



(12) 发明专利

(10) 授权公告号 CN 109640320 B

(45) 授权公告日 2021.07.27

(21) 申请号 201811491498.0

(22) 申请日 2018.12.07

(65) 同一申请的已公布的文献号
申请公布号 CN 109640320 A

(43) 申请公布日 2019.04.16

(73) 专利权人 南京邮电大学
地址 210003 江苏省南京市鼓楼区新模范
马路66号

(72) 发明人 吴伟 李想 王保云

(74) 专利代理机构 南京苏高专利商标事务所
(普通合伙) 32204

代理人 李淑静

(51) Int. Cl.

H04W 12/02 (2009.01)

H04W 24/02 (2009.01)

(56) 对比文件

CN 107682443 A, 2018.02.09

Zhiguo Ding等.Delay Minimization for
NOMA-MEC Offloading.《IEEE》.2018,

Yijin Pan等.Energy-Efficient NOMA-
Based Mobile Edge Computing Offloading.
《IEEE》.2018,

Zhiguo Ding等.Impact of Non-
Orthogonal Multiple Access on the
Offloading of Mobile Edge Computing.
《IEEE》.2018,

Ali Maatouk等.Frequency-Domain NOMA
With Two Sets of Orthogonal Signal
Waveforms.《IEEE》.2018,

审查员 许伶俐

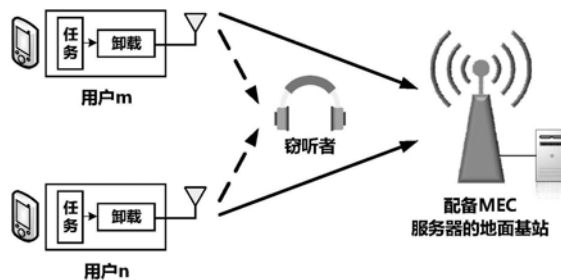
权利要求书2页 说明书8页 附图1页

(54) 发明名称

一种基于混合NOMA的移动边缘计算系统计算任务的安全卸载方法

(57) 摘要

本发明公开了一种基于混合NOMA移动边缘计算系统的计算任务安全卸载方法,在恶意窃听器存在的情况下,通过一个配备移动边缘计算服务器的地面基站为两个用户提供安全卸载和计算服务。在该系统中,对时延要求严格的用户采用NOMA方式将计算任务卸载到基站,而对时延要求相对宽松的用户则以混合NOMA方式进行卸载,地面基站再通过移动边缘计算服务器来执行相应的计算任务,同时利用物理层安全技术来保护用户计算卸载免受窃听。通过安全中断概率用来衡量系统的保密性能,可以。本发明在保证用户计算任务快速处理的同时,又提高了系统的频谱及能量利用率,降低了任务卸载过程中被恶意窃听的风险,使得系统整体的服务质量得到有效提升。



1. 一种基于混合NOMA的移动边缘计算系统计算任务的安全卸载方法,其特征在于,所述方法包括以下步骤:

(1) 建立包含用户和移动边缘计算服务器的系统:在所述系统中,配置一个具有单个天线的地面基站和单个天线的两个用户,即用户m和用户n,其中地面基站集成了移动边缘计算服务器,用来远程执行用户的卸载计算任务,用户采用混合NOMA传输方式,即在 D_m 期间,用户m与用户n共享 D_m ,并采用NOMA传输方式分别将各自的计算任务卸载到地面基站,接下来在 D_m 之后的时间间隔 T_n 期间内,用户n采用OMA的方式将剩余的计算任务全部卸载到地面基站,其中 D_m 为用户m的计算截止时间;

信道为频率非选择性准静态信道,且无线信道在给定时间块内保持不变,在该给定时间块内,每个用户具有总计 L_k 输入位的计算任务需要卸载,其中 $k \in \{m, n\}$, $|h_m|^2$ 和 $|h_n|^2$ 分别为用户m、n到地面基站的信道增益, $|g_m|^2$ 和 $|g_n|^2$ 分别为用户m、n到窃听者端的信道增益, P_m 表示用户m在 D_m 时隙的发送功率, $P_{n,1}$ 、 $P_{n,2}$ 分别代表用户n在 D_m 和 T_n 时隙的发送功率;

(2) 确定在 D_m 期间内两个用户安全卸载的条件:根据用户m、n均采用的传输方式,推导出用户m、n在地面基站端的信噪比,同时根据自适应传输及最坏情况假设,推导出用户m、n在窃听者端的信噪比,最后再推导出两个用户在 D_m 期间内安全卸载需要满足的条件,其中在 D_m 期间,采用NOMA传输的方式下,用户m、n完成全部计算任务卸载需满足的条件如下:

$$D_m \log\left(1 + \frac{|h_m|^2 P_m}{\sigma_b^2}\right) - D_m \log(1 + \beta_{e,m}) \geq L_m$$

$$D_m \log\left(1 + \frac{|h_n|^2 P_{n,1}}{|h_m|^2 P_m + \sigma_b^2}\right) - D_m \log(1 + \beta_{e,n,1}) \geq L_{n,1}$$

$\beta_{e,m}$ 和 $\beta_{e,n,1}$ 分别代表了在 D_m 期间用户m、n中冗余信息的传输速率 $R_{e,m}$ 、 $R_{e,n,1}$ 对应的信噪比; σ_b 为基站处复高斯噪声的方差; $L_{n,1}$ 为用户n在 D_m 期间的卸载到地面基站的计算任务;

(3) 确定在 T_n 期间内用户n安全卸载的条件:根据用户n采用的传输方式、自适应传输及最坏情况假设,推导出用户n在地面基站端和窃听者端的信噪比,再推导出用户n在 T_n 期间内安全卸载需要满足的条件,其中用户n在 T_n 期间采用OMA传输的方式下,完成全部计算任务卸载需满足的条件如下:

$$T_n \log\left(1 + \frac{|h_n|^2 P_{n,2}}{\sigma_b^2}\right) - D_m \log(1 + \beta_{e,n,2}) \geq L_{n,2}$$

