This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2016.2565579, IEEE Transactions on Wireless Communications

Cooperation via Spectrum Sharing for Physical Layer Security in Device-to-Device Communications Underlaying Cellular Networks

Rongqing Zhang, *Member, IEEE*, Xiang Cheng, *Senior Member, IEEE*, and Liuqing Yang, *Fellow, IEEE*

***Abstract*—In this paper, we investigate the cooperation issue via spectrum sharing when employing physical layer security concept into the Device-to-Device (D2D) communications underlaying cellular networks. First, we derive the optimal joint power control solutions of the cellular communication links and D2D pairs in terms of the secrecy capacity under a simple cooperation case and further propose a secrecy-based access control scheme with best D2D pair selection mechanism. Then, we consider a more general case that multiple D2D pairs can access the same resource block (RB) and one D2D pair is also permitted to access multiple RBs, and provide a novel cooperation mechanism in the investigated network. Furthermore, we formulate the provided cooperation mechanism among cellular communication links and D2D pairs as a coalitional game. Then, based on a newly defined Max-Coalition order in the constructed game, we further propose a merge-and-split based coalition formation algorithm for cellular communication links and D2D pairs to achieve efficient and effective cooperation, leading to improved system secrecy rate and social welfare. Simulation results indicate the efficiency of the proposed secrecy-based access control scheme and the proposed merge-and-split based coalition formation algorithm.**

I. Introduction

The increasing data rate demand for local area services and dramatically increased spectrum congestion have motivated research efforts for improving spectral efficiency in cellular networks. D2D communication [1], [2], which behaves as an underlay to cellular networks, can achieve cellular controlled short-range direct data transmission for local area services by reusing the cellular resources. In recent years, D2D communication employed in cellular networks has become a hot research topic in both academia and industry due to its advantages in improving resource utilization, enhancing cell capacity, increasing energy efficiency, and decreasing transmission delay among local users [3].

One of the most important issues in D2D communication is the interference problem caused by the resource sharing between the D2D communications and cellular communications. Thus, most literature on D2D communication focus on interference management [4]–[6] and resource allocation [7]–[9] to investigate how to enable the most potential benefits of D2D communications in cellular networks. In these works, interference caused by resource sharing is regarded as a harmful effect that needs to be eliminated or mitigated via various methods. However, most recently, some works [10]–[12] have proposed to utilize this interference to enhance the secrecy performance when introducing physical layer security issue into D2D communications underlaying cellular scenario.

The basic idea of physical layer security is to exploit the physical characteristics of wireless channels to provide secure communications. This line of work was pioneered by Wyner [13], who introduced the wiretap channel and the secrecy capacity, and showed that when the wiretap channel is a degraded version of the main channel, the two legitimate users can exchange secure messages at a non-zero rate without relying on a private key. In follow-up work [14], Wyner's result was generalized to a nondegraded discrete memoryless broadcast channel with common messages sent to both the receivers and confidential messages sent to only one of the receivers. In [15], the secrecy capacity of Gaussian wiretap channel was studied, and in [16], the secrecy capacity of quasi-static fading channel was investigated in terms of the outage probability. Note that the secrecy capacity is defined as the maximum achievable rate with perfect secrecy [15]. In recent works, cooperative relaying and cooperative jamming [17], [18] have been regarded as two promising means to effectively improve the secrecy capacity in a cooperative manner.

Back to the physical layer security issue in D2D communications underlaying cellular scenario, when we focus on the secrecy performance of cellular communication links, D2D pairs in the cellular network can act as friendly jammers [19]–[21] to provide efficient jamming service via spectrum sharing. In [10], the authors for the first time introduced D2D communications into the secrecy performance of the cellular communication as interference against eavesdropping and derived the optimal transmission power of the D2D pair in terms of secrecy outage probability. In [11], the authors

Manuscript received April 20, 2015; revised November 20, 2015 and February 26, 2016; accepted April 20, 2016. This work was supported by the National Natural Science Foundation of China under grant 61571020, the National 863 Project under grant SS2015AA011306, the National 973 Project under grant 2013CB336700, and the National Science Foundation under grant number CNS-1343189. This work was presented in part at the IEEE Global Communications Conference, San Diego, CA, USA, December 2015. The associate editor coordinating the review of this paper and approving it for publication was Dr. Andres Kwasinski.

Rongqing Zhang is with the State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics Engineering and Computer Science, Peking University, Beijing, China, and also with the Department of Electrical & Computer Engineering, Colorado State University, CO, USA (Email: rongqing.zhang@colostate.edu).

Xiang Cheng is with the State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics Engineering and Computer Science, Peking University, Beijing, China (Email: xiangcheng@pku.edu.cn).

