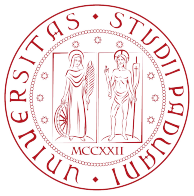

University of Padova

Department of Civil, Environmental and Architectural Engineering

Master Thesis in Mathematical Engineering

Age of information for quantum communication channels with monogamy of entanglement

Supervisor
Leonardo Badia
University of Padova

Master Candidate
Aygun Jabrayilova

Student ID
2013059

Academic Year
2023-2024

I would like to thank my friends and family for always being there for me.

Contents

Abstract

Communication systems play a key role in today's society due to the enormous flow of information that we share daily in every aspect of our lives. Among others, there is a continuous flow of information regarding status updates that has to be shared to assure the well-functioning of multiple devices. It is, therefore, mandatory to ensure that this information can be shared as fast as possible, and without the risk of being lost or accessed by the wrong recipients. Particularly, eavesdropping is a matter of great importance. In this thesis work, we analyze an information update system, where the communication between a sender and a receiver is taking place through quantum channels, and we consider the presence of two malicious eavesdroppers. To tackle this problem, we employed game theory as a modeling approach and utilized the computational tool MATLAB to identify the Nash equilibrium points. Finally, we analyze the transmission rate and eavesdropper probability, together with the total utility and the price of anarchy for the different Nash equilibrium points and for different cost values.

1 Introduction

It is well known that we are facing a data revolution. Thanks to technological advances, we are experiencing a constant multiplication of the amount of data that needs to be shared, stored, and analyzed every day. To observe this, it is sufficient to consider how annual mobile data traffic worldwide has grown in the past 10 years. As depicted in Figure 1[1], the growth is not linear, and it is expected to continue growing even more in the next 5 years, reaching the impressive amount of 403 exabytes per month in 2029.

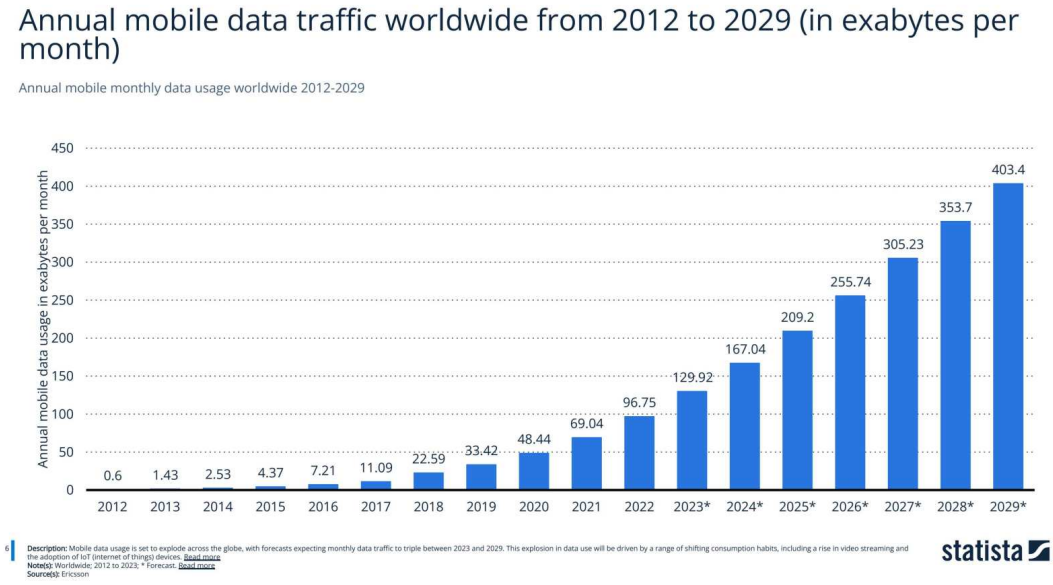

Figure 1: The graph provides the annual mobile data traffic from 2012 measured in exabytes per month, with forecasts extending until 2029.

It is thus imperative to provide systems that enable big data storage and fast computation while requiring lower power supply. One possible solution to address this matter is the introduction of quantum communication systems [1]. Thanks to the property of quantum mechanics known as entanglement, the particles exhibit a strong and unique connection, providing a more robust

[1] `https://www.statista.com/study/14634/big-data-statista-dossier/`

communication system [2]. Additionally, due to the superposition of the quantum state, this kind of communication is more difficult to intercept, providing a much more secure network compared to classical means. Furthermore, because of the mechanism of superadditivity, combining quantum channels results in a greater capacity than the sum of the channels themselves, resulting in bigger capability at the same cost.

These are some of the reasons why quantum communication has garnered significant attention in recent years: the funding for quantum communication sector worldwide has reached 1 billion U.S. dollars, with 72 startups worldwide as of December 2021[2].

Within communication technologies, quantum communication offers a revolutionary advancement with unparalleled security and efficiency. One of the main concepts of this advancement is the Age of Information (AoI), which quantifies the freshness of the information, making it a key factor in real-time communication systems [3]. As we will see on proceeding sections, decreasing AoI is a commonly desirable choice due to having fresh information on receiver's side in a quantum communication system. On the other hand, monogamy of entanglement is a principle stating that strongly entangled particles cannot be equally entangled with a third party. This is one of the cornerstones of quantum communication security [4]. Monogamy of entanglement plays especially crucial role when AoI is considered in scenarios involving more than one eavesdroppers [5]. While an eavesdropper takes an action to intercept the information, transmitter of the information adjusts its action to maintain lower AoI at the receiver's side. On top of that, in the presence of multiple eavesdroppers, eavesdroppers will try to minimize the AoI in their respective side, highlighting the effect of the monogamy of entanglement. This thesis focuses on the previous work done on the field, especially [5] and extending this paper to multiple eavesdroppers instead of one. Aim of the thesis is to explore and analyze the balance between AoI and secure communication while multiple eavesdroppers are present in a quantum communication channel with monogamy of entanglement.

State of the art within quantum communication channels and monogamy of entanglement is constantly developing with recent works also connecting these concepts to Age of Information (AoI). To start with, real-time status updates gained popularity, having affect on various areas such as news, weather reports, social media, temperature and humidity updates from a forest due to prevention of forest fires, information regarding the velocity and acceleration of a car in order to assist drivers in safer travel and logistics, etc. [3],[6],[7]. Although the list of the important results is not short, we give few examples of such works. To start with, [8] focuses on minimizing the age of status updates sent by vehicles over a carrier-sense multiple access (CSMA) network, [9] analyzes maximization

[2] https://www.statista.com/study/115330/quantum-computing/

of the freshness of data in warehouses to meet user demands, [10] delves into periodic transactions updating real time databases. Additionally, security in quantum communication channels is also analyzed in various works, including scenarios with one or multiple eavesdroppers [5],[11],[12],[13]. It is also to be highlighted that most of these works are considering quantum wiretap channel [14]. On the other hand, although there are examples of it, only few studies in the state of the art combine security, freshness of information and game theory [12]; and most of these studies focus on intentional jamming [15],[16]. Examples include [17], where friendly jamming in wireless LANs is analyzed, and [18], which is focusing on the the ease of implementation of friendly jamming with off-the-shelf smartphones. As mentioned before, the list of the related work is not limited to what has been discussed above; nevertheless it is important to highlight that the thesis is mainly focused on the work done in [3],[12],[19],[20],[21], and especially in [5].

Before we have an extensive look at the background information, we describe the organization of the thesis. Next section, *Preliminaries*, focuses on fundamental and relevant information to the thesis and covers core necessary parts before moving to the main section of the thesis, *Quantitative Analysis and Modelling*. *Preliminaries* is divided into three subsections: *Age of Information in Communication Systems*, *Quantum Entanglement and Communication Security*, and *Game Theory for Communication Systems*. Each of these subsections is covering fundamental definitions, statements, and arguments relevant to the age of information (AoI), quantum entanglement, and game theoretic scenarios in communication systems, respectively. Specifically, monogoamy of entanglement is discussed in section 2.2.2. The key contribution of the thesis is presented in the main section, *Quantitative Analysis and Modelling*. This section is divided into two subsections: *Theoretical Computation*, where mathematical equations are derived within the considered scenario, and *Numerical Results* where MATLAB is used for further complex computations and results are demonstrated in graphs. Finally, we represent the *Conclusion* and relevant *References*.

2 Preliminaries

2.1 Age of Information in Communication Systems

2.1.1 Fundamentals of AoI

It is no doubt that developing technology had an immense positive effect on information sharing on a global scale [22]. Subsequent increase in need of faster communication lead to the improvement in communication systems. However, improved communication systems and methods of information sharing also introduced complex problems to be tackled and focused on for further enhancement of such systems. One of the prominent examples, is the concept of *real-time status* updates which gained popularity and became a focus of further investigation with the increase of portable and modern devices [3]. Its importance in various systems, especially in wireless communication, is a driving reason for the current investigation.

Real-time status updates can be observed in various communication systems in numerous areas such as transportation and logistics, healthcare, finance and trading, emergency services, consumer services, smart home devices, information technology, and many other distinct areas where information sharing and communication network is of great importance. To list some tangible examples, real-time GPS updates allow companies to track shipments and optimize routes for more cost and time efficient delivery [23], real-time data transfer of patient's medical background could lead to immediate important decision making and saving lives [24], real-time updates on stock prices and market data enable traders and companies to execute informed and immediate financial strategies [25], etc. In all of these examples, the goal is to make sure that the recipient has access to up to date information and is able to monitor current relevant conditions and information. In other words, the core principal is the fact that a source generates time conditioned status updates which then are transmitted to the recipient through a communication system.

The critical aspect of real-time status updates is the freshness of the transmitted data, or in other words as timely as possible status transmission. Delay, throughput, queue length and several other performance metrics fail to fully capture the freshness, or timeliness of the data to be transmitted [26]. Delay, or also known as latency, is the time required for a packet of data to travel from a source to a recipient. In other words, it is the duration of time required to process data and deliver to a recipient by the system. Throughput is the rate at which the data is transmitted through communication system, and also referred as the capacity of a system to handle the data flow. Queue length indicates the number of packets of data waiting in a queue to be processed and delivered to

the recipient. It should be mentioned that the queue length can affect the delay and throughput of a system immensely. Nevertheless, the freshness of the transmitted data is not captured through neither of these examples of performance metrics. In order to focus on this crucial aspect of status updates, the concept of *Age of Information* (AoI) should be introduced. Consider a system where status update is to be sent from a source to a recipient, while the transmitted data is processed for a random time before being used. Given this information, we define the age of information at the side of the recipient at time t as follows [3]:

$$\delta(t) = t - \sigma(t) \tag{1}$$

where $\sigma(t)$ represents the instant when the recipient processed the transmitted data or update before time t. It is important to note that, for further parts of this thesis, we assume that all transmitted status updates carry fresh information to the recipient and the propagation time is instantaneous, setting the delay to zero [27].

