计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2019.20170838
56(3):533-543, 2019

能量收集与协作网络安全容量优化技术

吴嘉鑫[1] 武继刚[1,2] 陈 龙[1] 隋秀峰[2]
[1](广东工业大学计算机学院 广州 510006)
[2](计算机体系结构国家重点实验室(中国科学院计算技术研究所) 北京 100190)
(asjiaxinwu@outlook.com)

Secrecy Capacity Optimization Technique for Energy Harvest Cooperative Cognitive Radio Network

Wu Jiaxin[1], Wu Jigang[1,2], Chen Long[1], and Sui Xiufeng[2]
[1](*School of Computer Science and Technology, Guangdong University of Technology, Guangzhou* 510006)
[2](*State Key Laboratory of Computer Architecture (Institute of Computing Technology, Chinese Academy of Sciences), Beijing* 100190)

Abstract In order to maximize the primary secrecy rate, we researched the channel resource allocation of the primary user (PU) and the secondary user (SU) in the energy harvesting cognitive radio (EHCR) which is based on the cooperative communication and energy harvesting technology. In this network, the SU, which can harvest energy from the ambient, will assist the PU with cooperative communication. As a reward, the SU can get the opportunity to access the PU's spectrum resource when the cooperative communication is over. Given the QoS demand of SU transmission node, we design a computing method of maximizing the primary secrecy rate. Numerical results demonstrate that the secrecy capacity is inverse proportional to the energy harvesting ratio, and it is also direct proportional to the cooperative communication ratio. We also figure out that the secrecy capacity is achievable. In the end, we assume that the SU works at a constant low sending power, when the cooperative communication ratio changes from 0.2 to 0.5, our research is lifting 79.28%, 80.46%, 64.23%, 78.85% on average, respectively, on the maximization of the secrecy rate, in comparison to the existing strategy. Moreover, the proposed algorithm is about 7.34 times efficient than the existing algorithms averagely.

Key words cognitive radio; cooperative communication; energy harvesting; secrecy capacity; eavesdropper

摘 要 基于协作通信与能量收集技术,研究在能量收集认知无线电网络中,主用户和次用户的信道资源配置问题,目标是主用户安全容量最大.在该网络中,次用户发送节点具有能量收集功能,且帮助主用户发送节点进行协作传输.作为回报,在次用户协作主用户通信结束后,主用户发送节点分配频谱资源给次用户发送节点.在保证次用户服务质量的前提下,设计主用户安全容量最大化的计算方法.仿真实验结果表明:安全容量与能量收集因子成反比关系,与协作通信因子成正比关系.提出的算法可以保证

收稿日期:2017-11-06;**修回日期**:2018-04-08
基金项目:国家自然科学基金项目(61672171,61702115);广东省科技厅科技计划项目(2015B010129014,2018B030311007);中国博士后科学基金项目(2017M622632);计算机体系结构国家重点实验室开放课题(CARCH201303)
This work was supported by the National Natural Science Foundation of China (61672171, 61702115), the Special Research and Development Fund of Guangdong Provincial Department of Science and Technology (2015B010129014, 2018B030311007), the China Postdoctoral Science Foundation (2017M622632), and the Open Research Fund of the State Key Laboratory of Computer Architecture (CARCH201303).
通信作者:武继刚(asjgwucn@outlook.com)

主用户传输的安全容量.最后,假设次用户以恒定小功率工作,当协作通信因子从 0.2～0.5 变化时,提出的算法比现有策略在安全容量上平均高出 79.28%,80.46%,64.23%,78.85%,此外,提出的算法比现有算法的计算效率平均高出 7.34 倍.

关键词 认知无线电;协作通信;能量收集;安全容量;窃听者

中图法分类号 TP393

随着移动通信设备的爆炸性增长和无线通信网络规模的不断扩大,一方面,无线频谱资源变得愈加稀缺;另一方面,已分配的频谱资源的利用率尚待提高.作为一种新兴技术,认知无线电(cognitive radio, CR)[1]允许次用户(secondary user, SU)使用主用户(primary user, PU)的空闲频谱,从而有效解决"频谱饥饿"问题,提高频谱资源的利用率.由于传统移动设备的能量有限,单一的电池供能方式已经不能满足无线通信系统的需要.能量收集(energy harvesting, EH)技术[2]借助可再生能源,例如太阳能、风能等,从环境中汲取能量用于通信,其收集的能量可以是无限的.利用 EH 技术,可以极大提高清洁能源的利用率,延长无线通信设备的生命期.

如图 1 所示,在能量收集认知无线电(energy harvesting cognitive radio, EHCR)网络[3-4]中,存在主用户传输对和次用户传输对以及窃听节点(eavesdropper).其中,次用户发送节点具有能量收集功能.当次用户使用的是能量受限的无线通信设备时,能量收集技术可以延长设备持续稳定通信的时间.在窃听者存在的情况下,由于主用户发送节点直接以广播形式发送消息到主用户接收节点,存在被窃听的风险.因此,信息发送过程中的安全性不可忽视[4].虽然利用密码学加密技术可以有效保障通信安全,但是由于移动设备的计算能力受限,运行复杂度较高的加解密算法容易消耗设备较多的能量,从而降低设备的续航能力.

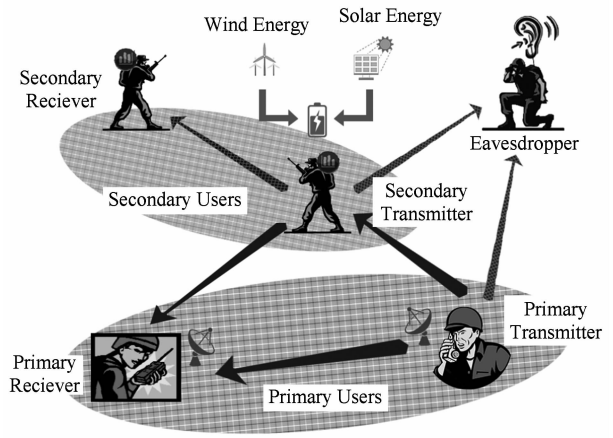


Fig. 1 Application of EHCR

图 1 EHCR 系统应用场景

安全容量(secrecy rate or secrecy capacity)[5]可以在物理层上保证信息的安全传输.主用户传输对发送速率与窃听者接收速率的差值称为安全容量.当安全容量大于零时,窃听者只能接收到一系列的高斯白噪声,从而实现了信息安全传输,进而减少设备的能量损耗,延长设备的生命周期.此外,使用协作通信[6]可以有效提高安全容量.在文献[7]中,次用户作为干扰源,向窃听者发送干扰噪声,以协助增强主用户的安全容量.然而,文献[7]假设所有节点拥有足够的能量,不适用于能量受限的场景.

当次用户发送节点能量受限时,在图 1 所示网络中,为了保证主用户的安全传输,有 4 种挑战:

1) 由于采用了能量收集技术,能量收集时隙应该添加到安全传输的时隙中.因此,现有的协作通信 2 阶段传输协议不能直接使用,因为在能量收集完成前,次用户没有足够的能量进行协作通信.

2) 能量收集时隙的长度将对安全容量产生直接影响.

3) 能量收集的效率以及次用户对发送速率的需求也会对安全传输产生影响.

