ISSN 1004-9037,CODEN SCYCE4
Journal of Data Acquisition and Processing Vol. 30,No. 4,Jul. 2015,pp. 766－773
DOI:10.16337/j.1004-9037.2015.04.007

http://sjcj.nuaa.edu.cn
E-mail:sjcj@nuaa.edu.cn
Tel/Fax:＋86-025-84892742

联合多用户调度与协作干扰选择的无线物理层安全研究

邹玉龙　蒋　元

(南京邮电大学通信与信息工程学院,南京,210003)

摘　要:物理层安全策略作为一种利用无线信道物理特性来对抗窃听者的有效手段,已经吸引了越来越多的关注。本文重点研究多用户调度与协作干扰技术在无线通信物理层安全方面的表现,并将两种技术有机结合,深入研究无线网络的通信安全。通过联合采用多用户调度方案与协作干扰技术以增强无线通信安全,在多用户无线通信网络中,采用多用户调度策略,在选择最优信道进行通信的同时,对窃听节点进行协作干扰,在合法用户端通过波束权重矩阵对干扰信号进行合并以消除干扰信号对接收端的影响,最终达到在不干扰合法通信的前提下极大地干扰窃听信道,最终增强无线网络的通信安全。数值仿真表明,联合多用户调度与协作干扰的方案的安全中断概率明显低于仅采用多用户调度的方案。
关键词:物理层安全;多用户调度;协作干扰;安全中断概率;安全分集度
中图分类号:TN911.1　　**文献标志码**:A

Physical Layer Secrecy Analysis of Joint User Scheduling and Jammer Selection

Zou Yulong, Jiang Yuan

(College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China)

Abstract: Physical layer security (PLS) is an effective means to protect communications against eavesdropping attacks by exploiting physical characteristics of wireless channels. As the information and communication technology (ICT) has been developed for decades, PLS attracts more and more attention of researchers. Here, PLS performance of the joint multi-user scheduling and the cooperative jammer selection is explored. With the combination of the two techniques, the wireless communication security is investigated. In a wireless communication system with multiple users, multi-user scheduling schemes are adopted to choose one legitimate user of the best channel to transmit signals. Meanwhile, the eavesdroppers are interfered to keep the transmissions between BS and legitimate users confidential for avoiding the interference to the legitimate users. CJ signal is designed so that nulls are formed at the legitimate users. Simulation results show that the joint multi-user scheduling and cooperative jammer scheme has a better performance of security than the multi-user scheduling scheme.
Key words: physical layer security; multi-user scheduling; cooperative jammer; secrecy outage probability; secrecy diversity order

---

基金项目:国家自然科学基金(61302104,61401223)资助项目;江苏省自然科学基金(BK20140887)资助项目;江苏省高校自然科学研究重大项目(15KJA510003)资助项目。
收稿日期:2015-06-05;**修订日期**:2015-06-30

引　　言

信息通信技术在社会的每个领域都起着极为重要的作用,而无线通信作为一种便捷有效覆盖广泛的通信技术,更是其中翘楚。无线通信利用无线电波传播距离远,无需铺设线路的优势,成为人们生活中密不可分的通讯手段。然而,由于无线信道广播的自然特性,在将用户特定用于窃听正在传输的数据时,所有在信道覆盖区域内的用户都可能窃听到信道传输的信号,无线通信安全愈发受到关注,无线通信系统使得合法接受节点成功接收信息的同时对抗潜在窃听节点的能力愈发重要,物理层安全策略在如此背景下应运而生。尽管传统的安全防护机制主要基于在通信更高层的加密算法,物理层通信安全还是在近来吸引了相当大的关注[1-4]。

在早期由 Wyner 和 Maurer 进行了基础的理论研究之后,经过一段时间的沉寂,物理层安全的研究工作在近十年开始复苏,重新回到了通信领域的研究前沿[5-6]。物理层安全的原理在于探索制约信息量的通信信道与噪声固有的随机性,针对无线网络中窃听者的存在,采取多种技术方法来降低窃听者的信道容量,增强合法通信信道的安全容量。为了提升无线衰落环境下的安全容量,研究人员近来探索了各种无线物理层安全增强方法,包括人工噪声[7-9]、波束成形[10]、协作中继[11]、多输入多输出(MIMO)[12]、多用户调度[1]和协作干扰[13-15]等技术手段。而干扰与反干扰策略,作为军方长期保有很强兴趣的研究方向,也逐步演化为科学研究以及民用的增强通信安全的手段[16]。

