Land Forces Academy Review
Vol. XXX, No. 4(120), 2025

DEFENSIVE DECEPTION IN NETWORK SECURITY – CONCEPTS AND GAME – THEORETIC APPROACHES

Răzvan FLOREA
"Gheorghe Asachi" Technical University of Iași, Romania
razvan.florea@student.tuiasi.ro

Mitică CRAUS
"Gheorghe Asachi" Technical University of Iași, Romania
mitica.craus@academic.tuiasi.ro

ABSTRACT

Defensive Deception is an advanced strategy in network security that aims to mislead, confuse, or delay cyber adversaries by introducing uncertainty and manipulating attacker perceptions. Unlike traditional defense mechanisms that focus on detection and prevention, deceptive techniques – such as honeypots, honeytokens, moving target defense, and decoy systems – proactively shape attacker behavior and create a more complex threat landscape. A critical aspect of modern defensive deception is the integration of game-theoretic models, which provide a rigorous mathematical framework for analyzing interactions between attackers and defenders. These models help in designing optimal deception strategies by anticipating adversary actions and balancing the trade-offs between risk, cost, and information gain. By leveraging deception and strategic reasoning, defenders can increase the attacker's cognitive and operational burden, shift the asymmetry in cyber conflict, and significantly enhance the resilience of network systems.

KEYWORDS: Defensive Deception, security, Game Theory

1. Introduction

Defensive Deception (DD) is a strategic practice in which a defender deliberately misleads an adversary to influence their perception and, consequently, their decision-making. Traditionally rooted in military doctrine, deception has long been used to obscure true intentions, capabilities, and strategies, with the ultimate aim of manipulating enemy behavior in favor of the deceiver's objectives. In such settings, deception enables a defender to proactively influence the adversary to act in a way that aligns with the defender's goals – either by provoking undesired behavior or deterring certain actions (Jajodia, 2017).

In recent years, this concept has gained significant relevance in the digital realm, evolving into what is now known as cyber deception. Almeshekah and Spafford (2014) define cyber deception as "*premeditated actions aimed at misleading or confusing attackers, prompting them to act (or refrain from acting) in ways beneficial to computer security defenses*" (Almeshekah & Spafford, 2016). Cyber deception encompasses a broad range of techniques including honeypots, fake data, moving target defenses, and decoy systems – all designed to mislead attackers and create strategic uncertainty in cyberspace.

While deception is a multidisciplinary concept, spanning fields such as psychology,

DOI: 10.2478/raft-2025-0063

military science, and computer security (Jafarian & Niakanlahiji, 2020), its underlying principle remains consistent: to induce an adversary to adopt a false perception and behave in a way that benefits the deceiver. According to Rowe and Rrushi (2016), the essence of deception lies in manipulation – either compelling the adversary to act in a desired manner or preventing them from executing harmful actions.

In this study, we focus specifically on defensive deception, where the defender uses deception to counteract a rational attacker and safeguard their assets. Understanding how to implement deception effectively requires a rigorous framework to model the interaction between the defender and the attacker. In this context, Game Theory provides a powerful tool set for analyzing strategic decision-making under conditions of conflict and uncertainty.

Game-theoretic models are particularly well-suited to capturing the adversarial dynamics of deception, as they allow for formal reasoning about the incentives, payoffs, and informational asymmetries that shape attacker and defender behavior. They facilitate the identification of equilibrium strategies, enabling defenders to design deceptive tactics that are not only effective but also rational under varying threat models and resource constraints.

The objective of this work is to explore the strategic application of defensive deception through a game-theoretic lens, developing a systematic understanding of how deception can be modeled, evaluated, and optimized in adversarial environments. Unlike conventional security mechanisms that rely heavily on detection and mitigation, deception introduces an active layer of defense that exploits the attacker's reasoning process. This paper contributes into the formalization of defensive deception strategies, with potential implications for both cybersecurity and broader security domains.

