6th International Conference on
Combinatorics, Cryptography, Computer Science and Computing
November. 17-18, 2021

Cybersecurity Games in Neutrosophic Fuzzy Environment

Hamid Bigdeli[1], Javad Tayyebi[2]
[1]Institute for the Study of War, Army Command and Staff University,
Tehran, I.R. Iran
[2]Department of Industrial Engineering, Faculty of Industrial and Computer Engineering,
Birjand University of Technology, Birjand, I.R. Iran.
Hamidbigdeli92@gmail.com; Javadtayyebi@birjandut.ac.ir

ABSTRACT

In this paper, we consider a type of security game in cyber space that called the cybersecurity game. In many of real-world applications, the information and data are vague and inaccurate. In this paper, vagueness and imprecision are modelled by fuzzy theory. The game payoffs are represented by the neutrosophic fuzzy numbers. The problem is formulated as a bi-level programming problem with fuzzy coefficients. The nearest interval approximation of neutrosophic fuzzy numbers is used to transform the problem to a bi-level programming problem with interval parameters. Using KKT conditions, the problem is rewritten into a single-level programming problem which can be solved by any solver. Finally, a numerical example is presented to consider the validity and applicability of the proposed method.

KEYWORDS: Cybersecurity, Neutrosophic fuzzy set, Game theory, Bi-level programming.

1 INTRODUCTION

The digital world has created a new threat which is called cyber warfare. Since information and communication technologies have developed to such an extent which become a major element of national power, cyber warfare has become a day problem. The critical infrastructures such as nuclear power plants, airports and oil pipelines are vulnerable under attacks. In cyber space, there are many weapons, such as upgraded viruses, trojan horses, worms, social engineering, flooding Denial-of-service (DOS), Distributed Denial-of-service (DDOS) or botnets, and advanced persistent threat (APTS).

Game theory provides a mathematical approach for deploying limited security resources to maximize their effectiveness. The connection between game theory and security has been studied for the last several decades [2,3,4]. Cybersecurity games are between a defender and an attacker. In this game defender try to detect the vulnerability. Detecting a vulnerability by the defender has two main implications on cyber weapons: 1) It makes the attacker's weapon exploiting the vulnerability ineffective and 2), he enhances the target's defence. The security games are studied by several authors [3,5]. Milind Tambe [5], in the "security game" book, reviewed the different works in this field. In this book, the applications of these games are studied in real world and the different approaches are considered to solve security game problems.

Since the payoffs of these games depend on the expert opinions, they are usually involved vagueness due to the lack of information and/or imprecision. For this purpose, the authors are considered these games with fuzzy payoffs. Studies of fuzzy games have been made by incorporating fuzzy set theory[1-4].

In this paper, we consider the cybersecurity game in which players' payoffs are expressed as fuzzy numbers and players' pure and mixed strategies are assumed to be crisp. We propose a fuzzy bi-level model for these games.

The remainder of this paper is organized as follows. In section 2, some preliminaries and definitions of fuzzy sets are presented. In Section 3, a method is proposed to solve the cyber security games with fuzzy

payoffs. In Section 4, a numerical example is presented to illustrate the mathematical approach. Conclusion is made in Section 5.

2 PRELIMINARIES

In this section, we provide some definitions and preliminaries that are required in this paper. The notations are taken from reference [4].

Definition2.1. Let X be a space of points (objects) with a generic element in X denoted by x i.e. $x \in X$. A neutrosophic set $\tilde{A}$ in X is characterized by truth-membership function $T_{\tilde{A}}$, indeterminacy-membership function $I_{\tilde{A}}$ and falsity-membership function $F_{\tilde{A}}$, where $T_{\tilde{A}}, I_{\tilde{A}}, F_{\tilde{A}}: X \to [0,1]$ that means $T_{\tilde{A}}, I_{\tilde{A}}, F_{\tilde{A}}$ are the real standard or nonstandard subset of $(0^-, 1^+)$.

