Age of Information for Quantum Communication Channels with Monogamy of Entanglement

Aygun Jabrayilova, Elena Camuffo, Laura Crosara, and Leonardo Badia
Dept. of Information Engineering, University of Padova, Italy
{aygun.jabrayilova, elena.camuffo, laura.crosara, leonardo.badia}@unipd.it

***Abstract*—For time-critical applications, the freshness of information often goes hand in hand with confidentiality to ensure the integrity of sensitive data. Quantum communications are expected to provide secure exchanges of information thanks to the principles of quantum mechanics, such as entanglement, to protect against data breaches. In this paper, we analyze an information update system, where communication between a sender and receiver occurs through a quantum channel, and we consider the presence of two malicious eavesdroppers. Quantum communications already allow consent to identify compromised data, but we show that the presence of multiple eavesdroppers is even more thwarted by a property of quantum channels known as *monogamy of entanglement*, which, in addition to revealing whether data have been intercepted, prevents multiple eavesdroppers from accessing the same content. Through a game-theoretic analysis, we compute the Nash equilibria of multiple eavesdroppers trying to minimize the age of information of the intercepted data, and we show how their inherent anarchy ensures a higher level of protection for the communication.**

***Index Terms*—Age of information; Quantum communications; Entanglement; Game theory.**

I. Introduction

Real-time status updates are needed for several applications in transportation and logistics, healthcare, finance and trading, emergency services, smart home devices. For example, real-time GPS updates allow companies to track shipments and optimize routes for more cost-effective and time-efficient delivery [1], data transfer of medical parameters implies important decision-making [2], and updates on stock prices and market data allow traders and companies to execute informed and immediate financial strategies [3].

An extremely critical aspect of real-time status updates is data freshness. Delay, throughput, queue length, and several other performance metrics do not fully capture the freshness or timeliness of the data to be transmitted [4]. The concept of *Age of Information* (AoI) is introduced to focus on this aspect. In particular, consider a system where status updates are sent from a source to a destination, taking a random time in the overall processing. AoI at time t is defined at the destination's side as [5]:

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

where $\sigma(t)$ represents the instant when the last data item successfully processed before time t was originally generated at the destination. We assume that all status updates carry fresh information and that the propagation time is instantaneous, setting the delay to zero.

Security is an essential part of communication networks, maintaining the confidentiality of the information transferred between a transmitter and a receiver, or in general of all involved parties. Although AoI does not directly affect the security of transferred information, it has indirect impacts on it. High AoI could potentially lead to poor decision-making and open to security threats. In addition, an eavesdropper in the communication network can anticipate the decision-making of the receiver. Again, this would not affect the security in the same sense as decryption and encryption would; however, it would affect the operation of the system [6]–[9]. In the presence of an eavesdropper, a transmitter can change the actions to make sure that the AoI at the receiver's side is as minimal as possible. This leads us to consider a game theoretic approach to such situations where one or more eavesdroppers are present in the communication network [10]. We use game theory to analyze the interaction between two eavesdroppers, where we also consider *monogamy of entanglement* as preventing both eavesdroppers from intercepting the communication at the same time. Unlike classical AoI-eavesdropping models, our quantum approach leverages monogamy of entanglement to prevent simultaneous interception, introducing inherent security constraints absent in classical systems. We further compute the resulting Nash equilibria (NEs) of this allocation, discussing both how many they are, how efficient they are, and to which parameters they depend upon. We discover a problem that in general has 3 NE (not all of them being close to Pareto efficiency), but sometimes only one. The latter case is better controllable to avoid information leakages.

The remainder of this paper is organized as follows. Section II provides the background. Section III describes the system and the proposed analysis, followed by numerical results in Section IV. Finally, Section V concludes the paper.

This work was supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.3, CUP D33C22001300002, PE00000014 – program "SEcurity and RIghts in the CyberSpace" (SERICS), Spoke 4 - project "Innovative Security Paradigms for beyond 5G" (ISP5G+).

[0]Monogamy of entanglement means that if two quantum systems are maximally entangled, they cannot be similarly entangled with a third. This restricts entanglement sharing and underpins the security of protocols like BB84. A formal example is the Coffman-Kundu-Wootters bound [11], which limits how bipartite entanglement can be distributed across three qubits.

