International Journal of Operations Research and Artificial Intelligence

www.ijorai.reapress.com

Int. J. Oper. Res. Artif. Intell. Vol. 2, No. 1 (2026) 31–42.

Paper Type: Original Article

Game-Theoretic Analysis of Adaptive Behavior Between Attacker and Intrusion Detection System in IoT Gateways

Mojtaba Sandoughi[1,*], Mohammad Malek Raeisi[1], Hamid Saadatfar[1]

[1] Department of Computer Engineering, Faculty of Electrical and Computer Engineering, University of Birjand, Birjand, Iran; mojtaba.sandoughi@iau.ac.ir; mohammad.malekraeisi@iau.ac.ir; saadatfar@birjand.ac.ir.

Citation:

Received: 01 October 2025 *Revised: 13 December 2025* *Accepted: 19 February 2026*	Sandoughi, M., Malek Raeisi, M., & Saadatfar, H. (2026). Game-theoretic analysis of adaptive behavior between attacker and intrusion detection system in IoT gateways. *International Journal of Operations Research and Artificial Intelligence, 2*(1), 31-42.

Abstract

With the rapid expansion of the Internet of Things (IoT) and the increasing dependence of smart infrastructures on communication gateways, securing these gateways against adaptive attacks has become a fundamental challenge in computer engineering. In many existing methods, the behavior of either the attacker or the Intrusion Detection System (IDS) is modeled statically or independently of the opponent's actions. However, in real-world scenarios, both sides continuously learn and adapt. In this study, a game-theoretic framework is proposed to analyze the adaptive behavior of an attacker and an IDS in IoT gateways. The interaction between the attacker and the IDS is modeled as a repeated game with memory-one strategies, and the mutual learning process is implemented using incremental optimization of each agent's long-term payoff. Furthermore, to adapt the model to the practical constraints of the IoT, the cost of processing resources and energy consumption of the IDS system is incorporated into its utility function. Numerical simulation results show that asymmetry in the learning speeds of the attacker and the IDS plays a decisive role in the stability of IoT gateway security. Specifically, when the IDS adapts at a faster rate than the attacker, the attacker's behavior is significantly suppressed, and the probability of successful attacks decreases, although the operational costs of the IDS increase. Conversely, for intermediate learning speeds, an adaptive competitive dynamic is observed in which neither party achieves a sustainable advantage. The results of this study can be utilized as an analytical tool for designing and tuning lightweight IDSs in IoT gateways.

Keywords: Internet of things, Intrusion detection system, Game theory, Adaptive learning, Network security.

1 | Introduction

The rapid expansion of the Internet of Things (IoT) in recent years has led to the widespread connection of heterogeneous smart devices with limited computational capabilities and energy resources. These devices

Corresponding Author: mojtaba.sandoughi@iau.ac.ir

https://doi.org/10.48314/ijorai.v2i1.86

typically connect to wide networks and cloud infrastructures through IoT gateways. IoT gateways act as central nodes for data aggregation, communication management, and the enforcement of control and security policies; hence, they have become prime targets for cyberattacks [1], [2]. Any intrusion or disruption in the performance of these gateways can bring serious consequences for the entire system, including privacy breaches, service downtime, and financial losses. In this regard, Intrusion Detection Systems (IDS) play an important role in enhancing security within IoT environments.

However, deploying an IDS in IoT gateways faces several challenges. On one hand, these gateways are constrained by hardware limitations such as processing power, memory, and energy consumption. On the other hand, attackers employ sophisticated and adaptive methods to identify and bypass defensive mechanisms [3], [4]. These conditions have rendered many static or rule-based methods ineffective against advanced attacks. In response to these challenges, numerous studies have proposed the use of machine learning and deep learning methods for intrusion detection in the IoT [5], [6]. Although these approaches provide adequate detection accuracy in many scenarios, they often assume that the attacker's behavior is independent of the defensive system's actions or that its changes over time are negligible. In real-world environments, however, attackers continuously update their strategies based on the reactions of security systems, forming a mutual learning and adaptation process between the attacker and defender [7]. Ignoring this two-sided dynamic can lead to unrealistic assessments of system security.

