Università
degli Studi
di Padova

Dipartimento
di Ingegneria
dell'Informazione

Master Thesis in ICT for Internet and Multimedia

Age of Information for Channels under Attack by an Adversary

Master Candidate

Kader Cicek

Student ID 2049526

Supervisor

Leonardo Badia

University of Padova

Academic Year
2022/2023
Date of Graduation/ December 12

KURDÎ: Ji bo kar û xebate dayika min Meryem Çîçek û bavê min Sebrî Çîçek heta vî temenî. Ji xwika min a hêja Aysel re ku ez hînî têkosînê kirim. Xwikên min ên delal Gulîstan, Adîle, Dîlan û Rojda, ji ber pistgirî, bawerî û keda wan a di her dijwariya ku min di rêya vê serkeftinê de dît.
Ji Profesor û sêwirmendê xwe Leonardo Badia re ji bo sebir û pistgiriya wî.
Û ji hemû jinan re, bi taybetî ji jinên Kurd re, ku serî li ber wan kesên ku layiqî wan tên dîtin, nacin, dest ji xeyalên xwe bernadin û titên ku dikarin bi dest bixin, hêviya xwe winda nakin û ji bo vê dozê têdikosin.

ENGLISH: To my mother Meryem Cicek and my father Sabri Cicek for their endeavours until this day. To my dear sister Aysel, who taught me to resist. To my beloved sisters Gülistan, Adile, Dilan and Rojda, for their support, belief and labour in every difficulty I have experienced on the road to this success.
To my Professor and my Mentor Leonardo Badia for his patience and for his support.
And to all women, especially Kurdish women, who do not give in to what they are treated as unworthy, who never give up on their dreams and what they can achieve, who do not lose hope and who fight for their dreams.

TURKCE: Annem Meryem Cicek ve babam Sabri Cicek'in bu yasima kadar verdikleri emeklere. Bana mücadele etmeyi ögreten canim ablam Aysel'e. Gülistan, Adile, Dilan ve Rojda, canim kardeslerimin bu basariya giden yolda her zorlukta bana olan desteklerine, inanclarina ve emeklerine.
Sabri ve destegi icin Profesörüm ve akil hocam Leonardo Badia'ya.
Ve kendisine layik görülenlere boyun egmeyip, hayallerinden ve basarabileceklerinden asla vazgecmeyen, umudunu yitirmeyip bu ugurda mücadele veren Kürt kadinlari basta olmak üzere bütün kadinlara.

Abstract

Since the world is becoming increasingly digitized safeguarding sensitive data has become a paramount concern. In particular measuring information freshness or timeliness or Age of Information (AoI) is becoming essential. This metric enables us to better appreciate how well a system understands the observed processes from source to recipient viewpoint. Hence this thesis presents how AoI is associated with security challenges including data breaches or cyber attacks that pose serious threats to valuable information. Moreover, it outlines various solutions developed specifically in an attempt to curb such risks in an AoI context effectively. By conducting in-depth research on these issues. This thesis endeavors to provide a comprehensive understanding of their implications, delivery into the realm of game theory's applicability to the interactions between information transmitters and adversaries, exploring their objectives, strategies, payoffs, and equilibrium points. By investigating how game theory can shed light on the complexities of security and communication, this research aims to provide insights into the robustness and vulnerabilities of information dissemination networks against intentional jamming attacks. The analysis contributes to a deeper understanding of the interplay between information dissemination, adversarial actions, and strategic decision-making, fostering the development of more resilient and secure communication protocols.

The thesis addresses important issues such as examining how the Information Age is connected with security issues. It aims to help us better understand this ever-changing field. The detailed information here provides the information needed by academics interested in information security or communication systems. It is also useful for people making decisions about rules and policies in these areas.

Contents

List of Figures

List of Tables

List of Code Snippets

1 Introduction

Over the past few years, the concept of the Age of Information (AoI) has emerged as a new performance metric for wireless communication systems that focuses on the freshness of received information [32]. AoI measures the time elapsed since the last update was generated by a source and delivered to the destination, and it is an effective tool for optimizing various aspects of wireless networks, such as remote process estimation, status updates, and data dissemination. In 2012, discussions on this topic were initiated by introducing Age of Information (AoI), an age metric that evaluates how fresh the data is received, given that some data might be stale upon its arrival to the recipient [30]. AoI has attracted high interest among researchers for two primary reasons. The first reason is the novelty brought by AoI in characterizing the freshness of information. The second reason is the need to characterize the freshness of information carried by packet data, which is crucial in a wide range of communication, information, and control systems [32]. In recent years, researchers have begun investigating the use of game theory-based approaches to analyze and optimize the performance of wireless networks in the context of the Age of Information metrics [35]. Game theory provides a powerful framework for modeling strategic interactions between agents in a network, and it can be used to design efficient allocation mechanisms, equilibria, and incentives that maximize the overall system performance while accounting for the selfish interests of individual agents. Game theory-based analysis of the Age of Information metrics for wireless networks is a relatively new area of research, but it holds great promise for improving the efficiency and security of wireless communication systems.

In particular, game theory can be used to address several key challenges and questions related to Age of Information metrics. For a detailed discussion, please refer to the insights in paper [11, 53].

This thesis comprises an exploration of the application of game theory to the interactions between information transmitters and adversaries. It investigates how game theory can offer insights into the optimization of information dissemination while accounting for potential adversarial actions, particularly intentional jamming attacks[29]. The subsequent chapters delve into the theoretical foundations of gossip-based protocols, challenges in information dissemination, the role of jamming attacks, and the application of game theory to model and analyze the interactions between information transmitters and adversaries. By combining these elements, this research aims to contribute to a comprehensive understanding of information security and communication in modern networks.

1.1 The Importance of Security

Security is crucial in the modern era due to the increasing reliance on digital systems and networks. Beyond the Age of Information problems, security has evolved into an established and critical field of study. The field of cybersecurity has expanded to encompass not only traditional information systems but also emerging technologies like the Internet of Things (IoT), artificial intelligence, and cloud computing. Instances of cyber threats, data breaches, and malicious activities highlight the constant need for robust security measures[19]. Researchers and practitioners in the field continually investigate new attack vectors and vulnerabilities, developing sophisticated techniques to safeguard against unauthorized access, data breaches, and service disruptions. This ongoing research and innovation are essential to maintaining the integrity, confidentiality, and availability of information in the face of evolving and sophisticated cyber threats. Several examples about this topic can be located in the papers referenced as [44],[36], [22].

1.2 Financial Fallout: Big Tech and the Cost of Security Breaches

Security breaches have profound economic implications for big tech companies, with financial repercussions extending beyond immediate damages to include costs related to investigations, legal actions, regulatory fines, and efforts to bolster cybersecurity measures[26]. While precise figures fluctuate based on the scale and severity of each breach, a few notable examples underscore the substantial financial impact. In 2017, the Equifax breach, exposing sensitive personal information, resulted in a settlement exceeding 575 million dollars in the United States [21]. Similarly, Yahoo, following a significant 2016 breach affecting billions of user accounts, witnessed a reduction in its acquisition price by Verizon, dropping from 4.8 billion dollars to 4.48 billion dollars [54]. Another instance involves Marriott, which, in 2018, grappled with a data breach affecting approximately 500 million guests, incurring an estimated cost of 200 million dollars [12]. These instances serve as cautionary tales, highlighting the necessity for robust cybersecurity measures and the tangible economic consequences that can arise from lapses in digital security. For the latest and company-specific information, referring to recent financial reports and official statements is paramount, ensuring an accurate understanding of the dynamic landscape surrounding cybersecurity expenditures and consequences for big tech companies.

1.3 Summary

This thesis is organized as follows. Chapter 2 explores the concept of Age of Information (AoI) as a metric for measuring information freshness in communication systems, covering its introduction, evolution, significance, metrics, impact of jamming attacks, and strategies to minimize AoI. Chapter 3 discusses the relationship between security challenges and the preservation of information freshness. It explores the role of physical Layer Security in safeguarding real-time status updates, addressing active jamming attacks, and introducing strategies such as artificial noise generation. Chapter 4 introduces game theory, tracing its historical evolution, applying Nash equilibrium to Age of Information (AoI) analysis in communication systems. Chapter 5 presents analytical methods, including game theory and numerical optimization, employing Python and MATLAB, to optimize Age of Information in adversarial communication, focusing on utility functions and Nash Equilibrium points for strategic decision-making. In chapter 6, we examine minimum Age of Information (AoI) values, utility matrices,Nash equilibrium points, and graphical representations, analyzing the strategic dynamics between a transmitter and an adversary. Finally, chapter 7 gives the conclusions and some future directions.

2

Age of Information

2.1 Introduction to Age of Information (AoI)

Starting with an introduction to the concept of AoI as a performance metric for measuring the freshness of information updates in communication systems. AoI quantifies the time elapsed since the last correct knowledge of a system's status at the receiver's side [32]. At any time instant, the age of information is defined as the amount of time elapsed since the most recently received update was generated. A large age indicates that the information about the physical process is outdated since the most recently received update was generated a long time ago.

Minimizing the age of information requires careful decisions on when to sample the process and send the samples. Suppose that we have just updated the status. On the one hand, we do not want to update the status immediately, because the update would be almost the same as the old update, and hence carry little fresh information. On the other hand, we do not want to wait for a long time before updating the status, because the previous update would become outdated before the next update [53]. In summary, we need to make sure that both the information sent and that received are fresh, to minimize the age of information [55, 45].

The attention AoI has been receiving is due to two factors. The first is the sheer novelty brought by AoI in characterizing the freshness of information versus for example that of the metrics of delay or latency. Second, the need for and importance of characterizing the freshness of such information is paramount in a wide range of information, communication, and control systems [32].