II. Background

We focus on a *First Come First Served* (FCFS) queue with memoryless arrivals and services. This means that status updates from a source are generated so that the interarrival times X_j are independent and identically distributed, following an exponential pdf with parameter λ, *i.e.*, they all have the same average $\mathbb{E}[X] = 1/\lambda$. Similarly, they get service times as independent identically distributed exponential random variables with $\mathbb{E}[Y] = 1/\mu$. The system time is also exponentially distributed with parameter $\mu - \lambda$, as long as $\lambda < \mu$.

We will evaluate the average Age of Information (AoI), denoted as $\Delta = \mathbb{E}[\delta t]$, where $\delta(t)$ represents the AoI, as defined in (1). In the context of the First-Come-First-Served (FCFS) system, it can be shown [5] that:

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

From (2), we get the average AoI of an M/M/1 system as:

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

where load factor $\rho = \lambda/\mu$ is less than or equal to 1.

This model allows for adjustments to the arrival rate λ and the service rate μ to optimize the system. Note that values close to 0 minimize packet delays, while values close to 1 maximize throughput. Since the service rate μ in (3) is just a scaling factor, we can assume $\mu = 1$, without loss of generality [12]. Then, (3) can be rewritten as:

$$\Delta = 1 + \frac{1}{\lambda} + \frac{\lambda^2}{1-\lambda}. \tag{4}$$

The introduction of an eavesdropper into 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 AoI at the receiver's side is minimal. Therefore, the transmitter can try to send status updates as quickly or timely as possible to ensure the freshness of the information at the receiver's side. However, situations including an eavesdropper in a communication network are usually modeled as a partially degraded wiretap channel. In such models, intercepted information is lost and therefore the existence of an eavesdropper directly affects the AoI at the receiver and leads to changes in strategies for the transmission of the data [6].

A way to improve the confidentiality of the information exchange would be to resort to quantum communications [13], e.g., leveraging entanglement. This can be described as a phenomenon of quantum mechanics, where the states of several particles become intertwined. In this case, the state of a single particle cannot be described independently of others, even when the particles are separated by large distances.

Quantum entanglement significantly affects computing and communication. Since the entangled particles are intertwined, this connection forms the basis for quantum teleportation and quantum key distribution. The main idea is based on the superposition principle of quantum mechanics, which 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 so that the measurement of one particle affects the state of the other particle at the same time.

Entanglement has various practical applications [14]–[16]; in particular, it can obtain communication protocols that are highly secure and, in fact, theoretically unbreakable. Another core principle of quantum mechanics is *monogamy of entanglement*, which limits the number of systems to which a given quantum system can be entangled to [17]. This has a direct impact on quantum communication security, especially when multiple eavesdroppers are present in a system. In a secure quantum communication system, two particles cannot independently entangle with a third party, as they are maximally entangled with each other.

Even though the monogamy of entanglement can be mathematically described by using specific quantum values, we are here only interested in its impact on AoI. In general, quantum information can be disturbed by environmental factors, potentially leading to loss of coherence and information.

However, a challenge is the presence of eavesdroppers, which can affect AoI [12]. An eavesdropper attempting to intercept the quantum information 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 channel is critical for quantum communication.

Typically, the impact of the monogamy of entanglement is studied through game theory, 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 [18].

In game theory, multiple players seek to maximize their own payoff. This makes it possible to model the competition of different parties to achieve a selfish goal, which is especially interesting to reflect strategic planning [12]. Game theory has been widely used over the past few years to prove the results in intrusion detection, the security of self-organizing networks, and the physical layer and media access control (MAC) [19], [20]. Moreover, a similar analysis with two *senders* is considered in [21], as opposed to the case of two eavesdroppers of the present paper. However, that paper does not exploit any aspect of quantum communications, different from what we do here. As we will show, the monogamy of entanglement offers further protection against wiretapping.

Finally, we remark that our analysis assumes ideal quantum communication, practical implementations must contend with physical limitations such as channel noise, quantum decoherence, and hardware imperfections, potentially impacting the AoI and security guarantees. Still, our analysis presents the first foundation result in this sense.

III. System Model

We consider a transmitter sending periodic information to a legitimate receiver. We denote the transmitter as Alice and the receiver as Bob, and model this scenario using an FCFS M/M/1 queue [7], making the assumption that the receiver is passive. Transmissions occur at rate λ and are served with rate μ=1.

We introduce two eavesdroppers, referred to as Eve and Frank, whose objective is to intercept the information sent from Alice to Bob. However, Eve and Frank act as independent players and do not cooperate in their attempts. The behavior of the eavesdroppers is modeled as follows: we assume that each can randomly intercept every package sent by Alice. We model this as an independently identically distributed Bernoulli process with parameter $\beta_i \in [0,1]$. Specifically, $\beta_1, \beta_2 \in [0,1]$ represent the parameters associated with Eve and Frank, respectively [6].

