Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

DOI: 10.37943/AITU.2021.96.94.001

B. Azibek
MSc, Teacher
balzhan.azibek@astanait.edu.kz, orcid.org/0000-0001-7389-7777
Astana IT University, Kazakhstan

S. Kusdavletov
MSc, Senior Lecturer
sanzhar.kusdavletov@astanait.edu.kz, orcid.org/0000-0003-0286-776X
Astana IT University, Kazakhstan

Aresh Dadlani
PhD, Assistant Professor
aresh.dadlani@nu.edu.kz, orcid.org/0000-0001-6841-9682
Nazarbayev University, Kazakhstan

Quoc-Viet Pham
PhD, Research Professor
vietpq@pusan.ac.kr, orcid.org/0000-0002-9485-9216
Pusan National University, South Korea

Behrouz Maham
PhD, Associate Professor
behrouz.maham@nu.edu.kz, orcid.org/0000-0002-5682-4039
Nazarbayev University, Kazakhstan

DEFENDER-ATTACKER MODELS FOR RESOURCE ALLOCATION IN INFORMATION SECURITY

Abstract. Today, information security in defender-attacker game models is getting more attention from the research community. A game-theoretic approach applied in resource allocation study requires security in information for successive defensive strategy against attackers. For the defensive side players, allocating resources effectively and appropriately is essential to maintain the winning position against the attacking side. It can be possible by making the best response to the attack, i.e., by defining the most effective secure defensive strategy. This present work develops one defender – two attackers game model to determine the defensive strategy based on the Nash equilibrium and Stackelberg leadership equilibrium solutions of one defender-one attacker game model. Both game models are designed and studied in two scenarios: simultaneous and sequential modes. Game modes are defined according to the information that is available for attackers. In the first one, the defender is not aware of the attack and makes a simultaneous decision of how many resources should be allocated. Meanwhile, in the second mode, the defender knows about the entrance of attackers into a market and is assumed to commit a better strategy. The budget constraints are studied for both modes, all calculations and proof are presented in the work. According to obtained game mathematical models, it can be highlighted that network value of customers is important through the introduction of new variables in modeling and performing game theory equilibriums. This paper underlines the importance of information availability, budget limitations, and network value of customers in resource allocation through mathematical models and proofs; and focuses on modeling and studying defender-attacker games to define defensive strategy.

DOI: 10.37943/AITU.2021.96.94.001

Keywords: Game theory, defender-attackers model, one defender-two attackers model, resource allocation, social networks, Nash equilibrium, Stackelberg leadership model, optimal resource allocation, information security

Introduction

Today, advancements in information technology brings new areas to research, and one of them is security in information. The problem in this area of game-theoretic applications in complex social networks is preventing damages and minimizing losses for defensive and attacking sides in resource allocation [8]. It might become more challenging when the defenders face different types of attackers with unpredictable strategies, and it is essential to be able to make an optimal decision considering all the constraints.

Developing the defense strategy against multiple attackers by constructing suitable game models is our main objective. In this work, we propose two models: one defender-two attackers and one defender-multiple attackers. We study the defender's behavior when there are two attackers by considering the same network value of all customers in the market. Then, we increase the number of attackers and find the best strategy for the defender to maintain its allocated resources. The study is conducted in two scenarios: when the incumbent (defender) acts simultaneously and when the incumbent predicts the attackers' attack. We believe that this study will help further studies aiming at the advancement of such models for multiple attackers. This study can help define an efficient and profitable strategy to allocate more resources in a market. The developed and proposed models can be applied in voter models, product promoting, cybersecurity as real time examples.

Preliminaries on Game Theory

Game Theory is a mathematical approach applied in many fields to study strategic and communication interactions between agents. In this thesis work, the following concepts of Game Theory were applied.

Cooperative Games

In cooperative games, decision-makers will cooperate when they agree together. Its outcome is expected to be better than the Nash or Stackelberg equilibriums. These cooperative games can be applied in this research to analyze the interaction between players in both groups of attackers and defenders.

Non-cooperative Games

In the method, players act independently, which resembles a competition between the participants. The most popular solutions of the non-cooperative games are Nash and Stackelberg leadership. In this study, the non-cooperative is used in modeling both one defender-two attackers and one defender-multiple attackers' games.

