Computer Communications 63 (2015) 1–10

Contents lists available at ScienceDirect

Computer Communications

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

Secure inter-cluster communications with cooperative jamming against social outcasts

Li Wang [*], Chunyan Cao, Huaqing Wu

Beijing Key Laboratory of Work Safety Intelligent Monitoring, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, PR China

ARTICLE INFO

Article history:
Received 8 October 2014
Received in revised form 16 December 2014
Accepted 17 February 2015
Available online 25 February 2015

Keywords:
D2D communications
Cooperative cluster
Jamming
Social trust
Secrecy rate

ABSTRACT

The concept of device-to-device (D2D) communications has recently attracted broad research and development interests owing to its simplicity and promise to improve spectrum and energy efficiency within existing cellular infrastructure. Because of their less sophisticated control plane, D2D user equipments (DUEs) themselves are not powerful enough against security breaches. This work investigates ways for D2D users to form clusters to shun social outcasts. We form reliable cooperative clusters by considering physical positions of candidate DUEs and by exploiting their social relationship to improve secrecy rate. Our cluster-assisted relay and jammer selection optimization scheme has the dual objective of maximizing the DUE secrecy rate under power constraint and satisfying the requisite signal-to-interference-plus-noise ratio (SINR) need of co-channel cellular user equipments (CUEs). To solve the non-convex optimization problem, we propose a generalized fractional programming (GFP) method by leveraging the Dinkelbach-type algorithm. We also study the impact of social trust and channel estimation error of these mobile nodes to demonstrate the robustness and reliability of the proposed approach. Numerical results show that the proposed scheme can achieve good performance through the underlying D2D cooperation.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

The continuous rapid growth of mobile wireless services and data traffics is severely straining the existing cellular infrastructure and particularly the base-stations. For this reason, there recently has been a heightened research interest and development in device-to-device (D2D) communications designed to offload base-station traffics by directly tunneling links between mobile nodes in proximity. With or without spectral reuse between D2D and cellular users, D2D can provide higher network throughput and spectral efficiency, or extend network coverage through D2D relaying [1].

D2D usually serves as an underlay to cellular network, controlled by the cellular radio network controller (RNC). D2D communication can reuse the same spectral resource with cellular links without severely impacting the cellular user equipment (CUEs). Spectrum reuse (sharing) is typically between the direct D2D link and the cellular link. Hence, many researchers have focused on D2D-related resource allocation, interference management, and mode selection [2–4], and also discussed the distance related network topology for D2D in underlay cellular networks [5]. However, we must point out that DUEs have less sophisticated control and are vulnerable to eavesdropping or information leakage to social outcasts. For example, unlike in a typical cellular network control mode, D2D can also work in a D2D cluster-assisted mode, in which a cluster head is responsible for managing and maintaining intra-cluster control signaling including synchronization, access control, and resource allocation as well as is in charge of data transmission. Thus, individual DUE with weak security protection should seek help from the cluster head, without having to switch back to its cellular mode [6].

D2D users, by forming collaborative clusters, can also achieve other advantages such as better coverage, enhanced reliability, improvement of spectrum efficiency and network capacity. On the other hand, formation of collaborative clusters may also bring certain security risks when certain cluster member nodes tend to mis-behave and are known social outcasts. Such internal risks can be troublesome and more difficult to protect against using traditional security features. Hence, we investigate physical-layer-based transmission approaches [7] to enhance cluster-mode network secrecy against social outcasts.

To the best of our knowledge, there has been little research on improving the secrecy performance for DUEs. Few works consider the physical layer security in cluster-assisted configurations against social outcasts, though some studies can be found on

[*] Corresponding author.
E-mail address: liwang@bupt.edu.cn (L. Wang).

http://dx.doi.org/10.1016/j.comcom.2015.02.012
0140-3664/© 2015 Elsevier B.V. All rights reserved.

related problems such as in basic D2D links, as well as in traditional wireless relay networks. The mechanism presented in [8] investigated the improvement of secrecy rate for cellular users by taking DUEs as friendly jammers. Note that, secrecy rate is defined with the difference of the channel capacities from Alice (Source node) to Bob (Destination node) and from Alice to Eve (Eavesdropper) [7,9,10]. In traditional cooperative relay networks, cooperative beamforming and cooperative jamming [11,12] can improve achievable secrecy rate. However, full channel state information (CSI) and synchronization are assumed for cooperative beamforming [11], which is harder to implement. Although cooperative jamming has been widely used to combat interception, existing techniques often require many unrealistic assumptions. Further, cluster-based relay cooperation has seldom addressed internal risks from compromised social outcasts. Thus, our work here is a timely endeavor.

There already exist related works invoking social contact information in wireless networking [14]. For example, the works in [6,15] used social relationship among users to help form cooperative clusters. Properties such as social tie, social trust, social reciprocity, and social outcast are incorporated in assisting D2D communications [16]. Exploiting social interaction information of different member nodes has improved the accuracy of resource allocation problem [13]. Cooperative communications is an efficient D2D paradigm where DUEs can help group members as relays. Ref. [17] had discussed the cooperative D2D group formation based on physical layer and social layer information simultaneously, leveraging the social trust and social reciprocity. For basic D2D communication setup, authors of [6,15] also take social interactions into account to form cooperative clusters or groups for wireless performance improvement.

