Usage of Mathematical Models for Cybersecurity Analysis

Alexey Stefanov[1], Iliyan Ivanov[2], Ivan Trenchev[3], Radoslav Stoev[4], Miglena Trencheva[5]

South-West University "Neofit Rilski", Bulgaria [1, 2, 3, 5]
University of Library Studies and Information Technologies, Bulgaria[4]

Abstract

In the early 1990s, the word "hacker" was used to describe a very good programmer who could construct complex logic. Unfortunately, over time, the word "hacker" has acquired a negative meaning vastly due to the media. A hacker is described as someone who discovers new ways of "hacking" into a system, be it in a computer system, a programmable logic controller, someone who is able to break into banking systems, steal credit card information, and more. This is the general picture of a hacker built by the media, but it is not completely true because everything has a positive and a negative side. Network attacks are usually defined as intrusions into the network infrastructure, achieved by analyzing the network, gathering information about existing open ports or vulnerabilities and in some cases unauthorized access to resources. Computer security training is very important in today's dynamic world. In this report, we will briefly present the mathematical methods and approaches we use in teaching our students in the field of computer security. We will present several mathematical principles for network attack analysis. We will mainly use Game Theory of the Nash equilibrium. It will describe mathematical models of linear optimization and how they can predict or prevent a future attack. We will analyze penetration through random processes with discrete time. We will use examples of game theory and operations research that will be adapted to cyber attacks. Training in computer security and protection against hacker attacks is very important at the University of Library Science and Information Technology and South- west University "Neofit Rilski". In this report we will describe practical ways to implement our training and the results we achieve.

Keywords: *game theory, mathematical models*

1. Introduction

Chess is a two-person game where each player has a strategy. The purpose of chess is to put the other player in a position where their king will be captured no matter what move they make. That would be a profit for the player. Poker is also a game where players bet money based on their cards. The payout that a player receives with a winning hand is the money in the bet. The loser in the game of poker also has a payout, but in their case it is negative, that is a penalty. Players have strategies based on how good their cards are and how well they believe other players' cards are. Cards are hidden, which means that the player does not have all the information before making their bets. Further, in poker, they may not be aware of the opponent's possible choices, may they be bluffing or willing to respond to our bluff according to situations?

This is against chess where the player knows what moves the other player has made and where all his pieces are. Both chess and blackjack have common themes. Players used strategies by players and revenge. We can abstract these concepts to create the mathematical field of game theory. Game theory has been applied in many fields and is a useful way to quantify the results that may depend on the actions of multiple players or strategic agents. For example, we can model network defender and network attacker interactions as a game. Apparently there are two players, the defender and the striker. The defender has strategies for protecting the network, while the attacker has strategies for breaking the network. Paying for an attacker is digital assets (PI, data, secrets, intelligence, crypto currencies, bank account numbers, etc.) can steal a defender, on the other hand, the defender works to avoid the penalty of losing them. Game theory is also applied in economics, as it is a way to model a competitive market. In social contracts, game theory can be used to consider people's cooperation against selfish actions. It can generally be used to model competitions that are present in different areas. This chapter covers the main games that are common in game theory analysis as well as game decisions. The solutions are the strategies used by the player to provide the best result or the highest payout [1-8].

Operations research, game theory and various mathematical methods and theories are combined. This discusses new scientific perspectives of an interdisciplinary nature that relate to several fields of

research in pure and applied mathematical sciences. These contributions focus on new developments in mathematical sciences with an emphasis on the solvability of the cybersecurity problem. Modeling through game theory and operations research is a fairly common technique for cyberattack analysis. In this report we will present examples developed by prominent Russian scientists in the study of operations and game theory - Zaichenko, Krasnoproshin and Vetel. These examples will be used in the research work of the two PhD students Radoslav Stoev and Ilian Ivanov. These examples will be used for traffic analysis and network attack modeling [1-4].

2. Methodology

However, not every matrix game has a saddle.

The price of the game, equal to zero, has all symmetrical games, ie. games with half-symmetric matrices $a_{ij} = -a_{ji}, i = 1,..,m; j = 1,..,n$

In symmetrical games, the optimal strategies of the opponents coincide and the cost of the game is zero [1-4].