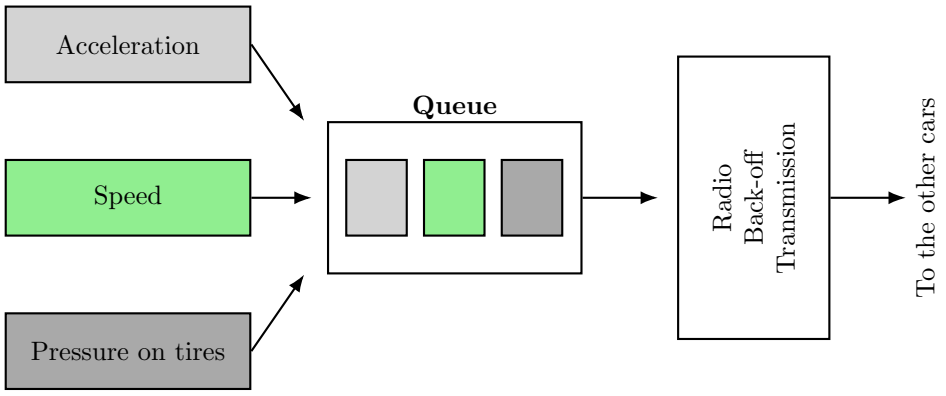

Figure 2: Status updates of vehicle sensors waiting in queue before being transmitted to other vehicles through in-vehicle radio.

Natural and initial strategy in order to have minimal AoI at the side of a recipient is to receive status updates instantaneously as they are generated by the source, while also letting the source generate status updates as quick as possible. However, this is not possible since the real life constraints causes status updates to be received at the side of a recipient only after nonzero and certain random

time in the system. Figure 2 [3] shows a simple diagram where status updates are generated by sensors within vehicle, for the acceleration, speed and pressure on tires, and queued to wait before being transmitted to the other cars through the in-vehicle radio. One of the main factors of this delay is the concept of queue [28] [29], which will be discussed in more detail in the next part.

2.1.2 AoI in M/M/1 Queue Systems

The study of queuing systems is a mathematical discipline that delves into the analysis of waiting lines. This field of study finds its origins in the early 1900s when it was initially formulated to describe the incoming call patterns at the Copenhagen Telephone Exchange Company. However, the applicability of queuing theory extends far beyond telecommunications and can be effectively employed in any system characterized by the presence of a source and a customer.

Queuing system models have found wide-ranging utility in numerous domains, offering insights into the behavior of communication systems, traffic management in industrial settings, and even facilitating efficient warehouse management in diverse facilities such as hospitals and retail establishments [6].

For the purpose of this discussion, we will concentrate on a specific scenario, namely, an information update system. In this context, there is a sender equipped with a sensor designed to provide information, a server responsible for processing and handling the signals, and a recipient that receives the processed information. Various protocols govern the signal processing procedures executed by the server [30]. The *First Come First Served* (FCFS) protocol is one in which the information is transmitted in the order it becomes available. This model is widely adopted and performs well in standard situations where the server is not overloaded with excessive information. However, if the server becomes congested and the FCFS protocol is still in use, new information may be discarded if there is no available storage space. In contrast to FCFS, the *Last Comes First Served* (LCFS) protocol prioritizes displaying the most recent information. While this ensures that the freshest data is presented, it may result in important information that gets queued but never displayed. A hybrid approach is the *Priority Queueing* (PQ) protocol, in which each piece of information is assigned a priority value. Information with higher priority is given precedence over those with lower priority, allowing it to be displayed first. For our investigative purposes, we will primarily focus on the FCFS protocol since our main objective is to optimize the system under normal, non-congested conditions.

We can consider an information update system as a single queue node, and we characterize its behaviour using the Kendall's notation [31]. According to this notation, a queue node can be

described as A/S/c where A stands for the distribution of the sender, S describes the distribution of the recipient and c describes the number of servers at the node. The interarrival time of information and the system time can be described by probability distributions. The most common probability distributions used to characterize these processes are as follows:

- If the frequency at which information is communicated or retrieved follows a Poisson distribution and does not depend on the delivery of previous information, the process is denoted as M representing Markov or Memoryless.
- If the information is communicated or retrieved at fixed intervals, the process is deterministic and it is denoted by D.
- When we do not specify a particular probability distribution, we refer to the process as general, denoted by the letter G.

The memoryless process are widely used in the modelling of queue systems, since the Poisson probability distribution expresses the likelihood that a certain number of events will occur in a fixed time window, assuming that these events occur with a specific rate and do not depend on when the last event occurred. The parameter of this distribution represents its mean value, namely if X represent a Poisson distribution of probability of parameter λ, than $\mathbb{E}[X] = \lambda$.

In this thesis, our focus will be on the M/M/1 process. In this scenario, both the sender and the recipient follow a Poisson distribution of probability, and there is only one server for the exchange of information [3]. Let λ be the arrival rate and μ be the service rate. We can thus model the interarrival times X_i as independent identical distributed exponential random variable with $\mathbb{E}[X] = 1/\lambda$ and the system times as independent identical distributed exponential random variable with $\mathbb{E}[T] = 1/\mu$.

An essential metric for evaluating the performance of a single-server information system is the average Age of Information (AoI), denoted as $\Delta = \mathbb{E}[\delta t]$, where $\delta(t)$ represents the AoI, as defined in equation (1). In the context of the First-Come-First-Served (FCFS) system, it can be shown [3] that:

$$\Delta = \lambda \left(\mathbb{E}[XT] + \frac{\mathbb{E}[X^2]}{2} \right). \tag{2}$$

Using Equation (2), we can derive the average AoI for the M/M/1 system as:

$$\Delta = \frac{1}{\mu}\left(1 + \frac{1}{\rho} + \frac{\rho^2}{1-\rho}\right). \tag{3}$$

In Equation (3), ρ denotes the load factor or server utilization, defined as the ratio between the arrival rate and the service rate. It must satisfy the following condition:

$$\rho = \frac{\lambda}{\mu} < 1. \tag{4}$$

The M/M/1 model allows for adjustments to the arrival rate λ and the service rate μ to optimize the system. It is known that values close to 0 minimize packet delays, while values close to 1 maximize throughput [3]. To optimize the average AoI, it can be shown that the optimal load factor value ρ^* must be chosen as $\rho^* \approx 0.53$.

Since the parameter μ representing the server rate appears in equation (3) as a rescaling factor, we can make the assumption, without any loss of generality, that $\mu = 1$. Under this assumption, equation (3) can be rewritten as follows:

$$\Delta = 1 + \frac{1}{\lambda} + \frac{\lambda^2}{1-\lambda} \tag{5}$$

It is worth noting that in this case, $\rho = \lambda$.

2.1.3 AoI in Secure Communications

Secure communication is an essential part of various communication networks, since it is maintaining the confidentiality of the information transferred between a transmitter and a receiver, or in general of all involved parties. Although AoI does not affect the security of the transferred information directly, it has indirect impacts on security in various ways and means. High AoI could potentially lead to a poor decision making which is considered a security risk in itself. Additionally, if there is an eavesdropper in the communication network, AoI on receiver's side could be affected immensely due to potential outdated information. Again, this would not affect the security in the same sense as decryption and encryption would; however it would affect the operational security of the system since the awareness of the receiver related to the current situation would be impacted [5], [32], [33],

[34]. Moreover, in the presence of an eavesdropper, a transmitter can change the behaviour of taken actions to make sure that the AoI on receiver's side is as minimal as possible. This leads to us to consider a game theoretical approach to such situations where one or more eavesdroppers are present in the communication network [21]. We will discuss this connection in more detail in section 2.3.

The presence of on eavesdropper within a communication network can lead to significant security concerns. If the information that has been intercepted by an eavesdropper can also reach the receiver, then there would be no need for additional strategies for the transmission of data since we consider the case where the goal of the transmitter is only to make sure that the AoI on receiver's side is minimal. Therefore, even though real life constraints are still existent, the transmitter will try to send status updates as quick or timely possible to ensure the freshness of the information on receiver's side. However, situations including an eavesdropper in a communication network are usually modelled as partially degraded wiretap channel. In such models, intercepted information is lost to the receiver and thus existence of an eavesdropper directly affects the AoI on receiver's side, and leads to changes in strategies for the transmission of the data [5].

Although we will talk about the game theoretic approach in situations including one or more eavesdroppers in more detail in section 2.3, we conclude this section by mentioning few critical parts of this approach. It is important to note that the goal of the transmitter, in such scenarios, is to minimize the AoI on receiver's side by adjusting the transmission rate of the information. On the other hand, an eavesdropper's goal is to minimize the AoI on its side by adjusting the taken action. Natural question to ask here would be whether it is better for an eavesdropper to constantly try to intercept information. Unfortunately, this approach is not always the best decision for an eavesdropper since we associate costs for actions taken by both the transmitter and an eavesdropper [5], [21], [13].

2.2 Quantum Entanglement and Communication Security

2.2.1 Principles of Quantum Entanglement

We begin the chapter by giving a definition for quantum state, which is a core part of quantum theory. Although there are several views and opinions on what they represent, we try to give a definition as to what they are to the best of our ability and information. A quantum state is a mathematical object in quantum theory, providing probability distribution of outcomes for each possible measurement on a given system [4]. Each state is described by a vector in a Hilbert space together with an inner product embedded into the space. Simplest example for a quantum state would be the state for a single qubit. This can be represented by the superposition of its basis states $|0\rangle$ and $|1\rangle$. Thus, we write the general state of a qubit as in following:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{6}$$

where $|\alpha|^2 + |\beta|^2 = 1$ and $\alpha, \beta \in \mathbb{C}$. It is also important to note here that a Hilbert space is a complex vector space [35], [36], [37].

On the other hand, quantum entanglement can be described as a phenomenon of quantum mechanics where quantum states of several particles become intertwined. This happens in a way that the state of a single particle cannot be described anymore independently with respect to other particles. What is more, this continues to be the case even when mentioned particles are separated by large distances. Entangled state can be written as below [38]:

$$|\Psi_{\text{entangled}}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \tag{7}$$

Moreover, quantum entanglement affects quantum computing and communication significantly, making it an important part of our analysis at the same time. Due to entangled particles being intertwined, this connection between particles forms the basis for quantum teleportation and quantum key distribution (QKD) [39][40].

The main idea of quantum entanglement is based on the superposition principle of quantum mechanics. This is the property that allows a quantum system to be in multiple quantum states at the same time, however, until it has been measured. Entangled particles can be represented by a combined quantum state as in (7). In this case, measurement of one particle affects the state of the

other particle at the same time.

Quantum entanglement has various practical applications including quantum computing, quantum teleportation and quantum communication [36], [37], [20]. In quantum computing, entanglement is used to enhance the speed of solving problems immensely, compared to modern day computers. In quantum teleportation, on the other hand, state of a particle is transferred from one location to another without the necessity of a physical transfer of the mentioned particle. Furthermore, in quantum communication, quantum entanglement is used to create or obtain communication protocols which are highly secure and in fact theoretically unbreakable. Lastly, we conclude this subsection by stating that quantum entanglement has been shown in various quantum systems, including photons, electrons, molecules, etc.

