Chapter 6
Game Theory for Network Security

ABSTRACT

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. It involves the authorization of access to data in a network, which is controlled by the network administrator. Usually, network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies, and individuals. This chapter explores network security.

INTRODUCTION

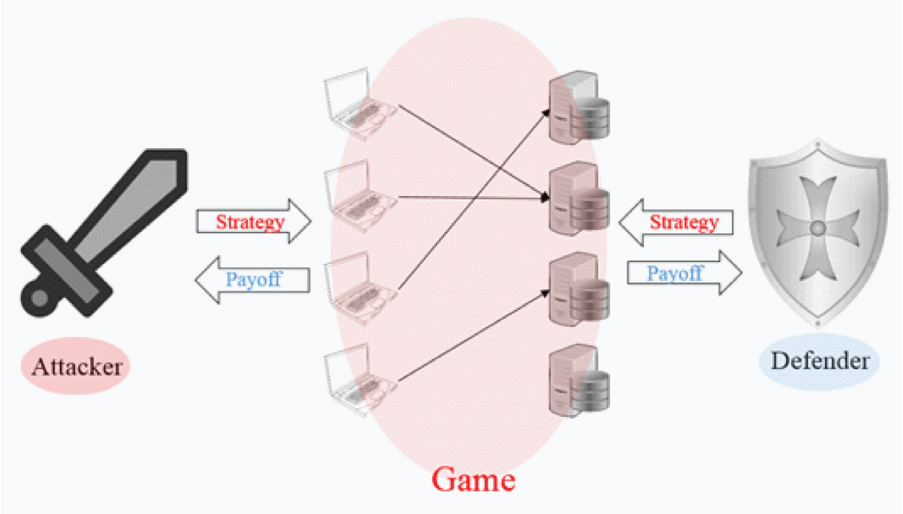
Security is a critical concern around the world that arises in protecting our ports, airports, transportation or other critical national infrastructure from adversaries. Nowadays, security arises in problems ranging from physical to cyber physical systems. In particular, network security becomes a challenging topic, and the research community has been paying attention to the network security problem. However, the problems are far from being completely solved. For more than one decade, game theoretic approach has been recognized as a useful tool to handle network attacks (Liang, & Xiao, 2013), (Tambe, Jain, Pita, & Jiang, 2012), (Roy, Ellis, Shiva, Dasgupta, Shandilya, & Wu, 2010). In this chapter, we review the existing game-theory based solutions for network security problems (Figure 1).

DOI: 10.4018/978-1-4666-6050-2.ch006

NON-COOPERATIVE GAMES FOR NETWORK SECURITY

Most game theoretic approaches applied in network security require attack-defense; the interactions between attackers and defenders may be formulated as non-cooperative behaviors which may then be described and solved using game theory (Liang, 2013). Therefore, the most existing game-theoretic research as applied to network security falls under non-cooperative games. Non-cooperative game models including two subclasses, static games and dynamic games. Moreover, within static and dynamic subclasses, game model can be further grouped in terms of whether they are of complete information or whether they are of perfect information (Liang, 2013).

Figure 1. Game theory for network security



Non-Cooperative Static Games

All static games are one-shot games of imperfect information. Therefore, static games with perfect information do not exist (Liang, 2013). According to the completeness of information, static games can be classified into two sub-classes - complete information static games and incomplete information static games. Complete information static games model the scenario of the interactions between attackers and defenders. The solution to complete information static games is the Nash equilibrium. When defenders could not always distinguish attackers from regular users, not only the interactions between attackers and defenders but also those between regular nodes and defenders should be considered. Therefore, the games are modeled as incomplete information static games, which could model the interactions not only between attackers and defenders, but also between regular nodes and defenders. In this game model, defenders keep an inference of the type (malicious or regular) of another node as its opponent. The solution to incomplete information static games is the Bayesian Nash equilibrium (Liang, 2013).

Static Games with Complete Imperfect Information

Complete imperfect information game is a game in which every player knows both the strategies and payoffs of all players in the game, but not necessarily the actions. In other words, this kind of game does not take into account the actions each player have already taken (Roy, 2010). Recently, some non-cooperative static games with complete imperfect information have been developed. Under information warfare scenario, attack-defense games are general-sum, two-player static games in which the action sets of the players are simply {attack, not attack} and {defend, not defend}. The payoff functions for the players capture the damage to the system and the costs to attack and to defend. The mixed strategy Nash equilibrium is obtained as the solution of game in the form of a combination consisting of the attacking probability and the defending probability (Liang, 2013). For investment efficient strategies in cyber security, attack-protect economic model was presented by using a computational approach to quantitative risk assessment. The main goal of this game model is