2. Literature Review

Defensive Deception has emerged as a proactive and strategic approach in cybersecurity and adversarial defense, offering an alternative to conventional reactive mechanisms. It operates by deliberately misleading adversaries, manipulating their perception of a system or environment, and guiding their behavior in ways that benefit the defender. As digital threats grow in complexity, the academic literature has increasingly emphasized both the potential and limitations of DD, as well as its relation to similar defense strategies such as Moving Target Defense (MTD) and obfuscation.

2.1. Principal Advantages of Defensive Deception

One of the core benefits of DD lies in its cost-effectiveness. Many deception-based techniques – such as honey files and honey tokens – are lightweight and inexpensive to deploy, yet highly effective in misleading attackers. Compared to more resource-intensive defenses like advanced access control systems or sophisticated intrusion detection, DD strategies often strike an efficient balance between deployment cost and security performance.

DD also functions well as a complementary defense, rather than a standalone solution (Ward, Perring, Ray, Farley & Lopez, 2018). It enhances traditional security infrastructures by adding layers of misdirection and uncertainty. For instance, honeypots can act as both surveillance tools and decoys, diverting attacks away from critical systems while collecting valuable intelligence about attacker behavior (Florea & Craus, 2022a).

Another strength is DD's versatility across system layers. Deception techniques can be implemented at the network, application, data, or system levels. This adaptability allows for flexible integration within diverse environments, supporting both legacy and modern infrastructures. In doing so, DD promotes a multi-layered defense strategy

that improves both system resilience and adaptability (Ward et al., 2018).

Moreover, DD has proven effective in countering automated threats. Techniques such as session obfuscation, code concealment, or dynamic response mechanisms hinder the effectiveness of bots and automated exploits, which often rely on predictable system behaviors or static configurations.

2.2. Challenges and Limitations of Defensive Deception

Despite these advantages, DD presents several challenges. One of the main issues is understanding attacker intent. Without accurate insight into an adversary's goals, motivations, or decision-making processes, it can be difficult to determine which deceptive strategies are appropriate or likely to succeed. This uncertainty complicates risk assessment and defensive planning.

Another limitation is the potential for operational confusion. Deception methods – such as honeypots, fake credentials, or bogus file systems – must be carefully designed to avoid interfering with legitimate users or administrators (Florea & Craus, 2022a). Also, Florea and Craus (2022a) provided evidence that poorly implemented deception can lead to increased false positives or misinterpretations by system operators.

Maintenance and upkeep also represent ongoing concerns. For DD to remain effective, deceptive systems must be consistently updated and refined. If neglected, adversaries may detect and circumvent these tactics. While some automation is possible – such as in the case of software obfuscation – many deception techniques require continuous oversight and reconfiguration.

Finally, the rising sophistication of attackers demands more advanced deception systems. For example, high-interaction honeypots, which convincingly replicate real systems, are more difficult for attackers to identify. However, these setups also come with increased operational cost and complexity, potentially outweighing the benefits in some environments.

2.3. Defensive Deception in Relation to Moving Target Defense and Obfuscation

Defensive deception shares significant conceptual overlap with Moving Target Defense and obfuscation, although each has distinct characteristics as seen in Figure no. 1. Like DD, MTD aims to create uncertainty for the attacker by changing system configurations, such as rotating IP addresses or randomizing network structures. However, MTD does not typically use false information. Instead, it focuses on altering real system properties to limit an attacker's ability to plan and execute an attack.

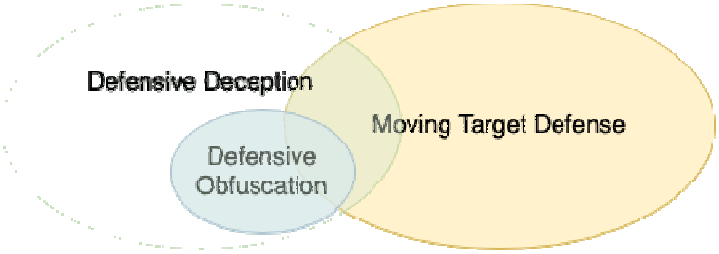

Figure no. 1: *Defensive Deception, Moving Target Defense, and Defensive Obfuscation*
(Source: Authors' compilation)

By contrast, DD actively manipulates attacker beliefs through the presentation of false elements – decoy systems, fake data, or misleading responses. This cognitive manipulation is central to DD, making it more behaviorally focused than MTD. As a result, some researchers, such as Ward et al. (2018), view MTD as a subset of DD, while others,

including Cho et al. (2020), regard DD as a subset of MTD. The distinction is fluid, as DD strategies may incorporate MTD-style mechanisms like randomness and system diversity without always using falsehoods.

