Nash Equilibrium Analysis of Attack and Defense Strategies in the Air Transportation Network

Renaud Horacio Gaffan, Issa Moussa Diop, Ndeye Khady Aidara, Cherif Diallo, Hocine Cherifi

FRCCS

Nash Equilibrium Analysis of Attack and Defense Strategies in the Air Transportation Network

Renaud Horacio Gaffan[1], Issa Moussa Diop[2✓], Ndeye Khady Aidara[1], Cherif Diallo[1] and Hocine Cherifi[3]

[1] *LACCA, Gaston Berger University, Saint-Louis, Senegal ; renaudgaffan@gmail.com,aidara.ndeye-khady@ugb.edu.sn, cherif.diallo@ugb.edu.sn*
[2] *I3S, Cote d'Azur University, Nice, France ; issa-moussa.diop@univ-cotedazur.fr*
3 *ICB Lab, UMR 6303 CNRS, University of Burgundy, Dijon, France; hocine.cherifi@u-bourgogne.fr*
✓ *Presenting author*

Abstract. This study explores the strategic dynamics within interconnected systems by integrating game theory with complex networks. It presents a static zero-sum game model to analyze attack and defense strategies in such networks. Investigating three strategies for attackers and defenders—random, degree centrality, and betweenness centrality—the study examines Nash equilibrium under equal resource assumptions. Analyzing the payoff matrix and players' responses identifies the dominant strategy as combining random attacks and betweenness-based defenses.

Keywords. *Game theory; Complex networks; Attacker-defender game; Attack and defense strategies; Nash equilibrium*

1 Introduction

The emergence of attack-defense games provides a strategic perspective for evaluating complex network security. Previous studies have explored these games extensively, focusing on achieving Nash Equilibrium, where players employ optimal strategies. For example, one study introduced a zero-sum game model to understand network robustness during attacker-defender confrontations[8]. Other studies proposed a game model considering network topology and system performance, analyzing interactions with limited budgets and targeted strategies [6][7]. This study extends this research by introducing novel defense strategies based on alternative centrality measures [11, 12, 13]. It shows that prioritizing nodes with high betweenness centrality offers an effective defense strategy against random attacks.

The game model assumes the presence of an attacker and a defender. It is a one-shot game, meaning players make their decisions simultaneously without knowing each other's choices. The model is based on two assumptions. The first is decision-maker rationality, which implies that players decide based on their interests and seek to maximize their payoffs. The second is their knowledge of each other's strategies, which means that players have perfect knowledge of the network and other players' strategies.

For the **attacker**, V^A is the set of attacked nodes, with $V^A \subseteq V$. θ_A is the attack range

parameter, with $\theta_A = \frac{|V^A|}{N}$. X is an attack strategy, with $X \in S^A = [x_1, x_2, ..., x_N]$, where S^A is the set of attack strategies. x_i is a binary variable for each node in the network. $x_i = 1$ if the corresponding node v_i is selected as the target of an attack ($v_i \in V^A$) and $x_i = 0$ otherwise. We obtain $\theta_A = \frac{1}{N}\sum_{i=1}^{N} x_i$. N is the number of nodes of the graph.

For the **defender**, one replaces A by D and X par Y. For example, Y is an defense strategy, with $Y \in S^D = [y_1, y_2, ..., y_N]$.

The payoff is defined as the reduction in network performance caused by the attack. In the attacker-defender game, it is important to note that both players move simultaneously without knowing each other's decisions. A node v_i is removed when attacked and not defended ($x_i = 1$ and $y_i = 0$). The removed nodes are denoted $\hat{V}$, where $\hat{V} \subseteq V$. The network after removing vulnerable nodes is denoted $\hat{G}$, with $\hat{G} = (V - \hat{V}, \hat{E})$, and we have $\hat{V} = V^A - V^A \cap V^D$. The performance measure function $\Gamma(G)$ is used in the study to evaluate network performance under different attack and defense strategies. It is defined as the size of the largest connected component of the network G after removing attacked but undefended nodes. The attacker's payoff is defined as follows:

$$U^A(X, Y) = \frac{\Gamma(G) - \Gamma(\hat{G})}{\Gamma(G)} \in [0, 1] \tag{1}$$

$\Gamma(G)$ is the network's performance before the attack, and $\Gamma(\hat{G})$ is the network's performance after the attack. The sum of the attacker's and defender's payoffs is always equal to zero, as the game is a zero-sum game. $U^D(X, Y)$ represents the defender's payoff.

$$U^A(X, Y) + U^D(X, Y) = 0 \tag{2}$$

2 Experimental Results

We examine the air transport network described in [2]. We assume that both players have an equal capacity to attack and defend nodes ($\theta_A = \theta_D$). Therefore, if both players choose the same targeted strategy, all attacked nodes are defended, resulting in zero payoffs. The strategies for attack and defense can either be random or targeted. Targeted strategies are centrality-based, with nodes prioritized in descending centrality order.

