Digital Communications and Networks (2015) 1, 68-74

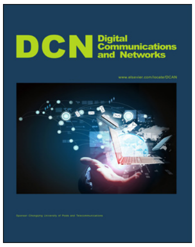
HOSTED BY

ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

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



Secrecy outage analysis of multi-user multi-eavesdropper cellular networks in the face of cochannel interference

Yuan Jiang, Jia Zhu, Yulong Zou*

School of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, PR China

Received 29 December 2014; received in revised form 2 February 2015; accepted 28 February 2015
Available online 24 March 2015

KEYWORDS
Physical layer security;
Eavesdropping attack;
Multi-user scheduling;
Cochannel interference;
Secrecy outage probability;
Secrecy diversity

Abstract

This paper studies the physical-layer security of a multi-user multi-eavesdropper cellular network, which is composed of multiple users communicating with a base station while the eavesdroppers may intercept the communications from users to the base station (BS). The cellular network is a time-slotted system with simultaneously transmission, in each time slot, a single user is scheduled to transmit messages to BS while the remaining users opportunistically receive information. Considering multiple users available in the cellular network, we present three multi-user scheduling schemes, namely the round-robin scheduling scheme as well as the suboptimal and optimal user scheduling schemes to improve the security of communication (from users to BS) against eavesdropping attacks. We only need to assume that the channel state information (CSI) of the main link spanning from users to BS is known in the suboptimal scheduling. On the contrary, the optimal scheduling is designed by assuming that the CSI of the main link and wiretap link (spanning from users to the eavesdropper) are available. We further carry out secrecy diversity analysis and show that the round-robin always achieves only one diversity order, whereas the suboptimal and optimal user scheduling schemes achieve the full diversity. In addition, numerical results illustrate that the optimal scheduling performs the best and the round-robin has the worst performance in terms of the secrecy outage probability. Last, as the number of users increases, the secrecy outage probabilities of the suboptimal and optimal scheduling schemes decrease significantly.

*Corresponding author.
E-mail addresses: tracykyle93@gmail.com (Y. Jiang), jiazhu@njupt.edu.cn (J. Zhu), Yulong.Zou@njupt.edu.cn (Y. Zou).

Peer review under responsibility of Chongqing University of Posts and Telecommunications.

http://dx.doi.org/10.1016/j.dcan.2015.02.002

1. Introduction

The major challenges in cellular networks include the co-channel interference mitigation and the eavesdropping attack defense [1]. Especially the security of communication has been a crucial issue for cellular networks [2]. By exploiting the physical characteristics of wireless channels, physical-layer security is now emerging as an effective means to protect the communications against eavesdropping [3-5]. If the main channel (from source to destination) is better than the wiretap channel (from source to eavesdropper), the source can transmit to the destination at a positive data rate reliably and securely [6]. Wyner introduced the notion of the secrecy capacity developed from an information theoretic prospective in a discrete memoryless wiretap channel, which is obtained as the difference of the capacity between the main channel and wiretap channel [3]. Besides, research efforts were devoted to improving the wireless physical-layer security by employing artificial noise [7-9]. We also consider cochannel interference management via cell splitting and beamforming transmission which improve the spectrum-efficiency and energy-efficiency of cellular network communication [10,11].

Focusing on the transmission capacity of secure communication, we analyze how to achieve a certain level of security in an interference-limited network [12]. This paper is focused on the secrecy performance with multi-user scheduling schemes in a cellular network. We examine the use of multi-user scheduling for improving the physical-layer security and analyze its secrecy outage probability in the presence of multiple eavesdroppers [6]. The secrecy outage probability is defined as the probability that the secrecy capacity drops below a secrecy rate (i.e., R_s). Furthermore, we investigate the effect of co-channel interference on secrecy outage probability performance.