Definition2.2. A single-valued neutrosophic set $\tilde{A}$ in a universe of discourse X, is given by $\tilde{A} = \{\langle x, (T_{\tilde{A}}, I_{\tilde{A}}, F_{\tilde{A}})\rangle : x \in X\}$, where $T_{\tilde{A}}, I_{\tilde{A}}, F_{\tilde{A}}: X \to [0,1]$ with the condition

$$0 \leq T_{\tilde{A}}(x) + I_{\tilde{A}}(x) + F_{\tilde{A}}(x) \leq 3, \forall x \in X$$

Definition2.3. A generalized single-valued triangular neutrosophic number $\tilde{A}$ with the set of parameters $c_1^F \leq b_1^I \leq a_1^T \leq c_2 \leq b_2 \leq a_2 \leq a_3^T \leq b_3^I \leq c_3^F$ denotes as $\tilde{A} = ((a_1^T, a_2, a_3^T; w_a), (b_1^I, b_2, b_3^I; \eta_a), (c_1^F, c_2, c_3^F; \tau_a))$ is the set of real numbers $\mathbb{R}$. The truth membership, indeterminacy membership and falsity membership functions of $\tilde{A}$ can be defined as follows:

$$T_{\tilde{A}} = \begin{cases} w_a \frac{x - a_1^T}{a_2 - a_1^T} & a_1^T < x < a_2 \\ w_a x = a_2 & \\ w_a \frac{a_3^T - x}{a_3^T - a_2} & a_2 \leq x \leq a_3^T \\ 0 & otherwise \end{cases}$$

Definition2.4. Let $\tilde{A} = ((a_1^T, a_2, a_3^T; w_a), (b_1^I, b_2, b_3^I; \eta_a), (c_1^F, c_2, c_3^F; \tau_a))$ be a generalized single-valued triangular neutrosophic number. An (α, β, γ) −cut is a crisp subset of $\mathbb{R}$ and is defined by $\tilde{A}_{\alpha,\beta,\gamma} = \{x | T_{\tilde{A}}(x) \geq \alpha, I_{\tilde{A}}(x) \leq \beta, F_{\tilde{A}}(x) \leq \gamma\} =$

$$\{[L^\alpha(\tilde{A}), R^\alpha(\tilde{A})], [L^\beta(\tilde{A}), R^\beta(\tilde{A})], [L^\gamma(\tilde{A}), R^\gamma(\tilde{A})]\}$$

$$= \left\{ \left[a_1^T + \frac{\alpha}{w_\alpha}(a_2 - a_1^T), a_3^T - \frac{\alpha}{w_\alpha}(a_3^T - a_2) \right], \left[b_1^I + \frac{\beta}{\eta_\alpha}(b_2 - b_1^I), b_3^I + \frac{\beta}{\eta_\alpha}(b_3^I - b_2) \right], \right.$$
$$\left. \left[c_1^F + \frac{\gamma}{\tau_\alpha}(c_2 - c_1^F), c_3^F + \frac{\gamma}{\tau_\alpha}(c_3^F - c_2) \right] \right\}$$

Now, we want to introduce the nearest interval approximation for neutrosophic number.

Let $\tilde{A}$ and $\tilde{B}$ be two neutrosophic numbers. The distance between them can be measured according to Euclidean metric as

$$\tilde{d}_E^2 = \frac{1}{2}\int_0^1 (T_{A_L}(\alpha) - T_{B_L}(\alpha))^2 + \frac{1}{2}\int_0^1 (T_{A_U}(\alpha) - T_{B_U}(\alpha))^2 d\alpha + \frac{1}{2}\int_0^1 (I_{A_L}(\alpha) - I_{B_L}(\alpha))^2 d\alpha$$
$$+\frac{1}{2}\int_0^1 (I_{A_U}(\alpha) - I_{B_U}(\alpha))^2 d\alpha + \frac{1}{2}\int_0^1 (F_{A_L}(\alpha) - F_{B_L}(\alpha))^2 + \frac{1}{2}\int_0^1 (F_{A_U}(\alpha) - F_{B_U}(\alpha))^2 d\alpha$$

The approximation of nearest interval of the neutrosophic number $\tilde{A}$ with respect to the metric $\tilde{d}_E$ is

$$C = \left[\int_0^1 \frac{T_{A_L}(\alpha)+I_{A_L}(\alpha)+F_{A_L}(\alpha)}{3} d\alpha, \int_0^1 \frac{T_{A_U}(\alpha)+I_{A_U}(\alpha)+F_{A_U}(\alpha)}{3} d\alpha\right]$$
$$= \left[\frac{a_1^T + b_1^I + c_1^F}{3} + \frac{a_2 - a_1^T}{6w_a} + \frac{b_2 - b_1^I}{6\eta_a} + \frac{c_2 - c_1^F}{6\tau_a}, \frac{a_3^T + b_3^I + c_3^F}{3} + \frac{a_2 - a_3^T}{6w_a} + \frac{b_3^I - b_2}{6\eta_a} + \frac{c_3^F - c_2}{6\tau_a}\right].$$