Nash Equilibrium

Each player in a game knows the strategies of the other players. The solution is chosen as the best response among strategies. This equilibrium will be used for all models for the case study to analyze players' simultaneous behavior when the defender does not know about the entrance of the attackers.

Stackelberg Equilibrium

This method allows the firm to dominate in the market to set its price first and subsequently, and the follower firms optimize their production and price. In our case, the leader is the

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

defender who dominates the market, and the followers are the attackers who want to enter the market. This method will be used to analyze the sequential behavior of players.

Related Works

The most important study in defender-attacker game modeling is Friedman [3]. This study describes five mathematical models on advertising allocation when the marketing campaign knows the contest success function. Besides this basic knowledge, we consider the roles of risk preferences [18], players [4], budget constraints [12], contest success function [14], which are essential in multiple defender-multiple attacker game models. Different strategies exist in a multi defender - attacker games. One of them aims to defend electric power systems against attacks [14]. This study proposes a defender-attacker- defender (DAD) model that considers the interactions between an attacker and a power system operator. Similarly, optimization for a microgrid defense resource planning and allocation against multi-period attacks is investigated using the defender–attacker–defender model [6]. Data injection attacks on smart grids with multiple adversaries are studied in [10]. An attack-defense game with a single attacker and multiple defenders is proposed in [1]. This proposed approach defends the system using a cooperative distributed strategy against the attacker. However, the study cannot guarantee that the attacker's budget can be higher than the defensive side's budget. The dynamic model for the defenders to mitigate the risk of power outages when a power grid is under attack is proposed in the study [20]. The dynamic model is formulated as a mixed-integer linear programming model and the game tree of a subgame perfect Nash equilibrium.

Moreover, defender-attacker models can be applied to a cloud control system (CCS). The interactions of defender and attackers in a cloud system can be modeled using a Stackelberg equilibrium in [16]. In this study, the defender needs to allocate its resources to different units serving different plants. Then, the attacker decides which units to allocate their resources to. Hence, this proposed model may define the profitable strategy only for attackers [10]. Such a game-theoretic approach can be used for robust, and privacy-preserving resource allocation in cloud computing [19]. Stackelberg game-based defense analysis against advanced persistent threats on cloud control system is studied in [16]. To defend the cloud system from APT launched by an attacker to reduce the quality of cloud service and deteriorate the system performance further, a defender needs to allocate defense resources to different units serving different plants to improve the overall system performance.

In addition, game-theoretic analysis is performed to study multiple attackers in wireless sensor networks [22], to define defense strategy using dynamic information flow tracking [9], to determine locations defense and attack dynamic Bayesian decision game [2], to defend only a single object considering time [21], to develop multiple-input multiple-output systems against smart attackers [7], to implement a memory-based multi-objective evolutionary algorithm to generate action strategies [11], to solve the multi targets case in security games [17], to model strategies for the defensive government against the terroristic attacking side [22].

One Defender - One Attacker Basic Model

The basic model was proposed by Masucci and Silva to analyze competing market campaigns between an incumbent and a challenger [8]. An incumbent is the firm that dominates the market, and a challenger enters the market. In our work, we consider these players as a defender and an attacker, respectively. As mentioned in the first chapter, one defender-one attacker model is designed by considering an intrinsic value and a network value of customers to allocate to market to the potential players. The authors performed the study in two scenarios: 1) the incumbent makes a simultaneous decision of how many resources to allocate to the customers,

DOI: 10.37943/AITU.2021.96.94.001

and 2) the incumbent knows about the challenger's attack and commits with a better strategy. The mathematical modeling of this model is given in [8].

We develop this concept by increasing the number of attackers and optimizing the defensive strategy against the attackers. Firstly, we introduce the model with two attackers, and then we present one defender-multiple attackers' model. The next section demonstrates game formulation for two and multiple attackers, the main notation, and assumptions.

Game Formulation

A one defender-multiple attackers game model is constructed on the basis of a one defender-two attackers' model. Therefore, it is essential to build a mathematical model for two attackers entering a market. We consider three main players: an incumbent (defender) and two challengers (two attackers). We consider that their budgets are positive as $D \geq 0$, $A_1 \geq 0$, and $A_2 \geq 0$. Here, we can formulate the main conditions as in Table 1. These conditions were chosen to depict and study the profit-customer relationship.