相关科学家提出了利用协作干扰的方法来改善无线物理层安全,即通过无线网络中的协作干扰节点产生人工噪声以提高点对点安全容量,分析表明在多天线通信链路中,目标节点与多个协作干扰节点按照约定协议工作,可以实现所产生的人工噪声在不影响接收节点的情况下有效干扰窃听节点,从而实现对合法用户通信不造成任何不利影响的前提下显著恶化窃听信道质量[17]。另外,由于频谱资源稀缺,绝大多数无线通信网络均使得多个合法用户分享同一频谱,即便在同一无线网络中,每个用户的信噪比仍然有着极大的差异。基于这种现实状况,一种为使得输出信息量最大化,通过选择拥有最佳瞬时信噪比的用户进行通信的策略也随之而生,称之为多用户调度[18]。

本文旨在联合采用多用户调度方案与协作干扰技术以增强无线通信安全,在多用户无线通信网络中,在选择最优信道进行通信的同时,对窃听节点进行协作干扰,在合法用户端通过波束权重矩阵对干扰信号进行合并以消除干扰信号对接收端的影响,最终达到在不干扰合法通信的前提下,极大地干扰窃听信道,最终增强无线网络的通信安全。

1　模型描述

如图 1 所示,本文所研究的无线通信系统由 1 个带有 L 个接收天线的目标节点 D、1 个窃听节点 E、M 个合法用户(U_i, $i=1,\cdots,M$)以及 K 个协作干扰节点(J_k,$k=1,\cdots,K$)构成,其中所有节点均共享同一频段进行通信。鉴于主要研究的是由合法用户到目标节点的通信情景,该情景是一个很经典的上行链路情景,在情景中,有 1 个窃听节点随时可能入侵上行链路以获取传输的信息。将 M 个用户简写为 $\{U_i|i=1,\cdots,M\}$,同理,将 K 个协作干扰节点简写为 $\{J_k|k=1,\cdots,K\}$。假设任何两个节点之间的无线信道均为瑞利衰落信道模型,并且衰落增益在一个时隙内保持不变。同时,假设所有接收节点均具有零均值和功率谱密度为 N_0 的高斯白噪声,那么在目标节点处接收到的噪声可以简写为 $n_b\sim CN(0,N_0)$,同理,在窃听节点处接收到的噪声简写为 $n_e\sim CN(0,N_0)$,同时干扰节点产生的人工噪声简写为 $\{S_k|k=1,\cdots,K\}$,其中 $E[|S_k|^2]=1$,且干扰节点处采用预编码矩阵使得目标节点接收的人工噪声为零空间,$\boldsymbol{W}^{\mathrm{T}}=[w_1,w_2,\cdots,w_K]^{\mathrm{T}}$,其中,$\|\boldsymbol{W}^{\mathrm{T}}\|^2=1$。此外,合法用户与协作干扰节点的发射功率分别记做 P_1 和 P_2。

假设在某时隙选择合法用户 U_i 传输信号 x_s 到目标节点 D 处,则目标节点接收到信号可表示为

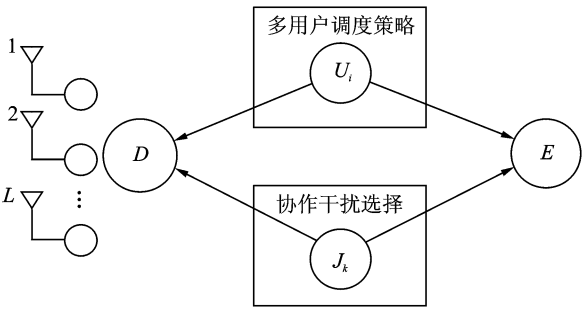

图 1 系统模型图

Fig. 1 System model

$$y_{id} = \sqrt{p_1}\, h_{id} x_s + \sqrt{p_2}\, \boldsymbol{H}_{K,L}^{D} \boldsymbol{W}^{\mathrm{T}} + n_d \quad i = 1, 2, \cdots, M \tag{1}$$