We consider Bob to be a passive player, while Alice, Eve, and Frank are active. 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, interception by either Eve or Frank prevents successful reception by Bob. If no interception occurs, the information reaches Bob with probability $(1-\beta_1)(1-\beta_2)$. If Eve attempts to intercept the information while Frank does not, the information is successfully intercepted by Eve with probability $\beta_1(1-\beta_2)$. Similarly, if Frank attempts to intercept the information while Eve does not, the information is successfully intercepted by Frank with probability $\beta_2(1-\beta_1)$.

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. The flow of updates generated by Alice splits into three memoryless flows with rates λ_B, λ_E, and λ_F, with

$$\lambda_B = \lambda\big(1-\beta_1\big)\big(1-\beta_2\big) \tag{5}$$
$$\lambda_E = \lambda\beta_1\big(1-\beta_2\big) \tag{6}$$
$$\lambda_F = \lambda\beta_2\big(1-\beta_1\big)\,. \tag{7}$$

Alternatively, we can consider a scenario, in which both Eve and Frank attempt to intercept the same information, resulting 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 [10], it is reasonable to assume $p_1 = p_2 = \frac{1}{2}$.

Now, the flow of updates generated by Alice again splits into three memoryless flows with rates λ_B, λ_E, and λ_F, where

$$\lambda_B = \lambda(1-\beta_1)(1-\beta_2) \tag{8}$$
$$\lambda_E = \lambda\left[\beta_1\big(1-\beta_2\big) + \frac{\beta_1\beta_2}{2}\right] \tag{9}$$
$$\lambda_F = \lambda\left[\beta_2\big(1-\beta_1\big) + \frac{\beta_1\beta_2}{2}\right] \tag{10}$$

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, which occurs when we set both probabilities p_1 and p_2 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 (11) and (12), for the average age of information values at Bob's and Eve's sides, respectively [5]. We observe that, in fact, (11) is the same equation as (4) where λ is replaced by $(1-\beta)\lambda$. This is expected since $(1-\beta)\lambda$ represents the probability that Eve does not intercept and Bob receives the information.

$$\Delta_B\big(\lambda,\beta\big) = 1 + \frac{1}{\big(1-\beta\big)\lambda} + \frac{\big(1-\beta\big)^2\lambda^2}{1-\big(1-\beta\big)\lambda} \tag{11}$$

$$\Delta_E\big(\lambda,\beta\big) = 1 + \frac{1}{\beta\lambda} + \frac{\beta^2\lambda^2}{1-\beta\lambda} \tag{12}$$

Once we introduce a second eavesdropper, Frank, we have to adjust the average AoI values for each side and define the average AoI at Frank's side, which is similar to the value at Eve's side. To do so, we replace λ in (4) with (8) for Bob's side, with (9) for Eve's side, and with (10) for Frank's side. We get the following average AoI values:

$$\Delta_B\big(\lambda,\beta_1,\beta_2\big) = 1 + \frac{1}{\big(1-\beta_1\big)\big(1-\beta_2\big)\lambda} + \frac{\big(1-\beta_1\big)^2\big(1-\beta_2\big)^2\lambda^2}{1-\big(1-\beta_1\big)\big(1-\beta_2\big)\lambda} \tag{13}$$

$$\Delta_E\big(\lambda,\beta_1,\beta_2\big) = 1 + \frac{1}{\lambda\big[\beta_1\big(1-\beta_2\big)+\frac{\beta_1\beta_2}{2}\big]} + \frac{\lambda^2\big[\beta_1\big(1-\beta_2\big)+\frac{\beta_1\beta_2}{2}\big]^2}{1-\lambda\big[\beta_1\big(1-\beta_2\big)+\frac{\beta_1\beta_2}{2}\big]} \tag{14}$$

By simplifying (14), we get

$$\Delta_E\big(\lambda,\beta_1,\beta_2\big) = 1 + \frac{1}{\lambda\big[\beta_1-\frac{\beta_1\beta_2}{2}\big]} + \frac{\lambda^2\big[\beta_1-\frac{\beta_1\beta_2}{2}\big]^2}{1-\lambda\big[\beta_1-\frac{\beta_1\beta_2}{2}\big]}\,. \tag{15}$$

Instead, Δ_F follows the same expression as Δ_E with β_1 and β_2 swapped.