Thus, our works in this paper study the problem of resource allocation based on the social trust based clustering. Cross two adjacent D2D clusters, we consider a scenario where source and destination nodes are far apart enough to necessitate the help of intermediate relay clusters. There exist known inter-cluster outcasts and intra-cluster outcasts. We stress that these (social) outcast nodes are not like the traditional passive eavesdroppers. Outcast nodes are nodes from which the cluster heads would like to hide certain sensitive transmissions including inter-cluster transmissions. They are eligible to receive and transmit certain less sensitive messages. Hence, they are not fully passive such that their channels may be reciprocally estimated via traditional or blind channel estimations [18]. Since practical considerations, our work shall also consider the effect of channel estimation error.

We mainly focus on means to make full use of D2D cluster's ability to help one another against outcasts. In particular, to hamper reception by social outcasts, we develop a cluster head-assisted optimized relay and jammer selection scheme with power allocation to maximize secrecy rate of DUEs under a sum transmit power constraint while guaranteeing the requisite SINR level to CUEs. Furthermore, we select an optimized relay to help transmit the message and a few dependable jammers from a socially trusted group to cooperate. As we shall show, the secrecy rate maximization problem is non-convex. As a result, we present a generalized fractional programming (GFP) solution based on the Dinkelbach-type algorithm to successfully solve the secrecy rate maximization problem [19].

We organize this paper as follows. Section 2 introduces the problem of cluster-assisted secure transmission in device-to-device communications. In Section 3, we present an optimal relay and jammer selection scheme from the candidate DUEs. Section 4 describes a generalized fractional programming based solution to optimize the formulated problem. Numerical results in Section 5 demonstrate the performance improvement of our proposed scheme before conclusions in Section 6.

2. System model and problem formulation

2.1. System model of clustered D2D communications

We consider D2D communications underlay in cellular networks as illustrated by Fig. 1, where M D2D pairs or clusters coexist with N CUEs served by the BS. From now on, we take D2D clusters for example, and call the members in it as DUEs. In particular, downlink resource sharing in D2D communications is considered here, any interference to DUEs caused by spectrum sharing from BS can be more easily mitigated by BS actions such as beamforming. Since BS has many antennas, it not only can target the CUEs better by focusing its energy, but can also estimate DUE locations by placing spatial nulls in those directions. We also assume a fully loaded cellular network scenario, that is, N active CUEs occupy the N orthogonal channels in the cell and there is no vacant spectral band.

In this paper, we assume that D2D clusters can be set up only when the minimum SINR requirement is guaranteed and their interference to the CUEs is below a threshold. In this case, we call it an admissible cluster and the CUE to be shared resource as reuse partners. Note that, a D2D cluster with several UEs shares at most one existing CUE's resource.

Although some works have investigated the secrecy issue of cellular users [8], seldom did they pay serious attention to the secrecy of D2D pairs or clusters. In practice, the secrecy requirements of D2D communications are gradually becoming more vital, given their intended role to enhance the overall system performance. For this reason, our work here focuses on how to maximize the secrecy rate of D2D users from the information theoretic perspective while constraining the inference to cellular users from D2D users.

In our problem formulation, we consider two adjacent D2D clusters of multiple DUEs, consisting of a source, a destination, and multiple intermediate nodes in between as relays. Of course, some of the nodes are compromised outcast. Each node is half-duplex with a single omni-directional antenna. We assume the channels from BS to CUEs follow a large-scale path loss model, and can be known in advance. Let channels between any pair of mobile nodes be independent, identically distributed (i.i.d.) and in flat fading, since DUEs tend to be of low mobility in a typical scenario. This is because in high mobility, it is difficult to maintain a D2D link. Thus, we consider the DUE channels follow slow fading and can be effectively estimated.

Secure transmission between a transmit cluster and its receive cluster is investigated by considering serval outcasts as shown in Fig. 1, including intra-cluster and inter-cluster outcasts which are not fully passive. There may be direct links between two cluster heads as well as from the transmit head to outcasts. Decode-and-forward (DF) relays are used. There are at least as many candidate jammers as the number of outcasts. Note that, here we only consider the minimum SINR of CUEs as a constraint to simplify the problem, while focusing on the more vulnerable DUEs secrecy rates.

Most existing works assumed perfect channel state information (CSI) [11,20]. However, for some outcasts their CSIs may be hard to obtain or may be inaccurate. In our approach, we find the reciprocal CSI of outcasts through (blind) channel estimation as they are not fully passive [18]. During clustering, we first select nodes as cluster heads based on factors such as distance, residual energy, trust-worthiness. Then cluster heads collect CSI of all nodes within its range before selecting nodes to form a jammer cluster. Consequently, the CSI of the inter-cluster outcast is obtained. For intra-cluster outcasts detection, we may apply the method from [21] where the receive cluster head periodically detects whether an active but compromised cluster member is

Download English Version:

https://daneshyari.com/en/article/447714

Download Persian Version:

https://daneshyari.com/article/447714

Daneshyari.com