Let $a = [a^L, a^R]$ be an interval. The interval a can also be represented in the form

$$a = \langle a_c, a_w \rangle = \{x \in \mathbb{R} | a_c - a_w \leq x \leq a_c + a_w\}$$

where $a_c = \frac{1}{2}(a^R + a^L)$ and $a_w = \frac{1}{2}(a^R - a^L)$ are the center and half-width of a respectively.
Note that an interval is the better than another one if its left side and centre be the greater then the other [1].

3 CYBERSECURITY GAME IN NEUTROSOPHIC ENVIRONMENT

A cyber security game is among two players: an attacker and a defender. In these games, the defender allocates the available resources to defend against an attacker whereas the attacker can attempt to compromise targets that the defender is protecting from possible attacks. The attacker and defender are most often considered as the agents in network security problems.

Let $T = \{t_1, t_2, \ldots, t_n\}$ be a set of n targets that are at the risk of being attacked and $S = \{s_1, s_2, \ldots, s_m\}$ a set of resources to protect the targets. A vector $\langle a_t \rangle$ can represent the attacker's mixed strategy where a_t is the probability of attacking the target t. The defender's mixed strategy is the vector $\langle p_t \rangle$ where the marginal probability of protecting the target t is p_t. Players' access to mixed strategies allows them to apply probability distributions over their pure strategies. A strategy profile $\langle a, c \rangle$ is a pair of mixed strategies for the attacker and the defender, respectively. Let $\tilde{r}_d(t)$ be the defender's reward if the attacked target t is covered and $\tilde{c}_d(t)$ his cost if the target is uncovered. Similarly, the attacker's reward is denoted by $\tilde{r}_a(t)$ if the attacked target t is uncovered and by $\tilde{c}_a(t)$ the attacker's costs if the attacked target t is covered. For the strategy profile $\langle a, c \rangle$, the expected payoffs of the two players are as

$$\tilde{E}_d(a, c) = \sum_{t \in T} a_t [p_t \tilde{r}_d(t) - (1 - p_t)\tilde{c}_d(t)]$$

and

$$\tilde{E}_a(a, c) = \sum_{t \in T} a_t [(1 - p_t)\tilde{r}_a(t) - p_t \tilde{c}_a(t)],$$

where $\tilde{r}_d(t), \tilde{c}_d(t), \tilde{r}_a(t)$ and $\tilde{c}_a(t)$ are the triangular neutrosophic fuzzy numbers. As we see these payoffs depend only on the attacked targets and their protection and these payoffs do not consider the targets that are not attacked. Now if the players move simultaneously, the solution of this cyber security game is a Nash equilibrium. However, if the game is played sequentially in which the defender moves first (leader) and commits to a strategy and the attacker (follower) reacts to the defender's move, Stackelberg equilibrium appears as the standard solution in this leader-follower interaction.

This problem is formulated as a bi-level problem as follows:

$$\max \ \tilde{E}_d(a, c) = \sum_{t \in T} a_t [p_t \tilde{r}_d(t) - (1 - p_t)\tilde{c}_d(t)]$$
$$\sum_{t \in T} p_t \leq m$$

$$0 \le p_t \le 1, \forall t \in T$$

where a_t solves

$$\max \ \tilde{E}_a(a,c) = \sum_{t\in T} a_t[(1-p_t)\tilde{r}_a(t) - p_t\tilde{c}_a(t)]$$

$$\sum_{t\in T} a_t = 1$$

$$a_t \ge 0, \forall t \in T \qquad (1)$$

Using nearest interval approximation of the neutrosophic fuzzy numbers, we have

$$\max \ \left[E_d^L(a,c), E_d^R(a,c)\right]$$

$$\sum_{t\in T} p_t \le m$$

$$0 \le p_t \le 1, \forall t \in T$$

where a_t solves

$$\max \ [E_a^L(a,c), E_a^R(a,c)]$$

$$\sum_{t\in T} a_t = 1$$

$$a_t \ge 0, \forall t \in T \qquad (2)$$

Using the KKT conditions for low-level problem, the problem is transformed as follows:

