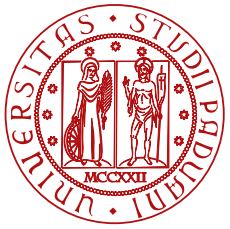

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

MASTER THESIS IN ICT FOR INTERNET AND MULTIMEDIA

Enhancing Security in Future Communication Networks Through Game Theory

MASTER CANDIDATE

Aynur Cemre Aka

Student ID 2071493

SUPERVISOR

Leonardo Badia

University of Padova

ACADEMIC YEAR
2023/2024
DATE OF GRADUATION
04.09.2024

First and foremost, I would like to thank my family for their unconditional love and support. I would also like to express my gratitude to my thesis advisor, Leonardo Badia, for teaching me since the first day of my Master's education and for always supporting me and collaborating with me on our work. A big thank you to Casa Majetti, who became my second family and helped me adjust to the country and the school when I first arrived in Italy. I would also like to extend my thanks to Mohammad, Shili, and Shayan, who stood by me during our shared struggles with coursework and always offered their support, as well as to Sezen, whom I met later but has since become like a sister to me, and to Sonia, who made the dormitory feel like home during the one year we lived together and never withheld her help and support.

Abstract

Protection of communication channels from malicious attacks is critical as the world grows more interconnected. When it comes to strategic transmissions, securing these channels demands creative solutions. This thesis focuses on using game theory to improve security when a transmitter and receiver must contend with an attacker who wants to obstruct their communication. To capture the relationship between the attacker and the transmitter, we model this situation as an adversarial setup. In particular, we explore scenarios where the struggle relates to the provision of real-time service, which the transmitter would like to be prompt and timely, whereas the adversary would like to increase the staleness of the information exchanged to worsen the quality of service. Age of Information (AoI) is used to measure the freshness or timeliness of information. When an attacker successfully breaks the communication channel for a period of time, AoI increases. This thesis investigates how the communication system's efficiency can be preserved and such disruptions reduced through the strategic decision to defend certain transmissions. We investigate the optimal strategies for the attacker and the transmitter, attempting to promote the creation of more robust communication protocols by exploring security issues in communication channels and applying game theory to these interactions. This thorough investigation of strategic defences and how well they work against network attacks can be helpful for researchers, decision-makers, and professionals working in the communication systems and information security fields.

Contents

List of Figures

List of Tables

List of Algorithms

1

Introduction

With the rapid expansion of the Internet of Things (IoT), our interactions with the surroundings have been completely transformed by enabling smooth real-time data transfer across multiple domains. Enormous numbers of devices connected to networks compose IoT systems, ranging from simple sensors and actuators to complex systems integrated into critical infrastructures like power grids, hospitals, and transportation networks [1], [2]. These systems continuously gather, analyze, and share information, allowing for unprecedented levels of automation and intelligence in various applications [3]. As daily life increasingly embraces IoT devices, the need for timely and dependable information becomes more pronounced [4].

The Age of Information (AoI) is a vital index developed to measure this timeliness. AoI quantifies the time elapsed between the generation of data and its reception by end-users, making it a crucial metric for real-time applications. Unlike latency, which measures the time taken by a packet to travel from one point to another, or throughput, which indicates how much data has been transmitted over a network, AoI specifically measures how current the data is. This makes AoI especially relevant in scenarios requiring real-time decision-making, such as autonomous vehicles, smart manufacturing, and telemedicine [5]–[7].

In recent years, the significance of AoI has gained attention in both academia and industry, particularly in applications where outdated information can lead to suboptimal or dangerous outcomes [8], [9]. For instance, in autonomous driving, where decisions

must be made within fractions of a second using the latest sensor data, a high AoI may result in delayed or incorrect responses, potentially leading to accidents [10]. Similarly, in industrial automation, where machines and processes rely on real-time data, high AoI can cause inefficiencies, downtime, or even hazardous conditions [11]. Furthermore, in patient monitoring systems, where continuous data streams are crucial for detecting and reacting to critical conditions, outdated information may result in missed diagnoses or delayed treatments [12].

As IoT networks grow larger and more complex, the management and optimization of AoI emerge as critical challenges [13]. The dynamic nature of these networks, with varying traffic patterns and intermittent connectivity, coupled with diverse applications requiring different quality of service (QoS) levels, complicates the problem [9]. This has inspired a large body of research focused on understanding the parameters that AoI depends on and how it can be optimized across various networks and applications [14]. Traditional network protocols and scheduling mechanisms often prove suboptimal for meeting these challenges, necessitating the development of new methods specifically aimed at minimizing AoI [7], [15].

1.1 Security Challenges in IoT Applications

The widespread adoption of IoT has also brought numerous security challenges. The characteristics that make IoT powerfulinterconnectedness, large-scale deployment, real-time data exchangealso make it vulnerable to various cyberattacks [1], [16]. Often, IoT devices are deployed in environments where physical and network security cannot be adequately ensured, making them easy targets for attackers [17]. Among the various security threats, jamming attacks, where an adversary interferes with update transmissions, are particularly devastating to the integrity and reliability of IoT systems [18], [19].

Jamming attacks can significantly increase AoI by causing delays or preventing the delivery of critical updates altogether [20]. Common attack scenarios involve an adversary injecting noise into the communication channel, leading to packet loss and retransmissions, which in turn increases AoI [21]. More sophisticated attacks focus on selectively jamming specific messages or time slots to maximize disruption while minimizing the chances of detection [21]. Such attacks can have drastic effects, especially in applications where real-time data is critical.

For example, in smart grid systems, where timely information about power consumption and distribution is essential for stability and efficiency, a jamming attack that increases AoI may result in suboptimal power distribution, energy loss, or even blackouts [22]. In healthcare, jamming attacks that disrupt the delivery of patient data can delay critical interventions, potentially putting lives at risk [23]. As the attack surface of IoT applications expands, protecting AoI from potential threats becomes increasingly important for ensuring the effective and proper functioning of these systems [16]. This calls for the development of strategies to mitigate the associated risks and enhance the resilience of IoT systems. Research has been conducted in areas such as physical layer security techniques, dynamic spectrum access, and game-theoretic models to understand and counter adversarial strategies [19], [24].

1.2 Research Objectives and Thesis Contributions

The main focus of this thesis is to explore AoI and security aspects within IoT networks. Specifically, it investigates how game theory can be applied as a modeling framework to analyze the strategic interactions between a sensor updating its state and an attacker attempting to disrupt these updates [25], [26]. The sensor engages in a minimization game of AoI with the adversary, who aims to maximize AoI by jamming the transmission of updates [19], [24]. The outcome of the game is determined by the simultaneous strategies of the players, despite the lack of knowledge about the adversary's moves [25].

Building upon foundational work in AoI and game theory, this thesis aims to contribute new insights into optimizing communication strategies in adversarial environments. By utilizing Nash equilibriuma strategy in which no player can improve their payoff by unilaterally changing their strategythis research seeks to develop optimal defense mechanisms that can reduce the impact of jamming attacks on AoI [19], [23]. The findings of this research have the potential to enhance the resilience of IoT networks against intentional disruptions, providing robustness and reliability in real-time systems, particularly in the face of adversarial threats [27], [28].

The main contributions of this thesis are:

- Devise an all-inclusive game-theoretic model to capture strategic interactions between IoT sensors and adversaries in the presence of jamming attacks for the reduction of AoI.

- Develop analysis for the Nash equilibrium over a range of scenarios, such as different network topologies and adversary capabilities or sensor strategies, to identify circumstances under which optimal strategies can be obtained.
- Introduce a new category of algorithms and protocols that can be realized in IoT networks to change the nature of the transmission schedules and power levels dynamically in reaction to jamming activities either detected or expected, hence minimizing the impact on AoI.
- Evaluate the proposed strategies through simulation and theoretical analysis to demonstrate their effectiveness in reducing AoI and improving the security and resilience of IoT networks.

The results of this thesis are expected to have significant implications for the design and operation of IoT networks, particularly in environments where security and real-time performance are critical. This research contributes to the development of more robust and efficient IoT systems capable of handling adversarial challenges by providing a deeper understanding of the interplay between AoI and security.

1.3 SUMMARY

This thesis takes the challenge to comprehensively study the game-theoretic methodology to tackle AoI optimization problems over communication networks in adversarial settings. The research is motivated by the key need for secure and timely information exchange in IoT systems, where disruptions, such as jamming attacks, can easily cause catastrophe in the performance of the system.

Organization:

- **Chapter 1: Introduction** - This chapter introduces the importance of secure communication channels within IoT, given the demand for timely information at every step in a decision-making process. It introduces AoI as one of the fundamental metrics with which data freshness could be assessed and points out the challenge of maintaining low AoI when adversarial threats such as jamming attacks are present.
- **Chapter 2: State of the Art** - This chapter will present a review of the existing literature with respect to AoI, jamming in wireless networks, and the application of game theory to network security. It will put into perspective how AoI has evolved as a performance metric, how IoT networks are susceptible to jamming attacks, and how game-theoretic approaches can model and mitigate such threats.
- **Chapter 3: Materials and Methods** - This methodology chapter discusses the adversarial model deployed in this work, where typically a transmitter or sensor and an adversary or jammer are in a strategic game for minimum or maximum AoI, respectively. Further elaboration is made on the system modeling, game-theoretic

analysis principles, and computational techniques used within analyzing strategic interactions by players.

- **Chapter 4: Results** - The results of the game-theoretic analysis will be provided in Chapter 4, including the identification of the optimal strategies for both the transmitter and the adversary. The performance of the proposed strategies in maintaining a low AoI in various network conditions should be simulated and theoretically analyzed.
- **Chapter 5: Conclusions and Future Work** - The last chapter summarizes the research, underlining the main contributions in optimizing AoI and network security. Besides, the prospects for future work will be discussed, which entails considering more complex scenarios of networks, developing the interaction between machine learning and game theory, and proposing advanced anti-jamming techniques.

This thesis develops a more robust and secure IoT system that gives deeper insight into strategic interactions driving AoI in adversarial environments. This is a very important result that may be used in designing robust communication protocols to efficiently mitigate the impact of network attacks on delivering, in a timely manner, critical information.

2

State of the Art

2.1 Introduction

The rapid growth of the Internet of Things in recent years has introduced a new challenge to the arena of wireless communication: how to timely and securely deliver information [1], [2], [4]. Among the various metrics developed to assess the performance of such networks, the Age of Information (AoI) has emerged as a key measure of data freshness [8]. This makes AoI an important metric in real-time applications since it quantifies the time that has elapsed since the last generated data packet was received [6], [13]. On the other hand, with the increasing attention that real-time applications have been given, this has also brought forward security issues related to wireless networks from malicious activities like jamming [20], [21], [29]. In addition, game theory applications to model and analyze strategic interactions among network entities have provided valuable insight into optimizing the Age of Information and network security [26], [30].

2.2 Age of Information (AoI)

The AoI can be said to refer to the freshness measurement of information in the context of a communication network, especially those that highly rely on timely updates. In its very core, AoI stands for the age of the time elapsed since the generation of a new

data or information update at the source until its reaching its destination for delivery. In contrast, AoI gives a holistic measure of information freshness at the receiver; this differs from metrics traditionally considered, such as latency-a measure of the time taken by a packet traveling between a sender and a receiver-or throughput, reflecting the total amount of data transmitted over a network. It is for this reason that AoI remains significant, especially when we talk about situations that demand rapid and updated decision-making based on current intelligence, as in autonomous vehicles, industrial processes, and even telemedicine.

This was the concept of AoI introduced by Kaul et al. in 2012 when this area was one of the most important developments with respect to studies concerning communication systems [8]. In this pioneering work, AoI was defined as the time that had elapsed since the last received update was generated by the source, proposing a fresh means of evaluating performance in communication networks. Unlike other conventional metrics concerning performance, AoI tackles the freshness of information needs directly; hence, it forms one of the essential considerations in designing systems where real-time information is crucial.

Kaul et al. showed that merely minimizing delay is not enough in order to guarantee information freshness [8]. They leveraged simple queuing models such as M/M/1 and M/D/1 to conduct AoI performance analysis in various network settings, showing that the AoI is not just simply related with the network delay, but also depends on update frequency and scheduling policies adopted. Their analysis showed that under certain network conditions and application demands, there indeed exists an optimal update rate that can achieve minimum AoI. This work cemented AoI as a key performance metric for real-time communication systems and set a foundation for later studies.