$\beta_{e,n,2}$ 代表了在 T_n 期间用户n中冗余信息的传输速率 $R_{e,n,2}$ 对应的信噪比; σ_b 为基站处复高斯噪声的方差; $L_{n,2}$ 为用户n在 T_n 期间的卸载到地面基站的计算任务;

(4) 通过安全中断概率分析整个系统传输过程的通信性能,根据步骤(2)和(3)的确定的条件得到安全中断概率表达式并推导出结果,确定用户卸载任务期间不会触发通信中断。

2. 根据权利要求1所述的基于混合NOMA的移动边缘计算系统计算任务的安全卸载方法,其特征在于,所述步骤(4)中,安全中断概率表达式的构建过程包括:用户若不能在规定的时间内完成计算任务卸载,即 $TR_{s,k} < L_k$, $k \in \{m, n\}$,则会引发通信中断;若窃听者端信道容量 $C_{e,k}$ 大于用户冗余信息传输速率 $R_{e,k}$,即 $C_{e,k} > R_{e,k}$,则秘密信息会有被窃听者窃听的风险,同样会引发通信中断;此外,如果 $C_{BS,k} < R_{t,k}$, $k \in \{m, n\}$,地面基站将不能把秘密信息解

码出来,此时也会通信中断,因此,安全中断概率定义为:

$$P_{SO} = 1 - P_r \{ C_{BS,k} \geq R_{t,k}, C_{e,k} \leq R_{e,k}, TR_{s,k} \geq L_k \}, k \in \{m, n\}$$

$C_{BS,k}$ 代表了用户k到地面基站的信道容量; $R_{t,k}$ 为用户k的整个码字传输速率;
 $TR_{s,k}$ 为用户k传输的安全信息比特数。

3.根据权利要求2所述的基于混合NOMA的移动边缘计算系统计算任务的安全卸载方法,其特征在于,所述安全中断概率表达式展开为:

$$P_{so} = 1 - P_r = 1 - P \left\{ \begin{array}{l} \gamma_{b,m} \geq \beta_{e,m}, \gamma_{b,n,1} \geq \beta_{e,n,1}, \gamma_{b,n,2} \geq \beta_{e,n,2}, \\ \gamma_{e,m} \leq \beta_{e,m}, \gamma_{e,n,1} \leq \beta_{e,n,1}, \gamma_{e,n,2} \leq \beta_{e,n,2}, \\ D_m \log(1 + \gamma_{b,m}) - D_m \log(1 + \beta_{e,m}) \geq L_m, \\ D_m \log(1 + \gamma_{b,n,1}) - D_m \log(1 + \beta_{e,n,1}) \geq L_{n,1}, \\ T_n \log(1 + \gamma_{b,n,2}) - D_m \log(1 + \beta_{e,n,2}) \geq L_{n,2} \end{array} \right\}$$

其中, $\gamma_{b,m}$ 和 $\gamma_{b,n,1}$ 分别表示 D_m 期间用户m和用户n在地面基站的信噪比, $\gamma_{b,n,2}$ 表示 T_n 期间用户n在地面基站的信噪比, $\gamma_{e,m}$ 和 $\gamma_{e,n,1}$ 分别表示 D_m 期间用户m和用户n在窃听者端的信噪比, $\gamma_{e,n,2}$ 表示 T_n 期间用户n在窃听者端的信噪比;

在满足用户k安全信息全部卸载的情况下,用户k到地面基站的信道容量 $C_{BS,k}$ 必然不小于用户k的码字传输速率 $R_{t,k}$,同理,用户k到窃听者的信道容量 $C_{e,k}$ 也不大于用户k到窃听者端的冗余信息传输速率 $R_{e,k}$,则最终安全中断概率简化为:

$$P_{so} = 1 - P \left\{ \begin{array}{l} D_m \log(1 + \gamma_{b,m}) - D_m \log(1 + \beta_{e,m}) \geq L_m, \\ D_m \log(1 + \gamma_{b,n,1}) - D_m \log(1 + \beta_{e,n,1}) \geq L_{n,1}, \\ T_n \log(1 + \gamma_{b,n,2}) - D_m \log(1 + \beta_{e,n,2}) \geq L_{n,2} \end{array} \right\}.$$

一种基于混合NOMA的移动边缘计算系统计算任务的安全卸载方法

技术领域

[0001] 本发明属于无线通信技术领域,具体涉及一种基于混合NOMA的移动边缘计算领域中的反窃听传输方法。

背景技术

[0002] 非正交多址接入(Non-orthogonal Multiple Access,NOMA)被认为是解决第五代网络中关键问题的一项非常重要的技术,与依赖于正交资源分配的正交多址接入(OMA)技术不同,NOMA通过在功率域或码字域中进行非正交资源分配,因此,能够在相同的频时资源上为多个用户提供服务,可以满足下一代网络系统对高频谱效率、大规模连接和超低传输延迟方面的需求。移动边缘计算在下一代无线网络中同样引起了极大的关注,它能够将用户的计算密集型任务卸载到边缘服务器进行处理,在减少计算任务延迟的同时,也提高资源利用率,有助于在大规模、低功率设备上实现计算扩展任务。

[0003] 由于NOMA在频谱效率方面优于OMA,因此可以通过将NOMA应用于移动边缘计算,这不仅可以避免严重的延迟,而且还可以进一步降低上行链路任务卸载所消耗的能量。虽然NOMA在移动边缘计算中的应用有诸多优点,但在某些应用场景下,单纯的NOMA移动边缘计算方案并不是首选,因为相同条件下NOMA的能耗要比OMA的能耗高。例如:在两用户的移动边缘计算系统中,当一个用户对其任务卸载有苛刻的延迟和能耗要求,而另一用户是普通要求时,若都采用NOMA传输方式则要消耗较多的资源。