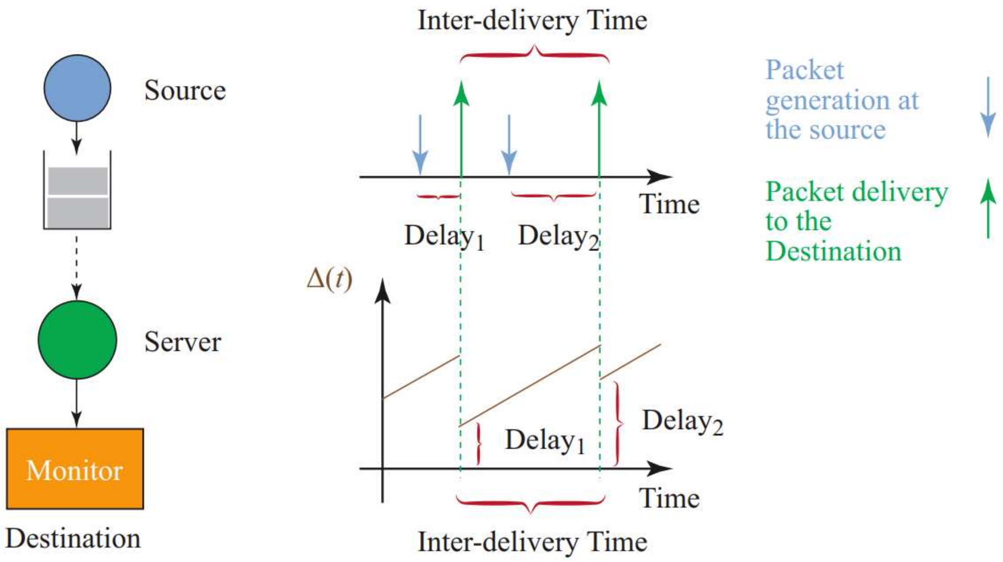

Figure 2.1: Evolution of AoI

Paper [9] explained considers an information update system where an information receiver requests updates from an information provider to minimize its age of information. The updates are generated at the information provider (transmitter) as a result of completing a set of tasks such as collecting data and performing computations on them. They refer to this as the update generation process.

AoI can be assessed at the receiver's side, offering valuable insights into how fresh the received data is, and thus enabling users to assess the reliability and relevance of the information. The metric helps optimize information-gathering strategies and communication protocols, facilitating decisions on when and how frequently to update the transmitted data. However, it had already become clear that timely updating a destination about a remote system is neither the same as maximizing the utilization of the communication system, nor ensuring that generated status updates are received with minimum delay [32].

In conclusion, the Age of Information presents a fresh perspective on assessing the timeliness of information updates in communication systems. By quantifying the freshness of received data, AoI enhances our understanding of real-time information dissemination and serves as a valuable tool for optimizing communication protocols. Through this thesis, one of our aims is to shed light on the significance of AoI and its potential impact on various communication systems, paving the way for more efficient and time-sensitive networks in the future.

2.1.1 Motivation and Importance of Studying Age of Information (AoI)

The motivation behind studying AoI lies in its potential to revolutionize communication protocols and enhance the performance of various communication scenarios, including Internet of Things (IoT) networks, wireless systems, remote sensing applications, and distributed systems.

- IoT Networks: In IoT networks, a myriad of interconnected devices, sensors, and actuators exchange information to facilitate smart automation, intelligent decision-making, and seamless user experiences. The real-time nature of IoT applications demands up-to-date data to enable timely actions and responses. AoI offers a quantifiable measure of information freshness, making it a valuable tool for optimizing communication strategies and minimizing delays in IoT applications [2].

- Wireless Systems: In wireless communication systems, efficient utilization of available resources is essential to achieve high data rates and reduced latency. We considered the problem of minimizing the age of information in wireless networks, consisting of several source-destination communication links, under general interference constraints. For a network with active sources, where fresh updates are available for every transmission, we show that a randomized stationary policy is peak age optimal and is also within a factor of two of the optimal average age [22]. AoI complements traditional performance metrics by capturing the freshness of information received at the destination, enabling better resource allocation and minimizing the time elapsed between data updates and their consumption.

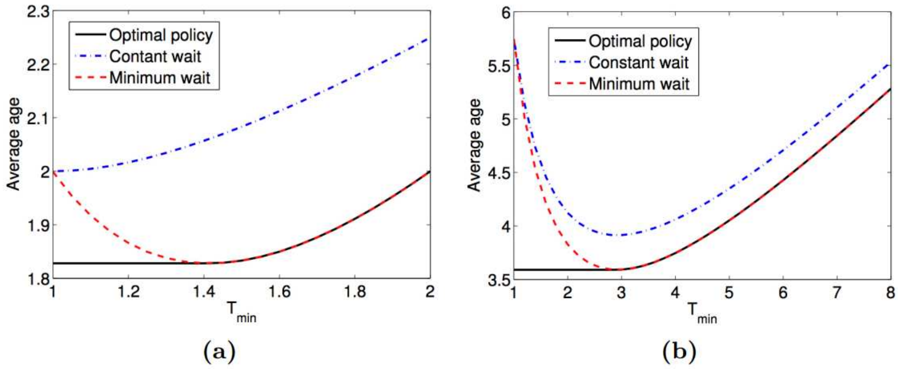

Figure 2.2: Average age vs Tmin for i.i.d. (a) discrete service times and (b) log-normal distributed service times provided by [45]

- Remote Sensing Applications: In remote sensing applications, timely and accurate information is critical for monitoring environmental conditions, weather forecasting, and disaster response. AoI allows researchers and stakeholders to assess the relevance of data received from remote sensors, ensuring that decision-makers have access to the most recent and reliable information for effective response strategies. There has been a recent flourishing of papers focusing on AoI evaluations, especially for remote sensing in IoT [6].

- Distributed Systems: Distributed systems involve multiple nodes or components that collaborate to perform complex tasks. These systems often rely on the exchange of real-time information to coordinate actions and ensure synchronization. AoI enables distributed systems to optimize data transmission strategies, reduce communication overhead, and improve overall system performance.

  The paper [34] investigates the joint optimization of Age of Information (AoI) and total energy consumption in Internet of Things (IoT) devices operating in a distributed system. The findings demonstrate that the proposed approach effectively reduces AoI and total energy consumption, showcasing the relevance of AoI in distributed systems. By leveraging real-time information exchange and cooperative optimization, the proposed algorithm enhances overall system performance and minimizes communication overhead.

2.2 Age of Information Metrics

To achieve the objective of minimizing AoI, certain considerations must be made:

- Fresh Information: Both the information being sent and the updates received by the receiver should be fresh. Sending stale or redundant information contributes to an increase in AoI. Therefore, the goal is to ensure that updates are relevant and capture the current state of the process. We consider a communication system in which status updates arrive at a source node and should be transmitted through a network to the intended destination node. The status updates are samples of a random process under observation, transmitted as packets, which also contain the time stamp to identify when the sample was generated. The age of the information available to the destination node is the time elapsed since the last received update was generated [32].

- AoI at Destination: This metric represents the age of the information at the intended destination node. It measures the time elapsed since the last update was generated or received at the destination. Numerous applications of communication networks require the transmission of information about the state of a process of interest between a source and a destination. The paper [16] focuses on applications of communication networks in which a random process is observed, and samples are made available to a source node at random times. The samples are transmitted to update the value of the process known at the destination node. For that reason, the transmitted messages are also called status updates.

- AoI Averaged over Time: This metric calculates the average AoI over a specific period. It provides insights into the average freshness of information during that duration [56].

- AoI Averaged over Sources: This metric computes the average AoI across multiple information sources or senders. It considers the collective freshness of information from different sources[56].

- AoI Probability Distribution: This metric characterizes the statistical distribution of AoI values over time. It provides a more comprehensive understanding of the age dynamics and variations in information freshness[27].

- Peak AoI: This metric identifies the maximum AoI value observed during a specific time. It indicates the worst-case age of the information. The paper distinguishes between "peak age" and "average age" as two metrics to measure AoI. Peak age is the average of the highest AoI values, while average age is the time-average of the AoI [46].

2.3 Communication Protocols and Strategies to Minimize AoI

Minimizing the Age of Information (AoI) in communication systems is a crucial objective to ensure timely and fresh information updates. Some of these approaches used in the literature include:

- Randomized Algorithms: Randomized algorithms have shown promise in minimizing AoI in certain scenarios. For instance, in contention-based access protocols like ALOHA, where multiple users compete for access to a shared channel, randomized user scheduling algorithms have been employed. In the paper [4] an evaluation of slotted ALOHA using game theory to capture the strategic choices of the nodes, considered as independent agents that attempt to obtain updates from a shared source, with collisions preventing them from getting a usable update. These algorithms randomly select users for transmission, reducing the chances of collisions and contention. By avoiding predictable patterns, randomized algorithms can help achieve more efficient and fair use of the communication channel, leading to lower AoI.

- Medium Access Control: Optimized medium access control is another strategy to minimize AoI. By adjusting the transmission power based on optimizing channel access, nodes can improve the reliability of communication and reduce the likelihood of retransmissions [8].

- User Scheduling Approaches: User scheduling strategies play a crucial role in multi-user communication systems, such as cellular networks or IoT applications. In such scenarios, the base station or access point needs to select which users to serve at each time slot. User scheduling algorithms can be designed to consider various factors, including channel conditions, buffer occupancy, and the urgency of information updates. By intelligently selecting users to transmit updates, the system can prioritize critical information, resulting in lower AoI.

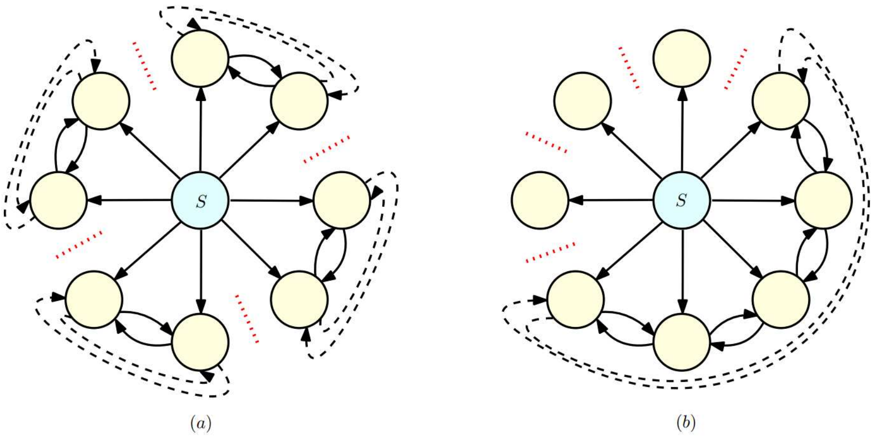

Figure 2.3: Jammer positions on a ring (a) most favorable, (b) most harmful

- Gossip-based Protocols: Gossip protocols have gained attention as efficient methods for information dissemination in large-scale networks. In a gossip-based protocol, nodes exchange information with random neighbors, leading to the rapid spread of updates across the network. These protocols have been investigated for their impact on AoI, as they offer a decentralized and scalable approach to minimize the time it takes for information to propagate through the network. AoI for gossip-type information dissemination was analyzed in [43, 15, 50]. Conversely, the study [29] also aims to identify the least harmful jammer configurations. These configurations correspond to scenarios where the presence of jammers has minimal impact on the version age, suggesting that certain placements or densities of jammers are relatively ineffective in disrupting gossip-based information dissemination.