Game theory, as a powerful analytical framework for studying interactions among rational agents, provides an appropriate tool for modeling the confrontation between attackers and defensive systems [8]. Specifically, repeated games allow for the study of player behavior in long-term, history-dependent interactions. Within this framework, memory-one strategies have garnered significant attention in multi-agent system analysis and cybersecurity due to their structural simplicity and high interpretability [9], [10].

Nevertheless, a major portion of existing studies either assumes one of the game parties to be fixed or fails to explicitly incorporate the operational costs and resource constraints of defensive systems into the model [11]. Recent studies in multi-agent learning have shown that asymmetry in agent learning speeds can give rise to complex dynamics, such as an adaptive arms race state where both sides continuously alter their behavior without achieving a sustainable advantage [12]. This phenomenon is particularly critical in IoT environments where defensive systems face resource constraints. Despite its importance, a systematic analysis of the relative learning speed effect between the attacker and the IDS within IoT gateways remains understudied.

In this research, the interaction between an attacker and an IDS in IoT gateways is modeled as a repeated game with two-sided adaptive learning. Within this framework, each party incrementally updates its decision-making strategies to maximize its long-term payoff. To align the model with practical conditions, costs arising from the processing resources and energy consumption of the IDS are factored into its decision-making process. This approach enables the simultaneous evaluation of system security, stability, and efficiency across various learning scenarios, providing a viable analytical perspective for designing lightweight IDSs in IoT environments.

The remainder of this paper is organized as follows: Section 2 reviews related work in IoT security, IDSs, and the application of game theory. Section 3 describes the system model and problem formulation. Section 4 elaborates on the adaptive learning framework and the proposed method. Section 5 presents and analyzes the simulation results, and finally, Section 6 concludes the paper and outlines future research directions.

2 | Related Work and Research Background

IoT security has become an active area of research in computer engineering over recent years. The distributed, heterogeneous, and resource-constrained nature of IoT systems means that traditional network security solutions lack the necessary efficiency and scalability in these environments. In this regard, related research can be broadly classified into three main categories: IDSs in IoT, the application of game theory in network and IoT security, and adaptive attacker-defender learning models.

2.1 | Intrusion Detection Systems in the IoT

A significant portion of IoT security research has focused on designing and implementing lightweight IDSs. These studies have attempted to identify common attacks in IoT networks using signature-based methods, anomaly analysis, or hybrid approaches [13], [14]. With the advancement of data-driven methods, the utilization of machine learning and deep learning algorithms for intrusion detection in IoT environments has received widespread attention [15], [16]. Although these approaches offer high detection accuracy in many cases, they often face challenges such as the need for large training datasets, high computational costs, and degraded performance under shifting attack patterns [17]. Furthermore, in many of these studies, the IDS is treated as a static entity, and the attacker's behavior is implicitly assumed to be independent of the defensive system's reaction. This assumption can lead to unrealistic analyses in real scenarios where attackers actively modify their behavior [8].

2.2 | Game Theory in Network Security and the IoT

Game theory, as a powerful analytical tool, has been widely used to model the interaction between attackers and defensive systems in network security. Early studies utilized static and non-cooperative games to analyze attacker-defender decision-making [8]. However, the complexity of real-world environments has driven researchers toward more dynamic models, including repeated games and stochastic games [18]. In the IoT domain, some studies have leveraged game theory to analyze security resource allocation, defensive policy selection, and risk management in gateways and edge nodes [19]. These works demonstrate that game-theoretic models can transparently and interpretably represent strategic interactions between attackers and defenders. Nevertheless, many of these models either focus on static equilibria or assume that one party follows a fixed strategy [8].

2.3 | Adaptive Attacker-Defender Learning and Repeated Games

In recent years, researchers' attention has increasingly turned toward adaptive learning models in security games. These studies emphasize that both attackers and defensive systems can utilize past experiences to improve future decision-making [11]. Repeated games with history-dependent strategies provide an appropriate framework for analyzing such dynamics. In particular, memory-one strategies have gained prominence in studying repeated interactions among adaptive agents due to their simple structure and analytical tractability [9].