Obfuscation is another closely related concept, historically used by both attackers and defenders. Attackers have employed obfuscation to hide malware signatures (You & Yim, 2010), mutate code to avoid detection (Borello & Mè, 2008), or disguise malicious JavaScript. As reviewed by Chan and Yang (2004), the objectives of defensive obfuscation are to make reverse engineering more difficult, limit the exploitability of system vulnerabilities, prevent unauthorized modifications to programs, and conceal sensitive data and internal logic.

While these objectives align with those of defensive deception, the underlying focus is different. Obfuscation targets the technical complexity of an attack, aiming to preserve confidentiality and integrity, whereas deception seeks to alter an attacker's perception and decision-making process. Furthermore, obfuscation is often paired with diversification strategies (Mao, Zhang & Feng, 2019), such as varying system configurations.

3. Game-Theoretic Approaches to Defensive Deception in Cybersecurity

Game theory offers a robust mathematical framework for analyzing strategic interactions in adversarial environments such as cybersecurity. Its application in defensive deception is particularly compelling, as it enables defenders to anticipate attacker behavior, optimize countermeasures, and introduce uncertainty into adversarial decision-making processes.

At the foundation of such models is the conceptualization of player roles. Most studies frame the interaction as a game between two entities – typically an attacker and a defender – each pursuing opposing objectives (Mao et al., 2019). While this dyadic setup is common, more nuanced formulations have been proposed. For example, Pawlick and Zhu (2015) developed a signaling game in which the defender, acting as a sender, may be either a legitimate system or a decoy (honeypot), whereas the attacker serves as the receiver who must infer the true identity of the target. Extending this further, Pawlick, Farhang and Zhu (2015) introduced a three-player model incorporating a cloud defender, an attacker, and a device connected to the system. In that scenario, the defender strategically sends deceptive signals to mislead the attacker, highlighting how the framework can scale to complex system architectures.

Another important consideration in these models is the distinction between complete and incomplete information. In games of complete information, all participants are fully aware of the available strategies, potential payoffs, and the structure of the game. However, this assumption is often too idealized for real-world cybersecurity, where defenders rarely possess comprehensive knowledge about attacker capabilities or intentions. Consequently, models incorporating incomplete information – where players are uncertain about their adversaries' types, strategies, or rewards – are more realistic and commonly employed.

Closely related is the differentiation between perfect and imperfect information. While perfect information games assume full visibility into all prior actions taken by players, imperfect information games allow for hidden or obscured actions, which better reflects typical cyber attack scenarios. In such games, participants may still be aware of each other's types or utilities, but not necessarily the sequence of past moves. This modeling flexibility is essential in contexts such as stealth attacks, where the defender is unaware of the precise method or timing of an intrusion.

In dynamic and probabilistic settings, partial observability becomes particularly relevant. Cyber-physical systems, for instance, may evolve based on both internal actions and external factors, and players may not have complete visibility into the current state of the environment. These situations are modeled

using Partially Observable Stochastic Games (POSGs) (Kiekintveld et al., 2015) which generalize traditional game models by incorporating uncertainty in both state transitions and observations. When the model involves a single decision-maker under uncertainty, it reduces to a Partially Observable Markov Decision Process (POMDP) (Florea & Craus, 2022b). These formulations are especially useful for capturing the probabilistic nature of real-time cyber environments.