式中 $\boldsymbol{W}^{\mathrm{T}}$ 即为协作干扰处的预编码矩阵，且 $\boldsymbol{W}^{\mathrm{T}} = [w_1, w_2, \cdots, w_K]^{\mathrm{T}}$，而 $\boldsymbol{H}_{K,L}^{D}$ 则为合法用户到目标节点的信道参量矩阵，且 $\boldsymbol{H}_{k,L}^{D} = [h_{k,1}^{d}, h_{k,2}^{d}, \cdots, h_{k,L}^{d}] \in \mathbf{C}^{k \times L}$，那么 $\boldsymbol{H}_{K,L}^{D} = [H_{1,L}^{D}, H_{2,L}^{D}, \cdots, H_{K,L}^{D}]^{\mathrm{T}} \in \mathbf{C}^{K \times L}$，根据 Shannon 信道容量定理，可以得到合法用户 U_i 到目标节点 D 的信道容量为

$$C_{id} = \log_2 \left(1 + \frac{p_1 \left| h_{id} \right|^2}{p_2 \left| \boldsymbol{H}_{K,L}^{D} \boldsymbol{W}^{\mathrm{T}} \right|^2 + N_0}\right) \tag{2}$$

由于无线电传播具有广播特性，那么合法用户 U_i 到目标节点 D 的信号传输可能也被窃听节点 E 所入侵并窃取信息，与在目标节点接收到的信号表达方式相似，在窃听节点接收到的信号可以表示为

$$y_{ie} = \sqrt{p_1}\, h_{ie} x_s + \sqrt{p_2}\, \boldsymbol{H}_{L}^{E} \boldsymbol{W}^{\mathrm{T}} + n_e \quad i = 1, 2, \cdots, M \tag{3}$$

式中 $\boldsymbol{W}^{\mathrm{T}}$ 即为协作干扰处的预编码矩阵，且 $\boldsymbol{W}^{\mathrm{T}} = [w_1, w_2, \cdots, w_K]^{\mathrm{T}}$，而 $\boldsymbol{H}_{K,L}^{E}$ 则为合法用户到目标节点的信道参量矩阵，且 $\boldsymbol{H}_{L}^{E} = [h_1^e, h_2^e, \cdots, h_L^e] \in \mathbf{C}^{1 \times L}$。根据 Shannon 信道容量定理，可以得到合法用户 U_i 到目标节点 E 的信道容量为

$$C_{ie} = \log_2 \left(1 + \frac{p_1 \left| h_{ie} \right|^2}{p_2 \left| \boldsymbol{H}_{L}^{E} \boldsymbol{W}^{\mathrm{T}} \right|^2 + N_0}\right) \tag{4}$$

根据物理层安全理论，在 Shannon 首先建立信息安全理论的基础下，Wyner 引入了一个弱化的窃听信道模型并且定义了安全速率这一量纲来衡量主信道容量与窃听信道容量之差，因此由合法用户 U_i 到目标节点 E 链路的安全速率可以表示为

$$C_i^s = C_{id} - C_{ie} \tag{5}$$

2 无线通信网络中的基于联合多用户调度与协作干扰选择的物理层安全分析

2.1 协作中继选择方案

由于模型中加入了多个协作干扰节点人为地干扰了窃听节点的信号接收，因此在通信过程中，需要考虑如何选择其中的部分协作干扰节点来使得在目标节点的信号接收不受影响的同时，窃听节点的信道容量最低。目标节点通常具备多天线接受信号能力来消除干扰信号带来的影响。其基本原理在于，多天线接受干扰信号时，由于目标节点与协作干扰节点事先约定将使用预定的干扰信号或者通过干扰设计使得目标节点提前获知干扰信号形式，因此实现降低窃听节点性能而不影响目标节点的信号接收。鉴于具有多天线的窃听节点有能力抵抗协作干扰信号，为了降低窃听节点天线阵的自由度，本文设计的协作干扰信号应该由多个独立发出的噪声构成。另外，为了避免干扰合法用户，本文设计协作干扰信号因此在合法用户处接收到的干扰信号为 0，那么协作干扰信号设计的问题就转变为设计一个预编码矩

