Self-reporting and Tampering in E-health with Game Theoretic Approach

Beliz Gunay
University of Padova
Department of Information Engineering
Information and Communication Technologies
beliz.guenay@studenti.unipd.it , 2080284

***Abstract*—E-health systems have revolutionized healthcare delivery, empowering individuals through features such as remote monitoring, customized care, and streamlined data organization. However, this transition also poses obstacles, such as the accuracy of self-reported information and the risk of tampering with health data. In this paper, we investigate a remote transmitter (patient) that is sending status updates about a process to a receiver (hospital), incurring a cost when doing so. The system is modeled as transiting between two conditions, implying that the receiver may start with correct knowledge about the process, but this information may become obsolete due to a natural drift of the process toward another regime and the lack of updates by the transmitter(patient). Ideally, we are exploring the scenario where a patient has a medical device at home and can voluntarily report their measurements to the hospital. However, the patient is not an expert and may report some wrong data. At the same time, we would like to see what happens if there is someone that is intentionally tampering with the data, so the sending of wrong data is not an accident. Game theoretic approach is used to evaluate the interaction these results; when there is no malicious user, we can refer to them as good users, and when there is malicious user, we can refer to them as bad players. We offer an examination to ascertain the parameters for the expenses borne by the participants and the effects of their choices on the system's overall performance.**

***Index Terms*—E-health, Self-reporting, Tampering, Security, Healthcare, Game theory**

I. Introduction

Digital technology is frequently used in the healthcare industry to search medical knowledge bases, monitor patient care quality, and enhance clinical support. [1] The E-health revolution has remarkably transformed healthcare, offering remote monitoring, customized treatment, and streamlined data management. However, this revolutionary shift also carries the risk of self-reporting errors and vulnerability to malicious tampering.

E-health tampering involves the unauthorized and intentional alteration of electronic health records (EHRs) or health-related information within electronic systems. This may include altering patient data, medical histories, diagnostic results, or treatment plans. Motivations for tampering range from bad faith to privacy violations. To solve this problem, strong security measures, encryption, access controls and auditing systems are implemented. Regular monitoring and compliance with data protection regulations such as HIPAA are essential to detect and prevent unauthorized changes and ensure the security and confidentiality of patient information in electronic health records. In order to sensitive healthcare data has strict privacy and confidentiality requirements, IT security is positioned as a primary concern in healthcare systems, services, and applications. There are various security challenges facing E-health, most of which are similar to those facing any essential infrastructure. [2]

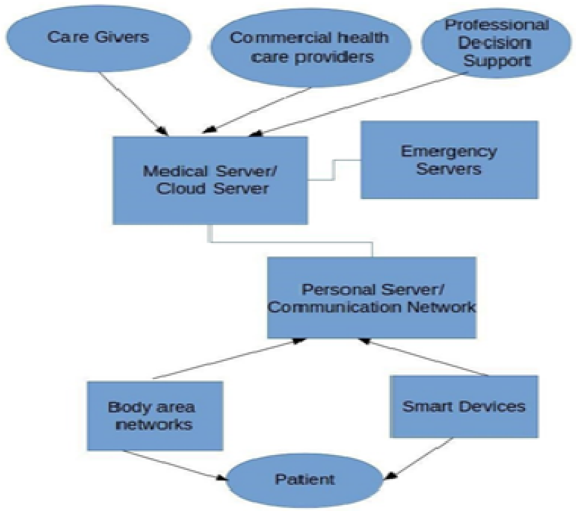
Care Givers
Commercial health care providers
Professional Decision Support
Medical Server/ Cloud Server
Emergency Servers
Personal Server/ Communication Network
Body area networks
Smart Devices
Patient

Fig. 1. End-to-End Architecture of an E-Health System [3].