Some studies have shown that asymmetry in agent learning speeds can lead to complex behaviors such as an adaptive arms race or stable oscillations [20]. Nonetheless, a major part of this research has been conducted in abstract contexts or classic games, failing to directly account for the practical constraints of IoT systems, specifically resource costs in IoT gateways [12].

2.4 | Summary and Research Gap

A review of related work reveals that while significant progress has been made in IDSs, game theory, and adaptive learning, gaps remain in modeling IoT security. Specifically, the simultaneous analysis of the adaptive behavior of both the attacker and the IDS as a repeated game, while accounting for the resource constraints of IoT gateways, has received little attention. This research gap highlights the necessity of providing frameworks that can seamlessly analyze mutual learning dynamics, operational costs, and security stability.

3 | System Model and Problem Formulation

In this research, a security scenario for IoT gateways is considered where the interaction between an adaptive attacker and an IDS is modeled as a dynamic, long-term process. The IoT gateway serves as the central communication point between resource-constrained devices and broader networks, and it is responsible for enforcing control and security policies. Given the critical role of these gateways, attackers attempt to exploit adaptive behavioral patterns to tailor their attacks to bypass intrusion detection mechanisms [21].

3.1 | System Scenario and Assumptions

In the proposed model, the interaction between two rational decision-making agents is modeled: The Attacker, who seeks to intrude, disrupt, or exploit system resources by sending malicious or quasi-malicious traffic; and the IDS deployed at the IoT gateway, which analyzes incoming traffic patterns and enforces control policies. Both agents operate under incomplete information and make decisions based on past experiences and observations of prior outcomes. The attacker can adjust the intensity and pattern of their attacks, while the IDS tunes the stringency of its security policies. This dynamic aligns with the operational constraints of the IDS, including limited processing resources and energy, where executing stricter policies incurs higher operational costs. These assumptions provide a realistic backdrop for strategically analyzing dynamic interactions in IoT environments [22].

3.2 | Modeling the Interaction as a Repeated Game

The interaction between the attacker and the IDS is modeled as a non-cooperative repeated game, where the stage game is repeated over consecutive time intervals. In each stage, the attacker selects one of two possible actions: a low-intensity or stealthy attack (low/stealthy attack), designed with minimal disruption to evade detection, or a high-intensity attack (high-intensity attack), which focuses on maximizing damage, though it increases the risk of exposure.

Similarly, the IDS chooses between two defensive policies: A lenient policy (lenient/allow), which permits traffic flow to minimize false positives, or a strict policy (strict/block), which neutralizes threats through aggressive filtering. The combination of these actions results in four possible states that describe the system's security status. These states represent conditions such as normal traffic passage, unnecessary blocking, successful attack, or detected and mitigated attack. This formulation allows for the analysis of the long-term behavior of the system within a game-theoretic framework [8].

3.3 | Memory-One Strategies and the Markov Model

In this study, both agents utilize memory-one strategies, meaning their decision at any stage depends solely on the outcome of the previous stage. While maintaining simplicity, this type of strategy provides the capability to model temporal dependence and adaptive behavior [23]. Given this assumption, the state transition process of the system can be modeled as a finite-state Markov chain. The transition probability from one state to another depends on the strategies chosen by the attacker and the IDS. Consequently, the long-term behavior of the system can be analyzed by calculating the stationary distribution of the Markov chain. This approach has been used in numerous studies to analyze security games and repeated interactions [18].

3.4 | Utility and Cost Functions

At each stage of the game, each agent receives a payoff that reflects the benefits and costs resulting from the actions taken. The attacker's payoff is a function of the attack's success or failure and can include gains from intrusion or costs from detection and blocking. Conversely, the payoff of the IDS includes not only the security benefits of detecting attacks but also the operational costs associated with enforcing strict policies. In this model, the resource cost of the IDS is explicitly included in its utility function to reflect the practical constraints of IoT gateways regarding energy consumption and processing power. This formulation allows for a concurrent evaluation of the security effectiveness and operational costs of the defensive system, leading to a more realistic analysis of system behavior [24].