阵的问题。

$$\begin{aligned} &\arg\max \left| \boldsymbol{H}_{K,L}^{E} \boldsymbol{W}^{\mathrm{T}} \right|^{2} \\ &\text{s. t.} \quad \boldsymbol{H}_{K,L}^{D} \boldsymbol{W}^{\mathrm{T}} = 0 \end{aligned} \tag{6}$$

即找到一组 $\boldsymbol{W}^{\mathrm{T}}=[w_1,w_2,\cdots,w_k]$,使得协作干扰信号对合法用户干扰最小,且对窃听用户干扰最大,此优化问题仅能找到局部最大值。

2.2 多用户调度方案的安全中断分析

本节提出 Round-robin 用户调度策略、Optimal 用户调度策略和 Suboptimal 用户调度策略 3 种多用户调度方案,首先以 Round-robin 用户调度策略进行安全中断分析,并以该策略为基准,用于与 Optimal 用户调度策略和 Suboptimal 用户调度策略的安全中断性能比较。同时,在提出多用户方案之前,假设所有链路的信道状态信息(Channel state information, CSI)状态均为已知,尤其是在 Optimal 用户调度策略中,因为其目的在于使得有合法用户到目标节点链路的安全速率最大化,需要 CCC(Centralized common controller)获得所有链路(包括窃听信道)的 CSI 并据此进行用户调度。然而,本文提出一种折中方案,兼顾多用户分集增益与安全容量,不同于 Optimal 用户调度策略要求极高,难以实现,从而改善调度方案的整体性能与效率,简称为 Suboptimal 用户调度策略。Suboptimal 用户调度策略的设计前提即是假设窃听信道 CSI 未知,因此,在 Suboptimal 用户调度策略中,只需假设主信道 CSI 已知即可。

2.2.1 Round-robin 用户调度策略

Round-robin 就是依次轮转对无线网络中的用户进行信号传输的调度,该策略使得在无线网络中的每个合法用户有均等的机会接入频谱进行信号传输。通常,为了衡量其他的多用户调度策略的性能,Round-robin 策略将被采用作为一个标杆。按照通常的定义,安全中断事件发生在安全速率低于一个预先设定的安全速率 R_s 时,那么,假设无线网络中某合法用户 U_i 传输信号到目标节点 D 中,可以得到 U_i-D 链路的安全中断概率表示如下

$$P_{\mathrm{out},i}=\Pr(C_i^s<R_s) \tag{7}$$

2.2.2 Optimal 用户调度策略

Optimal 用户调度策略是一种接近于完美的调度策略,其要求 CCC 对于无线网络中所有节点(包括窃听节点)的 CSI 均已知,因此可以得出通信系统的安全容量,并据此调度安全状况最佳的合法用户进行信号传输。那么在这个分段中,根据先前的定义,提出 Optimal 用户策略的标准如下

$$\text{Optimal User}=\max_{i\in M} C_i^s \tag{8}$$

那么在任意时隙被选中合法用户与目标节点信道的安全中断概率可以表示为

$$P_{\mathrm{out},i}^{\mathrm{Optimal}}=\Pr(\max_{i\in M} C_i^s<R_s) \tag{9}$$

2.2.3 Suboptimal 用户调度策略

Suboptimal 策略一般而言可用于替代 Optimal 策略,考虑到现实情景中 CCC 比较难以获取无线网络中基站到窃听节点处的 CSI,那么在具体决定使哪个用户进行信号传输时,便无法确保所选信道的安全容量最大,但是 CCC 对于无线网络中基站到用户间的 CSI 完全了解,即可采用 Suboptimal 策略,选择瞬时主信道容量最大的用户进行信号传输,其具体调度标准可以表示为

$$\text{Optimal User}=\max_{i\in M}\left| h_{ib} \right|^{2} \tag{10}$$

具有 M 个合法用户的 Suboptimal 用户调度策略的安全中断概率应为其最佳用户的安全中断概率,可以表示为

$$P_{\mathrm{out}}^{\mathrm{Sub}}=\Pr(C_o^s<R_s) \tag{11}$$

2.3 多用户调度方案分集增益的分析

安全中断概率仅能体现合法用户到目标节点的安全传输方面的表现,对于合法用户数量变化与窃

听节点数量变化均无直观的反映，因此需要对这 3 种多用户调度策略的多用户分集增益进行分析，通过分集度从另一角度来衡量多用户调度策略的安全性能。根据对传统分集度的定义，参照文献[19]中的描述，其表达式如下

$$d=-\lim_{\mathrm{SNR}\to\infty}\frac{\log P_e(\mathrm{SNR})}{\log \mathrm{SNR}} \tag{12}$$

