# Game-On: Game Theory Strategies to Mitigate On-Off Attacks in Fog Computing

Rasagna V
*Dept. of CSIS*
*BITS Pilani, Hyderabad Campus, India*
p20200019@hyderabad.bits-pilani.ac.in

G. Geethakumari
*Dept. of CSIS*
*BITS Pilani, Hyderabad Campus , India*
geetha@hyderabad.bits-pilani.ac.in

***Abstract*—In the rapidly evolving digital landscape, the integration of fog computing introduces unique cybersecurity challenges, particularly with regard to on-off attacks characterized by intermittent bursts of malicious activity. These attacks pose significant risks to organizations utilizing distributed computing architectures, as traditional static defense mechanisms often prove inadequate in such dynamic environments. This paper presents a novel game-theoretic model designed specifically for mitigating on-off attacks in fog computing contexts. By framing the cybersecurity scenario as a non-cooperative game, we analyze the strategic interactions between attackers and defenders across distributed nodes. The model incorporates various defender strategies, including low, medium, and high defense levels, along with attacker strategies of initiating attacks or remaining passive. Through extensive simulations, we evaluate the effectiveness of these strategies and their respective impacts on the players' payoffs. Our findings reveal that adaptive defensive strategies significantly improve the defender's success while reducing the attacker's effectiveness. Notably, the high-defense strategy consistently yields superior outcomes for defenders in fog environments, demonstrating its efficacy against aggressive on-off attack patterns. These results highlight the importance of employing game theory to develop dynamic defense mechanisms in fog computing, providing critical insights for organizations aiming to bolster their cybersecurity posture against evolving threats.**

***Index Terms*—Fog Computing, On-Off Attack, Game Theory**

## I. Introduction

In the digital age, cybersecurity has become a paramount concern for individuals and organizations, especially as the adoption of fog computing architectures increases. This distributed computing paradigm offers enhanced performance and reduced latency but also introduces unique security vulnerabilities, as highlighted by Stojmenovic and Wen's exploration of challenges specific to fog and edge environments [1]. Among the myriad of cyber threats, on-off attacks pose a significant challenge in fog environments due to their dynamic and adaptive nature. These attacks are characterized by intermittent bursts of malicious activity, where attackers exploit vulnerabilities during concentrated periods before retreating to evade detection [2], [3]. The unpredictability of on-off attacks complicates traditional defense mechanisms, necessitating more sophisticated approaches to safeguard distributed systems.

Despite advancements in cybersecurity technologies, many organizations struggle to effectively mitigate on-off attacks within fog environments. Conventional methods often rely on static defense mechanisms that lack the adaptability needed to respond to evolving threats [4], [5]. These static solutions are typically insufficient in dynamic environments like fog computing, where adaptive and resilient security mechanisms are required, as shown in recent studies on adaptive defense [6]. This limitation highlights the necessity for innovative strategies that can anticipate and counteract the intentions of attackers while considering the distributed nature of fog computing.

Game theory, a mathematical framework for analyzing strategic interactions among rational decision-makers, offers valuable insights for addressing these cybersecurity challenges [7], [8]. This approach has shown potential in modeling the adversarial interactions typical of cyber threats, allowing stakeholders to predict adversary strategies and enhance resilience in distributed architectures [9]. By modeling the interactions between attackers and defenders in a fog computing context as a game, stakeholders can better understand the potential outcomes of different strategies. This approach not only facilitates the development of more effective defensive measures but also enhances the ability to predict and adapt to an adversary's behavior.

This paper aims to explore the application of game theory in mitigating on-off attacks within fog environments. By formulating a game-theoretic model that captures the strategic dynamics between attackers and defenders, we seek to identify optimal defense strategies that can effectively disrupt the patterns of on-off attacks. Through extensive simulations, we will analyze the performance of these strategies and provide insights into their practical implications for cybersecurity practices in fog computing environments.

The rest of the paper is organized as follows: Section II summarizes the related work, Section III details the proposed approach. In IV details the effectiveness of the proposed approach and show cases the experimental results and finally, we conclude our work and briefly summarize the gaps and future work for this research in Section V.