- Covert Communication Strategies: In scenarios where security and privacy are paramount, covert communication strategies aim to minimize AoI while avoiding detection by eavesdroppers. Game-theoretic approaches have been applied to analyze the trade-off between minimizing AoI for legitimate receivers and reducing the likelihood of detection by adversaries [51]. In conclusion, various communication protocols and strategies have been developed to minimize AoI in different network scenarios. These approaches range from randomized algorithms to optimized transmission policies and user scheduling techniques. By intelligently managing communication resources and prioritizing timely updates, these strategies contribute to the efficient and reliable dissemination of information, ultimately reducing the Age of Information in communication systems.

2.4 Impact of Jamming Attacks on AoI in Wireless Networks

Jamming attacks in wireless networks involve malicious interference that disrupts communication between nodes. A jammer is a malicious entity that disrupts communication between two nodes, say by jamming the channel with noise [29]. This interference can significantly impact the Age of Information (AoI), which measures the freshness and reliability of information updates. Here's a summary of the key points:

- Reduced Information Freshness: Jammers disrupt communication, causing packet loss and delays in transmitting updates. This leads to increased AoI, reflecting the time elapsed since the last accurate system status update. In critical applications, higher AoI due to jamming can result in outdated information, undermining decision-making [18].

- Increased Update Latency: Jamming attacks introduce delays in update transmission. Lost or blocked packets may trigger retransmissions, further prolonging the AoI. This delays the system's ability to respond swiftly to changing conditions [18].

- Impact on Reliability: Jamming can lead to incomplete or corrupted data at the receiver's end, compromising the reliability of system status updates. This lack of trust in received information can have severe implications for critical applications. The jammer can also be a proxy for communication link failure, network partitioning, network congestion, or information corruption during transfer, prevalent in distributed networks [29].

2.5 Optimal Data Generation Rate

Optimizing the data generation rate is a critical consideration in the context of managing the Age of Information (AoI). This optimization entails striking a delicate balance between minimizing AoI at the receiver's end and addressing security concerns, especially when there is a risk of eavesdroppers or potential attackers. This concept involves a strategic approach where the data generation rate is fine-tuned to achieve a specific equilibrium between AoI reduction and safeguarding information from interception by unauthorized entities, such as eavesdroppers[16]. In essence, the optimal data generation rate is designed to achieve the lowest possible AoI while also proactively protecting against data breaches.

2.5.1 AoI Minimization

The primary goal of optimizing the data generation rate is to minimize the AoI at the receiver's end. AoI quantifies the freshness of information updates, and lower AoI values indicate more up-to-date knowledge of the system's status. Reducing AoI is essential in real-time monitoring and control applications, where timely and accurate information is critical for decision-making processes. We consider scheduling algorithms to minimize the age of information in a wireless network in an adversarial setting [7]. Designing algorithms to minimize the age of information in wireless networks is an active area of research. For an in-depth exploration, the findings in papers [24, 13] offer valuable insights. In wireless communication systems, security is a crucial concern, especially in the presence of eavesdroppers or potential adversaries. Eavesdroppers attempt to intercept and capture transmitted data, which can lead to privacy breaches, unauthorized access to sensitive information, or disruption of communication. The paper [20] analyzed a scenario of status updates between a transmitter and a legitimate receiver, considering the presence of an eavesdropper that is sometimes able to intercept data packets. The challenge arises in striking a balance between minimizing AoI and ensuring data security. If the data generation rate is too high, it might attract the attention of eavesdroppers, leading to increased security risks. On the other hand, if the data generation rate is too low to enhance security, it may result in higher AoI and less timely information updates.

Researchers use analytical frameworks and mathematical models to study the trade-off between AoI and security. Game theory and optimization techniques are often employed to find the optimal data generation rate that maximizes information freshness while minimizing the risk of interception. Several examples about this topic can be located in the papers referenced as [22, 5, 53]

3

Security Challenges and the Relevance to Age of Information

3.1 The Concept of Physical Layer Security and its Role in Protecting Information Freshness

With the quick proliferation of the Internet of Things (IoT) technologies, more and more devices and equipment are connected to the Internet. This brings severe security and privacy concerns considering that a large share of devices will be served by wireless communication technologies [44],[36]. It is worth mentioning here a handful of studies that investigated the problem of maintaining information freshness under active jamming attacks, see e.g., [53], [22], which is fundamentally different from the passive eavesdropping attacks considered in [16]. Since timely status updates are of particular importance to real-time monitoring and control systems, the attackers of these systems may specifically target their capability of timely updating the status [1]. Therefore, it is crucial to understand how an attacker would sabotage a real-time monitoring/control system, how should the system defend against the attack, and to what extent the attacker can degrade the timeliness of status updates.

3.1.1 Artificial Noise

Artificial noise is introduced by the transmitter to confuse eavesdroppers. By transmitting additional random signals in the same frequency band as the legitimate signal, the receiver at the destination can successfully decode the intended message, while the eavesdropper experiences significant interference. The authors [51] propose the use of AN generated by the FD receiver as a technique to enhance covertness. By introducing additional noise in the communication, the uncertainty for the warden is increased, making it more difficult to distinguish between the information-carrying signal and the noise.

3.1.2 Protection Against Passive Eavesdropping Attacks in Status Update Systems

Passive eavesdropping attacks involve an adversary intercepting the communication between nodes without actively disrupting the system. To protect against such attacks in status update systems, several security measures can be employed:

- Encryption: Encrypting the status updates to ensure that even if they are intercepted, the eavesdropper cannot understand the content of the updates[16].

- Secure Communication Channels: Establishing secure communication channels using protocols like Transport Layer Security (TLS) or Secure Shell (SSH) to prevent unauthorized interception of status updates[16].

- Traffic Analysis Countermeasures: Employing countermeasures to mitigate traffic analysis attacks, which involve inferring information from patterns or characteristics of the communication flow. Techniques such as adding dummy or decoy updates can help obfuscate the true information flow[51].

3.2 Introduction to Gossip-Based Information Dissemination

Gossip-based protocols are a class of protocols used for information dissemination in distributed systems. Gossip-based protocols operate in a similar manner, where nodes in a network exchange information with a subset of their neighbors, and this process continues until the information reaches all or a desired subset of nodes in the network [43].

Overall, gossip-based protocols provide a decentralized and scalable approach for information dissemination in large-scale networks. While they offer advantages such as scalability and robustness, addressing challenges related to information consistency, convergence speed, and security remains crucial for their effective deployment in real-world scenarios [29].

- Number of Jammers: The study [22] examines the effect of varying the number of jammers in the network. By increasing the number of jammers, researchers can observe how the version age is affected and whether there is a threshold beyond which the system's performance significantly deteriorates.

- Jammer Placement: Researchers analyze different placement strategies for the jammers. They may investigate scenarios where jammers are randomly distributed throughout the network or strategically positioned to maximize their disruptive impact. By considering different jammer placement approaches, the study can determine how the spatial distribution of jammers affects the system's performance [22].

- Jammer Density: In addition to the number of jammers, the study may explore the concept of jammer density, which refers to the concentration of jammers in a specific area or region of the network. By varying the density of jammers in different parts of the network, researchers can identify areas that are more vulnerable to jamming attacks and assess their impact on the overall version age [29].

3.2.1 Physical Layer Security

Beyond adjusting the data generation rate, physical layer security techniques can also be applied to enhance the security of wireless communication. These techniques involve transmitting artificial noise or using beamforming to make eavesdropping more challenging without significantly affecting the intended receiver's signal quality. In this context, physical layer security techniques that leverage the properties of wireless physical channels, such as interference and fading, to further strengthen the security of wireless communication systems, have been regarded as appealing complements or even alternative solutions [37].

4

Game theory and Nash Equilibrium

Game theory provides a formal language for the representation and analysis of interactive situations, that is, situations where several entities, called players, take actions that affect each other. Game theory is defined as the study of strategic interactions between individuals or entities making simultaneous choices. Game theory provides various ways to model the strategic behavior among different entities [28]. The first important text about Game Theory was written by John von Neumann and Oskar Morgenstern in 1944, followed by the contributions from John Nash, also winner of the Nobel Prize for his work developed in the 1950s.

This concept started to be applied to different fields after the 1970s, such as economics, diplomacy, and military strategy. Nowadays is used to study many interactive and strategic situations and to help understand how rational choices are made between different individuals. Game theory is an analytical tool that helps understand how decision-makers interact. It can be applied to various fields, even in everyday life and real-life situations. For an in-depth exploration, the findings in the paper [3] offer valuable insights. Fully analytical investigations based on game theory have shown how selfish players can behave efficiently in random access systems if they are driven by AoI-based objectives.

One of the aims of this thesis is to try to apply the concept of the Game Theory of Nash Equilibrium in AoI with security problems. The Nash equilibrium is a decision-making principle within game theory that states a player ought to achieve the desired outcome by not deviating from their initial strategy. In the Nash equilibrium, each players strategy is optimal when considering the decisions of other players. Every player wins because everyone gets the outcome that they desire. The prisoners dilemma is a common game theory example and one that adequately showcases the effect of the Nash equilibrium. The Nash equilibrium is often discussed in conjunction with the concept of a dominant strategy, which states that an actor's chosen strategy will lead to better results among all possible strategies, regardless of the strategy their opponent chooses. However, it is important to note that while Nash equilibrium captures a stable state in strategic interactions, it doesn't necessarily guarantee the selection of the most optimal strategy. Zero-sum games also represent strategic interactions between two players in which the sum of their payoffs equals zero for every possible outcome. In these games, specific solution approaches can be employed that are often more convenient than general methods. Additionally, the concepts of maximin and minimax, which are particularly relevant in the context of zero-sum games, can be generalized and applied to various other scenarios. Overall, zero-sum games and maxi-min/minimax are also typically encountered as applications of linear programming and artificial intelligence [17]. A zero-sum game can also be seen in many engineering problems with an adversarial setup, such as those related to network security. Here, some network performance metric is quantified and one player, representing the legitimate network user, tries to maximize it, hence it is called the maximizer, whereas an attacker plays the role of the minimizer, i.e., someone who wants to decrease the performance metric to its lowest possible values [32].