Really, let's x^* и y^* are the optimal mixed strategies for both players.

For each $y \in Y$ we have: $v \le E(x^*, y)$ we lay $x^* = y$ and considering that $a_{ij} = -a_{ji}$ we get $v \le E(x^*, x^*) = 0$. Similarly $v \ge E(y^*, y^*) = 0$

Therefore $v = 0$ и $x^* = y^*$.

If for a payment matrix game $A = (a_{ji})_{mxn}$, the price of the game is *V*, it is for a payment matrix game $A = (a_{ji} + w)_{mxn}, w = const$ the price of the game is $v + w$.

Really

$$E'(x,y) = \sum_{i=1}^{m}\sum_{j=1}^{n}(a_{ij}+w)x_i y_j = \sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_i y_j + w\sum_{i=1}^{m}x_i\sum_{j=1}^{n}y_j = E(x,y) + w$$

$$E'(x^*,y^*) = \max_{x\in X}\min_{y\in y}E'(x,y) = \max_{x\in X}\min_{y\in y}E(x,y) + w = E(x^*,y^*) + w = v + w$$

A random process occurring in system S is called Markovski if it satisfies the property:

For every moment of time t_0, the likelihood of any system status in the future (at $t > t_0$) it depends only on the state and at the moment (at $t > t_0$) and it does not depend on when or how she found herself in this condition.

We will only consider systems S with finite number of states S_1, S_2, ……, S_n.

The state graph (of system S) geometrically depicts the possible states of the system and the possibilities of transition from one state to another (in one step).

Example (Fig.1): S - an attacked computer that may be in one of the following states: S_1 - working, working; S_2 - defective, waiting for diagnosis; S_3 - diagnosed; S_4 - repair; S_5 - Fig. 1.

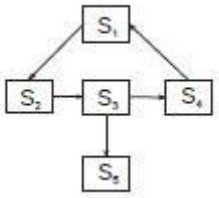

Figure.1 Attack server status graph

Discrete-Time Process: Transitions of the system from one state to another are only possible at strictly defined, pre-fixed times $t_1, t_2, \ldots$. Process with continuous. time: transitions are possible at any random time t.

3. Result

We start by looking at a simple game and then use it to build the foundations of game theory [8-10]. The game is called the prisoner's dilemma. It is a two-player game that models collaboration versus competition. There are applications in economics, politics, sociology, biology, psychology and political science, to name a few fields. Also called the game theory equivalent of an eye for an eye. The

scenario of the game is that two people, Alice and Bob, have been charged with a serious crime. Unfortunately for the police, they only have evidence of less crime [12-14]. Alice and Bob are placed in separate rooms and are given two options. They can be silent or confess If they are silent, they will only be charged with a minor violation. If one is silent while the other confesses, he is silent on being charged with a serious crime while the other is going out for free. If they both admit it, they will both be convicted of a serious crime, but the prosecutor will demand a lighter sentence. Alice has two actions in the game. She may be silent or confessing. Bob has the same two actions and the outcome of the game depends on both Bob and Alice's actions. Bob's choice may affect his outcome and may also affect Alice's. The geometric method is applicable to games in which at least one player has only 2 strategies[1, 8, 11-14].

Case 2 x 2. Let a 2 x 2 matrix game have no saddle point:

Player I	Player II	y_1	Y_2
x_1		a_{11}	a_{12}
$X_2=1- x_1$		a_{21}	a_{22}

The geometric method consists in constructing the lines y_1 and y_2 respectively on pairs of points $(0,a_{21})$, $(1, a_{11})$, and $(0,a_{22})$, $(1,a_{12})$. These two lines have the equations:

$y_1(x_1) = (a_{11} - a_{21})x_1+a_{21}$
$y_2(x_1) = (a_{12} - a_{22})x_1+a_{22}$

Clean strategies for the second player II	Expected winnings for the first player
1	$(a_{11} - a_{21})x_1+a_{21}$
2	$(a_{12} - a_{22})x_1+a_{22}$