4) 虽然文献[3]将协作通信 2 阶段用 α 进行了划分,但是将协作通信 2 阶段均等分配(如文献[8-9])才是标准的协作通信模型,而 α 并不一定能取到 1/2.

本研究对主用户和次用户的传输时隙进行合理划分,从而使主用户发送节点的安全容量最大.为了解决上述挑战,本研究主要有 5 方面贡献:

1) 研究协作通信 2 阶段划分策略为 1/2,且确保次用户服务质量(quality of service, QoS)的同时,通过对能量收集时隙、协作通信时隙以及回报时隙进行合理划分,最大化主用户的安全容量.

2) 仿真模拟实验结果表明:安全容量与能量收集因子 ρ 成反比关系,与协作通信因子 β 成正比关系.给定主用户发送节点的发送功率 P 和次用户发送节点的发送功率 P_R,存在一个最优值使得安全容量最大.

3) 研究 2 种协作通信划分策略在不同的次用户发送节点的发送功率 P_R 下的优势范围,在次用户发送功率较小时,1/2 划分策略优于文献[3]策略.

4) 研究本文算法和文献[3]算法在次用户发送节点改变发送功率 P_R 时,由于计算最大安全容量所产生的平均计算延迟,仿真实验结果表明:文献[3]算法的平均计算延迟比本文算法平均高出 7.34 倍.

5) 探索主用户发送节点具备能量收集功能时,在不同的能量收集效率 ε 以及主用户发送节点的发送功率 P 下,主用户需要进行能量收集的次数.

1 研究现状

文献[10]将认知无线电技术应用到了车载自组织网络,用于缓解频谱资源稀缺问题,提高车对车通信的频谱资源利用率. 与文献[10]不同,本研究主要专注于认知无线电网络下的安全容量优化问题. 文献[8]设计出最优能量收集策略,最大化 SU 的安全容量. 虽然,文献[8]中协作通信的2 个阶段被平均分配,但是文献[8]同样假定设备拥有足够的能量进行通信,不符合实际,例如,在战场环境下,SU 设备能量有限. 与文献[8]不同,本研究探索最大化主用户 PU 的安全容量. 文献[3]虽也采用协作通信技术最大化主用户的安全容量,但是文献[3]将协作通信的 2 个阶段用 α 跟 $1-\alpha$ 进行了划分,这并不是最优的方案. 此外,由于 α 会随着传输速率变化而变化,无线通信设备需要时常感知用户的传输速率,并对 α 进行调整. 一方面,这可能会造成通信的不稳定;另一方面,也会因为计算导致能量消耗. 文献[11]研究了多输入单输出的 EHCR 网络,为了同时提高主用户网络和次用户网络的安全性,提出了一个协作干扰策略,然而文献[11]未使用协作通信技术.

2 系统模型

2.1 网络模型

如图 2 所示,系统包括一个主用户发送节点 S、一个主用户接收节点 D、一个次用户传输对 R 和 O 以及一个窃听者 E,h_{XY} 表示 X 到 Y 的信道衰减因子. 其中,主用户传输节点对使用的是授权频段,当主用户有消息要传输时,主用户发送节点利用授权频段发送消息. 当所有的消息发送完毕之后,主用户暂停工作,此时的授权频段出现空闲. 次用户节点并没有分配到任何授权频段,为了避免与主用户发生冲突,只有当授权频段空闲之后,次用户才可以使用主用户的授权频段发送消息[8]. 但是,与其等待主用户独自发送完消息,次用户也可以协助主用户进行通信,使主用户提早完成发送任务,从而提供更多授权频段空闲的时间给次用户使用. 由此可见,协作通信可以有效提高信息发送效率.

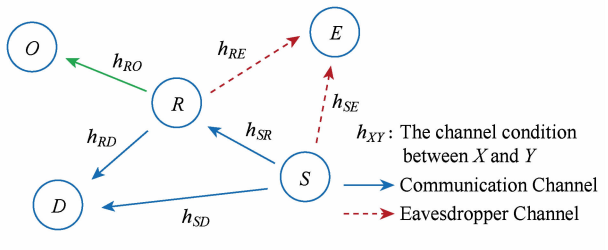


Fig. 2 System model

图 2 系统模型

为了实现协作通信①,SU 必须消耗收集到的能量帮助 PU 转发消息. 协作通信的方式有 2 种,本研究假设 PU 和 SU 之间的协作通信遵循解码-转发②(decode-and-forward, DF)机制[8].

此外,窃听节点 E 会窃听 S 和 R 之间的通信,并试图获取它们发送的原始信息. 本研究假定从 R 到 O 之间的通信是非秘密的,即不考虑次用户网络的安全容量,同时假定 S 和 D 拥有足够的能量,而 R 是能量受限的,且应该在工作前收集足够的能量以进行协作传输和自身消息传输[3]. 此外,本研究假设次用户收集能量时工作在保存然后发送(save-then-transmit)的模式,即次用户收集能量时无法发送消息(半双工)[13].

2.2 信道模型

如图 3 所示,对主用户和次用户的工作时隙进行划分,ρ 作为能量收集因子,表示次用户发送节点的能量收集时间的比例,β 作为协作通信因子,表示协作通信时隙在 $(1-\rho)T$ 时间所占的比例.

在 $[0,\rho T]$ 时间段,R 先从环境当中收集能量,例如太阳能、风能等,以供下一阶段协助 S 转发消息到 D 以及自己发送消息给 O 使用. 假设在一个时隙 T 内,R 收集的能量将全部用于发送消息且没有剩余,在每个时隙 T 开始之时,R 的能量储备都为空[8]. 当 R 正在收集能量时,无法协助 S 转发消息,

① 当 S 和 D 之间的信道质量比 S 到 E 还要差时,无法实现主用户安全容量. 因此,协作通信是需要的,为不失一般性,文献[12]假设 $|h_{SD}|^2<|h_{SE}|^2$.

② 放大-转发(amplify-and-forward, AF)模式与 DF 模式类似. 基于 DF 模式的机制可以被简单调整以适合 AF 模式.

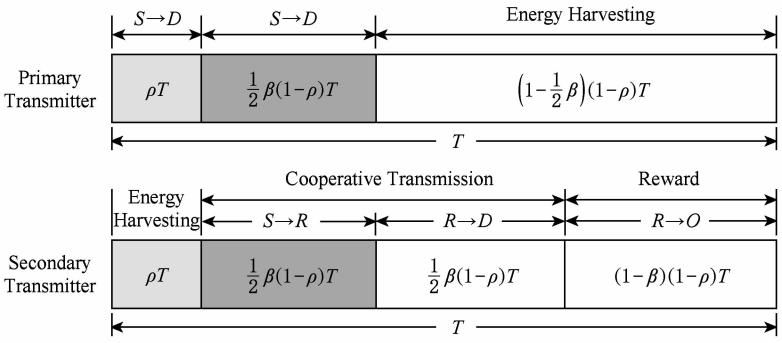


Fig. 3 Channel model

图 3 信道模型

此时 S 将直接传输消息到 D,该部分消息将被 E 窃听,因此,S 在$[0,\rho T]$时间段只能发送非秘密的消息到 D,秘密消息则在协作通信时隙转发. 如果 S 有较多的秘密消息待转发,但在一个时隙 T 内不能完全转发完成,那么可以在 nT 时隙内继续转发,其中 $n\in\{1,2,\cdots\}$[3]. 接着,S 和 R 进行协作通信,其中$[\rho T,\rho T+\frac{1}{2}\beta(1-\rho)T]$时隙作为协作传输的第 1 阶段,$S$ 将自己的秘密消息发送给 R. 由于是广播形式,D 和 E 也会收到 S 发送的消息. 在协作传输的第 2 阶段$[\rho T+\frac{1}{2}\beta(1-\rho)T,\rho T+\beta(1-\rho)T]$,$R$ 将会帮助 S 转发消息到 D,并且被 E 所侦听. 最后剩下$(1-\beta)(1-\rho)T$ 时隙留给 R 作为回报时隙. 此时 R 可以利用 S 的授权频段发送消息给 O. 此外,我们假设在这个通信网络中,各个用户之间进行通信时的信道带宽为 W(单位为 Hz).