Self-reporting in e-health involves individuals actively providing information about their health through electronic platforms and digital tools, contributing to electronic health records (EHRs) and overall health management. Particularly useful in chronic disease management, self-reporting allows patients to regularly share information about their condition, allowing healthcare providers to adjust treatment plans. Self-reporting through devices integrated into remote patient monitoring programs facilitates follow-up without the need for frequent in-person visits. While self-reporting offers advantages, it also presents challenges such as potential inaccuracies and missing information. Ensuring the security and confidentiality of self-reported data is crucial; it requires patient education, user-friendly interfaces, and robust safety measures for effective implementation. Patients are given central decision-making authority in emerging health care modalities. An E-health framework, which enables people to manage their own health as well as the health of their community, supports this approach to healthcare. According to the ultimate goals of health systems, patient-centered forms of health care give people the chance to become highly knowledgeable about sickness prevention and management, as well as to lower the cost of healthcare and boost patient satisfaction. [4]

We investigate the scenario where a patient has a medical device at home, and may report his/her measurements to the hospital on a voluntary basis. However, the patient is not an expert and may report some wrong data. At the same time, we would like to see what happens if there is someone that is intentionally tampering with the data, so the sending of wrong data is not an accident. Since patient treatment and decision-making depend heavily on the quality and integrity of health data, the problem of self-reporting and tampering in e-health systems can have major repercussions. Such problems can be examined and resolved through the use of game theory, a mathematical framework for simulating strategic interactions among rational decision-makers.

This paper delves into the pressing issue of tampering in E-health, emphasizing the seriousness of the situation and the potential harm it can cause through manipulation of information by malicious actors. In order to improve the accuracy of self-reporting and support E-health systems against manipulation, mitigating techniques can be used and improved the accuracy of self-reporting and strengthening E-health systems against tampering.

II. Related Work

E-health relates to tools and services using Information and Communication Technologies that can enhance prevention, diagnosis, treatment, monitoring and management for the benefit of the whole society by improving access and quality of care and making the healthcare sector more efficient. [5] Better access to diagnostic tests, increased provider coordination, better patient management, bridging physical gaps between patients and providers, and patient involvement in their own health and well-being are all signs of enhanced quality and innovative healthcare delivery. [6]

Patient self-reporting is considered a pragmatic and cost-effective approach in health research, but is plagued by issues with data validity, high loss to follow-up, and missing data. Glintborg et al. [7] indicate that despite these difficulties, patients' self-reports are generally reliable. On the other hand, routinely collected electronic data is emerging as a more accurate and practical alternative, especially for large patient groups; however, this requires cost and is dependent on data approval timelines. While patient self-reporting provides researchers with greater control, known limitations remain. Despite potential challenges, electronic datasets offer advantages such as accessibility, informativeness, standardization and reliability. In studies where secondary care plays a significant role, detailed electronic data may be considered superior, despite challenges such as data sharing agreements and extraction timelines. However, practical considerations and the need for a social perspective may still warrant the use of self-report methods in some cases. [8]

An electronic health record is information in an electronic format that contains medical data about a specific person. EHR systems are software platforms that physician offices and hospitals use to create, store, update, and maintain records for patients. For example, if a patient keeps his or her personal medical record electronically at home using a Word document, privacy concerns will not be of central importance. In this case, privacy concerns will not be of central importance. Our focus here is on the use of EHR systems by healthcare providers and how patients respond to the fact that their records are stored in these systems and may be made available to others through internet connections. In a public environment like this, the sensitivity of the data stored in a typical record system, demographic data about patients, their medical conditions, full medication list, family history, and possibly mental health data becomes increasingly important and worthy of investigation. [9]

Electronic health records (EHRs) are digital representations of a patient's medical history, and authorized healthcare professionals can access and share their health-related data. They provide a number of advantages over traditional paper-based medical records, including increased data accuracy, speed, and accessibility. They also make it easier for healthcare professionals to share patient data with other professionals, improving outcomes and care coordination. Overall, EHRs are an essential part of contemporary healthcare systems and significantly improve patient care and outcomes. They must be stored securely to protect patient privacy and stop unintended access, modification, or disclosure of personal health information. Security issues of the EHR arise from the possibility of unauthorized access to and alteration of private patient data. To protect them and stop tampering, it is critical to install strong security features, including security, access limits, and audit trails. Overall, maintaining patient trust and delivering high-quality healthcare depends on the security of EHRs. [10]

III. System Model

In certain scenarios [11], we may want to explore whether the status is still correct or has become wrong due to a drift. This can be modeled through a continuous time Markov chain with two states, namely, right (R) and wrong (W), whose transitions are as follows.