Table 1: Case Descriptions

Cases	Description of cases
Case I	When defender's budget is twice more than attackers' budget
Case II	When defender's budget is equal to attackers' budget
Case III	When defender's budget is twice less than attackers' budget
Scenario-1	When the defender does not know about the attack
Scenario-2	When the defender knows about the attack

The concept of resource allocation attacker-defender game models is illustrated in Fig. 1. Initially, there are n customers as seen in Fig. 1. Here, if n is 2, the game is modeled for two attackers. When the game starts, both defensive and attacking players start to allocate their resources and gather customers. Fig. 1 demonstrates the two formulated groups of customers in blue and red colors as the defender's and attacker's customers, respectively.

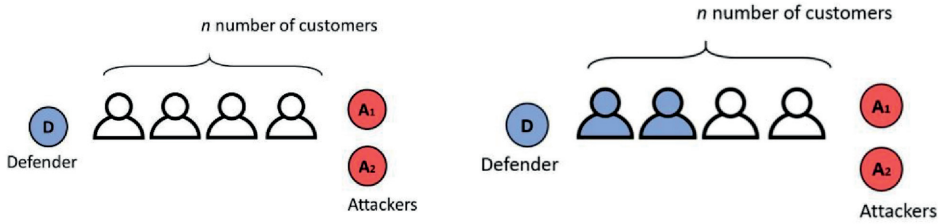

Fig. 1. The illustration model of general defender-attacker game: before and after the game

The contest success function (CSF) is in terms of the allocated $x_{i,j}$ which is the win on the customer *j* by the player *i*. The CSF includes $x_{-i,j}$ which is lost on the customer *j* by the opponent player -*i*. Similar to [8], the same assumption is made: CSF is proportional to the share of total advertising expenditure on customer. It is important to note that the same network value is assumed in the present work. Thus, considering different network values of customers and the probability that a random walk of length t that starts at j and ends up in j'. Therefore, by taking into account the same observation in [8], the following proposition related on the expected payoff for players is obtained. The next section explains the mathematical model of the game with two attackers.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

One Defender-Two Attackers Game Model

Proposition 1. For the case of one defender and two attackers, the following payoff can be obtained:

$$F_i(x_i, x_{-i}, v_i) = \sum_{j'=1}^{n} v_{i,j'} \frac{x_{i,j'}}{x_{i,j'}+x_{-i1,j'}+x_{-i2,j'}},$$

where $v_i = (v_{i,1}, v_{i,2}, .., v_{i,n})$ *is the network value of customer j' at time t. Here,* $x_{-i1,j'}$ *and* $x_{-i2,j'}$ *represent the opponents of player i.*

From the perspectives of the player *i*, there are the strategies x_{-i1} and x_{-i2}; therefore, the next step is to define the best response function to allocate the resources, which is done in the next proposition.

Proposition 2. The best response function for player i is given as:

$$x_{i,j} *= (x_{-i1,j} + x_{-i2,j}) +$$

$$+(D + A_1 + A_2)\frac{\sqrt{(v_{i,j}(x_{-i1,j}+x_{-i2,j})}}{\sum_{k=1}^{n}\sqrt{(v_{i,k}(x_{-i1,k}+x_{-i2,k})}}.$$

We can derive three best response equations for players D, A_1 and A_2 as follows:

$$x_{A1,j} = (x_{A2,j} + x_{D,j}) + (D + A_1 + A_2)\frac{\sqrt{(v_{A1,j}(x_{A2,j}+x_{D,j})}}{\sum_{k=1}^{n}\sqrt{(v_{A1,k}(x_{A2,k}+x_{D,k})}}, \quad (1)$$

$$x_{A2,j} = (x_{A1,j} + x_{D,j}) + (D + A_1 + A_2)\frac{\sqrt{(v_{A2,j}(x_{A1,j}+x_{D,j})}}{\sum_{k=1}^{n}\sqrt{(v_{A2,k}(x_{A1,k}+x_{D,k})}}, \quad (2)$$

$$x_{D,j} = (x_{A1,j} + x_{A2,j}) + (D + A_1 + A_2)\frac{\sqrt{(v_{D,j}(x_{A1,j}+x_{A2,j})}}{\sum_{k=1}^{n}\sqrt{(v_{D,k}(x_{A1,k}+x_{A2,k})}}. \quad (3)$$

Scenario-1: Nash Equilibrium

Nash equilibrium is the game strategy in which players choose the best response knowing other players' strategies [8]. Assuming the valuations of players are proportional to each other, the nest proposition can be formulated.