Figure 1 (left) depicts the attacker's payoffs as a function of the attack (defense) scope parameter, θ, when different profiles of targeted strategies compete. Neither player has a dominant strategy, so only one mixed-strategy Nash equilibrium exists. When $\theta \leq 0.5$, the gain of the Betweenness attack against the Degree defense is greater than that of the Degree attack against the Betweenness defense. Thus, attack and defense strategies based on the Betweenness are better than those based on Degree. On the other hand, when $\theta > 0.5$, the gain of the Betweenness attack against the Degree defense is equal to that of the attack-based Degree against the Betweenness defense. This means that attack and defense strategies based on the Betweenness give equivalent gain to Degree attack. In other words, when the proportion of airports to be attacked is high, the hubs are similar in the two strategies. However, with a limited budget for nodes and given the centrality anomaly [4] in the global air transport network, the hubs resulting from the two strategies differ. In addition, nodes with a very high Betweenness tend to connect distinct groups of nodes. Thus, neglecting to protect these critical nodes could potentially compromise the integrity of the network's giant component.

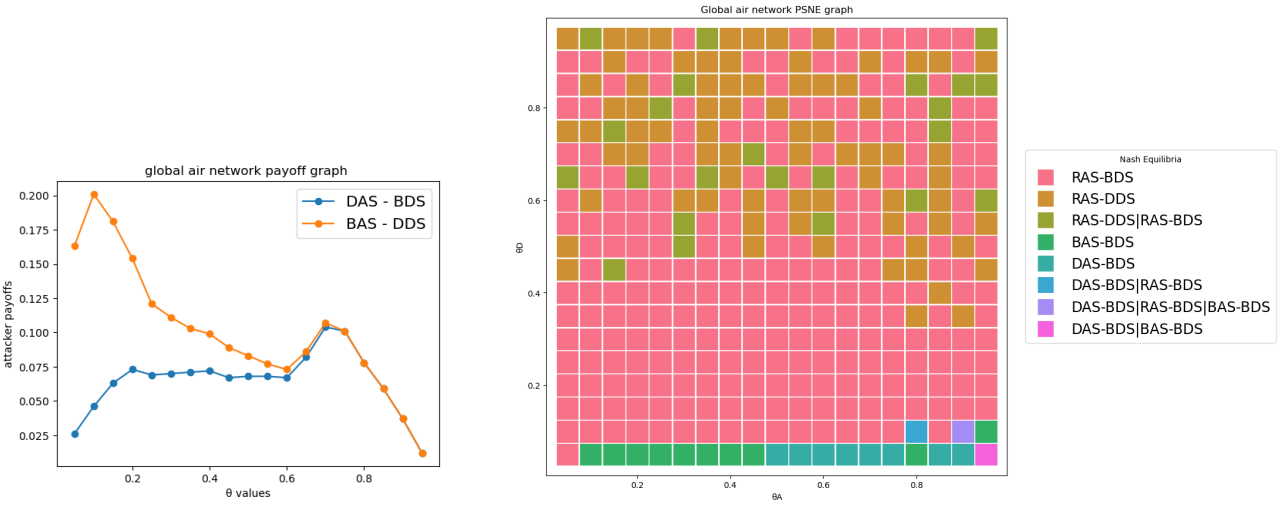

Figure 1: Left): The payoffs of the attacker as a function of the attack (defense) range parameter θ when Degree and Betweenness strategies clash in the global air network. On the x-axis, we represent the values of the attack (defense) range parameter θ, and on the y-axis the attacker's payoffs. DAS means Degree Attack Strategy, and BDS means Betweenness Defense Strategy. Right): Graph of pure strategy Nash equilibrium in the global airport network. On the x-axis, we represent attack resources θ_A, and on the y-axis, defense resources θ_D. Each tile represents an equilibrium strategy. The legend on the right shows the different game balances and the corresponding colors. RAS and RDS mean, respectively, Random Attack Strategy and Random Defense Strategy.

When analyzing conflicts between the random and targeted strategies (Degree or Betweenness). The attacker gains as a function of the attack (defense) range parameter θ when different targeted strategy profiles confront the random strategy in the global air network shows that the Degree or Betweenness attack against the random defense strategy gives a better gain than the random attack strategy against the random defense strategy which itself provides a better gain than the random attack strategy against the Degree or the Betweenness defense. So there is a Nash equilibrium in pure strategy (random attack, Degree defense) or (random attack,Betweenness defense).