This seminal work has since been extended to consider various aspects of AoI in different network scenarios. Work considering extensions from this seminal paper include Kam et al. [9], which updated the AoI framework to incorporate packet deadlines into the analysis. They considered that updates are useful only if they arrive within a certain packet deadline. They suggested updating the AoI calculation to include such packet deadlines. This allowed a more articulated understanding of how AoI could be managed within systems where data had to be highly time-sensitive, for example, military communications or critical infrastructure monitoring.

More recently, in 2017, Sun, Uysal-Biyikoglu, Yates, Koksal, and Shroff considered strategic update policies for the trade-offs between immediate and delayed updates [14].

Their research introduced the concept of the "optimal stopping rule" with which an update will adopt a strategy that minimizes AoI under various network conditions. This work adopted a more nuanced view of the tradeoffs between update frequency, network delay, and AoI, shaping subsequent research investigating AoI optimization.

In 2019, Sun et al. [13] published a comprehensive survey underlining the importance of AoI for ensuring information freshness in various communication systems. Applications of AoI in domains ranging from IoT systems to vehicular networks and wireless sensor networks were discussed in the survey. They put forward that AoI plays an important role when real-time applications come into play, where consequences in terms of severity may be observed due to outdated data.

Liu and Bennis contributed to the AoI literature by tackling challenges associated with managing the tail of maximal AoI in wireless industrial networks [11]. They did this work with regard to the possible hazards brought about by very large delays to refresh information, given the nature of most time-critical applications. They made suggestions on how to deal with such extreme values of AoI while insisting that reliability and effectiveness must be guaranteed in industrial communication systems.

It was in the same year that a comprehensive analysis of AoI on the IEEE 802.11p-based networks, most used in vehicular communications, was given by Baiocchi, Turcanu, Lyamin, Sjöberg, and Vinel [10]. Their investigation really provided some insights into the effective control of AoI in a real-world vehicular network since timely information exchanges between vehicles and infrastructure play an important role in safety and efficiency. The authors discussed how such networks can maintain low AoI considering the network congestion, variable traffic pattern, and vehicle mobility.

In fact, a comprehensive introduction and survey on AoI by Yates et al. also came in 2021. The paper synthesized the current literature on AoI into a unified framework for its applications in various communication systems [6]. The authors gave importance to AoI in real-time applications, discussing its relevance in contexts like smart cities, autonomous systems, and critical infrastructure. This paper is already a seminal reference for researchers and practitioners alike, providing a comprehensive blueprint for future research in the field.

The AoI study has evolved further in time, and recently, the review by Kahraman, Köse, Koca, and Anarm in 2024 focused on the challenges and opportunities of AoI in IoT systems [27]. It aimed at the particular complexities tied to the management of AoI in

large-scale and heterogeneous IoT networks. With the increased pervasiveness of IoT technologies, the role of AoI will become ever more critical in ensuring efficient and reliable operations of such networks. Further, the authors discussed a few strategies adaptable for AoI optimization in IoT environments by mentioning adaptive update policies, dynamic scheduling, and cross-layer optimization techniques.

The ever-growing research on the extensions of AoI underlines the importance of AoI as a key metric of modern communication systems. Current studies are continually exploring new paths toward AoI optimization, keeping in consideration the challenges imposed by various network environments and applications. Further understanding of AoI can give way to the establishment of more responsive, reliable, and efficient communication systems to meet the challenges thrown by real-time data exchange in various scenarios.

2.3 Jamming in Wireless Networks

The possibility of jamming is indeed an issue that affects the effective use of wireless communication networks. It relies heavily on the dependability of device-device interaction, especially in contexts like IoT. Essentially, jamming refers to the intentional perturbation in the signal transmission initiated through an adversary, with the objective of impeding the functionality of network operations. This type of attack is critical in IoT environments where service execution heavily relies on smooth interaction among devices. A seminal contribution in this domain goes back to 2005, when W. Xu, W. Xu, M.A.B. Shirazi, and W. Trappe conducted the very first comprehensive study on the feasibility of launching and detecting jamming attacks inside wireless networks [21]. The originality of the work by the authors came from the comprehensive understanding of the operational challenges with respect to jamming. It identified a few key vulnerabilities in the wireless networks that can be used by jammers and provided a framework on which works on finding detection and mitigation techniques would be based. It remains one of the most cited original works in the field of wireless security, informing a broad array of subsequent research in light of solving the threats imposed by jamming.

In 2018, B. Li, W. Li, and R. Zhang investigated the problems of jamming in wireless relay networks, considering the possible strategies for protecting such networks from attack [20]. Their work emphasized the importance of recognizing the particular vulnerabilities of relay networks, so often used to extend the coverage and improve the reliability of

wireless communications systems.

In the context of IoT, jamming is particularly serious because most applications of IoT are critical; hence, either continuous or reliable communication is always required. R. Verma, S.J. Darak, V. Tikkiwal, H. Joshi, and R. Kumar proposed countermeasures against jamming attacks in sensor networks in 2019 [29]. They also drew emphasis on how energy-efficient approaches would help in mitigating such effects through jamming, especially concerning maintaining low AoI even in adversarial activities. They further proposed some new methods regarding power management and timing constraints that are vital in ensuring IoT networks can still work effectively even in the presence of jammers.

Another great contribution to jamming attacks was given in 2011 by Q. Zhu, W. Saad, Z. Han, H. V. Poor and T. Basar who took into consideration the combined threat of eavesdropping and jamming in wireless networks [31]. With their research, a complete analysis could be obtained about how jamming can be used along with other attacks to compromise wireless security. It was able to produce, through the study, a prudent realization of the need to establish coordinated defense mechanisms that are able to handle multiple security threats at the same time.

With modern infrastructure being integrally composed of wireless communication networks, the threat of jamming, in addition to its implications for network security and reliability, remains a very critical area of research. Strong detection and mitigation against such malicious intent will help these networks retain their very important role in providing needed communication for critical applications related to IoT, industrial automation, and beyond.

2.4 Game Theory in Network Security

Game theory is the study of mathematics and economics concerning the strategic interaction of rational decision-makers or "players" who understand that their decisions have consequences for their own payoff and also on the payoffs of others. In other words, game theory provides a formal analytical framework and prediction of behavior in situations whereby players or agents with conflicting interests realize the outcome or payoff is dependent on actions or decisions taken by others. As one of the strongest tools for modeling and analyzing different strategic situations-simplistic competitive games to complex, real-world multi-stakeholder interactions.

In network security, game theory has emerged as an essential methodology for understanding and countering adversarial behaviors within modern communication networks. Networks, in particular next-generation radio and IoT systems, have become so complex and interdependent that they are increasingly susceptible to a myriad of security threats. These threats very often involve intentional adversaries attempting to disrupt or degrade network functions by various malicious acts, including jamming attacks, DoS attacks, and data breaches. In such a context, the defenders of the network have to predict and neutralize the moves of strategic and adaptive attackers [26], [32], [33].

At first, the seminal concepts of game theory for network security were given by D. Koller and N. Megiddo in 1992, who studied the problem of solving two-person zero-sum games in extensive form [30]. Their work established the mathematical foundation for a general class of security problems that considers the computational issues associated with such games. Understanding such challenges is crucial for applying game-theoretic analysis in realistic security settings in which the interactions between an attacker and a defender can be very complicated.

Building on this work, N. Michelusi, K. Stamatiou, L. Badia, and M. Zorzi employed game theory to operate energy-harvesting devices in adversarial settings in 2012 [32]. This work, in particular, has become very helpful in IoT because most of the IoT devices use scarce energy sources. In addition, the authors presented ways for further enhancement in energy efficiency while ensuring the security of the networks and putting deep emphasis on resource management within the context of secure communication using simulations of strategic interactions among devices and their respective adversaries.

In 2013, M.H. Manshaei, Q. Zhu, T. Alpcan, T. Bacsar, and J.-P. Hubaux have given an extensive review for game-theoretic approaches to network security and privacy problems [26]. From threat responses, jamming, denial-of-service attacks, to intrusion detection, a wide range of issues are discussed in their work. The importance of this survey is that it brings to light how game theory can be applied to protect communication infrastructures from various types of attacks through the strategizing and approaches that have been designed.

In the same year, G. Quer, F. Librino, L. Canzian, L. Badia, and M. Zorzi reviewed the incorporation of game theory into Bayesian networks for inter-network cooperation [33]. Their work identified possible strategic incentives of various networks to either cooperate or compete with others for resources; this has strong implications in terms of security and

efficiency. This work is significant in multi-network scenarios where strategic actions of network players contribute to overall performance and security.

Furthering it, M. Hajji, I. M. El Emary, and M. S. Obaidat have studied a game-theoretic model for jamming attacks in UAV networks [34]. This work contributes to understanding how game theory is able to model and counteract jamming attacks, especially relevant in view of the advent of emerging technologies such as unmanned aerial vehicles. This work illustrates the wide applicability of game theory to solve security problems in various types of networks.

In 2024, the work of E. Djokanovic, A. Munari, and L. Badia made further development in using game theory in accordance with the goal of AoI minimization in distributed sources [35]. The contribution is important within the context of including AoI factors into game-theoretic models by using Harsanyi's equilibrium selection. This is particularly relevant in real-time communicating systems where information freshness needs to be preserved. Minimizing AoI in such a multi-source environment, where sources need to coordinate their actions, was proposed by the authors, along with giving new insights into strategic management of information in distributed networks.

The cumulative conclusion from these research works is that game theory is an adaptive and important tool in solving many security issues in wireless networks. Game theory contributes to the fundamentals in modeling the strategic interactions of both the attackers and defenders, an important ingredient in the design of secure and reliable communication systems. As networks become increasingly complex, and as the threat landscape continues to evolve, game theory's role in enhancing network security is a cornerstone in ongoing development: resilient communication infrastructures.

2.5 Age of Information and Jamming

The interaction of AoI with jamming in wireless networks is a very critical domain of research, having to do with the reliability and timeliness of data transmission in hostile environments. Works in this domain investigate direct impacts of jamming on AoI and establish various ways to mitigate such impacts, taking into account practical methods that may not necessarily involve game-theoretic frameworks.

Understanding how jamming affects the timeliness of information and exploring mit-

igation methods is critical for any communication system's integrity and effectiveness, particularly those relying heavily on immediacy of data.

For instance, the work done by W. Xu, M.A.B. Shirazi, W. Xu, and W. Trappe in 2005 was an exploratory study critical to present foundational insights on the feasibility of detecting and launching jamming attacks on wireless networks [21]. This work laid the foundation for developing this dissertation concerning real-world challenges emanating from jamming-efficient methods of detection and mitigation should be developed to ensure sustained network performance.

In 2018, B. Li, W. Li, and R. Zhang contributed to the study of the jamming problem in wireless relay networks and developed strategies against jamming attacks. Although their work was not explicitly oriented toward AoI, it had important implications for the general performance of the network [20]. Their contribution was related to techniques that provided the reliability of the relay nodes, which are crucial in providing data transmission. Those methods can be generalized in order to enhance AoI in situations when real-time freshness of data is of prime importance.

Building on these, the authors A. Garnaev, W. Zhang, J. Zhong and R.D. Yates in 2019 explicitly considered the effects of jamming on AoI in wireless networks [25]. The authors had analyzed the work in order to see how malicious jamming can sharply degrade information freshness, therefore creating a higher AoI. The authors also developed various helpful techniques to maintain information freshness against a jamming attack. Thus, the valuable strategies were provided for the network operator in regard to timely data delivery in hostile conditions. The authors of the study identified that the most critical challenge is to balance the mitigation of jamming along with keeping AoI as low as possible and offered practical strategies that can be applied in real-world scenarios.

More recent works have continued in this vein, discussing ways through which the increase in AoI due to jamming can be curtailed by advanced techniques. For instance, in 2015, M. Scalabrin, V. Vadori, A.V. Guglielmi, and L. Badia proposed a zero-sum game approach against jamming, although the method itself can be viewed within the broader anti-jamming approaches outside the strict game-theoretic framing [24]. Their approach highlights how AoI-optimal planning is resolutely central in the face of unrelenting jamming threats.

This study, therefore, underlines the need for devising robust anti-jamming strategies to retain information freshness or currency in wireless networks. Although these studies

separately deal with feasible and practical solution spaces, they shed light on two different important insights in maintaining system performance during jamming attacks and ensuring that critical data stay relevant and current.

2.6 Game Theory and Age of Information

The use of game theory in AoI has been a highly captivating area, especially because of the increasing demands to optimize information freshness in complex and adversarial environments. Game theory provides a strong framework necessary for modeling strategic interactions among network entities such as sensors and transmitters with possible adversaries who may have competing objectives. This framework will be quite helpful for developing an intuition of how to keep the AoI low in settings where entities have to make decisions based on others' possible moves.

