Journal of Industrial Information Technology and Application Vol.2 No.1

ISSN(Online) : 2586-0852

Cognitive Game Theory Models for Cyber Security

Sankardas Roy [1*)], Yan Wu [2)]

[1)] CS Department, BGSU, Bowling Green, Ohio, USA

[2)] CS Department, BGSU, Bowling Green, Ohio, USA

Abstract. **Game theory is an attractive framework to model the conflicting interests of the cyber-attacker and defender, and researchers have used game models to determine an optimal defense strategy. The current model assumes that the players are rational, and based on that assumption it determines the equilibrium payoff of the players. However, in reality the attacker might have limited rationality, and the defender could reap a better payoff from the game if she can learn the attacker's intent. There comes the role of a cognitive model through which the defender can learn the attacker's intent from the attacker's prior actions, which can lead to a higher payoff for the defender. In this paper, we explore the existing cognitive models from the field of psychology, and investigate how the defender can leverage them to better protect the cyber space.**

Keywords; game theory, cognitive models, cyber security.

1. Introduction

Nowadays cyber-attacks are a big threat to government organizations as well as industries. Game theory framework poses great potential as it can model the conflicting interests of the attacker and defender. Prior researchers have used game models to determine optimal defense strategy. In a typical cyber attack, the attacker interacts with the system and the system administrator over long time. Typically, the attacker goes through a set of stages, such as reconnaissance, attack initiation, attack escalation, etc., which continue over a period of time such as hours. In a cyber scenario, since the game goes through multiple stages, the dynamic game model seems to be a good fit. However, the current game models typically assume that the players are rational, and based on that assumption they determine the equilibrium payoff of the players. Yet, in reality the attacker might have limited rationality, and the defender could reap a better payoff from the game if she can learn the attacker's intent. There comes the role of a cognitive model

* Corresponding author : sanroy@bgsu.edu

in which the defender attempts to learn the attacker's intent from attacker's prior actions. Assuming that the defender's learning is substantial, it can lead to a higher payoff for the defender. In this paper, we explore the existing cognitive models from the field of psychology, such as Cognitive Hierarchy (CH) model [1], ACT-R [2], and more. We investigate how the defender can leverage a cognitive model to better address the security threat. In particular, we identify the benefit of the cognitive models compared to the model-less defense. The main contributions of the paper are as follows: We show that using a cognitive model (of the attacker), the defender can potentially learn the attacker's intent, which can lead to better protection of the cyber space.

Organization. Section 2 presents an overview of a collection of cognitive models that are already present in the literature. In Section 3, we discuss how the defender can learn from her observations over the course of the game and hence can position her better by choosing a more effective strategy against the attacker. Section 4 concludes the paper.

2. Cognitive Models

Decision making, which is a complicated process, involves the interaction of the problem to be solved, the environment, attributes that contribute to the solution, and the players [3]. A game theory model assumes that players think strategically, meaning that they choose their own strategy by analyzing what others might do, then choose rational responses given their beliefs. In this process, they also assume that other players do the same with rational choices. However, prior studies of cyber-attack events indicate that the attacker often acts with limited rationality. The reality exposed several problems in the assumption of rationality in a game theory model: First of all, human being is not fully rational. Inevitably, emotions affect the reasoning process, which in turn affects their choice of strategy in a game. Second, in a scenario of multiple-stage long-run game, players tend to make their decisions based on only current deduction of the opponents' strategy, not considering the history information including previous actions and payoffs; players do not utilize the learned knowledge about behavior of the opponents. Third, in real world games, players believe that their opponents are not doing as much thinking as they are, e.g., bidders' common activities in the stock market [1].

According to prior literature, to make any conscious interpretation of human behavior, the assumption of rationality of the players is necessary, and there has been an uncritical acceptance of the idealized concept of rationality in the philosophy of psychology [4]. Cherniak also proposed a concept of minimal rationality, in which a person can have a less-than-perfect deductive ability.

If players in a game are with limited rationality, they may not be able to accurately predict other players' strategies and thus the game may not reach the equilibrium as predicted by the mainstream game theory. An alternative Cognitive Hierarchy (CH)

theory [1] describes player's decision as a step-by-step reasoning procedure, in which each player assumes that her strategy is the most sophisticated, and as a result, the equilibrium with full rationality assumption will not be reached. A beauty contest in which participants guess which faces others will judge to be the most beautiful [5] is cited to explain this CH theory. This beauty contest is not about choosing those who are really the prettiest according to the player's best judgment, nor even those who are thought to be the prettiest by average opinion. People actually have reached the third degree, where they try to predict what average opinion expects the average opinion to be. The essence of beauty contest game can be captured by a simplified number guessing game, in which players are asked to pick numbers from 0 to 100, and the player whose number is closest to 2⁄3 of the average wins a prize. According to equilibrium theory, each player will reason as follows: "Even if all the other players guess 100, I should guess no more than 2⁄3 times 100, or 67. Assuming that the other players reason in the same way, however, I should guess no more than 45... " and so on, finally concluding that the only rational and consistent choice for all the players is zero.