In the following, we consider the game's three typical strategies. Figures 1 (right), show the pure strategy Nash equilibrium of the game in the different networks when attack resource θ_A and defense resource θ_D are different. In real-world attack scenarios, attack and defense resources are unlikely to be equal. The primary Nash equilibrium occurs when the attacker employs a random attack strategy while the defender safeguards nodes with high betweenness. Following this equilibrium, the subsequent dominant Nash equilibrium emerges when the attacker selects airports arbitrarily, and the defender prioritizes the protection of airports with high degrees. In more detail, whether $\theta_A \geq 0.1$ and $\theta_D = 0.05$, the attacker chooses the attack-based Betweenness, and the defender also chooses the defense Strategy Based on Betweenness. On the other hand, when $\theta_A \geq 0.5$, and $\theta_D = 0.05$, the attacker chooses the Degree-based attack, and the defender maintains the nodes with the high Betweenness. There are also situations where we can have several Nash equilibria in pure strategy. Indeed, when $\theta_A > \theta_D$, the defender chooses the airports with high Betweenness and the attacker chooses the nodes randomly. When $\theta_A < \theta_D$, the defender chooses the defense-based Degree or the defense-based Betweenness, and the attacker chooses the random attack strategy.

3 Conclusion

This work analyzes attack and defense strategies in complex networks where attackers and defenders have equal resources. It shows that targeted attacks focusing on betweenness centrality are more effective than those with degree centrality, primarily when targeting only a few nodes. The analysis identifies critical strategies for both attackers and defenders, highlighting how differences in their available resources affect their equilibrium strategies. Future research will evaluate additional strategies based on different centrality measures [1, 5, 10]and networks[9, 3, 9]. Furthermore, we plan examining Nash equilibrium in mixed strategies.

References

[1] Debayan Chakraborty, Anurag Singh, and Hocine Cherifi. Immunization strategies based on the overlapping nodes in networks with community structure. In *Computational Social Networks: 5th International Conference, CSoNet 2016, Ho Chi Minh City, Vietnam, August 2-4, 2016, Proceedings 5*, pages 62–73. Springer International Publishing, 2016.

[2] Issa Moussa Diop, Chantal Cherifi, Cherif Diallo, and Hocine Cherifi. Revealing the component structure of the world air transportation network. *Applied Network Science*, 6:1–50, 2021.

[3] Zakariya Ghalmane, Chantal Cherifi, Hocine Cherifi, and Mohammed El Hassouni. Extracting backbones in weighted modular complex networks. *Scientific Reports*, 10(1):15539, 2020.

[4] Roger Guimera, Stefano Mossa, Adrian Turtschi, and LA Nunes Amaral. The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles. *PNAS*, 102(22):7794–7799, 2005.

[5] Manish Kumar, Anurag Singh, and Hocine Cherifi. An efficient immunization strategy using overlapping nodes and its neighborhoods. In *Companion Proceedings of the The Web Conference 2018*, pages 1269–1275, 2018.

[6] Ya-Peng Li, Suo-Yi Tan, Ye Deng, and Jun Wu. Attacker-defender game from a network science perspective. *Chaos*, 28(5), 2018.

[7] Yapeng Li, Ye Deng, Yu Xiao, and Jun Wu. Attack and defense strategies in complex networks based on game theory. *Journal of Systems Science and Complexity*, 32(6):1630–1640, 2019.

[8] Yapeng Li and Jun Wu. Modeling confrontations in complex networks based on game theory. In *2018 Int. Conf. on Computer Science, Electronics and Communication Engineering (CSECE 2018)*, pages 109–112. Atlantis Press, 2018.

[9] Khubaib Ahmed Qureshi, Rauf Ahmed Shams Malick, Muhammad Sabih, and Hocine Cherifi. Deception detection on social media: A source-based perspective. *Knowledge-Based Systems*, 256:109649, 2022.

[10] Stephany Rajeh and Hocine Cherifi. Ranking influential nodes in complex networks with community structure. *Plos one*, 17(8):e0273610, 2022.

[11] Stephany Rajeh, Marinette Savonnet, Eric Leclercq, and Hocine Cherifi. Interplay between hierarchy and centrality in complex networks. *IEEE Access*, 8:129717–129742, 2020.

[12] Stephany Rajeh, Marinette Savonnet, Eric Leclercq, and Hocine Cherifi. Characterizing the interactions between classical and community-aware centrality measures in complex networks. *Scientific reports*, 11(1):10088, 2021.

[13] Stephany Rajeh, Marinette Savonnet, Eric Leclercq, and Hocine Cherifi. Comparative evaluation of community-aware centrality measures. *Quality & Quantity*, 57(2), 2023.