3.5 | Long-Term Payoff and Agent Objectives

Since the interaction between the attacker and the IDS occurs over a long-term time horizon, the performance evaluation metric for each agent is considered to be its average long-term payoff at the system's steady state. This payoff is calculated by combining the stationary distribution of the Markov chain with the stage payoffs.

It is assumed that each agent updates its strategies incrementally with the goal of maximizing its expected long-term payoff. This formulation allows for investigating the impact of parameters such as the agents' relative learning speed and the resource cost of the IDS on system security stability, creating an appropriate platform for analyzing competitive and adaptive dynamics in IoT environments [12], [20].

4 | Proposed Method and Adaptive Learning Framework

In this section, the proposed framework for analyzing and simulating the adaptive behavior of the attacker and the IDS stationed at the IoT gateway is presented. The core concept rests on the premise that security interactions in the IoT are repeated and history-dependent; thus, this interaction can be modeled as a repeated game with memory-one strategies, and mutual learning can be implemented as the step-by-step optimization of each agent's long-term payoff. In this framework, rather than optimizing stage-wise profits, both agents target the long-term average payoff so that system behavior over an extended horizon is properly represented under adaptive dynamics.

4.1 | Strategy Representation and Parameter Space

It is assumed that each agent uses a memory-one strategy; therefore, each agent's decision at step t depends only on the state observed at step $t-1$. The four possible states (in conventional order) are:

$$S = \{CC, CD, DC, DD\},$$

where the first letter corresponds to the attacker's action and the second letter corresponds to the IDS action. In the implementation, actions are binary:

I. For the attacker: C (low-intensity/stealthy behavior) and D (high-intensity attack).

II. For the IDS: C (lenient/allow passage) and D (strict/blocking).

The attacker's strategy is represented by the following probability vector:

$$p = [p_{CC}, p_{CD}, p_{DC}, p_{DD}],$$

where $p_s = \Pr(\text{Attacker chooses } C \mid s)$. Similarly, the IDS strategy is described by the vector:

$$q = [q_{CC}, q_{CD}, q_{DC}, q_{DD}],$$

where $q_s = \Pr(\text{IDS chooses } C \mid s)$.

4.1.1 | Constraining the IDS space (IoT gateway compatible)

To make the model closer to IoT gateway scenarios (which typically have fixed or semi-fixed policies under certain conditions), the IDS is confined to a restricted class of strategies:

$$q = [1, q_2, 0, q_4].$$

(Factoring in ϵ to avoid exact zeros/ones), such that only q_2 and q_4 are learnable, while $q_1 \approx 1$ and $q_3 \approx 0$ are kept fixed. This constraint reduces complexity while significantly enhancing the interpretability of IDS behavior.

4.2 | Markov Transition Matrix Model

Given the memory-one strategies, the transition probability from the current state s to one of the four states in the next step depends on the product of the action probabilities. If we are in state s:

I. Probability of CC occurring: $p_s q_s$

II. Probability of CD occurring: $p_s(1 - q_s)$.

III. Probability of DC occurring: $(1 - p_s)q_s$.

IV. Probability of DD occurring: $(1 - p_s)(1 - q_s)$.

Consequently, a Markov chain with a transition matrix $M(p, q) \in \mathbb{R}^{4\times4}$ is constructed, where:

$$M_{ij} = \Pr(s_{t+1} = j \mid s_t = i).$$

4.3 | Stationary Distribution Calculation and Long-Term Payoff

To analyze long-term behavior, the stationary distribution of the Markov chain is computed:

$$\pi = \pi M, \quad \sum_{s\in S} \pi_s = 1.$$

In the implementation, this is executed using the power method to ensure numerical convergence of π.

If the stage payoffs of the attacker and the IDS in state s are $u_X(s)$ and $u_Y(s)$ respectively, the average long-term payoff is computed as:

$$S_X(p, q) = \sum_{s\in S} \pi_s \, u_X(s), \quad S_Y(p, q) = \sum_{s\in S} \pi_s \, u_Y(s).$$

4.3.1 | Incorporating IDS resource cost (IoT-centric innovation)

In IoT environments, IDS strictness incurs processing, energy, and latency costs. Thus, a cost component is added to the IDS payoff function. Generally:

$$u_Y(s) = \text{SecurityGains} - \lambda \cdot \text{OperationalCosts}$$

where λ is the resource cost weight for the IDS. This model forces the IDS to balance security and operational costs at its optimum.