2.2.2 Monogamy of Quantum Entanglement in Eavesdropping

Monogamy of quantum entanglement is another core principle of quantum mechanics which is also a crucial part of our analysis. This particular property limits the number of various and multiple other systems, to which a given quantum system can be entangled to [20], [41]. Therefore, monogamy of quantum entanglement has a direct and important effect to quantum communication security, especially in cases where multiple eavesdroppers are present in a system. In a secure quantum communication system, two particles cannot be independently entangled with a third party, given that they are maximally entangled with each other. To give an example, QKD is strongly dependent on the monogamy of entanglement. In systems such as QKD, presence of an eavesdropper can be detected thanks to the monogamy of entanglement. This is due to the fact that any attempt to entangle with communicating sides would disrupt the initial and original entanglement and thus can be noticed.

The monogamy of entanglement can be mathematically described by using fundamental definitions, entanglement measures and inequalities which are not to be discussed here in detail. However, we give the following inequality showing that if particles A and B are maximally entangled, then particle A cannot be entangled with particle C [41].

$$\tau_{A|BC} \geq \tau_{A|B} + \tau_{A|C} \tag{8}$$

We are able to estimate the degree of entanglement to a considerable extent mainly due to mathematical formulations and descriptions of entanglement. Consequently, this improves our com-

prehension of the security of a given quantum communication channel. Moreover, these mathematical expressions offer deep insights into secure information transmission and the detection of eavesdropper interception. Although monogamy of entanglement has been extensively studied recently, research on the subject is still ongoing and may eventually lead to a greater development in both theoretical knowledge of quantum communication channels and real-world applications in secure communication.

2.2.3 Quantum Channels and AoI

Quantum channels have an important role in various quantum communications systems. Quantum key distribution (QKD) and quantum teleportation systems are only two examples among many other important systems, where quantum channels are used to transmit quantum information [42]. This is usually done in the form of qubits, which has been introduced in previous sections. On the other hand, age of information (AoI) describes a metric for the timeliness or freshness of the transferred information, and is an important factor in quantum communication systems [43]. This is mainly due to the fact that the value of quantum information usually depends on how current or fresh it is. Especially in dynamic settings, where decisions are made instantly depending on the received information, freshness or timeliness of the transferred information is exceptionally important.

Age of information can be affected by various factors in a quantum channel. These factors could be stability of quantum states, efficiency of quantum information processing, presence of noise in the quantum channel, etc. On the other hand, quantum information can be easily disturbed by environmental factors, and thus this could potentially lead to loss of coherence and information. Therefore, impact of noise and the loss of quantum coherence on age of information is an important factor to be considered while quantum communication systems are designed. This is due to the fact that these features can immensely affect the reliability and the speed of transmission of information.

In quantum communication channels, the presence of an eavesdropper can also significantly impact the AoI. An eavesdropper attempting to intercept the quantum information which is being transmitted can introduce errors and delays in the communication channel. These disturbances can be detected by the legitimate parties, providing an indication of a potential security breach. The interplay between ensuring the freshness of information (decreasing AoI) and maintaining security and integrity of the quantum channel is a critical aspect of quantum communication research. Strategies to optimize AoI in quantum channels involve balancing the trade-offs between speed, reliability, and security, while considering both the physical limitations of the quantum systems and the potential threats from eavesdroppers [44] [45].

2.3 Game Theory for Communication Systems

In the following subsections we will presents the fundamentals of game theory, how is game theory used in Secure communication, and which are the common strategies to extend the setting from two to a greater finite number of players.

2.3.1 Game Theory Fundamentals

Game theory is a branch of mathematics that investigates situations in which multiple parties involved seek to optimize their own gains, and the choices made by each player influence the decisions and gains of the others [46]. This field of mathematics has witnessed significant development over the past 100 years. In 1928, Von Neumann became the first to formally define game theory in his paper *Theory of Parlor Games* and later, his book *Theory of Games and Economic Behavior* [47] sparked a revolutionary shift in the field of economics. The theory was subsequently applied to other disciplines such as psychology, sociology, and politics. The development of game theory continues to grow, with substantial contributions from renowned mathematicians such as John Maynard Smith, John Nash, and Roger Myerson, to name a few.

In a game theory setting we have a finite number of parts, called *players*, that wants to maximize their payoff [48]. Let's consider the most informative case of two players, since the generalization to multiple players can be derived from the case taken into account. We call the two players $Player_A$ and $Player_B$.

In the context of game theory, it is possible for all players to know all the variables at all times. In such cases, we refer to it as a game of complete information. Another common scenario involves players not having access to all the information about each other. This situation is referred to as a game of incomplete information or Bayesian games [49] [50].

Another crucial distinction is whether a game is static or dynamic. A game is considered static when the actions of the players occur only once. Conversely, a game is considered dynamic when players adjust their actions multiple times. In the scope of this thesis, we will focus on static games of complete information, as the emphasis will be on applying game theory to the communication system.

Each of the two player has a set of possible actions that can perform, let A be the set of possible action for the $Player_A$ and let B be the set of all possible action for the $Player_B$. The goal of $Player_A$ is to find the strategy a among the all possible strategy in A that maximize its payoff $J_A(a, b)$

$$\max_{a \in A} J_A(a, b) \tag{9}$$

while the goal of $Player_B$ is to find the strategy b among all the possible strategy in B that maximize its payoff $J_B(a, b)$:

$$\max_{b \in B} J_B(a, b). \tag{10}$$

As it can be seen inspecting the equation (9) and (10), it is clear that $Player_A$ payoff depends on its on choice as well as $Player_B$ choices. Therefore, it is not always possible to find the value of a and b that allows to maximize the two equation in the same time. This is why it is important to define the concept of equilibrium. In the context of non-cooperative game, it is useful to introduce the definition of Nash equilibrium.

We say that a pair of strategy $(a^*, b^*) \in (A, B)$ is a Nash equilibrium of the game if, for every $a \in A$ and for every $b \in B$, the following equation holds [48]:

$$J(a^*, b) \leq J(a^*, b^*), \quad J(a, b^*) \leq J(a^*, b^*). \tag{11}$$

Thanks to the Nash existence theorem [51], there always exists a Nash equilibrium for a finite number of players.

It is important to recognize that Nash equilibrium may not yield the optimal outcome. Essentially, a^* signifies the optimal decision for $Player_A$ after $Player_B$ has made their optimal choice, and the same principle applies to $Player_B$.

A classical example to better understand this situation is the example of the two prisoners. Let's assume that we have two prisoners has been captured; each prisoner's sentence is halved if they confess, they receive the full sentence if the other confesses but they do not, and they go free if neither confesses. Although the optimal outcome is for neither to confess, the Nash equilibrium occurs when both confess.

In general, it is a delicate matter to find the Nash equilibrium point. However, for static games with complete information, identifying the equilibrium point is feasible using computational tools such as MATLAB, especially when the payoff equations (specifically equations 9 and 10) are known.

It is also possible to have multiple Nash equilibrium points; when there are multiple Nash equilibrium points, we call the primary Nash equilibrium point the one that represents the best outcome for all the players with respect to the others.

2.3.2 Game Theory in Secure Communications

Communication systems are used in various aspects in today's world. Every time a piece of information is exchanged, a communication system is used, either physically or through a network.

Especially in wireless communication, it is crucial that the piece of information is protected and can reach the designated receiver. There are many cases in which there might be a malicious attack, either to prevent the information from reaching the receiver or to gain hold of the information itself. There are various strategies that can be applied to make the communication system safer, and all of them deal with managing finite resources [52] [53].

This is why Game Theory can come in handy [54]. In fact, using game theory, it is possible to model a situation in which different parties are competing against each other to reach a selfish goal, and their actions change based on what the other parties do. In a typical Game Theory setting, the actions that the players can perform are limited, and they are associated with a cost. By using a game theory setting, it is possible to analyze the situation globally, and each player can find the best strategy assuming that the other players will do the same.

Game Theory has been widely used in the past years to enhance communication systems [55]. From various applications, interesting results have been proven in intrusion detection systems, security of self-organizing networks, and at the physical layer and media access control (MAC) layers. It is worth paying attention to the physical and MAC layer since it is where attacks like jamming and eavesdropping can occur.

2.3.3 Extension to Multiple Players

In most cases, game theory is presented for two players. The reason for this is that the approach to a game theory setting remains the same when dealing with a finite number of players, while the approach changes completely when dealing with an infinite number of players. However, the latter case is outside the scope of our work. Since we will apply game theory in a setting with more than two players, we now present the theory for a finite number N of players for completeness [48].

Let us assume we have a finite number N of different players, whom we will refer to as $Player_1$, $Player_2$, ..., $Player_N$. We will consider a static, non-cooperative game of complete information. This means that all the N players have different goals and will use a strategy to achieve their individual goals. Each player selects its action just once, simultaneously. Additionally, since it is a game of complete information, each player knows the state of the system and the action each other player performed. Let X_i be the set of all possible actions $\mathbf{x}_i$ that $player_i$ can perform for each $i \in , \ldots, N$. Each player has associated its utility function $J_i(\mathbf{x}_1, \ldots, \mathbf{x}_N)$. The goal of each player is to find the action that maximizes its utility function:

$$\max_{\mathbf{x_i} \in X_i} J_i(\mathbf{x}_1, \ldots, \mathbf{x}_N) \tag{12}$$

As for the case of two players, we define the Nash equilibrium. Let $\mathbf{x}^* = (\mathbf{x}_i^*, \mathbf{x}_{\_i}^*)$ be a set containing a strategy for each player, where $\mathbf{x}_i^*$ denotes the strategy for $player_i$ and $\mathbf{x}_{\_i}^*$ denotes $N-1$ strategies for all the remaining players. We say that $\mathbf{x}^*$ is a Nash equilibrium if [48]

$$J_i(\mathbf{x}_i^*, \mathbf{x}_{\_i}^*) \geq J_i(\mathbf{x}_i, \mathbf{x}_{\_i}^*) \quad \forall \mathbf{x}_i \in X_i. \tag{13}$$

As for the case of two players, it is possible that the Nash equilibrium does not represent the best outcome possible for all the players, and it is possible to have multiple Nash equilibrium points.

3 Quantitative Analysis and Modelling

3.1 Theoretical Computation

In the following scenario, we find ourselves with a transmitter sending periodic information to a legitimate receiver. For clarity, we will denote the transmitter as Alice and the receiver as Bob. We model this scenario using an FCFS M/M/1 model, making the assumption that the receiver is passive, and the transmitter transmits with an update rate equal to λ [5]. Additionally, without loss of generality, we set the service rate μ to be equal to 1, as explained in Section 2.1.2. The communication in our model takes place through a quantum channel.

In this model, we introduce two eavesdroppers, referred to as Eve and Frank. Their objective is to intercept the information transmitted from Alice to Bob. However, Eve and Frank act as independent players and do not cooperate in their attempts to retrieve the information. The behavior of each eavesdropper is modeled as follows: we assume that each eavesdropper can intercept each package sent by Alice, as detailed in Section 2.2. We model the process of each eavesdropper as a family of independent identically distributed Bernoulli processes with a parameter $\beta \in [0, 1]$. Specifically, $\beta_1 \in [0, 1]$ represents the parameter associated with Eve, and $\beta_2 \in [0, 1]$ represents the parameter associated with Frank [5].