Transitions from W to R happen because the transmitter sends updates to the remote station (hospital), which occurs with rate p ¿ 0. It is not restrictive to assume that the updates are always successful, since in case they can be missed with a certain probability, one can correspondingly re-scale the value of p [12]. The remote system is aware that a malicious agent is present, but is unable to distinguish between the updates sent by the transmitter and the malicious user. We remark that characterizing the actions of the involved rational agents (the transmitter and the malicious) just through their activity rates p and q is a standard approach that allows to define a clear-cut strategic action of these agents as players in a game [13], [14], [15].

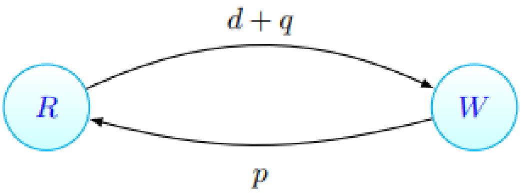

Fig. 2. Illustration of a continuous time Markov process with the respective rates of moving to one state to one another [16].

From the mathematical standpoint, the system respects the Markov property as all the three events of an update from the transmitter, a natural drift, and false data injection by the malicious are independent of one another, so the transitions are memoryless, and the two last ones just sum up to cause the transition rate from R to W be equal to d+q. The resulting Markov model is summarized in Fig. 2. The receiver possesses a correct measure of the output of the system until a drift occurs or a malicious agent sends false sensor reading.

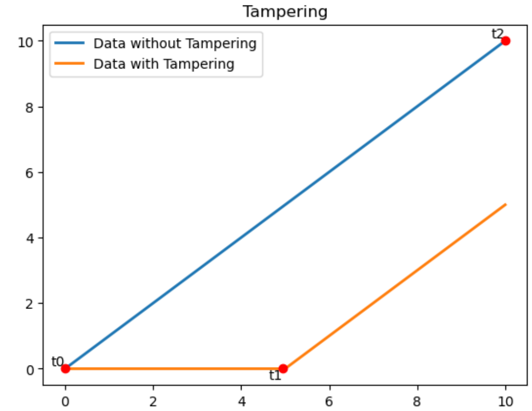

Fig. 3. Data metrics are initialized to 0 at t0. From that moment onwards, Data without Tampering increases linearly, whereas Data with Tampering initially remains at 0 (status is obsolete but correct). At t1, Data with Tampering starts increasing as well due to a drift. At t2, the status is refreshed, returning to its original position as observed at t0.

The expected value Δ can be computed by averaging over a period between any two subsequent updates, thus obtaining

$$\Delta = \frac{1/(2p)^2}{1/p + 1/b} \tag{1}$$

where $b = d + q$ [16].

If no malicious user is present in the system, the optimal transmission rate p is just obtained from balancing the cost term C · p, solving an unconstrained optimization of the controller's utility function defined as

$$u_N(p) = -\Delta - Cp \tag{2}$$

$$u_N(p) = -\Delta - Cp = -\frac{\frac{1}{2}(\alpha p)^2}{\frac{1}{\alpha p} + \frac{1}{(1-\alpha)p}} - Cp \tag{3}$$

With a malicious user trying to compromise communication, the term Δ also depends on q, and the utility in (1) must be written as $u_M(p,q)$. We assume that the malicious user incurs a cost Cq, with direct proportionality to the injection rate q through a coefficient C $>$ 0, limiting its false data injection.

The utility of the malicious user, whose aim is a high tampering, can be written as

$$u_M(p,q) = \Delta - Cm \tag{4}$$

$$u_M(p,q) = \Delta - Cm = \frac{\frac{1}{2}(\alpha p)^2}{\frac{1}{\alpha p} + \frac{1}{(1-\alpha)p+m}} - Cm \tag{5}$$

TABLE I
SUMMARY OF NOTATIONS

Parameter	Symbol
Transmission cost for sensors	C
Injection cost for malicious agent	K
Natural drift rate of the physical system	d
Variable	**Symbol**
Probability of measurement	p
Probability of wrong measurement	q

- d = system drift. This is the frequency of changes in the parameters. The patient makes a measurement but the measurement is no longer accurate, which implies a transition from R to W.
- p = probability of measurement. This is the frequency of correct measurements by the patient. When the system is in state W, it goes to R because we now have the right value.
- q = probability of wrong measurement. This is the frequency that something is wrong. When the system is in state R, it becomes W.