为计算安全容量,对不同节点的发送速率分别进行分析. 由香农公式可知,R 的瞬时发送速率为[3,8]

$$V_R=W\,\mathrm{lb}\left(1+\frac{P|h_{SR}|^2}{WN_0}\right),\tag{1}$$

其中,P 表示节点 S 的发送功率($P>0$),N_0 表示单面功率延展密度(one-side power spread density)[14]. 由于 D 在协作传输的第 1 阶段跟第 2 阶段都收到消息,由最大比例结合(maximal ratio combining, MRC)可知,D 的瞬时发送速率为[3]

$$V_D=W\,\mathrm{lb}\left(1+\frac{P|h_{SD}|^2}{WN_0}+\frac{P_R|h_{RD}|^2}{WN_0}\right).\tag{2}$$

同理,E 在协作传输的 2 个阶段都收到了消息,因此,E 的瞬时发送速率可表示为[3]

$$V_E=W\,\mathrm{lb}\left(1+\frac{P|h_{SE}|^2}{WN_0}+\frac{P_R|h_{RE}|^2}{WN_0}\right).\tag{3}$$

本研究采用 DF 协作传输机制,因此 D 和 E 总的发送速率等于协作传输 2 个阶段的最小值[3,14],即①

$$\bar{V}_D=\min\left\{\frac{1}{2}\beta(1-\rho)V_R,\frac{1}{2}\beta(1-\rho)V_D\right\},\tag{4}$$

以及

$$\bar{V}_E=\min\left\{\frac{1}{2}\beta(1-\rho)V_R,\frac{1}{2}\beta(1-\rho)V_E\right\}.\tag{5}$$

结合式(1)~(5)可得:

$$\bar{V}_D=\frac{1}{2}\beta(1-\rho)W\min\left\{\mathrm{lb}\left(1+\frac{P|h_{SR}|^2}{WN_0}\right),\mathrm{lb}\left(1+\frac{P|h_{SD}|^2}{WN_0}+\frac{P_R|h_{RD}|^2}{WN_0}\right)\right\},\tag{6}$$

$$\bar{V}_E=\frac{1}{2}\beta(1-\rho)W\min\left\{\mathrm{lb}\left(1+\frac{P|h_{SR}|^2}{WN_0}\right),\mathrm{lb}\left(1+\frac{P|h_{SE}|^2}{WN_0}+\frac{P_R|h_{RE}|^2}{WN_0}\right)\right\}.\tag{7}$$

由安全容量的定义可得,主用户安全容量 r_{SEC} 为

$$r_{\mathrm{SEC}}=[\bar{V}_D-\bar{V}_E]^+,\tag{8}$$

其中,$[x]^+$ 定义为$[x]^+\triangleq\max\{0,x\}$. 将式(6)(7)代入式(8),得到:

$$r_{\mathrm{SEC}}=\frac{1}{2}\beta(1-\rho)[\min\{V_D,V_E\}-V_E]^+.\tag{9}$$

2.3 能量模型

参照文献[3],假定在每个时隙 T 内,S 发送 Q(单位为 b)数据,发送速率为 V_p,则在$[0,\rho T]$时间段,S 发送的数据为 $V_p\rho T$(单位为 b),且该部分数据应为非秘密数据. 剩下的秘密数据$(Q-V_p\rho T)$(单位为 b)需要通过协作通信传输. 此外,令 ε 表示 R 的能量收集效率,则在$[0,\rho T]$时间段,R 收集到的能量为 $\varepsilon\rho T$,假定 R 的发送功率为 P_R,则协作传输消耗能量为 $P_R\beta(1-\rho)T$,剩余能量 $\varepsilon\rho T-P_R\beta\times(1-\rho)T$ 将支持 R 发送消息到 O.

① 本研究的信道划分与文献[3]有所不同.

3 主用户安全容量最优问题研究

3.1 问题定义

从时间上看,根据协作传输机制,R 为 S 转发消息使 S 更快完成任务,从而 S 就能腾出足够的时间给 R 使用授权频段发送消息.为了激励 R 参与 S 的协作传输,R 的回报时隙应该大于 0,即 $(1-\beta)(1-\rho)T>0$.此外,β 决定了协作传输时隙以及回报时隙的大小,这 2 个时隙既不能大于整个时隙 T,也不能为 0,即 $0<\frac{1}{2}\beta(1-\rho)<1$, $0<(1-\beta)(1-\rho)<1$.在能量方面,由于 R 是能量受限的,因此在协作传输之前,R 必须先收集足够的能量,同时留出足够的时间进行协作传输以及自身发送消息,于是有 $0<\rho<1$.其次,由于次用户发送节点的能量约束,R 的发送功率 P_R 不应大于最大发送功率 $P_R^{\max}$.此外,秘密数据应该发送在协作传输阶段,有 $Q-V_p\rho T>0$.最后,R 在完成协作传输之后,剩余的能量应当足够支持 R 到 O 之间的消息发送,即 $\varepsilon\rho T-P_R\beta(1-\rho)T>0$.经过整理以及化简,主用户安全容量最大化问题可以表示为 OPT[3] 问题:

$$\begin{aligned}&\text{Obj: } \max\{r_{\text{SEC}}\}\\&\text{s.t. } (1-\beta)(1-\rho)>0,\\&0<\beta<1,\\&0\leqslant P_R\leqslant P_R^{\max},\\&0<\rho<\min\{\frac{Q}{V_pT},1\},\\&\varepsilon\rho T-P_R\beta(1-\rho)T>0.\end{aligned}\tag{10}$$

尽管 OPT 试图优化主用户 S 的安全容量,但是仍不足以保证 R 有足够的能量发送自己的消息到 O.因此,需要设计 QoS 保障机制以满足 R 自身的传输需求[3].

引理 1. 假定 R 到 O 的发送速率至少为 V_{RO},则当 $\beta\neq0$,$0<\rho<1$ 时,有:

$$P_R\geqslant f(\beta,\rho),$$

其中,$f(\beta,\rho)=[2^{\frac{V_{RO}}{(1-\beta)(1-\rho)W}}-1]WN_0/|h_{RO}|^2$.

证明. 由文献[14]可知,R 与 O 之间的发送速率为 $(1-\beta)(1-\rho)W\,\text{lb}(1+\frac{P_R|h_{RO}|^2}{WN_0})$,该速率需大于最低发送速率 R_{RO},则:

$$(1-\beta)(1-\rho)W\,\text{lb}(1+\frac{P_R|h_{RO}|^2}{WN_0})\geqslant V_{RO}\Rightarrow$$

$$2^{(1-\beta)(1-\rho)W\,\text{lb}(1+\frac{P_R|h_{RO}|^2}{WN_0})}\geqslant 2^{V_{RO}}\Rightarrow$$

$$(1+\frac{P_R|h_{RO}|^2}{WN_0})^{(1-\beta)(1-\rho)W}\geqslant 2^{V_{RO}}\Rightarrow$$

$$(1+\frac{P_R|h_{RO}|^2}{WN_0})\geqslant 2^{\frac{V_{RO}}{(1-\beta)(1-\rho)W}}\Rightarrow$$

$$P_R\geqslant\frac{[2^{\frac{V_{RO}}{(1-\beta)(1-\rho)W}}-1]WN_0}{|h_{RO}|^2}.\tag{11}$$

证毕.

引理 2. 当能量收集效率 $\varepsilon>0$ 以及 $0<\rho<1$ 时,R 的发送速率小于 $\varepsilon\rho/(1-\rho)$.

证明. 在进行协作传输之后,R 剩余的能量为 $\varepsilon\rho T-P_R\beta(1-\rho)T$,又 R 和 O 之间发送消息所需能量为 $P_R(1-\beta)(1-\rho)T$,为保证 RO 之间的数据能够完全发送,则需:

$$\varepsilon\rho T-P_R\beta(1-\rho)T\geqslant P_R(1-\beta)(1-\rho)T\Rightarrow$$

$$\varepsilon\rho\geqslant P_R(1-\rho)\Rightarrow$$

$$P_R\leqslant\frac{\varepsilon\rho}{1-\rho}.\tag{12}$$

证毕.

由引理 1 和引理 2,可得到定理 1.

定理 1. 给定固定发送速率 V_{RO},当 $\varepsilon>0$,$\beta\neq0$ 以及 $0<\rho<1$ 时,有:

$$f(\beta,\rho)\leqslant P_R\leqslant\frac{\varepsilon\rho}{1-\rho}.\tag{13}$$

证明. 由引理 1 跟引理 2 可知,定理 1 成立.

证毕.

由式(13)可以将优化目标 OPT 简化为:

$$\begin{aligned}&\text{Obj: } \max\{r_{\text{SEC}}\}\\&\text{s.t. } 0<\beta<1,\\&0<\rho<\min\{\frac{Q}{V_pT},1\},\\&f(\beta,\rho)\leqslant P_R\leqslant\frac{\varepsilon\rho}{1-\rho}.\end{aligned}\tag{14}$$

由文献[9]可知,$\text{lb}(1+snr)\approx snr$,并且将式(2)(3)代入式(9),可得:

$$r_{\text{SEC}}=\begin{cases}\frac{1}{2}\beta(1-\rho)f^{(1)}, & V_R>V_D \text{ 且 } V_R>V_E,\\0, & V_D<V_R<V_E,\\\frac{1}{2}\beta(1-\rho)f^{(2)}, & V_E<V_R<V_D,\\0, & V_D>V_R \text{ 且 } V_R<V_E,\end{cases}\tag{15}$$

其中,

$$f^{(1)}=\frac{P|h_{SD}|^2+P_R|h_{RD}|^2-P|h_{SE}|^2-P_R|h_{RE}|^2}{N_0},$$

$$f^{(2)}=\frac{P|h_{SR}|^2-P|h_{SE}|^2-P_R|h_{RE}|^2}{N_0}.$$

3.2 最优安全容量求解

文献[3]采用与本研究不同的协作通信划分策略,主要区别在于,文献[3]将协作通信的2个阶段分别用α和$1-\alpha$进行划分,而本研究则是将2个阶段均等划分,也就是协作通信的第1阶段跟第2阶段各占1/2.这是因为α随传输速率变化而变化,移动设备为达到最优安全容量,需对α不断进行调整,从而导致通信不稳定以及能量过多消耗.

为不失一般,文献[3]假设次用户发送节点R是最优的中继节点,同时$V_D>V_E$[14],得出引理3如下:

引理3[3]. 当β和ρ已知,最优α值可以被定义为$\alpha^*=\dfrac{V_R}{V_R+V_D}$.

证明过程详见文献[3].由文献[3]得出引理4:

引理4[3]. 最大化r_{SEC}等价于最大化

$$r_{\mathrm{SEC}}=\frac{\beta(1-\rho)V_R(V_D-V_E)}{V_R+V_D}. \tag{16}$$

最后,令$\mathrm{lb}(1+snr)\approx snr$[9],将式(1)~(3)代入式(16),可得:

$$r_{\mathrm{SEC}}=\beta(1-\rho)P|h_{SR}|^2(P|h_{SD}|^2+P_R|h_{RD}|^2-P|h_{SE}|^2-P_R|h_{RE}|^2)/[N_0(P|h_{SR}|^2+P|h_{SD}|^2+P_R|h_{RD}|^2)]. \tag{17}$$

3.3 主用户发送节点具有能量收集功能

在3.1节讨论中,假设主用户发送节点是能量充足的.但在现实生活中,主用户发送节点不总是能量充足,因此在本节,拓展研究主用户发送节点S能量受限,且具有能量收集功能.在该限制条件下,可得到主用户发送节点S在整个时隙T发送消息所消耗的总能量为$E_S=P[\rho T+\frac{1}{2}\beta(1-\rho)T]$.

假设主用户发送节点S的能量收集效率也为ε,并且在第1个T时隙发送消息前,主用户发送节点S刚好拥有足够发送消息的能量,并将在第1个T之后完全消耗.由于S是先发送消息,再开始能量收集,那么在第1个T时隙内收集到的能量将会用于下一个T时隙的前半部分发送消息操作,如图3可知,主用户发送节点S用于能量收集的时间为$(1-\frac{1}{2}\beta)(1-\rho)T$,要使得主用户发送节点$S$收集的能量足够下一个$T$时间的能量消耗,则需满足:

$$\varepsilon(1-\frac{1}{2}\beta)(1-\rho)T\geqslant E_S. \tag{18}$$

又因为无线通信设备每次从能量收集模式切换为发送消息模式时,可能需要消耗额外的切换状态能量,记为δ.此外,当能量收集效率ε太小时,主用户发送节点S在一个能量收集时隙内收集到能量可能不够下一次发送消息的需要,故假设主用户发送节点S在收集到足够的能量才会开始发送消息,以保证主用户发送节点始终以最优的P值进行发送,进而保障安全容量r_{SEC}的最大化.在第1个T时间的后半部分,假如S没有收集到足够的能量,接下来的$(n-1)$个T时间S将全部用来进行能量收集.在此前提下,将式(18)改写为

$$\varepsilon(1-\frac{1}{2}\beta)(1-\rho)T+(n-1)\varepsilon T\geqslant P[\rho T+\frac{1}{2}\beta(1-\rho)T]+\delta, \tag{19}$$

其中,n表示经过n个T时隙主用户发送节点才收集到足够的能量用于发送消息.主用户发送节点S具有能量收集功能的优势在于,当有一定的数据量在缓存中等待发送时,假如主用户发送节点S的能量有限,可能在数据发送完毕之前S就已经耗尽能量,这在战场上可能是致命的.但是,假如S具备从环境当中收集能量的功能,因绿色能量的供应持续稳定,理论上S能够长期工作.