## II. Related Work

Game theory has emerged as a potent tool for addressing security challenges in distributed systems, including fog computing and wireless sensor networks. This section discusses several key studies that have applied game-theoretic concepts to enhance network security and mitigate potential threats.

The foundational concepts of game theory as applied to network security trace back to the collaboration between Morgenstern and von Neumann [10], who pioneered the mathematical formulation of strategic interactions. Their work laid the groundwork for subsequent research by providing a formal framework for analyzing conflicts in competitive environments. However, the application of classical game theory models to modern network security faces challenges due to the assumptions of complete information and rational behavior. In many security scenarios, adversaries may act unpredictably or have incomplete knowledge of the system, limiting the applicability of traditional models.

Sun et al [7] propose a security mechanism based on evolutionary game theory tailored to fog computing environments. The authors argue that fog computing, characterized by its decentralized nature, presents unique security challenges that require adaptive strategies. The evolutionary game model they introduce is dynamic and capable of adjusting to the changing behavior of attackers and defenders. However, while the proposed mechanism shows promise in maintaining system stability under fluctuating attack strategies, it assumes rational behavior from adversaries, which may not always hold true in practical scenarios. Furthermore, the work lacks a detailed analysis of the computational overhead involved in implementing the proposed game-theoretic strategies in real-world fog networks, which might limit its practical applicability.

Abdalzaher et al [11] provide a comprehensive survey of how game theory has been employed to address security requirements and mitigate threats in wireless sensor networks (WSNs). The survey categorizes existing game-theoretic solutions, focusing on defense mechanisms against various types of attacks, such as denial of service and eavesdropping. While the survey is thorough and covers a broad spectrum of security applications, it does not delve into how these solutions can be extended to more complex environments like fog computing, where similar threats exist but with increased complexity due to the distributed nature of fog nodes. Additionally, the authors primarily highlight theoretical models without sufficient emphasis on practical case studies or performance evaluations of the surveyed strategies.

Manshaei et al [9] explore the intersection of game theory, network security, and privacy, providing a detailed survey of game-theoretic approaches in these domains. They categorize existing models based on the type of security threats, such as jamming and intrusion, and the game-theoretic techniques employed, including zero-sum, cooperative, and evolutionary games. The survey is notable for its focus on privacy aspects, a crucial factor often overlooked in other studies. Nonetheless, the work heavily relies on theoretical formulations, with limited discussion on how these models perform in dynamic, real-world scenarios. The study also does not sufficiently address how these game-theoretic frameworks can be adapted to emerging technologies, such as fog computing, that require more nuanced strategies due to their heterogeneity and scalability concerns.

In summary, while the existing literature provides a solid foundation for applying game-theoretic approaches to network security, there remain gaps in practical applicability, particularly concerning adaptive and scalable solutions in environments like fog computing. The current literature often lacks practical case studies or real-world applications that demonstrate how game-theoretic models can be implemented effectively in operational environments. There is a pressing need for empirical studies that validate these theoretical approaches and showcase their effectiveness in mitigating actual cyber threats.

## III. Proposed Game Theoretic Framework for On-Off Attack Mitigation

This section details our proposed approach for mitigating on-off attacks using a game-theoretic framework. We aim to model the strategic interactions between attackers and defenders, facilitating the identification of optimal defensive strategies.

### A. Game Model Development

We define a non-cooperative game involving two players: the defender (D) and the attacker (A). Each player has a finite set of strategies. The strategies are formalized as follows:

- **Defender Strategies** ($S_D$):
  - $s_{D1}$: Continuous monitoring and anomaly detection.
  - $s_{D2}$: Dynamic resource allocation based on current threat levels.
  - $s_{D3}$: Deployment of deception techniques (e.g., honeypots).
- **Attacker Strategies** ($S_A$):
  - $s_{A1}$: Execute on-off attacks with a defined frequency.
  - $s_{A2}$: Modify attack patterns based on the defender's observed actions.