[0004] 随着现代生活中普遍采用的无线设备,通过无线信道传输前所未有的私密和敏感数据量。因此,与无线网络相关的保密问题也变得至关重要。另一方面,由于无线介质的开放性,无线信道上的收发器之间的信息交换易受窃听影响。因此,对无线传输的保密问题的研究具有重要意义。根据当前署名的发明人的工作,在设计混合NOMA移动边缘计算方案时,发现针对具有适当保密性和安全传输性能指标的外部窃听者的设计问题尚未得到研究,在这种情况下,发射机不知道窃听者的瞬时信道信息,这通常无法实现完美的保密率,这促使为实际场景设计安全的混合NOMA移动边缘计算方案的必要性。

发明内容

[0005] 发明目的:针对现有技术的不足,本发明提出一种基于混合NOMA的移动边缘计算系统进行计算任务的安全卸载的方法,能够有效解决现有移动边缘计算系统在两个用户的场景下能效和时延不平衡、安全性不能得到有效保证的问题。

[0006] 技术方案:为实现以上目的,本发明采用的技术方案如下:

[0007] 一种基于混合NOMA的移动边缘计算系统计算任务的安全卸载方法,包括以下步骤:

[0008] (1) 建立包含用户和移动边缘计算服务器的系统:在所述系统中,配置一个具有单个天线的地面基站和单个天线的两个用户,即用户 m 和用户 n ,其中地面基站集成了移动边

缘计算服务器,用来远程执行用户的卸载计算任务,用户采用混合NOMA传输方式,即在 D_m 期间,用户 m 与用户 n 共享 D_m ,并分别将各自的计算任务卸载到地面基站,接下来在 D_m 之后的时间间隔 T_n 期间内,用户 n 采用OMA的方式将剩余的计算任务全部卸载到地面基站;

[0009] 信道为频率非选择性准静态信道,且无线信道在给定时间内保持不变,在该时间块内,每个用户具有总计 $L_k, k \in \{m, n\}$ 输入位的计算卸载任务, $|h_m|^2$ 和 $|h_n|^2$ 分别为用户 m 、 n 到地面基站的信道增益, $|g_m|^2$ 和 $|g_n|^2$ 分别用户 n 到窃听者端的信道增益, P_m 表示用户 m 在 D_m 时隙的发送功率, $P_{n,1}$ 、 $P_{n,2}$ 分别代表用户 n 在 D_m 和 T_n 时隙的发送功率;

[0010] (2) 确定在 D_m 期间内两个用户安全卸载的条件:根据用户 m 、 n 均采用的传输方式,推导出用户 m 、 n 在地面基站端的信噪比,同时根据自适应传输及最坏情况假设,推导出用户 m 、 n 在窃听者端的信噪比,最后再推导出两个用户在 D_m 期间内安全卸载需要满足的条件;

[0011] (3) 确定在 T_n 期间内用户 n 安全卸载的条件:根据用户 n 采用的传输方式、自适应传输及最坏情况假设,推导出用户 n 在地面基站端和窃听者端的信噪比,再推导出用户 n 在 T_n 期间内安全卸载需要满足的条件;

[0012] (4) 通过安全中断概率分析整个系统传输过程的通信性能,根据步骤2和3的确定的条件得到安全中断概率表达式并推导出结果,确定用户卸载任务期间不会触发通信中断。

[0013] 优选地,所述步骤2中,在 D_m 期间,采用NOMA传输的方式下,用户 m 、 n 完成全部计算任务卸载需满足的条件如下:

$$[0014] \quad D_m \log\left(1 + \frac{|h_m|^2 P_m}{\sigma_b^2}\right) - D_m \log(1 + \beta_{e,m}) \geq L_m$$

$$[0015] \quad D_m \log\left(1 + \frac{|h_n|^2 P_{n,1}}{|h_m|^2 P_m + \sigma_b^2}\right) - D_m \log(1 + \beta_{e,n,1}) \geq L_{n,1}$$

[0016] $\beta_{t,m}$ 和 $\beta_{t,n,1}$ 分别代表了在 D_m 期间用户 m 、 n 中冗余信息的传输速率 $R_{e,m}$ 、 $R_{t,n,1}$ 对应的信噪比; σ_b 为基站处复高斯噪声的方差。

[0017] 优选地,所述步骤3中,用户 n 在 T_n 期间采用OMA传输的方式下,完成全部计算任务卸载需满足的条件如下:

$$[0018] \quad T_n \log\left(1 + \frac{|h_n|^2 P_{n,2}}{\sigma_b^2}\right) - D_m \log(1 + \beta_{e,n,2}) \geq L_{n,2}$$

[0019] $\beta_{t,n,2}$ 代表了在 T_n 期间用户 n 中冗余信息的传输速率 $R_{t,n,2}$ 对应的信噪比; σ_b 为基站处复高斯噪声的方差。

[0020] 优选地,所述步骤4中,安全中断概率表达式的构建过程包括:用户若不能在规定的时间内完成计算任务卸载,即 $TR_{s,k} < L_k, k \in \{m, n\}$,则会引发通信中断;若窃听者端信道容量 $C_{e,k}$ 大于用户冗余信息传输速率 $R_{e,k}$,即 $C_{e,k} > R_{e,k}$,则秘密信息会有被窃听者窃听的风险,同样会引发通信中断;此外,如果 $C_{BS,k} < R_{t,k}, k \in \{m, n\}$,地面基站将不能把秘密信息解码出来,此时也会通信中断,因此,安全中断概率定义为:

$$[0021] \quad P_{SO} = 1 - P_r\{C_{BS,k} \geq R_{t,k}, C_{e,k} \leq R_{e,k}, TR_{s,k} \geq L_k\}, k \in \{m, n\}$$