式中 SNR 为信噪比，而 P_e(SNR)则为在信噪比 SNR 下的误码率(此时误码率为信噪比的函数)，而当合法用户发射信号功率趋近于无穷大时，其安全中断概率趋近于一个非零常量，且当合法用户发射信号功率趋近于无穷大时，其安全中断概率仅由主信道衰落系数 h_{id} 和窃听信道衰落系数 h_{ie} 决定，其所受干扰与噪声几乎可以忽略不计，这意味着传统分集度定义式对本节的具体参量并不适用，需要对该定义式进行变换。此时需引入主信道与窃听信道比值(Main-to-eavesdropper ratio，MER)这一参量，其定义式为 $\lambda=\frac{\sigma_m^2}{\sigma_e^2}$，其中 σ_m^2 与 σ_e^2 分别为主信道衰落系数与窃听信道衰落系数的方差，根据文献[19]中的定义，其变换后的表达式如下

$$d=-\lim_{\lambda\to\infty}\frac{\log P_{\mathrm{out,floor}}}{\log\lambda} \tag{13}$$

式中 $P_{\mathrm{out,floor}}$ 即为当合法用户发射信号功率 P_1 趋近于无穷大时，其安全中断概率无限接近的极限值。文献[21]对这 3 种多用户调度方案的分集度已经进行了相关的推导与证明，由最终 3 种多用户调度策略的分集度可以看出，Optimal 用户调度策略与 Suboptimal 用户调度策略的分集度均为满分集度，其多用户分集增益均可以达到最大，当无线网络中合法用户数相应增加时，其获得的多用户分集增益也越大。而 Round-robin 用户调度策略的分集度则为 1，无论用户数如何变化，其多用户分集增益始终较差。

(1) Round-robin 用户调度策略

具有 M 个合法用户的 Round-robin 用户调度策略的分集度为 $d_{\mathrm{Round}}=1$，这表明，无论用户数如何变化，Round-robin 用户调度策略的分集度始终为 1，其对于无线通信系统的分集增益情况较差，无论用户数如何变化，其多用户分集增益始终较差。

(2) Optimal 用户调度策略

具有 M 个合法用户的 Optimal 用户调度策略的分集度为 $d_{\mathrm{Optimal}}=M$，这表明，无论用户数如何变化，Optimal 用户调度策略的分集度始终在数值上等于用户数，因此，其对于无线通信系统的分集增益情况较好，当无线网络中合法用户数相应增加时，其获得的多用户分集增益也越大。

(3) Suboptimal 用户调度策略

具有 M 个合法用户的 Suboptimal 用户调度策略的分集度为 $d_{\mathrm{Sub}}=M$，这表明，无论用户数如何变化，Suboptimal 用户调度策略的分集度始终在数值上等于用户数，因此，其对于无线通信系统的分集增益情况较好，当无线网络中合法用户数相应增加时，其获得的多用户分集增益也越大。

3 数值结果与分析

针对多用户调度策略进行物理层安全方面的理论分析，多用户分集无论对系统的平均输出还是安全中断现象均有增益。本文还提出一种基于多协作干扰的选择方案，由多个独立干扰节点发出人工噪声对窃听节点进行误导，根据 Shannon 信道容量理论，通过降低窃听信道容量，削弱窃听节点解码与信号接收的能力来增强系统的信息安全。所有实验均在 Matlab 2012b 环境下编写调试完成。

本文通过对基于联合多用户调度与协作干扰选择的方案给出一系列的数值结果进行比较，针对 Round-robin 用户调度策略、Suboptimal 用户调度策略与 Optimal 用户调度策略，结合协作干扰方法，用 Matlab R2012b 软件平台进行数值仿真。通过首先对系统中的无线信道进行仿真模拟，以较大的信道