$$max \ \left[E_d^L(a,c), E_d^R(a,c)\right]$$

$$\sum_{t\in T} p_t \le m$$

$$0 \le p_t \le 1, \forall t \in T$$

$$\lambda^L \frac{\partial(E_a^L(c,a))}{\partial a_t} + \lambda^R \frac{\partial(E_a^R(c,a))}{\partial a_t} - \mu_0 + \mu_t = 0, t = 1, \dots, n$$

$$\mu_t a_t = 0, t = 1, \dots, n$$

$$\sum_{t\in T} a_t = 1$$

$$a_t \ge 0, \forall t \in T$$

$$0 \le \alpha \le 1, \lambda^L \ge 0, \lambda^R \ge 0, \mu_t \ge 0, t = 1, \dots, n. \qquad (3)$$

We recall that the interval is the better in which the left side and the centre of interval is the greater [1]. So, we have the following bi-objective programming model.

$$max \left\{E_d^L(a,c), \frac{E_d^L(a,c) + E_d^R(a,c)}{2}\right\}$$

$$\sum_{t\in T} p_t \le m$$

$$0 \le p_t \le 1, \forall t \in T$$

$$\lambda^L \frac{\partial(E_a^L(c,a))}{\partial a_t} + \lambda^R \frac{\partial(E_a^R(c,a))}{\partial a_t} - \mu_0 + \mu_t = 0, t = 1, \dots, n$$

$$\mu_t a_t = 0, t = 1, \dots, n$$

$$\sum_{t\in T} a_t = 1$$

$$a_t \ge 0, \forall t \in T$$

$$\lambda^L \ge 0, \lambda^R \ge 0, \mu_t \ge 0, t = 1, \dots, n.$$

We solve this problem by the weighted sum approach. For this purpose, consider $w_1 = w_2 = \frac{1}{2}$ as the important degrees associated to the objective functions. Thus, we have

$$\max \ \frac{3E_d^L(a,c) + E_d^R(a,c)}{4}$$
$$\sum_{t\in T} p_t \le m$$
$$0 \le p_t \le 1, \forall t \in T$$
$$\lambda^L \frac{\partial(E_a^L(c,a))}{\partial a_t} + \lambda^R \frac{\partial(E_a^R(c,a))}{\partial a_t} - \mu_0 + \mu_t = 0, t = 1,\dots,n$$
$$\mu_t a_t = 0, t = 1,\dots,n$$
$$\sum_{t\in T} a_t = 1$$
$$a_t \ge 0, \forall t \in T$$
$$\lambda^L \ge 0, \lambda^R \ge 0, \mu_t \ge 0, t = 1,\dots,n. \qquad (4)$$

By solving this problem, we obtain the Pareto optimal strategies of the defender and the attacker.

4 NUMERICAL EXAMPLE

We consider a game between a defender and an attacker. In this game, there are 4 targets and two resources that defender can cover any of the two targets. For each target, there are two payoffs: the payoff of the defender and the payoff of the attacker. Each payoff consists of two parts: a reward and a cost. The defender can cover a target and get a reward if the target is attacked. He can also leave the target uncovered and incur a cost if it is attacked. The attacker can attack a target and get a reward if the target is uncovered. He can also incur a cost if the target is covered. The information of the problem presented in the following matrix.

	Defender's payoff		Attacker's payoff	
	Reward	Cost	Reward	Cost
Target1	(3,4,5; 0.3) (2.5,5,6; 0.3) (2,6,4; 0.6)	(2,3,5; 0.4) (3,4,5; 0.3) (1.5,2,4; 0.3)	(8,9,10; 0.5) (7.5,8.5,9; 0.3) (7,9,11; 0.3)	(5,6,7; 0.5) (4,6,8; 0.5) (3,5,7; 0.5)
Target2	(2,3,5; 0.4) (1.5,3,4; 0.3) (2,4,5; 0.4)	(1,2,3; 0.6) (. 5,2.5,3.5; 0.4) (1,3,4; 0.3)	(5,7,8; 0.4) (6,7,9; 0.3) (6,8,10; 0.3)	(5,6,7; 0.5) (6,7,8; 0.4) (4,6,8; 0.3)
Target3	(5,6,7; 0.4) (4,6,8; 0.3) (5,7,8; 0.4)	(2,4,6; 0.8) (1,3,5; 0.3) (3,4,6; 0.5)	(10,11,12; 0.6) (9,10,12; 0.7) (10,12,14; 0.3)	(7,8,9; 0.5) (6,8,10; 0.5) (8,8,8; 0.6)
Target4	(2,3,4; 0.3) (1,2,3; 0.8) (1,3,4; 0.5)	(1,2,4; 0.6) (2,3,5; 0.3) (1,3,5; 0.5)	(11,12,13; 0.6) (10,11,14; 0.5) (10,12,14; 0.6)	(5,6,7; 0.5) (6,7,8; 0.4) (4,6,8; 0.3)