[0022] $C_{BS,k}$ 代表了用户 k 到地面基站的信道容量; $R_{t,k}$ 为用户 k 的整个码字传输速率; $TR_{s,k}$ 为用户 k 传输的安全信息比特数。

[0023] 优选地,所述中断概率表达式展开为:

$$[0024] \quad P_{so} = 1 - P_r = 1 - P \left\{ \begin{array}{l} \gamma_{b,m} \geq \beta_{t,m}, \gamma_{b,n,1} \geq \beta_{t,n,1}, \gamma_{b,n,2} \geq \beta_{t,n,2}, \\ \gamma_{e,m} \leq \beta_{e,m}, \gamma_{e,n,1} \leq \beta_{e,n,1}, \gamma_{e,n,2} \leq \beta_{e,n,2}, \\ D_m \log(1 + \gamma_{b,m}) - D_m \log(1 + \beta_{e,m}) \geq L_m, \\ D_m \log(1 + \gamma_{b,n,1}) - D_m \log(1 + \beta_{e,n,1}) \geq L_{n,1}, \\ T_n \log(1 + \gamma_{b,n,2}) - D_m \log(1 + \beta_{e,n,2}) \geq L_{n,2} \end{array} \right.$$

[0025] 其中, $\gamma_{b,m}$ 和 $\gamma_{b,n,1}$ 分别表示 D_m 期间用户 m 和用户 n 在地面基站的信噪比, $\gamma_{b,n,2}$ 表示 T_n 期间用户 n 在地面基站的信噪比, $\gamma_{e,m}$ 和 $\gamma_{e,n,1}$ 分别表示 D_m 期间用户 m 和用户 n 在窃听器端的信噪比, $\gamma_{e,n,2}$ 表示 T_n 期间用户 n 在窃听器端的信噪比, $\beta_{t,m}$ 和 $\beta_{t,n,1}$ 分别代表了在 D_m 期间用户 m 、 n 中冗余信息的传输速率 $R_{e,m}$ 、 $R_{t,n,1}$ 对应的信噪比, $\beta_{t,n,2}$ 代表了在 T_n 期间用户 n 中冗余信息的传输速率 $R_{t,n,2}$ 对应的信噪比;

[0026] 在满足用户 k 安全信息全部卸载的情况下,用户 k 到地面基站的信道容量 $C_{BS,k}$ 必然不小于用户 k 的码字传输速率 $R_{t,k}$,同理,用户 k 到窃听者的信道容量 $C_{e,k}$ 也不大于用户 k 到窃听器端的冗余信息传输速率 $R_{e,k}$,则最终安全中断概率简化为:

$$[0027] \quad P_{so} = 1 - P \left\{ \begin{array}{l} D_m \log(1 + \gamma_{b,m}) - D_m \log(1 + \beta_{e,m}) \geq L_m, \\ D_m \log(1 + \gamma_{b,n,1}) - D_m \log(1 + \beta_{e,n,1}) \geq L_{n,1}, \\ T_n \log(1 + \gamma_{b,n,2}) - D_m \log(1 + \beta_{e,n,2}) \geq L_{n,2} \end{array} \right\}.$$

[0028] 有益效果:本发明利用混合NOMA的传输方式进行移动边缘计算任务的卸载,和现有两个用户场景下的移动边缘计算系统相比,在保证了对时延要求严格且复杂度高的计算任务快速处理的同时,又提高了系统的频谱及能量利用率。同时,本发明使用安全中断概率来衡量系统的保密性能,并推导出了最小化安全中断约束问题的封闭形式解决方案,降低了计算任务卸载过程中被恶意窃听的风险,使得系统整体的服务质量得到有效提升。

附图说明

[0029] 图1为本发明的基于混合NOMA的反窃听移动边缘计算系统模型图;

[0030] 图2为本发明中用户 m 、 n 在 D_m 和 T_n 时隙内的工作模式图;

[0031] 图3为本发明中在 $P_{n,2} = 20\text{dB}$ 时,用户 m 、 n 发送功率和安全中断概率关系图。

具体实施方式

[0032] 下面结合附图对本发明的技术方案作进一步说明。

[0033] 参照图1,实施例中提供了一种基于混合NOMA的反窃听移动边缘计算系统包括两个用户、一个恶意窃听者和配备移动边缘计算服务器的地面基站,通过混合NOMA的传输方式及安全中断概率的应用,在保证了对时延要求严格且复杂度高的计算任务快速处理的同时,又提高了系统的频谱及能量利用率,使得系统整体的服务质量得到有效提升。具体地,基于所述混合NOMA的反窃听移动边缘计算系统的计算任务安全卸载方法包括以下步

骤:

[0034] 步骤1:在所述系统中,配置一个具有单个天线的地面基站和单个天线的两个用户(即用户 m 和用户 n),其中地面基站集成了移动边缘计算服务器,用来远程执行用户的卸载计算任务。需要注意的是,此处的两个用户并不是对实际小区中用户数量的限制,而是与NOMA自身的特性有关。随着NOMA系统中用户数量的不断增加,接收端译码的复杂度和错误传播的积累也会随之增加。所以在实际工程中,均是将用户分为多组,每组尽量由少量用户(通常为两个用户)进行复用。因此在本发明中只提出针对其中一组用户任务的卸载方法,当关注的系统性能得到提高的情况下,这样的卸载方法可以扩展到多组用户。

[0035] 两个用户具有不同的服务质量要求,使用参数对 $\{L_k, D_k\}$, $k \in \{m, n\}$ 来表示每个用户的任务,定义如下:

[0036] • L_k 表示任务中包含的bit数;