样本容量进行安全中断现象统计,最终得出安全中断概率的仿真值(统计值)。

图 2 设定的参量数值为:无线网络内合法用户数 $M=8$,协作中继数 $K=3$,安全速率 $R_s=1$ bit/s/Hz,协作干扰发射功率与用户信号发射功率比 $P_1/P_2=1/5$,另外,合法用户 U_i 与目标节点 D 通信的主信道方差 $\sigma_{ib}^2=1$,合法用户 U_i 与窃听节点 E 通信的窃听信道方差 σ_{ie}^2 以及协作干扰节点 J_k 与窃听节点 E 通信的干扰信道方差 σ_{ke}^2 均等于 0.4。图 2 中给出了 Round-robin 用户调度策略、Suboptimal 用户调度策略与 Optimal 用户调度策略在以上参量下的安全中断概率图,分为不加协作干扰情景与附加协作干扰情景两部分,当合法用户的发射功率 P 趋近于无穷大时,Round-robin 用户调度策略、Suboptimal 用户调度策略与 Optimal 用户调度策略相对应的安全中断概率随之递减,而当合法用户的发射功率 P 增加至超过一定数量时,这 3 种调度策略对应的安全中断概率均逐渐逼近于一个非零常量,该非零常量就是所谓的安全中断概率下界。图 2 也很好地印证了 Optimal 用户调度策略相对于其他用户调度策略具有最佳安全性能的推断,而 Suboptimal 用户调度策略也具有较好的安全性能,且 Round-robin 用户调度策略的安全性能较差。

图 3 设定的参量数值为:无线网络内合法用户数 $M=8$,协作中继数 $K=3$,用户信号发射功率 $q_1=10$,协作干扰发射功率与用户信号发射功率比 $q_2/q_1=1/5$,另外,合法用户 U_i 与目标节点 D 通信的主信道方差 $\sigma_{ib}^2=1$,合法用户 U_i 与窃听节点 E 通信的窃听信道方差 σ_{ie}^2 以及协作干扰节点 J_k 与窃听节点 E 通信的干扰信道方差 σ_{ke}^2 均等于 0.4。图 3 中给出了 Round-robin 用户调度策略、Suboptimal 用户调度策略与 Optimal 用户调度策略在以上参量下的安全中断概率图,分为不加协作干扰情景与附加协作干扰情景两部分,当系统既定安全速率逐渐增加时,Round-robin 用户调度策略、Suboptimal 用户调度策略与 Optimal 用户调度策略相对应的安全中断概率随之递增,而当系统既定安全速率达到一定数量时,这 3 种调度策略对应的安全中断概率均逐渐逼近于 1。图 3 也很好地印证了 Optimal 用户调度策略相对于其他用户调度策略具有最佳安全性能的推断,而 Suboptimal 用户调度策略也具有较好的安全性能,且 Round-robin 用户调度策略的安全性能较差。

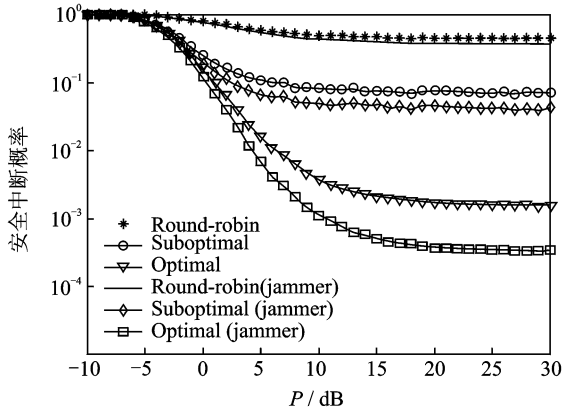

图 2 随信号发射功率 P 变化的基于联合多用户调度与协作干扰的性能比较图

Fig. 2 Secrecy outage probability versus maximum transmit power P of the Round-robin scheduling, the Suboptimal user scheduling and the Optimal user scheduling schemes