Proposition 3. If $v_{i,j} = \alpha v_{-i1,j} = \beta v_{-i2,j}$ *for* $\alpha, \beta > 0$*, then the Nash Equilibrium will be:*

$$x_{i,j} = B_i \frac{v_{i,j}}{V_i},$$

where the network value $V_i = \sum_{j=1}^{n} v_{i\,j}$*, and* B_i *is a total budget.*

Proof. We considered Model I in the study by about time dependent Nash equilibrium results [15], and proof is available.

In this case, the problem is to zero-sum game for three players, where each player tries to optimize the payoff function mentioned in Proposition 1. A scaling factor between the valuations of the players does not change their equilibrium strategies

Proposition 4. Assuming that $v_{A1,k} = v$ *and* $v_{A2,k} = g$ *for* $1 < k < n$ *and if there exist* $k, k' \in \{1 \dots n\}$ *such that* $v_{D,k} = v_{D,k'}$*, then*

$$x_{A1,k} + x_{D,k} = x_{A1,k'} + x_{D,k'},$$
$$x_{A2,k} + x_{D,k} = x_{A2,k'} + x_{D,k'}.$$

It is important to note that the valuations previously assumed to be proportional among three players cannot be applied every time. In real time, the valuation of the defender can be

DOI: 10.37943/AITU.2021.96.94.001

different (non-proportional) from the attacking players. In the next proposition we can see different strategies by the players.

Even in the case of two communities within the social network, where the valuations for the attacker are the same and the valuations for the defender are different for each community, the players have very different strategies than the previously considered.

Proof can be found in following equations. From (2) and (3), we can have

$$x_{A1,j} + x_{A2,j} + x_{D,j} = \gamma_{A1}\sqrt{x_{A1,j} + x_{D,j}}, \tag{4}$$

$$x_{A1,j} + x_{A2,j} + x_{D,j} = \gamma_{A2}\sqrt{x_{A2,j} + x_{D,j}}, \tag{5}$$

where

$$\gamma_{A1} = \frac{(D+A_1+A_2)}{\sum_{k=1}^{n}\sqrt{(x_{A1,k}+x_{D,k})}}, \tag{6}$$

$$\gamma_{A2} = \frac{(D+A_1+A_2)}{\sum_{k=1}^{n}\sqrt{(x_{A2,k}+x_{D,k})}} \tag{7}$$

do not depend on *j*. By rearranging (4) and (5), we can obtain

$$x_{A1,j} + x_{D,j} = k_{A1}^2 v_{D,j}(x_{A1,j} + x_{A2,j}), \tag{8}$$

$$x_{A2,j} + x_{D,j} = k_{A2}^2 v_{D,j}(x_{A1,j} + x_{A2,j}), \tag{9}$$

where

$$k_{A1}^2 = \frac{\sum_{k=1}^{n}\sqrt{(x_{A1,j}+x_{D,j})}}{\sum_{k=1}^{n}\sqrt{(v_{A1,k}(x_{A1,k}+x_{A2,k})}}, \tag{10}$$

$$k_{A2}^2 = \frac{\sum_{k=1}^{n}\sqrt{(x_{A2,j}+x_{D,j})}}{\sum_{k=1}^{n}\sqrt{(v_{A2,k}(x_{A1,k}+x_{A2,k})}} \tag{11}$$

also do not depend on *j*. Replacing (8) and (9) into (4) and (5), respectively,

$$x_{A2,j} + k_{A1}^2 v_{D,j}(x_{A1,j} + x_{A2,j}) = \gamma_{A1}\sqrt{k_{A1}^2 v_{D,j}(x_{A1,j} + x_{A2,j})}, \tag{12}$$

$$x_{A2,j} + k_{A2}^2 v_{D,j}(x_{A1,j} + x_{A2,j}) = \gamma_{A2}\sqrt{k_{A2}^2 v_{D,j}(x_{A1,j} + x_{A2,j})}. \tag{13}$$

