Adapting to the Unseen: Enhancing Cybersecurity through Dynamic Adaptive Game Theory ⋆

Baoguanyan Kang[1]

Duke Kunshan University, Kunshan, Jiangsu 215316, China
`your email`
LinkedIn

Abstract. Amidst the ever-evolving landscape of cybersecurity threats, traditional game theory's static models falter in accurately simulating the dynamic strategic interactions between defenders and attackers. This paper argues, as supported by Camerer (2003)[1], that conventional approaches inadequately capture the complexities of real-time adaptation and information asymmetry inherent in cybersecurity conflicts. To address this shortfall, we propose a Dynamic Adaptive Game Theoretic (DAGT) model that encapsulates the continuous strategic evolution of cybersecurity agents. Our DAGT model allows defenders to iteratively refine their security postures in response to changing attack methodologies, while attackers concurrently adapt their tactics to navigate defensive barriers and remain undetected. By leveraging the principles of evolutionary game theory and algorithmic behavioral analysis, the DAGT model exhibits enhanced predictive power and strategic depth. Through a series of simulated interactions, we demonstrate that the DAGT approach significantly fortifies defense mechanisms and improves resilience against cyber threats. This study extends beyond theoretical advancements, presenting a pragmatic framework for developing more responsive and adaptive cybersecurity strategies in contrast to the limitations of traditional static models.

Notes: In submission to Problem Set 2 for COMPSCI/ECON 206 Computational Microeconomics, 2024 Spring Term (Seven Week - Fourth) instructed by Prof. Luyao Zhang at Duke Kunshan University.

Keywords: computational economics · game theory · innovative education · DAGT

⋆ **Acknowledgments**: when writing acknowledgments for a research paper, start by expressing sincere gratitude to your instructor and supervisor for their guidance. Then, extend thanks to your colleagues for their support, and to your classmates for their engaging discussions and input. Conclude with a personal note of appreciation for friends and family who offered encouragement throughout your research endeavor. This sequence ensures that gratitude is shown to both professional and personal supporters who have contributed to your academic journey.

1 Introduction

Based on Camerer (2003)[1], traditional game theory often fails to capture the dynamic and evolving nature of strategic interactions, particularly in scenarios with incomplete information and heterogeneous agents, limiting its applicability in real-world contexts. In a sentence, static models of game theory struggle to represent the complexity of dynamic environments, leading to suboptimal strategies and inaccurate predictions in scenarios such as cybersecurity conflicts

If we design a game about a cybersecurity scenario where defenders and attackers engage in an ongoing battle. Traditional game theory approaches cannot effectively model the continuous adaptation of strategies by both parties and the asymmetrical information prevalent in cybersecurity, resulting in inadequate defense mechanisms and increased vulnerability to cyber threats. To show my way's efficiency, in the cybersecurity example, DAGT allows defenders to adapt their defense strategies in response to evolving attack patterns, while attackers can dynamically adjust tactics to exploit vulnerabilities and evade detection. This real-time adaptation and strategic evolution lead to more robust defense mechanisms and increased resilience against cyber threats compared to traditional static game theory approaches.

[luyao] **New: provide in formal academic paper writing the research description that extends the Q&A research interview on the GitHub.**

2 Background

Traditionally, game theory has been constrained by its focus on rational human agents within well-defined game environments. However, with the advancement of AI and the potential emergence of General Artificial Intelligence (GAI), the landscape of strategic interactions is evolving. According to Bostrom (2014)[2], here's a reimagined framework: 1. Expanded Agents Spectrum: Rather than solely focusing on rational human agents, the framework should encompass a broader spectrum of agents, including AI agents ranging from simple algorithms to advanced GAI systems. This expanded spectrum acknowledges the diversity of decision-making entities in complex systems. 2. Dynamic Game Environment: Move beyond static game environments to dynamic and adaptive settings. With the integration of AI, game environments can evolve in real time based on the actions and interactions of agents, leading to more realistic and complex scenarios. 3. Learning and Adaptation: Incorporate mechanisms for learning and adaptation within the framework. AI agents can learn from past interactions, predict opponents' behaviors, and adapt their strategies, accordingly, leading to the emergence of more sophisticated and

strategic decision-making. It can also help recognize the interconnectedness of various systems and how they influence strategic interactions, which should build complex systems integration. Game theory should integrate insights from complexity science to analyze emergent behaviors, feedback loops, and non-linear dynamics within complex socio-technical systems. 4. Ethical Considerations: Address ethical implications arising from the interaction between AI and human agents. Ensuring fairness, transparency, and accountability in AI decision-making processes is crucial to foster trust and stability in strategic interactions.

3 An Illustration Example

We can think a scenario about online financial transactions.Imagine a scenario where online financial transactions are targeted by a sophisticated cyber-attack. Traditional static game theory might model this scenario with fixed strategies for both attackers and defenders. The defenders' strategy might be a standard set of security protocols that are updated only periodically based on past data.In the cybersecurity landscape, traditional static game theory approaches often fall short in effectively countering cyber threats due to their inability to adapt to evolving scenarios. Without the use of Dynamic Adaptive Game Theory (DAGT), defenders are forced to rely on static security measures. This rigidity allows attackers to exploit vulnerabilities that remain unpatched due to the delayed response inherent in static systems. The consequence is often a successful attack, leading to significant financial losses and diminished trust among users, ultimately impacting human welfare adversely.

