用户b；$U^{1,a}$：与BS^1关联的授权用户a；$U^{1,c}$：与BS^1关联的授权用户c。

提取非高斯信号，并在实际应用中消除不确定的噪声功率所带来的不利影响。根据感知结果，频隙状态（P）可以表示为$P = \{P_{f_j} \mid j = 1, 2, \ldots, q_0\}$，其中$j$是频隙的数量，$P_{f_j}$代表第$j$个频隙的状态，且$P_{f_j} \in \{0,1\}$。如果$P_{f_j} = 1$，说明第$j$个频隙$f_j$已经被占用，否则频隙$f_j$可以使用。基站可以从$F_0$中移除被干扰的频隙，获得有$q$个频隙的可用频隙集$F_s$，其中$q$表示空闲频隙的数量。因此，$BS^\varphi$应该从$F_s$中为授权用户选择并分配频隙，确保在传输期$t_1 - t_p$内安全可靠地传输数据。确定$F_s$的具体步骤如算法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_jth frequency slot is occupied by interference, otherwise f_j is available
4. Remove the set of the occupied frequency slots $F_1 = \{f_j \mid P_{f_j} = 1\}$ from F_0
5. Update the set of frequency slots F_0 and the number of frequency slots

Output: The available frequency slots F_s with q frequency slots

在所考虑的HCN中，每个BS^φ可以指导本地用户选择在每个时隙中占用哪些频隙，从而有序完成数据包传输。$U^{\varphi,k}$表示由BS^φ服务的用户U_k。因此，$U^{\varphi,k}$在一个传输期内所占用的频隙可以用DSC序列$\boldsymbol{x}^{\varphi,k} = \{x_i^{\varphi,k} \mid i = 1, 2, \ldots, p\}$表示，其中$x_i^{\varphi,k} \in \{f_j \mid j = 1, 2, \ldots, q\}$代表用户$U^{\varphi,k}$应该在第$i$个时隙占用第$j$个频隙完成数据包传输。图2给出了利用该DSC辅助方案得到的与BS^1 ($\boldsymbol{x}^{1,a}$)关联的U_a的传输决策，以及与BS^M ($\boldsymbol{x}^{M,b}$)关联的U_b的传输决策的示例。如图2所示，该DSC辅助传输方案为与BS^1关联的$U^{1,a}$提供了序列$\boldsymbol{x}^{1,a}$，$\boldsymbol{x}^{1,a} = \{f_3, f_1, f_q, f_5, f_2, \ldots, f_4\}$，为由$BS^M$控制的$U^{M,b}$提供了序列$\boldsymbol{x}^{M,b}$，$\boldsymbol{x}^{M,b} = \{f_3, f_1, f_4, f_1, f_q, \ldots, f_5\}$。

在下文中，提出了一种可以根据频谱感知结果动态调整的DSC辅助传输方案，该方案具有较高的安全性能。该DSC辅助传输方案可以产生一系列的DSC序列来代表授权用户的传输决策。在该方案下，多位授权用户可以在同一时期安全地接收数据包，降低被动窃听者破译传输方案的可能性，由此实现授权用户安全通信的目标。生成该DSC辅助传输方案的过程总结在算法2中。