The first player's I win is $\bar{y} = \min\{ y_1, y_2\}$ and he strives to maximize his profits $\bar{y}$.

reaches a maximum at $y_1 = y_2$ i.e. at

$$(a_{11} - a_{21})x_1 + a_{21} = (a_{12} - a_{22})x_1 + a_{22}$$

Therefore

$$x_1^* = \frac{a_{22} - a_{21}}{a_{11} + a_{22} - a_{21} - a_{12}},\ x_2^* = 1 - x_1^*$$

Dimensions y_1^* and y_2^* are determined similarly, but according to the points
$(0,a_{12})$, $(1, a_{11})$, and $(0,a_{22})$, $(1,a_{21})$.
which define the do respectively y_1 and y_I.
$y_I(y_1) = (a_{11} - a_{21})\, y_1 + a_{12}$.

Formulating a matrix game as an linear programing problem allows for a player to determine the optimal winning strategy. Let x_i be defined as a vector that consists of all probabilities that the first player follows, such that $x_i \geq 0$ and $\sum x_i = 1$. Similarly, a vector y_j can be defined as the probabilities that describe the second player's actions. Then, the expected payoff from the first player to the second can be expressed as $\sum x_i p_{ij} y_j = x^T P y$.

Noting that this is a zero-sum game, the optimal strategy for the first player to employ is to minimize the pay off $x^T P y$ to the second player [1]. Therefore, a generalized optimal strategy for the first player can be represented as the following LP[10-14]:

$$\min \sum x^T P y$$

[1] The formulation of game theory as a linear optimization problem is taken as a ready-made text from the site https://optimization.mccormick.northwestern.edu/index.php/Matrix_game_(LP_for_game_theory)

$$\text{s.t.} \sum_{i=1}^{m} x_i = 1$$

$$x > 0$$

Note that, on the other hand, the optimal strategy of the second player is to maximize the payoff from the first player (Fig. 2, Fig. 3). Given the objective of the first player, the objective of the second player can be expressed as $\max_y \min_x x^T P y$

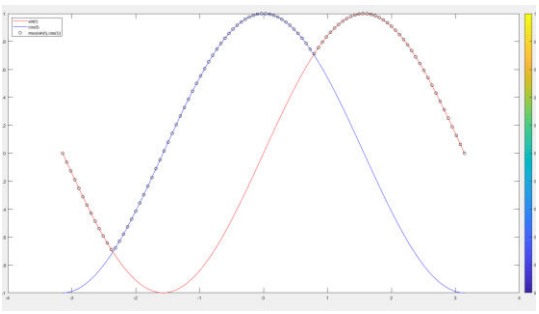

Figure. 2 Solving the fminimax function in Matlab

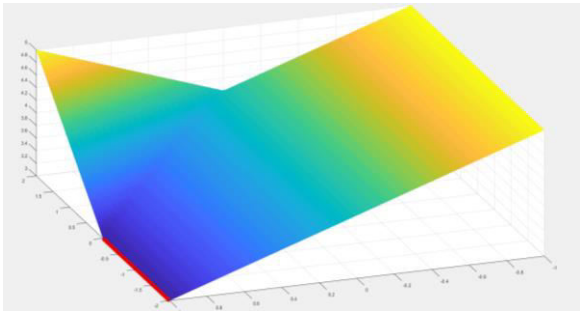

Figure. 3 Solving the fminimax function in Matlab in space

On the left are the derivatives of probabilities. On the right, there are as many members as there are arrows that associate the condition with other states. If the arrow goes out of state, the corresponding member has a “minus” sign. If the arrow enters the status, the “plus” sign is [5, 6, 8]. Each member is equal to the product of the density of transition probabilities corresponding to the given arrow multiplied by the probability of that state from which the arrow originates (Fig. 4) .