IV. GAME THEORETIC ANALYSIS

We denote the transmitter and the adversary as two rational agents N (no malicious) and M (malicious), respectively. They play a continuous game of complete information with continuous valued actions p and q, both chosen in (0,∞). Cournot duopoly, is a model of imperfect competition in which two with identical cost functions compete and both of them will receive profits derived from a simultaneous decision [13] which are $u_N(p,q)$ and $u_M(p,q)$. Values p and q are determined by N(no malicious) and M(malicious), respectively. The NE is derived from

$$\frac{\partial u_M(p,q)}{\partial q} = 0 \qquad \frac{\partial u_N(p,q)}{\partial p} = 0 \tag{6}$$

$$\frac{\partial \Delta}{\partial p} = -C \qquad \frac{\partial \Delta}{\partial m} = C \tag{7}$$

$$\begin{cases} p = \frac{\sqrt{1-\alpha}}{\sqrt{2\alpha C}} \\ q = -p + \frac{1}{\sqrt{2C}} \end{cases} \tag{8}$$

We accept that $K = C$, so $p > 0$ and $q > 0$. To obtain the best solution, we look at the cases $p >= 0$, because p cannot be less than 0 and we may ignore $q < 0$ situation because malicious user doesn't increase the transmission rate. Since the probability is $[0, 1]$, and the range is $[0, \infty)$, we can say that our result is meaningful. Thus, the NE conditions are

$$p = \begin{cases} (2\alpha C)^{-0.5} \quad if\ C < \left(\frac{\sqrt{1-\alpha}}{\sqrt{2\alpha C}} + (1-\alpha)p \right)^{-2} /2 \\ \frac{1}{2(\alpha p)^2} \left(\frac{1}{\alpha p} + \frac{1}{(1-\alpha)p} \right) - Cp \quad otherwise \end{cases} \tag{9}$$

$$q = \begin{cases} -p + \frac{1}{\sqrt{2C}} \quad if\ C < \left(\frac{\sqrt{1-\alpha}}{\sqrt{2\alpha C}} + (1-\alpha)p \right)^{-2} /2 \\ \frac{1}{2(\alpha p)^2} + \frac{1}{(1-\alpha)p+m} - Cm \quad otherwise \end{cases} \tag{10}$$

where the second part of (9) comes from minimizing (2).

V. NUMERICAL RESULTS

As in Fig. 4, we can observe the behaviour of p value with different alpha values and across with increasing cost. As we can see from the graphs, we are achieving the best p value when alpha is small and cost is small. As alpha value or cost is increased, our p value is decreasing.

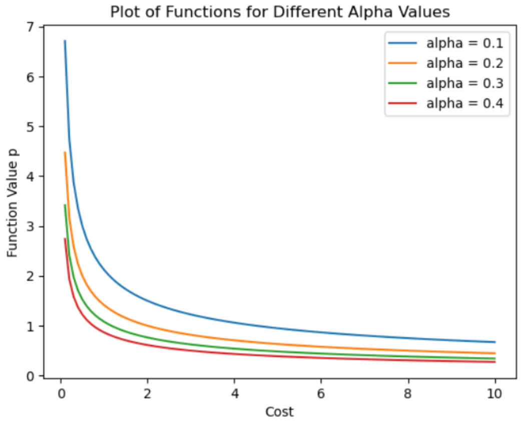

Fig. 4. Different alpha values relationship between Function value p and Cost

Fig. 5 investigates how the transmitter can choose its activity rate and show that utility $u_N(p, q)$ with fixed p has a maximum in alpha. As the alpha increases, the maximum of $u_N(p, q)$ increases as well. However, as the value p increases, the utility decreases. This is due to the fact that the transmitter has to transmit more often to minimize tampering, resulting in lower utility. The figure investigates a different alpha values from alpha = 0.1 to 0.4, respectively.

