J. Parallel Distrib. Comput. ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

J. Parallel Distrib. Comput.

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

Socially-conforming cooperative computation in cloud networks

Tao Li [a,*], Brij Bhooshan Gupta [b], Roberto Metere [c]

[a] School of Information Science and Electrical Engineering, Ludong University, Yantai, China
[b] Department of Computer Engineering, National Institute of Technology Kurukshetra, India
[c] School of Computing Science, Newcastle University, UK

HIGHLIGHTS

- Boost cooperation among rational parties by applying the notion of social conformity.
- Simulate social conformity in cloud network to show cooperation is possible and fairness can be achieved.
- Propose a general model to bridge mutual cooperation in social conformity and fairness in secure two-party computation.

ARTICLE INFO

Article history:
Received 29 December 2016
Received in revised form 2 June 2017
Accepted 9 June 2017
Available online xxxx

Keywords:
Game theory
Cloud cooperation
Fairness
Social conformity

ABSTRACT

In the context of two-party computation, such as file exchange or contract signing, the security property of fairness is of great importance. After the impossibility result of Cleve for achieving complete fairness in general, recent research proposes to circumvent such impossibility by assuming that parties behave as rational players of a game. However, such works involve rational parties as independent individuals without considering the impact of the environment. In our work, we apply the notion of social conformity to show that under certain assumptions rational parties belonging to a cloud will choose to cooperate. Then, we simulate a real setting to show that party in fact cooperates and achieves fairness. Finally we discuss a general model to describe the connection between mutual cooperation in social conformity and fairness in secure two-party computation.

1. Introduction

A cloud is a computer network whose hosts (servers) constitute the cloud infrastructure, cooperate to compute specific tasks and eventually provide services to the clients [30,31]. Many clouds are available through the Internet and offer services of data storage and computation delegation [27,36,39,50,54]. Some companies subscribe to third party clouds becoming their clients to save costs [28,29,32], especially when the subscription is cheaper than maintaining an internal system for performing the same operations.

Two servers in the cloud may exchange services and run two-party computation protocols to do so. One of them can abort after receiving the service, in which case the other receives nothing. Clearly, the one who receives the service gains advantage. Therefore, a security requirement in services exchanging is fairness, i.e. both servers either receive the service after the protocol or receive nothing. However, Cleve has shown that fairness is generally impossible in two-party computation [8]. To circumvent this impossibility result, additional assumptions are required; for example, when an trusted third party is available. Recently, several researchers showed how to achieve fairness when parties can be assumed to behave rationally, applying a combination of game theory and cryptography [1,4,13,18,35]. Some of such works rely on physical channels like paper envelopes and ballot boxes [19,24], some others sacrifice round efficiency by setting a high number of rounds before which the parties cannot learn the output, increasing the round complexity [4,12,13,18,35]. We show that in a cloud network, protocols do not require the above limitations, which are clearly impractical for real software implementation.

In game theory, players of a game are called rational when they decide their strategy in order to maximise their own payoffs at the end of the game. The payoffs are the result of *utility* functions of the strategies adopted by all the players. Therefore under the assumption that the two participants of a two-party protocol are rational, the protocol can be studied as a game played by the two parties, whose strategies describe their possible behaviours, and the payoffs are what the parties earn at the end of the game. Several studies showed that under such assumption and particular utilities, the parties would cooperate and achieve fairness [4,12,13,18].

* Corresponding author.
E-mail addresses: litao_ldu@163.com (T. Li), gupta.brij@gmail.com (B.B. Gupta), r.metere2@ncl.ac.uk (R. Metere).

http://dx.doi.org/10.1016/j.jpdc.2017.06.006
0743-7315/

Hence to show that a two-party protocol achieves fairness, one can show that the assumption of having rational participants is realistic in the setting of study, and the utilities capture both the strategies and the outcomes of the setting. A two-party protocol allowing parties to prematurely stop can be described from a game theoretical point of view with the prisoner's dilemma [44]. Here each prisoner can choose either to be silent (cooperate) or betray the other (defect). If both stay silent, they will serve 1 year in jail; if both betray the other, they will serve 2 years in jail; and if only one betrays the other, then she will be freed but the betrayed one will serve 3 years in jail. Game theory shows that, if they are rational, distrustful and cannot communicate, both of them will choose to betray the other, even if intuitively they should choose to be silent and both get less time to serve in jail.

In this paper, we focus on two-party protocols engaged by servers belonging to the same cloud. Here, we show that the servers may cooperate conforming their strategies to the majority of the other participants, which means that we cannot use the original prisoner's dilemma game. This concept has been borrowed from psychology, where this behaviour is known as social conformity. Social conformity is a kind of social influence that is new neither in computer science nor in game theory [14–17,26,33,47,53]; in fact, social conformity is strictly relating to reinforcement learning, where machines may modify their behaviour according to the environment to maximise some *cumulative* advantage. For example, in the prisoner's dilemma game, players should choose to betray the other since it is the best strategy for them. However, many experiments showed that parties belonging to the same group prefer to cooperate due to social conformity [6,38,42].