3.4 算法设计

文献[3]提出了一个多项式时间复杂度安全容量最大算法(secrecy rate maximization algorithm, SRMA)来求出主用户的安全容量,但是文献[3]安全容量的计算方式只有一种,而本研究的安全容量分4种情况进行计算,因此改进原有算法以满足本研究实验部分的需求,下面给出算法伪代码:

算法1. SRMA算法.

输入:能量收集因子ε、主用户发送功率P、协作通信因子β、传输数据量Q、各信道衰减因子、约束条件V_{RO}、信道带宽W、时隙T、主用户发送速率V_p及ρ的矩阵$\boldsymbol{\Gamma}$;

输出:最大安全容量矩阵$\boldsymbol{R}_{\mathrm{SEC}}^{\max}$.

```
FOR i=1 TO length (Γ)
 /* 计算 P_R 上下界 P_Rupper(i)以及 P_Rlower(i) */
  IF P_Rupper(i)<P_Rlower(i) THEN
    /* 设置一个临时矩阵 P_Rtemp,矩阵的长度
       与 Γ 相同 */
    P_Rtemp=[P_Rlower…P_Rupper];
  ELSE
    P_Rtemp=Null;
  END IF
  FOR j=1 TO length (Γ)
    /* 分情况求出 r_SEC */
```

IF $P|h_{SR}|^2>P|h_{SD}|^2+P_{\text{Rtemp}}(j)|h_{RD}|^2$
THEN
IF $P|h_{SR}|^2>P|h_{SE}|^2+P_{\text{Rtemp}}(j)|h_{RE}|^2$
THEN
/* 此时 $V_R>V_D$ 且 $V_R>V_E$ */
参照式(15)进行计算;
ELSE
$r_{\text{SEC}}=0$; /* 此时 $V_D<V_R<V_E$ */
END IF
ELSE
IF $P|h_{SR}|^2>P|h_{SE}|^2+P_{\text{Rtemp}}(j)|h_{RE}|^2$
THEN
/* 此时 $V_E<V_R<V_D$ */
参照式(15)进行计算;
ELSE
/* 此时 $V_D>V_R$ 且 $V_R<V_E$ */
$r_{\text{SEC}}=0$;
END IF
END IF
END FOR
求出当前最大 r_{SEC},存入矩阵 $\boldsymbol{R}_{\text{SEC}}^{\max}$;
END FOR
Return $\boldsymbol{R}_{\text{SEC}}^{\max}$.

定理 2. 设矩阵 $\boldsymbol{\Gamma}$ 中的元素个数为 n,则改进的 SRMA 算法时间复杂度为 $O(n^2)$.

证明. 改进的 SRMA 算法的主体部分由 2 个嵌套的 for 循环构成,外层循环的次数为矩阵 $\boldsymbol{\Gamma}$ 中的元素个数 n,内循环的次数也为 n,不难看出,总的时间复杂度为 $O(n^2)$. 证毕.

4 实验结果与分析

实验采用 Matlab R2016b,操作系统为 Windows 7. 参照文献[3]所设置的参数,以及在实际操作中对部分参数的随机调整,本次实验① 的主要参数介绍具体如表 1 所示,其中,ε 的单位为 mJ/s[16]:

Table 1 Main Experiment Parameters
表 1 实验主要参数设置

Variable	Value
$\lvert h_{SR}\rvert^2,\lvert h_{SE}\rvert^2,\lvert h_{SD}\rvert^2$	0.6,0.4,0.3
$\lvert h_{RD}\rvert^2,\lvert h_{RE}\rvert^2,\lvert h_{RO}\rvert^2$	0.8,0.3,0.2
$\varepsilon,P,V_{RO},V_\rho,W,Q$	10,3,0.05,5,1,2

4.1 基础实验

如图 4 所示,当 $\beta=0.2$,$P=3$ W 以及固定 P_R 时,随着 ρ 的增加,主用户最大安全容量 $r_{\text{SEC}}^{\max}$ 呈线性下降,即 $r_{\text{SEC}}^{\max}$ 跟 ρ 成反比关系. 这是因为随着 ρ 增大,协作通信时隙减少,使得 D 和 E 的总发送速率 $\overline{V}_D$,$\overline{V}_E$ 随之减小,由式(8)可知,r_{SEC} 的值也相应减小. 当固定 β 跟 P,在相同的 ρ 下,有 $r_{\text{SEC}}(P_R=0.8\text{ W})<r_{\text{SEC}}(P_R=1.4\text{ W})<r_{\text{SEC}}(P_R=1.0\text{ W})<r_{\text{SEC}}(P_R=1.2\text{ W})$,这是因为,当 $P_R=0.8$ W 以及 $P_R=1.0$ W 时,此时 $V_R>V_D$ 且 $V_R>V_E$,而当 $P_R=1.2$ W 以及 $P_R=1.4$ W 时,$V_E<V_R<V_D$.

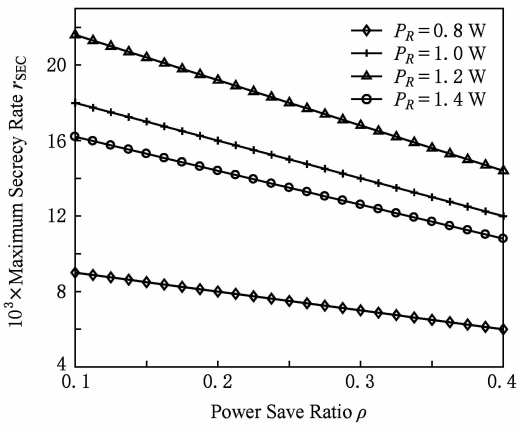


Fig. 4 Relationships between r_{SEC} and ρ for $\beta=0.2$ and $P=3$W
图 4 当 $\beta=0.2$,$P=3$W 时 ρ 与 r_{SEC} 的关系

如图 5(a)所示,固定 $P=3$W,$\beta=0.2$,在不同 P_R 下,安全容量计算公式不同. 当 $V_R>V_D$ 以及 $V_R>V_E$ 时,由于 $|h_{RD}|^2>|h_{RE}|^2$,由式(15)可知,随着 P_R 增大,r_{SEC} 增大,成正比关系;而当 $V_E<V_R<V_D$ 时,由式(15)可知,随着 P_R 增大,r_{SEC} 减小,成反比关系.

如图 5(b)所示,当固定 $P=3$W,$\beta=0.2$ 时,由于 ρ 不同,所以 P_R 的范围也不同,图 5(b)中的前 4 个箭头分别标出了在不同 ρ 下 P_R 的上界分布,后 4 个箭头分别表示了 P_R 的下界分布. 当固定 P,β 时,ρ 越小,对应的最大安全容量值越大. 由图 5(a)可知,在当前设置下,安全容量 r_{SEC} 的计算公式只能是式(15)中 Case 1,2,4 的其中 1 种,经过计算可知,各曲线安全容量为零的前半部分为 Case 1,但是在实际计算的过程中,$r_{\text{SEC}}<0$,所以由 $[x]^+$ 的定义知,$r_{\text{SEC}}=0$,在之后的曲线上升部分,也属于 Case 1,

① 所有实验的数据为 100 次实验的平均值,同时,为了实验方便,设置 P 取值在 1~5 W 之间[3,15],设置 ρ 取值在 0.2~0.5 之间[3,8],为方便表示,所有数据在文中省略单位.