Now, since β_1 and β_2 must be equal for symmetry at the NE [10], we take $\beta_1 = \beta_2 = \tilde{\beta}$ and further simplify (13) and (15) as follows.

$$\Delta_B\big(\lambda,\tilde{\beta}\big) = 1 + \frac{1}{\big(1-\tilde{\beta}\big)^2\lambda} + \frac{\big(1-\tilde{\beta}\big)^4\lambda^2}{1-\big(1-\tilde{\beta}\big)^2\lambda} \tag{16}$$

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

To avoid an unrealistic effect where both Alice and two eavesdroppers increase their activity as much as they like, we assume that all players are subject to a cost directly proportional to their action value [6]. Thus, the players'

utilities take the following forms in (17), (18) and (19), where c is the cost assigned to Alice, k_1 to Eve and k_2 to Frank.

$$u_A(\lambda,\beta_1,\beta_2) = \left[\Delta_B(\lambda,\beta_1,\beta_2)\right]^{-1} - c\lambda \tag{17}$$

$$u_E(\lambda,\beta_1,\beta_2) = \left[\Delta_E(\lambda,\beta_1,\beta_2)\right]^{-1} - k_1\beta_1 \tag{18}$$

$$u_F(\lambda,\beta_1,\beta_2) = \left[\Delta_F(\lambda,\beta_1,\beta_2)\right]^{-1} - k_2\beta_2 \tag{19}$$

Once again, since $\beta_1 = \beta_2 = \tilde{\beta}$ due to the symmetry of the NE, we can simplify the utility functions. Additionally, we assume that costs are also equal for Eve and Frank for the same reason. Thus, we take $k_1 = k_2 = \tilde{k}$.

$$u_A(\lambda,\tilde{\beta}) = \left[\Delta_B(\lambda,\tilde{\beta})\right]^{-1} - c\lambda \tag{20}$$

$$u_E(\lambda,\tilde{\beta}) = \left[\Delta_E(\lambda,\tilde{\beta})\right]^{-1} - \tilde{k}\tilde{\beta} \tag{21}$$

$$u_F(\lambda,\tilde{\beta}) = \left[\Delta_F(\lambda,\tilde{\beta})\right]^{-1} - \tilde{k}\tilde{\beta} \tag{22}$$

Note that, $u_E(\lambda,\tilde{\beta}) = u_F(\lambda,\tilde{\beta})$ since $\Delta_E(\lambda,\tilde{\beta}) = \Delta_F(\lambda,\tilde{\beta})$. Now, we look at the NEs of the game. For this, we write down the best response (BR) functions for each side. In (23) and (24), $\lambda^*(\tilde{\beta})$ represents the best response of Alice to the choices of Eve and Frank, while $\tilde{\beta}^*(\lambda)$ represents the best responses of Eve and Frank to the choice of Alice.

$$\lambda^*(\tilde{\beta}) = \underset{\lambda\in[0,\infty)}{\operatorname{argmax}}\ u_A(\lambda,\tilde{\beta}) \tag{23}$$

$$\tilde{\beta}^*(\lambda) = \underset{\tilde{\beta}\in[0,1]}{\operatorname{argmax}}\ u_E(\lambda,\tilde{\beta}) = \underset{\tilde{\beta}\in[0,1]}{\operatorname{argmax}}\ u_F(\lambda,\tilde{\beta})\,. \tag{24}$$

Finally, we analyze the price of anarchy (PoA) within our model. The sum of utilities of Alice, Eve, and Frank is taken as a criterion for social welfare [6]. Then, we define the price of anarchy (PoA) as below in (25), where $\lambda_w, \tilde{\beta}_w$ represents the worst possible NE, while $\lambda_0, \tilde{\beta}_0$ is the social optimum [1]. The social optimum can be regarded as the outcome with maximum welfare. It has been shown in [6] that a first NE corresponds to achieving the social optimum, and the PoA is 1 if the system admits only one NE. In general,

$$\text{PoA} = \frac{u_A(\lambda_0,\tilde{\beta}_0) + u_E(\lambda_0,\tilde{\beta}_0) + u_F(\lambda_0,\tilde{\beta}_0)}{u_A(\lambda_w,\tilde{\beta}_w) + u_E(\lambda_w,\tilde{\beta}_w) + u_F(\lambda_w,\tilde{\beta}_w)}\,. \tag{25}$$

IV. Numerical Results

We show numerical evaluations based on the theoretical computations of the previous section. Fig. 1 illustrates the best responses of Alice and the two eavesdroppers for varying values of λ and $\tilde{\beta}$, when costs c and $\tilde{k}$ are equal to 0. We obtain only one NE at the intersection of the best responses. If we consider the best response for Alice, it makes sense to increase the value of λ as $\tilde{\beta}$ increases, since there is no cost for either side. However, this increase stops, and the value becomes stationary after $\tilde{\beta}$ increases beyond a certain limit. The reason is that Alice does not want status updates to be lost due to losing the entanglement on 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, $\tilde{\beta}$ can be increased as much as the eavesdroppers would like without any consequence.