In our model, we consider Bob to be a passive element, while Alice, Eve, and Frank are active players. Therefore, there are three M/M/1 queues: one at Bob's end, one at Eve's end, and one at Frank's end. Due to the nature of the quantum channel, if Eve or Frank intercepts the information, it will not reach Bob. However, if neither Eve nor Frank attempts to intercept the information, it successfully reaches Bob with a probability of

$$(1 - \beta_1)(1 - \beta_2). \tag{14}$$

If Eve attempts to intercept the information while Frank does not, the information is successfully intercepted by Eve with a probability of

$$\beta_1(1 - \beta_2). \tag{15}$$

Similarly, if Frank attempts to intercept the information while Eve does not, the information is

successfully intercepted by Frank with a probability of

$$\beta_2(1-\beta_1). \tag{16}$$

A different scenario arises when both Eve and Frank attempt to intercept the same information. Due to the monogamy of entanglement, we focus on two main and highly informative scenarios, as others can be derived from those presented here.

In the simpler case, we assume that when both Eve and Frank attempt to intercept the same information, the information is lost. This situation is illustrated in Figure 3. In this scenario, the flow of updates generated by Alice splits into three memoryless flows with rates λ_B, λ_E, and λ_F, taking the form presented in the following equations (17), (18) and (19).

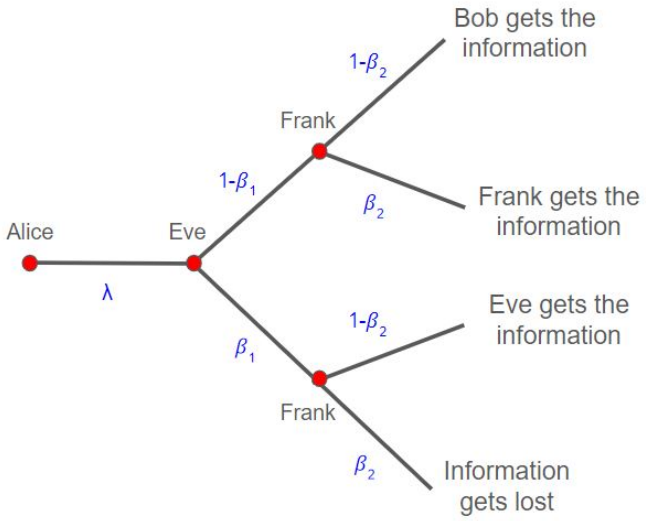

Figure 3: Tree diagram depicting the case where Eve and Frank attempts to intercept the same information and information gets lost.

$$\lambda_B = \lambda\big(1-\beta_1\big)\big(1-\beta_2\big) \tag{17}$$

$$\lambda_E = \lambda\beta_1\big(1-\beta_2\big) \tag{18}$$

$$\lambda_F = \lambda\beta_2\big(1-\beta_1\big) \tag{19}$$

Alternatively, we can consider a scenario where both Eve and Frank attempting to intercept the same information results in a probability $p_1 \in [0,1]$ that Eve intercepts the information and a complementary probability $p_2 = 1-p_1$ that Frank intercepts the information. Due to the symmetry of the eavesdroppers [21], it is reasonable to assume

$$p_1 = p_2 = \frac{1}{2}. \tag{20}$$

This scenario is depicted in Figure 4. In this case, the flow of updates generated by Alice again splits into three memoryless flows with rates λ_B, λ_E, and λ_F, assuming the form presented in the following equations (21), (22) and (23).

$$\lambda_B = \lambda\big(1-\beta_1\big)\big(1-\beta_2\big) \tag{21}$$

$$\lambda_E = \lambda\left[\beta_1\big(1-\beta_2\big) + \frac{\beta_1\beta_2}{2}\right] \tag{22}$$

$$\lambda_F = \lambda\left[\beta_2\big(1-\beta_1\big) + \frac{\beta_1\beta_2}{2}\right] \tag{23}$$

Upon inspecting the equations for λ_B, λ_E, and λ_F, it becomes evident that the scenario in which neither Eve nor Frank can retrieve the information is a special case of the latter. This special case occurs when we set the probabilities p_1 and p_2 to be both equal to 0. Consequently, our focus will be on the broader scenario, as it provides more informative insights.

Before we delve into the case where we have two eavesdroppers, we note down below equations (24) and (25), for the average age of information values at Bob's and Eve's sides respectively [3]. We observe that in fact (24) is the same equation as (5) where λ is simply replaced by $(1-\beta)\lambda$. This

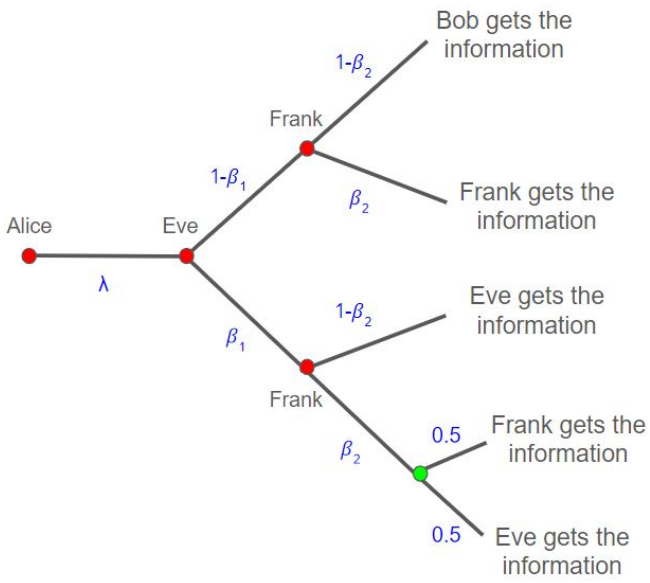

Figure 4: Tree diagram depicting the case where Eve and Frank attempts to intercept the same information and each has a success rate of 0.5.

is expected since $(1-\beta)\lambda$ represents the probability where Eve does not intercept and Bob receives the information.

$$\Delta_B(\lambda,\beta) = 1 + \frac{1}{(1-\beta)\lambda} + \frac{(1-\beta)^2\lambda^2}{1-(1-\beta)\lambda} \tag{24}$$

$$\Delta_E(\lambda,\beta) = 1 + \frac{1}{\beta\lambda} + \frac{\beta^2\lambda^2}{1-\beta\lambda} \tag{25}$$

Once we introduce a second eavesdropper, Frank, we have to adjust average age of information values for each side and define the average age of information value for Frank's side which is quite similar to the value at Eve's side. In order to do so, we replace λ in (5) with (21) for Bob's side, with (22) for Eve's side, and with (23) for Frank's side. Therefore we get the following average age

of information values (26), (27), (28), for Bob's, Eve's, and Frank's side respectively.

$$\Delta_B\big(\lambda,\beta_1,\beta_2\big) = 1 + \frac{1}{\big(1-\beta_1\big)\big(1-\beta_2\big)\lambda} + \frac{\big(1-\beta_1\big)^2\big(1-\beta_2\big)^2\lambda^2}{1-\big(1-\beta_1\big)\big(1-\beta_2\big)\lambda} \tag{26}$$

$$\Delta_E\big(\lambda,\beta_1,\beta_2\big) = 1 + \frac{1}{\lambda\left[\beta_1\big(1-\beta_2\big) + \frac{\beta_1\beta_2}{2}\right]} + \frac{\lambda^2\left[\beta_1\big(1-\beta_2\big) + \frac{\beta_1\beta_2}{2}\right]^2}{1-\lambda\left[\beta_1\big(1-\beta_2\big) + \frac{\beta_1\beta_2}{2}\right]} \tag{27}$$

$$\Delta_F\big(\lambda,\beta_1,\beta_2\big) = 1 + \frac{1}{\lambda\left[\beta_2\big(1-\beta_1\big) + \frac{\beta_1\beta_2}{2}\right]} + \frac{\lambda^2\left[\beta_2\big(1-\beta_1\big) + \frac{\beta_1\beta_2}{2}\right]^2}{1-\lambda\left[\beta_2\big(1-\beta_1\big) + \frac{\beta_1\beta_2}{2}\right]} \tag{28}$$

By simplifying equations (27) and (28) we get the following equations (29) and (30).

$$\Delta_E\big(\lambda,\beta_1,\beta_2\big) = 1 + \frac{1}{\lambda\left[\beta_1 - \frac{\beta_1\beta_2}{2}\right]} + \frac{\lambda^2\left[\beta_1 - \frac{\beta_1\beta_2}{2}\right]^2}{1-\lambda\left[\beta_1 - \frac{\beta_1\beta_2}{2}\right]} \tag{29}$$

$$\Delta_F\big(\lambda,\beta_1,\beta_2\big) = 1 + \frac{1}{\lambda\left[\beta_2 - \frac{\beta_1\beta_2}{2}\right]} + \frac{\lambda^2\left[\beta_2 - \frac{\beta_1\beta_2}{2}\right]^2}{1-\lambda\left[\beta_2 - \frac{\beta_1\beta_2}{2}\right]} \tag{30}$$

Now, since β_1 and β_2 must be equal for symmetry at the Nash equilibrium [21], we take $\beta_1 = \beta_2 = \tilde{\beta}$ and further simplify (26), (29) and (30) as below in (31), (32), and (33) respectively. We denote simplified average age of information values at Bob's, Eve's and Frank's side as before except replacing β_1 and β_2 with $\tilde{\beta}$.

$$\Delta_B\big(\lambda,\tilde{\beta}\big) = 1 + \frac{1}{\big(1-\tilde{\beta}\big)^2\lambda} + \frac{\big(1-\tilde{\beta}\big)^4\lambda^2}{1-\big(1-\tilde{\beta}\big)^2\lambda} \tag{31}$$

$$\Delta_E(\lambda,\tilde{\beta}) = 1 + \frac{2}{\lambda\tilde{\beta}(2-\tilde{\beta})} + \frac{\lambda^2(\tilde{\beta})^2(2-\tilde{\beta})^2}{4-2\lambda\tilde{\beta}(2-\tilde{\beta})} \tag{32}$$

$$\Delta_E(\lambda,\tilde{\beta}) = 1 + \frac{2}{\lambda\tilde{\beta}(2-\tilde{\beta})} + \frac{\lambda^2(\tilde{\beta})^2(2-\tilde{\beta})^2}{4-2\lambda\tilde{\beta}(2-\tilde{\beta})} \tag{33}$$

At this point, it is intuitive to consider whether it is logical for both Alice and two eavesdroppers, Eve and Frank, to increase their actions as much as they like. However, this scenario would be unrealistic without any consequence applied to each side. Therefore, we say that all sides are subject to a cost which is directly proportional to their action value [13]. Moreover, we observe that the goal for each side is to decrease the average age of information, while it is the opposite for the utility functions in game theory. In the case of a single eavesdropper, utility functions would be defined as follows, assuming the costs c and k assigned to Alice and Eve respectively.

$$u_A(\lambda,\beta) = \left[\Delta_B(\lambda,\beta)\right]^{-1} - c\lambda \tag{34}$$

$$u_E(\lambda,\beta) = \left[\Delta_E(\lambda,\beta)\right]^{-1} - k\beta \tag{35}$$

Since we are considering the case with two eavesdroppers, utility functions takes following forms in (36), (37) and (38), where c is the cost assigned to Alice, k_1 to Eve and k_2 to Frank.