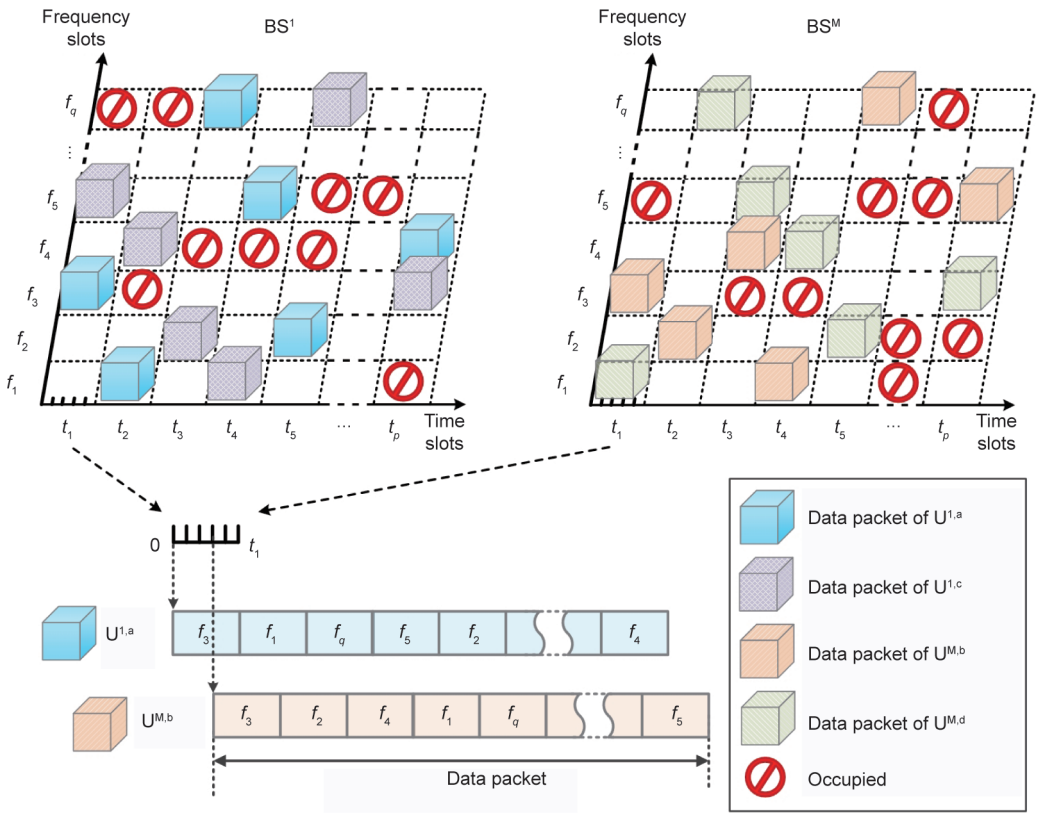

图2. 传输方案的示意图。f_q：第q个频隙。

Algorithm 2. The proposed DSC-assisted transmission scheme.

Input: The set of available frequency slots F_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 $\boldsymbol{Z}^{\varphi,k} = \{z_i^{\varphi,k} \mid k = 1, 2, \ldots, K\}$ based on the block cryptography
3. Upon applying $s_i^{\varphi,k} = (s_{i-1}^{\varphi,k} + z_i^{\varphi,k} + i) \bmod (q)$, 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 ith time slot satisfies $s_i^{\varphi,k} = s_i^{\varphi,w}$ (the authorized user $w = 1, 2, \ldots, K$; $w \neq k$), let $x_i^{\varphi,k} = (s_i^{\varphi,k} + r_i) \bmod (q)$, where the orthogonal transformation factor $r_i = \min(r \mid (s_i^{\varphi,k} + r) \bmod (q) \neq s_i^{\varphi,w})$, otherwise, $x_i^{\varphi,k} = s_i^{\varphi,k}$
5. **End for**

Output: The DSC sequence family $\boldsymbol{X}^{\varphi,k} = \{\boldsymbol{x}^{\varphi,k}; k = 1, 2, \ldots, K\}$

详细步骤如下。

• 生成一个基本序列：授权用户$U^{\varphi,0}$的随机基本序列$\boldsymbol{Z}^{\varphi,0} = \{z_i^{\varphi,0} \mid i = 1, 2, \ldots, p\}$应该由时钟（time of day, TOD）序列t_i ($i = 1, 2, \ldots, p$)和用户密钥识别产生。$z_i^{\varphi,0} = f_j$ ($j \in \{1, 2, \ldots, q\}$)表示$U^{\varphi,0}$在第$i$个时隙占用第$f_j$个频隙传输数据包。为了同时向$k \in (1, 2, \ldots, K)$名用户提供难以被被动窃听者破译的传输决策，该基本序列扩展为一个包含k个序列的序列组。

• 通过迭代操作扩展基本序列：根据分区密码算法[40]，产生$z_i^{\varphi,0}$的初始迭代因子$P_i^{\varphi,0}$迭代k轮，即$P_i^{\varphi,k} = P_i^{\varphi,k-1} \oplus \text{key}_i \oplus \text{box}_g(P_i^{\varphi,k-1})$，其中⊕表示异或运算，$\text{key}_i$是第$i$个时隙中与BS$^{\varphi}$关联的授权用户的识别符号，$g$ ($g = 1, 2, 3, \ldots$)是迭代操作盒的数量。因此，由一组基本序列$\boldsymbol{Z}^{\varphi,k} = \{z_i^{\varphi,1}, z_i^{\varphi,2}, \ldots, z_i^{\varphi,k} \mid i = 1, 2, \ldots, p\}$可以得到$z_i^{\varphi,k} = P_{i1}^{\varphi,k} \oplus P_{i2}^{\varphi,k} \oplus \ldots \oplus P_{i,j}^{\varphi,k}$。然后，将$Z_i^{\varphi,k} \in \boldsymbol{Z}^{\varphi,k}$与最佳决策阈值相比较，可以产生两种不同的映射关系。如果$z_i^{\varphi,k}$小于阈值，则$s_i^{\varphi,k} = z_i^{\varphi,k}$，否则$s_i^{\varphi,k} = (s_{i-1}^{\varphi,k} + z_i^{\varphi,k} + i) \bmod (q)$。因此可以得到$\boldsymbol{S}^{\varphi,k} = \{s_i^{\varphi,1}, s_i^{\varphi,2}, \ldots, s_i^{\varphi,K}; i = 1, 2, \ldots, p\}$。

• 将序列组正交：当$s_i^{\varphi,k} = s_i^{\varphi,w}$ ($w = 1, 2, \ldots, K$; $w \neq k$)时，可以得到$x_i^{\varphi,k} = (s_i^{\varphi,k} + r_i) \bmod (q)$，其中正交变换因子$r_i = \min(r \mid (s_i^{\varphi,k} + r) \bmod (q) \neq s_i^{\varphi,w})$，否则$x_i^{\varphi,k} = s_i^{\varphi,k}$。由此得到DSC序列族$\boldsymbol{X}^{\varphi,k} = \{\boldsymbol{x}^{\varphi,k}; k = 1, 2, \ldots, K\}$，其中序列$\boldsymbol{x}^{\varphi,k}$代表$U^{\varphi,k}$在传输期间传输数据包所占用的频隙。