### B. Payoff Structure

To model the payoffs, we define the payoff functions for both players:

$$U_D(s_D, s_A) = \alpha \cdot R_D(s_D, s_A) - \beta \cdot C_D(s_D) \tag{1}$$

$$U_A(s_D, s_A) = \gamma \cdot R_A(s_D, s_A) - \delta \cdot C_A(s_A) \tag{2}$$

Where: - $U_D(s_D, s_A)$ and $U_A(s_D, s_A)$ are the payoffs for the defender and attacker, respectively. - $R_D(s_D, s_A)$ is the reward for the defender based on their strategy $s_D$ against the attacker's strategy $s_A$. - $C_D(s_D)$ and $C_A(s_A)$ represent the costs incurred by the defender and attacker for their respective strategies. - $\alpha$, $\beta$, $\gamma$, and $\delta$ are constants representing the weight of rewards and costs.

### C. Reward and Cost Functions

The reward and cost functions can be defined as follows:

1. Defender Reward Function:

$$R_D(s_D, s_A) = \begin{cases} 1 & \text{if attack is detected} \\ 0 & \text{if attack is not detected} \end{cases}$$

2. Defender Cost Function:

$$C_D(s_D) = c_m \cdot M + c_r \cdot R$$

Where: - $c_m$ is the cost per monitoring action. - $M$ is the number of monitoring actions. - $c_r$ is the cost per resource allocated. - $R$ is the total resources allocated.

3. Attacker Reward Function:

$$R_A(s_D, s_A) = \begin{cases} 1 & \text{if attack is successful} \\ 0 & \text{if attack fails} \end{cases}$$

4. Attacker Cost Function:

$$C_A(s_A) = c_a \cdot A$$

Where: - $c_a$ is the cost per attack action. - $A$ is the number of attacks executed.

### D. Equilibrium Analysis

To determine the optimal strategies, we will analyze the game for Nash equilibria, where neither player can improve their payoff by unilaterally changing their strategy. The conditions for Nash equilibrium can be formulated as follows:

$$U_D(s_D^*, s_A^*) \geq U_D(s_D, s_A^*) \quad \forall s_D \in S_D \tag{3}$$

$$U_A(s_D^*, s_A^*) \geq U_A(s_D^*, s_A) \quad \forall s_A \in S_A \tag{4}$$

Where $s_D^*$ and $s_A^*$ are the equilibrium strategies for the defender and attacker, respectively.

### E. Simulation Design

To validate our model, we will conduct simulations that replicate various scenarios of on-off attacks. The simulation framework will consider the following parameters:

- Attack frequency ($f$): The average number of attacks per time unit. - Detection rate ($d$): The probability that the defender successfully detects an attack. - Resource allocation ($R$): The amount of resources allocated by the defender to various strategies.

The simulations will allow us to evaluate the effectiveness of different strategies under varying conditions, such as changes in attack patterns and resource constraints.

In summary, our proposed approach combines game theory with a detailed analysis of on-off attacks, providing a robust framework for developing effective defense mechanisms against these evolving threats.

**Algorithm 1** Algorithm for Game-On

**Initialize Parameters**
- Set the number of rounds ($N$)
- Define probabilities:
  - Attack success probability ($P_{\text{success}}$)
  - Defender detection rate ($P_{\text{detection}}$)
- Define defender and attacker strategies:
  - Defender strategies: Low Defense ($S_{D0}$), Medium Defense ($S_{D1}$), High Defense ($S_{D2}$)
  - Attacker strategies: Attack ($S_{A0}$), No Attack ($S_{A1}$)

**Initialize Payoff Matrices**
- Create payoff matrix for the defender ($U_D$)
- Create payoff matrix for the attacker ($U_A$)