The CH model described the iterative, k-step decision process, and the corresponding frequency distribution value of each step. The hierarchical process starts with "step 0", in which the players do not assume anything about their opponents and merely choose their strategies according to certain probability distribution. "Step k" thinkers assume that their opponents are distributed, according to a normalized Poisson distribution, from step 0 to step k - 1; that is, they accurately predict the relative frequencies of players doing fewer steps of thinking, but ignore the possibility that some players may be doing as much or more.

ACT-R [2] architecture was applied on associative learning that cumulates item-to-item associations by strengthening or weakening associations via repeated exposures. This account of model provides the clue of how people learn from history and recall memory when met relevant situation, or simply recall elements from their memory. Erev and Barron [6] proposed a model of Reinforcement Learning Among Cognitive Strategies (RELACS) to explain the payoff variability effect and other deviations from maximization. RELACS assumes that a decision maker follows one of three cognitive strategies in each choice, and that the probability of using a strategy is determined by previous experiences with the strategy.

In a multi-stage game, players with limited rationality tend to under-estimate opponents' strategy in a naïve way, and miss the possibility that opponents may do further thinking than themselves. (If defender can make use of these traits to defend, it might be helpful). Also, the information of strategy and the corresponding payoffs collected from opponents provides their behavior patterns, and defender could reinforce the model of opponents' strategy to predict future behavior.

3. LEARNING-BASED Defence Mechanism

In a real cyber-attack scenario, the attacker or the defender does not often have complete picture of the opponent. For instance, the sensors that the defender uses to probe the system or to sense the attack activities may not be perfect. In such an imperfect or incomplete game, the defender faces uncertainties about the attacker's action space, and the attacker's level of knowledge. Another challenge is that the defender needs to be careful about the following: more probing she does to gather information about the attacker (or the attack strategy), more information she leaks to the attacker; more information the attacker gets about the defender (or the defense strategy) more advantage the attacker enjoys. It is advisable for the defender to be aware of the above tradeoff.

Given the uncertainties of the system, the defender needs to leverage a learning technique to (select and to) adapt the defense strategy. The defender may take one of the following approaches: model-less and model-supported.

A. Model-less Approach

In the model-less approach, the defender does not attempt to model the attacker's behavior. Instead, the defender observes over the course of the game the players' actions and the effects of those actions. Using the prior observations, the defender attempts to figure out her best possible action at any stage of the game. In this approach, the defender does not consider that the attacker could have a hidden intent. Instead, the defender sees the attacker as a part of the system. The defender basically attempts to learn the association between the players' actions and the game outcomes, and the defender adapts the defense strategy accordingly. There is interaction among the game-theory model, the system, and the defender's learning agent. We assume the presence of the "standard attack strategy" module (inside the game theory framework), which conservatively predicts the attacker's strategy given the system states and event logs.

B. Model-supported Approach

In the model-supported approach the defender builds and maintains a cognitive model for the attacker's behavior. The cognitive model allows the defender to deduce the attacker's intent. In particular, through the employed sensors the defender collects the logs of system events. By analyzing these logs, the cognitive model tries to gauge the cognitive process of the attacker. For instance, the cognitive process of an insider attacker can be different from that of an outsider attacker. Furthermore, cognitive process of a state-sponsored cyber-attacker can be different from that of a hacktivist group (e.g., Anonymous) or that of a terrorist organization. Moreover, the motivation factor can be different for these attackers, which can be influenced by different recent news items. A cognitive model attempts to keep track of such pieces of information. Furthermore, an attacker typically leaves a trail of artifacts (which are potentially picked by defender's

sensors) while he goes through different steps, e.g., reconnaissance, passive data stealing, active disruption, and so on. Along with such artifacts, the cognitive model attempts to observe the attacker's language and pattern of communication. Through the help of all of these pieces of information, the cognitive model tries to reveal attacker's intentions as well as his reasoning process. After sufficient learning, the cognitive model also attempts to predict attacker's next action.