4.4 | Two-Sided Learning Dynamics

The objective of each agent is to maximize its own long-term payoff. Therefore, a concurrent learning process is defined where:

I. The attacker updates learnable parameters in p to increase S_X.

II. The IDS updates learnable parameters in q to increase S_Y.

4.4.1 | Learning speed asymmetry (parameter ω)

To model differences in adaptation speeds, the IDS learning rate is determined as a function of ω:

$$\alpha_Y = \omega\alpha_X, \quad \omega \in (0,1),$$

where:

I. $\omega \to 0$: Very slow IDS (nearly static).

II. $\omega \to 1$: IDS adapts at the same speed as the attacker.

III. Intermediate ω: Allows for the emergence of an adaptive arms race dynamic.

4.5 | Gradient Approximation and Parameter Updates

Since $S_X(p,q)$ and $S_Y(p,q)$ may lack complex analytical closed-form derivatives (particularly due to the numerical calculation of π), each agent's gradient is approximated via Central Finite Difference. For a learnable parameter θ_k, we have:

$$\frac{\partial S}{\partial \theta_k} \approx \frac{S(\theta_k + \delta) - S(\theta_k - \delta)}{2\delta},$$

where δ is the difference step. The updates are then executed via gradient ascent:

$$\theta_{t+1} = \theta_t + \alpha \nabla S(\theta_t).$$

4.5.1 | Numerical stabilization (clipping)

To prevent instability caused by probabilities landing exactly on 0 or 1 and to improve numerical convergence, probabilities are clipped to the interval $[\epsilon, 1-\epsilon]$ after each update. Furthermore, fixed constraints for the IDS (such as $q_1 \approx 1$ and $q_3 \approx 0$) are re-applied after each learning step.

The overall learning process is presented algorithmically below.

Algorithm 1. Adaptive learning of attacker and IDS in IoT gateway.

Initialize $p \to p^{(0)}$, $q \to q^{(0)}$
Apply clipping to p and q
Set $\alpha_Y \to \omega \cdot \alpha_X$
for $t = 1$ to T do
 Construct transition matrix $M(p,q)$
 Compute stationary distribution π using power iteration method
 Compute long-term payoffs $S_X(p,q)$ and $S_Y(p,q)$
 Approximate attacker gradient $\nabla_{\theta_X} S_X$ using central difference
 Update attacker parameters: $\theta_X \to \theta_X + \alpha_X \cdot \nabla_{\theta_X} S_X$
 Apply clipping to p
 Approximate IDS gradient $\nabla_{\theta_Y} S_Y$ using central difference
 Update IDS parameters: $\theta_Y \to \theta_Y + \alpha_Y \cdot \nabla_{\theta_Y} S_Y$
 Apply clipping to q
 Enforce IDS fixed constraints
 Store $S_X(t), S_Y(t), p(t), q(t)$
end for
Return payoff time series and strategy evolution paths.

5 | Results and Analysis

In this section, the results obtained from simulating the proposed framework to analyze the adaptive behavior of the attacker and the IDS in IoT gateways are presented and discussed. The primary analytical focus lies on evaluating the impact of learning speed asymmetry between the two agents and the role of IDS resource costs in system security stability. The simulation outputs include each agent's long-term payoff and the evolution paths of strategy parameters over the learning process. (note: Refer to the original document figures for the plots mentioned below).

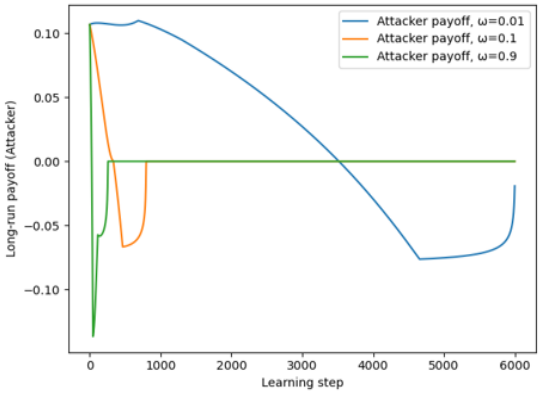

Fig. 1. Changes in the attacker's long-term payoff for different values.