In this paper, we study physical layer security in the uplink of cellular networks, where multiple users simultaneously transmit confidential messages to BS. Meanwhile the confidential messages transmitted to BS may be tapped by the eavesdroppers, which also suffer from the co-channel interference [1,12]. In the beginning, we employ three multi-user scheduling schemes (namely the round-robin, the suboptimal, the optimal scheduling schemes) to protect the users–BS transmissions against the eavesdroppers. Unlike the suboptimal scheduling that only needs to know the CSI of the main channel, the optimal scheduling requires the perfect CSI of both the main link and the wiretap link. Since the CSI of the eavesdroppers are challenging to obtain in cellular networks, the suboptimal scheduling scheme is more attractive from this perspective. Then, we derive calculus-form secrecy outage probability expressions for the multi-user scheduling schemes to help analyze the secrecy performance. Finally, we figure out the secrecy diversity order of three schemes and observe that the round-robin achieves the diversity order of only one, while the suboptimal and optimal user scheduling schemes achieve the diversity order of M, where M is the number of users.

The reminder of the paper is organized as follows. First, we describe the system model of a multi-user multi-eavesdropper cellular network in Section 2. Then, Section 3 presents the round-robin scheduling scheme, the suboptimal and optimal user scheduling schemes for protecting the cellular transmissions against eavesdropping. In Section 4, the calculus-form expressions of secrecy outage probability are derived for the diversity analysis, followed by Section 5, where numerical secrecy results are provided. In Section 6, we finally provide some conclusions.

2. System model and problem formulation

Taking a cellular network presented in Fig. 1 into consideration, which is made up of one BS, M users and N eavesdroppers (uncoordinated) and K co-BS sharing the same spectrum. Users transmit signals to BS through uplinks, in which interferers are from the neighbouring cochannel base stations. Considering M users communicate with BS, which is a typical uplink transmission scenario in cellular networks, that are N eavesdroppers attempting to intercept the packets transmitted from users to BS. We denote M users and N eavesdroppers by $\mathcal{S}=\{\mathrm{U}_i|i=1,2,\ldots,M\}$ and $\mathcal{E}=\{\mathrm{E}_j|j=1,2,\ldots,N\}$, for convenience. In addition, the thermal noises received at BS and eavesdroppers are complex Gaussian distributed. Therefore, the noise at BS which is denoted by n_b can be modeled as a complex Gaussian random variable with zero mean and variance N_0, which is written by $n_b \sim \mathcal{CN}(0,N_0)$. We can similarly model the noise received at eavesdroppers E_j, denoted by n_{e_j}, as a complex Gaussian random variable i.e. $n_{e_j} \sim \mathcal{CN}(0,N_0)$, respectively.

Considering that U_i transmits signal x_i to BS with power p while co-channel interference i_k is transmitted at the power of q, hence we can express the signal received at BS as

$$y_{ib} = \sqrt{p}h_{ib}x_i + \sum_{k=1}^{K} \sqrt{q}g_{kb}i_k + n_b \tag{1}$$

where h_{ib} is the fading coefficient of the channel from U_i to BS, K is the number of total cochannel interferers, g_{kb} is the channel from k-th interferer to BS, $n_b \sim \mathcal{CN}(0,N_0)$ represents the thermal noise received at BS. By applying Shannon's channel capacity formula, we can obtain the

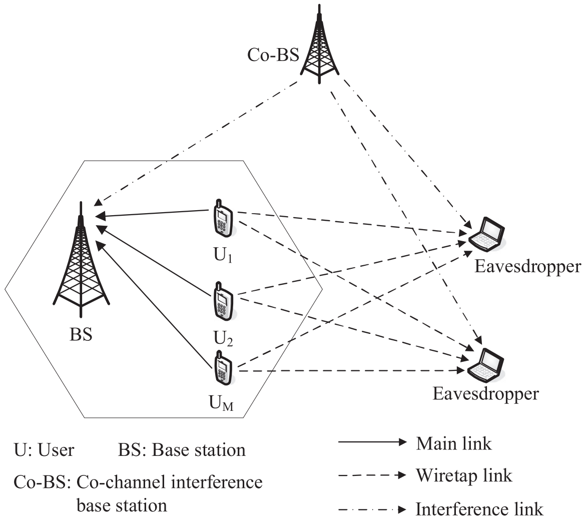


Fig. 1 A multi-user single-eavesdropper cellular network system.