基于生成的DSC序列族$\boldsymbol{X}^{\varphi,k}$，授权用户可以占用每个时隙的空闲频隙。很明显，同一微蜂窝小区的授权用户可以在mBS的控制下同步访问该微网络。由于不同微蜂窝小区的时钟不同，与不同的mBS和MBS关联的用户将异步访问共享的频谱资源。如图2所示，不同通信小区的两位授权用户（U^{1,a}和U^{M,b}）独立随机发送占用L（$L \leqslant p \ll q$）个连续时隙的数据包。

4. HCN 中数据传输的安全分析

本节对采用 DSC 辅助传输方案的两位授权用户之间的碰撞概率进行了理论分析。基于对碰撞概率的分析，本文还推导出了授权用户能够安全接收所传输数据包的概率和窃听者无法获得传输数据包的概率的解析表达式。

4.1. 碰撞概率

考虑这些通信小区的 TOD 不同，MBS 和 mBS 的授权用户可能同时占用同一频隙，这就造成了碰撞并产生了传输干扰。假设数据包到达共享传输信道的过程遵循泊松分布，到达率为 G。

因此，在 L 个时隙中传输数据包 n 的概率密度函数（PDF）可以用 $f_{\mathrm{PDF}}(n)$表示。

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

请注意，在 HCN 中，授权数据传输造成的干扰要比背景噪声的干扰功率大得多。由于碰撞会严重影响数据传输性能，所以需要分析数据传输的碰撞概率。在本文构建的 HCN 中，授权用户的碰撞概率是指授权用户在该网络中传输数据包时，与其他用户在同一时隙占据相同频隙的概率。请注意，在该 DSC 辅助传输方案下，同一基站中的授权用户遵循正交序列，不会发生碰撞。因此，由 MBS 传输的数据只会与 mBS 传输的数据发生碰撞。此外，考虑 mBS 的覆盖区域互不重叠，mBS 中的授权用户只会与 mBS 的数据传输发生碰撞。在下文中，分析了用户 $\mathrm{U}^{\mathrm{l,a}}$（与 BS^{l} 关联）和 $\mathrm{U}^{\mathrm{M,b}}$（与 BS^{M} 关联）传输数据包时的碰撞概率。

位于 BS^{l} 通信小区的 $\mathrm{U}^{\mathrm{l,a}}$ 和 $\mathrm{U}^{\mathrm{M,b}}$ 的数据包传输过程如图 3 所示。图 3 中的符号 $x_i^{\mathrm{l,a}}$ $(i=1,2,\cdots,L)$和 $x_i^{\mathrm{M,b}}$ 分别对应 $\mathrm{U}^{\mathrm{l,a}}$ 和 $\mathrm{U}^{\mathrm{M,b}}$ 在第 i 个时隙占用的频隙。考虑不同通信小区的时钟是相互独立的，$\mathrm{U}^{\mathrm{M,b}}$ 数据传输的开始时间可能与 $\mathrm{U}^{\mathrm{l,a}}$ 的时间不一致。如图 3 所示，$\mathrm{U}^{\mathrm{M,b}}$ 在 $\mathrm{U}^{\mathrm{l,a}}$ 即将完成第二个时隙的传输任务时才开始传输。假设在传输期间，这两个数据包之间有 l 个时隙重叠。在本例中，在 $\mathrm{U}^{\mathrm{M,b}}$ 的数据传输期间，$\mathrm{U}^{\mathrm{M,b}}$ 的每个时隙都与 $\mathrm{U}^{\mathrm{l,a}}$ 的连续两个时隙重叠，$\mathrm{U}^{\mathrm{M,b}}$ 的第 l 个时隙只与 $\mathrm{U}^{\mathrm{l,a}}$ 的第 L 个时隙重叠，而 $\mathrm{U}^{\mathrm{M,b}}$ 的其余时隙不与 $\mathrm{U}^{\mathrm{l,a}}$ 重叠。有一个特殊情况，即只有 $\mathrm{U}^{\mathrm{M,b}}$ 的第一个时隙与 $\mathrm{U}^{\mathrm{l,a}}$ 的最后一个时隙重叠。

定理 1：给定有 q_{s} 个频隙的可用频隙集 F_{s}，每个可用频隙 f_j 都可被授权用户占用，概率为 $\Pr\left(x_i^{\varphi,k}=f_j \mid i=1,2,\cdots,L;j=1,2,\cdots,q\right)$。如果两个异步访问 HCN 的授权用户之间有 c 个时隙重叠，当 $P_1=P_2=\cdots=P_q=1/q$ 时，可以得到这两名用户的最大不碰撞概率，即

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

证明：在不失一般性的情况下，如果两个数据包在每个时隙占用不同的频隙，可以认为它们不发生碰撞。由于不同时隙的数据传输相互独立，$\mathrm{U}^{\mathrm{l,a}}$ 和 $\mathrm{U}^{\mathrm{M,b}}$ 传输的两个数据包的不碰撞概率为

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

式中，$x_r^{\mathrm{M,b}}$ 是与 BS^{M} 关联的用户 U_{b} 在第 r 个时隙占用的频隙；r 是从 1 到 $l-1$ 的实数。假设 $\mathrm{U}^{\mathrm{M,b}}$ 在第 r 个时隙占用第 j 个频隙的概率为 $\Pr(x_r^{\mathrm{M,b}}=f_j)=\mathrm{P}_j$。