The single-level model of this problem is as

$$\max \ 9.3a_1p_1 - 3.8a_1 + 7.3a_2p_2 - 3.2a_2 + 12.2a_3p_3 - 4.7a_3 + 6.4a_4p_4 - 3.4a_4$$
$$p_1 + p_2 + p_3 + p_4 \le 2$$
$$0 \le p_t \le 1, t = 1,2,3,4$$
$$\lambda^L(8.4 - 14.1p) + \lambda^R(11 - 19.4p) - \mu_0 + \mu_1 = 0,$$
$$\lambda^L(7.75 - 14.61p) + \lambda^R(10.81 - 19.67p) - \mu_0 + \mu_2 = 0,$$
$$\lambda^L(11.29 - 19.29p) + \lambda^R(13.98 - 23.28p) - \mu_0 + \mu_3 = 0,$$
$$\lambda^L(11.5 - 18.36p) + \lambda^R(14.94 - 23.8p) - \mu_0 + \mu_4 = 0,$$

$\mu_t a_t = 0, t = 1,2,3,4$
$a_1 + a_2 + a_3 + a_4 = 1$
$a_t \geq 0, t = 1,2,3,4$
$\lambda^L \geq 0, \lambda^R \geq 0, \mu_t \geq 0, t = 1,2,3,4.$

The optimal solution of the problem obtained by Lingo software is

$$P = (o.47,0.46,0.52,0.55),$$
$$a = (0,0,1,0).$$

5 CONCLUSION

In this paper, a cybersecurity game with payoffs of neutrosophic fuzzy numbers was considered. For solving the problem, the model was formulated as a bi-level programming problem with fuzzy coefficients. By introducing the concept of nearest interval approximation of the fuzzy neutrosophic numbers, the mentioned problem was rewritten as a bi-level programming problem with interval coefficients. The KKT optimality conditions were applied in lower level of bi-level problem. By this approach, the bi-level programming problem was transformed to a single level programming problem with interval coefficients in objective functions. Finally, the validity and applicability of the method were illustrated by a practical example.

REFERENCES

[1] H. Bigdeli, H. Hassanpour., “satisfactory strategy of multi-objective two person matrix games with fuzzy payoffs,” Iranian Journal of Fuzzy Systems, 13(4) (2016), 17-33.

[2] H. Bigdeli, H. Hassanpour. J. Tayyebi, " Constrained bimatrix games with fuzzy goals and its application in nuclear negotiations" Iranian Journal of Numerical Analysis and Optimization, 8(1) (2018), 81-110.

[3] H. Bigdeli, H. Hassanpour, J. Tayyebi, " Multiobjective security game with fuzzy payoffs " Iranian Journal of Fuzzy Systems, 2019; 16(1): 89-101. doi: 10.22111/ijfs.2019.4486.

[4] H. Bigdeli, H. Hassanpour, "Solving Defender-Attacker Game with Multiple Decision Makers Using Expected-Value Model" Caspian Journal of Mathematical Sciences (CJMS) peer, 2020; doi: 10.22080/CJMS.2020.18275.1466.

[5] M. Sarkar, T. K. Roy, Neutrosophic optmization and its application on structural designs.Brussels: Pons, 2018.

[6] A. Sokri, "Optimal resource allocation in cyber security: a game theoritic approach", The 13th international conference on future networks and communications, 2018, 283-288.

[7] M. Tambe, “ Security and Game Theory, Algorithms, Deployed Systems, Lessons Learned,” Cambridge university press, 2012.