$$u_A(\lambda,\beta_1,\beta_2) = \left[\Delta_B(\lambda,\beta_1,\beta_2)\right]^{-1} - c\lambda \tag{36}$$

$$u_E(\lambda,\beta_1,\beta_2) = \left[\Delta_E(\lambda,\beta_1,\beta_2)\right]^{-1} - k_1\beta_1 \tag{37}$$

$$u_F(\lambda,\beta_1,\beta_2) = \left[\Delta_F(\lambda,\beta_1,\beta_2)\right]^{-1} - k_2\beta_2 \tag{38}$$

Once again, since $\beta_1 = \beta_2 = \tilde{\beta}$ for the symmetry at Nash equilibrium, we can simplify the above given utility functions. Additionally, we assume that costs are also equal for Eve and Frank due the

same reason. Thus, we take $k_1 = k_2 = \tilde{k}$.

$$u_A\big(\lambda, \tilde{\beta}\big) = \big[\Delta_B\big(\lambda, \tilde{\beta}\big)\big]^{-1} - c\lambda \tag{39}$$

$$u_E\big(\lambda, \tilde{\beta}\big) = \big[\Delta_E\big(\lambda, \tilde{\beta}\big)\big]^{-1} - \tilde{k}\tilde{\beta} \tag{40}$$

$$u_F\big(\lambda, \tilde{\beta}\big) = \big[\Delta_F\big(\lambda, \tilde{\beta}\big)\big]^{-1} - \tilde{k}\tilde{\beta} \tag{41}$$

Note that, $u_E\big(\lambda, \tilde{\beta}\big) = u_F\big(\lambda, \tilde{\beta}\big)$ since $\Delta_E\big(\lambda, \tilde{\beta}\big) = \Delta_F\big(\lambda, \tilde{\beta}\big)$ as can be seen from (32) and (33). Now, the next logical step would be to look at Nash equilibria of the system. Observing that choices of Alice and two eavesdroppers are connected, we write down best response (BR) functions of each side. In particular in below equations (42) and (43), $\lambda^*\big(\tilde{\beta}\big)$ represents the best response of Alice to the choice of Eve and Frank, while $\tilde{\beta}^*\big(\lambda\big)$ represents best response of Eve and Frank to the choice of Alice.

$$\lambda^*\big(\tilde{\beta}\big) = \underset{\lambda \in [0,\infty)}{\operatorname{argmax}}\ u_A\big(\lambda, \tilde{\beta}\big) \tag{42}$$

$$\tilde{\beta}^*\big(\lambda\big) = \underset{\tilde{\beta} \in [0,1]}{\operatorname{argmax}}\ u_E\big(\lambda, \tilde{\beta}\big) = \underset{\tilde{\beta} \in [0,1]}{\operatorname{argmax}}\ u_F\big(\lambda, \tilde{\beta}\big) \tag{43}$$

As the last part of this chapter, we consider and analyze the price of anarchy (PoA) within our model. To begin with, we note that the sum of utilities of Alice, Eve and Frank is taken as a criterion for social welfare [5]. Then, we define the price of anarchy (PoA) as below in (44), where $\lambda_w, \tilde{\beta}_w$ represents the worst possible Nash equilibrium, while $\lambda_0, \tilde{\beta}_0$ represents the social optimum [56]. Social optimum can also be regarded as choices maximizing the social welfare. It has been shown [5] that primary Nash equilibrium corresponds to achieving the social optimum, and the PoA is 1 if the system admits only one Nash equilibrium.

$$\text{PoA} = \frac{u_A\big(\lambda_0, \tilde{\beta}_0\big) + u_E\big(\lambda_0, \tilde{\beta}_0\big) + u_F\big(\lambda_0, \tilde{\beta}_0\big)}{u_A\big(\lambda_w, \tilde{\beta}_w\big) + u_E\big(\lambda_w, \tilde{\beta}_w\big) + u_F\big(\lambda_w, \tilde{\beta}_w\big)} \tag{44}$$

3.2 Numerical Results

In this section, we will examine numerical evaluations based on the previous section where theoretical computations has been discussed. We derived the results through MATLAB with originally developed code. To begin with, Figure 5 illustrates how best responses of Alice and two eavesdroppers change with varying values of λ and $\tilde{\beta}$, when costs c and $\tilde{k}$ are equal to 0. Here we have only one Nash equilibrium, at the intersection point of best responses. If we consider the best response curve for Alice, it makes sense to increase the value of λ as the value of $\tilde{\beta}$ increases, since there is no cost for either side. However, this increase will be put on halt and follow a stationary value after the value of $\tilde{\beta}$ increases beyond certain limit. The main reason for this is that Alice does not want status updates to be lost while being eavesdropped due to the quantum channel, which would directly impact the AoI on Bob's side. On the other hand, if we consider the best response curve for eavesdroppers, $\tilde{\beta}$ value can be increased as much as eavesdroppers would like since there is no cost imposed on their actions. It is clear from this curve as well that λ value decreases while $\tilde{\beta}$ value increases, due to an analogous reason mentioned for the previous curve.

Figure 6 depicts nine similar graphs as in Figure 5, with different c and $\tilde{k}$ values. Case for $c = \tilde{k} = 0$ provides one Nash equilibrium, while cases where $0.01 \leq c = \tilde{k} \leq 0.13$ have three Nash equilibria. Moreover, starting from the case $c = \tilde{k} = 0.14$ and onward, we still obtain one Nash equilibrium. On following graphs, we will see that numerical evaluations is done for mostly three Nash equilibria.

Since AoI values change based on different unit prices $\tilde{k}$ and c, it is interesting to examine the behaviour of AoI dependent on different unit prices. Figures 7, 8 and 9 illustrates this behaviour at the primary, secondary and third Nash equilibrium respectively. Figure 7 shows that while the unit price $\tilde{k}$ increases, AoI values for eavesdroppers increase, at the primary Nash equilibrium. This is expected since higher cost would lead to less often action by eavesdroppers and thus consequently increasing their AoI. On the other hand, AoI of transmitter is decreasing while the unit price $\tilde{k}$ increases. Yet again, since increasing unit price $\tilde{k}$ lead to an increase in AoI values of eavesdroppers, it also leads to an increased rate of action on transmitter's side. This would directly impact the AoI on Bob's side and thus decrease the AoI value.

Conversely, we observe slightly different behaviour in Figure 8, which is taking place at the secondary Nash equilibrium. Here, increasing unit price $\tilde{k}$ leads to an increase in AoI on Bob's side. This is true also for eavesdroppers, however on a limited scale compared to the former. On broader sense, the reason lies on the inefficiency of Nash equilibria except primary ones [5]. This is even

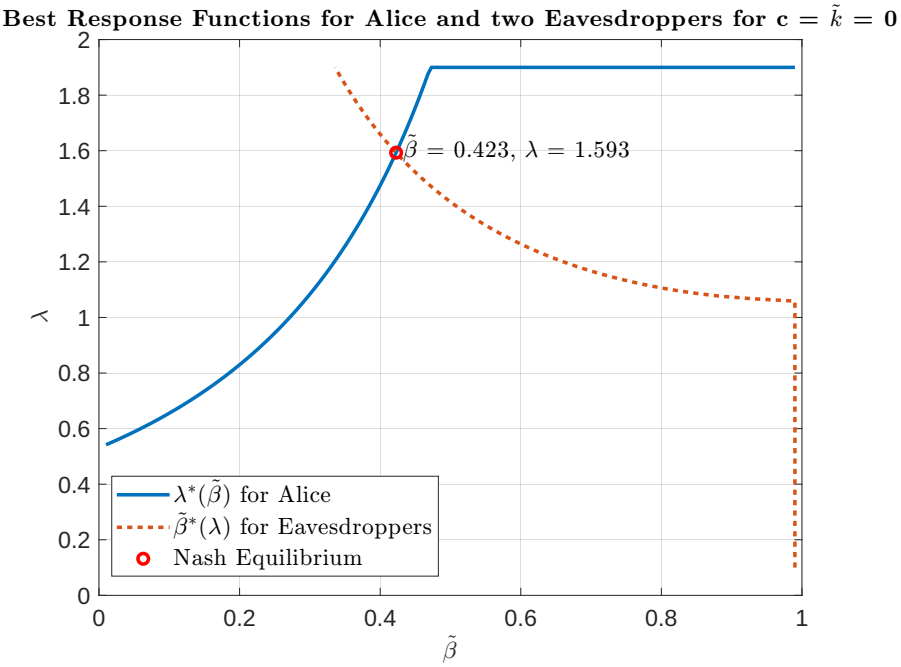

Figure 5: Best response curves of Alice and two eavesdroppers varying under different $\tilde{\beta}$ and λ values, where costs c and $\tilde{k}$ are equal to 0.

more evident from Figure 9 where evaluations are done on the third Nash equilibrium. In this figure, AoI values decrease while unit price $\tilde{k}$ increases. In order to further demonstrate what we mean, we use Figure 10. This figure depicts the relationship between the total utility and the unit price $\tilde{k}$ for $c = 0$, $c = 0.04$, $c = 0.08$, and $c = 0.12$ at primary, secondary and third Nash equilibria. In particular, the continuous lines describe the relationship between the total utility and the unit price for the eavesdroppers $\tilde{k}$ at the primary NE, while the dashed lines and the dotted lines describe this relationship at the secondary and third NE, respectively. It is thus clear that the total utility is always higher at primary Nash equilibria compared to secondary and third Nash equilibria. Figure 10 also shows that while the unit price $\tilde{k}$ increases, the total utility decreases.