由于 $\mathrm{U}^{\mathrm{l,a}}$ 在第 t_{L-l+r} 个时隙和第 $t_{L-l+r+1}$ 个时隙占用的频隙是相互独立的，可以得出

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

同样地，当 $\Pr(x_l^{\mathrm{M,b}}=f_j \mid \hat{j}=1,2,\ldots,q)=P_j$ 时，可以得到

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

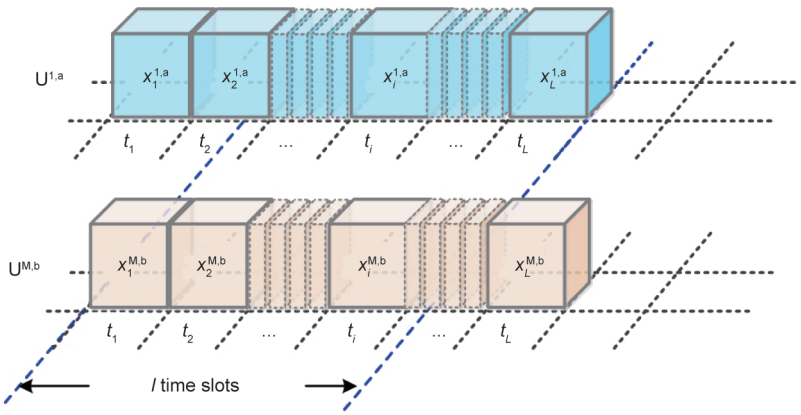

图 3. $\mathrm{U}^{\mathrm{l,a}}$ 和 $\mathrm{U}^{\mathrm{M,b}}$ 的数据包传输。l：一个传输期内两个数据包之间重叠的时隙数。$x_L^{\mathrm{l,a}}$：$\mathrm{U}^{\mathrm{l,a}}$ 在第 L 个时隙占用的频隙；$x_i^{\mathrm{l,a}}$：$\mathrm{U}^{\mathrm{l,a}}$ 在第 i 个时隙占用的频隙；$x_L^{\mathrm{M,b}}$：$\mathrm{U}^{\mathrm{M,b}}$ 在第 L 个时隙占用的频隙；$x_i^{\mathrm{M,b}}$：$\mathrm{U}^{\mathrm{M,b}}$ 在第 i 个时隙占用的频隙；t_L 和 t_i 分别为第 L 和第 i 个时隙。

考虑$\mathrm{U}^{\mathrm{M,b}}$可以在第$r$个时隙和第$l$个时隙随机占用一个可用频隙（即$\sum_{j=1}^{q}\Pr\left(x_r^{\mathrm{M,b}}=f_j\right)=\sum_{\hat{j}=1}^{q}\Pr\left(x_l^{\mathrm{M,b}}=f_{\hat{j}}\right)=1$），借助条件概率公式和经典概率理论，可以得到

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

式中，$\sum_{j=1}^{q}P_j=\sum_{\hat{j}=1}^{q}P_{\hat{j}}=1,\ 0\le\{P_j,P_{\hat{j}}\}\le 1$。

为了得到$\Pr(\mathrm{U}^{\mathrm{l,a}},\mathrm{U}^{\mathrm{M,b}})$的最大值，本文推导了拉格朗日乘数表达式$\mathscr{L}$。

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

式中，ε是一个代表拉格朗日参数的实数；$g(\cdot)$是一个等于零的约束函数。

接着，推导出$L(\mathrm{U}^{\mathrm{l,a}},\mathrm{U}^{\mathrm{M,b}})$关于$P_1,P_2,\ldots\ldots,P_q,\varepsilon$的偏导数，使该偏导数等于零，由此可以得到公式（8）。

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

由于$0\le\{P_j,P_{\hat{j}}\}\le 1,\{j,\hat{j}\}=1,2,\ldots,q$，显然只有当$P_1=P_2=\ldots=P_q=1/q$时，$\Pr(\mathrm{U}^{\mathrm{l,a}},\mathrm{U}^{\mathrm{M,b}})$才能取最大值。因此，不碰撞概率的最大值为公式（2）。

因此，只有当所有可用频隙被授权用户占用的概率相等时，才能获得不碰撞概率的最大值。

基于定理1，本文分析了HCN中n个数据包实现无碰撞传输的概率。

定理2：假设在构建的HCN中，授权用户能够以相等的概率$1/q$占据F_{s}中的频隙。当用户$U^{\varphi,\tau}$($\tau\in\{1,2,\ldots,K\}$)传输数据包时，有k($k\leqslant K$)名用户可能与$U^{\varphi,\tau}$发生碰撞（当$\varphi=\mathrm{M}$时，k名授权用户由所有的mBS提供服务；当$\varphi=1,2,\ldots,m$时，k名授权用户由MBS提供服务）。因此，$U^{\varphi,\tau}$在L个数据传输时隙中传输数据包而不发生碰撞的概率为

