Engineering Applications of Artificial Intelligence 37 (2015) 145–153

Contents lists available at ScienceDirect

Engineering Applications of Artificial Intelligence

journal homepage: www.elsevier.com/locate/engappai

A Stackelberg security game with random strategies based on the extraproximal theoretic approach

Kristal K. Trejo [a], Julio B. Clempner [b,*], Alexander S. Poznyak [a]

[a] Department of Control Automatics, Center for Research and Advanced Studies, Av. IPN 2508, Col. San Pedro Zacatenco, 07360 Mexico City, Mexico
[b] Center for Economics, Management and Social Research, National Polytechnic Institute, Lauro Aguirre 120, col. Agricultura, Del. Miguel Hidalgo, 11360, Mexico City, Mexico

ARTICLE INFO

Article history:
Received 19 May 2014
Received in revised form
2 September 2014
Accepted 3 September 2014
Available online 2 October 2014

Keywords:
Security games
Strong Stackelberg equilibrium
Extraproximal method
Finite Markov chains

ABSTRACT

In this paper we present a novel approach for representing a real-world attacker–defender Stackelberg security game-theoretic model based on the extraproximal method. We focus on a class of ergodic controlled finite Markov chain games. The extraproximal problem formulation is considered as a nonlinear programming problem with respect to stationary distributions. The Lagrange principle and Tikhonov's regularization method are employed to ensure the convergence of the cost functions. We transform the problem into a system of equations in a proximal format, and a two-step (prediction and basic) iterated procedure is applied to solve the formulated problem. In particular, the extraproximal method is employed for computing mixed strategies, providing a strong optimization formulation to compute the Stackelberg/Nash equilibrium. Mixed strategies are especially found when the resources available for both the defender and the attacker are limited. In this sense, each equation in this system is an optimization problem for which the minimum is found using a quadratic programming approach. The model supports a defender and *N* attackers. In order to address the dynamic execution uncertainty in security patrolling, we provide a game-theoretic based method for scheduling randomized patrols. Simulation results provide a validations of our approach.

1. Introduction

1.1. Stackelberg game solution

The classical Nash original equilibrium solution concept (Nash, 1951) provides a reasonable non-cooperative equilibrium solution when the strategy profiles of the players are symmetric (no single player dominates the decision process). Nevertheless, there are other types of non-cooperative decision problems that introduce a hierarchical equilibrium solution concept that differs in many aspects from the classical Nash's approach. In these games, the player who has the ability to enforce his strategy on the other player(s) and knows the rational reaction set of his/her opponent is called the leader. The other players are called the followers. The equilibrium solution concept is the Stackelberg equilibrium solution and the corresponding game is called Stackelberg game, named after Heinrich von Stackelberg in recognition of his pioneering work on static games (von Stackelberg, 1934). The main problem arising in this concept is that, for each fixed strategy of the leader, there may exist several (or a set of) Nash equilibria (Clempner and Poznyak, 2011, 2013) for the followers.

The Stackelberg strategy for dynamic games was introduced in the works of Chen and Cruz, (1972), and of Simaan and Cruz, (1973a, 1973b), who also introduced the concept of a feedback Stackelberg solution, with the restriction that the follower's response was unique for each strategy of a leader. Its complement in the context of infinite games was first studied in Basar and Olsder (1995). Such a strategy exhibits an information bias between players leading to establishing a hierarchy between them. In addition, more recently, the scope of the applicability of the Stackelberg equilibrium concept in the field of game-theoretic modeling of preferences in hierarchical systems can be found in the work of Kołodziej and Xhafa (2011).

The *extraproximal approach* (Antipin, 2005) can be considered as a natural extension of the proximal and the gradient optimization methods used for solving the more difficult problems for finding an equilibrium point in game theory. The simplest and most natural approach for solving the proximal method is to use a simple iteration by omitting the prediction step. However, as shown in Antipin (2005), this approach fails. A more versatile procedure would be to perform an "*extraproximal step*," i.e., gathering certain information on the future development of the process. Using this information, it is possible to execute the

* Corresponding author. Tel.: +(52) 55 5729 6000 x 63105.
E-mail addresses: ktrejo@ctrl.cinvestav.mx (K.K. Trejo), julio@clempner.name (J.B. Clempner), apoznyak@ctrl.cinvestav.mx (A.S. Poznyak).

http://dx.doi.org/10.1016/j.engappai.2014.09.002
0952-1976/

"principle step" based on the preliminary position. Such iterative procedure realizes the application of a two-step method during each iteration: (a) at the first step, a "predictive approximation" of the current position is calculated; (b) at the second (basic) step, this prediction is used to complete the current iteration. It seems natural to call this procedure an "extraproximal method" (because of the use of extrapolation, Antipin, 2005). Along with the extragradient method (Polyak, 1987), the extraproximal method can be considered as a natural extension of the proximal and gradient optimization methods to resolve more complicated game problems, such as the Stackelberg–Nash game.

In particular, the formulation of the problem is considered as a nonlinear programming problem for finding the Stackelberg/Nash equilibrium point based on cost-functions that are supposed to be (not necessarily strictly) convex and differentiable on the corresponding sets (Moya and Poznyak, 2009). In addition, Tikhonov's regularization method is employed to ensure the convergence of the cost-functions to a Stackelberg/Nash equilibrium point. Tikhonov's regularization is one of the most popular approaches to solve discrete ill-posed problems represented in the form of a not necessarily strict convex function. Then, we transform the problem into a system of equations inn proximal format. Each equation in this system is an optimization problem for which the minimum is found using a quadratic programming approach. We present a two-step iterated procedure for solving the extraproximal method in terms of Markov chains: *the first step* (the extraproximal step) consists of a "prediction" which calculates the preliminary position approximation to the equilibrium point, and *the second step* is designed to find a "basic adjustment" of the previous prediction.