And summing the above two equations (12) and (13),

$$\begin{gathered}(x_{A1,j} + x_{A2,j}) + (k_{A1}^2 + k_{A2}^2)v_{D,j}(x_{A1,j} + x_{A2,j}) = \\ (\gamma_{A1}k_{A1} + \gamma_{A2}k_{A2})\sqrt{v_{D,j}(x_{12,j} + x_{A2,j})}.\end{gathered} \tag{14}$$

From (14), we can obtain

$$x_{A1,j} + x_{A2,j} = \frac{(\gamma_{A1}k_{A1}+\gamma_{A2}k_{A2})^2 v_{D,j}}{(1+(k_{A1}^2+k_{A2}^2)v_{D,j})^2}. \tag{15}$$

Assuming that $k, k' \in \{1 \dots n\}$ such that $\omega = v_{D,j} = v_{D,k} = v_{D,k'}$, then

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

$$x_{A1,k} + x_{A2,k} = \frac{(\gamma_{A1}k_{A1}+\gamma_{A2}k_{A2})^2\omega}{(1+(k_{A1}^2+k_{A2}^2)\omega)^2} = x_{A1,k'} + x_{A2,k'}. \quad (16)$$

From (8) and (9), and by considering (16), we obtain:

$$x_{A1,k} + x_{D,k} = \frac{k_{A1}^2(\gamma_{A1}k_{A1}+\gamma_{A2}k_{A2})^2\omega}{(1+(k_{A1}^2+k_{A2}^2)\omega)^2} = x_{A1,k'} + x_{D,k'}, \quad (17)$$

$$x_{A2,k} + x_{D,k} = \frac{k_{A2}^2(\gamma_{A1}k_{A1}+\gamma_{A2}k_{A2})^2\omega}{(1+(k_{A1}^2+k_{A2}^2)\omega)^2} = x_{A2,k'} + x_{D,k'}. \quad (18)$$

It is important to note that the valuations previously assumed to be proportional among three players cannot be applied every time. In real time, the valuation of the defender can be different (non-proportional) from the attacking players. In the next proposition, we can see different strategies by the players.

Even in the case of two communities within the social network, where the valuations for the attacker are the same and the valuations for the defender are different for each community, the players have very different strategies than the previously considered.

Conclusion

In this work, one defender-two attackers' model was studied. Not only the intrinsic value of customers was included in mathematical modeling, but also network value was considered. The importance of the profit-customer relationship is highlighted; thus, the customer-oriented defensive strategy is identified. The present game models were analyzed for two cases: a) the defender does not know about the entrance of the attackers into a market, and b) the defender does know about the entrance of the attackers into a market. The simulation of the game model is completed for both cases considering budget constraints.

Several promising research directions can be further investigated in the future study of the dependency of the defender's decision on each attacker who wants to enter the market. We plan to consider following aspects of this study:

Stackelberg equilibrium. Along with budget constraints, the time constraint also has to be studied. In this thesis work, it is assumed that all players start the game at the same time. However, there might be cases when some attackers will decide to join the game after s time.

*Multiple attackers***.** Since the cooperative game models are expected to give better output, it is essential to investigate the possibility of the interaction of the attackers. Grouping of attackers can be also studied.

Cybersecuirty principles. We need to apply the basics of securing practices to ensure the resource allocation to be efficient and optimal. In formation security is important in defining defensive strategy.

References

1. Deng, Z., & Kong, Z. (2020). Multi-Agent Cooperative Pursuit-Defense Strategy Against One Single Attacker. *IEEE Robotics And Automation Letters*, *5*(4), 5772-5778. https://doi.org/10.1109/lra.2020.3010740
2. Fu, J., Li, Z., Sun, D., & Liu, W. (2013, November). Modeling multiple locations defence and attack dynamic Bayesian decision game. In *2013 Sixth International Conference on Business Intelligence and Financial Engineering* (pp. 449-453). IEEE.
3. Friedman, L. (1958). Game-Theory Models in the Allocation of Advertising Expenditures. *Operations Research*, *6*(5), 699-709. https://doi.org/10.1287/opre.6.5.699