[0037] • D_k 表示任务的计算截止时间。

[0038] 注意,两个用户执行NOMA与在LTE-A中实现NOMA的方式一致。出于能效以及时延等多方面的考虑,这里采用的是混合NOMA传输方式。参照图2,在 D_m 期间,用户 m 与用户 n 共享信道资源,即用户 m 与用户 n 可以在同时间、同频段内分别将各自的计算任务卸载到地面基站。 D_m 表示为用户 m 的计算截止时间,即为用户 m 需要在 D_m 期间内将全部计算任务卸载到基站中。 D_n 表示为用户 n 的计算截止时间,由于用户 n 在 D_m 期间内已经将部分任务卸载到基站了,所以在 D_m 结束后、 D_n 截止前的一段时间用户 n 需要将剩余的计算任务卸载到基站,剩余计算任务卸载的时间就是 T_n 。这里的 $T_n \leq D_n - D_m$,因为用户 n 可能在 D_n 结束前就已进将全部任务卸载完成了。接下来在 D_m 之后的时间间隔 T_n 期间内,用户 n 采用OMA的方式将剩余的计算任务全部卸载到地面基站。值得注意的是,用户 n 与用户 m 共享 D_m 的同时,不能对用户 m 造成干扰,于是这里采用了连续干扰消除的方法。

[0039] 对于信道,考虑为频率非选择性准静态信道模型,且无线信道在感兴趣的给定时间内保持不变。在该时间块内,每个用户 k 具有总计 L_k , $k \in \{m, n\}$ 输入位的计算任务,该计算任务应该在该块结束之前执行。考虑全部卸载情况,即用户 k 的全部任务都用于卸载。假设地面基站完全知道所有用户的计算信息和信道状态信息。根据这些信息,地面基站可以协调这些用户的计算卸载。

[0040] $|h_m|^2$ 、 $|h_n|^2$ 分别为用户 m 、 n 到地面基站的信道增益,对应的概率密度函数分别为

$$f_{|h_m|^2}(x) = \frac{1}{\lambda_m} e^{-\frac{x}{\lambda_m}}, \quad f_{|h_n|^2}(z) = \frac{1}{\lambda_n} e^{-\frac{z}{\lambda_n}},$$

其中 λ_m 、 λ_n 分别为对应复高斯分布的方差,这里的 x 就是自变量 $|h_m|^2$,同样, z 是自变量 $|h_n|^2$ 。以 $|g_m|^2$ 和 $|g_n|^2$ 分别表示用户 m 、 n 到窃听端的信道增益, P_m 表示用户 m 在 D_m 时隙的发送功率, $P_{n,1}$ 、 $P_{n,2}$ 分别代表用户 n 在 D_m 和 T_n 时隙的发送功率。

[0041] 为了达到保密的目的,本发明采用了维纳安全编码方案和零空间辅助信令技术来混淆窃听者。对于安全编码,将冗余信息插入到安全信息中,并分别以速率 $R_{s,k}$ 和 $R_{e,k}$, $k \in \{m, n\}$ 进行传送, $R_{s,k}$ 表示保密信息速率, $R_{e,k}$ 表示冗余信息速率,以此抵抗窃听者的恶意窃听,则整个码字速率 $R_t = R_s + R_e$ 。用户到地面基站和用户到窃听者之间的信道容量分别为 $C_{b,k} = \log(1 + \gamma_{b,k})$ 、 $C_{e,k} = \log(1 + \gamma_{e,k})$, $k \in \{m, n\}$,其中 $\gamma_{b,k}$ 、 $\gamma_{e,k}$ 分别为用户到地面基站和用户到窃听者之间的信噪比。如果 $C_{b,k} < R_{t,k}$,则地面基站无法恢复安全信息,就会引发通信中断。如果 $C_{e,k} \geq R_{e,k}$,则安全信息可能被窃听者所解码,也会引发通信中断。

[0042] 步骤2:在 D_m 期间内,根据用户 m 、 n 均采用NOMA的传输方式,推导出用户 m 、 n 在地面基站端的信噪比,同时根据自适应传输及最坏情况假设,推导出用户 m 、 n 在窃听者端的信噪比,最后再推导出两个用户在地面基站期间内安全卸载需要满足的条件。

[0043] 在 D_m 时间内,用户 n 在不影响用户 m 的情况下,与用户 m 共享 D_m ,地面基站和窃听者接收到的信号分别为:

$$[0044] \quad y_b = \sum_{k=m,n} \sqrt{p_k} h_k s_k + n_b \quad (1)$$

$$[0045] \quad y_e = \sum_{k=m,n} \sqrt{p_k} h_k s_k + n_e \quad (2)$$

[0046] 这里 h_k 服从的是复高斯分布,即 $h_k \sim \mathcal{CN}(0, \lambda_k)$ 。 n_b 、 n_e 分别为基站、窃听者处的复高斯噪声,且分别服从复高斯分布,即 $n_b \sim \mathcal{CN}(0, \sigma_b^2)$, $n_e \sim \mathcal{CN}(0, \sigma_e^2)$ 。

[0047] 由于上行链路采用NOMA方式来传输,地面基站可以采用连续干扰消除对接收的消息进行解码。在基站服务器处理过程中,用户 n 的信息先于用户 m 被解码,然后服务器再将用户 n 的消息从收到的消息中去除,剩余部分就是用户 m 的信息了,这样就避免了用户 n 对用户 m 的干扰。此时用户 m 和用户 n 在地面基站的信噪比分别为:

$$[0048] \quad \gamma_{b,m} = \frac{|h_m|^2 P_m}{\sigma_b^2} \quad (3)$$

$$[0049] \quad \gamma_{b,n,1} = \frac{|h_n|^2 P_{n,1}}{|h_m|^2 P_m + \sigma_b^2} \quad (4)$$