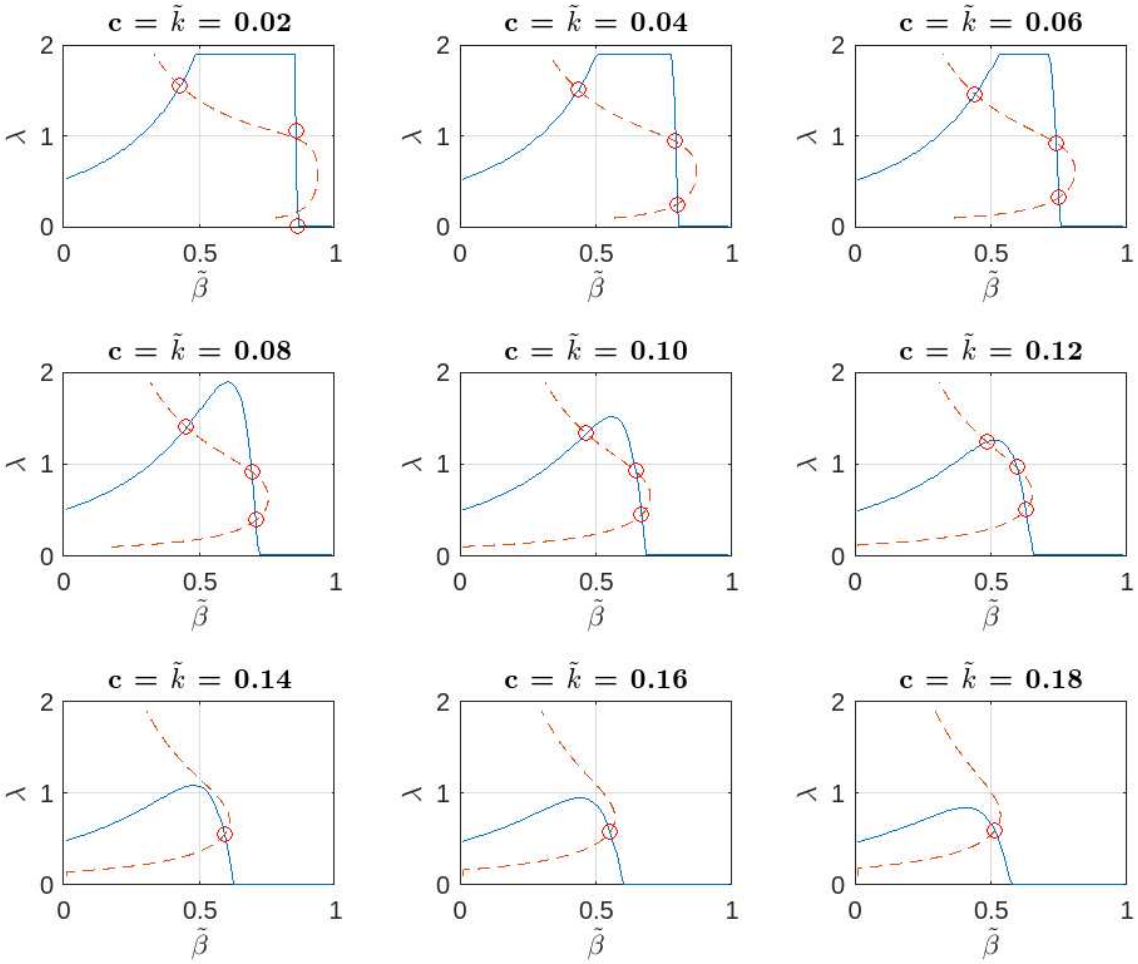

Figure 6: Best response curves of Alice and two eavesdroppers varying under different $\tilde{\beta}$ and λ values, where costs c and $\tilde{k}$ values are different for each subgraph.

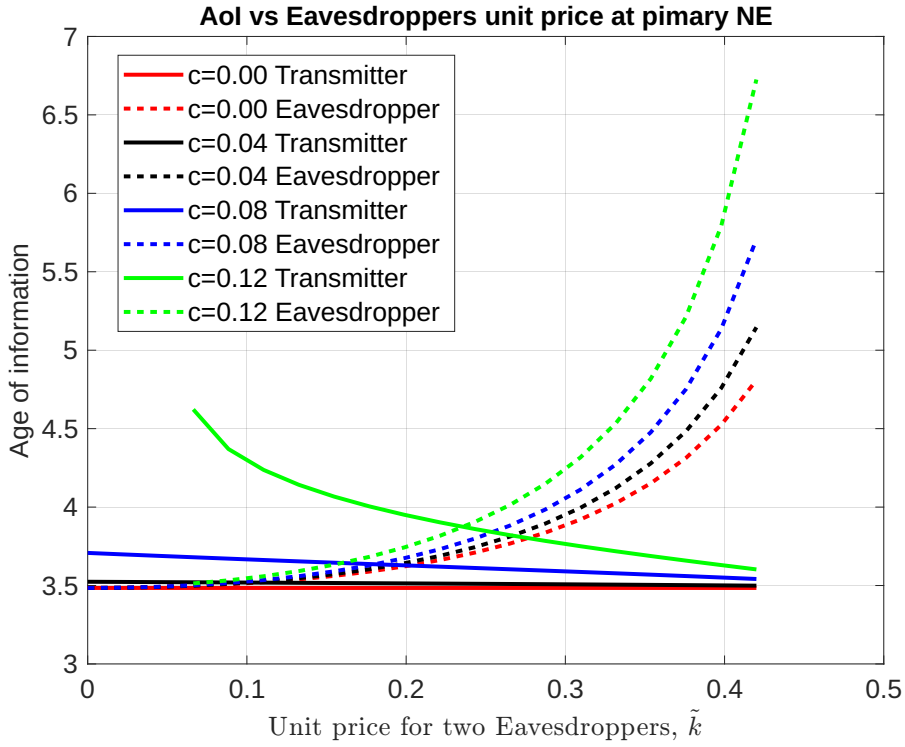

Figure 7: Age of Information values changing dependent on the unit price $\tilde{k}$, for $c = 0$, $c = 0.04$, $c = 0.08$, and $c = 0.12$ at primary Nash equilibrium.

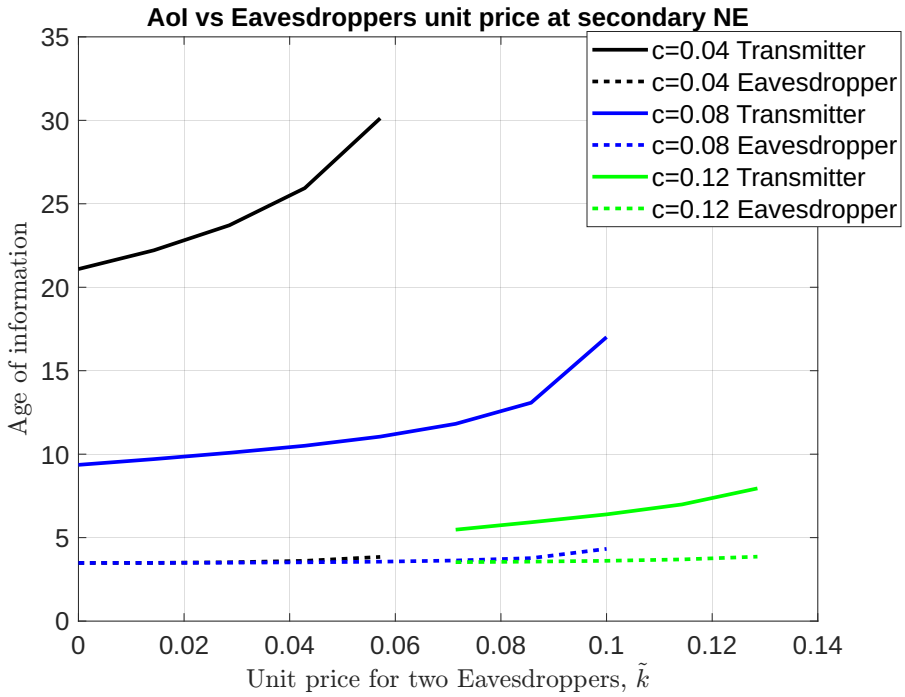

Figure 8: Age of Information values changing dependent on the unit price $\tilde{k}$, for $c = 0.04$, $c = 0.08$ and $c = 0.12$ at secondary Nash equilibrium.

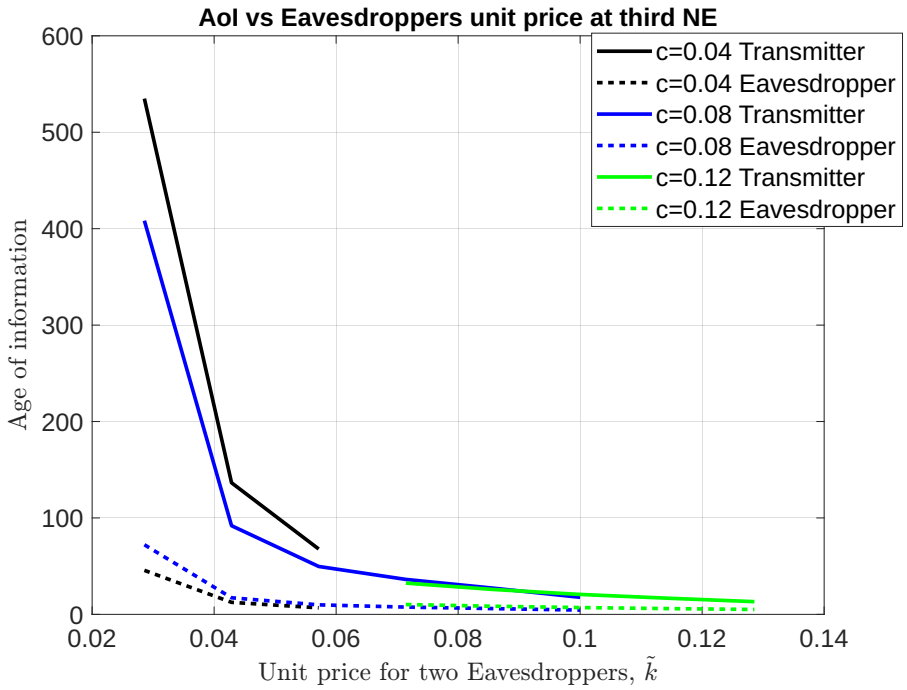

Figure 9: Age of Information values changing dependent on the unit price $\tilde{k}$, for $c = 0.04$, $c = 0.08$ and $c = 0.12$ at third Nash equilibrium.

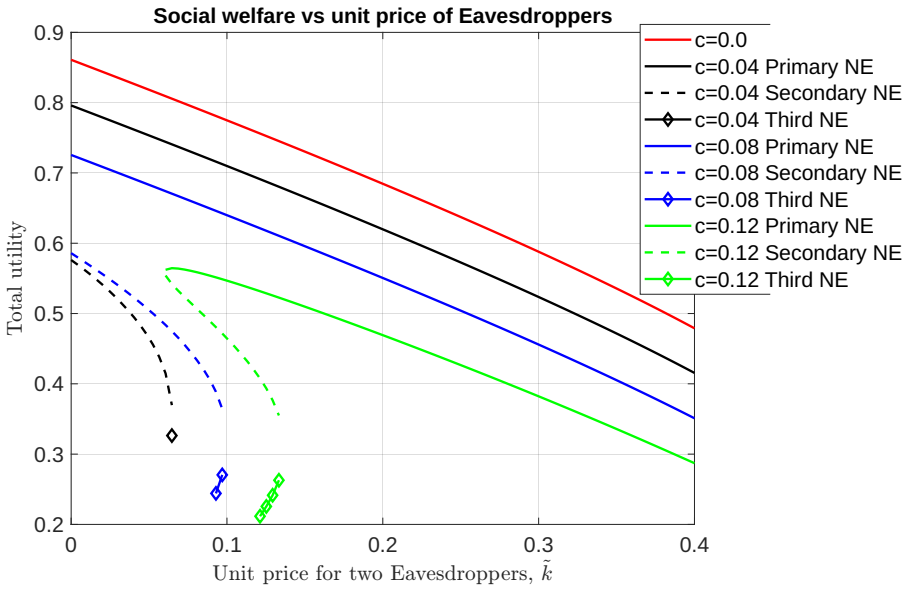

Figure 10: Total utility changing based on the unit price $\tilde{k}$ for different values of c at primary, secondary and third Nash equilibria.