The adaptation of game theory into AoI began with early work aimed at understanding the strategic interactions in communication networks in which timely information delivery is crucial. Perhaps one of the first key works is that by Nguyen et al. (2018), where the authors investigated the possibility of users sharing an interference channel to choose strategic timing for transmission with the goal of achieving minimum AoI. Their game-theoretic analysis provided insight into how the competition amongst the users could be managed to achieve overall network lower AoI [36].

Building on this, Garnaev et al. (2019) investigated the influence of jamming on AoI in wireless networks using tools from game theory. It was shown that malicious jamming can considerably increase AoI and therefore degradation of the information quality perceived by end-users. The authors formulated the problem of the interaction between jammers and network defenders as a game and derived methods to diminish the impact of jamming on AoI relevant to ensure information freshness in adversarial settings [25].

In 2020, M. Abd-Elmagid and H. S. Dhillon developed further insight by integrating deep reinforcement learning approaches with game theory methods in an AoI minimization problem for UAV-assisted networks. The considered novelty modelled the UAVs as players in a non-cooperative game, wherein each UAV learns over time to adapt its strategy in optimally selecting AoI for dynamic network conditions. This is a big stride in applying machine learning and game theory to practical implementation against realistic network scenarios [37].

Chen et al. 2021 extended this work by bringing game theory into the AoI in Gaussian multiple access channels. The paper highlights how different transmitters that utilize a given channel may update their transmission policies optimally to minimize AoI, and demonstrates in the process how game-theoretic methodology can balance out various network users with heterogeneous interests for overall better performance [38].

Bonagura et al. (2023) have further reviewed the interplay of game theory and AoI with security challenges while assessing strategic interactions that are coupled with AoI for cyber-physical systems in the context of injection of false data and jamming. Their work underlines that it is rather complicated to keep AoI low in adversarial settings, where opponents strive to actively disrupt communication processes. Treating these interactions as a strategic game, they derived the effective strategies which would minimize the impact of such an attack; very useful for critical infrastructure systems [18].

More recently, I examined game theoretic approaches with A. Buratto, S.Sadeghzadeh, and L.Badia to maintaining AoI under intensively-held conjectures of eavesdropping in dual sender networks, their contribution summarizing the ever-expanding frontiers of game theory in AoI research and demonstrating how strategic decision-making can assist in protecting the freshness of information even within devastatingly adversarial environments [39].

Indeed, as this cutting-edge field keeps evolving, emerging research now addresses how best the challenges of AoI in complexly growing networks can be met by further integrating advanced techniques in machine learning with game-theoretic models. In fact, such integration will indeed become an important milestone in the roadmap toward the design of next-generation communication systems, where the capability to keep information fresh and timely becomes a fundamental performance metric.

All these together bring into focus the prominence of game theory in AoI optimization over a wide range of network environments. By modeling the strategic interactions of network entities, analysts can determine the equilibrium strategies which effectively minimize AoI in the face of competing interests or adversarial acts. Game theory will be adopted increasingly in AoI research due to the intricately complex and intertwined nature that has come to characterize modern communication networks. In fact, the integration of game-theoretic analysis into AoI research has become highly essential for the assurance of the reliability and performance of real-time systems.

2.7 Game Theory and Jamming

The jamming attacks are considered one of the serious security threats to paralyze the wireless communication networks. The attack is performed by intentionally interfering with the network by creating interference that prohibits the legitimate users from accessing the channel. While wireless networks remain crucial in critical applications, from military operations and critical infrastructures to everyday IoT devices, developing robust strategies against such jamming has become of prime importance. Game theory offers a strong framework for modeling and analyzing strategic interactions between attackers (jammers) and defenders (network operators) and provides valuable insight into how to mitigate the impact of such attacks.

The application of game theory to jamming began with foundational work that sought to understand the strategic dynamics between jammers and network defenders. In 2011, Q. Zhu et al. explored a game-theoretic approach to both eavesdropping and jamming in next-generation wireless networks [31]. The research provided a wide framework for analyzing the interactions between multiple adversaries and network defenders. It showed how game theory could be used to formulate coordinated defense strategies, since there were multiple security threats that needed to be tackled at the same time.

Extending further, M. Scalabrin et al. (2015) proposed a zero-sum game model in wireless scenarios in order to study the strategic interaction between jammers and defenders [24]. Their work considered cases in which jammers have incomplete knowledge of the position of the network, and the contributions focused on strategic decision-making under uncertainty. The results of this work had important implications for how defenders of the network could optimally adapt their approach to reduce, as far as possible, the effectiveness of any jamming attack, even by an attacker who may have an informational advantage.

In 2018, B. Li, W. Li, and R. Zhang extended game-theoretic approach to apply in wireless relay networks, with an attack issue concerning the jamming attack [20]. The authors have focused on how effectively deployed relay nodes are critical in enhancing the coverage area and reliability of wireless networks, as this can be used strategically to neutralize the effect of jamming. The authors modeled the interaction of the jammers and the relay nodes as a strategic game and proposed several strategies that improved the resilience of the network, maintaining communication reliability even under continuous jamming.

The work of M. Hajji, I. M. El Emary, and M. S. Obaidat (2020) [34], has been continued to investigate the applicability of game theory in overcoming jamming in the context of UAV networks. They derived a game theoretic model of the interactions between UAVs and jammers with a particular emphasis on how these airborne networks could dynamically change their strategies to mitigate the effects of jamming. Their work focused on the necessity of dynamic and adaptive strategies in maintaining the operational integrity of UAV networks, which are increasingly deployed in environments that are sensitive and/or have high-stakes interests.

In 2024, E. Djokanovic, A. Munari, and L. Badia introduced the state-of-the-art application of game theory in a distributed network setup for the minimization of AoI under jamming conditions [35]. Their work presented a manner in which strategic interactions between distributed sources and jammers have been described using Harsanyi's equilibrium selection, enabling a whole new dimension toward Information Freshness in real-time communication systems. This work points to an increasingly complex set of strategic interactions in contemporary networks, with multiple objectives that are involved-such as AoI minimization and anti-jamming-that need to be balanced against each other.

The aggregate of these works using game theory and jamming shows the imperative of strategic thinking in network security. By considering jammers and defenders as players in several games, researchers have been able to develop complex strategies that can effectively anticipate and counteract diverse attempts at jamming with a view to continued assurance of the reliability and security of wireless communication networks. As jamming methods become increasingly sophisticated, so game theory is going to be even more important in creating adaptive robust mechanisms of defense.

Future research is expected to further investigate even more complex scenarios involving multi-player games with multiple jammers and defenders, incorporating machine learning techniques to enable real-time dynamic adjustment of strategies. Game-theoretic models will be developed further in including these aspects for next-generation secure wireless communications systems, where the risk from data disruption is the greatest.

2.8 Conclusion

While significant research has been carried out in each of these areas separately, the novelty in this thesis lies in its integrated approach: AoI, jamming, and game theory are

addressed together within IoT network settings. In so doing, this research joins the dots between these areas and provides a more complete framework with which to understand and mitigate impacts that adversarial actions have on information freshness. In particular, this thesis makes the following contributions:

- It develops a game-theoretic model of strategic interactions between IoT sensors and adversaries in the presence of jamming attacks with the goal of AoI minimization.
- It extends traditional game-theoretic analyses by incorporating AoI as a critical performance metric and hence providing a more holistic approach toward network security.
- It provides deep Nash equilibrium analysis over various network topologies that provide insight into conditions whereby optimal defense strategies can be reached.

In short, this thesis makes novel contributions in all of these fronts and then ties them together into one unified approach for improving IoT network security and performance. This is an integrated approach-a particularly timely proposition for the next generation of IoT systems, where the ability to ensure real-time data integrity and availability against sophisticated attacks needs to be paramount.

3

Materials and Methods

3.1 Introduction

This chapter describes the methodologies used to examine strategic interaction between an adversary (jammer) and a sensor (transmitter) in the context of AoI. The analysis is enabled under the adversarial model using game-theoretic approaches with the goal of optimizing the performance of the communication system. In this regard, the chapter explains the system model, definition of AoI, game-theoretic analysis, and computational techniques that will be used to establish and verify the results.

3.2 System Model

3.2.1 Overview of the Communication Setup

The communication model consists of a single sensor continuously updating a receiver during a normalized time interval $[0, 1]$. This model is vastly relevant to the context of Internet of Things (IoT) systems, as it ensures the freshness of information, through a minimized Age of Information (AoI), for subsequent instant decision-making. The sensor, or Player 2 as called hereafter, prepares n updates during the pre-scheduled temporal

instants, called milestones, that are equally spaced and given by:

$$\mathcal{N} = \left\{ \frac{1}{n+1}, \frac{2}{n+1}, \ldots, \frac{n}{n+1} \right\}.$$

Let those be milestones for the points in time where the sensor forwards updates to the receiver. The aim is to reduce AoI, which in this context refers to the time since the last update forwarded to the receiver and that it received successfully. Under normal operation, without any failures, it is possible to derive the baseline average AoI over the time window as:

$$\Delta_0 = \frac{1}{2(n+1)}.$$

This metric is critical in ensuring that the decisions based on the received information are made with the most current data, as discussed in [5], [6].

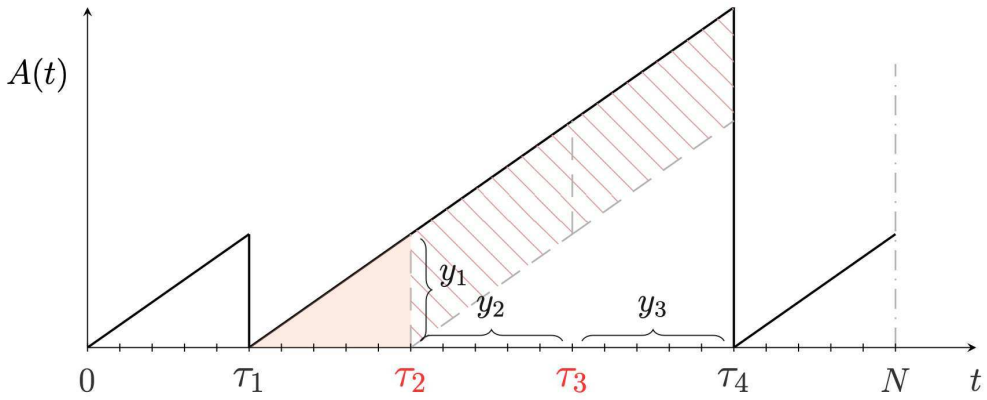

Figure 3.1: Example timeline for the AoI evolution over time. In the considered case, four transmissions are performed over a time horizon of duration N, but the second and third transmissions failed.

In this adversarial model, the jammerPlayer 1serves at trying to interrupt the sensor's communication with the receiver. The latter picks a subset of such milestones, $\mathcal{A} \subseteq \mathcal{N}$, where $a = |\mathcal{A}|$ represents the number of milestones that he jams. The jammer aims to maximize AoI at the receiver by making none of the updates reset it, which would usually drop to zero upon the successful receipt of a newly arrived update [19], [36].

In contrast, the sensor can respond to this attack by protecting a subset of milestones. The defense strategy is denoted as the set $\mathcal{D} \subset \mathcal{N}$, and involves the selection of $d =$

$|\mathcal{D}|$ milestones for protection. The protection achieved can be made by increasing the transmission power or, in general, adopting the use of anti-jamming techniques such as spread spectrum methods. The aim of the sensor is to keep the age of information as low as possible, regardless of the actions of the jammer, so that information stays fresh at the receiver [12], [40].

3.2.2 Player 1: Adversary (Jammer)

Player 1, the adversary or jammer, is strategically positioned to disrupt the communication between the sensor and the receiver. In the context of IoT and cyber-physical systems, the role of the jammer is particularly critical because it targets the Age of Information (AoI), a key metric that measures the freshness of the data received by the receiver. The adversary's objective is to increase the AoI at the receiver by selectively jamming a subset of the milestones, denoted as $\mathcal{A} \subseteq \mathcal{N}$, where $a = |\mathcal{A}|$ represents the number of milestones chosen for jamming.

This also forms a choice of the milestones, and the adversary chooses them in such a way as to obtain maximal disruption through the maximal-induced delay on information updates. The delay added to the age of information might end up in taking important decisions based on outdated information and, hence, reducing the dependability and safety of the system. Various scenarios have been considered for the effectiveness of these jamming methods: quantum communication schemes and wireless networks-both point to a strong impact of such malicious activities on the overall performance of a system [19], [24], [36].