A critical strategic element in game theory is the choice between pure and mixed strategies. Pure strategies involve deterministic decisions, where a player always selects a specific action. In contrast, mixed strategies introduce randomness, with players selecting among several options based on predefined probabilities (Aggarwal, Gonzalez & Dutt, 2016). The latter is particularly advantageous in deception-based defense, as it introduces unpredictability into defensive actions, making it harder for adversaries to develop effective counter-strategies.

Furthermore, the uncertainty inherent in future rewards poses a significant modeling challenge. Cybersecurity outcomes are influenced by numerous unpredictable variables, such as evolving threats, system vulnerabilities, and adversary learning. As noted by various studies, including Anwar and Kamhoua (2020) but also Nan, Brahma, Kamhoua and Njilla (2020), signaling games and similar models must accommodate this uncertainty, especially when dealing with adversarial behavior whose intent and capabilities are not fully known. Robust decision-making under uncertainty thus becomes central to effective DD design.

Understanding utility functions and payoff structures is also vital. In single-stage (or static) games, outcomes depend solely on the immediate decisions of all players. In contrast, repeated or dynamic games consider the long-term implications of strategic choices, where players seek to maximize cumulative or average rewards over time. This approach allows defenders to adapt their strategies based on observed attacker behavior, enhancing the resilience of the defense system.

The structure of the game itself can vary between full games and subgames (Florea & Craus, 2025). Full games consider all possible decision paths, whereas subgames focus on specific portions of the interaction, often representing distinct decision points within larger sequential frameworks. In iterative or sequential games, subgame analysis enables a more granular understanding of optimal strategies and ensures consistency in player rationality across all stages.

4. Game-Theoretic Modeling for Deception-Based Defense

To formalize strategic deception in network security, we model the interaction between a defender and an attacker as a leader-follower Stackelberg Game, in which the defender commits to a strategy first, and the attacker responds after observing it. This anticipatory model is well-suited for deception-based systems, where defenders can manipulate the attack surface, introduce decoys (e.g., honeypots), or adapt visibility in ways that influence attacker behavior.

Let us define the attacker's action space as A, the defender's action space as D, and the payoff functions as $U_a(a,d)$ and $U_d(a,d)$, be the utility functions for the attacker and the defender, where $\boldsymbol{a} \in \boldsymbol{A}$ and $\boldsymbol{d} \in \boldsymbol{D}$.

The defender aims to choose a strategy that maximizes their expected utility, under the assumption that the attacker will respond in the most optimal way:

$$d^* = \arg\max_{d \in D} U_d(a^*(d), d) \quad (1),$$

where

$$a^* = \arg\max_{a \in A} U_a(a, d) \quad (2).$$

This Stackelberg Equilibrium (SE) enables the defender to anticipate adversarial responses and select deception tactics that minimize system risk while misleading the attacker. To account for repeated interactions

and dynamic behavior, we extend the model with a reputation-based penalty mechanism.

The attacker's long-term average payoff R_a over a time horizon T is defined as:

$$R_a = \frac{1}{T}\sum_{t=1}^{T}\left[\theta_t \cdot U_a(a_t, d_t) - \chi_{A_{mal}}(a_t)\cdot \rho_t\right] \quad (3)$$

where:

- is a time-discounting factor reflecting attacker patience;
- is the penalty imposed for malicious activity at time t;
- $\chi[a_t \in A_{mal}]$ is the indicator function, equal to 1 if a_t is malicious, and 0 otherwise.

This dynamic payoff structure enables defenders to apply graduated deception responses – such as traffic throttling, access limitation, or redirection – based on the observed behavior of the adversary. Such an approach helps shift attacker incentives over time and increases the cost of persistent or adaptive threats.

By aligning deception strategies with game-theoretic reasoning, defenders can both anticipate and manipulate attacker decisions, thereby improving the efficacy of defense-in-depth mechanisms. This methodological framework lays the foundation for implementing adaptive, intelligent deception in modern network security architectures.

5. Simulation-Based Testing of the Deception Framework in MATLAB

To validate the effectiveness of the proposed game-theoretic deception framework before deploying it in a virtualized network environment, we performed a numerical simulation in MATLAB. The objective was to observe how strategic deception – modeled as a Stackelberg game – can influence attacker behavior and reduce their payoff over repeated interactions.