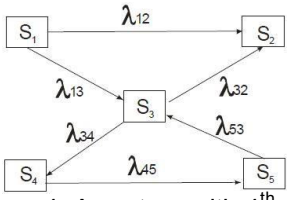

Figure. 4. A system with 4th transitions and given transition densities

Example Define p_i (t) (these are functions of time). The system S is given with five states and the corresponding densities.

$$\frac{dp_1(t)}{dt} = -(\lambda_{12} + \lambda_{13)} p_1(t)$$

$$\frac{dp_2(t)}{dt} = -\lambda_{12} p_1(t) + \lambda_{32} p_3(t)$$

$$\frac{dp_3(t)}{dt} = -(\lambda_{32} + \lambda_{34}) p_3(t) + \lambda_{13} p_1(t) + \lambda_{53} p_5(t)$$

$$\frac{dp_4(t)}{dt} = -\lambda_{45} p_1(t) + \lambda_{34} p_3(t)$$

$$\frac{dp_5(t)}{dt} = -\lambda_{53} p_1(t) + \lambda_{45} p_3(t)$$

With initial conditions at *t=0* $p_1=1$ $p_2=p_3=p_4=p_5=0$

Acknowledgments

This paper (result) is (partially) supported by the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICTinSES)", financed by the Ministry of Education and Science.

References

[1] Зайченко Ю. “Исследование операций”, Киев, 1988, Головное издательского ISBN 5-11-00226-6

[2] Краснопрошин В. В. Исследование операций: учеб. пособие / В. В. Краснопрошин, Н. А. Лепешинский. - Минск: БГУ, 2013.

[3] Миланов П. Тренчев И. “Финансова иконометрия”, 2013 ЮЗУ “Неофит Рилски”. https://www.scribd.com/document/81926934/Финансова-иконометрия

[4] Ветель Е. “Исследование операций”, Высшая школа, 2007 г. https://techlibrary.ru/b/2j1f1o1t1x1f1m2d_2m.2z._2q1s1s1m1f1e1p1c1a1o1j1f_1p1q1f1r1a1x1j1k._2p1a1e1a1y1j,_1q1r1j1o1x1j1q2c,_1n1f1t1p1e1p1m1p1d1j2g.pdf
[5] Вентцель Е. С. “Теория вероятностей (первые шаги)”.— М.: Знание, 1977
[6] Вентцель Е. С. “Элементы динамического программирования”. М.: Наука, 1964
[7] Gordon L., Loeb M., Lucyshyn M., Zhou L., “Externalities and the magnitude of cybersecurity underinvestment by private sector firms: a modification of the Gordon-Loeb model”. JInf. Secur. 6, 2015, 24–30
[8] Meza J., Campbell S., Bailey D., “Mathematical and Statistical Opportunities in Cyber Security”. Report LBNL-1667E, Lawrence Berkeley National Laboratory, 2009
[9] Panos M. Pardalos et al. “Operations Research, Engineering, and Cyber Security Trends in Applied Mathematics and Technology” . Springer Optimization and Its Applications, ISBN 978-3-319-51498-7 http://www.gametheory.net/
[10] lectures/business.p
[11] Hristov P., W Dimitrov “The blockchain as a backbone of GDPR compliant frameworks Calitatea” 20 (S1), 2017, 305IG
[12] Kovatcheva E., Dimitrov W., Koleva M., Kostadinova I., “Competency In Nuggets For Cyber Security Trainings” 11th International Conference on Education and New Learning Technologie 2019
[13] Dimitrov W, et al. ...”Toward Overcoming The Disproportion Between The Demand For Professionals And The Provision Of Training In Cybersecurity” 11th International Conference on Education and New Learning Technologies, 2017, 34-45
[14] Denchev S., Trencheva T., Planska K., “ Intellectual Property Problems on Photographic Information Analysis in University Environment”, Conference: International Conference on New Perspectives in Science Education Location: Florence, ITALY Date: MAR 21-22, 2019 PIXEL NEW PERSPECTIVES IN SCIENCE EDUCATION, 8TH EDITION, 2019, 182-186,
[15] Denchev S., Trencheva T., “Intellectual Property as a Basic Part of the University's Information Literacy”, Conference: 2nd International Conference on Education and Management Science (ICEMS) Location: Beijing, PEOPLES R CHINA Date: MAY 28-29, 2016 2ND INTERNATIONAL CONFERENCE ON EDUCATION AND MANAGEMENT SCIENCE (ICEMS 2016) , 2016, 74-78