Asymptotically Optimal Cooperative Jamming for Physical Layer Security

Jun Yang, Soheil Salari, Il-Min Kim, Dong In Kim, Seokki Kim, and Kwangae Lim

Abstract: **Design of effective cooperative jamming (CJ) algorithm is studied in this paper to maximize the achievable secrecy rate when the total transmit power of the source and multiple trusted terminals is constrained. Recently, the same problem was studied in [1] and an optimal algorithm was proposed involving a one-dimensional exhaustive searching. However, the computational complexity of such exhaustive searching could be very high, which may limit the practical use of the optimal algorithm. We propose an asymptotically optimal algorithm, involving only a fast line searching, which can guarantee to achieve the global optimality when the total transmit power goes to infinity. Numerical results demonstrate that the proposed asymptotically optimal algorithm essentially gives the same performance as the algorithm in [1, (44)] but with much lower computational complexity.**

Index Terms: **Cooperative jamming, physical layer security, secrecy rate.**

I. INTRODUCTION

THE fundamental idea of physical layer security is to exploit the physical characteristics of the wireless medium in order to communicate confidential messages. Secure communication from information-theoretic point of view was first studied by Wyner [2] for the classical wiretap channel and later extended for Gaussian channels in [3] and [4]. One of the effective methods for physical layer security is to transmit artificial jamming signal [5] to the eavesdropper using multiple antenna or cooperating terminals. This technique is often called artificial noise or cooperative jamming (CJ), which was studied in [5]–[11] based on information-theoretic approaches.

For the CJ networks, the use of achievable secrecy rate as the benchmark of security was considered in [12]–[15].[1] The works in [12]–[14] were the first few to investigate the design of CJ weight vectors under different types of power constraints. In [13], the authors assumed that each individual node (including the source node and each of the trusted terminals) had its own transmit power constraint, and derived an optimal CJ algorithm using a combination of convex optimization and a line searching. In [14], the authors assumed the source transmit power and the total transmit power of all trusted terminals were constrained separately, and proposed an optimal solution using an iterative approach. The scenario that the total transmit power of source and trusted terminals is constrained, which is referred to as the combined power constraint in this paper, was first discussed in [1] and [12]. In [12], a *suboptimal* CJ vector and the corresponding power allocation were obtained in closed forms by adding an extra constraint to completely null out the jamming signal at the destination. However, as shown in [15], the CJ vector proposed in [12] is not optimal in general. The optimal algorithm for the combined power constraint scenario was recently derived in [1, (44)] based on a one-dimensional *exhaustive* searching. However, the computational complexity of exhaustive searching can be very high, which may limit the application of the optimal algorithm in practice. Thus, computationally effective algorithms that give performance close to the optimal algorithm in [1, (44)] are desirable.

The contribution of our work is that we derive a *fast* asymptotically optimal algorithm for the combined power constraint that has much lower computational complexity than the optimal one in [1, (44)]. More specifically, we mathematically prove that our proposed asymptotically optimal algorithm guarantees to obtain the global maximum point when the transmit power goes to infinity, or the signal-to-noise ratio (SNR) goes to infinity. To study the performance of our proposed method in the finite SNR, we performed extensive simulation trials from various aspects. All of the simulation studies indicates that the proposed asymptotically optimal algorithm and the optimal one [1, (44)] essentially give the same performance over the entire SNR range, not necessarily high SNR values. Our extensive experiments not only show that the searching range of our proposed asymptotical algorithm is narrower than that of the exhaustive searching method derived in [1, (44)], but also confirm that, in this narrower range, the objective function is quasi-concave[2]. This means there is at most one critical point that must be the global maximum point. Thus, any of the existing effective line searching algorithms, such as bisection method, steepest decent method, and Newton's method [18], can be applied to compute the global maximum point, which requires much lower computational complexity than the exhaustive-searching method of [1].

It is well known that the reduction of the total power con-

Manuscript received December 17, 2014; approved for publication by Hong-Chuan Yang, Division II Editor, July 30, 2015.

This work was supported by the ICT R&D program of MSIP/IITP, Republic of Korea. [14-000-04-001, Development of 5G Mobile Communication Technologies for Hyper-connected smart services].

J. Yang is with the Department of Statistical Sciences, University of Toronto, Toronto, Canada, email: jun@utstat.toronto.edu.

S. Salari and I.-M. Kim are with the Department of Electrical and Computer Engineering, Queen's University, Kingston, Canada, emails: {soheil.salari, ilmin.kim}@queensu.ca.

D. I. Kim is with the School of Information and Communication Engineering, Sungkyunkwan University (SKKU), Suwon, Korea, email: dikim@skku.ac.kr.

S. Kim and K. Lim are with the Electronics and Telecommunications Research Institute (ETRI), Korea, emails: {kimsk0729, kjlim}@etri.re.kr.

Digital object identifier 10.1109/JCN.2016.000011

[1]Another possible security measure is the signal to interference plus noise ratio (SINR). Based on the SINR security measure, some effective CJ schemes have been proposed (for example, see [16] and [17] and the references therein). In this paper, however, we focus only on the achievable secrecy rate (not SINR) because it is the ultimate security measure.

[2]Note that this property does not hold for the exhaustive searching method derived in [1, (44)].