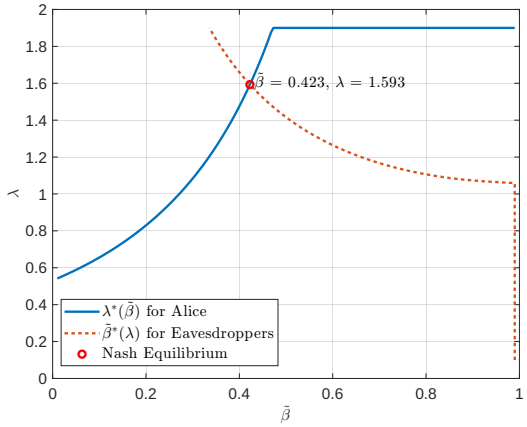

Fig. 1. Best response curves of Alice and two eavesdroppers varying under different $\tilde{\beta}$ and λ values, where costs c and $\tilde{k}$ are equal to 0.

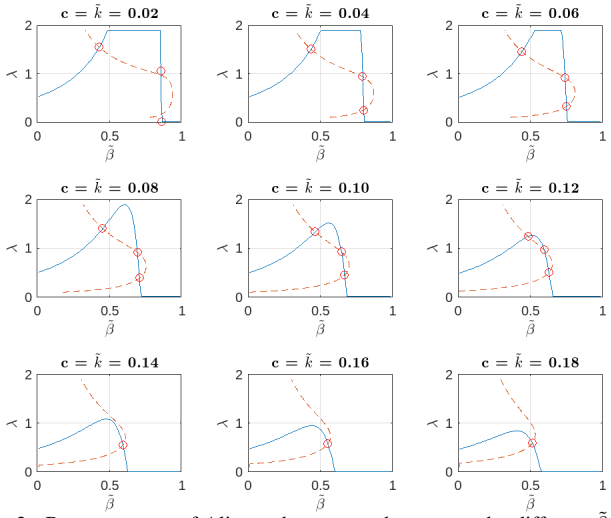

Fig. 2. Best responses of Alice and two eavesdroppers under different $\tilde{\beta}$ and λ values, where costs c and $\tilde{k}$ values are different for each subgraph.

Fig. 2 depicts 9 graphs similar to Fig. 1, with different c and $\tilde{k}$ values. The case $c = \tilde{k} = 0$ provides one NE, whereas the cases where $0.01 \le c = \tilde{k} \le 0.13$ have three. Moreover, starting from the case $c = \tilde{k} = 0.14$ and onward, we still obtain one NE. In Fig. 2, we illustrate different cases of c and $\tilde{k}$ spanning from 0.02 to 0.18. In the following graphs, we will see that the plots show up to three NEs.

It is interesting to examine the behavior of AoI as a function of unit prices c and $\tilde{k}$. Figs. 3–5 illustrate this behavior at the first, second, and third NE, respectively. Fig. 3 shows that while the unit price $\tilde{k}$ increases, the average AoI of the eavesdroppers in the first NE increases. This is expected since a higher cost would lead to lower activity by the eavesdroppers, consequently increasing their AoI. On the other hand, the average AoI of the transmitter decreases while the unit price $\tilde{k}$ increases. Yet, since increasing unit price $\tilde{k}$ leads to an increase in the average AoI of eavesdroppers, it also leads to increased activity on the transmitter's side, which reduces the AoI on Bob's side.