Conversely, the implementation of DAGT transforms the security paradigm by enabling defenders to continuously analyze transaction data through AI-driven anomaly detection systems. This proactive approach allows for the immediate adaptation to new attack patterns, with defense mechanisms dynamically adjusting to evolving threats. As a result, attackers find it increasingly challenging to exploit vulnerabilities, since the defense evolves more swiftly than the attackers can adjust their strategies. The outcome of employing DAGT is a notable decrease in successful attacks, safeguarding financial assets and bolstering user trust and safety, thereby enhancing overall human welfare.

A The Pioneers in the History of Game Theory

According to John Nash (1951)[3], the elevator talks' limitations are primarily focusing on pure strategies, but failing to capture the nuanced decision-making scenarios where players adopt mixed strategies

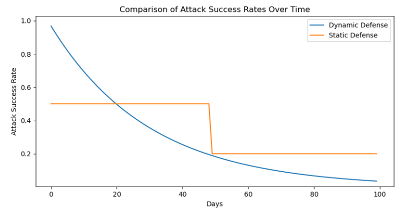

Fig. 1. Comparison of two models

to maximize their payoffs. For example, consider a scenario where two players play a game of matching pennies. Previous frameworks considered only pure strategy and did not adequately simulate the strategic complexity observed when players randomly choose heads or tails to outwit their opponents. In other words, just as Harsanyi mentioned, people usually miss some important variables, such as the economy, and politics. In my opinion, we can use mixed-strategy Nash equilibrium, which provides a more nuanced understanding of strategic interactions by acknowledging the strategic variability inherent in the decision-making process. As a result, if we put this new strategy in the previous example, it reveals strategic patterns that players randomly select to achieve equilibrium, providing a more accurate description of real-world strategic decision dynamics than previous pure strategy frameworks.

B Review Classic Games, Nash Equilibrium and the Analytical Tools

- provide the definition, theorem, and proof from the two textbooks (source must be cited) on **Bayesian (Subgame Perfect)** Nash Equilibrium
- you must utilize the headings of subsection, subsubsection, and paragraph to structure the section
- you must use the definition, theorem, and proof environment
- you must provide basic discussions to compare the definition, theorem, and proof

B.1 Exploring Inspirational Games in Strategic or Normal Form

This Game of Coordination is a model that captures the essence of strategic decision-making where the primary goal is to align actions with another player. Economists and psychologists are also interested in strategic settings where opportunities for communication and reciprocity are limited perhaps due to the large number of people involved. (Goeree, 2002)[4] The Game of Coordination fascinates me

because it simplifies the complex dynamics of mutual expectations and conventions into a clear, analyzable format. It highlights the importance of implicit communication and common understanding in achieving optimal outcomes. This game teaches that sometimes the best strategy is not about competing but aligning with others. This game is showcased in strategic or normal form as follows:

1.Two players choose between two options, say A and B.

2.The payoff matrix is typically structured to reward coordination and penalize misalignment.

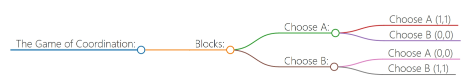

Fig. 2. Game cordination

B.2 Delving into Extensive-Form Games

The Ultimatum Game is an extensive-form game where two players decide how to divide a sum of money. Player 1 proposes how to split the sum, and Player 2 can either accept or reject this proposal. If Player 2 accepts, the money is split according to the proposal; if Player 2 rejects, both players get nothing. Game Structure: Stage 1: Player 1 offers to split a fixed sum, say 100, into two portions. Stage 2: Player 2 decides to accept or reject the offer. Acceptance means both players receive the proposed shares. Rejection means both receive nothing.

This game is intriguing because it often yields results that contradict the predictions of traditional economic theory. Rational choice theory would predict that Player 2 should accept any non-zero offer, as receiving a small amount of money is preferable to receiving nothing. However, experimental results frequently show that unfair offers are often rejected, indicating that players are willing to forgo monetary gains to punish what they perceive as unfair behavior by Player 1.

B.3 Critiquing Nash Equilibrium and Envisioning Innovations:

The concept of Nash Equilibrium is a fundamental tool in game theory, providing a prediction of outcomes in strategic interactions where no player can benefit by unilaterally changing their strategy.

The core problem is each side is unwilling to adjust its strategy given by the other. Static nature, which is traditional Nash Equilibrium analysis typically focuses on static games where players make decisions simultaneously or are fully aware of the game's structure.

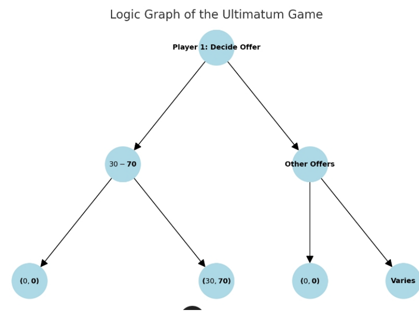

Fig. 3. Ultimatum game

This doesn't always capture the dynamic nature of decision-making that occurs in sequential games or those with evolving strategies over time. On the other hand, another important problem is that if our conditions are not enough, or not very accurate to let the model make the decision, the result will be inaccuracy.