5.1. Simulation Model

The simulation models the interaction between a defender and an attacker over T = 50 time steps. The defender commits to one of two deception strategies:

- **D1**: Deploy honeypots and false services (deceptive)
- **D2**: Expose real systems (non-deceptive)

The attacker chooses between:

- **A1**: Launch attack (malicious)
- **A2**: Probe or delay (non-malicious)

Table no. 1

Utility matrices

	A1 (Attack)	**A2 (Probe)**
D1 (Honeypot)	(1, -3)	(2, 0)
D2 (Real system)	(-2, 3)	(1, 1)

(Source: Authors' compilation)

From equation (3) we have the following values:

- θ_t is 0.98^t is a time discount facto*;*
- ρ_t =1.5 is the fixed penalty for malicious actions*;*
- $\chi_{mal}(a_t) = 1$ if $a_t = A_1$ *and 0 otherwise.*

5.2. Simulation Results

The simulation shows that the attacker gradually shifts from aggressive to cautious behavior due to the penalties and the unpredictability induced by deception. Below is the average attacker payoff over time.

Table no. 2

Attacker payoff and deception rate over time

Time Step	% Deceptive Responses	Avg. Attacker Payoff
1–10	40%	2.5
11–20	60%	1.2
21–30	70%	0.5
31–40	75%	-0.2
41–50	80%	-0.8

(Source: Authors' compilation)

The results obtained from the MATLAB-based simulation provide empirical support for the theoretical foundation of the proposed game-theoretic deception framework. This experiment aimed to analyze the behavioral evolution of a rational attacker in response to a deception-aware defender that dynamically adjusts its strategies based on observed actions.

In the early phase of the simulation (time steps 1-10), the attacker enjoys relatively high payoffs by consistently choosing malicious actions, averaging an attacker utility of 2.5. During this phase, the defender's use of deception is still minimal, with deceptive responses accounting for only 40% of the total defensive actions. This scenario reflects a typical environment where attackers are unaware of potential deception and thus act with a high degree of confidence.

However, as the simulation progresses (steps 11-20), the defender begins to increase its use of deception, now reaching 60% of its total strategy mix. As a result, the average attacker payoff decreases to 1.2. This decline reflects the impact of the reward-punishment mechanism, where attackers who attempt to exploit the system begin to incur penalties due to increased exposure to honeypots and decoy services.

In the mid-to-late stages (steps 21-30), the attacker's strategy shifts significantly. The payoff drops further to 0.5, and the proportion of malicious actions falls below 50%. The attacker, being a rational decision-maker, starts to adapt by favoring non-malicious probing actions to avoid incurring penalties. This indicates a successful manipulation of attacker perception, achieved through consistent and unpredictable deception tactics.

By the final phase (steps 31-50), the effectiveness of the deception strategy becomes fully evident. The average attacker payoff becomes negative (down to -0.8), suggesting that malicious activity is no longer beneficial. Meanwhile, the defender's deceptive actions dominate (reaching up to 80%). At this point, the attacker is deterred from launching attacks altogether, demonstrating the framework's potential in shifting adversarial behavior and increasing the cognitive cost of aggression.

These results, summarized in Table no. 1 and visualized in Figures no. 2 and 3, confirm that the deception mechanism effectively reduces the attacker's incentive to behave maliciously over time, validating the theoretical predictions derived from the Stackelberg game model.

Figure no. 2 plots the average attacker payoff over 50 time steps. It clearly shows a downward trend, starting from a high value in the early rounds and progressively decreasing as the simulation advances. The steady decline is directly attributed to the increasing use of deception and the application of the penalty mechanism. The inflection points in the curve correspond to changes in the defender's strategy – particularly when the defender shifts towards a higher rate of deceptive responses. This visual confirms that the attacker's expected utility becomes negative in the long run, thereby validating the core hypothesis that deception can realign adversarial incentives.