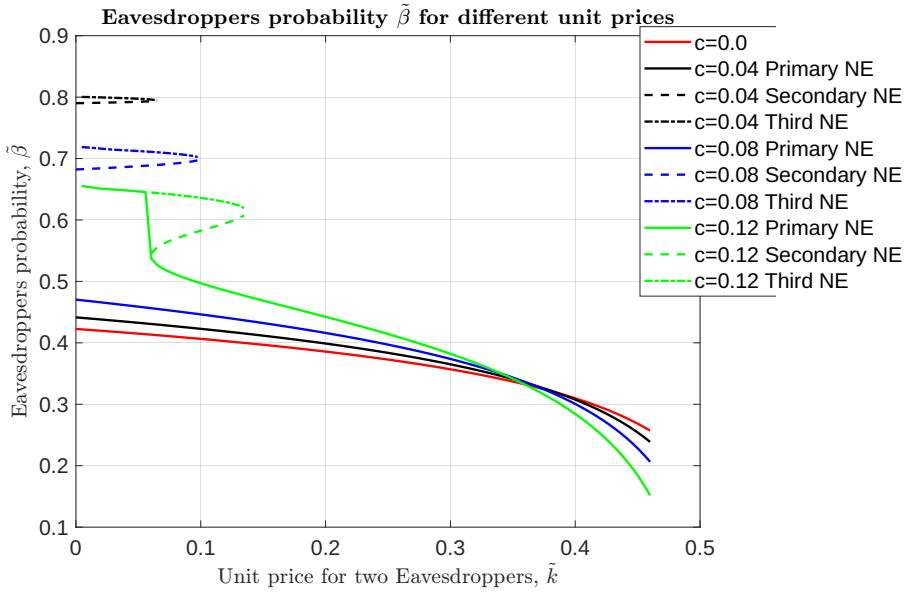

Figure 11: $\tilde{\beta}$ changing with varying unit price $\tilde{k}$, for different values of c at primary, secondary and third Nash equilibria.

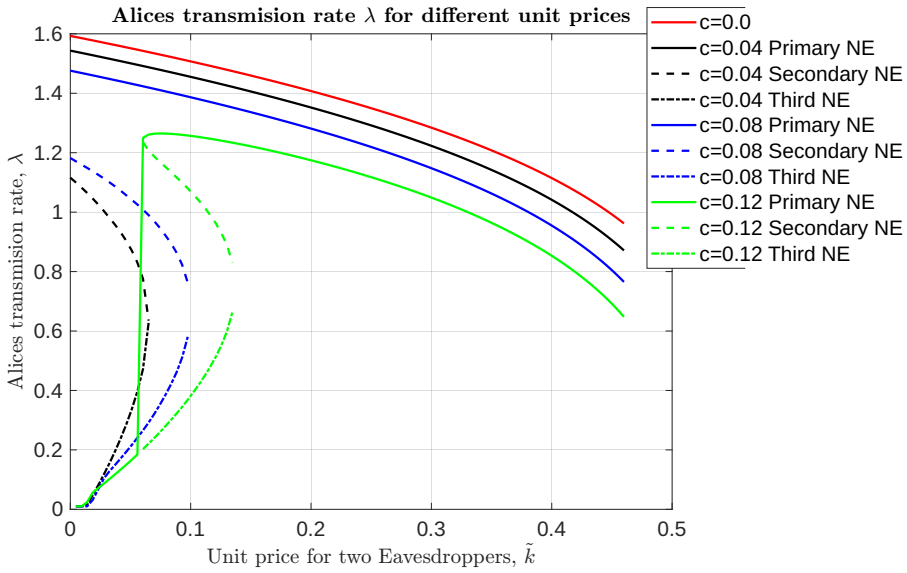

Figure 12: λ changing with varying unit price $\tilde{k}$, for different values of c at primary, secondary and third Nash equilibria.

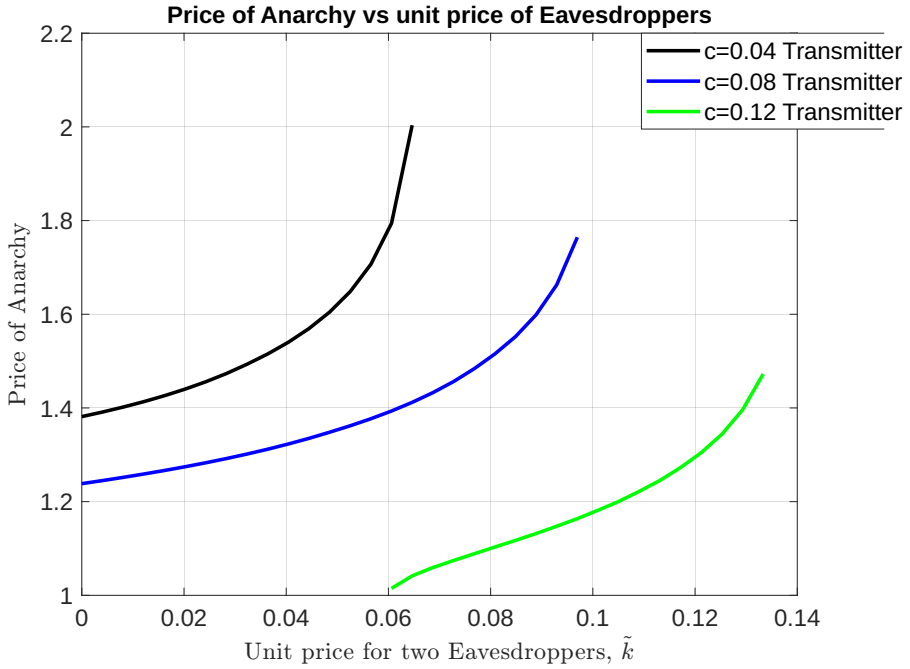

Figure 13: PoA changing based on the unit price $\tilde{k}$ for $c = 0.04$, $c = 0.08$, and $c = 0.12$.

We want to show how the eavesdropper probability $\tilde{\beta}$ and the transmission rate λ change for different unit prices at the different Nash equilibria. Figure 11 and Figure 12 show changing values of $\tilde{\beta}$ and λ, respectively, based on the unit price $\tilde{k}$ for $c = 0$, $c = 0.04$, $c = 0.08$, and $c = 0.12$ at primary, secondary and third Nash equilibria. In both cases values for $\tilde{\beta}$ and λ decrease while the unit price $\tilde{k}$ increases. It is important to note that in almost everywhere in Figure 11, $\tilde{\beta}$ values are higher for increasing c values. This is reasonable since with the imposed high cost on transmitter, eavesdroppers would increase their rate of action. On the other hand, in Figure 12 it is shown that higher c values result in decreased λ values. This also makes sense since the transmitter would decrease the rate of action if the imposed cost increases.

Finally, we examine the changing price of anarchy value based on the unit price $\tilde{k}$ for various c values, as depicted in Figure 13. As mentioned in equation (44), the price of anarchy quantifies the inefficiency in a system, representing the ratio between the worst possible Nash equilibrium with respect to the social optimum. The PoA is equal to 1 only if there is only one Nash equilibrium

point. Here, it can be seen that regardless of the c value, PoA value increases while the unit price $\tilde{k}$ is increasing. We conclude by stating that for relatively lower values of c and $\tilde{k}$, PoA can get very high [5].

Based on the context of quantum communication channels, in game-theoretic sense, it is crucial to investigate what consequences will arise when people make certain choices, and how those choices affect each other. In fact, numerical results provided above shows that there is an important balance between making decisions in such cases, and keeping the information safe. To be concrete, as seen from above figures and our earlier comments on them, it is safe to argue that the way prices are set for using quantum communication networks can affect how secure and efficient they are. Additionally, by studying how prices influence network behavior, we can come up with newer methods to make sure the information stays safe. Consequently, methods of enhancing quantum communication channels combines ideas not only from quantum physics but also from economics, cybersecurity, etc.

4 Conclusions

In this thesis work, we investigated the problem of eavesdropping in communication systems. After presenting an overview of the state of the art in the field, we detailed the theoretical concepts at the basis of our work. First, we outlined the key concept and general properties of the Age of Information. Next, we addressed the matter of quantum entanglement in communication systems, and finally, we presented the key concepts of game theory. We then explored the problem of multiple eavesdroppers in communication systems.

We considered a framework where there is a sender (named Alice) and a designated receiver (named Bob) who communicate through quantum channels. We also introduced two eavesdroppers (Eve and Frank) whose goal is to intercept the information shared between Alice and Bob. To analyze this system, we adopted a static game of complete information approach within the game theory setting. We derived the Age of Information for the sender and the two eavesdroppers. Using the Age of Information, we determined the utility function for the players, and we identified the Nash equilibrium points using the computational tool MATLAB for different values of the costs c for Alice and $\tilde{k}$ for Eve and Frank. We discovered that there are three different Nash equilibrium points for values of c and $\tilde{\beta}$ between 0.01 and 0.14, while there is one Nash equilibrium point in other cases.

Finally, we analyzed how the Age of Information of the players varies for different Nash equilibrium points and for meaningful values of c and $\tilde{k}$. Additionally, we presented the graph of the total utility and the price of anarchy for the different Nash equilibrium points and various values of the costs. We also provided graphs of the eavesdropper probability $\tilde{\beta}$ for different unit prices at the various Nash equilibrium points, as well as the transmission rate λ. By analyzing the graphs, we were able to demonstrate the inefficiency of the secondary and third Nash equilibrium points.

To be concise, in this thesis work, we explored in detail how eavesdropping on quantum communication channels can affect the status-quo in game theoretic sense. There are multiple possible future developments that could use the current research as its basis and enhance our understanding of security in quantum communication channels. One example, to continue this research, is to look into how quickly information travels in quantum communication channels and how different people involved in the channel, such as senders, receivers, and eavesdroppers, interact with each other. It could also be interesting to study how the role of the quantum entanglement changes and affects the quantum communication channel, when there are more than two eavesdroppers are present. Additionally, exploring a possible connection between the age of information and quantum cryptography, and how we can use machine learning to better protect against eavesdropping in real-time, could

also be investigated to further deepen our understanding of the security in quantum communication channels. Consequently, this will help make quantum communication systems stronger and more efficient.

One straightforward and concrete extension of the theoretical work in this thesis, is based on Figure 3 and Figure 4. If we want to explore the case with three eavesdroppers instead of two, we could simply add another node to the tree diagrams depicted in Figure 3 and Figure 4, following the node specified for Frank. We could then define β_3 as the parameter associating with the third eavesdropper, say Charlie, and follow a similar pattern in deriving new equations required for further computation and investigation. This process can also be done for n eavesdroppers, by simply adding a node after the last node specified for the eavesdropper number $n-1$. At first, this might seem to include lots of computation; however, considering that we can take $\beta_1 = \beta_2 = \beta_3 = \cdots = \beta_n$, it is possible to derive simplified equations. Although, at this point, symmetricity at the Nash equilibrium and thus the equality of β_i's should be further investigated to explore the efficiency or the correctness of this assumption.

It is also important to explore new ways to understand how people make decisions in game-theoretic situations. Studying games where players do not have all the information or where the information changes over time, are few examples of possible research areas which could also enhance the work done in this thesis. By doing this, we could possibly find better ways to keep information safe in quantum communication channels. It might also be possible to use a method called reinforcement learning, where players learn from their past experiences to make better decisions in the future, to further develop and investigate dynamic settings in quantum communication channels including several eavesdroppers.

