Chapter XIII
A Study of Malicious Agents in Open Multi-Agent Systems: The Economic Perspective and Simulation

Pinata Winoto
Hong Kong Baptist University, Hong Kong

Tiffany Y. Tang
Hong Kong Polytechnic University, Hong Kong

ABSTRACT

This chapter focuses on the issue of malicious agents in open multi-agent systems (MAS) with discussions in relation to existing crime study, that is, supply-demand analysis and deterrence theory. Our work highlights the importance of mechanisms to make intervention to the MAS, in an attempt to deter malicious agents from maximizing their utilities through illegal actions. Indeed, in market-oriented MAS, human interventions sometimes would be necessary, given the condition that these interventions would not destroy the ecological stability of the agent society. However, an automatic intervention mechanism seems to be the winning card in the end, among them, the reputation mechanism, agent coalition formation, and so forth. It is our hope that our work can shed light on these issues as well as their deployment in MAS.

INTRODUCTION

In the context of human criminal studies, crimes can broadly be grouped as economically driven crimes and non-economically driven crimes. Economically driven crimes (or *economic crime*, for short) are primarily driven by financial gains and presumably follow the utilitarian concept; that is, it is controlled by manipulating its pains (punishments) and gains (rewards). Generally, if there are victims left by a crime, it is called a predatory crime. In human society, crime is a

complex phenomenon. In the agent society, crime is less complex due to a specific agent's intention/purpose, for instance, violating committed contract for bidding agent, sending misleading information for advertising agents, entering restricted area for search agents, and so forth.

The context of this chapter is on the study of malicious agent society, which is characterized by economic and predatory crimes. However, the model used is based on the economic model of 'human' crime, which is still a controversial issue. For example, it is commonly assumed in the model that all criminals follow rational choice behavior, while in the real world many 'real' criminals are addicted to alcohol/drugs. Yet, rational choice model may fit better in agent society, since all agents are preprogrammed to make rational decisions to maximize rewards. Therefore, one of the potential applications of this study is to seek optimal multi-agent system (MAS) policy, especially when heterogeneous agents may behave maliciously.

Controlling malicious agents in MAS is not new. Through punishment and probability of arrest/conviction (Winoto, 2003a, b), we make an effective way of governing these malicious agents. Specifically, agents with common goals are deployed in a malevolent game: compete with other agents by means of malevolent actions. In this chapter, we will discuss several general models that may be used in open MAS. Open MAS are characterized by heterogeneous agents who may use various strategies (including malevolent behaviors), enter and exit the system freely, and compete to maximize individual utility. An example of open MAS is an open electronic marketplace, where agents (including human agents) make transactions for goods or services using specific negotiation protocols.

Motivational Examples

The following examples illustrate the potential application of our work.

- **Scenario 1.** Suppose there is an electronic marketplace where agents may sell/buy a used laptop using a bargaining protocol. Assume that all negotiations are initiated by the sellers. In order to facilitate the bargaining, the authority (electronic market) allows an agent to negotiate with multiple agents simultaneously. However, a nasty buyer may replicate her buying agent into several different agents who negotiate with the same seller. As the seller rejects one of them, the buyer may replicate an agent to join the negotiation again. Since the seller cannot detect the 'real' identity of the buying agents, the seller will be exploited until the buyer makes his final decision. More seriously, if the seller uses a learning algorithm in its decision, such as predicting the market price, then the buying agent will manipulate the seller's belief. What puts a seller at a disadvantage is that it reveals the same information (e.g., item being sold); thus replicating itself into multiple sellers cannot help much. To deal with this issue, the authority may prohibit any buyer/seller from using more than one agent in the same negotiation, for instance, by checking the identity of all agents' owners or by asking for some deposit for each agent registered in the market; however, the former will burden the server while the latter will burden the users. Alternatively, the authority may check the identity of agents randomly and impose punishment for an offense.
- **Scenario 2.** Suppose 1,000 deep-sea autonomous voyagers from a joint mission of various enterprises are sent to explore the bottom of the Atlantic Ocean. In order to facilitate their mission, 10 mobile power stations are sent to accompany them such that they can recharge their batteries without going to the surface. The service is on a first-come-first-serve and limited-charging-time basis. However, some voyagers may collude