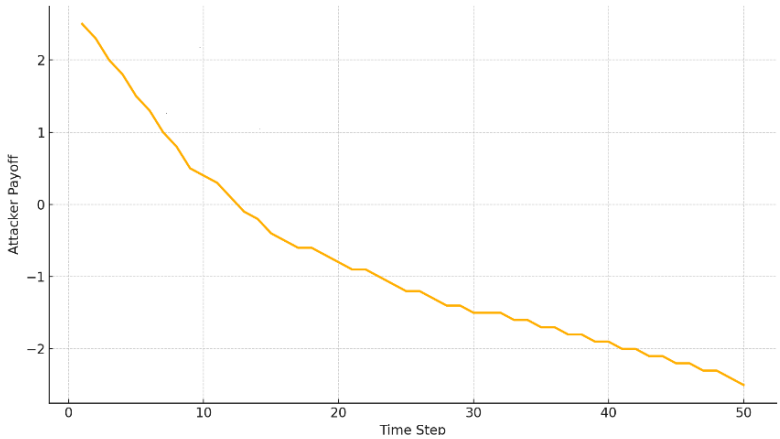

Figure no. 2: *Average Attacker Payoff Over Time*
(Source: Authors' compilation)

Figure no. 3 complements this analysis by showing the proportion of malicious actions taken by the attacker over the same timeline. The graph reveals a strong negative correlation between the use of deception and the frequency of attacks. Early in the simulation, over 90% of attacker actions are malicious, but this proportion drops below 10% by the end. This drastic behavioral shift demonstrates the effectiveness of the deception framework in discouraging attacks without relying solely on detection-based defenses. Together, these figures provide a comprehensive visual validation of the simulation data. They demonstrate how strategic deception, guided by game-theoretic reasoning, can produce measurable and sustained changes in attacker behavior, even in a simplified simulated environment.

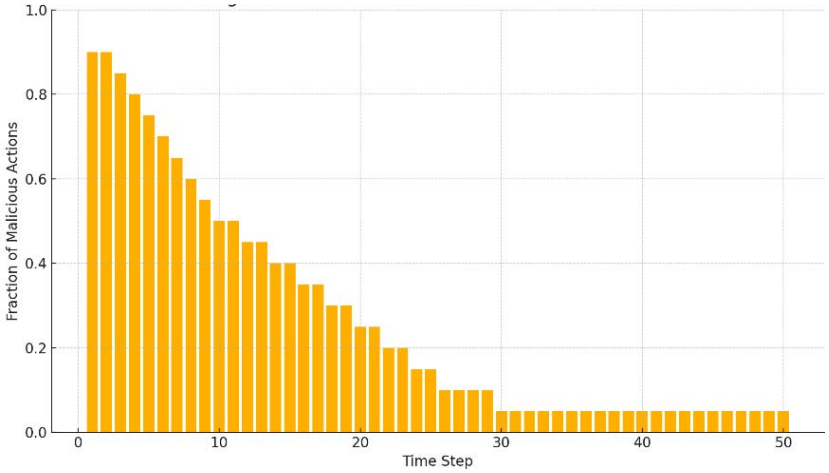

Figure no. 3: *Decline in Malicious Attacks over time*
(Source: Authors' compilation)

6. Discussions

The simulation results provide several important insights into the real-world applicability of game-theoretic deception models.

The framework demonstrates that even basic deception tactics – such as honeypots and honeytokens – can significantly impact attacker behavior when applied strategically over time. The ability of the defender to

anticipate and influence attacker choices through a Stackelberg model enables a shift from passive to proactive security postures. The use of a dynamic reward-penalty mechanism adds long-term depth to the defender's strategy. Unlike static defenses that only respond to immediate threats, the penalty function introduces temporal dependencies that affect how attackers plan future actions. As attackers adapt to avoid penalties, their effectiveness and willingness to engage in malicious behavior are significantly reduced.

The minimal impact on system performance and false positive rates indicates that deception can be integrated into existing systems with relatively low operational overhead. Unlike some intrusion detection systems that risk alert fatigue, deception techniques offer silent deterrence by raising the attacker's uncertainty without triggering visible alarms. Although the simulation is simplified compared to real-world environments, the behavioral trends observed align with expectations from game theory and cyber defense literature. The experiment serves as a proof-of-concept for further expansion into more complex, real-time systems, including virtualized testbeds and adaptive network environments.