**Simulation Loop**
**for** each round from 1 to $N$ **do**
    Randomly select defender strategy ($s_D$) from $\{S_{D0}, S_{D1}, S_{D2}\}$
    Randomly select attacker strategy ($s_A$) from $\{S_{A0}, S_{A1}\}$
    **Evaluate outcomes based on selected strategies:**
    **if** $s_A = S_{A0}$ (Attack) **then**
        Generate a random number to determine success:
        **if** random ¡ $P_{\text{success}}$ **then**
            Attack succeeds
            Calculate defender payoff: $U_D(s_D, S_{A0})$
            Calculate attacker payoff: $U_A(S_{A0}, s_D)$
        **else**
            Attack fails
            Calculate defender payoff: $U_D(s_D, S_{A1})$
            Calculate attacker payoff: $U_A(S_{A1}, s_D)$
        **end if**
    **else**
        No Attack
        Defender payoff: $U_D(s_D, S_{A1}) = 0$
        Attacker payoff: $U_A(S_{A1}, s_D) = 0$
    **end if**
**end for**
**Calculate Average Payoffs**
Output average payoffs for defender and attacker.

## IV. Experimental Results

To assess the effectiveness of the proposed game-theoretic model in mitigating on-off attacks, we performed a set of simulations across 100 rounds. The primary objective of these simulations was to evaluate the average performance scores for both the defender and the attacker, considering various strategic interactions and decision-making behaviors throughout the process.

### A. Simulation Setup

The simulation consisted of two key participants: the defender and the attacker. Each player had a set of strategies to choose from, allowing them to make strategic decisions

throughout the simulation. Specifically, the defender had access to three distinct strategies, while the attacker could select from two available strategies. These strategies represent different approaches each player could take in response to the actions of the other, providing a foundation for analyzing their interactions.

To accurately model and evaluate the dynamics of this game, a series of parameters were defined, which influenced the outcomes of the simulation. These parameters were carefully selected to reflect realistic conditions and potential scenarios that the defender and attacker might encounter in a practical environment. By adjusting these parameters, the simulation aimed to explore various strategic outcomes under different circumstances, allowing for a comprehensive analysis of the model's effectiveness in mitigating on-off attacks. The parameters used for the simulation are as follows:

- Number of rounds: 100
- Probability of attack success: 0.5
- Defender detection rate: 0.6
- Total resources allocated by the defender: 100

The defender's strategies included:

- Low Defense (Strategy 0)
- Medium Defense (Strategy 1)
- High Defense (Strategy 2)

The attacker's strategies were:

- Attack (Strategy 0)
- No Attack (Strategy 1)

### B. Results Overview

The average scores for both players across the simulation rounds are summarized in Table I. The **High Defense** strategy yielded the lowest total attacker score (110) and the lowest average attacker score (3.793103). This indicates that high defense is effective in mitigating attacks, as it consistently results in fewer successful attacker actions.

| Defender Strategy | Total Attacker Score | Average Attacker Score |
|---|---|---|
| Low Defense | 270 | 6.428571 |
| Medium Defense | 170 | 5.862069 |
| High Defense | 110 | 3.793103 |

TABLE I
SUMMARY OF ATTACKER SCORES AGAINST DEFENDER STRATEGIES

The **Medium Defense** strategy also performs reasonably well, with a total attacker score of 170 and an average of 5.862069, but it is less effective than the High Defense strategy.

The **Low Defense** strategy, in contrast, has the highest total attacker score (270) and the highest average score (6.428571). This highlights its vulnerability, as attackers can exploit this strategy more easily.

### C. Comparison of Average Scores

The average attacker score serves as a crucial metric for evaluating the effectiveness of each defense strategy, as it directly reflects how well each approach thwarts attack attempts. A lower average attacker score indicates a stronger defense, underscoring the strategy's success in reducing the overall impact and success rate of attacks. Observations from the average scores reveal that more robust defense strategies, such as High Defense, substantially decrease the success rate of attackers, demonstrating a clear advantage over weaker strategies. However, the diminishing returns observed as defense levels increase from Low to High suggest that while stronger defenses continue to improve security, the rate of improvement may lessen at higher levels. This trend highlights the balance that must be achieved between the cost of implementing stronger defenses and the relative gains in security effectiveness. Figure 1 illustrates the average attacker scores for each defense level: Low, Medium, and High using a bar chart that visually compares the effectiveness of each strategy. A notably lower score for attackers under the High Defense strategy indicates its relative superiority in minimizing attack success rates. This visual comparison helps underscore the impact of progressively stronger defense measures, with the High Defense strategy emerging as the most effective at mitigating attacks and safeguarding the system.