由式(15)可知,P_R 增大,安全容量 r_{SEC} 随之增大,且有 P_R^{max} 使得安全容量最大;当 $P_R>P_R^{max}$ 时,此时计算公式变为 Case 3,由式(15)可知,随着 P_R 增大,安全容量 r_{SEC} 减小,直至为 0;在此之后进入 Case 4,安全容量 r_{SEC} 恒为 0,直至到达 P_R 上界.

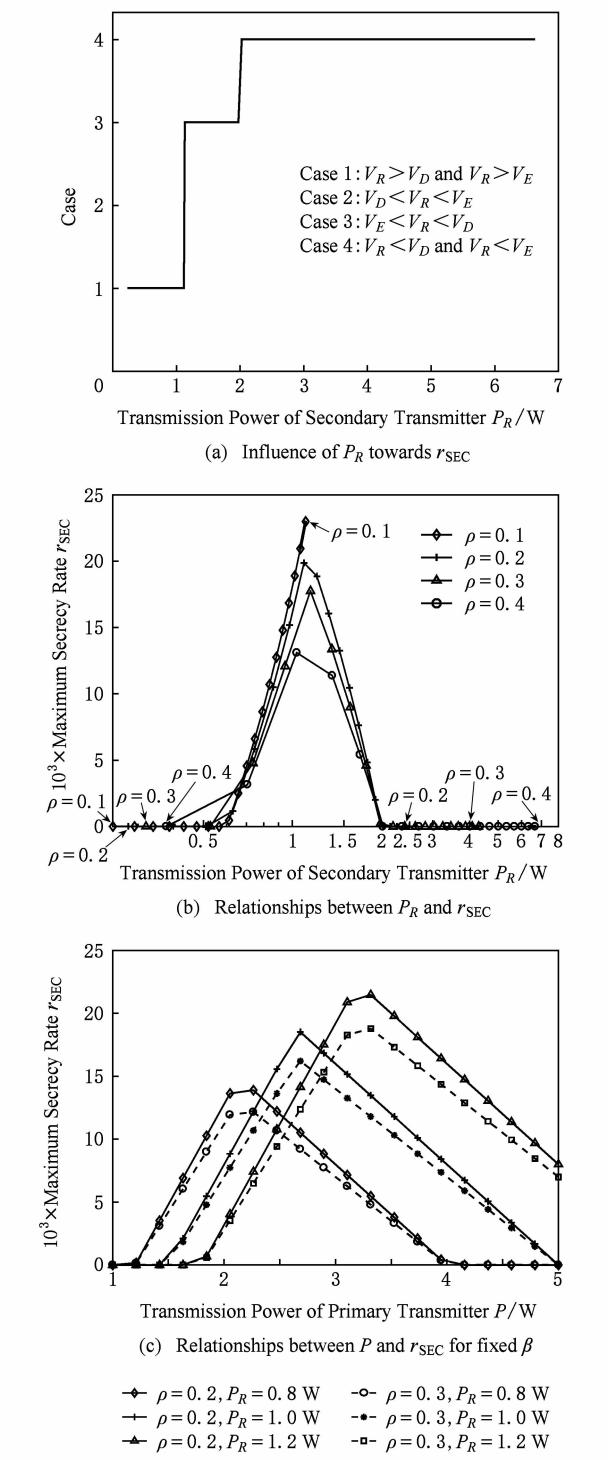


Fig. 5 The influence of different parameter settings on r_{SEC}

图 5 不同参数设置对 r_{SEC} 的影响

如图 5(c)所示,对于 $\beta=0.2$,当固定 ρ,P_R 时,随着主用户发送节点 S 发送功率 P 的增长,安全容量 r_{SEC} 的值遵循"0—递增—递减—最后 0"的规律.固定 β,ρ 时,P_R 越大,r_{SEC}^{max} 越大,同时对应的使 r_{SEC} 最大的 P 值也越大.固定 β,P_R 时,不同的 ρ 对应的安全容量曲线轨迹基本一致,同时 ρ 越小,安全容量 r_{SEC} 的值越大.如图 5(c)所示,P_R 对 r_{SEC}^{max} 的影响比 ρ 对 r_{SEC}^{max} 的影响要大,例如当固定 $P_R=0.8$ W,ρ 取 0.2 和 0.3 时,r_{SEC}^{max} 相差 0.017 3,而当固定 $\rho=0.2$,P_R 取 0.8 W 和 1.2 W 时,r_{SEC}^{max} 相差 0.046 4,即 P_R 增加 0.1 W,r_{SEC}^{max} 就多 0.023 2 增量.这是因为当次用户发送节点 R 作为中继节点发送数据时,其发送功率越大,发送速率也随之增大,也就是 D 的总发送速率 $\bar{V}_D$ 会越来越大;而 ρ 的改变只是影响了次用户发送节点 R 收集能量的时间,且存在 $0<\rho<1$,所以 ρ 对安全容量 r_{SEC} 的影响有限.

如图 6 所示,对于 $P=3$W,$P_R=1.4$W,固定 ρ,随着 β 的增大,安全容量 r_{SEC} 随之增大,且呈线性增长,这是因为协作通信的时隙增大,导致安全容量 r_{SEC} 也随之增大.取 $\rho=0.5$ 时,当 β 大于一定值之后,安全容量 r_{SEC} 的值为空,这是因为随着 β 的增大,P_R 的下界也随之增大,当 $\beta=0.72$ 时,P_R 下界已经达到 1.404 4,超过了原先设定的 $P_R=1.4$ W,所以在 β 之后的取值中,r_{SEC} 为空.当 β 取值较小时,不同 ρ 对应的安全容量 r_{SEC} 的值相差不大,当 β 逐渐增大,不同 ρ 对应的安全容量的差值越来越大.如当 $\beta=0.1$ 时,安全容量 r_{SEC} 在 $\rho=0.2$ 和 $\rho=0.3$ 处的差值为 0.000 9,当 $\beta=0.647\,4$ 时,安全容量 r_{SEC} 在 $\rho=0.2$ 和 $\rho=0.3$ 时的差值为 0.058 2,这是因为随着协作通信时隙因子 β 的增大,协作通信在对提高安全容量 r_{SEC} 的值上的作用越来越显著,所以差值随着 β 的增大而增大.

