Goal Recognition Assisted Decision Making in Security Games: A Real-time Attack Graph Interdiction Game

Kaiming Xiao[1], Cheng Zhu[1], Kai Xu[2], Yun Zhou[1], Xianqiang Zhu[1], Weiming Zhang[1]
1. Science and Technology on Information Systems Engineering Laboratory, NUDT, Changsha, 410073, China
2. The Institute of Simulation Engineering, College of Information System and Management, NUDT, Changsha, 410073, China
kmxiao@nudt.edu.cn

Abstract

Security games provide a methodology for making decisions when taking attackers' reactions into account, whereas attack graph is an efficient modelling technique for security risk assessment. In this paper, we proposed a real-time attack graph interdiction game by utilizing inferred knowledge from goal recognition, as well as a strategy to bridge the gap between the observation and decision making. Initial experimental results show the effectiveness and accuracy of the proposed methods.

1 Introduction

Cyber security is an epitome of asymmetric, strategic conflict between defenders and attackers, which is usually modelled as Stackelberg security games [Wilczynski *et al.*, 2016]. Specifically, the attacker launches a series of intrusion actions persistently such as network scanning and vulnerability exploiting to penetrate the targeting network, while the defender deploys countermeasures such as intrusion detection/prevention systems, firewalls and honeypots on selected componets to protect the network from cyber attacks [von Solms and van Niekerk, 2013].

Attack graph, on the other hand, is one of the tools for analysing the security landscape of a network; thus can provide both players in the security game with an overview of the battlefield, which contains all possible penetrating paths towards critical goal nodes. Although, abundance of studies have been conducted on generating algorithms and analysis methods of attack graphs [Yi *et al.*, 2013], few studies have utilized knowledge from attack graphs thereby assisting defenders in making better decisions in security games.

Recently, some researchers have studied static security games on attack graphs, such as the game-theoretical approach for honeypot deployments using attack graph information [Durkota *et al.*, 2016], the network interdiction game based on attack graphs [Nandi *et al.*, 2016]. However, real-time decision making in security games on attack graphs, as well as the utilization of knowledge from attack graphs, remains an open question. Therefore, we propose a Model Predictive Control (MPC) strategy to bridge the gap between the goal recognition and decision making in the real-time Attack Graph Interdiction (AGI) game, which is based on a proposed Markov Decision Process (MDP) -based goal recognition and a Bi-level Mixed Integer Programming (BLMIP).

2 MPC Strategy for the Real-time AGI Game

2.1 Problem Definition

In the real-time AGI game, the attack graph is donated by $G(N, A)$, where node set N represents attack states of the networked system and arc set A represents atomic attacks. Let c_k denote the attack cost on the arc $k = (i, j) \in A, \forall\, i, j \in N$, whereas r_k and d_k denotes the defence cost and the added attack cost caused by the countermeasures on arc (i, j) respectively. The attacker aims to penetrate to a certain node $g \in N$ in G from an initial state node s at the lowest cost, while the defender attempts to deploy limited countermeasure resources R on a selected set of arcs in order to maximize the lowest cost of the attacker in real time. That is, both the attacker and the defender adopt an observe-and-response action rather than an once-and-for-all decision. Meanwhile, we assume that the attacker's exact goal node g is unknown for the defender, which is rife and reasonable in real conflicting games in cyberspace. Hence, we can formulate the real-time AGI game as a multi-stage BLMIP problem:

$$\textbf{[RTAGI-P]} \quad \max_{\mathbf{x_t} \in X} \min_{\mathbf{y_t}} \sum_{k \in A} (c_k + x_{kt} d_k) y_{kt}$$

$$s.t. \sum_{k \in FS(i)} y_{kt} - \sum_{k \in RS(i)} y_{kt} = \begin{cases} 1 & \text{for} \quad i = s_t \\ 0 & \forall i \in N \backslash \{s_t, g_1, \cdots, g_m\} \\ -p(g_j) & \forall i = g_j, j \in \{1, \cdots, m\} \end{cases}$$

$$x_{kt} \in \{0, 1\},\ \forall k \in A; \quad y_{kt} \geq 0,\ \forall k \in A$$

where $X = \{\mathbf{x_t} \in \{0,1\}^{|A|} | \mathbf{r}^T \mathbf{x_t} \leq R_t\}$, and $\sum_t R_t \leq R$ is an overall constraint for the whole multi-stage game. $k \in FS(i) (k \in RS(i))$ denotes arcs directed out of (into) node i. x_{kt} and y_{kt} are decision variables, where $x_{kt} = 1$ if arc k is interdicted by the defender; else $x_{kt} = 0$; $y_{kt} = 1$ if arc k is exploited by the attacker; else $y_{kt} = 0$. Besides, $0 \leq p(g_j) < 1, \sum_{j=1,\cdots,m} p(g_j) = 1$, the probabilistic distribution over the possible goals $g_1, \cdots, g_m$.

2.2 MDP-based Goal Recognition

The aim of goal recognition is to provide the defender with probabilistic distribution over the possible goals. The proposed MDP model is a combination of three

parts: a) the standard MDP; b) the agent goal and c) the goal termination variable, which are denoted by a tuple $< s_0, S, G, e, A, P_a(s'|s), O >$ where s_0 is the initial state, S denotes the non-empty state space with goal states $G \subseteq S$. $e = \{0, 1\}$ denotes the termination states, and A, O denotes the set of actions and observations respectively. $P_a(s'|s)$ is the probability for $a \in A$, $s, s' \in S$. Essentially, the model is a Dynamic Bayesian Network, in which all causalities could be depicted. Thus, the behaviour of system evolution can be described using a state transition function ($P_{s_t} = p(s_t|s_{t-1}, a_t)$) and a observation function ($P_{o_\tau} = p(o_t|s_t)$).