In the setting of our study, we have servers that run two-party computation protocols and that belong to one cloud network; we assume that they are rational but record history. With this variation, they choose their strategies according to social conformity instead of self-interest only. Note that even if the servers are configured to cooperate, they still have incentives to deviate from doing that. Therefore, we must design some mechanism to prevent them from deviating. The setting of our experiment is the Zachary network [55], since we describe the cloud network as a complex network. We design our experiment to show that rational parties have incentives to cooperate with each other in the cloud. Then, we implement the above result (mutual cooperation is possible) to rational two-party computation. Finally, we propose a new model between prisoner's dilemma game and rational two-party computation. The basic idea is showing that once two rational parties cooperate, then fairness can be achieved. Note that, we only consider rational servers in this paper.

1.1. Related works

We define the utility functions similarly to the prisoner's dilemma game in the works of Dawes [9] and Osborne [44]. Here, rational parties have no incentives to cooperate with others.

Other works try to encourage cooperation by applying usual methods from game theory, such as indefinitely iterated prisoner's dilemma games. Axelrod [6] explored whether mutual cooperation is possible in the iterated prisoner's dilemma game. He proved that altruistic strategies are more likely to be adopted in iterated prisoner's dilemma game. Other strategies assume to start with cooperation in iterated prisoner's dilemma game, like the tit-for-tat strategy [38,42]; therefore, they relate to our contribution only from the point of view of showing feasibility. Extending the work of Axelrod, other researchers showed methods to get further properties [22,37] on a mutual cooperation setting. In this paper, we draw on the experience of these achievements and apply them into new practical settings.

(Social) conformity is a social influence introduced in psychology where agents try to achieve the approval of others by conforming to the majority of them. Social conformity is based on the principle of reinforcement learning, as shown by Klucharev et al. [21] by using functional magnetic resonance imaging. They also showed that conformity can be evoked through learning mechanism. In [2,46], the authors combine game theory with modern psychological and neuro-scientific methods. They conclude that the players of the prisoner's dilemma game would cooperate about half of the times when prisoner's dilemma game is iterated. Such mutual cooperation in the prisoner's dilemma game can be Nash equilibrium when given proper parameters [23]. In the same paper it is shown that parties try to train others in the same group when they repeated play one game.

Recently, game theory has been applied to secret sharing schemes and secure multiparty computation [4,18,20]. Ong et al. [43] presented a secret sharing scheme with a honest minority and a rational majority. Lysyanskaya and Triandopoulos [34] discussed rational secure multiparty computation in the presence of rational parties and malicious adversaries in the universally composable (UC) model [7]. Other works show how to achieve Nash equilibrium (and other stronger equilibriums) by using physical communications such as paper envelopes and ballot boxes [19,24,25]. Garay et al. [10] discussed the incentives in rational cryptographic protocols and model them as two-party games between a protocol designer and an external attacker.

We base the last part of our contribution on the work by Groce and Katz [13], in which they describe a rational two-party protocol which achieves fairness with high probability. However, their protocol requires a high round complexity and it is infeasible in real settings. We show that in the cloud, when the party behaves in accordance to social conformity, we can drastically decrease the round complexity.

1.2. Organisation

This paper is organised as follows. In Section 2, we present some preliminaries about game theoretical approaches to two-party computation and cloud networks. In Section 3, we present the model of social conformity and simulate it. In Section 4, we analyse the security properties of two-party computation protocols when the parties act in social conformity. At the end of the section, we propose a general model to bridge mutual cooperation in iterated prisoner's dilemma game and fairness in rational two-party computation. Our model considers the impact of the environment on parties' strategies. In Section 5, we conclude our discussion and suggest some directions of future works.

2. Preliminaries

Many rational two-party computation protocols are based on rational secret sharing scheme [4,18,20]. So we first give basic notions commonly used in game theory and two-party computation protocols that are useful in the description of our work.

In secure two-party computation, we have two entities P_1 and P_2 who hold a value each, x and y, and want to compute a function $f = (f_1(x, y), f_2(x, y))$, while keeping the inputs private. In the settings in which assuming that P_1 and P_2 behave as players of a game, i.e. rational, the protocol can be described as a game in game theory.

Please cite this article in press as: T. Li, et al., Socially-conforming cooperative computation in cloud networks, J. Parallel Distrib. Comput. (2017), http://dx.doi.org/10.1016/j.jpdc.2017.06.006.