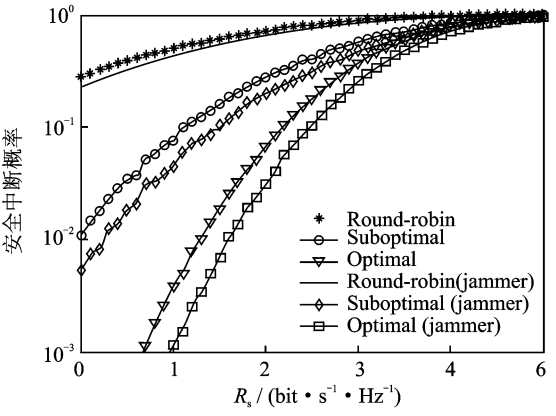

图 3 随既定安全速率 R_s 变化的基于联合多用户调度与协作干扰的性能比较图

Fig. 3 Secrecy outage probability versus secrecy rate R_s of the Round-robin scheduling, the Suboptimal user scheduling and the Optimal user schedulig schemes

图 4 中，设定的协作中继数 $K=3$，安全速率 $R_s=1$ bit/s/Hz，用户信号发射功率 $q_1=10$，协作干扰发射功率与用户信号发射功率比 $q_2/q_1=1/5$，另外，合法用户 U_i 与目标节点 D 通信的主信道方差 $\sigma_{ib}^2=1$，合法用户 U_i 与窃听节点 E 通信的窃听信道方差 σ_{ie}^2 以及协作干扰节点 J_k 与窃听节点 E 通信的干扰信道方差 σ_{ke}^2 均等于 0.4。图 4 中给出了 Round-robin 用户调度策略、Suboptimal 用户调度策略与 Optimal用户调度策略在以上参量下的安全中断概率图，分为不加协作干扰情景与附加协作干扰情景两部分，当系统中合法用户数增加时，Round-robin 用户调度策略、Suboptimal 用户调度策略与 Optimal 用户调度策略相对应的安全中断概率随之递减，然而 Round-robin 用户调度策略几乎没有变化（变化极小），这表示 Round-robin 用户调度策略几乎不会因为用户数变化而得到增益，而 Suboptimal 用户调度策略与 Optimal 用户调度策略的安全中断概率随着用户数增加而极大地减小。图 4 也很好地印证了 Optimal 用户调度策略相对于其他用户调度策略具有最佳安全性能的推断，而 Suboptimal 用户调度策略也具有较好的安全性能，且 Round-robin 用户调度策略的安全性能较差。因此，如果应用 Suboptimal 用户调度策略与 Optimal 用户调度策略，可以通过增加合法用户数来增强系统中主链路的通信安全。

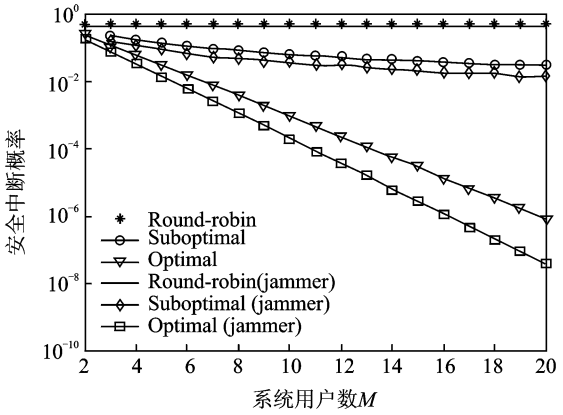

图 4 随网络中合法用户数变化的基于联合多用户调度与协作干扰的性能比较图

Fig. 4 Secrecy outage probability versus the number of users M of the Round-robin scheduling, the Suboptimal user scheduling and the Optimal user scheduling schemes

4 结束语

本文对一个多用户无线网络进行了安全中断概率与分集度的理论与数值分析，针对联合多用户调度与协作干扰选择对抗窃听者的方案，给出了充分的图例与理论依据来证明其极强的安全性能。当无线网络中的合法用户向目标节点传输信号时，存在窃听者可能入侵该链路并窃取信息，本文提出了一种结合了协作干扰选择与多用户调度方案，对 Round-robin 用户调度策略、Suboptimal 用户调度策略与 Optimal 用户调度策略这 3 种策略在不加协作干扰情景与附加协作干扰情景进行理论与仿真分析，结果表明，Optimal 用户调度策略相对于其他用户调度策略具有最佳安全性能的推断，而 Suboptimal 用户调度策略也具有较好的安全性能，且 Round-robin 用户调度策略的安全性能最差。另外，本文还从安全中断概率的理论表达式中推导出 3 种策略相对应的分集度，通过分集度从用户数这个角度来衡量多用户调度策略的安全性能，由最终 3 种多用户调度策略的分集度可以看出，Optimal 用户调度策略与 Suboptimal用户调度策略的分集度均为满分集度，其多用户分集增益均可以达到最大，而 Round-robin 用户调度策略的分集度则为 1，无论用户数如何变化，其多用户分集增益始终较差。鉴于 3 种策略对于无线网络中不同节点的 CSI 要求存在一定的差别，考虑到具体实现的公平性问题，Suboptimal 用户调度