The jamming device can then implement various types of strategies in practical settings to achieve this goal, including power-constrained jamming, where the adversary has to carefully allocate resources to jam a small set of milestones, or probabilistic jamming, where the adversary creates ambiguity by randomly jamming sets of milestones. These methods are found to work effectively, particularly in an environment with limited sensor defensive strength that limits its power in attack prediction and counteraction. As such, Verma et al. [29] argue that the ability to intentionally interfere with specific links of communication could significantly reduce the quality of service in IoT network applications, with higher AoI characterizing disqualification and reduced operational function of the system.

Moreover, the strategic nature in jamming requires an understanding of the potential defense mechanism of a sensor. The adversary must be one step ahead of the sensor to effectively bypass the defenses and maximize AoI. This game-theoretic approach to jammingwherein an adversary and sensor are involved in a zero-sum gamehighlights that managing AoI in networked systems is a highly challenging task with high stakes [19].

3.2.3 Player 2: Transmitter/Sensor

The transmitter or, in other words, Player 2, plays an important role in keeping the information at the receiver fresh by sending updates across the communication network. In such an adversarial environment, the main objective of the sensor will be the minimization of AoI by ensuring timely arrivals of updates at the receiver. This sensor works under resource constraints which limit its protecting ability from all the communication milestones which may come under jamming attack. Therefore, it has to wisely choose a subset of the milestones to defend which is denoted by set $\mathcal{D} \subset \mathcal{N}$, such that $d = |\mathcal{D}|$ gives the number of defended milestones.

It is therefore crucial that the sensor's defensive strategy operates to prevent the attacker from pushing up AoI. By selecting the right milestones to defend, the sensor is sort of guaranteed that the most important updates cannot get jammed, which in turn keeps the AoI low. This becomes an important consideration when it comes to use-cases that require real-time data such that decisions can be made on the application layer itself, e.g., industrial automation, healthcare, and smart grid systems. In these applications, a higher AoI may allow for decisions based on information that by this time may have already become outdated and which can subsequently lead to severe operational inefficiencies or safety hazards [7], [27].

The defense against these milestones can take multiple dimensions, including increasing transmit power, frequency hopping, and spread spectrum. Each of these methods is highly dependent on resource limitations of the sensor. For example, while increased transmission power may effectively cross jamming at some thresholds, it has a negative implication on energy consumption that could be limiting in battery-powered IoT devices [25]. Similarly, the spread spectrum techniques can make the jamming more difficult or completely impossible if the signal is spread over a larger bandwidth. On the other hand, the implementation of these techniques may involve more complex hardware and software

settings that might strain the resources of the sensor as well.

Its decisions on which milestones to defend would thus be based on the sensor's perception of what an opponent might attempt. In this context, the sensor needs to be able to reasonably predict which milestones are most likely to get jammed so that it optimizes its strategy of defense for those critical points. This anticipation forms a considerable constituent of the game-theoretic model wherein both players make the best decisions based on expectations from the opponent [19].

In other words, the sensor's job is not only to forward updates but also to protect, effectively, the most important updates from potential jamming attacks. It can significantly minimize the AoI by doing this and ensure the freshness of information received by the end user. This makes the interaction between the sensor and the jammer a strategic issue of paramount importance, especially when robust defense mechanisms become an important need for protecting the integrity and timely delivery of communication in IoT and other networked systems [5], [27].

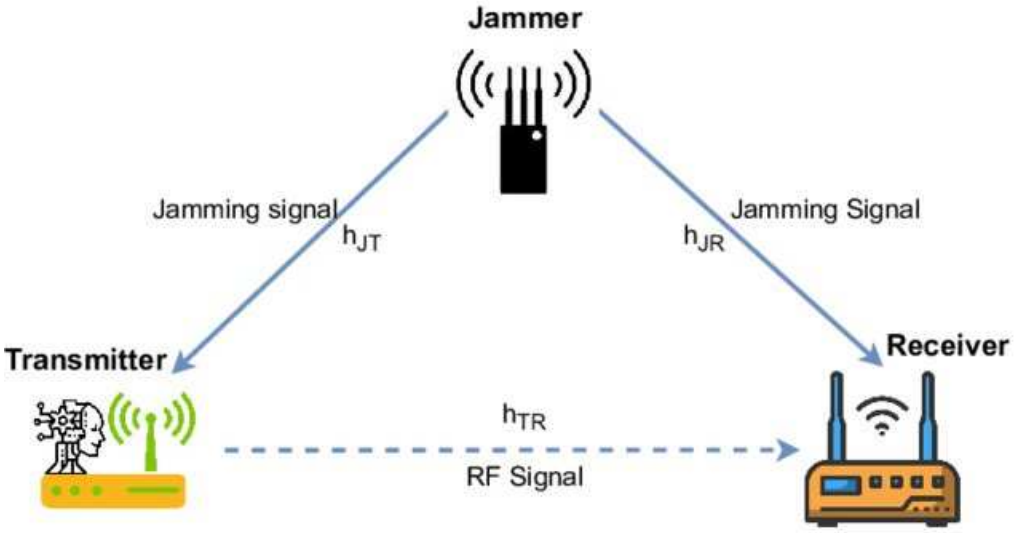

Figure 3.2: System topology is composed of the transmitter, receiver, and jammer. The transmitter tries to communicate with the receiver in the presence of a jamming attack [41]

3.2.4 Player Strategies: Attack and Defense

In this model, both an adversary (Player 1) and a sensor (Player 2) are resource-bounded, meaning they can only select a limited number of milestones to attack or defend. The set $\mathcal{A} \subset \mathcal{N}$, selected by the adversary, is an attack set with $a = |\mathcal{A}|$ milestones selected for jamming. Similarly, the defense set $\mathcal{D} \subset \mathcal{N}$ is the set of $d = |\mathcal{D}|$ milestones that the sensor chooses to defend.

This choice of strategy is literally at the heart of the game-theoretic investigation for AoI. On this account, although the adversary will always try to maximize AoI by distorting the communication at the most critical checkpoints, the sensor will try to minimize AoI by protecting the critical points. This sets up a zero-sum game at equilibrium, since one player's gain in increasing the AoI corresponds to another player's loss and vice versa.

Thus, the problem is combinatorial: each player needs to choose an optimal subset of milestones out of the total set to attack and defend. In particular, the problem becomes increasingly hard as the number of milestones increases because the number of combinations of possible attacks and defenses grows exponentially. For example, since there are n landmarks, then the number of possible attack combinations for the adversary is given by the binomial coefficient $\binom{n}{a}$, while the number of combinations that the sensor can make in defense is $\binom{n}{d}$.

In such a game, each player's strategy would involve a look at all sets of attack and defense combinations against the gains or losses from each set. The game-theoretic method could pursue the best strategy of both players; for example, solving for the Nash Equilibrium, wherein no player can unilaterally improve his or her payoffs assuming the strategy the opponent decides upon [11], [33], [40].

3.2.5 Age of Information (AoI) Calculation

AoI is a critical metric reflecting the freshness of the information received by the receiver. The baseline average AoI, assuming no jamming, is calculated as:

$$\Delta_0 = \frac{1}{2(n+1)}.$$

Algorithm 1 Calculate Attack and Defense Combinations

Require: $n \geq 0$ ▷ Total number of milestones
Require: $a \geq 0$ ▷ Number of milestones to attack
Require: $d \geq 0$ ▷ Number of milestones to defend
Ensure: $attackCombCount$ ▷ Number of possible attack combinations
Ensure: $defenceCombCount$ ▷ Number of possible defense combinations
Ensure: $attackCombinations$ ▷ List of possible attack combinations
Ensure: $defenceCombinations$ ▷ List of possible defense combinations

if $a > n$ **then**
    error "Attack count cannot be greater than the number of milestones."
end if
if $d > n$ **then**
    error "Defense count cannot be greater than the number of milestones."
end if
$attackCombCount \leftarrow$ calculate number of combinations($\binom{n}{a}$)
$defenceCombCount \leftarrow$ calculate number of combinations($\binom{n}{d}$)
$attackCombinations \leftarrow$ generate all possible combinations of a items from n items
$defenceCombinations \leftarrow$ generate all possible combinations of d items from n items
return $attackCombCount$, $defenceCombCount$, $attackCombinations$, $defenceCombinations$

If jamming is successful, the AoI increases over time until the next successful update, leading to an increased AoI, given by:

$$\Delta = \Delta_0 + \sum_{k \in \mathcal{K}} \frac{k^2}{(n+1)^2},$$

where $\mathcal{K}$ represents the set of intervals with consecutive successful jamming attacks. This metric captures the impact of both the number and sequence of successful jamming events on the AoI [6], [42].

3.3 Game-Theoretic Analysis

3.3.1 Zero-Sum Game Framework

The interaction between the adversary (Player 1) and the sensor (Player 2) is modeled as a zero-sum game, where the adversary's gain is the sensor's loss, and vice versa. This

game is formally represented as:

$$G = \{P, \mathcal{S}, U\}$$

where:

- $P = \{A, D\}$ represents the players, with A as the adversary (Player 1) and D as the sensor (Player 2).
- $\mathcal{S} = \{\mathcal{A}, \mathcal{D}\}$ denotes the strategy sets, where $\mathcal{A}$ and $\mathcal{D}$ are the sets of milestones chosen by the adversary and the sensor, respectively.
- $U = \{\Delta(\mathcal{A}, \mathcal{D}), -\Delta(\mathcal{A}, \mathcal{D})\}$ is the utility function, with $\Delta(\mathcal{A}, \mathcal{D})$ representing the AoI based on the strategies chosen by the players.

This framework is essential for analyzing the strategic interactions between the players and is grounded in foundational works on game theory and its applications in network security [26], [30].

3.3.2 Nash Equilibrium and Strategy Optimization

The Nash Equilibrium (NE) is an important concept in game theory and refers to a stable state in a strategic game where no player has an incentive to change its strategy. In the current study, a strategic game which occurs between an enemy and a sensor (both of them use strategies in order to maximize given objective functions) is taken into consideration. In fact, here the adversary is intending to maximize AoI to the sensor by launching attacks, while the sensor is focusing on minimizing AoI through defense mechanisms. Mathematically, the NE is found by solving:

$$\min_{\mathcal{D} \subset \mathcal{N}} \max_{\mathcal{A} \subset \mathcal{N}} \Delta(\mathcal{A}, \mathcal{D}),$$

where $\Delta(\mathcal{A}, \mathcal{D})$ is the AoI resulting from the adversary's attacks and the sensor's defenses. The NE represents the most stable and optimal strategies for both players in this adversarial setup [5], [32].

It lies in this competitive setup that the NE represents a pair of strategies $(\mathcal{A}^*, \mathcal{D}^*)$, where no player can do better by deviating from one of the strategies, assuming that the strategy of the drifting player is fixed. The computation of NE is in finding out the optimal mixed strategies; this may sometimes call for iterative algorithms, linear programming

approaches, among others in solving the min-max optimization problems. Essentially, the general steps taken in computing the Nash Equilibrium theoretically include:

1. **Specify the Payoff Functions:** It should be clear what the payoff function of each player is. In this work, the payoff function of the adversary is the AoI, $\Delta(\mathcal{A}, \mathcal{D})$, and he is looking to maximize it, whereas the payoff of the sensor would be the negation of AoI that he wants to minimize.
2. **Payoff Matrix Construction:** With the few selected discrete strategy sets, a payoff matrix with all entries is made, giving the outcome corresponding to any particular pair of attacking and defending strategies. This matrix is the basic step to determine the strategy/s, which is/are optimal.
3. **Identify Best Responses:** For each possible strategy of the opponent, the sensor identifies its best responses and vice versa. A best response is a strategy from which a player receives its maximum payoff assuming a response from the opponent.
4. **Iterate to Convergence:** Let, with an algorithm like Iterative Best Response or Gradient Descent, iteratively change strategies at every step so that no player can increase their payoff by unilaterally changing their strategy. In this process, the algorithm converges to Nash Equilibrium.
5. **Verify Stability:** After receiving the above-mentioned combined solution set, check whether the resultant strategy profile fulfills the Nash Equilibrium conditions, under which no player has a profitable deviation from the others regarding strategy selection.

In the area of the AoI, Nash Equilibria advise the most stable and optimal strategies of the adversary and sensor to strike a balanced tradeoff between the effectiveness of attack and efficiency of defense. These equilibria are necessary in developing robust systems able to keep AoI low even under adversarial actions.