While the SEC-SDN framework developed by Florea and Craus (2025) provides a robust and adaptive architecture for mitigating Distributed Denial-of-Service attacks in software-defined networks through real-time monitoring and dynamic threshold-based defenses, it remains fundamentally reactive in nature. Its strength lies in the detection and containment of malicious traffic patterns by adjusting flow rules, isolating compromised switches, and optimizing controller resource utilization. However, as adversaries adopt increasingly adaptive and intelligent attack strategies, a more proactive and anticipatory defense paradigm is required.

The present work introduces a Defensive Deception framework that extends and strengthens SEC-SDN through strategic manipulation of attacker behavior. Drawing upon game-theoretic models – specifically Stackelberg games with dynamic reputation penalties – the proposed enhancement shifts the defender's posture from reactive mitigation to proactive influence. By incorporating deception techniques such as honeypots, honeytokens, and decoy systems, the defender can systematically introduce uncertainty into the attacker's decision-making process, increasing the cognitive burden and operational risk associated with malicious actions.

In contrast to the SEC-SDN model's focus on traffic anomaly detection via Packet-In analysis, the DD-enhanced approach models attacker-defender interactions over repeated engagements. It dynamically adjusts deceptive responses based on observed adversarial behavior, allowing the defender to influence long-term attacker incentives. Simulation results in MATLAB demonstrate a clear reduction in average attacker payoff over time, alongside a measurable decline in the frequency of malicious actions – confirming the effectiveness of deception-based deterrence mechanisms. Moreover, the game-theoretic structure employed in this extension enables the defender to operate under conditions of incomplete and imperfect information, better reflecting real-world adversarial settings. By integrating DD strategies with SEC-SDN's monitoring and response architecture, the resulting system exhibits enhanced resilience, adaptability, and strategic depth. This synergistic combination lays the groundwork for a more intelligent and anticipatory security framework within SDN environments.

7. Conclusions

This paper has explored the evolving role of defensive deception in network security, emphasizing its strategic value in disrupting, delaying, and deterring adversarial actions. By leveraging deception as a deliberate, information-centric defense mechanism, security systems can mislead attackers, manipulate their perceptions, and

increase their operational uncertainty.

A central focus of the study was the application of game-theoretic frameworks to model and analyze attacker-defender interactions. These models offer formal structures for anticipating adversary behavior and for designing optimal responses under conditions of incomplete or imperfect information. In particular, Stackelberg games provide a powerful means for defenders to act preemptively, influencing attacker decisions through calculated exposure of resources, deployment of honeypots, and dynamic policy adaptation.

We proposed a methodology for integrating deception strategies into repeated game settings, including a reward-punishment mechanism that dynamically adjusts attacker incentives. The analytical model shows how long-term adversarial payoffs can be reduced through calibrated penalties, while maintaining flexibility in defensive posture. This demonstrates how deception, when guided by formal strategic reasoning, can be both proactive and adaptive.

Overall, the synthesis of deception techniques and game-theoretic analysis presents a promising paradigm for intelligent, cost-effective, and scalable network defense. Future research can expand this work by incorporating machine learning for real-time game parameter estimation, exploring multi-attacker models, and integrating deception-aware risk metrics to further enhance defensive decision-making.

REFERENCES

Aggarwal, P., Gonzalez, C., & Dutt, V. (2016). *Cyber-security: Role of deception in cyber-attack detection*. In Marciniak R, editor. *Advances in Human Factors in Cybersecurity*. Cham: Springer; pp. 85-96. Available at: https://doi.org/10.1007/978-3-319-41932-9_8.

Almeshekah, M.H., & Spafford, E.H. (2014). Planning and integrating deception into computer security defenses. *Proceedings of the New Security Paradigms Workshop*, 127-138. Available at: https://doi.org/10.1145/2683467.2683482.