[0050] 在考虑窃听者端信噪比时,假设窃听者已经知道地面基站的解码顺序,而且窃听者在尝试解码用户 m 的消息之前已经解码了用户 n 消息。该假设意味着在设计系统时采用最坏情况假设,即高估窃听者的窃听能力。事实上,窃听者可能知道也可能不知道解码顺序。然而,合法用户无法知道窃听者的情况,因为窃听者不会告知地面基站其窃听能力和瞬时信道状态信息。因此,由于安全研究规定的保守性,必须从合法用户的角度采用最坏情况假设。因此,窃听者端的信噪比为:

$$[0051] \quad \gamma_{e,m} = \frac{|g_m|^2 P_m}{\sigma_e^2} \quad (5)$$

$$[0052] \quad \gamma_{e,n,1} = \frac{|g_n|^2 P_{n,1}}{\sigma_e^2} \quad (6)$$

[0053] 在这种情况下,用户 m 、 n 到窃听者的信噪比必须不大于冗余信息传输对应的信噪比,以便在任何可能的窃听通道下安全卸载。即:

$$[0054] \quad \gamma_{e,m} \leq \beta_{t,m} \quad (7)$$

$$[0055] \quad \gamma_{e,n,1} \leq \beta_{t,n,1} \quad (8)$$

[0056] 这里 $\beta_{t,m}$ 和 $\beta_{t,n,1}$ 分别代表了在 D_m 期间用户 m 、 n 中冗余信息的传输速率 $R_{e,m}$ 、 $R_{t,n,1}$ 对应的信噪比,且 $\beta_{t,m} = 2^{R_{e,m}} - 1$, $\beta_{t,n,1} = 2^{R_{t,n,1}} - 1$ 。

[0057] 同时用户也需要在 D_m 时隙内将各自规定的计算任务卸载到地面基站,即需满足:

$$[0058] \quad D_m (R_{t,k} - R_{e,k}) \geq L_k \Rightarrow D_m \log(1 + \beta_{t,k}) - D_m \log(1 + \beta_{e,k}) \geq L_k, k \in \{m, n\} \quad (4)$$

[0059] 在自适应情况下,用户码字的传输速率 $R_{t,k}$ 可以达到合法信道的信道容量 $C_{b,k}$,也即 $R_t = C_b \Rightarrow \gamma_{t,k} = \gamma_{b,k}$ 。

[0060] 即用户 m, n 在 D_m 时间内需要满足:

$$[0061] \quad D_m \log(1 + \gamma_{b,m}) - D_m \log(1 + \beta_{e,m}) \geq L_m \quad (9)$$

$$[0062] \quad D_m \log(1 + \gamma_{b,n,1}) - D_m \log(1 + \beta_{e,n,1}) \geq L_{n,1} \quad (10)$$

[0063] 步骤3:在 T_n 期间内,根据用户 n 采用的传输方式、自适应传输及最坏情况假设,推导出用户 n 在地面基站端和窃听者端的信噪比,再推导出用户 n 在 T_n 期间内安全卸载需要满足的条件。

[0064] 在 D_m 时隙结束后,用户 m 的计算任务已经全部卸载完成,所以用户 n 可以独享时隙 T_n ,此时用户 n 采用OMA方式实现任务卸载。则用户 n 在地面基站的信噪比为:

$$[0065] \quad \gamma_{b,n,2} = \frac{|h_n|^2 P_{n,2}}{|\sigma_b|^2} \quad (11)$$

[0066] 与 D_m 时隙相似,在这里也同样考虑的是最坏情况假设,即高估窃听者的窃听能力。则用户 n 到窃听者的信噪比为:

$$[0067] \quad \gamma_{e,n,2} = \frac{|g_n|^2 P_{n,2}}{\sigma_e^2} \quad (12)$$

[0068] 同样需保证用户 n 到窃听者的信噪比必须不大于冗余信息传输对应的信噪比,以便能确保秘密信息不被窃听,即:

$$[0069] \quad \gamma_{e,n,2} \leq \beta_{t,n,2} \quad (13)$$

[0070] 在 T_n 时隙中用户 n 仍然采用自适应方式传输,即用户 n 的码字传输速率 $R_{t,n,2}$ 可以达到合法信道的信道容量 $C_{b,n,2}$,同时用户 n 需能够在时间 T_n 内将剩余任务卸载完成,即需要满足:

$$[0071] \quad T_n \log(1 + \gamma_{b,n,2}) - D_m \log(1 + \beta_{e,n,2}) \geq L_{n,2} \quad (14)$$

[0072] 根据所得到的两个用户在两个时隙需要满足的条件,按照该条件来设置用户的信噪比、传输时间。

[0073] 步骤4:定义安全中断概率来分析整个系统传输过程的通信性能。

[0074] 经过上文的分析发现,用户若不能在规定的时间内完成计算任务卸载,即 $TR_{s,k} < L_k, k \in \{m, n\}$,则会引发通信中断。若窃听者端信道容量 $C_{e,k}$ 大于用户码字传输速率 $R_{e,k}$,即 $C_{e,k} > R_{e,k}$,则秘密信息会有被窃听者窃听的风险,同样会引发通信中断。此外,如果 $C_{BS,k} < R_{t,k}, k \in \{m, n\}$,地面基站将不能把秘密信息解码出来,此时也会通信中断。综上所述,安全中断概率可以定义为:

$$[0075] \quad P_{SO} = 1 - P_r \{C_{BS,k} \geq R_{t,k}, C_{e,k} \leq R_{e,k}, TR_{s,k} \geq L_k\}, k \in \{m, n\} \quad (15)$$

[0076] 则 P_r 可以展开为:

$$[0077] \quad P_r = P \left\{ \begin{array}{l} \gamma_{b,m} \geq \beta_{t,m}, \gamma_{b,n,1} \geq \beta_{t,n,1}, \gamma_{b,n,2} \geq \beta_{t,n,2}, \\ \gamma_{e,m} \leq \beta_{e,m}, \gamma_{e,n,1} \leq \beta_{e,n,1}, \gamma_{e,n,2} \leq \beta_{e,n,2}, \\ D_m \log(1 + \gamma_{b,m}) - D_m \log(1 + \beta_{e,m}) \geq L_m, \\ D_m \log(1 + \gamma_{b,n,1}) - D_m \log(1 + \beta_{e,n,1}) \geq L_{n,1}, \\ T_n \log(1 + \gamma_{b,n,2}) - D_m \log(1 + \beta_{e,n,2}) \geq L_{n,2} \end{array} \right\} \quad (16)$$