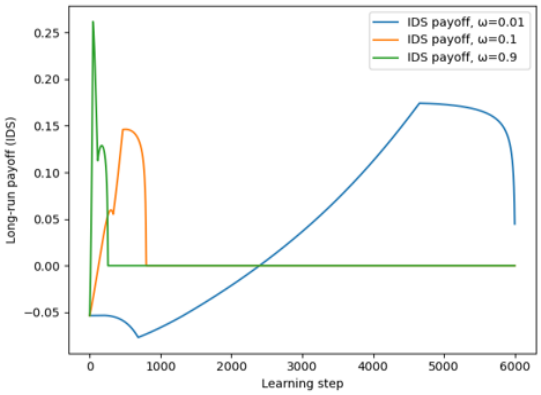

Fig. 2. Changes in the IDS long-term payoff for different values.

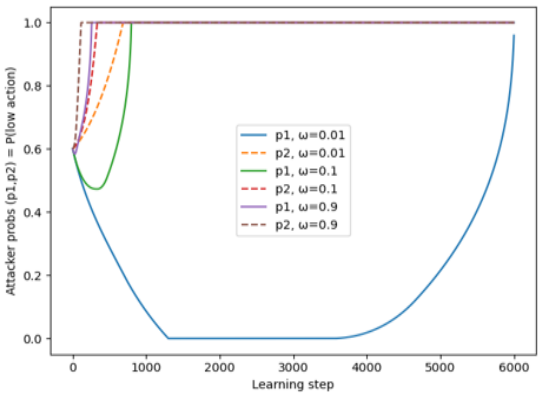

Fig. 3. Evolution path of the attacker's strategy parameters.

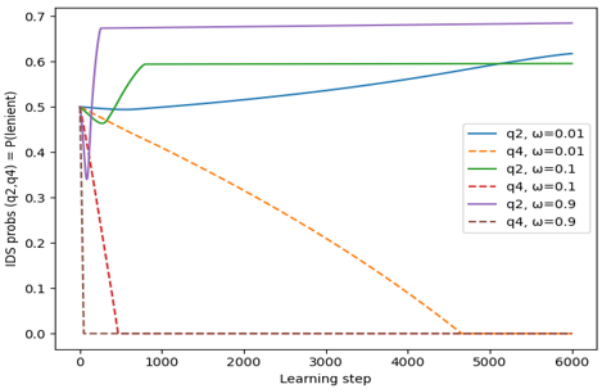

Fig. 4. Evolution path of the IDS strategy parameters.

5.1 | Analysis of Attacker Long-Term Payoff

Fig. 1 illustrates the variations in the attacker's long-term payoff across different values of the relative learning speed parameter. The results indicate that when the IDS adapts at a much slower rate than the attacker, the attacker is capable of securing a positive payoff in the early stages. This state reflects the relative success of attacks against a slow or under-responsive defensive system. However, even under these conditions, with the passage of time and accumulation of experience, the attacker's behavior undergoes a shift, and its long-term payoff declines. Conversely, when the learning speed of the IDS increases, the attacker's long-term payoff drops rapidly, ultimately converging to values near zero or negative. This outcome demonstrates that rapid adaptation of the defensive system can effectively curtail the attacker's capacity to sustain successful attacks in the long run. From a security standpoint, such behavior signifies the establishment of a deterrent property within the system.

5.2 | Analysis of IDS Long-Term Payoff

Fig. 2 displays the long-term payoff of the IDS under various learning speed scenarios. In the case where the IDS adapts slowly, its payoff is initially negative due to leaked attacks and subsequent security damage. However, it gradually converges to positive values as defensive policies update, indicating an improvement in the system's security posture. In high learning speed scenarios, although the IDS can suppress attacks within a shorter timeframe, its long-term payoff converges to limited values due to the inclusion of operational resource costs. These results demonstrate that increasing defensive strictness does not always yield a higher net profit for the IDS, and resource constraints play a decisive role in its optimal behavior. Hence, a payoff close to zero under these conditions can be interpreted as a sign of equilibrium between security and operational expenditure.