We observe a slightly different behavior in Fig. 4, which shows the second NE. Here, increasing the unit price $\tilde{k}$

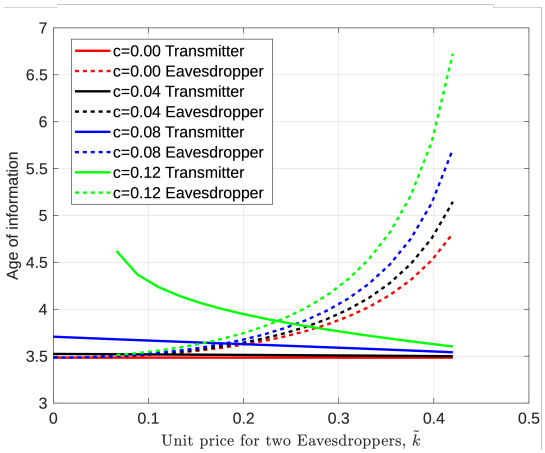

Fig. 3. Average AoI vs. the unit price $\tilde{k}$, for $c = 0$, $c = 0.04$, $c = 0.08$, and $c = 0.12$ at first Nash equilibrium.

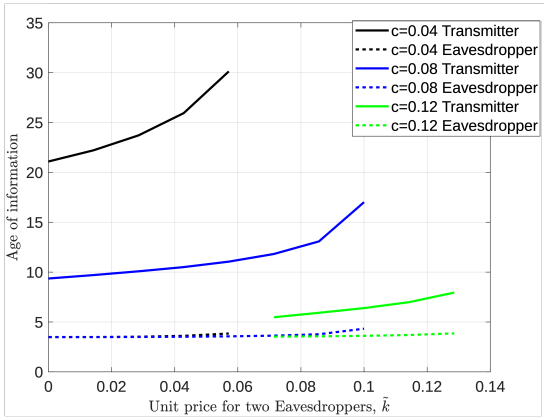

Fig. 4. Average AoI vs. unit price $\tilde{k}$, for $c = 0.04$, $c = 0.08$ and $c = 0.12$ at second Nash equilibrium.

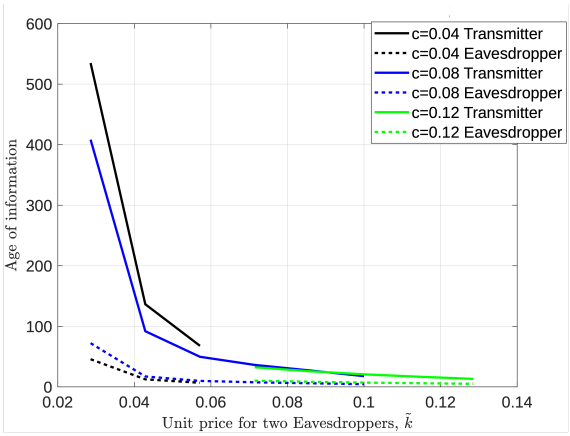

Fig. 5. Age of Information values vs. unit price $\tilde{k}$, for $c = 0.04$, $c = 0.08$ and $c = 0.12$ at third Nash equilibrium.

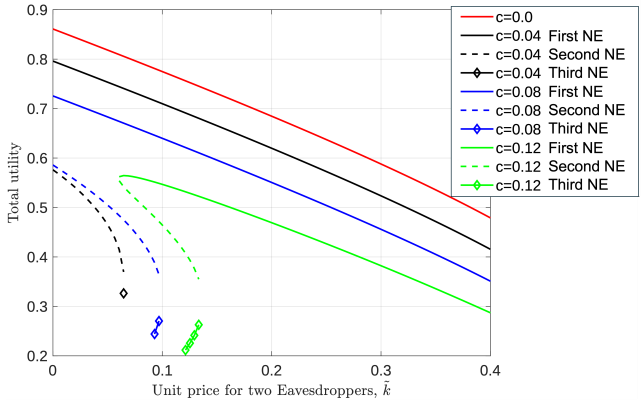

Fig. 6. Total utility vs. unit price $\tilde{k}$ for different values of c at first, second and third Nash equilibria.

leads to an increase in AoI on Bob's side. This is also true for the eavesdroppers, albeit on a limited scale. The reason lies in the inefficiency of the extra NEs beyond the first [6], and is even more evident in Fig. 5 showing the third NE. In this figure, AoI values decrease as the unit price $\tilde{k}$ increases. For further demonstration, consider Fig. 6, showing the relationship between total utility and unit price $\tilde{k}$ for $c = 0$, $c = 0.04$, $c = 0.08$, and $c = 0.12$ at the first, second, and third NEs. Solid lines describe the relationship between the total utility and the unit price of the eavesdroppers $\tilde{k}$ at the first NE, while dashed and dotted lines describe the second and third equilibria, respectively. Thus, it is clear that the total utility is always higher in the first NE compared to second and third. Fig. 6 also shows that while the unit price $\tilde{k}$ increases, the total utility decreases.