[0078] 分析上式可以发现,在满足用户k安全信息全部卸载的情况下,用户k到地面基站的信道容量 $C_{BS,k}$ 必然不小于用户k的码字传输速率 $R_{t,k}$ 。同理,用户k到窃听者的信道容量 $C_{e,k}$ 也不大于用户k到窃听者端的冗余信息传输速率 $R_{e,k}$ 。概率 P_r 可以简化为:

$$P_r = P \left\{ \begin{array}{l} D_m \log(1 + \gamma_{b,m}) - D_m \log(1 + \beta_{e,m}) \geq L_m, \\ D_m \log(1 + \gamma_{b,n,1}) - D_m \log(1 + \beta_{e,n,1}) \geq L_{n,1}, \\ T_n \log(1 + \gamma_{b,n,2}) - D_m \log(1 + \beta_{e,n,2}) \geq L_{n,2} \end{array} \right\} \quad (17)$$

$$[0079] \quad = P \left\{ \begin{array}{l} D_m \log\left(1 + \frac{|h_m|^2 P_m}{\sigma_b^2}\right) - D_m \log(1 + \beta_{e,m}) \geq L_m, \\ D_m \log\left(1 + \frac{|h_n|^2 P_{n,1}}{|h_m|^2 P_m + \sigma_b^2}\right) - D_m \log(1 + \beta_{e,n,1}) \geq L_{n,1}, \\ T_n \log\left(1 + \frac{|h_n|^2 P_{n,2}}{\sigma_b^2}\right) - D_m \log(1 + \beta_{e,n,2}) \geq L_{n,2} \end{array} \right\}$$

$$= P \left\{ \begin{array}{l} |h_m|^2 \geq \left(2^{L_m/D_m + \log(1 + \beta_{e,m})} - 1\right) \frac{\sigma_b^2}{P_m}, \\ |h_n|^2 \geq \max \left\{ \begin{array}{l} \left(2^{L_{n,1}/T_m + \log(1 + \beta_{e,n,1})} - 1\right) \frac{P_m + \sigma_b^2}{P_{n,1}}, \\ \left(2^{L_{n,2}/T_m + \log(1 + \beta_{e,n,2})} - 1\right) \frac{\sigma_b^2}{P_{n,2}} \end{array} \right\} \end{array} \right\}$$

[0080] 为了表达方便,这里令 $a = \left(2^{L_m/D_m + \log(1 + \beta_{e,m})} - 1\right) \frac{\sigma_b^2}{P_m}$, $b = \left(2^{L_{n,1}/T_m + \log(1 + \beta_{e,n,1})} - 1\right) \frac{P_m + \sigma_b^2}{P_{n,1}}$,

$$c_1 = \left(2^{L_{n,2}/T_m + \log(1 + \beta_{e,n,2})} - 1\right) \frac{\sigma_b^2}{P_{n,2}}, \quad c_2 = \frac{2^{L_{n,1}/D_m + \log(1 + \beta_{e,n,1})} - 1}{P_{n,2}}。$$

[0081] 对式(17)分析后发现,需分以下两种情况进行讨论。

[0082] 1) 当 $b \geq c_1$ 时,即 $|h_n|^2 \geq \frac{2^{L_{n,2}/T_m + \log(1 + \beta_{e,n,2})} - 1}{2^{L_{n,1}/T_m + \log(1 + \beta_{e,n,1})} - 1} \frac{P_{n,1} \sigma_b^2}{P_{n,2} P_m} - \frac{\sigma_b^2}{P_m}$, 令

$$d = \frac{2^{L_{n,2}/T_m + \log(1+\beta_{e,n,2})} - 1}{2^{L_{n,1}/T_m + \log(1+\beta_{e,n,1})} - 1} \frac{P_{n,1}\sigma_b^2}{P_{n,2}P_m} - \frac{\sigma_b^2}{P_m}。$$

[0083] 若此时 $d \geq a$,则:

$$[0084] \quad P_r = \int_d^{+\infty} \int_b^{+\infty} \frac{1}{\lambda_m} e^{-\frac{x}{\lambda_m}} \frac{1}{\lambda_n} e^{-\frac{z}{\lambda_n}} dx dz = \frac{\gamma_2}{c_2 P_m \gamma_1 + \gamma_2} e^{-\frac{c_2 P_m d + c_2 \sigma_b^2}{\gamma_2} \frac{d}{\gamma_1}}$$

[0085] 若此时 $d < a$,则:

$$[0086] \quad P_r = \int_c^{+\infty} \int_b^{+\infty} \frac{1}{\lambda_m} e^{-\frac{x}{\lambda_m}} \frac{1}{\lambda_n} e^{-\frac{z}{\lambda_n}} dx dz = \frac{\gamma_2}{c_2 P_m \gamma_1 + \gamma_2} e^{-\frac{c_2 P_m a + c_2 \sigma_b^2}{\gamma_2} \frac{a}{\gamma_1}}$$

[0087] 2) 当 $b < c_2$ 时,若此时 $d \geq a$,则:

$$[0088] \quad P_r = \int_c^{+\infty} \int_a^d \frac{1}{\lambda_m} e^{-\frac{x}{\lambda_m}} \frac{1}{\lambda_n} e^{-\frac{z}{\lambda_n}} dx dz = \frac{\gamma_2}{c_2 P_m \gamma_1 + \gamma_2} e^{-\frac{c_2 P_m a + c_2 \sigma_b^2}{\gamma_2} \frac{a}{\gamma_1}}$$