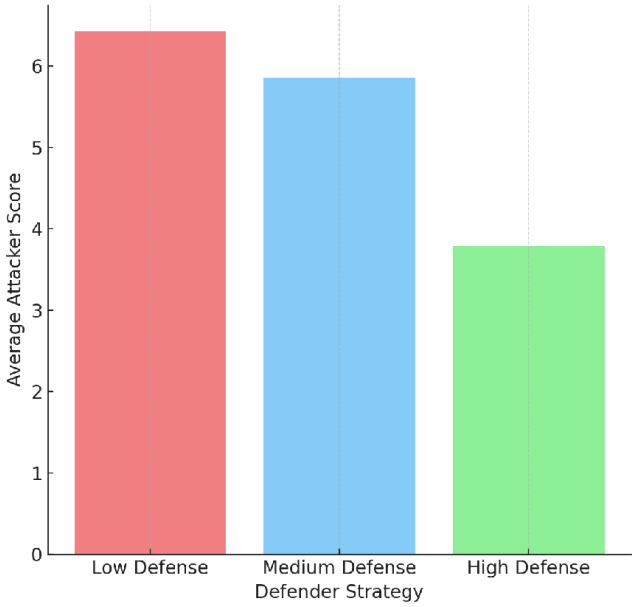


Fig. 1. Average Attacker Scores by Defender Strategy

### D. Further Considerations

Although the simulation provides a snapshot of the effectiveness of static defense strategies, it is essential to acknowledge that, in real-world scenarios, attackers continuously adapt. Attackers often analyze the defenses they encounter, adjusting their tactics to exploit identified weaknesses. Future studies should consider the impact of adaptive defense strategies that can evolve based on observed attack patterns, allowing organizations to remain resilient against these dynamic threats. Additionally, examining variations in attack success probabilities will provide insights into how defenders can tailor their strategies based on the likelihood of different attacks occurring. It is also crucial to explore the introduction

of multiple attacker strategies, as attackers may collaborate or coordinate efforts, making it imperative for defenders to develop comprehensive approaches that can effectively counter a range of tactics in a real-time environment. Ultimately, embracing adaptability in defense mechanisms will enhance cybersecurity effectiveness in increasingly complex digital landscapes.

To thoroughly assess the effectiveness of various defender strategies against on-off attacks, we ran simulations over an extensive 1000-round series. This approach aimed to capture performance trends and provide a comprehensive view of how each strategy operates under prolonged attack conditions. The results are represented in a range of plots, with Figure 2 illustrating the fluctuations in attacker scores across simulation rounds for each defense level. In this figure, the Y-axis represents attacker scores, ranging from 0 to 10, while the X-axis denotes the number of rounds, extended here to 300 rounds to observe long-term trends. The plot reveals that, despite variations in defense strategies, the majority of lines hover near the maximum score of 10, suggesting that attackers maintain a high success rate even when faced with supposedly robust defense mechanisms. By continuously refining defense models, organizations can create a proactive security environment that not only mitigates current threats but also anticipates future attack vectors. This forward-looking approach is essential in building resilience, ensuring that defenses are not only reactive but also preemptively strengthened against emerging tactics.

This persistent trend towards high attacker success raises questions about the real-world applicability of the tested defense strategies, particularly concerning the High Defense strategy, which theoretically should lower attacker scores more substantially. The line chart demonstrates that, across all defender strategies, attacker performance remains both high and relatively stable, indicating that the model may lack sufficient adaptability or complexity to disrupt attacker success significantly. This consistent success rate suggests that the defense strategies, as modeled, may not fully capture the nuanced, adaptive responses that would be required to mitigate on-off attacks in dynamic environments. As such, these results underscore the need for model enhancements, such as incorporating adaptive defense mechanisms or response delays, to more accurately simulate and counteract the dynamics of real-world cybersecurity threats. Future studies might focus on integrating these elements to develop a more resilient defense model capable of reducing attacker success over time. This would help ensure that the model reflects the complexity and adaptability required to defend against modern, persistent, and evolving cyber threats.