Different works have explored the application of NE in AoI optimization problems, underlining its importance in networked systems, wireless communications, and cyber-physical systems, among others. For example, Uysal et al. [5] addressed the role of semantic communication in reducing AoI, while in one of my research papers conducted with Badia, Duranoglu Tunc, Bassoli, and Fitzek [19] we analyzed strategic interactions over AoI in quantum communication systems and demonstrated practical implications of Nash Equilibria regarding information freshness.

Such works as that done by Zhang et al. [40], have extended the NE analysis up to heterogeneous traffic in wireless networks and placed the complication and necessity of AoI scheduling in optimal ways in centre stage for secure communications. The use of NE in such cases is therefore the dual benefit of having a theoretical framework in understanding strategic interactions and getting practical solutions to real-world AoI optimization.

3.3.3 Scenario Analysis and Strategic Variations

Many more scenarios are analyzed by varying the parameters a (number of attacks) and d (number of defenses) as well as varying conditions in the network. These help to find out in what way changes in strategies of attack and defense affect AoI on the whole. This also considers the impact of diverse network topologies and adversary capabilities for identifying the best defense strategies under a variety of given conditions [12], [43].

3.4 Computational Techniques and Simulations

3.4.1 MATLAB Implementation for AoI Calculation

In this study, MATLAB was used to implement the Age of Information calculations. These included determining AoI values for each potential attack-defense strategy combination over the entire time horizon by iterating through all possible strategy combinations. For each combination, the impact on the time intervals between updates was assessed by considering successful attacks and defenses, leading to the calculation of AoI. Additionally, the implementation computed the number of possible attack and defense combinations based on the total number of milestones, attacks, and defenses. The output was matrices representing the AoI for each strategy combination, which were then used for game-theoretic analysis [11], [22], [28].

Explanation:

- **Initialization**:
  - *Area Calculation*: The total "area" is computed as per the number of milestones plus one. It is this area that is used for the purpose of normalizing the AoI contributions.
  - *AoI Initialization*: Let the AoI at the beginning be zero and the AoI be accumulated over the iterations.
  - *Small Triangle*: Calculate a small constant, small_triangle, which is the minimum contributing to AoI in cases where the attacks fail. This is the supposedly idle increase in AoI with time elapsing.
  - *Counter*: Set a counter to zero with the purpose of maintaining the number of consecutive successful attacks.

- **Iteration Over Milestones:**

Algorithm 2 Calculate Single AoI

Require: $horizonCount \geq 0$, $attacks$ (list of integers), $defenses$ (list of integers)
Ensure: AoI (calculated Age of Information)

$area \leftarrow (horizonCount + 1) \times (horizonCount + 1)$ ▷ Calculate the total area based on the number of milestones
$AoI \leftarrow 0$ ▷ Initialize the Age of Information (AoI) to 0
$small\_triangle \leftarrow \frac{1}{area \times 2}$ ▷ Smallest possible contribution to AoI when no attacks are successful
$counter \leftarrow 0$ ▷ Initialize a counter to track consecutive successful attacks
for $i \leftarrow 1$ **to** $horizonCount + 1$ **do** ▷ Iterate over each milestone
    $successful\_attack \leftarrow (i \in attacks) \wedge (i \notin defenses)$ ▷ Check if the current milestone is successfully attacked (attacked but not defended)
    if $successful\_attack$ **then** ▷ If the attack is successful
        $counter \leftarrow counter + 1$ ▷ Increment the counter for consecutive successful attacks
    else
        if $counter > 0$ **then** ▷ If there were previous successful attacks
            $AoI \leftarrow AoI + \frac{(counter+1) \times (counter+1)}{area \times 2}$ ▷ Add the AoI contribution for the block of successful attacks
            $counter \leftarrow 0$ ▷ Reset the counter after processing the block of attacks
        else
            $AoI \leftarrow AoI + small\_triangle$ ▷ If no successful attacks, add the minimum possible AoI contribution
        end if
    end if
end forreturn AoI ▷ Return the calculated Age of Information (AoI)

  - Iterates over milestones from 1 to `horizonCount + 1`.
  - *Successful Attack Check*: for every milestone, it checks whether the milestone is attacked and not defended, i.e., whether it is a successful attack or not.
  - *Counter Increment*: In case of a successful attack, the counter should be incremented.

- **Handling Consecutive Successful Attacks**:

  - *Block Processing*: If the current milestone is not successfully attacked, and there was any block of consecutive successful attacks, then AoI contribution for this block is calculated and added to the total AoI. AoI contribution is taken to be proportional to the square of block length, and normalized over the area of the entire total.
  - *Reset Counter*: Reset the counter to zero after a successful attack block.
  - *Small Triangle Contribution*: Add the small baseline AoI contribution, `small_triangle`, if no successful attacks occurred at this milestone

- **Final Return**:
  - Finalizing the total AoI has to be done for all the milestones iterated.

Summary: The AoI will be the result of the systematic calculation in this pseudocode, which takes a sequence of attacks and defenses, with a baseline for periods of no successful attack. The consequential sequence of successful attacks should cause both the frequency and the magnitude of disruption by the attacker to be properly reflected in the AoI.

Algorithm 3 Find Nash Equilibrium for AoI Game

Require: $payoffMatrix$ (matrix), $tol \geq 0$ ▷ Tolerance for equilibrium detection
Ensure: $nashEquilibrium$ (list of tuples), $strategies$ (list of mixed strategies)

$numStrategiesA \leftarrow$ `number of rows in` $payoffMatrix$ ▷ Number of strategies for Player 1 (adversary)
$numStrategiesD \leftarrow$ `number of columns in` $payoffMatrix$ ▷ Number of strategies for Player 2 (sensor)
$nashEquilibrium \leftarrow []$ ▷ Initialize list to store Nash Equilibria
$strategies \leftarrow []$ ▷ Initialize list to store mixed strategies
for $i \leftarrow 1$ **to** $numStrategiesA$ **do** ▷ Iterate over all possible strategies for Player 1
    for $j \leftarrow 1$ **to** $numStrategiesD$ **do** ▷ Iterate over all possible strategies for Player 2
        $rowPayoff \leftarrow payoffMatrix[i, :]$ ▷ Payoffs for Player 1 against all strategies of Player 2
        $colPayoff \leftarrow payoffMatrix[:, j]$ ▷ Payoffs for Player 2 against all strategies of Player 1
        $maxRowPayoff \leftarrow$ `max`$(rowPayoff)$ ▷ Maximum payoff for Player 1
        $minColPayoff \leftarrow$ `min`$(colPayoff)$ ▷ Minimum payoff for Player 2
        if $payoffMatrix[i, j] \geq maxRowPayoff - tol$ **and** $payoffMatrix[i, j] \leq minColPayoff + tol$ **then**
            $nashEquilibrium \leftarrow nashEquilibrium + [(i, j)]$ ▷ Add the strategy pair (i, j) to the list of Nash Equilibria
            $strategies \leftarrow strategies$+[(`mixed strategy for Player 1 at` i,`mixed strategy` ▷ Store the corresponding mixed strategies
        end if
    end for
end for
    return $nashEquilibrium, strategies$ ▷ Return the list of Nash Equilibria and the mixed strategies

Explanation:

- **Initialization**:

  - *Number of Combinations*: The number of possible attack and defense combinations are computed with the `size` function which returns the number of rows of the `attackCombinations` and `defenseCombinations` matrices. It gives the total number of strategies that each player can decide on.
  - *Matrix Initialization*: Two matrices are created:
    * `AoI_matrix`: An empty matrix, which will contain each possible combination of attack-defense pairs and its AoI.
    * `AoI_values`: A matrix of zeros with a dimensionality equal to the number of attack-defense combinations. This matrix will store only the calculated AoI values for every combination.

- **Nested Iteration Over Combinations**:

  - This algorithm makes use of a two nested loop to iterate over all attack and defense combinations.
  - For each pair of combinations:
    * *AoI Calculation*: Calculate the AoI for this attack and defense combination using the function `calculate_single_AoI` with the given `horizonCount` and current attack and defense combinations.
    * *Store AoI in Values Matrix*: The calculated AoI is stored in the corresponding entry within the `AoI_values` matrix.
    * *Update AoI Matrix*: The current attack combination, the defense combination, and the calculated AoI are appended as a new row to the matrix `AoI_matrix`. This matrix will keep the record of all the combinations and their AoI values.

- **Final Return**:

  - Returns, after processing all combinations, two matrices by the algorithm:
    * `AoI_matrix`: All attack and defense combinations with their AoI values.
    * `AoI_values`: A matrix containing only the AoI values, indexed by the combination indices of attack and defense.

Summary: This pseudocode is efficient in calculating the AoI for each possible combination of attack and defense strategies over the given time horizon. This allows the algorithm, after fully running from top to bottom, to store into matrices under what conditions the AoI is dependent. These matrices can be used for further game-theoretic study, such as solution concepts or optimal strategies for both players.

Attacker / Defender	**(1,2)**	**(1,3)**	**(1,4)**	**(2,3)**	**(2,4)**	**(3,4)**
(1,2)	0.10	0.14	0.14	0.14	0.14	0.22
(1,3)	0.14	0.10	0.14	0.14	0.18	0.14
(1,4)	0.14	0.14	0.10	0.18	0.14	0.14
(2,3)	0.14	0.14	0.22	0.10	0.14	0.14
(2,4)	0.14	0.18	0.14	0.14	0.10	0.14
(3,4)	0.22	0.14	0.14	0.14	0.14	0.10

Table 3.1: AOI / Utility values for Horizon 4, Attack = 2, and Defense = 2. Rows represent the attacker's strategies, and columns represent the defender's strategies.

3.4.2 Python Implementation for Game-Theoretic Analysis

Game-theoretic analysis played an important role in treating the adversary versus sensor strategic interaction with a view to AoI minimization and maximization. The work was implemented in Python, exploiting the powerful libraries available for combinatorial calculations and matrix operations. The Python version emulates the MATLAB code, adding flexibility and the ability to execute even more complicated computations. The process starts with the generation of all combinations of attacks and defences using combinatorial methods. These will, in turn, be used to create a strategy space for both players, in which the adversary tries to maximize AoI, while the sensor tries to minimize it. Python is a very good language to perform numerical computations, especially with the help of libraries such as NumPy and SciPy, through which the above-mentioned computation of combinations and analysis of outcomes has been performed. Once the strategy space was defined, each pair of attack and defense strategies had their AoI payoff calculated, and the payoffs were obtained in the zero-sum game matrix. Further, the payoffs yielded a matrix analyzed by game-theoretic tools to obtain the Nash Equilibrium. The Nash Equilibrium is one of the stable states of the game in which no player can unilaterally change their strategy to improve their payoff, given the strategy of the other player [18], [27], [42]. In this context, the Nash Equilibrium was found by using a mixed-strategy approach, whereby players randomize over their sets of available strategies with some specific probabilities. Such an approach is useful in those games where pure strategies do not yield a stable solution. It indicates, by computing the equilibrium, the way of optimally distributing the strategies for both the adversary and the sensor to make the communication system robust against adversarial actions. These results were demonstrated by plotting the AoI matrices and showing the Nash equilibrium. That showed the effectiveness of applying

different strategies in different conditions. This dual implementation in MATLAB and Python allowed the cross-verification of results to make sure that AoI calculations and solutions of Nash Equilibrium are consistent and reliable.

Algorithm 4 Find Nash Equilibrium for AoI Game

Require: payoffMatrix (matrix), tol ≥ 0 (tolerance for equilibrium detection)

Ensure: nashEquilibrium (list of tuples), strategies (list of mixed strategies)

```
numStrategiesA ← number of rows in payoffMatrix
numStrategiesD ← number of columns in payoffMatrix
nashEquilibrium ← []
strategies ← []
for i ← 1 to numStrategiesA do
    for j ← 1 to numStrategiesD do
        rowPayoff ← payoffMatrix[i, :]
        colPayoff ← payoffMatrix[:, j]
        maxRowPayoff ← max(rowPayoff)
        minColPayoff ← min(colPayoff)
        if payoffMatrix[i, j] ≥ maxRowPayoff - tol and payoffMatrix[i, j] ≤ minCol-
Payoff + tol then
            nashEquilibrium ← nashEquilibrium + [(i, j)]
            strategies ← strategies + [(mixed strategy for Player 1 at  i,
mixed strategy for Player 2 at  j)]
        end if
    end for
end for
    return nashEquilibrium, strategies
```

Explanation:

- **Initialization**:
  - *Number of Strategies*: The number of strategies that each player has can be initialized based on the dimensions of the payoff matrix.
  - *Lists Initialization*: Two empty lists `nashEquilibrium` and `strategies` are initialized to store the Nash Equilibria and their corresponding mixed strategies.