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

证明：假设授权用户$\mathrm{U}^{\mathrm{l,a}}$和$\mathrm{U}^{\mathrm{M,b}}$的数据传输有$l$个时隙的重叠。由于数据包到达传输信道的过程遵循泊松分布，授权用户在任何时隙传输信息的概率都是相等的。因此可以得到，两个数据包重叠l个时隙的概率为

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

因此，两名授权用户传输数据包而不发生碰撞的概率为

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

在本文提出的DSC辅助传输方案中，所划分的频隙数量远大于数据传输所占用的时隙数量（即$q\gg L$）。运用泰勒级数并忽略高阶项后，上述公式（11）可以进一步表示为

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

因此，该数据包与所有其他k个数据包之间的不碰撞概率可表示为公式（9）。

由定理2可以得到两条备注。

备注1：对于固定的k，$\Pr(L,k,q)$是L/q比率的幂函数，而且该函数随着L/q值的增加而单调递减。

备注2：对于固定的L/q，$\Pr(L,k,q)$是k的指数函数。此外，由于$0<1-L/q<1$，$\Pr(L,k,q)$随着k的增加而减小。

推论1：基于定理2，$U^{\varphi,\tau}$和其他基站的k名用户之间的碰撞概率可以表示为

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

式中，$L \ll q$。借助泰勒级数，公式（13）可以进一步表示为

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

4.2. 可靠传输概率

在HCN中，对传输信息的干扰主要来自三个方面：背景噪声（N_0）、未经授权的恶意干扰设备（I_{un}），以及数据传输过程中授权用户之间的碰撞（I_{c}）。因此，授权用户的SINR（$\mathrm{SINR_u}$）可以表示为

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

式中，P_{u}代表授权用户从关联基站接收的功率；$I_{\mathrm{c,u}}$代表由传输碰撞造成的来自其他授权用户的干扰。未经授权的恶意干扰设备对授权用户$I_{\mathrm{un,u}}$传输的数据包的影响可以通过算法1避免（即$I_{\mathrm{un,u}} = 0$）。此外，N_0是一个均值为零的复高斯随机变量。同样地，窃听者的SINR（$\mathrm{SINR_e}$）可以表示为

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

式中，P_{e}是窃听者接收的数据包的功率；$I_{\mathrm{c,e}}$表示在窃听者观察到的频隙内传输的数据包与其他授权传输的数据包之间的碰撞。未经授权的信号对窃听者观察到的频隙的干扰$I_{\mathrm{un,e}} = 0$。

正如Wyner [27]首次证明的那样，为了破译所接收的数据包，授权用户的SINR应该大于破译阈值（δ_{u}）。本文将可靠传输概率定义为所有传输信息都能被授权用户接收的概率，可以表示为

$$P(\delta_{\mathrm{u}}) = \Pr\left(\min\left(\mathrm{SINR_{u,BS}}\right) \geq \delta_{\mathrm{u}}\right) \tag{17}$$

式中，$\mathrm{SINR_{u,BS}}$是与$\mathrm{BS^M}$相关的授权用户的SINR。

在DSC辅助方案中，MBS占用一个可用频隙$(f_j \in F_{\mathrm{s}}; j = 1,2,...,q)$的概率为$\Pr(f_j)$。授权用户（$P_{\mathrm{u,BS}}$）收到的期望数据传输的功率则可以表示为

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

式中，P_{BS}是$\mathrm{BS^M}$的功率；θ是与$\mathrm{BS^M}$关联的授权用户数量；$g(\mathrm{u,BS}) = |\mathrm{h_{u \cdot f_j \cdot l}}|^2$表示第$l$个时隙$\mathrm{BS^M}$和授权用户之间的信道增益，遵循参数为$\alpha^2$的指数分布；u代表授权用户。此外，其他授权用户占用同一时隙所造成的干扰功率为

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

式中，P_{BS^φ} ($\varphi = 1, 2, \cdots, m$)是mBS的功率。此外，假设$g(\mathrm{u,bs}) = |h_{\mathrm{m_u} \cdot f_j \cdot l}|^2$是$\mathrm{BS}^\varphi$和授权用户之间的信道增益，遵循参数为$\beta_\varphi^2$的指数分布。

将公式（14）、公式（18）和公式（19）代入公式（15）后，授权用户的SINR可以改写为

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

基于公式（20），可以推导出以下命题。

命题1：授权用户从MBS接收数据包的可靠传输概率为

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

式中，P_{bs}表示mBS的功率。

证明：请参考附录A。

同样地，对于与mBS (BS^φ, $\varphi = 1, 2, \cdots, m$)相关的授权用户，可靠传输概率可以表示为

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

式中，P_{bs}代表mBS所服务的用户数。

4.3. 保密概率

为了防止被动窃听者破译授权设备间传输的信息，任何窃听者的SINR都应低于破译阈值δ_{e}。

因此，本文将有效信息不能被任何窃听者获取的概率定义为保密概率：

$$P(\delta_{\mathrm{e}}) = \Pr\left(\max\left(\mathrm{SINR_{e,BS}}\right) \leq \delta_{\mathrm{e}}\right) \tag{23}$$