To conclude, studying how quantum communication channels, the speed of information, and game theory work together can help us make future quantum networks safer and more efficient. This research and above mentioned possible future developments based on it, can help create better ways to protect information and make sure it gets to where it needs to go. By using what we learned from this thesis work and adding more details and new ideas, we can make sure quantum communication stays reliable, especially given the fact that connectedness is increasing faster every passing year. This thesis work and its possible future developments require looking at different areas of science and technology, and critically thinking about how they might change in not so distant future.

References

[1] Abhishek Pandey and V Ramesh. Quantum computing for big data analysis. *Indian Journal of Science*, 14(43):98–104, 2015.

[2] Seid Koudia, Angela Sara Cacciapuoti, Kyrylo Simonov, and Marcello Caleffi. How deep the theory of quantum communications goes: Superadditivity, superactivation and causal activation. *IEEE Communications Surveys & Tutorials*, 24(4):1926–1956, 2022.

[3] Sanjit Kaul, Roy Yates, and Marco Gruteser. Real-time status: How often should one update? In *2012 Proceedings IEEE INFOCOM*, pages 2731–2735. IEEE, 2012.

[4] Riccardo Bassoli, Holger Boche, Christian Deppe, Roberto Ferrara, Frank HP Fitzek, Gisbert Janssen, and Sajad Saeedinaeeni. *Quantum communication networks*, volume 23. Springer, 2021.

[5] Leonardo Badia, Hilal Sultan Duranoglu Tunc, Aynur Cemre Aka, Riccardo Bassoli, and Frank HP Fitzek. Strategic interaction over age of information on a quantum wiretap channel. proceedings european wireless conf., 2023. *dei.unipd.it*.

[6] Alan Mainwaring, David Culler, Joseph Polastre, Robert Szewczyk, and John Anderson. Wireless sensor networks for habitat monitoring. In *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pages 88–97, 2002.

[7] Panos Papadimitratos, Arnaud De La Fortelle, Knut Evenssen, Roberto Brignolo, and Stefano Cosenza. Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. *IEEE communications magazine*, 47(11):84–95, 2009.

[8] Sanjit Kaul, Marco Gruteser, Vinuth Rai, and John Kenney. Minimizing age of information in vehicular networks. In *2011 8th Annual IEEE communications society conference on sensor, mesh and ad hoc communications and networks*, pages 350–358. IEEE, 2011.

[9] Alexandros Karakasidis, Panos Vassiliadis, and Evaggelia Pitoura. Etl queues for active data warehousing. In *Proceedings of the 2nd international workshop on Information quality in information systems*, pages 28–39, 2005.

[10] Ming Xiong and Krithi Ramamritham. Deriving deadlines and periods for real-time update transactions. *IEEE Transactions on Computers*, 53(5):567–583, 2004.

[11] Jiawei Wu, Zaisheng Lin, Liuguo Yin, and Gui-Lu Long. Security of quantum secure direct communication based on wyner's wiretap channel theory. *Quantum Engineering*, 1(4):e26, 2019.

[12] Laura Crosara, Nicola Laurenti, and Leonardo Badia. It is rude to ask a sensor its age-of-information: Status updates against an eavesdropping node. proceedings ieee balkancom. 2023.

[13] Leonardo Badia, Simone Merlin, Andrea Zanella, and Michele Zorzi. Pricing vowlan services through a micro-economic framework. *IEEE Wireless Communications*, 13(1):6–13, 2006.

[14] Holger Boche, Minglai Cai, Ning Cai, and Christian Deppe. Secrecy capacities of compound quantum wiretap channels and applications. *Physical Review A*, 89(5):052320, 2014.

[15] Valentina Vadori, Maria Scalabrin, Anna V Guglielmi, and Leonardo Badia. Jamming in underwater sensor networks as a bayesian zero-sum game with position uncertainty. In *2015 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2015.

[16] 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)*, pages 1–8. IEEE, 2022.

[17] Daniel S Berger, Francesco Gringoli, Nicolo Facchi, Ivan Martinovic, and Jens B Schmitt. Friendly jamming on access points: Analysis and real-world measurements. *IEEE Transactions on Wireless Communications*, 15(9):6189–6202, 2016.

[18] Matthias Schulz, Francesco Gringoli, Daniel Steinmetzer, Michael Koch, and Matthias Hollick. Massive reactive smartphone-based jamming using arbitrary waveforms and adaptive power control. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 111–121, 2017.

[19] Laura Crosara, Nicola Laurenti, and Leonardo Badia. Strategic status updates in an eavesdropping game, proceedings european wireless conf., 2023. *dei.unipd.it*.

[20] Anne Broadbent and Eric Culf. Rigidity for monogamy-of-entanglement games. proceedings itcs. 2023.

[21] Leonardo Badia and Francesco Gringoli. A game of one/two strategic friendly jammers versus a malicious strategic node. *IEEE Networking Letters*, 1(1):6–9, 2019.

[22] David Stephen Alberts, Daniel S Papp, et al. *The information age: An anthology on its impacts and consequences*. Center for Advanced Concepts and Technologies, 1997.

[23] AHM Shamsuzzoha and Petri T Helo. Real-time tracking and tracing system: Potentials for the logistics network. In *Proceedings of the 2011 international conference on industrial engineering and operations management*, pages 22–24. Kuala Lumpur, Malaysia, 2011.

[24] Hassan Khader Y Almathami, Khin Than Win, and Elena Vlahu-Gjorgievska. Barriers and facilitators that influence telemedicine-based, real-time, online consultation at patients' homes: systematic literature review. *Journal of medical Internet research*, 22(2):e16407, 2020.

[25] Suppawong Tuarob, Poom Wettayakorn, Ponpat Phetchai, Siripong Traivijitkhun, Sunghoon Lim, Thanapon Noraset, and Tipajin Thaipisutikul. Davis: a unified solution for data collection, analyzation, and visualization in real-time stock market prediction. *Financial innovation*, 7:1–32, 2021.

[26] U Narayan Bhat. *An introduction to queueing theory: modeling and analysis in applications*, volume 36. Springer, 2008.

[27] Leonardo Badia, Alberto Zancanaro, Giulia Cisotto, and Andrea Munari. Status update scheduling in remote sensing under variable activation and propagation delays. *Ad Hoc Networks*, 163:103583, 2024.

[28] Andrea Munari and Leonardo Badia. The role of feedback in aoi optimization under limited transmission opportunities. In *GLOBECOM 2022-2022 IEEE Global Communications Conference*, pages 1972–1977. IEEE, 2022.

[29] Alireza Javani, Marwen Zorgui, and Zhiying Wang. On the age of information in erasure channels with feedback. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2020.

[30] Randolph W Hall. Queueing methods: for services and manufacturing.pearson college div. *(No Title)*, 1991.

[31] Jie Zhang, Guangjie Han, and Yujie Qian. Queuing theory based co-channel interference analysis approach for high-density wireless local area networks. *Sensors*, 16(9):1348, 2016.

[32] Roy D Yates, Yin Sun, D Richard Brown, Sanjit K Kaul, Eytan Modiano, and Sennur Ulukus. Age of information: An introduction and survey. *IEEE Journal on Selected Areas in Communications*, 39(5):1183–1210, 2021.

[33] Maice Costa, Marian Codreanu, and Anthony Ephremides. On the age of information in status update systems with packet management. *IEEE Transactions on Information Theory*, 62(4):1897–1910, 2016.

[34] Mohammad Moltafet, Markus Leinonen, and Marian Codreanu. Average AoI in multi-source systems with source-aware packet management. *IEEE Transactions on Communications*, 69(2):1121–1133, 2020.

[35] Siddhant Garg and Goutham Ramakrishnan. Advances in quantum deep learning: An overview. *arXiv preprint arXiv:2005.04316*, 2020.

[36] Matthew F Pusey, Jonathan Barrett, and Terry Rudolph. On the reality of the quantum state. *Nature Physics*, 8(6):475–478, 2012.

[37] Michael A Nielsen and Isaac L Chuang. Quantum computation and quantum information. *Phys. Today*, 54(2):60, 2001.

[38] Giuliano Benenti, Giulio Casati, and Giuliano Strini. *Principles of quantum computation and information*. World scientific, 2004.

[39] Anton Zeilinger. Quantum teleportation. *Scientific American*, 282(4):50–59, 2000.

[40] Carlos Cardoso-Isidoro and Francisco Delgado. Shared quantum key distribution based on asymmetric double quantum teleportation. *Symmetry*, 14(4):713, 2022.

[41] Jeong San Kim, Gilad Gour, and Barry C Sanders. Limitations to sharing entanglement. *Contemporary Physics*, 53(5):417–432, 2012.

[42] A guide to global quantum key distribution networks. proceedings FICC. 2022.

[43] Antzela Kosta, Nikolaos Pappas, Vangelis Angelakis, et al. Age of information: A new concept, metric, and tool. *Foundations and Trends® in Networking*, 12(3):162–259, 2017.

[44] Jaya Prakash Champati, Hussein Al-Zubaidy, and James Gross. Statistical guarantee optimization for aoi in single-hop and two-hop fcfs systems with periodic arrivals. *IEEE Transactions on Communications*, 69(1):365–381, 2020.

[45] Yoshiaki Inoue, Hiroyuki Masuyama, Tetsuya Takine, and Toshiyuki Tanaka. A general formula for the stationary distribution of the age of information and its application to single-server queues. *IEEE Transactions on Information Theory*, 65(12):8305–8324, 2019.

[46] Drew Fudenberg and Jean Tirole. *Game theory*. MIT press, 1991.

[47] John Von Neumann and Oskar Morgenstern. Theory of games and economic behavior, 2nd rev. 1947.

[48] Alberto Bressan. Noncooperative differential games. *Milan Journal of Mathematics*, 79:357–427, 2011.

[49] Yu Liu, Cristina Comaniciu, and Hong Man. A bayesian game approach for intrusion detection in wireless ad hoc networks. In *Proceeding from the 2006 workshop on Game theory for communications and networks*, pages 4–es, 2006.

[50] Nicola Bastianello and Leonardo Badia. Decentralized intersection control using bayesian game theory. In *2022 2nd International Seminar on Machine Learning, Optimization, and Data Science (ISMODE)*, pages 442–447. IEEE, 2022.

[51] Martin J Osborne et al. *An introduction to game theory*, volume 3. Oxford university press New York, 2004.

[52] Anna V Guglielmi and Leonardo Badia. Analysis of strategic security through game theory for mobile social networks. In *2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pages 1–6. IEEE, 2017.

[53] Tansu Alpcan and Tamer Basar. A game theoretic approach to decision and analysis in network intrusion detection. In *42nd IEEE international conference on decision and control (IEEE Cat. No. 03CH37475)*, volume 3, pages 2595–2600. IEEE, 2003.

[54] Tansu Alpcan. *Game Theory for Security*, pages 1–5. Springer London, London, 2019.

[55] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Bacşar, and Jean-Pierre Hubaux. Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)*, 45(3):1–39, 2013.

[56] Lorenza Prospero, Roberto Costa, and Leonardo Badia. Resource sharing in the internet of things and selfish behaviors of the agents. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 68(12):3488–3492, 2021.