- **Nested Iteration Over Strategies**:
  - It plays through every possible pair of strategies (i, j) where i is a strategy of player 1 (the Adversary), and j is a strategy of player 2 (the Sensor).
  - For the given pair of strategies:
    * *Payoff Extraction*: The payoffs for Player 1 across all strategies of Player 2 and for Player 2 across all strategies of Player 1.
    * *Max/Min Payoffs*: Maximum payoff for Player 1: (`maxRowPayoff`), Minimum payoff for Player 2: (`minColPayoff`). These are very important values in the context of figuring out whether the current strategy pair is a Nash Equilibrium.

- **Nash Equilibrium Check**:
  - The payoff of the current strategy pair (i, j) must satisfy the following two conditions:
    * The payoff for Player 1 playing strategy i should be close to or equal to the maximum payoff, which is attainable with the strategy played by Player 2.
    * The payoff for Player 2 when playing strategy j would have to be at least less than or equal to the minimum payoff that can be picked up by Player 1's strategies.
  - If both are met, within a tolerance, add strategy pair (i, j) to the list of Nash Equilibria.
  - Store the respective mixed strategies for post-analysis as well.

- **Final Return**:
  - Once the algorithm has evaluated all possible pairs of strategies, it would report back the list of Refinery of Nash Equilibria and the respective mixed strategies.

Summary: This is a straightforward pseudocode to derive simple Nash equilibria in the game-theoretic analysis of AoI. This algorithm sequentially tests all possible pairs of strategies to verify whether they are in the Nash Equilibrium. It will return all strategy profiles that were stablemeaning no player will have an incentive to unilaterally change their strategy. Positive results of mixed strategies would provide stronger analyses where pure strategies are unavailable. The results would be important for understanding how both players should obtain an optimal distribution of their resources to maximize or minimize the AoI.

3.5 Applications and Implications

The implications for the design and functioning of secure, resilient communication systemsparticularly in IoT networks, where timely information delivery is the keyof such findings are critical. With AoI still considered an emergent metric for the assessment of data freshness in communication systems, the understanding on how adversarial impacts on AoI can be mitigated has to be ensured for the effectiveness of modern networks.

3.5.1 Enhancing IoT Network Security

The IoT networks are representative of those contemporary systems whose functioning relies on the very essence of continuous and super-fast data exchange; therefore, they are very sensitive to delays induced by jamming attacks. In this regard, game-theoretic strategies derived from this study have set a path for the development of advanced anti-jamming techniques that will be deployed to secure these networks. By amodelling the interaction with an adversary, a jammer and that of a sensor, a transmitter, as a zero-sum ame, the present study allows identification of optimal defenses that minimize recently introduced, the age of information, in persistent attack scenarios [19], [32]. This is particularly important since IoT finds increasing usage in various critical applications, such as healthcare, industrial automation, and smart cities. In such environments, even a small dislocation in information circulation may go all the way to causing serious consequences, which range from loss of operational efficiency to the safety of people. Therefore, these findings of the game-theoretic analysis can be used to devise resource allocation policies first and foremost for defending the most critical communication links against jamming and hence to increase overall resilience in IoT networks [5], [40].

3.5.2 Development of Anti-Jamming Techniques

These findings of this work could also provide insight into the design of anti-jamming techniques that can be tailored to the various needs of the different systems. For instance, the adoption of mixed strategies in game theory would result in the development of probabilistic defense mechanisms where the sensor would randomly change its transmission parameters-from frequency hopping to power level switching-with the view to confusing

the jammer. This will significantly reduce the power of jamming attacks by the adversary, since it will be very difficult to predict the sensor defense actions.[24], [29]. Another important point is that the strategic distribution of rare resources-energy or bandwidth-such that the most probable points of attack are protected, as revealed by the Nash Equilibrium analysis, allows the communication system to be resilient against sophisticated jamming strategies. Such a setting is particularly important in scenarios where the sensor operates under tight power constraints, like in battery-powered IoT devices [20], [25].

3.5.3 Broader Impact on Networked Systems

The implications of this research go well beyond IoT to all those networked systems where AoI is a critical performance metric. For instance, CPS relies on timely data delivery for control and monitoring in real time; hence, the capability of maintaining low AoI against adversarial interference is crucial in guaranteeing stability and reliability. These strategic interaction models developed in this work can be employed for the optimization of AoI in various CPS application scenarios such as smart grids, autonomous vehicles, and industrial control systems [18], [26]. Moreover, it is more than likely to yield strong cross-verification of results by performing the analysis in a dual mode involving both MATLAB and Python. Hopefully, it will serve as an indication of the flexibility of this game-theoretic approach in dealing with complex scenarios relating to the real world. The developed approach is, therefore, cross-platform compatible to ensure smooth integrability of the proposed strategies with other existing communication protocols and, thus, with no difficulty being adopted in operationally varied environments [11], [27].

4

Results

This section provides a thorough examination of the outcomes and conclusions. The main goals, which center on optimizing the Age of Information (AoI) and negotiating the strategic choices of the transmitter and the adversary, have produced a number of notable results.

4.1 Impact of Number of Nash Equilibria

The number of Nash Equilibria (NE) obtained from the different time horizons sheds light on the complexity of the strategic interaction between the transmitter and the adversary. This section synthesizes the implications of the number of Nash equilibria on the game dynamics, with a focus on the scenarios with different numbers of attacks and defenses.

We depict the number of Nash equilibria for different time horizons in Figures 4.1 and 4.2. These plots give an indication of how the number of attacks and the number of defenses impact the number of Nash equilibria.

It is obvious from the figures that with the increase in the length of the time horizon, the number of Nash equilibria shows an increasing trend. For instance, the game settings with relatively shorter horizons-like a 2- or 3-milestone-game setup-end up showing fewer Nash equilibria than that of longer horizons-for example, 4- or 5-milestone-game setups.

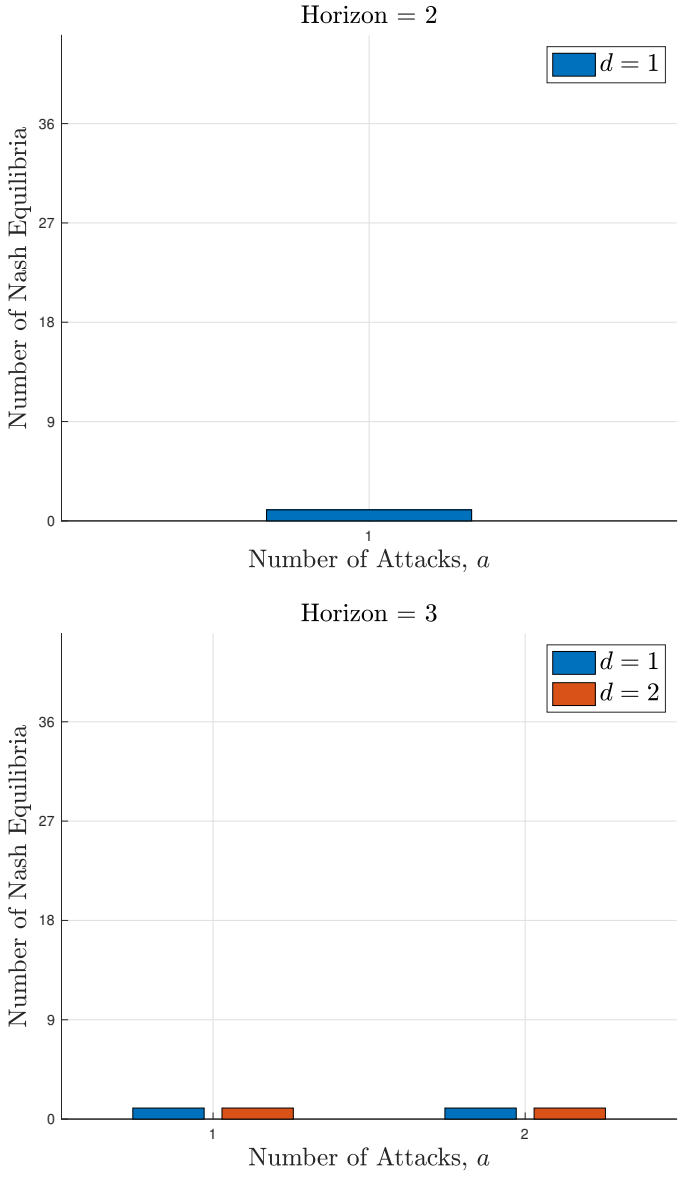

Figure 4.1: Number of Nash equilibria found for horizons 2 and 3.

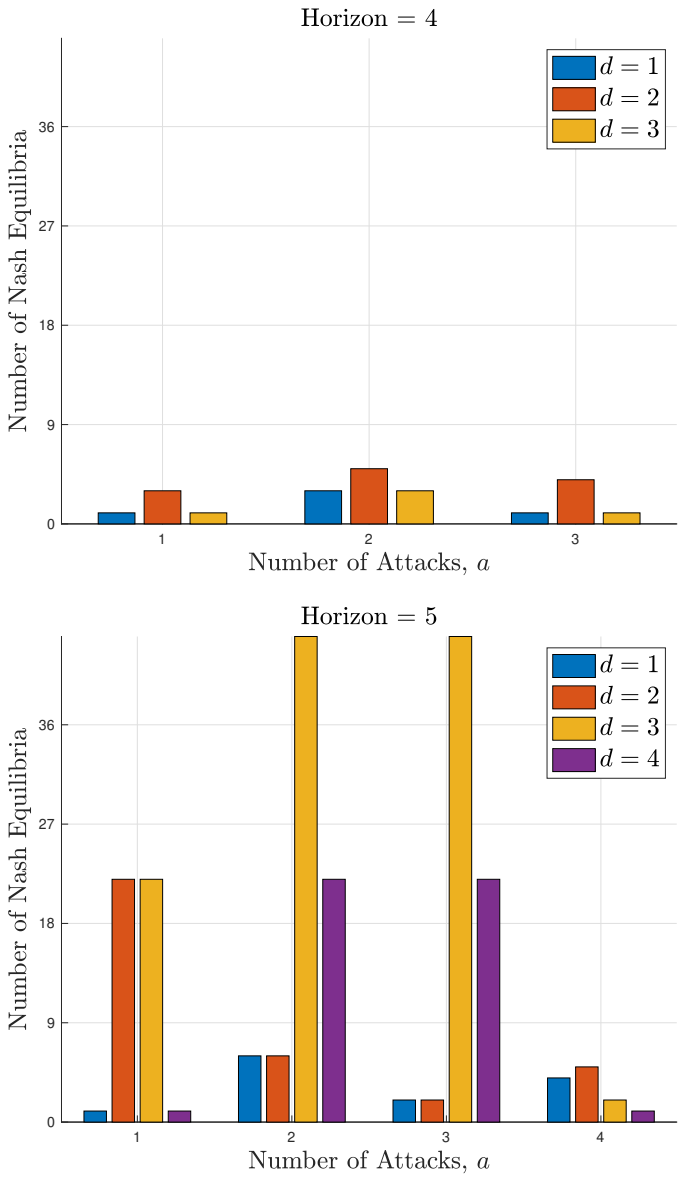

Figure 4.2: Number of Nash equilibria found for horizons 4 and 5.

It seems to indicate that with regard to quantity, as the sets of strategic options available for both players increase, the game thereby becomes more complex, resulting in more equilibria.

This finding of greater numbers of Nash equilibria as the horizon lengthens does indeed demonstrate that a longer time horizon makes the game strategically richer and nuanced. Such an increase is a reflection of greater variability in the outcomes possible, since both transmitter and adversary have more opportunities to optimize over their strategies.

4.2 Payoff Analysis

The following sections present the analysis of game value at Nash Equilibrium (NE) for cases with different time horizons. In this regard, the results depict several figures and tables based on the impact of the number of attacks and defenses on AoI.

4.2.1 Impact of Number of Defenses

Figure 4.3 plots the number of defenses deployed by sensor versus the game value in Nash Equilibrium. It plots it for different number of attacks by the adversary. The x-axis is the number of defenses and the different curves correspond to the number of the attacks. Game value, which is the average AoI, decreases as number of the defenses increase. This outcome aligns with theoretical expectations whereby increasing defenses serves to reduce the strategic effect of the adversary's jamming. Notably, it is when the number of defenses starts to approach and surpass the number of attacks that the game value experiences a much larger decrease. This agrees with such findings showing that the strategic advantage tends to favor the defender when they have equal or more strategic options compared to the attacker. This underlines the need to make available adequate defensive resources that can neutralize attempts at jamming by an adversary.