Now, we show how the eavesdropping probability $\tilde{\beta}$ and the transmission rate λ at the NEs change for different unit prices. Figs. 7 and 8 show $\tilde{\beta}$ and λ, respectively, versus the unit price $\tilde{k}$ for $c = 0$, $c = 0.04$, $c = 0.08$, and $c = 0.12$ at first, second, and third Nash equilibria. Both values of $\tilde{\beta}$ and λ decrease as the unit price $\tilde{k}$ increases. It is important to note that almost everywhere in Fig. 7, $\tilde{\beta}$ values are higher for increasing c values. This means that eavesdroppers increase their activity because they anticipate that the transmitter will send data less frequently. On the other hand, in Fig. 8 it is shown that higher c values result in lower λ values. This also makes sense since the transmitter would decrease the rate of action if the imposed cost increases.

Finally, we plot the PoA vs. unit price $\tilde{k}$ for various values of c, as shown in Fig. 9. The PoA computed in (25) quantifies the inefficiency of a system as the ratio between utilities at the worst possible NE and the social optimum. Here, it can be seen that regardless of c, the PoA increases with the unit price $\tilde{k}$. We conclude by stating that for relatively lower values of c and $\tilde{k}$, PoA can be very high [6].

V. Conclusions

We considered a sender and a designated receiver communicating through a quantum channel and two eavesdroppers trying to intercept the information and minimize the average AoI of leaked data. We defined a static game of complete information, deriving the average AoI for the involved parties. We identified 3 different NEs for the values of cost c and eavesdropping rate $\tilde{\beta}$ between 0.01 and 0.14, while there is one NE in the other cases.

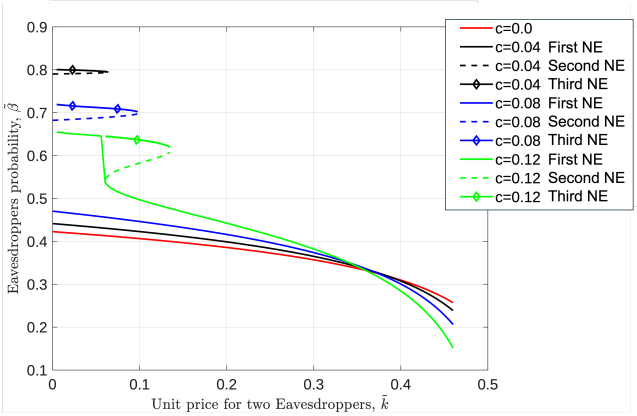

Fig. 7. $\tilde{\beta}$ vs. unit price $\tilde{k}$, for different values of c at first, second, and third Nash equilibria.

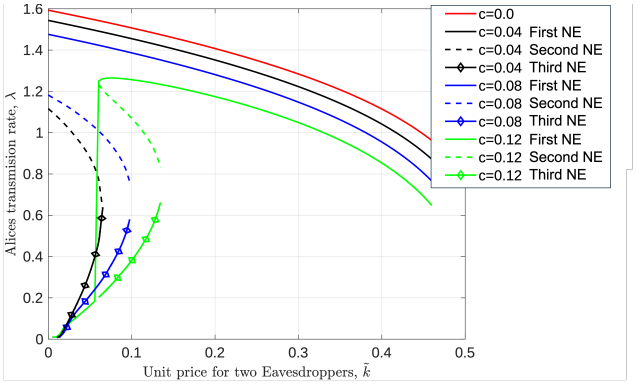

Fig. 8. λ vs. unit price $\tilde{k}$, for different values of c at first, second and third Nash equilibria.

This current research can be used as a basis for multiple developments in order to enhance our understanding of security in quantum communication channels. For example, monogamy of entanglement can be even more useful in the presence of more than 2 eavesdroppers, prompting a side investigation on whether multiple eavesdroppers adopt symmetric behavior or not [22]. Other possible extensions include games where the players have partial information on each other or the channels modify their characteristics over time. In this sense, future work may explore dynamic or incomplete information settings, where the strategies evolve over time or players lack full knowledge of others' actions or utilities. Such extensions would require the use of Bayesian games or reinforcement learning [8], [23], further enhancing the applicability of this model to more realistic scenarios.