式中，$\mathrm{SINR_{e,BS}}$是监测$\mathrm{BS^M}$传输信号的窃听者的SINR。

假设窃听者不知道序列族$\boldsymbol{X}^{\varphi,k}$，这也是大多数实际系统的常见情况。因此，每位窃听者都会随机选择一个频隙来拦截所传输的数据包。因此，在窃听$\mathrm{BS^M}$的信息传输时，窃听者U_{e} (P_{e})截获数据包的总功率和对U_{e}的小区间干扰（$I_{\mathrm{c,e}}$）可以表示为

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

式中，e指的是窃听者；窃听者和MBS之间的信道增益$g(\mathrm{e,BS}) = |h_{\mathrm{e} \cdot ff \cdot l}|^2$遵循参数为$\lambda^2$的指数分布。同样地，窃听

者和mBS之间的信道增益$g(\mathrm{e,bs})=|h_{\mathrm{me}\cdot f_j\cdot l}|^2$也遵循参数为$\omega^2$的指数分布。

将公式（14）和公式（24）代入公式（16），窃听者的SINR可以改写为

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

通过公式（25），可以推导出以下命题。

命题2：保密概率可以表示为

$$P\left(\delta_{\mathrm{e}}\right)_{\mathrm{BS}}=1-\left(\frac{\left(P_{\mathrm{BS}}/L\right)\lambda^2}{\left(P_{\mathrm{BS}}/L\right)\lambda^2+P_{\mathrm{bs}}\theta\omega^2\delta_{\mathrm{e}}/q}\right)^m\cdot \exp\left(-\frac{\delta_{\mathrm{e}}N_0q\theta L}{P_{\mathrm{BS}}\lambda^2}\right) \tag{26}$$

证明：命题2的验证方式与命题1类似，所以此处省略具体证明。

对一位与MBS关联的授权用户而言，保密概率可以表示为

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

5. 网络容量分析

根据第4节的分析，可以发现，可靠传输概率和保密概率都取决于HCN中的用户数量。因此，本节将推导出网络容量的上限与下限（即网络可支持的用户数量），从而保证可靠安全的数据传输概率。

5.1. MBS的网络容量

假设$P_{\mathrm{r,min}}$是HCN所要求的最小可靠传输概率，根据命题1可以得到以下关系。

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

即

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

$$\ln P_{\mathrm{r,min}}+\frac{\delta_{\mathrm{u}}N_0\theta L}{P_{\mathrm{BS}}\alpha^2}+m\cdot\ln\left(\frac{(P_{\mathrm{BS}}/L)\alpha^2+P_{\mathrm{bs}}\theta\beta^2\delta_{\mathrm{u}}/q}{(P_{\mathrm{BS}}/L)\alpha^2}\right)\le 0$$

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

利用朗伯W函数，即xe^x的反函数，可以得到HCN中BS^{M}的网络容量上限：

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

式中，W是朗伯W函数。

只要与BS^{M}关联的授权用户数量不超过该网络的最大容量，数据传输就能成功完成。

同样地，当HCN受到最小保密概率（$P_{\mathrm{s,min}}$）的约束时，可以获得以下关系

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

即

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

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

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

借助朗伯W函数，可以推导出HCN中宏蜂窝网络容量在$P_{\mathrm{s,\,min}}$约束下的下限

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

因此，与BS^{M}关联的授权用户数量应该大于网络容量的下限，以确保BS^{M}中传输的数据包无法被窃听者破译。

5.2. mBS的网络容量

mBS的网络容量可以通过与第5.1节类似的分析得出。mBS网络容量的上限为

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

而微蜂窝网络容量的下限为

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

$$\frac{qP_{\mathrm{bs}}\omega^2}{LP_{\mathrm{BS}}\lambda^2\delta_{\mathrm{e}}}$$

为此，可以根据实际应用场景对HCN可靠传输概率$P_{\mathrm{r,min}}$和保密概率$P_{\mathrm{s,min}}$的要求，得到允许接入网络的授权用户数量的上下限。因此，通过合理限制接入网络的用户数量，可以有效地提高多名用户在同一传输期内成功传输数据包的可能性，同时减少窃听的可能性。

6. 数值结果

本节通过仿真验证了HCN安全性和网络容量的理论分析。此外，本文将DSC辅助传输方案与一个基准方案进行比较，以此证明该方案的有效性。

6.1. 仿真条件设置

本文考虑的是一个双层HCN的场景，由一个MBS和10个mBS组成。此外，有10位被动窃听者随机分布在HCN中。MBS和mBS的功率分别为P_{BS} = 43 dBm（相对于一毫瓦的分贝数）和P_{bs} = 30 dBm。MBS和授权用户之间的平均信道增益参数为$\alpha^2 = 5$，MBS和窃听者之间的平均信道增益参数为$\lambda^2 = 3$。同样地，mBS和授权用户之间的平均信道增益参数为$\beta^2 = 2$，mBS和窃听者之间的平均信道增益参数为$\omega^2 = 1$。此外，共享传输信道的带宽设置为300 MHz。除非另有说明，否则本节中的所有结果都是在上述参数设置下获得的。

6.2. 安全性能评估

（1）不同的SINR阈值δ_{u}和δ_{e}。图4显示了当q = 128、L = 8时，不同信噪比（signal-to-noise ratio, SNR）的平均可靠传输概率和保密概率。从图中可以发现：