In this case, our NE is optimal when the alpha value is higher, closer to 1, and the p value is minimized, closer to 0. Conversely, when we increase the p value or reduce the alpha, the NE decreases accordingly.

On the other hand, Fig. 6 investigates how the transmitter can choose its activity rate and show that utility $u_M(p, q)$ with fixed q has a maximum in alpha. As the alpha increases, the maximum of $u_M(p, q)$ decreases. Moreover, as the value q increases, the utility decreases. This is due to the fact that the transmitter has to transmit more often to maximize tampering, resulting in lower utility. The figure investigates a different alpha values from alpha = 0.1 to 0.4, respectively.

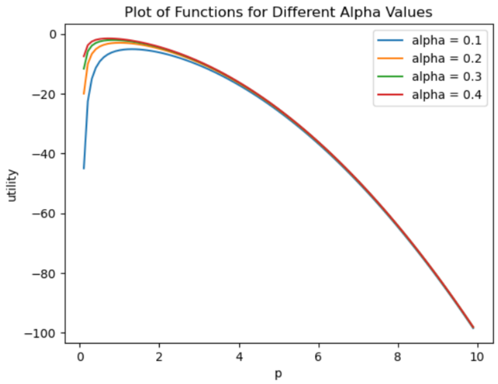

Fig. 5. Different alpha values relationship between utility and p

As m increases until it reaches 0, the utility decreases. After 0, the utility increases but we can observe that the bigger utility comes with a small alpha value (i.e. alpha = 0.1). Conversely, when we increase the m value or reduce the alpha, the NE increases accordingly.

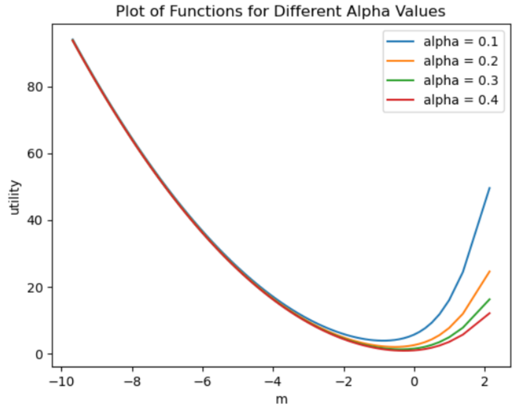

Fig. 6. Different alpha values relationship between utility and m

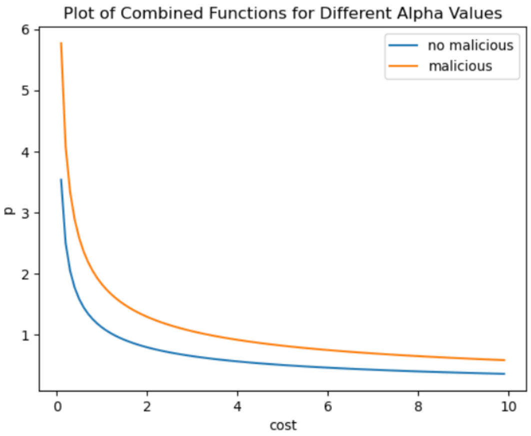

Fig. 7. relationship between p and cost for no malicious and malicious

Fig. 7 shows the strategic value of p depending on the presence (or not) for M (malicious) in the game at a fixed rate of alpha (for which, alpha = 0.1) and fixed range of cost C (for which, C = [0, 10], continuous).

The malicious causes an increase in the transmission cost of the transmitter, and as it increases, the difference between the two cases decreases. This is because a high transmission cost makes it inconvenient for the transmitter to increase the transmission rate, which is advantageous for the malicious user.

Fig. 8 shows the strategic value of m depending on the presence (or not) for M (malicious) in the game at a fixed rate of alpha (for which, alpha = 0.1) and fixed range of cost C (for which, C = [0, 10], continuous).