## V. Conclusion

The experimental results underscore the effectiveness of employing game-theoretic models in developing adaptive defense strategies against on-off attacks. Through simulation, it is evident that implementing higher levels of defensive strategies yields significant advantages for defenders, resulting in improved outcomes and a marked reduction in attacker success. This adaptive approach demonstrates the potential for real-time adjustments to threat landscapes, highlighting how game theory can dynamically assess and respond to varied attack patterns. These findings provide valuable insights for organizations seeking to enhance their cybersecurity posture through strategic, data-informed defense planning. By integrating such models, organizations can anticipate potential attack vectors and adjust their defensive mechanisms proactively, reducing the likelihood of successful breaches and establishing a robust, resilient cybersecurity framework that can adapt to the complexities of modern threats.

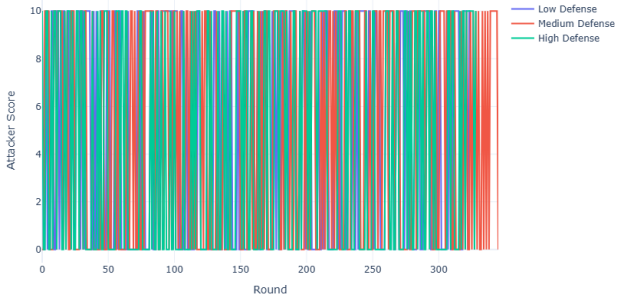


Fig. 2. Attacker Scores Over Rounds for Different Defender Strategies

## References


[1] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *2014 federated conference on computer science and information systems*. IEEE, 2014, pp. 1–8.

[2] A. A.-N. Patwary, A. Fu, R. K. Naha, S. K. Battula, S. Garg, M. A. K. Patwary, and E. Aghasian, "Authentication, access control, privacy, threats and trust management towards securing fog computing environments: A review," *arXiv preprint arXiv:2003.00395*, 2020.

[3] M. Mukherjee, L. Shu, and D. Wang, "Survey of fog computing: Fundamental, network applications, and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1826–1857, 2018.

[4] J. Al Muhtadi, R. A. Alamri, F. A. Khan, and K. Saleem, "Subjective logic-based trust model for fog computing," *Computer Communications*, vol. 178, pp. 221–233, 2021.

[5] J. Caminha, A. Perkusich, and M. Perkusich, "A smart trust management method to detect on-off attacks in the internet of things," *Security and Communication Networks*, vol. 2018, no. 1, p. 6063456, 2018.

[6] X. Qin, F. Jiang, M. Cen, and R. Doss, "Hybrid cyber defense strategies using honey-x: A survey," *Computer Networks*, vol. 230, p. 109776, 2023.

[7] Y. Sun, F. Lin, and N. Zhang, "A security mechanism based on evolutionary game in fog computing," *Saudi journal of biological sciences*, vol. 25, no. 2, pp. 237–241, 2018.

[8] C. T. Do, N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou, and S. S. Iyengar, "Game theory for cyber security and privacy," *ACM Computing Surveys (CSUR)*, vol. 50, no. 2, pp. 1–37, 2017.

[9] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys (CSUR)*, vol. 45, no. 3, pp. 1–39, 2013.

[10] O. Morgenstern, "The collaboration between oskar morgenstern and john von neumann on the theory of games," *Journal of Economic Literature*, vol. 14, no. 3, pp. 805–816, 1976.

[11] M. S. Abdalzaher, K. Seddik, M. Elsabrouty, O. Muta, H. Furukawa, and A. Abdel-Rahman, "Game theory meets wireless sensor networks security requirements and threats mitigation: A survey," *Sensors*, vol. 16, no. 7, p. 1003, 2016.