Editorial

Rajgopal Kannan and Costas Busch

Department of Computer Science,
Louisiana State University,
Baton Rouge, LA 70803, USA
Fax: +1 225 578 1465
E-mail: rkannan@csc.lsu.edu
E-mail: busch@csc.lsu.edu

Abstract: This special issue is dedicated to algorithmic game theory, which is an emergent research field in the broad area of computer algorithms. The papers that appear in this issue represent current research directions in algorithmic game theory. The papers give particular emphasis on communication networks and fall into two categories: network security games and packet forwarding games.

Keywords: algorithmic game theory; packet forwarding games; security games.

Biographical notes: Rajgopal Kannan graduated with a BTech in Computer Science and Engineering from the Indian Institute of Technology, Bombay in 1991 and then obtained his PhD from the University of Denver in 1996. Currently, he is an Associate Professor in Computer Science Department at Louisiana State University. His areas of interest are in wireless sensor networks, algorithms, game-theoretic network control, power management, security and interconnection networks.

Costas Busch graduated with an BSc in 1992 and an MSc in 1995 from the Department of Computer Science, University of Crete, Greece. He received his PhD in Computer Science from Brown University in 2000. Currently, he is an Assistant Professor in Computer Science Department of Louisiana State University. His areas of interest are distributed computing algorithms, communication algorithms for wireless, sensor and optical networks and algorithmic game theory.

1 Introduction

Game-theory offers a formal mechanism for studying complex interactions between multiple rational participants. The emergence of the internet as a dominant communication platform has brought to the surface many interesting game theoretic problems that arise from the interplay of the entities that manage and use the internet. Algorithm and network designers, in general are interested in analysing outcomes of these interactions. This has resulted in the formation of the new research area of algorithmic game theory which brings together two important scientific fields: economics and computer science. In addition, algorithmic game theory covers problems that arise outside the internet. In this new research area, games are studied from the perspective of

algorithmic issues which, for example, include the design of algorithms that compute equilibria, measurement of equilibria quality and generally the design of new games that can be analysed with algorithmic techniques. Motivated by the strong current interest in the area of game-theoretic modelling of network interactions and its algorithmic analysis, the purpose of this special issue is to give a snapshot of the latest work from the algorithmic and game-theoretic communities in this exciting area of research.

2 Overview of the issue

The papers that appear in his special issue can be divided into two categories:

1 network security games

2 packet forwarding games.

The network security research topic is particularly interesting because of the vulnerabilities of modern network infrastructures. In the journal, there are two papers on network security games, the first paper concerning a virus attacker–defender game and the second examines a wireless network jamming game. In addition, packet forwarding is a very important topic because it is a fundamental task in any network that needs to be performed particularly efficiently in heterogenous wireless networks. In this issue, there are two papers on packet forwarding games, the first paper examines strategies that minimise the amount of payment to the forwarding nodes, while the second paper examines efficient strategies that take into account the non-perfect conditions of the network. Below is an overview of the papers that appear in the journal.

2.1 Network security games

A graph theoretic network security game: This paper considers viral infection problems, where there is a network vulnerable to attacks from viruses and a defender software protecting the network. A virus (attacker) chooses to infect a node in the network with some probability. The network can be protected by a security software (protector) which protects a limited part of the network. The attacker attempts to avoid being catched by the protector, while the protector wants to catch as many attackers as possible. This attacker–protector scenario is modeled as a non-cooperative multi-player game in a graph. The main question examined is the existence and quality of Nash equilibria in such games. Mixed Nash equilibria can be found in polynomial time for interesting classes of networks including regular graphs, and graphs with perfect matchings and trees. The quality of the Nash equilibria is measured with respect to the price of anarchy which expresses the ratio of the social cost in the worst Nash equilibrium to the social cost in optimal uncoordinated solution. It is shown that the price of anarchy can be bounded with respect to the size of the graph. The problem of determining the existence of pure Nash equilibria is NP-complete.

Jamming games in fast-fading wireless channels: The wide employment of wireless networks and their vulnerability to attacks from interference and other sources of jamming, has emerged the importance for the design of appropriate anti-jamming strategies to defend against wireless network attacks. Further, anti-jamming strategies are important due to the increased demand for wireless security. The paper formulates the

interaction between wireless channel jammers and wireless transceivers as non-zero sum games on the physical layer of the network, where the interactions take place as interference in the physical transmission channel (the jammer is taken to be Gaussian). The payoff of the players is expressed with respect to the outage probability of the transmission channel, where the goal of a legitimate transceiver pair is to reduce the outage probability, while the goal of the outside jammer is to increase the outage probability. The paper establishes the existence of pure Nash equilibria in the setting of fast fading channels and in peak and average power constraints. They examine the maxmin and minmax scenarios where either the jammer or the transceiver pair makes the first move, respectively.

2.2 Packet forwarding games

Routing game in hybrid wireless mesh networks with selfish mesh clients: This paper studies hybrid wireless mesh networks (WMNs) which consist of mesh routers and mesh clients, where the clients connect to the network through the mesh routers or through other clients. The clients may not follow a prescribed protocol, since the may act selfishly promoting only their own interests. A method to force the nodes to follow prescribed protocols is through algorithmic mechanism design that incorporate incentive policies that force the nodes to be truthful. A typical framework of truthful incentive policies are VCG mechanisms. The paper shows that classical VCG-based routing protocols come at a high price since the payments of the nodes are very expensive. The paper proposes an alternative VCG-based method which reduces the total payment, but may not be a truthful mechanism. The authors also propose a novel routing protocol which could achieve Nash equilibrium with low payments.

Optimal forwarding for wireless ad hoc networks with game theory: This paper studies cooperative mechanisms and the authors derive optimal criteria in packet forwarding. The paper considers realistic scenarios such as noise, non-simultaneously (where players are not synchronised when taking actions), non-perfect measurement (where a player's actions may be observed with errors by other players), and different packet forwarding strategies by the nodes where different players in the network may not follow the same forwarding strategy. The paper explores optimal strategies considering the above scenarios.