Recognizing the evader's goal is an inference problem trying to find the real goal behind agent actions based on observations online. To achieve this, we use Particle Filter method which is an approximate inference method designed to handle non-Gaussian, nonlinear and high-dimensional problems.

2.3 MPC Strategy for Decision Making

The MDP-based goal recognition model serves as the system model in this MPC framework, and the optimizer is defined to solve the [RTAGI-P] as a single-stage static problem in a rolling horizon manner.

In each stage t, we solve the [RTAGI-P] optimally for decisions x^*_{kt}; however, only the decisions relating to $FS(s_t)$, i.e., the outgoing set of the current source node s_t, are implemented at stage t. That is,

$$x_{kt} = x^*_{kt},\ \forall k \in FS(s_t); \quad x_{kt} = 0.\ \forall k \notin FS(s_t)$$

Thus, only a small part of countermeasure resources are deployed in each stage t as the urgent and necessary deployment, i.e., $R_t = \sum_k r_{kt} x_{kt},\ \forall k \in FS(s_t)$.

The remaining resources are still available for future deployment. That is, using this MPC strategy the defender can adopt an observe-and-response decision adaptively. This helps the defender reduce the decision-making risk due to the uncertainty of its opponent's intention. Accordingly, the defender can avoid countermeasures resources waste and achieve more robust decisions.

3 Experiments

A set of attack graphs are generated according to the method in [Nandi *et al.*, 2016] and are used to illustrate the efficacy and efficiency of the proposed MDP-based goal recognition and the MPC strategy for real-time AGI game.

We run the agent decision model of the attacker repeatedly and collect a test dataset consisting of 100 labeled traces on a simulated 20×40 attack graph. Our inference method is evaluated and validated in Table 1 by measuring its precision, recall and *F*-score, which are frequently used to measure overall accuracy of the recognizer. It can be observed that when the progress rate is bigger than 40% and 50%, the values of three measures are over 80% and 95% respectively.

The performance of proposed MPC strategy for decision making is then compared with a static interdiction strategy, as shown in Figure 1 (Error-bar). A defender who adopts the MPC strategy achieves more payoff (i.e., the added penetrating cost of its opponent) than those who adopt the static defence strategy when given the same amount of countermeasure resources. Besides, this superiority of MPC strategy increases as the growth of available countermeasure resources (a certain percentage of $\sum_k r_k$). As shown in Figure 1, the added penetrating cost under the proposed MPC strategy is nearly 2 times of that under the static strategy, which is an overwhelming improvement for the defender's decision making.

Progress Rate	Precision	Recall	F-score
10%	0.282	0.298	0.290
20%	0.445	0.529	0.484
30%	0.610	0.616	0.612
40%	0.843	0.814	0.828
50% - 100%	> 0.950	> 0.950	> 0.950

Table 1: Inference Evaluation

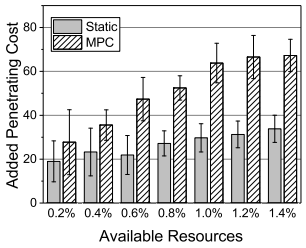

Figure 1: Interdiction Performance

4 Conclusion

We present a real-time attack graph interdiction problem using a game-theoretical approach, and a MPC strategy is proposed to bridge the gap between the observation and decision making. Experimental results show the effectiveness and accuracy of our methods as well as the value of inferred knowledge utilization to decision making in security games.

Acknowledgments

This work is sponsored by the National Natural Science Foundation of China under Grants No.71571186 and No.71471176.

References

[Durkota *et al.*, 2016] Karel Durkota, Viliam Lisỳ, Christopher Kiekintveld, Branislav Bošanskỳ, and Michal Pěchouček. Case studies of network defense with attack graph games. *IEEE Intelligent Systems*, 31(5):24–30, 2016.

[Muñoz-González *et al.*, 2016] Luis Muñoz-González, Daniele Sgandurra, Andrea Paudice, and Emil C Lupu. Efficient attack graph analysis through approximate inference. *arXiv preprint arXiv:1606.07025*, 2016.

[Nandi *et al.*, 2016] Apurba K Nandi, Hugh R Medal, and Satish Vadlamani. Interdicting attack graphs to protect organizations from cyber attacks: A bi-level defender–attacker model. *Computers & Operations Research*, 75:118–131, 2016.

[von Solms and van Niekerk, 2013] Rossouw von Solms and Johan van Niekerk. From information security to cyber security. *Computers & Security*, 38:97 – 102, 2013.

[Wilczynski *et al.*, 2016] Andrzej Wilczynski, Agnieszka Jakóbik, and Joanna Kolodziej. Stackelberg security games: Models, applications and computational aspects. *Journal of Telecommunications and Information Technology*, (3):70, 2016.

[Yi *et al.*, 2013] Shengwei Yi, Yong Peng, Qi Xiong, Ting Wang, Zhonghua Dai, Haihui Gao, Junfeng Xu, Jiteng Wang, and Lijuan Xu. Overview on attack graph generation and visualization technology. In *Anti-counterfeiting, security and identification (asid), 2013 IEEE international conference on*, pages 1–6. IEEE, 2013.