Chapter 80
A Proactive Defense Strategy to Enhance Situational Awareness in Computer Network Security

Yi Luo
The University of Arizona, USA

Ferenc Szidarovszky
The University of Arizona, USA

ABSTRACT

With the development of situational awareness in intrusion defense, a proactive response is a realistic and effective approach against the attackers. It is assumed that each player can update knowledge of the opponent and assess possible future scenarios of the dynamic game based on their previous interactions. Therefore, finding the best current move of the defender is modeled as a discrete-time stochastic control problem. An on-line, convergent, scenario based proactive defense (SPD) algorithm considering adaptive learning is developed based on differential dynamic programming (DDP) to solve the associated optimal control problem. Numerical experiment shows that the new algorithm can help the defender in finding the best dynamic strategies quickly and efficiently. Moreover, the SPD algorithm can provide optimal defensive efforts against possible future attacks within an appropriate time window, so the success of the attack in the possible future interactions can be assessed, improving situational awareness in computer network security.

BACKGROUND

With the development of information technology and computer network systems, cybersecurity is one of the most critical issues in almost every aspect of our society such as administration, business, finance, personal life, etc. Attackers often launch multi-stage attacks which can last several days, weeks and even months (Stewart, 2010). They are the most dangerous types of attacks, since the attackers use intelligence to break the defense of the system to reach their goals. Therefore, defense strategies against these attacks are becoming more and more important in cyber space and they had been intensively studied recently (Foo et al., 2005; Foo et al., 2008; Stakhanova

DOI: 10.4018/978-1-4666-4707-7.ch080

et al., 2007; Toth and Kruegel, 2002). The accurate and timely situational awareness can help the defender find its efficient response strategies against multi-stage attacks quickly. On the other hand, a well-designed response strategy with an appropriate way to model the attacker's and the defender's decision processes and their interactions can affect current situational awareness, and it is the main objective of this chapter. Classical game theory examines decision making problems with more than one decision maker and conflicting interests. In cyber security, the outcomes of the attack and the defense depend on the efforts of both of them, therefore game theoretic analysis is the most appropriate approach to model and analyze their interactions. Many scholars used multi-player sequential decision making models as stochastic (Markovian) games (Lye and Wing, 2005; Shen et al., 2007), while others applied partially observable Markov decision processes (POMDP) to model the attacker's actions (Carin et al., 2008; Luo et al., 2009b; Zhang and Ho, 2009). However, the main disadvantage of the Markovian and the POMDP models is the extremely large state space, and therefore the solutions are hard to compute. Some scholars in the intrusion defense research community claim that the dynamic game approach is more efficient than the application of Markovian games under many situations (Liu and Zang, 2003; Siever et al., 2007), and proactive defense strategies need to be considered for intrusion defense system (Wood et al., 2000) as well. Therefore, a discrete-time dynamic evolutionary game and proactive response mechanisms are employed in this chapter to enhance situational awareness in computer network defense.

INTRODUCTION

In this chapter, the interactions between an attacker and the defender of a computer network are modeled as a system of two-person non-zero-sum non-cooperative dynamic evolutionary games with incomplete information. In the dynamic evolutionary games, the type of the players, their strategy sets, the prediction of future interactions, etc. are uncertain. The payoffs of the players are therefore random at each interaction of the game. The classical equilibrium approach has its limitations to find the solutions under this situation, so risk analysis is used often to complement the equilibrium approach to capture the uncertainty of the random elements in the players' payoff functions (Hausken, 2002; Banks and Anderson, 2006; Bier and Azaiez, 2008).

The nature of the distribution of a random variable mathematically can be described by the central moments (Samuelson, 1970). Clearly, the characterization of a random variable becomes more accurate if higher moments are employed. However, the complexity of the computation process increases as well. The first moment is usually used by researchers to describe the payoffs of the players leading to expected value analysis (Bier et al., 2005; Azaiez and Bier, 2007; Levitin, 2007; Zhuang and Bier, 2007), while a linear combination of the expectation and variance is considered as the certain equivalent of the random payoff value. A risk attitude coefficient is assigned to the variance and can be learned by the opponent along the evolutionary game. This is a well-known approach to describe the uncertainty of the dynamic system in economic literature. However, the probability distribution of the players' future possible activities is a concern in our response strategies. For updating the defender's knowledge and for the evaluation of the probability distributions of possible future attacks, we refer to our earlier works (Luo et al., 2009a; 2010; 2011). In this chapter, we assume that the players are able to update their knowledge of the opponent after each interaction, they can predict on-line the opponents' activities and the probabilities of their occurrences. Finding the best proactive defense strategy at any time period of the game is therefore modeled as an optimal control problem.