策略结合协作干扰的方案被认为最为合理且易于实现。

参考文献:

[1] Zou Yulong, Wang Xianbin, Shen Weiming. Physical-layer security with multiuser scheduling in cognitive radio networks [J]. IEEE Transactions Communications, 2013,61(12):5103-5113.

[2] Schneier B. Cryptographic design vulnerabilities [J]. IEEE Computer, 1998,31(9):26-33.

[3] Kapoor G, Piramithu S. Vulnerabilities in some recently proposed RFID ownership transfer protocols[J]. IEEE Commun Lett, 2010,14(3):260-262.

[4] Barenghi A, Breveglieri L, Koren I, et al. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures[J]. Proc IEEE, 2012,100(11):3056-3076.

[5] Mukherjee A, Ali S, Fakoorian A, et al. Principles of physical layer security in multiuser wireless networks: A survey[J]. IEEE Communications Surveys & Tutorials, 2014,16(3):1550-1573.

[6] 胡爱群,李古月.无线通信物理层安全方法综述[J].数据采集与处理,2014,29(3):341-350.
Hu Aiqun, Li Guyue. Physical layer security in wireless communication: A survey[J]. Journal of Data Acquisition and Processing, 2014,29(3):341-350.

[7] Goel S, Negi R. Guaranteeing secrecy using artificial noise[J]. IEEE Trans Wireless Commun, 2008,7(6):2180-2189.

[8] Zhou X, McKay M. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation[J]. IEEE Trans Veh Technol, 2010,59(8):3831-3842.

[9] Massey J L. An introduction to contemporary cryptology[J]. Proceedings of the IEEE, 1988,76(5):533-549.

[10] Shafiee S, Liu N, Ulukus S. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel[J]. IEEE Trans Inf Theory, 2009,55(9):4033-4039.

[11] Zou Y, Wang X, Shen W. Optimal relay selection for physical layer security in cooperative wireless networks [J]. IEEE J Sel Areas Commun, 2013,31(10):2099-2111.

[12] Tang X, Liu R, Spasojevic P, et al. Interference assisted secret communication[J]. IEEE Trans Inf Theory, 2009,57(5):3153-3167.

[13] Khisti A, Wornell G. Secure transmission with multiple antennas—I: The MISOME wiretap channel[J]. IEEE Trans Inf Theory, 2010,56(7):3088-3104.

[14] Renna F, Laurenti N, Poor H V. Physical-layer secrecy for OFDM transmissions over fading channels[J]. IEEE Trans Inf Forensics Security, 2012,7(4):1354-1367.

[15] Larsson E G. On the combination of spatial diversity and multiuser diversity[J]. IEEE Communications Letters, 2004,8(8):517-519.

[16] Deng Hao, Wang Huiming, Guo Wei, et al. Secrecy transmission with a helper: To relay or to jam[J]. IEEE Transactions on Information Forensics and Security, 2015,10(2):293-307.

[17] Yang J, Kim Il-Min, Kim Dong In. Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers[J]. IEEE Transactions on Wireless Communications, 2013,12(6):2840-2852.

[18] Spencer Q H, Peel C B, Swindlehurst A L, et al. An introduction to the multi-user MIMO downlink[J]. IEEE Commun Mag, 2004,42(10):60-67.

[19] Zou Yulong, Li Xuelong, Liang Yingchang. Secrecy outage and diversity analysis of cognitive radio systems [J]. IEEE Journal on Selected Areas in Communications, 2014,32(11):2222-2236.

作者简介:

邹玉龙(1984-),男,教授、博士生导师,研究方向:认知无线电、中继协作通信、以及无线网络安全等无线通信前沿技术,E-mail:yulong.zou@njupt.edu.cn。

蒋元(1993-),男,硕士研究,研究方向:无线网络安全、认知无线电等。