4.2.2 Impact of Number of Attacks

Figure 4.4 puts a wider angle of view on how the number of attacks and defenses is interacting in determining the game value at Nash Equilibrium. The x-axis gives the number of attacks, while the different curves represent different numbers of defenses.

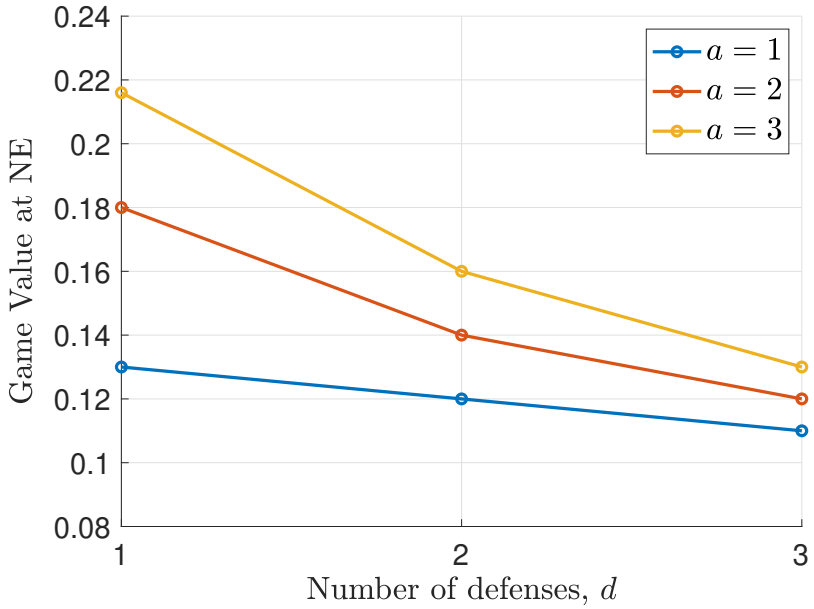

Figure 4.3: Impact of the number of defences and attacks on the game value at Nash Equilibrium for a time horizon with n = 4 milestones.

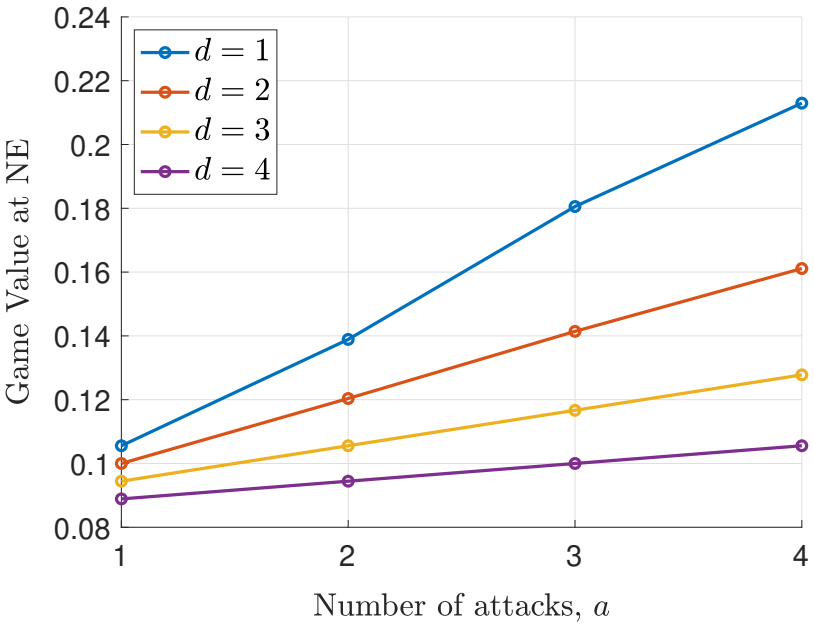

Figure 4.4: Impact of the number of attacks and defenses on the game value at Nash Equilibrium for a time horizon with n = 5 milestones.

The figure shows the general increasing value of the game with attacks while AoI increases much more significantly when defenses are outnumbered by the attacks. The situation is exactly opposite when the defenses start outweighing or matching the number of attacks; the AoI and hence the value of the game is low, indicating a successful containment of the adversarial impact.

These results really bring out the critical balance between offensive and defensive strategies. One general observation to be made is that the game becomes increasingly favorable to the defender as the number of available strategic options-both attacks and defenses-increases. In doing so, the defender is able to dilute the impact of the adversary's attacks by spreading out defenses effectively, thus neutralizing the potential damage, especially in scenarios where the number of defenses is maximized.

4.2.3 Analysis of Payoff Tables for Different Horizons

The payoff tables for different horizons provide a detailed numerical insight into the game value at Nash Equilibrium for varying numbers of attacks and defenses.

Table 4.1: Payoff Table for Horizon 2

Attack / Defense	**1 Defense**
1 Attack	0.2222

Table 4.2: Payoff Table for Horizon 3

Attack / Defense	**1 Defense**	**2 Defenses**
1 Attack	0.1667	0.1458
2 Attacks	0.2188	0.1667

Table 4.3: Payoff Table for Horizon 4

Attack / Defense	**1 Defense**	**2 Defenses**	**3 Defenses**
1 Attack	0.13	0.12	0.11
2 Attacks	0.18	0.14	0.12
3 Attacks	0.216	0.16	0.13

- **Horizon 2 (Table 4.1):** Only 1 attack vs. 1 defense, game value is 0.2222, it shows the minimal strategic complexity, both players have limited choice to lead to higher AoI.

Table 4.4: Payoff Table for Horizon 5

Attack / Defense	1 Defense	2 Defenses	3 Defenses	4 Defenses
1 Attack	0.1056	0.1	0.0944	0.0889
2 Attacks	0.1389	0.1204	0.1056	0.0944
3 Attacks	0.1806	0.1414	0.1167	0.1
4 Attacks	0.2130	0.1611	0.1278	0.1056

- **Horizon 3 (Table 4.2):** If the horizon is stretched to 3 milestones, adding more defenses reduces the game value. Take, for instance, the case of 1 attack and 2 defenses. Its game value now reduces to 0.1458, which reflects how well the defender can deplete the impact of the attack now.

- **Horizon 4 (Table 4.3):** For a 4-milestone horizon the interaction between attacks and defense is subtler. As it is possible to see from the table, increasing the number of defenses-especially when these are more than the attacks-decreases the game value.

- **Horizon 5 (Table 4.4):** The 5-milestone horizon represents the richest problem. The payoff table underlines that, for 4 defenses against 4 attacks, the value of the game is 0.1056, which means a well-balanced strategic setting where the actions of both players are highly influential on the AoI.

Taken together, these payoff tables convey the same basic message as the figures: the more defenses deployed, the lower the AoI tends to be, especially as the strategic complexity of the game increases with longer horizons.

4.2.4 Histogram of Expected Utilities for the Attacker

Figure 4.5 shows the histogram of the attacker's expected utilities obtained by running 10,000 simulations of the game where random strategies were played. The x-axis shows the range of utilities, while the y-axis depicts the frequency of each utility. Variations in utilities are shown on the x-axis, whereas the frequencies of utilities are plotted on the y-axis. The red dashed lines represent the expected payoffs at NE.

This plot is intuitive and captures the essence of the variability in the outcomes with randomly chosen strategies as compared to deterministic outcomes at NE. The concentration of the histogram around specific values intuitively conveys that while random strategies are free to result in a wide range of outcomes, the strategic NE gives the attacker some more favorable and predictable expected utilities.

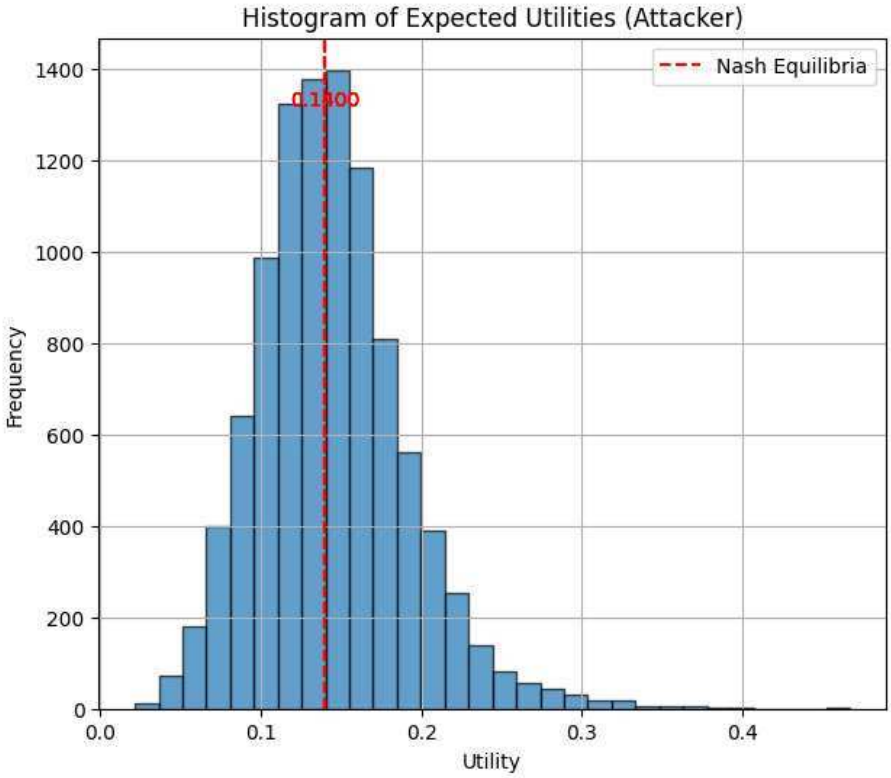

Figure 4.5: Histogram of Expected Utilities for the Attacker over 10,000 simulations. The red dashed lines indicate the expected payoffs at Nash Equilibria.

4.2.5 Cumulative Distribution Function (CDF) of Expected Utilities

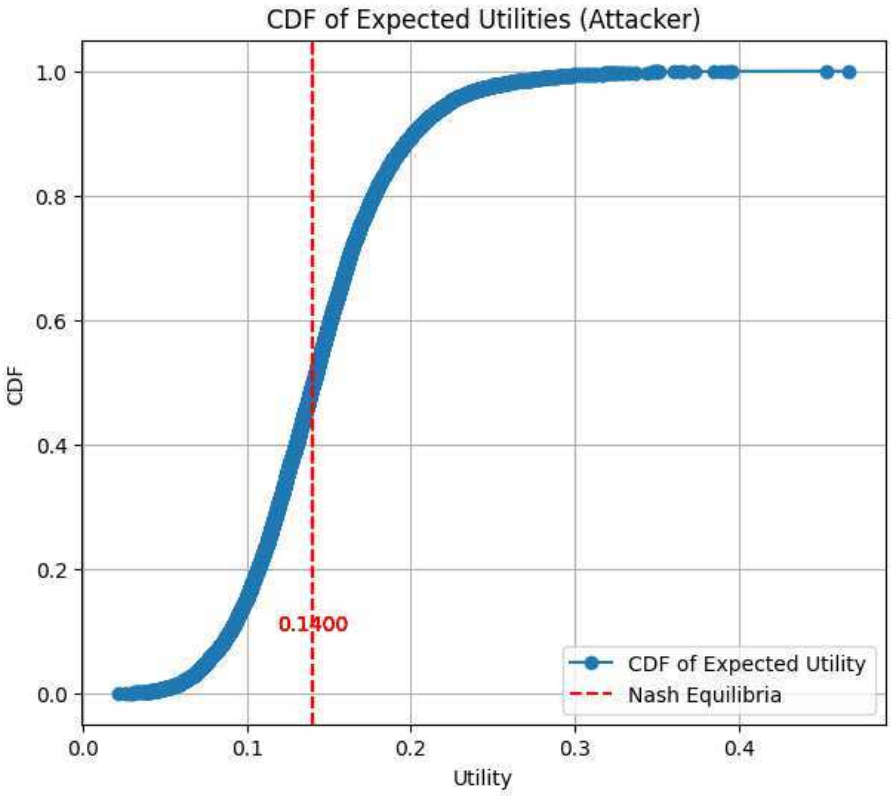

Figure 4.6: Cumulative Distribution Function (CDF) of Expected Utilities for the Attacker over 10,000 simulations. The red dashed lines indicate the expected payoffs at Nash Equilibria.