• 可靠传输概率随着SNR的增加而增加，而保密概率则大致呈线性下降。当SNR在−5~10 dB时，这一现象尤其明显。表明在本文提出的DSC辅助传输方案下，当通信环境改善时，可靠传输的概率可以迅速增加，但窃听者截获信息的概率也略有增加。

• 当破译阈值δ_{u}和δ_{e}从2增加到3时，可靠传输概率下降，而保密概率增加。表明随着成功传输数据的信道条件要求变得更加严格，HCN更容易受到安全威胁。

• 本文将该方案与传统的OFDM传输方法和人工噪声辅助的OFDM方法进行比较[22]。传统的OFDM传输方案旨在提高资源利用效率，实现更好的网络性能。在传统OFDM传输方案的基础上，人工噪声辅助OFDM方案通过引入人工噪声来打击窃听行为并提高网络安全性。从仿真结果中可以看到，该DSC辅助方案可以获得最大的可靠传输概率和保密概率。此外，该方案没有引入额外信号源，也不需要事先了解授权用户的位置。因此，该辅助方案比人工噪声辅助的OFDM方案的传输功率更小，并且比其他两种方案的实施复杂性低。

• 如图4所示，理论结果与仿真结果匹配，证实了理论分析的正确性。在下文中，将使用理论结果来评估不同参数对该方案性能的影响。

（2）L和q对可靠传输概率的影响。图5显示了时隙数L和频隙数q对HCN、平均可靠传输概率的影响。BS和授权用户δ_{u}之间传输链路的破译阈值为3。当每次数据传输占用L = 8个时隙时，可靠传输概率随着q的增加而增加，因为划分更多的频隙可以有效减少数据传输碰撞的概率，授权用户之间的同频干扰从而减少。换言之，可靠传输概率提高了成功传输数据包的概率。然而，当可用频段数q为128时，可靠传输概率随着L的增加而下降。原因在于，一次数据传输所需要的时隙越多，共道干扰就越大，碰撞概率随之增加。