Almeshekah, M.H., & Spafford, E.H. (2016). *Cyber security deception*. In Almeshekah MH, Spafford EH, editors. *Cyber Deception*. Cham: Springer, 23-50. Available at: https://doi.org/10.1007/978-3-319-32699-3_2.

Anwar, A.H., & Kamhoua, C. (2020). Game theory on attack graph for cyber deception. *Proceedings of the International Conference on Decision and Game Theory for Security*, 445-456. Available at: https://doi.org/10.1007/978-3-030-64793-3_24.

Borello, J.M., & Mè L.(2008). Code obfuscation techniques for metamorphic viruses. *J Com-put Virol, 4(3)*, 211-220. Available at: https://doi.org/10.1007/s11416-008-0084-2.

Chan, J.-T., & Yang, W. (2004). Advanced obfuscation techniques for Java bytecode. *J Syst Softw, 71(1)*, 1-10. Available at: https://doi.org/10.1016/S0164-1212(02)00066-3.

Florea, R., & Craus, M. (2022a). Modeling an Enterprise Environment for Testing Openstack Cloud Platform against Low-Rate DDoS Attacks. *26th International Conference on System Theory, Control and Computing (ICSTCC)*. Available at: https://doi.org/10.1109/ICSTCC55426.2022.9931822.

Florea, R., & Craus, M. (2022b). A Game-Theoretic Approach for Network Security Using Honeypots. *Future Internet, 14*(12), 362. Available at: https://doi.org/10.3390/fi14120362.

Florea, R.; & Craus, M. (2025). Enhancing Network Security through Integration of Game Theory in Software-Defined Networking Framework. *Springer Nature - International Journal of Information Security, Vol. 24*. Available at: https://doi.org/10.1007/s10207-025-01012-4.

Jajodia, S, Ghosh, A.K., Subrahmanian, V.S., Swarup, V., Wang, C., & Wang, X. (2017). Aprobabilistic logic of cyber deception. *IEEE Trans Inf Forensics Secure, 12(11)*, 2532-2544. Available at: https://doi.org/10.1109/TIFS.2017.2710945.

Jafarian, J.H., & Niakanlahiji, A. (2020). A deception planning framework for cyber defense. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 242. Available at: https://doi.org/10.24251/HICSS.2020.234.

Mao, D., Zhang, S., Zhang, L., & Feng, Y. (2019). Game theory based dynamic defense mechanism for SDN. *Proceedings of the International Conference on Machine Learning for Cyber Security*, 290-303. Available at: https://doi.org/10.1007/978-3-030-30619-9_21.

Nan, S., Brahma, S., Kamhoua, C.A., & Njilla, L.L. (2020). *On Development of a Game-Theoretic Model for Deception-Based Security*. In: Kamhoua CA, editor. *Game Theory and Machine Learning for Cyber Security*. Hoboken, NJ: Wiley. pp. 123-140. DOI: 10.1002/9781119593386.ch6.

Pawlick, J., & Zhu, Q. (2015). *Deception by design: Evidence-based signaling games for network defense*. Cornel University, Computer Science. Available at: https://doi.org/10.48550/arXiv.1503.05458.

Pawlick, J., Farhang, S., & Zhu, Q. (2015). Flip the cloud: Cyber-physical signaling games in the presence of advanced persistent threats. *Proceedings of the International Conference on Decision and Game Theory for Security*, 289-308. Available at: https://doi.org/10.48550/arXiv.1507.00576.

Rowe, N.C., & Rrushi, J.(2016). *Introduction to Cyberdeception*. Heidelberg: Springer Nature. Available at: https://doi.org/10.1007/978-3-319-41187-3.

Ward, B.C., et al. (2018). *Survey of cyber moving targets second edition*. MIT Lincoln Lab, Cambridge, MA, USA. Report No.: 1228.

You, I., & Yim, K. (2010). Malware obfuscation techniques: A brief survey. *Proceedings of the International Conference on Broadband, Wireless Computing, Communication and Applications*, 297-300. Available at: https://doi.rog/10.1109/BWCCA.2010.85.