4.1 Game-Theoretic Approaches

4.1.1 Game-Theoretic Approaches in Age of Information (AoI) Analysis

Game theory provides a powerful framework to study the strategic interactions between network entities in communication systems, including transmitters, receivers, and adversaries. By integrating game theory with AoI analysis, researchers can gain valuable insights into how individual entities make decisions to optimize their utility, which in turn influences AoI-related decision-making and system performance. Let's explore how game theory enhances the understanding of strategic interactions and their impact on AoI-related decision-making:

Modeling Strategic Interactions

In communication systems, various entities may have conflicting objectives, leading to strategic interactions. For example, in wireless networks, multiple users may contend for limited resources, such as a shared channel or a base station's attention. Each user seeks to minimize its own AoI by transmitting updates as frequently as possible, but this may lead to congestion and interference, affecting the overall system performance. Game theory allows researchers to model these strategic interactions and analyze the dynamics between competing entities. You can find a comprehensive analysis of this concept in paper [4].

Nash Equilibrium

One of the central concepts in game theory is the Nash equilibrium, where no player has an incentive to unilaterally change its strategy, given the strategies of other players. In the context of AoI analysis, Nash equilibrium represents a stable state where all entities have settled into strategies that are optimal given the strategies of others. Studying Nash equilibria helps us understand how entities converge to stable points in their decision-making process, impacting the overall AoI experienced in the system. To delve deeper into this topic, consult the findings presented in paper [3, 22].

Stackelberg Equilibrium

Stackelberg games involve a leader-follower scenario, where one entity (the leader) chooses its strategy first, and the other entities (followers) respond based on the leader's decision. In the context of AoI analysis, Stackelberg games can capture scenarios where a central controller (leader) adjusts the system's behavior, and other nodes (followers) adapt accordingly. For instance, a base station in a wireless network can act as the leader, dynamically adjusting its transmission policies to influence the AoI experienced by users. You can find a comprehensive analysis of this concept in paper [39].

Trade-Off Analysis

AoI-related decision-making often involves trade-offs between different metrics and objectives. For example, in secure communication scenarios, the transmitter may adjust the generation rate of status updates to balance the AoI at the receiver's side while ensuring a certain level of security against eavesdropping. Game theory allows researchers to analyze these trade-offs and identify optimal strategies that achieve a balance between conflicting objectives. Integrating game theory with AoI analysis provides a comprehensive understanding of strategic interactions between network entities and their influence on AoI-related decision-making. This approach enables researchers to derive optimal strategies, study trade-offs, and design efficient communication protocols in various network scenarios. By leveraging game-theoretic approaches, communication systems can be better optimized for achieving low AoI, enhanced security, and improved overall performance[14].

4.2 Problem Statements and Research Objectives

In the context of communication systems, particularly in adversarial scenarios, optimizing the Age of Information (AoI) entails making strategic decisions regarding the frequency of information updates while accounting for potential adversarial disruptions. This multifaceted challenge necessitates the delicate equilibrium between minimizing AoI to enhance information freshness and managing the costs and risks associated with transmission attempts.

To address this challenge effectively, it is common to formulate the problem as a game, employing a specific utility function that quantifies the trade-offs between AoI minimization and cost control. The crux of the problem is to identify a Nash equilibrium (NE) within this strategic game, where both the transmitter and adversary make decisions that optimize their respective objectives while considering the actions of the other party. This equilibrium represents a stable state where no unilateral changes in strategies result in improvements for either player. A typical approach to study such problems is to model it as a game, with a particular utility function, and then try to find a Nash equilibrium (NE) for it [33].

The central question in this thesis is, 'How can we find and analyze the Nash equilibria in this game-theoretic framework to inform decision-making processes that balance the dynamics of AoI minimization, cost control, and adversarial interactions?' Solving this problem holds profound implications for optimizing communication systems in adversarial environments, ensuring timely, secure, and cost-effective information updates.

The research objective is to understand how to optimize the Age of Information (AoI) in communication systems, particularly in scenarios involving adversarial elements. The presence of adversaries complicates the reliability and cost aspects of information transmission, making the quest for optimal AoI values the core objective of this study.

Secondly, this study examines the interactions between the data sender and the adversary using a game theory approach. Analyzing these strategic interactions where both parties strive to balance minimizing AoI and controlling costs is another significant goal.

Lastly, the outcomes of this research should yield practical implications for real-world applications. These results should assist us in understanding how to inform decision-making processes in scenarios where AoI needs to be optimized. Thus, the research objective is to contribute to the field of communication theory by bridging theoretical modeling and practical applications.

5

Materials and Methods

5.1 Introduction to Numerical Optimization and Methodology

In this chapter, we delve into the Game Theory, Nash Equilibrium, and the numerical optimization techniques used for improving the Age of Information and methodology employed to address the adversarial game scenario with costs and the minimization of the Age of Information (AoI). We will discuss the specific steps taken to analyze the game and find the optimal values of key variables. This section provides an in-depth exploration of the numerical optimization techniques and methodology employed in the research. It focuses on the optimization process, parameter settings, and the code utilized for achieving the results.

5.2 Methodologies and Libraries

5.2.1 Game Theoretical Approach

Our research harnesses the power of game theory to model and analyze the interaction between a transmitter and a jammer within a communication system. This modeling is accomplished using Python 3.9 in conjunction with the Jupyter Lab [31] environment. The following methodologies are fundamental to our analysis:

- Nash Equilibrium: Central to our research is the concept of Nash Equilibrium, a stable state where neither the transmitter nor the jammer can unilaterally improve their strategies. Nash Equilibrium serves as a cornerstone for understanding strategic interactions in our communication game.

- Best Response Strategies: Both the transmitter and jammer continually adapt their strategies to maximize their utilities. The concept of best response strategies is pivotal to our research. It dictates that each player responds to the other's strategy in pursuit of their maximum payoff.

5.2.2 Data Analysis and Visualization

- fmincon : We employ the "fmincon" library as the cornerstone of our research, facilitating the minimization of Age of Information (AoI) across diverse M and p combinations. This optimization tool enables us to iteratively refine our strategies, ensuring that we achieve the lowest possible AoI. By defining optimization options, setting constraints, and storing results in matrices, we capture the minimum AoI values for specific M and p pairings. "fmincon" empowers our research by systematically reducing AoI and enhancing our strategies [49].

- NumPy: NumPy is employed for efficient numerical computations, especially for creating and manipulating arrays and matrices. It streamlines mathematical operations on the AoI matrix and strategy [23].

- Pandas: Pandas are employed to structure and organize data, simplifying our work with the research results. Data frames are used to store and manage the Nash Equilibrium strategies and associated utility values [48].

- Seaborn and Matplotlib: These visualization libraries are essential for creating line plots. These line plots serve to visualize Nash Equilibrium strategies and utility values across various combinations of cost parameters, facilitating a visual understanding of how equilibrium evolves with changing parameters [52, 25].

5.3 Finding Minimum Age of Information (AoI) Values and Nash Equilibrium Points

In this section, we provide detailed insights into our approach to finding the minimum Age of Information (AoI) values for a wide array of combinations of M (transmissions by the transmitter) and p (failure probability set by the adversary). Additionally, we elaborate on the methods employed to determine Nash equilibrium points, which are the linchpin of our research in adversarial communication scenarios.

5.4 Numerical Optimization Techniques

5.4.1 Finding Minimum AoI Values

The crux of our research revolves around obtaining the minimum AoI values for diverse combinations of M and p. We accomplish this through the use of the fmincon optimization function, which allows us to iteratively refine our strategies, minimizing the AoI. Our optimization process is comprehensive and includes defining optimization options, setting constraints to ensure valid solutions, and storing results in matrices where each element corresponds to the minimum AoI achieved for a specific M and p combination.

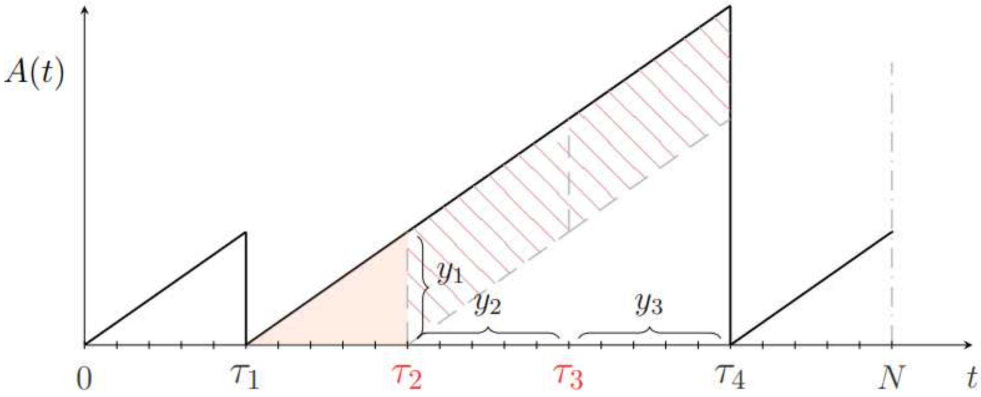

Figure 5.1: Example timeline for the AoI evolution over time. In the considered case, four transmissions are performed over a time horizon of duration N, and the second and third transmissions fail

The Age of Information, represented as (y), is defined based on these intervals. It comprises two vital components: the area of triangles associated with each update interval, representing the cost of transmitting information, and the area of parallelograms formed by pairs of intervals, contributing to AoI only in cases of transmission failures[38]. The average AoI over the finite time horizon can easily be computed as a function of y as:

$$\Delta(y) = \frac{1}{N} \sum_{i=0}^{M} \left(\frac{y_i^2}{2} + \sum_{j=i+1}^{M} y_i \cdot y_j \cdot (1-p)^{j-i} \right) \tag{5.1}$$

where the first contribution within brackets accounts for the area of the triangle of side yi that is always associated to the i-th update, whereas the subsequent summation captures the area of the parallelograms of sides yi and yj that contribute to the AoI only in case of failure of the i-th (and possibly of the following) transmission(s), weighted by the corresponding probabilities. An example of this reasoning is visually available in 6.1, where the loss of the second and third updates adds the dashed parallelogram areas y1 y2 and y1 y3 to the overall computation [38]. By summing up these components across all intervals, we arrive at the average AoI over the finite time horizon. This AoI function represents the core metric that we seek to minimize while considering the strategic actions of both the transmitter and the adversary. Our approach provides a systematic framework for understanding and optimizing AoI in adversarial communication scenarios, offering valuable insights into decision-making processes.

