Solving Stackelberg Security Games For Multiple Defenders and Multiple Attackers

Cesar U. Solis and Alexander S. Poznyak
Department of Control Automatics,
Center for Research and Advanced Studies
Av. IPN 2508, Col. San Pedro Zacatenco,
07360 Mexico City, Mexico
Email: {csolis,apoznyak}@ctrl.cinvestav.mx

Julio B. Clempner
Center for Economics, Management and Social
Research, National Polytechnic Institute,
Lauro Aguirre 120, col. Agricultura,
Mexico City, 11360, Mexico
Email: julio@clempner.name

***Abstract*—In the last years, there has been a substantial effort in the application of Stackelberg game-theoretic approaches in the security arena, in which security agencies implement patrols and checkpoints to protect targets from criminal attacks. The classical game-theoretic approach employed successful to solve security games is that of a Stackelberg game between a defender (leader) and an attacker (follower).**

In this work we present a novel approach for computing optimal randomized security policies in non-cooperative Stackelberg security games for multiple defenders and attackers. The solution is based on the extraproximal method and its extension to Markov chains. We compute the unique Stackelberg/Nash equilibrium of the security game employing the Lagrange principle and introducing the Tikhonov regularizator method. We consider a game-theory realization based on a discrete-time random walk of the problem supported by the Kullback-Leibler divergence. Finally, we illustrate the usefulness of the proposed method with an application example in the security arena.

I. Introduction

A central assumption in the literature on Stackelberg security games is that limited security resources must be deployed strategically considering differences in priorities of targets requiring security coverage and the responses of the adversaries to the security position (see, for example, [1], [5], [6], [12]). In the dynamics of the game defenders commit to a probabilistic defense target and the attackers observe the probabilities with which each target is covered. Conitzer and Sandholm [7] described a method to commit to optimal randomized strategies in Stackelberg security games. Kiekintveld et al. [11] introduced a class of Stackelberg games focused on security settings. Subsequently this seminal works a number of follow-up papers come forward in the literature. For instance, Clempner and Poznyak [6] presented a shortest-path method to represent the Stackelberg security game as a potential game using the Lyapunov theory. Trejo et al. [22] employed the extraproximal method for computing the Stackelberg/Nash equilibrium in the case of one defender and multiple attackers. Yang et al. [25] and Nguyen et al. [13] based on bounded rationality computed the optimal strategies of a security game. An et. al [2] proposed to restrict the set of targets that attackers can feasibly attack. Jain et. al [9], Yin and Tambe [26] and Jiang et. al [10] used Bayesian Stackelberg game models to represent security games. Other approaches are presented in [5], [12], as well as implementations in the field, such as ARMOR [14], IRIS [23], [9], GUARDS [3], [15], PROTECT [3], [18], [19], [8] and, RaPtoR [24].

In our model, we consider a non-cooperative Stackelberg security games in which the realization is based on handling a Kullback-Leibler divergence random walk. The realization is given by a Markov Decision Processes (MDPs) [17]. The dynamics is as follows: at each time step the defenders and attackers observes the state of the game and choose an action. The game then randomly transitions to its next state considering the transition probability established by the current state and the action chosen. In our MDP game realization, it is assumed that the cost/utility functions and the transition probabilities are known in advance, the policies are previously computed applying the extraproximal method for solving the game, and the optimality criterion is forward-looking. We allow the leaders and followers to select the state transitions directly, so that actions correspond to fixed probability distributions on the underlying state space. For presenting a real-world solution to the problem, the control penalizes the leaders' deviation from the followers position.

This paper present the following contributions. We present a novel method for computing optimal randomized security policies in non-cooperative Stackelberg security games for multiple defenders and attackers. For solving the problem we employ the extraproximal method and its extension to Markov chains. we employ the Lagrange principle and introduce the Tikhonov regularizator method for computing and ensuring the existence of a unique Stackelberg/Nash equilibrium. We also consider a game-theory realization of the problem that involves defenders and attackers performing a discrete-time random walk over a finite state space based on the Kullback-Leibler divergence.

The remainder of the paper is organized as follows. Section II presents the Stackelberg security game model and the extrapoximal method. Section III suggest a model for random walk based on the Kullback-Leibler divergence studying two models for the security agencies one using a classical approach and the other model penalizes the agencies' deviation from the thieves' location. Some simulation results are presented in Section IV. We close, in Section V by summarizing our