Adversarial Organization Modeling for Network Attack/Defense

Ji Wu, Chaoqun Ye, and Shiyao Jin
Collage of Computer Science and Technology,
National University of Defense Technology,
Changsha 410073, China
{wwujji, cqyie, Syjin1937}@163.com

Abstract. To appropriately address the problem of large-scale distributed cyber attacks and defenses, issues such as information exchange, work division and coordination must be addressed. We believe that focusing on logical foundations for information assurance construction provides the theme that drives how various defense components work together. This paper proposes an opponent agent’s mental model based on the theory of Belief-Desire-Intention, adopts the notions of agent, group and role to specify the organizational structure of distributed network attacks/defenses, and applies the computational framework of agent team to model organizational dynamics of network attacks/defenses.

1 Introduction

Throughout the rise of commercial interest in the Internet has lead to the integration of the information infrastructure as a core component of the economy. However, an increasing number of cyber attacks and threats of cyber attacks on world-wide networks have shown that energy, transportation and finance infrastructures are vulnerable with potentially dire consequences. Protecting these infrastructures has become a critical and key area of interest. Unfortunately, the existing theoretical base for information assurance in large-scale systems does not correspond to the indicated tendencies. We think that the majority of problems in information assurance are caused by immaturity of logical foundations for construction of integrated adaptive security systems operating in adversarial environments. This paper seeks to address this problem by introducing opponent modeling under adversarial environment on network attack/defense.

This paper proposes an opponent agent’s mental model based on the BDI (Belief-Desire-Intention) theory[1], adopts the notions of agent, group and role to specify the organizational structure of distributed network attacks/defenses, and applies the computational framework of agent team to model organizational dynamics of network attacks/defenses. The goals of the paper are as follows: 1) development of formal framework for modeling and simulation of a wide spectrum of network attacks/defenses based on multi-agent system methodology; 2) elaboration of formal specifications of a representative spectrum of such attacks/defenses; 3) instantiation of an agent-based organizational model making it possible to simulate network attacks and respective defense; 4) seeking enhancement of co-evolution modeling in organizational levels.
The paper will be organized as follows. First, we will formalize the mental state of an opponent agent according to the BDI theory. Next we describe the AGR (agent-group-role) model for network attack/defense organization structure. We also show that using agent team, a computational model organizational dynamics of network attacks/defenses can be developed. Finally, we conclude with a discussion of issues related to network attack/defense modeling and simulation.

2  Opponent Agent Model

Based on the BDI theory[^1], mental states of deliberative cyber-war agent can be modeled as

\[ \text{\( MS \equiv <G, T, B, D, I, K > \)}\]

where \( G \) described agent’s goal; \( T \) is time set which marks the dynamic of agent mental states; \( B, D, I \) are primary definition of agent’s \textit{Belief}, \textit{Desire}, and \textit{Intension}; \( K \) is knowledge owned by agent. Below describe the model in more details:

- \( G: G\times T\times M\rightarrow G' \) – Goal of cyber-war agent is transitional function of original goal and external environment events \( M \), which are abstracted as message serial. Agent’s goal will dynamically change with time and external events, then form a goal serial;
- \( B: B\times T\times M\rightarrow B' \) – Belief of cyber-war agent transitional function of original belief and external environment events \( M \). Agent’s belief will dynamically change with time and external events, then form a belief serial;
- \( D: D\times T\times M\rightarrow D' \) – Desire of cyber-war agent transitional function of original desire and external environment events \( M \). Agent’s desire will dynamically change with time and external events, then form a desire serial;
- \( I: I\times T\times M\rightarrow I' \) – Intention of cyber-war agent transitional function of original intention and external environment events \( M \). Agent’s intention will dynamically change with time and external events, then form an intention serial;
- \( K: K\times T\times M\rightarrow K' \) – Knowledge of cyber-war agent transitional function of original knowledge and external environment events \( M \). Agent’s knowledge will dynamically change with time and external events, then form a knowledge serial.

Mental state of cyber-war agent is dynamic rather than static. With the advancing of attack or defense, agent’s mental state will correspondingly evolve, for example, if attack has been chased, then the attack goal will be abandoned. The evolve mode of agent mental state can be modeled as \( <\text{ms}^0, \text{next}_\text{act}, \text{next}_\text{MS}> \), where \( \text{ms}^0 \in MS \) denotes the initial mental state; \( \text{next}_\text{act}: MS\times ACT\rightarrow ACT \), is select function mapping mental state set to attack/defense atomic action set; \( \text{next}_\text{ms}: MS\times ACT\rightarrow MS \), denotes mapping function which generates a new mental state after attacker or defendant execute a atomic action.

During the warfare, agents achieve their goals by make appropriate action plan, which are generated based on each agent’s mental state, resources in hand and cost evaluation. Extending to the formalism of [2], an agent action plan can be described as such a quad-tuple: