Chapter 12

Applications of Game Theory for Physical Layer Security

Kaizhi Huang
National Digital Switching System Engineering and Technological Research Center, China

Mingliang Li
National Digital Switching System Engineering and Technological Research Center, China

Zhou Zhong
National Digital Switching System Engineering and Technological Research Center, China

Hua Zhao
National Digital Switching System Engineering and Technological Research Center, China

ABSTRACT

This chapter provides a comprehensive review of the domain of game theory based physical layer security in wireless communications. By exploiting the wireless channel characteristic and secure cooperation of nodes, physical layer security is to enable the exchange of confidential messages over a wireless medium in the presence of unauthorized eavesdroppers, without relying on higher-layer encryption. However, the selfness of nodes seriously affects the secure cooperation; game theory can model the influence of the selfness on physical layer security. This chapter firstly describes the physical layer security issues in the wireless networks and the role of game theory in the research on physical layer security. And then the typical applications of game theory in physical layer security are subsequently covered, including zero-sum game, Stackelberg game, auction theory, coalition game. Finally, the chapter concludes with observations on potential research directions in this area.

INTRODUCTION

The broadcast and superposition nature are the two fundamental characteristics of the wireless medium, which extend the communication range and improve the performance of wireless system respectively, but make the wireless signal easier to be eavesdropped and jammed (Kashyap, Basar, & Srikant, 2004). Therefore the eavesdropping and jamming become the hidden dangers of the wireless communication. At present the high-layer enciphering techniques is also the main methods to solve these problems (Massey, 1988). However, in dynamic wireless networks this raises some issues such as key distribution for symmetric cryptosystems, and high computational complexity of asymmetric cryptosystems (Schneier, 1998).

DOI: 10.4018/978-1-4666-8642-7.ch012
In the wireless communication, different communication links have different channel characteristics, which is different from the wire communications. Inspired by it, in 1975, Wyner built the wiretap channel model considering the channel imperfections and theoretically proved the feasibility of physical layer security (Wyner, 1975). At present, the physical-layer security methods can be divided into internal security methods and external security methods. Internal security methods guarantee secure communication by exploiting the difference of the wireless channel and background noise observed by the different communication nodes (Leung-Yan-Cheong & Hellman, 1978). External security methods guarantee secure communication by using target-specified artificial jamming to selectively jam the eavesdropper (Negi & Goel, 2005).

But the traditional physical-layer security methods also have some limitations, for example, in a multi-node wireless network, there is usually one optimization target with the single policymaker responsible for the communication strategy design of all the nodes. However, the nodes operate under its own steam and the communication state of the nodes also dynamically change in the real network. According to the other nodes’ communication strategies, each node can choose its strategy for maximizing its interest. So every node has the different but related optimization target. Obviously, the traditional physical layer security methods can not roundly model the real communication scenario and measure the dynamic secrecy performance of the wireless network.

Game theory (Osborne & Rubinstein, 1994) is a formal framework with a set of mathematical tools to study the complex interactions among interdependent rational players, which can model the confrontation behavior and selfishness of the nodes in the scenarios with secrecy requirement. Further, the secrecy communication strategy of every node can be selected based on the prediction of the game result. This chapter uses game theory to analyze the dynamic secrecy performance of the wireless network.

**Background**

As shown in Figure 1, there are N legitimate nodes (legitimate transmitter, friendly relay, and friendly jammer, legitimate receivers), and L malicious nodes (untrusted relay, malicious jammer and eavesdropper) in the network. We denote jammer and relay by helper. A non-cooperative game in strategic (or normal) form can be denoted by \( G = (N, S, U) \), where \( \lambda(0) \) denotes a finite set of players including the set \( A \) of legitimate nodes, and the set \( E \) of malicious nodes. \( S = (S^A, S^E) \) denotes the set of available strategies for all the players, where \( S^A \) is the set of strategies for legitimate nodes including sending useful signal, forwarding signal, sending friendly jamming, sending artificial noise and so on, \( S^E \) is the set of strategies for malicious nodes including eavesdropping and jamming. \( U = \{ u_i(s) \} \) is the set of utility/payoff function for all the players. For any player \( i \), \( s = (s_i, s_{-i}) \) is referred to a strategy profile, where \( s_i \) is the strategy of player \( i \), \( s_{-i} \) denotes the vector of strategies of all players except player \( i \).

Although the utility function for the different players varies with the secrecy communication scenario, in general, the sum of payoff for legitimate nodes denoted by \( \sum_{i \in A} u_i \) reflects their tendency to improve the secrecy performance (e.g. secrecy rate outage probability, secrecy freedom degree), the sum \( \sum_{i \in E} u_i \) of payoff for malicious nodes reflects their tendency to break the secrecy performance.

According to \( s^* \), the player \( i \) chooses the strategy maximizing its payoff, the optimal strategy for player \( i \) is \( s^*_i = \max_{s_i \in S^A} u_i (s_i, s_{-i}), i \in A \), \( s^*_i = \max_{s_i \in S^E} u_i (s_i, s_{-i}), i \in E \). The strategy profile \( s^* \) is Nash equilib-