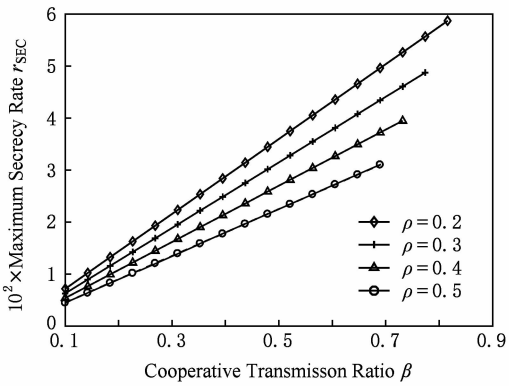


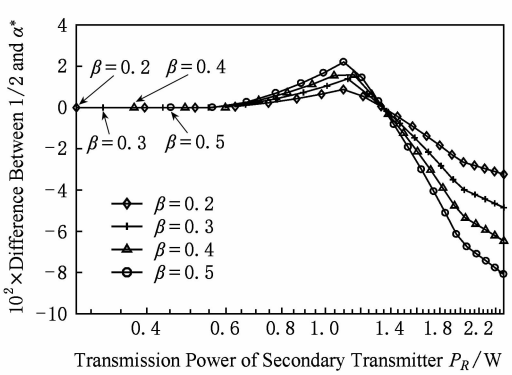
Fig. 6 Influence of β towards r_{SEC} for fixed P_R, P

图 6 固定 P_R,P 时 β 对 r_{SEC} 的影响

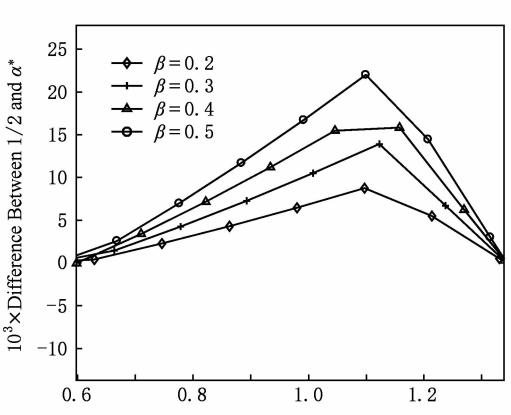
4.2 安全容量增益

为比较 2 种不同协作通信划分策略的优劣,定义安全容量增益为 $r_{\text{gain}}=r_{\text{SEC}}^{\text{half}}-r_{\text{SEC}}^{\alpha}$,其中 $r_{\text{SEC}}^{\text{half}}$ 表示协作通信划分策略为 1/2 的安全容量,r_{SEC}^{α} 表示协作通信划分策略为 α 时的安全容量.在这里,为了实验方便,将 β 设置在 0.2～0.5 之间[3].

如图 7 所示,固定 $\rho=0.2$,$P=3$ W,横坐标为次用户发送节点 R 的发送功率 P_R,纵坐标为 r_{gain} 的值,当 $r_{\text{gain}}>0$ 时,表示协作通信划分策略为 1/2 的更好,反之,如果 $r_{\text{gain}}<0$,则表示协作通信划分策略为 α 更好.如图 7 所示,当 $P_R<1.3$ W 时,协作通信划分策略为 1/2 时表现更好,而当 $P_R>1.3$ W 时,协作通信划分为 α 的策略逐渐占据了优势,但是由图 8 可知,α 策略的最优值 α^* 是不断变化的,其取值范围在[0.383 0,0.615 9]之间.



(a) Complete graph



(b) Partial enlarged detail

Fig. 7 Contrast between strategy α and 1/2 for fixed ρ,P

图 7 两种协作通信划分策略的差值比较

如图 9 所示,对于 $\beta=0.3$,$\rho=0.2$,次用户发送节点 R 的发送功率 P_R 从 0.3 W 递增变化到 2.5 W,由式(2)和引理 3 可知,随着 P_R 增大,α^* 减小,在计算 α^* 的过程中,节点 R 不可避免地产生计算延迟.

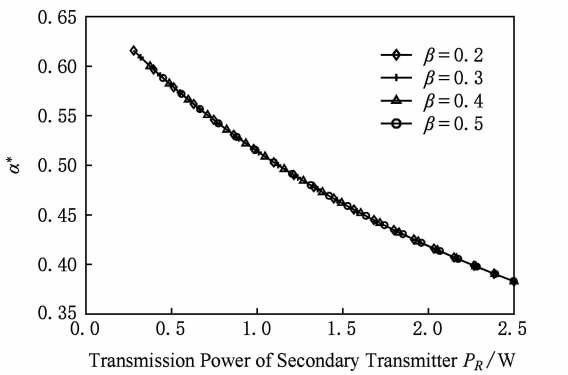


Fig. 8 Influence of P_R towards α^* for fixed ρ,P

图 8 当 $\rho=0.2$,$P=3$W 时 P_R 对 α^* 的影响

图 9 统计了每次 P_R 变化所产生的平均计算延迟,其中每个离散的点为经过 1 000 次 Matlab 仿真实验得出的数据平均值,曲线由多项式拟合得出.可以看出,当 P_R 变化时,2 个算法均有一定计算延迟,由于文献[3]算法除计算最优安全容量以外,还需调整计算 α^*,而本文算法只需计算最优安全容量,经过计算,文献[3]算法的平均计算延迟较本文算法平均多出 7.34 倍.

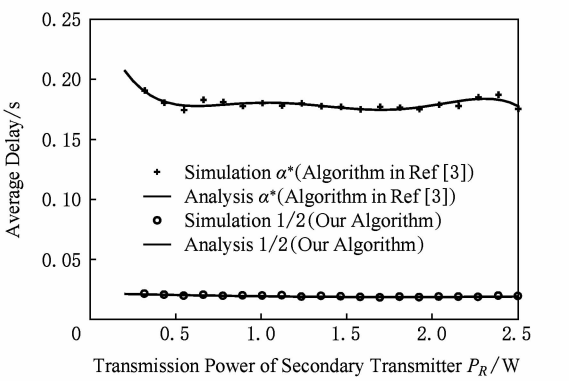


Fig. 9 The average delay when the transmission power of secondary transmitter changes

图 9 次用户发送节点变化发送功率时的平均计算延迟

此外,当 β 取不同值时,P_R 的上界处于不同的位置,在图 7 中已经用箭头标示出来,同时,当 β 值越大,2 种策略之间的差距越显著.在前半部分的差值中,存在着一个最优的 P_R 使得 2 种策略之间的差值最大.通过计算,在最优 P_R 处,当 β 从 0.2～0.5 变化时,本研究策略比 α 策略分别高出 79.28%,80.46%,64.23%,78.85%.

4.3 主用户发送节点能量收集频率变化

本实验研究当主用户发送节点 S 也具备能量收集功能时,在不同的能量收集效率 ε 以及发送功率 P 下,能量收集频率的变化.

如图 10 所示,对于 $\rho=0.2$, $P=3$W, $\beta=0.2$, $\delta=5$,能量收集效率 ε 越高,主用户发送节点能量收集频率越低,因此,适当提高 S 的能量收集效率,有利于提高主用户发送节点 S 的发送效率.