5.3 | Analysis of Attacker Strategy Evolution Path

Fig. 3 displays the evolution path of the attacker's strategy parameters during the learning process. The results indicate that the attacker's behavior is heavily contingent upon the adaptation speed of the IDS. Under conditions where the IDS acts slowly, the attacker shifts toward adopting more aggressive behaviors that boost the likelihood of attack success. In contrast, as the IDS learning speed accelerates, the attacker progressively moderates its behavior, leaning toward low-intensity or stealthy patterns. This behavioral shift implies that when facing an adaptive defensive system, the attacker prefers to minimize the risk of high-intensity attacks. From a practical perspective, this result underscores the importance of designing defensive systems with rapid response capabilities to diminish the attacker's incentive to launch destructive attacks.

5.4 | Analysis of IDS Strategy Evolution Path

Fig. 4 displays changes in the decision-making parameters of the IDS during the learning process. The results show that the IDS adaptively tunes its level of strictness. In the initial phases, the IDS may deploy harsher policies to prevent attacks from getting through; however, when considering resource costs, this strictness does not remain absolute or permanent. Over the long term, the IDS converges to a balanced policy wherein defensive strictness is applied solely under high-risk conditions, while costly policies are avoided in other states. This adaptive behavior highlights the capacity of the proposed framework to model realistic decision-making for security systems within resource-constrained environments.

6 | Conclusion and Future Work

In this study, a game-theoretic framework was presented to analyze the adaptive behavior of an attacker and an IDS in IoT gateways. By modeling the security interaction as a repeated game and factoring in mutual learning based on long-term payoffs, realistic dynamics of the confrontation between an attacker and a defensive system were examined. Unlike many prior studies, the operational costs of the IDS were explicitly incorporated into its decision-making process to reflect resource constraints in IoT environments.

Simulation results demonstrate that asymmetry in the learning speeds of the attacker and the IDS plays a critical role in system security stability. When the IDS adapts faster than the attacker, the attacker's behavior is effectively suppressed, lowering the probability of successful attacks. However, expanding defensive strictness does not always improve the net utility of the IDS, as resource costs can forge a practical compromise between security and efficiency. Furthermore, for intermediate learning speeds, an adaptive arms race phenomenon is observed where neither side attains a lasting edge.

As future research pathways, the proposed framework can be extended to more complex scenarios, including the consideration of multiple attackers, diverse attack types, and multi-tier defensive policies. Additionally, combining the repeated game model with reinforcement learning methods and evaluating the framework's performance in real laboratory environments or on edge hardware (such as actual IoT gateways) could enhance the applicability of the findings. These directions will facilitate the development of adaptive, lightweight IDSs for the next generation of IoT infrastructures.

Conflict of Interest

The authors declare that there are no financial, personal, institutional, or other relationships that could be perceived as influencing the work reported in this manuscript. The authors confirm that they have no competing interests regarding the publication of this article.

Data Availability

The data supporting the findings of this study are fully included within the manuscript. No additional datasets were generated or analyzed beyond those presented in the text. Further information regarding the data may be obtained from the corresponding author upon reasonable request.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. The study was conducted without external financial support, and all aspects of the research, including study design, data collection, analysis, interpretation, and manuscript preparation, were carried out independently by the authors.

References

[1] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

[2] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

[3] Naik, S., & Maral, V. (2017). Cyber security — IOT. *2017 2nd IEEE international conference on recent trends in electronics, information & communication technology (RTEICT)* (pp. 764–767). IEEE. https://doi.org/10.1109/RTEICT.2017.8256700

[4] Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future generation computer systems*, *78*, 680–698. https://doi.org/10.1016/j.future.2016.11.009

[5] Ferrag, M. A., Maglaras, L., Janicke, H., & Smith, R. (2019). Deep learning techniques for cyber security intrusion detection: A detailed analysis. *6th international symposium for ICS & scada cyber security research 2019*. BCS Learning & Development. https://www.scienceopen.com/document_file/1fa0ec04-6960-436c-8d6c-b8cacb7283fa/ScienceOpen/126_Ferrag.pdf

[6] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016). Threat analysis of iot networks using artificial neural network intrusion detection system. *2016 international symposium on networks, computers and communications (ISNCC)* (pp. 1–6). IEEE.