5.4.2 Optimization

```matlab
function val = delta(y, p, N)
    M = length(y) - 1;
    sum1 = 0;
    for i = 0:M
        sum2 = 0;
        for j = i + 1:M
            sum2 = sum2 + y(i + 1) * y(j) * (1 - p)^{j - i};
        end
        sum1 = sum1 + (y(i + 1)^2) / 2 + sum2;
    end
    val = sum1;
end
```

Code 5.1: The AoI function in Matlab format

The process of optimization plays a crucial role in our research, enabling us to identify optimal strategies and solutions. Our primary tool for this purpose is the fmincon function within MATLAB. The primary objective is to minimize delta values, representing the inefficiency of the system due to communication delay and jamming.

- Linear Equality and Inequality Constraints: Our optimization process adheres to linear equality and inequality constraints, ensuring that the sum of strategies equals one and that strategies remain non-negative.

5.4.3 Discretization of Variables

To enhance our numerical analysis, we discretize the variables M and p as follows:

- Discrete M Values: We explore eight distinct values for M, representing the number of transmissions by the transmitter. These values include 2, 3, 4, 5, 6, 7, 8, and 9. This discrete approach enables us to systematically investigate various communication strategies.

- Discretized p Values: While the adversary's failure probability, p, is theoretically continuous, we discretize it into ten values within the range of [0, 1]. These values (0.02, 0.07, 0.13, 0.15, 0.19, 0.23, 0.29, 0.35, 0.41, and 0.51) cover a broad spectrum of adversarial disruption scenarios, facilitating a comprehensive analysis of the strategic landscape.

5.5 The Game Between Transmitter and Adversary and Nash Equilibrium

This section provides an in-depth exploration of the strategic considerations of both Player 1, the transmitter, and Player 2, the adversary, within the context of Age of Information (AoI) optimization. These players are driven by their respective utility functions, and our primary objective is to gain insights into how they make decisions in the face of various challenges, including transmission costs and potential adversarial disruptions.

5.5.1 Player 1 - The Transmitter

Player 1, the transmitter, has the objective of minimizing the Age of Information (AoI) denoted as AoI(M, p). The transmitter's utility function takes into account both the optimization of AoI and the cost associated with its actions. This utility function is defined as follows: Transmitter's Utility

$$\text{Transmitter's Utility} = \text{AoI}(M, p) - C \cdot M \tag{5.2}$$

This utility function encompasses three critical components:

AoI Minimization: The primary goal of the transmitter is to reduce the Age of Information (AoI). Lower AoI values indicate more up-to-date information and improved system performance. The AoI(M, p) function quantifies the delay in information updates.

- Transmission Cost: The transmitter considers the cost associated with the number of transmissions, which is represented by M. The cost parameter C reflects the relationship between the number of transmissions and their associated expenses. The transmitter must strike a balance between minimizing both AoI and the cost of transmission, crucial for efficient communication.

- Adversary Considerations: In addition to optimizing AoI and managing transmission costs, the transmitter takes into account the actions of an adversary, denoted by p. The adversary has the capacity to engage in jamming attacks that disrupt communication. Therefore, the transmitter's decisions must factor in the potential challenges posed by the adversary.

5.5.2 Player 2 - The Adversary

Player 2, known as the adversary, holds a different objective in our strategic communication game. The adversary's primary goal is to maximize the Age of Information (AoI), represented by AoI(M, p). However, this objective must be balanced with the cost incurred due to elevating the failure probability, denoted as p. The adversary's utility function is expressed as follows: Adversary's Utility

$$\text{Adversary's Utility} = \text{AoI}(M, p) - K \cdot p \tag{5.3}$$

Here's an overview of the components of the adversary's utility function:

- AoI Maximization: The adversary's primary objective is to maximize the Age of Information (AoI). Higher AoI values represent delayed information updates, which can be advantageous in certain scenarios. The adversary strategically selects actions that lead to increased AoI. This delayed information can serve various purposes, such as reducing the real-time effectiveness of the communication.

- Cost Considerations: Simultaneously, the adversary considers the costs associated with raising the failure probability (p). The cost parameter (K) reflects the trade-off between elevating AoI and incurring additional costs. The adversary aims to balance these factors effectively. While increasing AoI can be beneficial, it must be done cost-effectively to avoid excessive expenses.

- Transmitter Considerations: The adversary takes into account the strategies and actions of the transmitter (Player 1). It recognizes that the transmitter seeks to minimize AoI and control costs. Therefore, the adversary strategically selects actions to counter the transmitter's efforts. This adversarial interaction adds complexity to the game, as both players aim to optimize their utility functions while reacting to each other's choices.

5.5.3 Utility Matrices and Strategic Decision-Making

To analyze the strategic decisions of both the transmitter and the adversary, we construct utility matrices. These matrices encapsulate their respective objectives under different parameter settings and provide valuable insights into how each player optimizes their utility function. Utility matrices are indispensable tools for understanding the interplay between the transmitter and the adversary.

These matrices rely on AoI values obtained for a diverse array of (M, p) pairs. Through systematic exploration of these pairs, we gain a comprehensive understanding of the strategic landscape in adversarial communication scenarios.

Our research employs a multifaceted approach to identify Nash Equilibrium points. Nash Equilibrium serves as a pivotal concept that characterizes stable states where strategic adjustments by one player do not lead to unilateral improvements. Our multifaceted approach involves modeling, numerical analysis, and iterative optimization to identify these crucial equilibrium points.

By employing the methodologies, techniques, and tools outlined in this chapter, our research lays the foundation for an in-depth exploration of the Age of Information optimization in adversarial communication scenarios. Our process is rigorous, and the findings aim to provide invaluable insights into decision-making processes in adversarial settings.

5.6 Scenario of The Game

After having utility matrices we see that a matrix game uses different costs (C and K). Changing these costs creates varied situations. At first, we used low costs for both the transmitter and jammer. The transmitter sends signals all the time, and the jammer jams continuously. When we increase the costs, the transmitter sends signals less often due to the expense, and the jammer must decide when to jam, considering the cost. It's like a game where both players aim to make the best choices.

The challenge lies in finding the Nash equilibrium, a point on the plot where neither player can improve by changing their strategy. The matrices for the transmitter and jammer change a lot with different costs, making it a puzzle. We try different combinations of C and K values, running simulations to discover these Nash equilibrium points.

Finding Nash equilibrium involves two matrices one for the transmitter and one for the jammer. These matrices should make sense on their own. The game scenario is that players really hate each other so player 1 wants to achieve fresh transmission and the other player 2 wants that player 1 gets old transmission instead. It's a bit like a ZERO SUM game, where they share the Age of Information but want opposite things. The transmitter wants to minimize it, and the adversary wants to maximize it. Adding costs makes the game more realistic; otherwise, the transmitter would use a massive M, and the adversary would employ a very high P if there were no costs. We played around with various numbers to get the best utilities and pinpoint the top-notch Nash points. All these results were neatly organized into a table, and from there, we cherry-picked the Nash equilibrium points. To visualize this, we whipped up some Python code using Seaborn to create plots.

6 Results

In this section, we present a detailed analysis of the results and findings obtained through our multifaceted approach to identifying Nash equilibrium points in adversarial communication scenarios. The primary objectives, which revolve around optimizing the Age of Information (AoI) and minimizing costs while navigating the strategic decisions of the transmitter and the adversary, have yielded several noteworthy outcomes.

6.1 Minimum AoI Values

Our research began by systematically computing the minimum AoI values for diverse combinations of transmission attempts (M) by the transmitter and failure probabilities (p) set by the adversary. The resulting data provides a comprehensive foundation for our strategic analysis. These AoI values, captured in Table 6.1, depict the relationship between the number of transmissions and the probability of successful information delivery. Initially, we compute and record the minimum AoI values for a wide range of combinations of M (transmissions by the transmitter) and p (failure probability set by the adversary).

Table 6.1: Age of Information (AoI) Results for Different Scenarios

$M\backslash p$	**0.02**	**0.07**	**0.13**	**0.15**	**0.19**	**0.23**	**0.29**	**0.35**	**0.41**	**0.51**
2	1.7	1.8	1.9	2.0	2.1	2.2	2.3	2.4	2.5	2.7
3	1.3	1.4	1.5	1.5	1.6	1.7	1.8	1.9	2.1	2.2
4	1.0	1.1	1.2	1.3	1.3	1.4	1.5	1.6	1.7	1.9
5	0.9	0.9	1.0	1.1	1.1	1.2	1.3	1.4	1.5	1.7
6	0.7	0.8	0.9	0.9	1.0	1.0	1.1	1.2	1.4	1.6
7	0.6	0.7	0.8	0.8	0.9	0.9	1.0	1.1	1.2	1.4
8	0.6	0.6	0.7	0.7	0.8	0.8	0.9	1.0	1.1	1.3
9	0.5	0.6	0.6	0.6	0.7	0.7	0.8	0.9	1.0	1.2

These values serve as the foundation for our strategic analysis.

6.2 Utility Matrices

The construction of utility matrices encapsulates the objectives of both the transmitter and the adversary within the context of varying cost parameters, C and K. The utility matrices, which serve as a blueprint for strategic decision-making, offer a snapshot of how both players optimize their utility functions while reacting to changes in cost parameters. The findings from these matrices lay the groundwork for our subsequent analysis.

6.3 Nash Equilibrium Identification

The identification of Nash equilibrium points was instrumental in understanding the strategic landscape of adversarial communication scenarios. The findings revealed the interactions influenced by cost parameters, strategic choices, and the dynamic nature of the game. Notably, we observed the deterrent effect of elevated costs on both players, leading to changes in their strategies and the overall outcome of the game. Leveraging the minimum AoI values and utility matrices, we employ a Python-based function to systematically identify Nash equilibrium points.