（3）L和q对保密概率的影响。图6显示了δ_{e} = 3时的

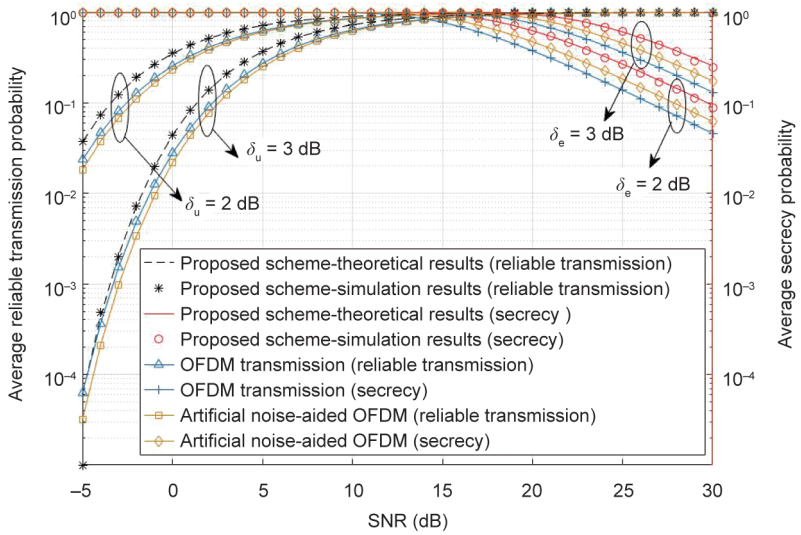

图4. 当$q = 128$、$L = 8$时，平均可靠传输概率和平均保密概率随信噪比变化。dB：分贝。

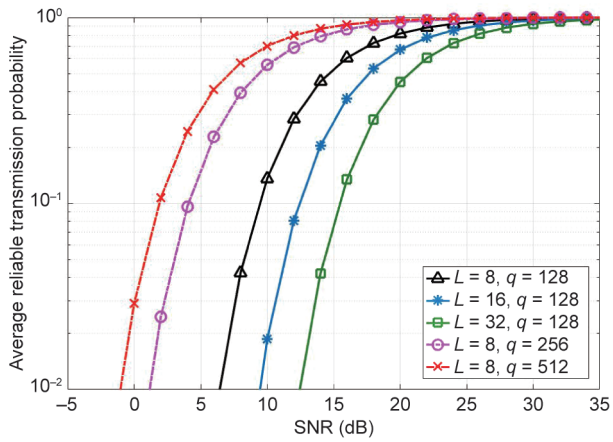

图5. 当$\delta_u = 3$时，不同L和q下的平均可靠传输概率随信噪比的变化。

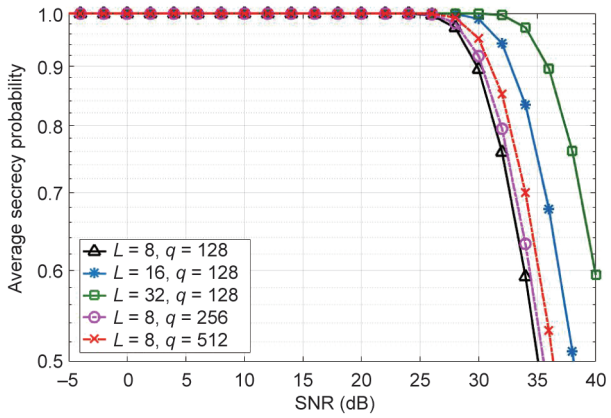

图6. 当$\delta_e = 3$时，不同L和q下的平均保密传输概率随信噪比的变化。

平均保密概率曲线。与图5的结果不同，保密概率随着SNR的增加而降低。此外，由图6可得，当q固定时，保密概率随着L的增加而增加。一旦L确定，保密概率也会随着q的增加而增加。在DSC辅助传输方案下，窃听者不知道每个时隙中的目标数据传输占用了哪个频隙。如果窃听者一直监测一个或几个可用频隙，也只能接收不同数据包传输的数据片段。由于每个数据包传输在不同的时隙占用不同的频隙，窃听者必须成功拦截所有的数据片段才能破译并获得整个数据包。L和q越大，窃听者就需要花越长时间监测更多频隙，获得目标授权用户传输的完整数据包。因此，在该DSC辅助传输方案中，如果L和q较大，窃听者便难以破译所传输的数据包，从而提升网络安全性能。

6.3. 网络容量评估

本文研究了不同参数设置对所提方案的网络容量的影响。图7显示了$L = 8$、$\delta_u = \delta_e = 2$时HCN的网络容量。图7（a）表明，随着可靠传输概率最小值要求增加，网络容量的上限略有下降。这是因为当成功传输数据包的要求变严格时，允许接入网络的用户更少，这样可以减少利用有限频谱资源传输的数据包碰撞的概率。图7（b）反映了随着保密概率最小值要求增加，网络容量的下限也会提高。为了使窃听者更难截获HCN中的数据包，接入网络的用户数量应该增加，以便在不同的时隙占用更多频隙。

如图7（a）、（b）所示，$P_{r,min}$或$P_{s,min}$固定时，q较大意味着更多授权用户可以接入网络。此外，仿真结果表明，q大于128时，网络容量的下限将降到零以下。这表明无论网络中有多少用户，HCN的保密要求总是可以得到满足。通过以上观察，可以得出结论，对可靠传输概率和保密概率的要求固定时，可以通过调整DSC辅助传输方案中的参数来容纳更多用户，实现安全可靠的传输。

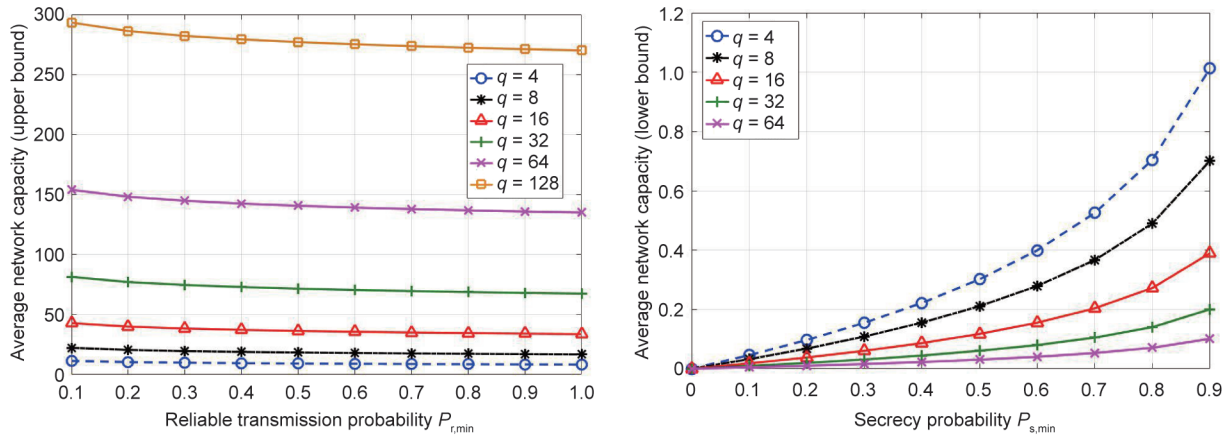

图7. 当P_{BS} = 43 dBm、P_{bs} = 30 dBm、L = 8、$\delta_u = \delta_e$ = 2时，不同可靠传输概率和保密概率要求下的平均网络容量。（a）在不同的q值下，可靠传输概率要求对平均网络容量上限的影响；（b）在不同的q值下，保密概率要求对平均网络容量下限的影响。

7. 结论和未来展望

本文研究了HCN中可靠和安全传输的问题。具体来说，提出了一种DSC辅助传输方案，可以灵活调整授权数据传输在不同时隙的频谱占用。此外，还分析并得出了碰撞概率、可靠传输概率、保密概率和网络容量的解析表达式。该方案可以有效利用有限的频谱资源，并且通过灵活调整方案中的参数（如L和q），在保证安全传输的同时提高网络容量。本工作中的方案设计和理论分析可以为未来增强无线网络安全的研究提供有益指导。未来，将在工作中引入无害干扰源，研究干扰源的选择和功率分配，旨在进一步提高可靠安全传输概率。

致谢

本研究得到了国家自然科学基金项目（61825104和91638204）、国家留学基金管理委员会（CSC）、加拿大自然科学与工程研究委员会（NSERC），以及高校创新平台建设项目（2019921815KYPT009JC011）的支持。

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 FALOHA 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.