Liuqing Yang is with the Department of Electrical & Computer Engineering, Colorado State University, CO, USA (Email: lqyang@engr.colostate.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2016.2565579, IEEE Transactions on Wireless Communications

utilized a weighted bipartite graph to formulate the one-to-one pairing and resource allocation problem between cellular users and D2D pairs with respect to the secrecy concern of cellular users. In [12], the authors derived the secrecy outage probability for the D2D and cellular system in the presence of a multi-antenna eavesdropper. Although physical layer security issue in D2D communications underlaying cellular networks has been investigated in some existing works, the investigated interference scenario in all these related works (as in [10]–[12]) is only a simple one, in which on one resource block (RB), at most one D2D pair can access it to help improve the secrecy performance of the corresponding cellular communication link and one D2D pair cannot access multiple RBs.

In this paper, we investigate the physical layer security issue in D2D communications underlaying cellular networks from a cooperation perspective. We formulate this cooperation as a coalition formation game which can achieve efficient and effective cooperation among cellular communication links and D2D pairs to both sides' benefits. Besides, different from previous related works, we consider a more general interference scenario that multiple D2D pairs can access the same RB and one D2D pair is also permitted to access multiple RBs. The main contributions of this paper can be summarized as follows.

1. We first derive the optimal power control solutions for the cellular communication links and D2D pairs to maximize the secrecy capacity performance of the investigated cellular communication under a simple cooperation case and further propose a secrecy-based access control scheme with best D2D pair selection mechanism. Note that this derivation is under the same interference channel model assumption as that in [10]. Although [10] also obtained the optimal transmission power of D2D communications, our work differs with [10] from at least two aspects: 1) The power control solution we obtain is a joint consideration of the transmission power of both cellular communication links and D2D pairs in different channel conditions, while [10] only considered the transmission power of D2D pairs; 2) the optimization objective is the secrecy capacity in our work, while [10] focused on the secrecy outage probability.
2. We provide a novel cooperation mechanism to investigate the physical layer security problem in the D2D communications underlaying cellular network. Cooperation via spectrum sharing among cellular communication links and D2D pairs can yield mutual benefits in the presence of an eavesdropper. When information secrecy is a concern, cellular communication links may benefit from simultaneous transmissions of D2D pairs via spectrum sharing to increase the secrecy capacity, while D2D pairs can also benefit from spectrum sharing permission to transmit their individual data. Also different from the existing related works, in our proposed cooperation mechanism, D2D pairs have its own utilities to pursue and they are positive partners rather than "selected" or "matched" candidates as in [10], [11]. This cooperation mechanism is beneficial for improving the social welfare defined as the sum of the secrecy capacity of cellular communication links and the transmission rate of D2D pairs.
3. Considering a more general case that multiple D2D pairs can access the same RB and one D2D pair is also permitted to access multiple RBs, we formulate the win-win cooperation mechanism among cellular communication links and D2D pairs as a coalitional game with transferable utility (TU) [33]. Different from the conventional coalitional game, the constructed game is further divided into several sub-games, each addressing the cooperation process of one specific RB. Each player can only participate in one sub-game at a time but can make a decision to change its identify and join in another sub-game next round. These sub-games can process the cooperation process simultaneously and in a distributed manner.
4. Based on a newly defined Max-Coalition order in the constructed game, we further propose a merge-and-split based coalition formation algorithm for cellular communication links and D2D pairs to achieve efficient and effective cooperation, leading to both improved system secrecy rate and social welfare.

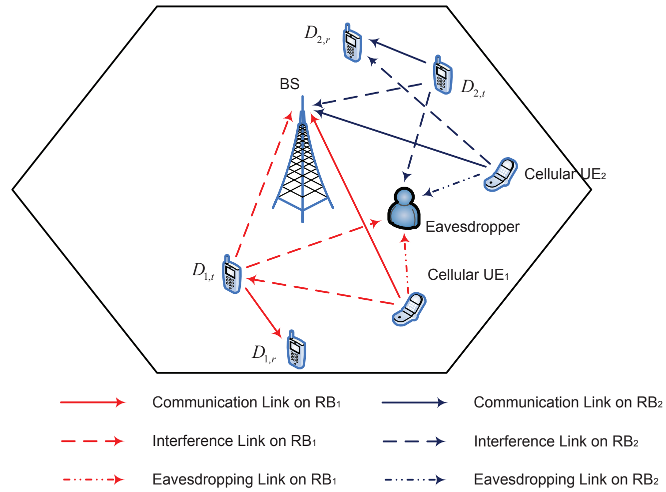

Fig. 1. System model for D2D communication underlaying uplink cellular network in the presence of an eavesdropper.

The remainder of this paper is organized as follows. In Section II, system model is described and the cooperation problem is formulated. In Section III, we derive the optimal power control solutions of the cellular communication links and D2D pairs to maximize the secrecy capacity performance and further propose a secrecy-based access control scheme. In Section IV, we first provide a novel cooperation mechanism and formulate it as a coalitional game. Then, we propose a merge-and-split based coalition formation algorithm. Simulation results and analysis are provided in Section V and the conclusions are given in Section VI.

II. System Model and Problem Formulation

A. System Description

As illustrated in Fig. 1, we consider an uplink transmission scenario in a D2D communications underlaying cellular