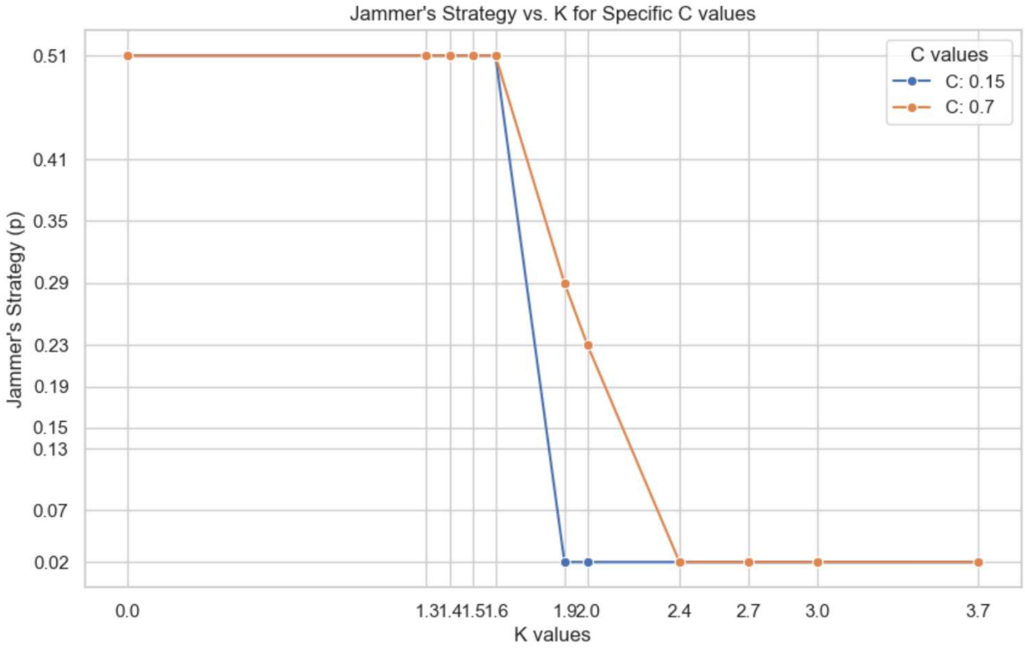

Figure 6.1: Dynamic Shifts in Nash Equilibrium Points with Varied Transmission Costs (C) and Adversary's Influence (K)

This function considers the cost parameter C for the transmitter (M) and the cost parameter K for the adversary (p), enabling us to pinpoint the optimal strategies for both players within a game-theoretic framework.

Analyzing the Figure 6.1 gives us some big ideas. As we move along the K-axis, showing the jammer's cost parameter, we see changes in Nash equilibrium points. Importantly, different C values bring out different Nash equilibria, showing how transmission costs really matter in deciding what strategies the transmitter goes for. Also, the lines on the graph show the complicated relationship between the transmitter trying to minimize AoI and the adversary trying to maximize it, making it clear how tricky this communication game can be.

In the Figure 6.2, we can have several key insights:

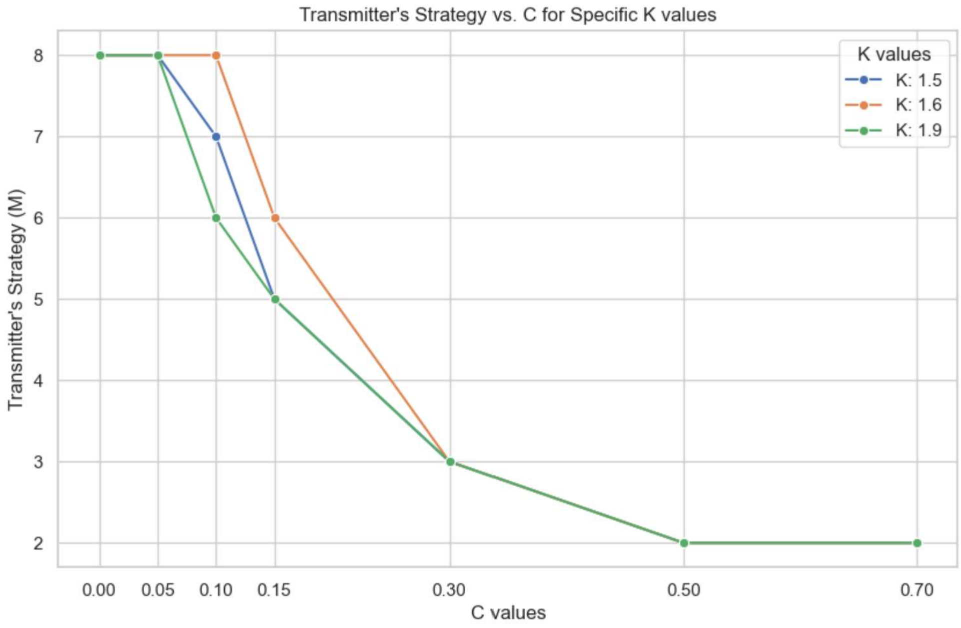

Figure 6.2: Cost Parameter Impact on Transmitter Strategy. Insights into transmitter decisions (M) under varying cost (C) and jammer strategy (K). Nash Equilibrium points marked.

- Cost Effect: There's a clear pattern when the cost goes up (C), the transmitter picks fewer strategies (M). This shows that higher costs make the transmitter less likely to try sending messages as often.

- Jammer's Strategy Impact (K): The different lines on the graph, each linked to various ways the jammer acts (K), really highlight how the jammer affects what the transmitter decides to do.

- Nash Equilibrium: The circles on the graph show Nash Equilibrium points. These are moments where both the transmitter and jammer have sort of agreed on choices that make their overall performance the best it can be.

To sum it up, the graph shows the balance between cost, the jammer's strategy, and the choices made by the transmitter. This representation, explained in this thesis, gives us a look into how these factors interact in game theory.

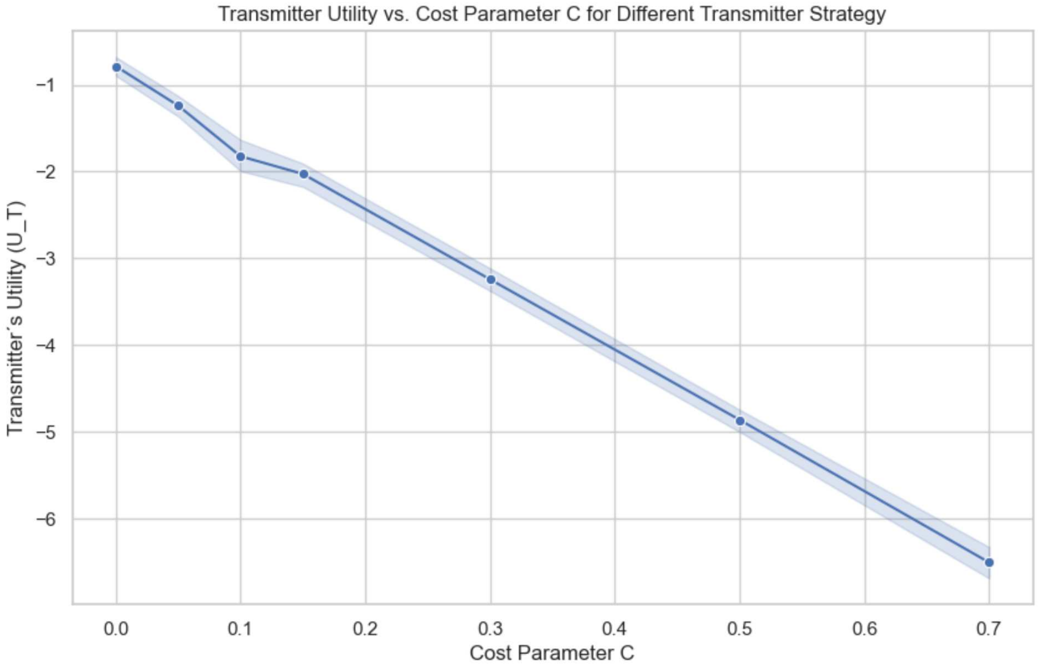

Figure 6.3: Cost (C) vs. Transmitter Utility (UT). Shows how increasing costs reduce transmitter utility for different strategic choices

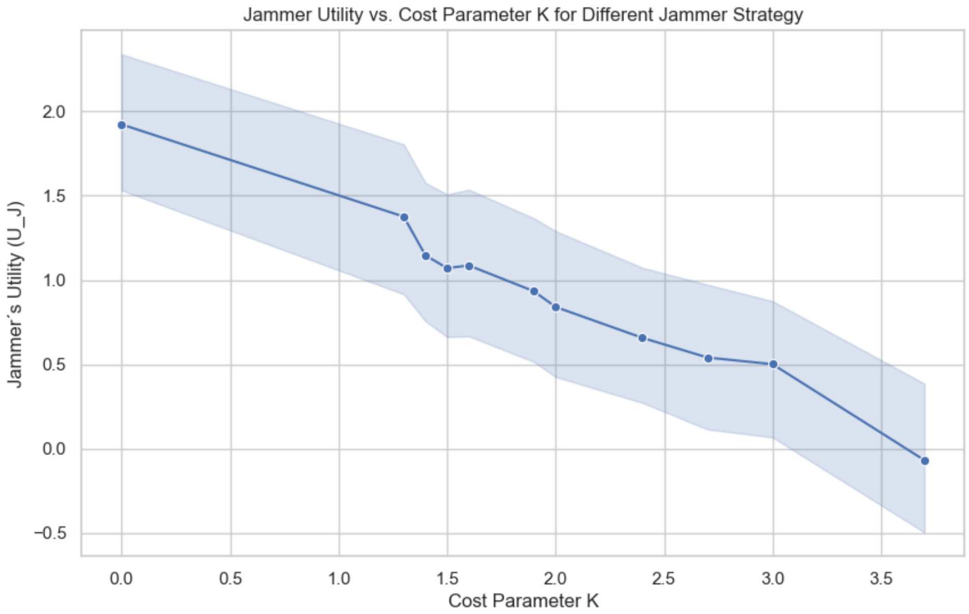

Figure 6.4: Cost (K) vs. Jammer Utility (UJ). Illustrates the decrease in jammer utility with rising costs and different strategic choices.

Figure 6.3, focuses on the perspective of the transmitter, with the cost parameter (C) as the main focus. On the graph, the X-axis shows different cost levels, and the Y-axis represents the utility (UT) gained from the chosen transmitter strategy (M). Each line on the graph represents a specific transmitter strategy, and circular markers highlight important data points. As the cost (C) goes up, the transmitter's utility (UT) goes down, showing that higher costs discourage the transmitter and result in lower utility. The various lines emphasize how different transmitter strategies (M) significantly impact utility, highlighting the importance of strategic decision-making in scenarios where costs matter. Figure 6.4, where strategic decisions are influenced by the cost parameter (K). On the graph, the X-axis shows different cost parameters, while the Y-axis represents the jammer's utility (UJ). Similar to the first graph, each line on this one represents a different jammer strategy, and circular markers highlight important data points.

When you look closely, you'll notice that when the cost factor (K) goes up, the jammer's (UJ) goes down. This means that higher costs discourage the jammer, affecting their actions in a bad way. The various lines on the graph show how the choices we make (p) play a big role in shaping the jammer's situation.