[7] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future generation computer systems*, *78*, 544–546. https://doi.org/10.1016/j.future.2017.07.060

[8] Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., & Hubaux, J. P. (2013). Game theory meets network security and privacy. *ACM comput. surv.*, *45*(3), 1–39. https://doi.org/10.1145/2480741.2480742

[9] Press, W. H., & Dyson, F. J. (2012). Iterated Prisoner's Dilemma contains strategies that dominate any evolutionary opponent. *Proceedings of the national academy of sciences*, *109*(26), 10409–10413. https://doi.org/10.1073/pnas.1206569109

[10] Stewart, A. J., & Plotkin, J. B. (2016). Small groups and long memories promote cooperation. *Scientific reports*, *6*(1), 26889. https://doi.org/10.1038/srep26889

[11] Zhu, Q., & Basar, T. (2015). Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems. *IEEE control systems magazine*, *35*(1), 46–65. https://doi.org/10.1109/MCS.2014.2364710

[12] Wang, L., Fu, F., & Chen, X. (2024). *Mathematics of multi-agent learning systems at the interface of game theory and artificial intelligence*. https://doi.org/10.48550/arXiv.2403.07017

[13] Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning ddos detection for consumer internet of things devices. *2018 IEEE security and privacy workshops (SPW)* (pp. 29–35). IEEE. https://doi.org/10.1109/SPW.2018.00013

[14] Roman, R., & Lopez, J. (2012). Security in the distributed internet of things. *Trusted systems* (pp. 65–66). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-35371-0_6%0A%0A

[15] Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review. *Applied sciences*, *11*(18), 8383. https://doi.org/10.3390/app11188383

[16] Tsimenidis, S., Lagkas, T., & Rantos, K. (2021). Deep learning in IoT intrusion detection. *Journal of network and systems management*, *30*(1), 8. https://doi.org/10.1007/s10922-021-09621-9

[17] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE communications surveys & tutorials*, *18*(2), 1153–1176. 10.1109/COMST.2015.2494502

[18] Rass, S., König, S., & Schauer, S. (2022). Defending against advanced persistent threats using game-theory. *PLOS one*, *20*(1), e0317848. https://doi.org/10.1371/journal.pone.0317848

[19] Chi, C., Wang, Y., Tong, X., Siddula, M., & Cai, Z. (2021). Game theory in internet of things: A survey. *IEEE internet of things journal*, *9*(14), 12125–12146.

[20] Bloembergen, D., Tuyls, K., Hennes, D., & Kaisers, M. (2015). Evolutionary dynamics of multi-agent learning: A survey. *Journal of artificial intelligence research*, *53*, 659–697. https://doi.org/10.1613/jair.4818

[21] Ghorbani, H. R., & Ahmadzadegan, M. H. (2017). Security challenges in internet of things: Survey. *2017 ieee conference on wireless sensors (ICWISE)* (pp. 1–6). IEEE. https://www.researchgate.net/profile/Hamidreza-Ghorbani-3/publication/338331684_Security_challenges_in_Internet_of_Things_survey/links/5e0d0399a6fdcc28374fe3ce/Security-challenges-in-Internet-of-Things-survey.pdf

[22] Chanal, P. M., & Kakkasageri, M. S. (2020). Security and privacy in IoT: A survey. *Wireless personal communications*, *115*(2), 1667–1693. https://doi.org/10.1007/s11277-020-07649-9

[23] LaPorte, P., Hilbe, C., & Nowak, M. A. (2023). Adaptive dynamics of memory-one strategies in the repeated donation game. *PLoS computational biology*, *19*(6), e1010987. https://doi.org/10.1371/journal.pcbi.1010987

[24] Wang, Y., Wang, Y., Liu, J., Huang, Z., & Xie, P. (2016). A survey of game theoretic methods for cyber security. *2016 IEEE first international conference on data science in cyberspace (DSC)* (pp. 631–636). IEEE. 10.1109/DSC.2016.90