13th International Conference on Applied Informatics
Eszterházy Károly Catholic University
Eger, Hungary, February 19–21, 2026

Investigating computer network security using a game theory model

Szabolcs Baják[a], **Teréz Nemes**[b]

[a]Obuda University
John von Neumann Faculty of Informatics
bajak.szabolcs@uni-obuda.hu

[b]Obuda University
John von Neumann Faculty of Informatics
nemes.terez@uni-obuda.hu

Abstract

"Our troops are fighting! The government is in place."[**1**] Today, the connections of battles with real weapons and cyberattacks are increasingly transforming the options of offensive and defensive strategies. The need for defense is imperative in the corporate sector, in state institutions and armies, and the external creation of security for private users. We know that we need a really perfect defense against future attacks on networks and other systems. We are in a continuous and permanent fight, trying to protect our systems against the already known and continuously developing new attack vectors. We use AI, we create AI-controlled honeypots, which are going to help us learn about new patterns and prepare our systems and our users to recognize and avoid known vulnerabilities and zero-day exploits, as well as social engineering attacks. Unfortunately, these options and AI support are equally available to attackers. Our goal can only be perfect protection, taking care of our data assets and our resources. There is only one prerequisite for one hundred percent protection, the ability to dispose of endless material and human resources. If we don't have endless resources, then we need a tool that can help us find the best distribution for finite resources to organize defense as effectively as possible, to optimize the use of resources and human knowledge.

A seemingly effective mathematical tool for this task is game theory, which can analyze attack situations with the models of its various games and find the best

location of resources with the help of payoff functions. In recent years, several classic game theory models were used to investigate computer network security. There is a continuous battle between system administrators and threat actors, and these models may help better understand the patterns and strategies threat actors follow to make security measures more effective against the attacks [**2**].

The Stackelberg competition is a sequential, non-cooperative game that can be used to model strategic interactions between a proactive defender and a reactive attacker. It is sometimes called a leader-follower game, where the leader moves first and then the followers move sequentially [**3**]. The foundational assumption for using Stackelberg games is that security forces (leader), who act first, commit to a randomized strategy, while the attackers (followers) choose their best response after surveillance of the leader's randomized strategy. It had been used to decribe an oligopoly market in economics, but later proved to be a significant and useful approach to compute strategies for various security forces in several areas including security at airports, transportation and other infrastructure. This motivated the use of this approach in protecting power grids, oil pipelines, subway systems, as well as computer networks [**4**], [**5**], [**6**].

However, original Stackelberg security games have some assumptions. The most important assumptions are that the participants make their decision sequentially, they do not cooperate, and all participants are subject to the same utility and cost function. Our aim is to investigate in what cases these conditions hold in computer network security. Then, we present some applications and also the challenges in applying these models. We examine how the Stackelberg game model can help in the most efficient use of the resources of an IT system, and whether it can help the defenders gain advantage.

In-text citations

[**1**], **Imre Nagy**, Words of Prime Minister Imre Nagy from his final radio address in 1956, http://1956.mti.hu/pages/Audio.aspx

[**2**], **Z. Han, D. Niyato, W. Saad, T. Başar**, Game Theory for Next Generation Wireless and Communication Networks. Cambridge University Press 2019.

[**3**] **B. An, M. Tambe**, **Stackelberg Security Games (SSG) Basics and Overview**, Improving Homeland Security Decisions, Cambridge University Press, pp. 485-507, 2017.

[**4**] **A. Wilczyński, A. Jakóbik, J. Kołodziej**, Stackelberg Security Games: Models, Applications and Computational Aspects. Journal of Telecommunications and Information Technology, 3/2016.

[**5**] **D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, M. Tambe**, Stackelberg vs. Nash in Security Games: An Extended Investigation of Interchangeability, Equivalence, and Uniqueness. Journal of Artificial Intelligence Research 41 (2011), pp. 297-327.

[**6**] **A. Sinha, F. Fang, B. An, C. Kiekintveld, M. Tambe**, Stackelberg Security Games: Looking Beyond a Decade of Success. Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, 2018.