The graph helps us see the big picture and adds a visual element to our strategic insights. The outcomes at Nash equilibrium give decision-makers and researchers in communication theory a complete understanding of strategic moves and their results in tough situations.

In summary, our research has been a mix of different fields, we have used mathematical modeling, numerical optimization, and the principles of game theory to deal with the big challenge of optimizing the Age of Information (AoI) in adversarial communication scenarios. In this chapter, we've explained step by step how we did it and the tools we used, giving a clear picture of what we've discovered. Our method has helped us understand the complicated decisions that they make. By using mathematical modeling and game theory, we've their objectives, constraints, and interactions, paving the way for more effective communication strategies in adversarial environments. Our research shows how bringing different fields together can make a real impact. It proves that we can connect what we know from theory to real-world problems, especially in the fast-changing world of communication theory and improvement.

7

Conclusions and Future Works

This research was driven by the ambition to optimize the Age of Information (AoI) in adversarial communication scenarios, a challenge within the realm of communication theory. Our primary goal was to minimize AoI while considering the strategic interactions between a transmitter and an adversary, both guided by their utility functions and influenced by cost parameters. This conclusion provides a structured summary of our research journey, highlighting the key steps we took and the significant results we achieved.

We leveraged the power of game theory, numerical optimization, and data analysis. The methodologies and libraries we utilized included Python for game theory modeling and utility computation, MATLAB for numerical optimization, and various data analysis and visualization tools such as NumPy, Pandas, Seaborn, and Matplotlib.

Our findings have discussed the relationship between the number of transmission attempts (M) and the failure probability set by the adversary (p). We systematically computed minimum AoI values for various combinations of M and p, forming the bedrock of our strategic analysis. The construction of utility matrices provided a blueprint for understanding how both the transmitter and the adversary optimize their utility functions while reacting to changes in cost parameters, C and K.

The identification of Nash equilibrium points, in a Python-based environment, allowed us to pinpoint the optimal strategies for both players within a game-theoretic framework. The graphical representations of these equilibrium points offered a visual insight into the dynamic interplay of cost parameters, strategic choices, and the complex dynamics of the game.

The observed trends in the relationship between cost parameters and utility values hold practical relevance. Higher costs emerged as a deterrence factor, impacting both the transmitter and the adversary in their strategic decisions. The graphical representations, particularly the Nash equilibrium points, offer decision-makers and researchers a visual grasp of the nuanced interplay of these pivotal parameters in adversarial communication.

Acknowledging the limitations of this research, especially in terms of simplifications made in modeling, we acknowledge that real-world scenarios may involve more complexities. Nonetheless, our work opens the door to a new understanding of AoI optimization in adversarial communication, providing valuable insights for real-world applications.

The research by [53] and [16] has offered valuable insights into the resilience of real-time monitoring and control systems against jamming attacks, emphasizing dynamic game models and stationary equilibriums at the MAC layer. These studies have contributed distinct viewpoints to the AoI optimization discourse, emphasizing the need for adaptability and equilibrium strategies.

Furthermore, [39] delves into the physical layer of security, providing profound insights into the ongoing interactions between legitimate users and potential attackers. The static game model introduced in [39] offers an alternative approach, highlighting the development of dynamic defense policies to effectively counter adversarial threats over time.

In parallel, [20], while not directly addressing jamming attacks, adds an essential dimension by considering eavesdroppers. This work emphasizes the optimal generation rate for status updates, effectively balancing the age of information between legitimate receivers and eavesdroppers while focusing on the critical aspect of confidentiality.

Moreover, [3] significantly enriches our understanding of AoI by exploring a scenario involving two strategic information sources. In this scenario, these sources independently determine the timing of information updates at a receiver, taking into account their individual update costs and the global benefit derived from reducing the receiver's AoI. The game-theoretic analysis in [3] uncovers distinct Nash equilibria and emphasizes the role of coordination to achieve efficiency in decision-making.

These research papers collectively contribute to our understanding of the multifaceted approaches and strategies available for mitigating the age of information in adversarial environments. As the digital landscape continues to evolve, these insights empower us to confront the dynamic challenges posed by adversaries in enhancing information security and fortifying the robustness of communication systems. The synthesis of dynamic game models, stationary equilibriums, physical layer security, trade-offs, and synchronization strategies deepens our collective understanding of AoI and reinforces our capacity to safeguard the integrity of critical information flows.

In essence, this thesis has effectively tackled the challenges of optimizing AoI in adversarial communication scenarios. Our work not only expands theoretical understanding but also furnishes practical solutions applicable in real-world contexts where AoI optimization is imperative.

7.1 Future Research Directions

Age of Information (AoI), a dynamic metric with wide-ranging applications in communication systems, presents several promising avenues for future research. Here are some of the key directions:

1. **Dynamic Network Topologies:** Investigating AoI in dynamically changing network structures and understanding how it evolves in response to network dynamics [10].

2. **Energy-Constrained Systems:** Analyzing AoI in scenarios with strict energy constraints, such as battery-powered IoT devices, and optimizing energy-efficient communication [57].

3. **Security and Privacy:** Exploring the interplay between AoI optimization and security measures to develop strategies that are robust against adversarial actions.

4. **Machine Learning and AI Integration:** Investigating the integration of machine learning and artificial intelligence techniques to enhance AoI-aware decision-making processes[42].

5. **AoI in Edge Computing:** Understanding the implications of AoI in edge computing environments, where data processing occurs closer to the data source[47].

6. **AoI-Aware Scheduling:** Investigating scheduling algorithms that take AoI metrics into account for timely data updates and transmission[41].

7. **AoI in Cyber-Physical Systems:** Understanding the role of AoI in cyber-physical systems, where timely information is crucial for control and automation[40].

These research paths, collectively, have the potential to not only advance our comprehension of Age of Information but also to contribute to the development of communication strategies that are robust, efficient, and adaptable to the ever-changing landscape of modern networks.

References

[1] N. Abuzainab and W. Saad. “Dynamic connectivity game for adversarial internet of battlefield things systems”. In: *IEEE Internet of Things J.* (2018).

[2] A. Asheralieva and D. Niyato. “Optimizing Age of Information and Security of the Next-Generation Internet of Everything Systems”. In: *IEEE INTERNET OF THINGS JOURNAL* 9.20 (Oct. 2022).

[3] L. Badia. “Age of Information from Two Strategic Sources Analyzed via Game Theory”. In: *IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. 2021.

[4] L. Badia. “Impact of Transmission Cost on Age of Information at Nash Equilibrium in Slotted ALOHA”. In: *IEEE Networking Letters* 4.1 (Mar. 2022), pp. 30–33. DOI: 10.1109/LNET.2021.3133220.

[5] L. Badia and A. Munari. “A Game Theoretic Approach to Age of Information in Modern Random Access Systems”. In: *2021 IEEE Globecom Workshops (GC Wkshps)*. Madrid, Spain, 2021, pp. 1–6. DOI: 10.1109/GCWkshps52748.2021.9682065.

[6] L. Badia, A. Zanella, and M. Zorzi. “Game Theoretic Analysis of Age of Information for Slotted ALOHA Access With Capture”. In: *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. New York, NY, USA, 2022, pp. 1–6. DOI: 10.1109/INFOCOMWKSHPS54753.2022.9797974.

[7] Subhankar Banerjee and Sennur Ulukus. "Age of Information in the Presence of an Adversary". In: *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. New York, NY, USA: IEEE, 2022, pp. 1–6. DOI: 10.1109/INFOCOMWKSHPS54753.2022.9798166.

[8] Subhankar Banerjee, Sennur Ulukus, and Anthony Ephremides. "Age of Information of a Power Constrained Scheduler in the Presence of a Power Constrained Adversary". In: (Jan. 2023). Submitted on 3 Jan 2023. DOI: 10.48550/arXiv.2301.01276. arXiv: arXiv:2301.01276 [cs.IT].

[9] M. Bastopcu and S. Ulukus. "Age of Information for Updates With Distortion: Constant and Age-Dependent Distortion Constraints". In: *IEEE/ACM Transactions on Networking* 29.6 (Dec. 2021), pp. 2425–2438. DOI: 10.1109/TNET.2021.3091493.

[10] Ahmed M. Bedewy, Yin Sun, and Ness B. Shroff. "Age-Optimal Information Updates in Multihop Networks". In: *IEEE Transactions on Information Theory* (2023). Dept. of ECE, Dept. of CSE, The Ohio State University, Columbus, OH. Emails: {bedewy.2, sun.745, shroff.11}@osu.edu.

[11] V. Bonagura et al. "A Game of Age of Incorrect Information Against an Adversary Injecting False Data". In: *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*. Venice, Italy, 2023, pp. 347–352. DOI: 10.1109/CSR57506.2023.10224952.

[12] Thomas Brewster. "Marriott". In: *Forbes* (2018). https://www.forbes.com/sites/thomasbrewster/2018/11/30/marriott-hackers-stole-data-on-500-million-guests---passports-and-credit-card-info-included/?sh=1f103c5e3b94.

[13] B. Buyukates, A. Soysal, and S. Ulukus. "Age of Information in Multihop Multicast Networks". In: *Journal of Communications and Networks* 21.3 (June 2019), pp. 256–267. DOI: 10.1109/JCN.2019.000032.

[14] Yi Cao, Xinyan Qian, and Dawei Zeng. "Game-theoretic Analysis for the Trade-Off Between RD and Marketing in Chinese Cosmetic Market". In: *Proceedings of the 2022 7th International Conference on Financial Innovation and Economic Development (ICFIED 2022)*. Atlantis Press, 2022, pp. 541–547. ISBN: 978-94-6239-554-1. DOI: `10.2991/aebmr.k.220307.087`. URL: `https://doi.org/10.2991/aebmr.k.220307.087`.

[15] A. Chaintreau, J.-Y. Le Boudec, and N. Ristanovic. "The age of gossip: Spatial mean field regime". In: *ACM SIGMETRICS Perform. Eval. Rev.* 37.1 (June 2009), pp. 109–120.

[16] He Chen et al. "Secure Status Updates under Eavesdropping: Age of Information-based Physical Layer Security Metrics". In: (Feb. 2020). DOI: `10.48550/arXiv.2002.07340`. arXiv: `arXiv:2002.07340 [cs.CR]`.

[17] Wikipedia contributors. *Zero-sum game*. URL: `https://en.wikipedia.org/wiki/Zero-sum_game`.

[18] M. Costa, M. Codreanu, and A. Ephremides. "On the Age of Information in Status Update Systems With Packet Management". In: *IEEE Transactions on Information Theory* 62.4 (Apr. 2016), pp. 1897–1910. DOI: `10.1109/TIT.2016.2533395`.