4. Ab Ghani, A. T., & Tanaka, K. (2011). Network Games with Many Attackers and Defenders. *Proceedings of Research Institute for Mathematical Sciences (RIMS) Kôkyûroku Kyoto University*, *1729*, 146-151.
5. Korzhyk, D., Conitzer, V., & Parr, R. (2011, June). Security games with multiple attacker resources. In *Twenty-Second International Joint Conference on Artificial Intelligence*.
6. Lei, H., Huang, S., Liu, Y., & Zhang, T. (2019). Robust optimization for microgrid defense resource planning and allocation against multi-period attacks. *IEEE Transactions on Smart Grid*, *10*(5), 5841-5850. https://doi.org/10.1109/tsg.2019.2892201
7. Li, Y., Xiao, L., Dai, H., & Poor, H. V. (2017, May). Game theoretic study of protecting MIMO transmissions against smart attacks. In *2017 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.
8. Masucci, A. M., & Silva, A. (2015, December). Defensive resource allocation in social networks. In *2015 54th IEEE Conference on Decision and Control (CDC)* (pp. 2927-2932). IEEE.
9. Sahabandu, D., Moothedath, S., Allen, J., Clark, A., Bushnell, L., Lee, W., & Poovendran, R. (2019, December). Dynamic information flow tracking games for simultaneous detection of multiple attackers. In *2019 IEEE 58th Conference on Decision and Control (CDC)* (pp. 567-574). IEEE.
10. Sanjab, A., & Saad, W. (2016). Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective. *IEEE Transactions on Smart Grid*, *7*(4), 2038-2049. https://doi.org/10.1109/tsg.2016.2550218
11. Vejandla, P., Dasgupta, D., Kaushal, A., & Nino, F. (2010, August). Evolving gaming strategies for attacker-defender in a simulated network environment. In *2010 IEEE Second International Conference on Social Computing* (pp. 889-896). IEEE.
12. Wang, C., Hou, Y., & Ten, C. W. (2016). Determination of Nash equilibrium based on plausible attack-defense dynamics. *IEEE Transactions on Power Systems*, *32*(5), 3670-3680. https://doi.org/10.1109/tpwrs.2016.2635156
13. Xiang, Y., & Wang, L. (2018). An improved defender–attacker–defender model for transmission line defense considering offensive resource uncertainties. *IEEE Transactions on Smart Grid*, *10*(3), 2534-2546. https://doi.org/10.1109/tsg.2018.2803783
14. Xu, Z., & Zhuang, J. (2019). A study on a sequential one-defender-N-attacker game. *Risk Analysis*, *39*(6), 1414-1432. https://doi.org/10.1111/risa.13257
15. Ye, M., & Hu, G. (2015). Distributed seeking of time-varying Nash equilibrium for non-cooperative games. *IEEE Transactions on Automatic Control*, *60*(11), 3000-3005. https://doi.org/10.1109/tac.2015.2414817.
16. Yuan, H., Xia, Y., Zhang, J., Yang, H., & Mahmoud, M. S. (2019). Stackelberg-game-based defense analysis against advanced persistent threats on cloud control system. *IEEE Transactions on Industrial Informatics*, *16*(3), 1571-1580. https://doi.org/10.1109/tii.2019.2925035
17. Zhang, J., & Zhuang, J. (2019). Modeling a multi-target attacker-defender game with multiple attack types. *Reliability Engineering & System Safety*, *185*, 465-475. https://doi.org/10.1016/j.ress.2019.01.015
18. Zhang, J., Zhuang, J., & Jose, V. (2018). The role of risk preferences in a multi-target defender-attacker resource allocation game. *Reliability Engineering & System Safety*, *169*, 95-104. https://doi.org/10.1016/j.ress.2017.08.002
19. Zhang, L., & Li, J. (2018). Enabling robust and privacy-preserving resource allocation in fog computing. *IEEE Access*, *6*, 50384-50393. https://doi.org/10.1109/access.2018.2868920
20. Zhang, X., Hipel, K. W., Ge, B., & Tan, Y. (2019). A game-theoretic model for resource allocation with deception and defense efforts. *Systems Engineering*, *22*(3), 282-291. https://doi.org/10.1002/sys.21479
21. Zhang, X., Li, X., & Yuan, Z. (2019, October). Defending a single object in a defender-attacker game considering time. In *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)* (pp. 506-510). IEEE.
22. Zhu, Q., Bushnell, L., & Başar, T. (2012, December). Game-theoretic analysis of node capture and cloning attack with multiple attackers in wireless sensor networks. In *2012 IEEE 51st IEEE Conference on Decision and Control (CDC)* (pp. 3404-3411). IEEE.