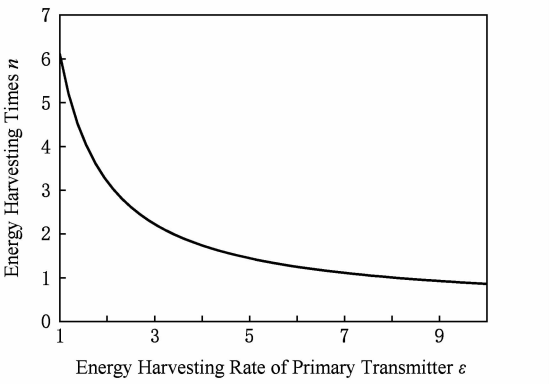


Fig. 10 Energy harvesting times under different ε

图 10 不同 ε 下 S 需要进行能量收集的次数

如图 11 所示,横坐标为主用户发送节点 S 用来发送消息的发送功率 P,纵坐标为在不同的发送功率 P 下,主用户发送节点需要用来收集能量的时间 T 的个数,即能量收集频率. 对于 $\rho=0.2$, $\varepsilon=5$, $\beta=0.2$, $\delta=5$,当主用户发送节点 S 的发送功率增大,能量收集频率呈线性增长. 这是因为在主用户发送节点发送消息时,需要保证发送功率 P 的稳定,当能量收集效率 ε 固定时,每一次 T 时间内收集得到的能量固定,而 P 越大,所需收集的能量就越多,能量收集频率也越高.

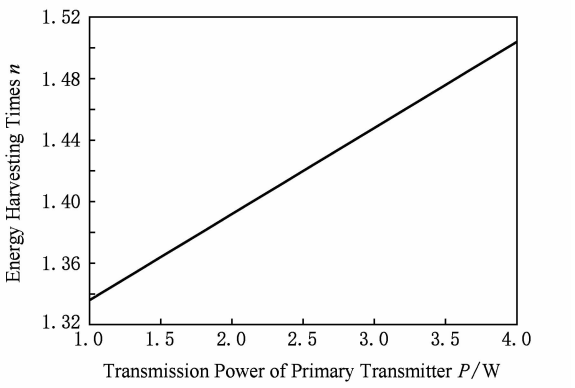


Fig. 11 Energy harvesting times of primary transmitter under different P

图 11 不同 P 下主用户发送节点 S 的能量收集频率

5 总结与展望

在次用户发送节点具有能量收集功能的 EHCR 网络中,本研究对主用户和次用户的传输时隙进行划分,同时设定次用户与主用户之间的协作通信划分策略为 1/2,使得主用户发送节点的安全容量最大. 仿真实验结果表明,主用户最大安全容量 $r_{\mathrm{SEC}}^{\max}$ 与 ρ 成反比. 次用户发送节点的发送功率 P_R 存在最优值,使得主用户安全容量最大,在实际应用中,可以通过实验得出 P_R. 此外,适当增大主用户发送节点的发送功率 P 或者协作通信因子 β 也有助于提高主用户的安全容量. 通过比较 2 种协作通信划分策略的优劣,当 P_R 较小时,本研究的策略表现得较好,而当超过一定阈值之后,α 策略性能更优.

未来将搭建实际物理平台,针对本研究提出的算法进行验证. 同时,我们将深入研究主用户和次用户同时满足安全通信的情况,设计恰当的信道模型,提出合适的算法. 此外,假设消息需要严格在 τ 时间内发送完成,则需调节用户的发送功率或能量收集时长,未来将针对此问题设计自适应算法以满足发送需求.

参 考 文 献

[1] Mitola J I, Maguire G Q J. Cognitive radio: Making software radios more personal [J]. IEEE Personal Communications, 1999, 6(4): 13-18

[2] Paradiso J A, Starner T. Energy scavenging for mobile and wireless electronics [J]. IEEE Pervasive Computing, 2005, 4(1): 18-27

[3] Chen Long, Huang Liusheng, Xu Hongli, et al. Primary secrecy is achievable: Optimal secrecy rate in overlay CRNs with an energy harvesting secondary transmitter [C] //Proc of the 24th Int Conf on Computer Communication and Networks. Piscataway, NJ: IEEE, 2015

[4] Han Biao, Li Jie. Secrecy capacity maximization for secure cooperative ad-hoc networks [C] //Proc of the 32nd IEEE INFOCOM. Piscataway, NJ: IEEE, 2013: 2796-2804

[5] Wyner A D. The wire-tap channel [J]. Bell Labs Technical Journal, 1975, 54(8): 1355-1387

[6] Nosratinia A, Hunter T E, Hedayat A. Cooperative communication in wireless networks [J]. IEEE Communications Magazine, 2004, 42(10): 74-80

[7] Feng Xiaofeng, Gao Xinbo, Zong Ru. Cooperative jamming for enhancing security of cognitive radio networks with multiple primary users [J]. China Communications, 2017, 14(7): 93-107

[8] Yin Sixing, Zhang Eeqing, Qu Zhaowei, et al. Optimal cooperation strategy in cognitive radio systems with energy harvesting [J]. IEEE Transactions on Wireless Communications, 2014, 13(9): 4693-4707

[9] Song Zhengyu, Ni Qiang, Navaie K, et al. On the spectral-energy efficiency and rate fairness tradeoff in relay-aided cooperative OFDMA systems [J]. IEEE Transactions on Wireless Communications, 2016, 15(9): 6342-6355

[10] Zhang Huyin, Wang Jing, Tang Xing. Joint routing and scheduling in cognitive radio vehicular ad hoc networks [J]. Journal of Computer Research and Development, 2017, 54(11): 2445-2455 (in Chinese)
(张沪寅, 王菁, 唐星. 认知无线车载自组织网络中的联合路由调度[J]. 计算机研究与发展, 2017, 54(11): 2445-2455)

[11] Huang Yangchao, Li Zan, Zhou Fuhui, et al. Robust AN-aided beamforming design for secure MISO cognitive radio based on a practical nonlinear EH model [J]. IEEE Access, 2017, 5: 14011-14019

[12] Han Yang, Ting S H, Pandharipande A. Cooperative spectrum sharing protocol with secondary user selection [J]. IEEE Transactions on Wireless Communications, 2010, 9(9): 2914-2923

[13] Luo Shixin, Rui Zhang, Teng J L. Optimal save-then-transmit protocol for energy harvesting wireless transmitters [J]. IEEE Transactions on Wireless Communications, 2013, 12(3): 1196-1207

[14] Zhang Ning, Lu Ning, Cheng Nan, et al. Cooperative networking towards secure communications for CRNs [C]//Proc of the 11th Wireless Communications and Networking Conf. Piscataway, NJ: IEEE, 2013: 1691-1696

[15] Zhang Haiyang, Li Chunguo, Huang Yongming, et al. Simultaneous wireless information and power transfer in a MISO broadcast channel with confidential messages [C]//Proc of the 58th IEEE Global Communications Conf. Piscataway, NJ: IEEE, 2015

[16] Paradiso J A, Starner T. Energy scavenging for mobile and wireless electronics [J]. IEEE Pervasive Computing, 2005, 4(1): 18-27

Wu Jiaxin, born in 1995. PhD candidate. His main research interests include wireless sensor network, cognitive radio network and mobile edge computing.

Wu Jigang, born in 1963. Professor and PhD supervisor. Member of CCF. His main research interests include theoretical computer science, parallel and distributed computing.

Chen Long, born in 1988. PhD, post doctor. His main research interests include wireless sensor network, cognitive radio network, game theory and mobile edge computing. (lonchen@mail.ustc.edu.cn)

Sui Xiufeng, born in 1982. PhD, associate professor of the Institute of Computing Technology, Chinese Academy of Sciences. His main research interests include high performance computer architectures, system performance modeling and evaluation, and cloud computing. (suixiufeng@ict.ac.cn)