1.2. Related work

There has been an important research interest in employing Stackelberg game-theoretic approaches with the purpose to protect physical infrastructure. The classical problem is that security agencies have to protect a large number of targets with limited resources (people, money, time), making it impossible to defend all targets at the same time. The security agencies are responsible for protecting airports, ports, etc. In addition, the security agencies are required to patrol specific areas to prevent all crimes tear the fabric of civil society. Producing always the same resulting behavior can be exploited by intelligent attackers that carry out surveillance before an attack, so it is often desirable for the security agencies to have a system in which randomness is involved in allocating their resources. Game theory offers a formal mathematical framework for reasoning about the security problem.

Game-theoretic approaches have been used in multiple deployed applications, including: (1) ARMOR security system, including the randomized allocation of checkpoints and canine units at the Los Angeles International Airport (Pita et al., 2009; Jain et al., 2010) and, (2) IRIS, deployed by the Federal Air Marshals Service (Tsai et al., 2009; Jain et al., 2011) for randomizing Marshals on commercial flights, GUARDS: game-theoretic unpredictable and randomly deployed security (An et al., 2011; Pita et al., 2011) under development for the Transportation Security Administration (TSA) and, (4) PROTECT: Port Resilience Operational/Tactical Enforcement to Combat Terrorism under development for the United States Coast Guard (An et al., 2011; Shieh et al., 2012; Tambe, 2011) for randomizing port security patrols at the Boston Coast Guard. These are security games between a defender (allocating defensive resources), and an attacker (deciding on targets to attack): (1) the defender considers what the target (best-reply) of the attacker is; (2) then, holding the attacked target fixed, the defender picks a quantity that minimizes its payoff; (3) the attacker actually observes this and in equilibrium picks the expected quantity that maximizes its payoff as a response.

These applications (Pita et al., 2009, 2011; Jain et al., 2010, 2011; Tsai et al., 2009; An et al., 2011; Shieh et al., 2012; Tambe, 2011) use the (two-players) leader–follower Stackelberg game-theoretic formulation for solving the security problem, providing a randomized strategy for the defender (leader) and attacker (follower). Defenders are forced to execute a different patrol strategy from the planned one, due to unexpected events. On the other hand, there may be significant uncertainty regarding the amount of surveillance conducted by the attackers. The dynamics of the game is as follows: the defender first commits to a (pure/mixed) strategy, and the attacker plays the best-respond after observing the leader's strategy.

Further than the security applications presented above, the Stackelberg game-theoretic approach has been studied in depth in many other security problems related to patrolling in adversarial domains (Conitzer and Korzhyk, 2011; Conitzer and Sandholm, 2006; Hernández et al., 2014; Jain et al., 2010, 2011; Kiekintveld et al., 2009; Korzhyk et al., 2010, 2011; Letchford and Conitzer, 2010; Letchford et al., 2009, 2012; Paruchuri et al., 2008; Pita et al., 2010, 2009; von Stengel and Zamir, 2010).

1.3. Main contributions

To overcome the difficulties presented above, this work presents four major contributions. First, to address execution and observation uncertainty, our model presents a novel approach in Stackelberg security games that uses the extraproximal method for computing mixed strategies, providing a strong optimization formulation to calculate the Stackelberg/Nash equilibrium. Second, addressing the uncertainty of the strategies, we provide an extraproximal model that supports a defender and $\mathcal{N}$ attackers. The defender commits first to a strategy x in the Markov chains game. Then, the attackers simultaneously realize a Nash solution obtaining $\varphi_l(\cdot,\cdot|x)$ $(l=\overline{1,\mathcal{N}})$. The optimal action x of the defender is then chosen to minimize its payoff $\varphi_0(\cdot,\cdot|x)$. Third, each equation in this system is an optimization problem for which the minimum is found using a quadratic programming approach. This solution formulation also allows to represent the limited resources available for both the defender and the attackers. Fourth, in order to address the dynamic execution uncertainty in security patrolling, we provide a game-theoretic formulation method able to generate randomized patrol schedules based on a Markov decision process.

1.4. The structure of the paper

The paper is organized as follows. The next section introduces the necessary background to understand the rest of the paper and the formulation of the problem for an $\mathcal{N}-$player game. A Stackelberg game for a class of ergodic controllable finite Markov chains using the extraproximal method is given in Section 3. In Section 4, a numerical example related with *security games* validates the proposed method. Final comments and future works are outlined in Section 5.

2. Preliminaries

2.1. Controllable Markov chains

A *controllable Markov chain* is a 4-tuple $MC=\{S,A,\Upsilon,\Pi\}$ where S is a finite set of states, $S\subset\mathbb{N}$, endowed with discrete topology; A is the set of actions, which is a metric space. For each $s\in S$, $A(s)\subset A$ is the non-empty set of admissible actions at state $s\in S$. Without loss of generality we may take $A=\cup_{s\in S}A(s)$; $\Upsilon=\{(s,a)|s\in S, a\in A(s)\}$ is the set of admissible state-action pairs, which is a measurable subset of $S\times A$; $\Pi(k)=[\pi_{(i,j|k)}]$ is a stationary transition controlled