For the new tool, I recommend DSGA. It is the work addresses the problem of efficient online exploration and mapping using multi-robot teams via a new distributed algorithm for multi-robot exploration, distributed sequential greedy assignment (DSGA), which is based on sequential greedy assignment (SGA). While SGA permits bounds on suboptimality, robots must execute planning steps sequentially. Rather than plan for each robot sequentially as in SGA, DSGA assigns plans to subsets of robots using a fixed number of sequential planning rounds. (McIntyre, 2019)[5]

[luyao] **more hints**

B.4 A Subsection Sample

Please note that the first paragraph of a section or subsection is not indented. The first paragraph that follows a table, figure, equation etc. does not need an indent, either.

Subsequent paragraphs, however, are indented.

Sample Heading (Third Level) Only two levels of headings should be numbered. Lower level headings remain unnumbered; they are formatted as run-in headings.

Sample Heading (Fourth Level) The contribution should contain no more than four levels of headings. Table **??** gives a summary of all heading levels.

Definitions and Theorems from Multiagent Systems

Game Theory Definitions

Definition 1 (Perfect-information Game). *A perfect-information game in extensive form is defined as a tuple $G = (N, A, H, Z, \chi, \rho, \sigma, u)$, where:*

- *N denotes the collection of players involved in the game.*
- *A signifies the universal set of possible actions available in the game.*
- *H is the set comprising all decision points that are not final.*
- *Z encapsulates all terminal points in the game, distinct from H.*
- *χ is the action mapping function that allocates a subset of actions to each decision point.*
- *ρ is the player mapping function that attributes each decision point in H to a specific player in N.*
- *σ is the successor function that assigns a subsequent decision or terminal point following a player's action.*
- *u represents the utility function for each player, mapping terminal points to real values.*

Definition 2 (Imperfect-information Game). *An imperfect-information game in extensive form can be articulated as a tuple $G = (N, A, H, Z, \chi, \rho, \sigma, u, I)$, expanding upon the perfect-information game structure, where $I = (I_1, \ldots, I_n)$ designates the information partitioning for player i, consolidating nodes at which player i cannot distinguish the game's progression due to incomplete information.*

Definition 3 (Subgame Perfect Nash Equilibrium). *A Subgame Perfect Nash Equilibrium in a game G is comprised of strategy profiles s that sustain Nash Equilibrium across every conceivable subgame G' of G. Here, s', a strategy limited to G', must secure a Nash Equilibrium in G'. It is understood that the entire game G can be viewed as a subgame of itself, thus endorsing the notion that every SPNE corresponds to a Nash Equilibrium.*

Discussion

These definitions and the theorem illustrate the complexities of modeling strategic interactions in both perfect and imperfect information settings. The addition of information partitions in the definition of imperfect-information games introduces an extra layer of strategic depth, necessary for analyzing real-world scenarios where players' knowledge about the game state is often incomplete.

Table 1. Glossary of Basic Game Theory Terms

Term	**Definition**	**Reference**
Nash Equilibrium	A set of strategies, one for each player, such that no player has anything to gain by changing only their own strategy.	nash1951[3]
Dominant Strategy	A strategy that results in the highest payoff for a player, no matter what the other players do.	gibbons1992[6]
Pareto Efficiency	An allocation of resources from which it is impossible to reallocate so as to make any one individual better off without making at least one individual worse off.	pareto1896[7]
Zero-sum Game	A situation in which one person's gain is equivalent to another's loss, so the net change in wealth or benefit is zero.	von Neumann1928[8]
Minimax Strategy	In zero-sum games, a strategy that minimizes the maximum loss that a player can suffer.	von Neumann1944[9]

Bibliography

[1] C. Camerer, "Behavioral game theory: Experiments in strategic interaction," 2003.

[2] N. Bostrom, *Superintelligence: Paths, Dangers, Strategies.* Oxford University Press, 2014.

[3] J. Nash, "Non-cooperative games," *Annals of Mathematics*, vol. 54, pp. 286–295, 1951.

[4] J. K. Goeree and C. A. Holt, "Stochastic game theory: For playing games, not just for doing theory," *Proceedings of the National Academy of Sciences*, vol. 96, pp. 10 564–10 567, 2002.

[5] H. D. McIntyre, P. Catalano, C. Zhang, G. Desoye, E. R. Mathiesen, and P. Damm, "Gestational diabetes mellitus," *Nature reviews Disease primers*, vol. 5, no. 1, p. 47, 2019.

[6] R. Gibbons, *A Primer in Game Theory.* Harvester Wheatsheaf, 1992.

[7] V. Pareto, *Cours d'Économie Politique.* Lausanne: Rouge, 1896.

[8] J. von Neumann, "Zur theorie der gesellschaftsspiele," *Mathematische Annalen*, vol. 100, pp. 295–320, 1928.

[9] J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior.* Princeton: Princeton University Press, 1944.