Figure 4.6 shows the Cumulative Distribution Function (CDF) of the attacker's expected utilities, all from the same 10,000 simulations. The x-axis gives expected utility values, while the y-axis gives cumulative probability to achieve utility less than or equal to that given by x. The red dashed lines give the expected payoffs at Nash Equilibria.

The CDF of utility helps capture the probability with which an attacker can receive a certain level of utility or better. It also contrasts expected utilities at NE with the overall distribution. Indeed, the red lines in the plots of the NE values represent specific points on the CDF curve that show the strength of those strategies in their expected utility.

The following histogram and CDF analysis underlines the strategic importance of following the Nash Equilibrium strategies; they are predictable and often optimal in

the context of the game, while random strategy selection is subject to a big range of possibilities.

5

Conclusions and Future Works

5.1 Conclusions

In this thesis, we investigated strategic interactions between a sensor and an adversary in the context of Age of Information minimization for IoT networks. We have focused on jamming attacks, as it is specifically devastating in applications relying on real-time information. The research presented herein addressed the problem of low AoI maintenance in adversarial settings through the use of game-theoretic models. The major contributions of this work are:

- Game-theoretic Model Development: We develop a comprehensive game-theoretic model that captures key strategic interactions between an IoT sensor and an adversary. This model takes into account the adversary's objective of maximally increasing AoI by launching a jamming attack, while the sensor aims to minimize AoI by protecting critical communication milestones.

- Nash Equilibrium Analysis: By carrying out an extensive analysis, we could extract the Nash Equilibrium strategies concerning sensor and adversary in different network conditions. That provided insights into what is the best possible defense mechanism sensors can adapt to mitigate the effect of jamming on AoI.

- Simulation and Theoretical Validation: We performed simulations that validate the efficiency of the proposed strategies in maintaining low AoI in adversarial conditions. The results show that our proposed game theoretic strategies enhance significantly the resiliency of IoT networks and reduce the negative impact of jamming attacks on information freshness.

- Application of Mixed-Strategy Approaches: By developing some mixed strategies, we proved that probabilistic defense mechanisms are capable of neutralizing sophisticated jamming attacks and make it much harder for an adversary to determine and disrupt the key communication links.

This work represents a significant contribution to the field of security in IoT networks because of the integration of AoI, jamming, and game theory into one framework. The results provide deep understanding for the optimization of communication strategies in adversarial environments with the goal of making IoT systems robust and reliable, even under persistent threats.

5.2 Future Works

The goal of this thesis has been to provide a good foundation for understanding and mitigating the impact of jamming attacks on AoI in IoT networks. This leaves several avenues open for future research in the following areas:

- More Complex Network Topologies: This model can be extended in the future by considering more complex and heterogeneous topologies for networks. This involves multi hop networks, dynamic environments with mobile nodes, quantum wiretap channel, and large-scale IoT deployments. Indeed, understanding how AoI optimization strategies perform in these settings is of high importance when developing a more generalizable solution.
- Item Investigating Collaborative Defense Mechanism: Another interesting direction could be to explore collaborative defense mechanisms in which sensors or nodes work together to defend an attack in general or jamming attacks in particular. Game-theoretic models can include expansions to cope with cooperative games where the nodes share information and resources aiming at achieving better global network resilience.
- Application to Other Adversarial scenarios: Although this thesis focused on jamming attacks, the framework developed could be adapted to address adversarial scenarios such as DoS, eavesdropping, and data injection. This could extend the developed game-theoretic analysis to such contexts and therefore provide relevant insights for securing a wide range of IoT applications.
- Real-world Implementation and Testing: Finally, the implementation of the proposed strategies within real-world IoT systems and testing them in real environments would practically validate the theoretical and simulated results that ensure the validity and feasibility of the proposed strategy in actual deployments.

This thesis has therefore laid the foundation for further research into the optimization of AoI against adversarial threats. The proposed game-theoretic approaches would thus provide promising solutions toward enhanced security and performance in the IoT network.

In this regard, as the IoT system continues to grow and gets complicated, further research and development will always be needed to ensure that such important systems are robust.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] M. Li, S. Li, A. X. Liu, and X. Guan, "Learning-based multi-source data collection for fresh iot applications," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1918–1931, 2018.

[4] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, 2014.

[5] E. Uysal, O. Kaya, A. Ephremides, J. Gross, M. Codreanu, P. Popovski, M. Assaad, G. Liva, A. Munari, and B. Soret, "Semantic communications in networked systems: A data significance perspective," *IEEE Netw.*, vol. 36, no. 4, pp. 233–240, 2022.

[6] R. D. Yates, Y. Sun, D. R. Brown, S. K. Kaul, E. Modiano, and S. Ulukus, "Age of information: An introduction and survey," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 5, pp. 1183–1210, 2021.

[7] L. Badia, "Age of information from two strategic sources analyzed via game theory," in *Proc. IEEE Int. Wkshp Comp. Aided Model. Design Commun. Links Netw. (CAMAD)*, 2021, pp. 1–6.

[8] S. Kaul, R. Yates, and M. Gruteser, "Real-time status: How often should one update?" *Proc. IEEE INFOCOM*, pp. 2731–2735, 2012.

[9] C. Kam, S. Kompella, G. D. Nguyen, J. E. Wieselthier, and A. Ephremides, "Age of information with a packet deadline," *Proc. IEEE ISIT*, pp. 2564–2568, 2016.

[10] A. Baiocchi, I. Turcanu, N. Lyamin, K. Sjöberg, and A. Vinel, "Age of information in ieee 802.11p," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manag.*, 2021, pp. 1024–1031.

[11] C.-F. Liu and M. Bennis, "Taming the tail of maximal information age in wireless industrial networks," *IEEE Commun. Lett.*, vol. 23, no. 12, pp. 2442–2446, 2019.

[12] G. Cisotto, A. V. Guglielmi, L. Badia, and A. Zanella, "Joint compression of eeg and emg signals for wireless biometrics," in *Proc. IEEE Globecom*, 2018, pp. 1–6.

[13] Y. Sun, I. Kadota, R. Talak, and E. Modiano, "Age of information: A new metric for information freshness," *Synth. Lect. Commun. Netw.*, vol. 12, no. 2, pp. 1–224, 2019.

[14] Y. Sun, E. Uysal-Biyikoglu, R. Yates, C. E. Koksal, and N. B. Shroff, "Update or wait: How to keep your data fresh," *IEEE Trans. Inf. Theory*, vol. 63, no. 11, pp. 7492–7508, 2017.

[15] W. Pan, Z. Deng, X. Wang, P. Zhou, and W. Wu, "Optimizing the age of information for multi-source information update in internet of things," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 2, pp. 904–917, 2022.

[16] A. Mishra, S. Tanwar, N. Kumar, and M. S. Obaidat, "Iot-based energy-efficient multimedia data compression for smart healthcare," *IEEE Netw.*, vol. 35, no. 5, pp. 76–82, 2021.

[17] R. Zhang, R. Zhang, and K. Ren, "Iot security: Ongoing challenges and research opportunities," *Proc. IEEE CNS*, pp. 473–478, 2014.

[18] V. Bonagura, S. Panzieri, F. Pascucci, and L. Badia, "Strategic interaction over age of incorrect information for false data injection in cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, 2025, To be published.

[19] L. Badia, H. S. D. Tunc, A. C. Aka, R. Bassoli, and F. H. P. Fitzek, "Strategic interaction over age of information on a quantum wiretap channel," *European Wireless 2023; 28th European Wireless Conference, Rome, Italy, 2023, pp. 388-394*, 2023.

[20] B. Li, W. Li, and R. Zhang, "Jamming attack on wireless relay networks: A game theoretic approach," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6977–6990, 2018.

[21] W. Xu, W. Xu, M. A. B. Shirazi, and W. Trappe, "The feasibility of launching and detecting jamming attacks in wireless networks," *Proc. MobiHoc*, pp. 46–57, 2005.

[22] M. Borgo, B. Principe, L. Spina, L. Crosara, L. Badia, and E. Gindullina, "Attack strategies among prosumers in smart grids: A game-theoretic approach," in *Proc. IEEE icSmartGrid*, 2023, pp. 01–06.

[23] L. Badia, V. Bonagura, F. Pascucci, V. Vadori, and E. Grisan, "Medical self-reporting with adversarial data injection modeled via game theory," in *Proc. IEEE ICCSPA*, 2012, pp. 5782–5787.

[24] M. Scalabrin, V. Vadori, A. V. Guglielmi, and L. Badia, "A zero-sum jamming game with incomplete position information in wireless scenarios," in *Proc. European Wireless Conf. VDE*, 2015, pp. 1–6.

[25] A. Garnaev, W. Zhang, J. Zhong, and R. D. Yates, "Maintaining information freshness under jamming," in *Proc. IEEE Infocom Whshps*, 2019, pp. 90–95.

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

[27] I. Kahraman, A. Köse, M. Koca, and E. Anarm, "Age of information in internet of things: A survey," *IEEE Internet Things J.*, vol. 11, no. 6, pp. 9896–9914, 2024.

[28] R. Hazra, M. Banerjee, and L. Badia, "Machine learning for breast cancer classification with ann and decision tree," in *Proc. IEEE IEMCON*, 2020, pp. 0522–0527.

[29] R. Verma, S. J. Darak, V. Tikkiwal, H. Joshi, and R. Kumar, "Countermeasures against jamming attack in sensor networks with timing and power constraints," in *Proc. IEEE COMSNETS*, 2019, pp. 485–488.

[30] D. Koller and N. Megiddo, "The complexity of two-person zero-sum games in extensive form," *Games Econ. Behav.*, vol. 4, no. 4, pp. 528–552, 1992.

[31] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Baar, "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach," in *Proceedings of the IEEE MILCOM*, 2011, pp. 119–124.

[32] N. Michelusi, K. Stamatiou, L. Badia, and M. Zorzi, "Operation policies for energy harvesting devices with imperfect state-of-charge knowledge," in *Proc. IEEE ICC*, 2012, pp. 5782–5787.

[33] G. Quer, F. Librino, L. Canzian, L. Badia, and M. Zorzi, "Inter-network cooperation exploiting game theory and bayesian networks," *IEEE Trans. Commun.*, vol. 61, no. 10, pp. 4310–4321, 2013.

[34] M. Hajji, I. M. E. Emary, and M. S. Obaidat, "A game-theoretic model for jamming attack in a uav network," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8822–8830, 2020.

[35] E. Djokanovic, A. Munari, and L. Badia, "Harsanyi's equilibrium selection for distributed sources minimizing age of information," in *Proc. IEEE MedComNet*, 2024.

[36] G. D. Nguyen, S. Kompella, C. Kam, J. E. Wieselthier, and A. Ephremides, "Information freshness over an interference channel: A game theoretic view," in *Proc. IEEE Infocom*, 2018, pp. 908–916.

[37] M. Abd-Elmagid and H. S. Dhillon, "Deep reinforcement learning for minimizing age-of-information in uav-assisted networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 6, pp. 1614–1617, 2019.

[38] X. Chen, X. Ma, and Z. Yang, "Age of information in a gaussian mac: A game-theoretic approach," *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, pp. 6838–6850, 2021.

[39] A. Buratto, A. C. Aka, S. Sadeghzadeh, and L. Badia, "Eavesdropping fresh information: A game theoretical approach in dual sender networks," *Proc. European Wireless Conference (EW2024)*, 2024, To be published.

[40] Q. Zhang, Z. Xu, X. Lan, J. Chen, J. He, W. Ma, and Q. Chen, "Optimal age of information and throughput scheduling in heterogeneous traffic wireless physical layer security communications," *IEEE Internet Things J.*, vol. 11, no. 13, pp. 23 644–23 660, 2024.

[41] A. Ali, S. Naser, and S. Muhaidat, *Defeating proactive jammers using deep reinforcement learning for resource-constrained iot networks*, Jul. 2023.

[42] L. Badia, A. Zancanaro, G. Cisotto, and A. Munari, "Status update scheduling in remote sensing under variable activation and propagation delays," *Ad Hoc Networks*, vol. 163, p. 103 583, 2024.

[43] S. Banerjee, S. Ulukus, and A. Ephremides, "Age of information of a power constrained scheduler in the presence of a power constrained adversary," in *Proc. IEEE Infocom Whshps*, 2023, pp. 1–6.