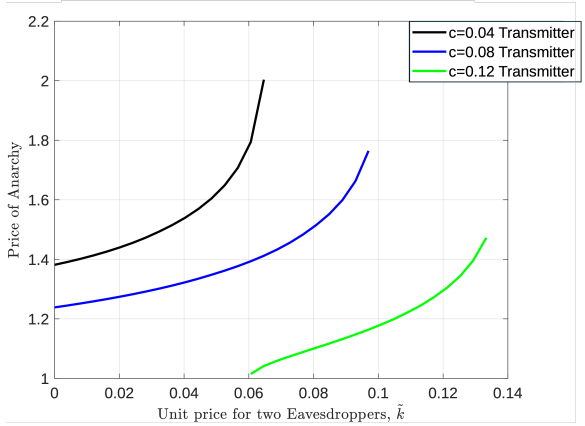

Fig. 9. PoA vs. unit price $\tilde{k}$ for $c = 0.04$, $c = 0.08$, and $c = 0.12$.

References

[1] M. Favero, C. Schiavo, A. Buratto, and L. Badia, "Price of anarchy for green digital twin enabled logistics," in *Proc. IEEE Symp. Comp. Commun. (ISCC)*, 2025.

[2] G. Cisotto, M. Capuzzo, A. V. Guglielmi, and A. Zanella, "Feature stability and setup minimization for EEG-EMG-enabled monitoring systems," *EURASIP J. Adv. Signal Proc.*, vol. 2022, no. 1, p. 103, 2022.

[3] M. Wen, P. Li, L. Zhang, and Y. Chen, "Stock market trend prediction using high-order information of time series," *IEEE Access*, vol. 7, pp. 28299–28308, 2019.

[4] A. Buratto, A. Munari, and L. Badia, "Strategic backoff of slotted ALOHA for minimal age of information," *IEEE Commun. Lett.*, vol. 29, no. 1, pp. 155–159, 2025.

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

[6] L. Badia, H. S. Duranoglu Tunc, A. C. Aka, R. Bassoli, and F. H. Fitzek, "Strategic interaction over age of information on a quantum wiretap channel," in *Proc. European Wirel.*, pp. 388–394, 2024.

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

[8] D. E. C. R. Catania, A. Buratto, and G. Perin, "Static and repeated cooperative games for the optimization of the AoI in IoT networks," in *Proc. IEEE Medit. Commun. Comp. Netw. Conf. (MedComNet)*, 2025.

[9] M. Moltafet, M. Leinonen, and M. Codreanu, "Average AoI in multi-source systems with source-aware packet management," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 1121–1133, 2020.

[10] L. Crosara, N. Laurenti, and L. Badia, "Age of information is not just a number: Status updates against an eavesdropping node," *Ad Hoc Networks*, vol. 155, p. 103388, 2024.

[11] V. Coffman, J. Kundu, and W. K. Wootters, "Distributed entanglement," *Phys. Rev. A*, vol. 61, no. 5, p. 052306, 2000.

[12] L. Crosara, N. Laurenti, and L. Badia, "Strategic status updates in an eavesdropping game," in *Proc. European Wirel.*, pp. 290–295, 2023.

[13] A. S. Cacciapuoti, J. Illiano, and M. Caleffi, "Quantum internet addressing," *IEEE Network*, vol. 38, no. 1, pp. 104–111, 2023.

[14] M. F. Pusey, J. Barrett, and T. Rudolph, "On the reality of the quantum state," *Nature Phys.*, vol. 8, no. 6, pp. 475–478, 2012.

[15] C. Cicconetti, D. Sabella, P. Noviello, and G. D. Paduanelli, "Quantum-safe edge applications: How to secure computation in distributed computing systems," in *Proc. IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. (PIMRC)*, 2024.

[16] A. Broadbent and E. Culf, "Rigidity for monogamy-of-entanglement games," *arXiv preprint arXiv:2111.08081*, 2021.

[17] J. S. Kim, G. Gour, and B. C. Sanders, "Limitations to sharing entanglement," *Contemp. Phys.*, vol. 53, no. 5, pp. 417–432, 2012.

[18] D. Fudenberg and J. Tirole, *Game theory*. MIT press, 1991.

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

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

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

[22] L. Crosara and L. Badia, "Strategic age of information under different correlation of sources," in *Proc. IEEE Wirel. Commun. Netw. Conf. (WCNC)*, 2025.

[23] E. Camuffo, L. Gorghetto, and L. Badia, "Moving drones for wireless coverage in a three-dimensional grid analyzed via game theory," in *Proc. IEEE Asia Pacific Conf. Circ. Syst. (APCCAS)*, pp. 41–44, 2021.