[0089] 若式 $d < a$,则 $P_r = 0$ 。于是中断概率 P_{SO} 的结果为:

$$[0090] \quad P_{SO} = \begin{cases} 1 - \frac{\gamma_2}{c_2 P_m \gamma_1 + \gamma_2} e^{-\frac{c_2 P_m d + c_2 \sigma_b^2}{\gamma_2} \frac{d}{\gamma_1}}, & b \geq c_1 \text{ 且 } d \geq a \\ 1 - \frac{\gamma_2}{c_2 P_m \gamma_1 + \gamma_2} e^{-\frac{c_2 P_m a + c_2 \sigma_b^2}{\gamma_2} \frac{a}{\gamma_1}}, & b \geq c_1 \text{ 且 } d < a \\ 1 - e^{-\frac{c_1 a}{\gamma_2 \gamma_1}} + e^{-\frac{c_1 d}{\gamma_2 \gamma_1}}, & b < c_1 \text{ 且 } d \geq a \\ 1, & b < c_1 \text{ 且 } d < a \end{cases}$$

[0091] 得到系统安全中断概率最终表达式后,在实际部署中,就可以依此进行对用户的发送功率、计算卸载的任务量进行联合优化,从而在满足用户卸载需求的情况下,得到最优的安全中断概率,使得系统的安全性能达到最佳。

[0092] 图3为本发明中在 $P_{n,2} = 20\text{dB}$ 时,用户 m, n 发送功率和安全中断概率关系图。从图中可以看出,用户 m, n 在 D_m 期间发送功率 $P_m, P_{n,1}$ 均较低时,安全中断概率较高。这是因为用户发射功率过低,则不能将计算任务卸载全部到地面基站,从而引起通信中断。从图中还可以看出,当 $P_{n,1}$ 一定时,随着 P_m 增加到一定程度,安全中断概率也会变大,这是因为在 D_m 期间, P_m 过大时,用户 m 对用户 n 造成的干扰也就越大,使得用户 n 就无法将规定的计算任务全部卸载出去,同样引起通信中断。

[0093] 以上所述仅为本发明的较佳实施例,并不用以限制本发明,凡在本发明精神和原则之内所做的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

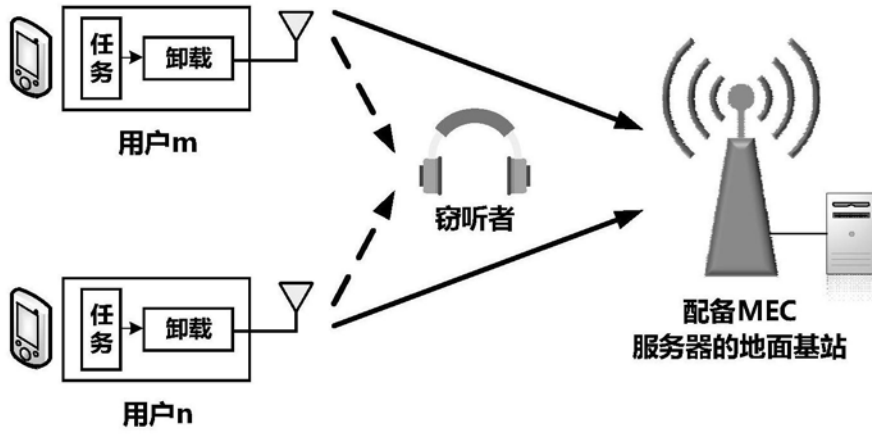


图1

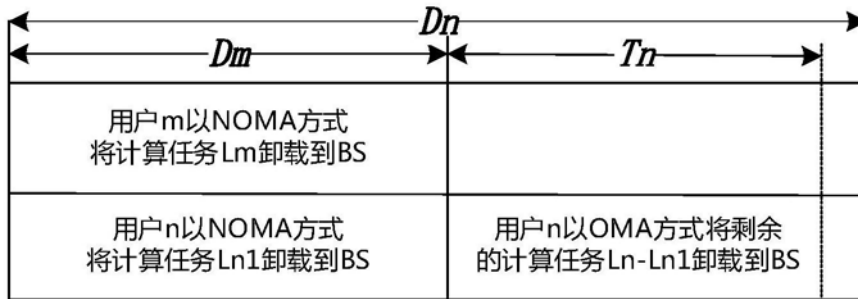


图2

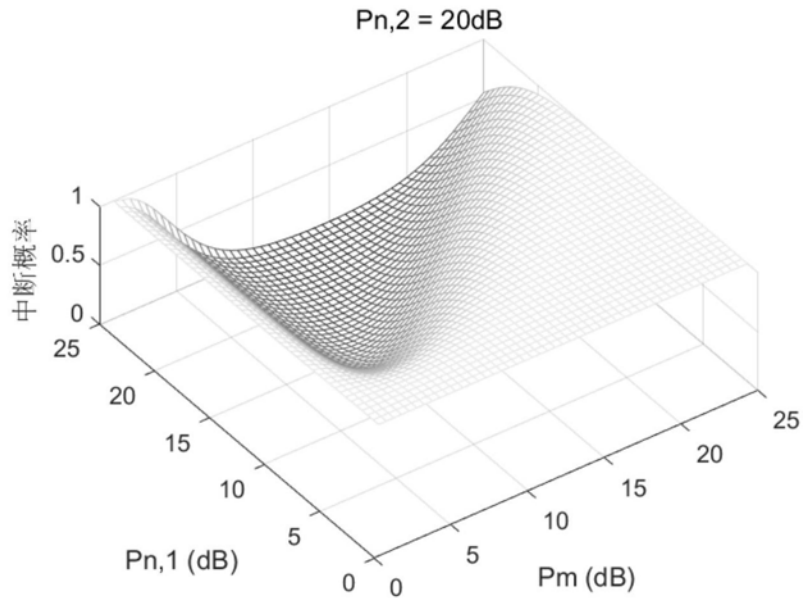


图3