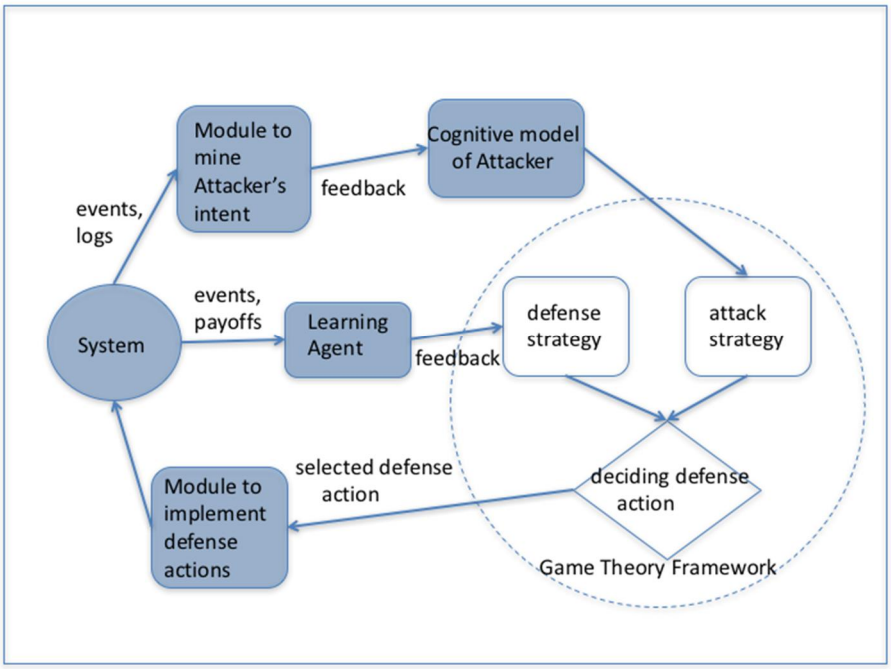

Figure 1: Model-supported learning-based defense

Figure 1 illustrates the interaction among the cognitive model ("modeling the attacker"), the game theory framework, defender's learning agent, and the system. Note the feedback coming from the "intent mining" module to the cognitive model, which allows the defender to leverage the event logs to make corrections in the cognitive model in an iterative fashion.

The cognitive model can also detect possible deception of the attacker. Through systematic analysis of the language and pattern of the attacker's communication (collected through system logs as well as out-of-bound communication, such as social networks), the cognitive model can distinguish realistic threats from hoaxes. As discussed before, attackers can have different resources, incentives or goals. We hypothesize that it is possible to extend Dennet's Theory of Intent [7] to build a cognitive

model, which will potentially enable the defender to detect attacker's deception. Such a rich cognitive model may help reduce the false alarm rate for the attack detection. This can also help the defender in taking a proactive defense strategy. For instance, to counter against attacker's deception, the defender can inject more randomness into the system via schemes like moving target system or decoy placement.

As in a typical cyber-attack scenario the defender does not have perfect or complete information about the attacker's set of actions or motives, defender's modeling the attacker's intent helps the defender choose a more effective strategy for the security game. Thus leveraging a cognitive model often leads to a higher payoff for the defender.

4. Conclusion

Prior researchers and practitioners observed that a typical cyber attacker might have limited rationality. In this paper we illustrated how the defender could reap a better payoff from the game if she can learn the attacker's true intent. We showed using a cognitive model (of the attacker) the defender can learn the attacker's intent from the attacker's prior actions. We explored the existing cognitive models from the literature, and discussed how the defender can leverage them to better protect the cyber space. We identified the benefit of such cognitive models compared to the model-less defense. As a future work, we plan to run several experiments through simulation to measure the performance of model-less and model-supported defense schemes in several system setting, and we will perform a comparative study.

References

[1] G. Camerer, C. F., Ho, T. H., & Chong, J. K., "A cognitive hierarchy model of games." The Quarterly Journal of Economics, 2004, pp. 861-898.

[2] Thomson, R., Pyke, A. A., Trafton, J. G., & Hiatt, L. M., "An account of associative learning in memory recall". In Proceedings of the Annual Meeting of the Cognitive Science Society, 2015.

[3] Saaty, T. L., How to make a decision: the analytic hierarchy process. European Journal of Operational Research, 48(1), 1990, pp. 9-26.

[4] Cherniak, C., Minimal rationality. Mind, 90(358), 1981, pp. 161-183.

[5] Keynes, J. M., The General Theory of Interest, Employment and Money London: Macmillan, 1936.

[6] Erev, I., & Barron, G., On adaptation, maximization, and reinforcement learning among cognitive strategies. Psychological Review, 112(4), 2005, pp. 912-931.

[7] Dennett, Daniel, "Intentional systems theory". The Oxford handbook of philosophy of mind, 2009, pp. 339-350.