[19] Frank Cremer et al. "Cyber risk and cybersecurity: a systematic review of data availability". In: 47 (2022). Open Access, pp. 698–736.

[20] Laura Crosara, Nicola Laurenti, and Leonardo Badia. "It Is Rude to Ask a Sensor Its Age-of-Information: Status Updates Against an Eavesdropping Node". In: (June 2023). Submitted on 14 Jun 2023. Focus to learn more. DOI: `10.48550/arXiv.2306.08475`. arXiv: `arXiv:2306.08475v1 [cs.CR]`.

[21] "Equifax". In: *The New York Times* (2017). `https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html`.

[22] A. Garnaev et al. "Maintaining Information Freshness under Jamming". In: *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. Paris, France, 2019, pp. 90–95. DOI: 10.1109/INFCOMW.2019.8845146.

[23] Charles R. Harris et al. "Array programming with NumPy". In: *Nature* 585 (2020), pp. 357–362. DOI: 10.1038/s41586-020-2649-2.

[24] Q. He, D. Yuan, and A. Ephremides. "Optimal link scheduling for age minimization in wireless systems". In: *IEEE Transactions on Information Theory* 64.7 (July 2018), pp. 5381–5394.

[25] J. D. Hunter. "Matplotlib: A 2D graphics environment". In: *Computing in Science & Engineering* 9.3 (2007), pp. 90–95. DOI: 10.1109/MCSE.2007.55.

[26] iLink Digital. *Financial Impact of Cyber Breaches on Business Costs*. URL: https://www.ilink-digital.com/insights/blog/financial-impact-cyber-breaches-business-costs/.

[27] Yoshiaki Inoue. "The Probability Distribution of the AoI in Queues with Infinitely Many Servers". In: *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, July 2020, pp. 1–6. ISBN: ISBN Information. DOI: 10.1109/INFOCOMWKSHPS50562.2020.9162968.

[28] Charles A. Kamhoua, Niki Pissinou, and Kazem Makki. "Game theoretic modeling and evolution of trust in autonomous multi-hop networks: Application to network security and privacy". In: *Proc. IEEE Int. Conf. Commun. (ICC)*. IEEE. 2011, pp. 1–6.

[29] P. Kaswan and S. Ulukus. "Age of Gossip in Ring Networks in the Presence of Jamming Attacks". In: *2022 56th Asilomar Conference on Signals, Systems, and Computers*. Pacific Grove, CA, USA, 2022, pp. 1055–1059. DOI: 10.1109/IEEECONF56349.2022.10051981.

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

[31] Thomas Kluyver et al. "Jupyter Notebooks – a publishing format for reproducible computational workflows". In: *Positioning and Power in Academic Publishing: Players, Agents and Agendas*. Ed. by F. Loizides and B. Schmidt. IOS Press. 2016, pp. 87–90.

[32] A. Kosta, N. Pappas, and V. Angelakis. "Age of Information: A New Concept, Metric, and Tool". In: *Foundations and Trends in Networking* 12.3 (2017), pp. 162–259.

[33] Rahul Vaze Kumar Saurav. "Game of Ages". In: *arXiv e-prints* (2020). eprint: `2001.04427`. URL: `https://arxiv.org/abs/2001.04427`.

[34] P. D. Mankar, M. A. Abd-Elmagid, and H. S. Dhillon. "Spatial Distribution of the Mean Peak Age of Information in Wireless Networks". In: *IEEE Transactions on Wireless Communications* 20.7 (July 2021), pp. 4465–4479. DOI: `10.1109/TWC.2021.3059260`.

[35] M. E. Mkiramweni et al. "Game-Theoretic Approaches for Wireless Communications with Unmanned Aerial Vehicles". In: *IEEE Wireless Communications* 25.6 (Dec. 2018), pp. 104–112. DOI: `10.1109/MWC.2017.1700250`.

[36] A. Mukherjee. "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints". In: *Proc. of IEEE* 103.10 (Oct. 2015), pp. 1747–1761.

[37] A. Mukherjee et al. "Principles of physical layer security in multiuser wireless networks: A survey". In: *IEEE Commun. Surv.* 16.3 (2014), pp. 1550–1573.

[38] A. Munari and L. Badia. "The Role of Feedback in AoI Optimization Under Limited Transmission Opportunities". In: *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*. Rio de Janeiro, Brazil, 2022, pp. 1972–1977. DOI: `10.1109/GLOBECOM48099.2022.10001535`.

[39] G. D. Nguyen et al. "Impact of Hostile Interference on Information Freshness: A Game Approach". In: *2017 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*. Paris, France, 2017, pp. 1–7. DOI: 10.23919/WIOPT.2017.7959909.

[40] Paulo César Prandel and Priscila Solis Barreto. "Computational Modeling of Age of Information for Cyber-physical Systems". In: *IEEE Latin-American Conference on Communications (LATINCOM)*. IEEE. IEEE, Nov. 2021, Page Range. DOI: 10.1109/LATINCOM53176.2021.9647854.

[41] Z. Qin et al. "AoI-Aware Scheduling for Air-Ground Collaborative Mobile Edge Computing". In: *IEEE Transactions on Wireless Communications* 22.5 (May 2023), pp. 2989–3005. DOI: 10.1109/TWC.2022.3215795.

[42] Yalin E. Sagduyu, Sennur Ulukus, and Aylin Yener. "Age of Information in Deep Learning-Driven Task-Oriented Communications". In: *arXiv preprint arXiv:2301.04298* (2023). arXiv:2301.04298 [cs.IT]. URL: https://doi.org/10.48550/arXiv.2301.04298.

[43] J. Selen et al. "The Age of Information in Gossip Networks". In: *Analytical and Stochastic Modeling Techniques and Applications*. Ed. by A. Dudin and K. De Turck. Vol. 7984. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2013. DOI: 10.1007/978-3-642-39408-9_26.

[44] S. Sicari et al. "Security, privacy and trust in the internet of things: The road ahead". In: *Computer networks* 76 (2015), pp. 146–164.

[45] Y. Sun et al. "Update or wait: How to keep your data fresh". In: *IEEE Trans. Inf. Theory* 63.11 (Nov. 2017), pp. 7492–7508.

[46] R. Talak, S. Karaman, and E. Modiano. "Improving Age of Information in Wireless Networks With Perfect Channel State Information". In: *IEEE/ACM TRANSACTIONS ON NETWORKING* 28.4 (Aug. 2020).

[47] Z. Tang et al. "Age of Information Analysis of Multi-user Mobile Edge Computing Systems". In: *2021 IEEE Global Communications Conference (GLOBECOM)*. Madrid, Spain, 2021, pp. 1–6. DOI: 10.1109/GLOBECOM46510.2021.9685769.

[48] The pandas development team. *pandas-dev/pandas: Pandas*. Version latest. Feb. 2020. DOI: 10.5281/zenodo.3509134. URL: https://doi.org/10.5281/zenodo.3509134.

[49] The MathWorks, Inc. *fmincon: MATLAB Optimization Toolbox*. https://www.mathworks.com/help/optim/ug/fmincon.html. February 22, 2023.

[50] S. Wang et al. "Distributed Reinforcement Learning for Age of Information Minimization in Real-Time IoT Systems". In: *IEEE Journal of Selected* (Apr. 2022).

[51] Y. Wang et al. "Covert Communications With Constrained Age of Information". In: *IEEE WIRELESS COMMUNICATIONS LETTERS* 10.2 (Feb. 2021).

[52] Michael L. Waskom. "seaborn: statistical data visualization". In: *Journal of Open Source Software* 6.60 (2021), p. 3021. DOI: 10.21105/joss.03021. URL: https://doi.org/10.21105/joss.03021.

[53] Y. Xiao and Y. Sun. "A Dynamic Jamming Game for Real-Time Status Updates". In: *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. Honolulu, HI, USA, 2018, pp. 354–360. DOI: 10.1109/INFCOMW.2018.8407017.

[54] "Yahoo Hack: 3 Billion Users' Data Stolen". In: *The New York Times* (2017). https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

[55] R. D. Yates. "Lazy is Timely: Status Updates by an Energy Harvesting Source". In: *2015 IEEE International Symposium on Information Theory (ISIT)*. Hong Kong, China, 2015, pp. 3008–3012. DOI: 10.1109/ISIT.2015.7283009.

[56] R. D. Yates et al. “Age of Information: An Introduction and Survey”. In: *IEEE J. Sel. Areas Commun.* 39.5 (2021), pp. 1183–1210.

[57] F. Zhao et al. “AoI-Constrained Energy Efficiency Optimization in Random-Access Poisson Networks”. In: *2022 IEEE Wireless Communications and Networking Conference (WCNC)*. Austin, TX, USA, 2022, pp. 1123–1128. DOI: `10.1109/WCNC51071.2022.9771861`.

Acknowledgments

ZAZAKÎ: Eya perwerdeya ma Padovadi ma dîya tî her wext ver midîb. Rê rehar mî, wati mi, patdayiya min Mesut Yalinkaya tû her wext mîra yinu kerd her wext vêr mdib. Ez tûra zaf we û war bîya.
TURKCE: Padova'daki egitim süreci boyunca, bana her zaman destek olan, yol arkadasim, sevgilim, destekcim Mesut Yalinkaya'ya yapabileceklerime her zaman inandigi ve yanimda oldugu icin tesekkür ediyorum.

TURKCE: Uzun yillardir hayatimda olan ve asla beni yalniz birakmayan canim dostum, kiz kardesim Gizem Ugur'a bu surecte verdigi destekler icin tesekkur ediyorum.

KURDÎ: Ez spasiya Berfîn Kurhan, Dîlek Kurhan, Alis Ideli, Marianna Carrano, Özlem Uc Çicek û Abdullah Çîçek dikim, ku tevî du sal in ez wan nas dikim, malbata min a duyemîn in, ku her tim bi min bawer kirin û bi min re bûn alî.

TURKCE: Kisa zamanda tanistigim ve bana her konuda destegini esirgemeyen canim arkadasim Rabia Yapicioglu'na tesekkur ediyorum.

TURKCE: Son olarak kucucuk bir sehirden dunyaya acilip asla hayallerinden vazgecmeyen, herseyi bir sekilde halledip yoluna koymayi basarabilen kendimle gurur duyuyorum. Yasanilan butun zorluklara ragmen her zaman dik durmaya ve daha iyi basarilara imza atmaya.