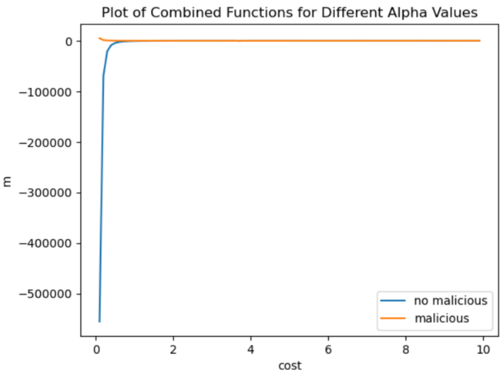

Fig. 8. relationship between m and cost for no malicious and malicious

When we looked for the existing conditions, the injection cost (C or K, assuming equal costs for both malicious and no malicious scenarios) should ideally decrease with increasing values of p and q. Under these conditions, the q occurs if and only if it is greater than 0. However, previous graphs have indicated an increase in q, which contradicts this expectation.

When the q value is less than 0, injecting false data becomes disadvantageous for malicious user. Consequently, as depicted in Figure 8, our focus shifts to the scenario where the q value for malicious user is equal to or close to 0. The graph shows that, under these circumstances, the malicious user remains more stable at that value. Meanwhile, the no malicious user is always more stable as it increases from a negative value. As a result, it can be inferred that malicious user becomes more advantageous than no malicious user in this specific situation.

VI. CONCLUSION

In this study, we investigated a scenario involving status updates between a transmitter (patient) and a remote station or receiver (hospital) over a network in the presence of a malicious agent that sends fake status updates. We provided a game theoretic approach of the interaction between no malicious user (good user) and malicious (bad) user. The no malicious user seeks to minimize tampering at the remote station and minimize its own cost, whereas the malicious user wants to maximize tampering at the remote station and its own cost.

We computed the NE, which is guaranteed to exist and be unique. The NE implies certain conditions that may cause the malicious to be inactive and the problem to revert to a plain nonlinear optimization. Even when this does not happen, our formulation as a continuous game of complete information with continuous valued actions p and q stands like Cournot duopoly. As a result, we observed that the malicious user has in more advantegeous condition. This also highlights the importance of careful monitoring, pre-emptively detecting, and being aware of a potential threat to its existence. Future researches may extend these results more general scenarios and advanced strategic interactions.

REFERENCES

[1] Paul, M., Maglaras, L., Ferrag, M. A.,& Almomani, I. (2023). Digitization of Healthcare Sector: A Study on privacy and security concerns. ICT Express, 9(4), 571–588. https://doi.org/10.1016/j.icte.2023.02.007

[2] Security and resilience in eHealth Infrastructures and services. ENISA. (2021, August 26). https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services

[3] Francis, T., Madiajagan, M., Kumar, V. (2015). Privacy issues and techniques in E-Health Systems. Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research. https://doi.org/10.1145/2751957.2751981

[4] De Raeve, P., Gomez, S., Hughes, P., Lyngholm, T., Sipilä, M., Kilanska, D., Hussey, P.,& Xyrichis, A. (2016). Enhancing the provision of health and social care in Europe through . International Nursing Review, 64(1), 33–41. https://doi.org/10.1111/inr.12266

[5] Pagliari1, C., Sloan2, D., Gregor2, P., Sullivan3, F., Detmer4, D., Kahan5, J. P., Oortwijn5, W., MacGillivray3, S., 1Division of Clinical and Community Health Sciences (General Practice Section), & Pagliari, C. A. (n.d.). What is eHealth (4): A scoping exercise to map the field. Journal of Medical Internet Research. https://www.jmir.org/2005/1/e9/

[6] World Health Organization. (n.d.). Health Systems. World Health Organization. https://www.who.int/data/gho/data/themes/theme-details/GHO/health-systems

[7] Glintborg B, Hillestrom P, Olsen L, Dalhoff K, Poulsen H. Are patients reliable when self-reporting medication use? Validation of structured drug interviews and home visits by drug analysis and prescription data in acutely hospitalized patients. Journal of Clinical Pharmacoepidemiology 2007; 47: 1440–1449.

[8] Taylor, M. J., Matata, B., Stables, R., Laws, A., England, D., & Lisboa, P. J. (2011). Issues in online patient self-reporting of Health Status. Health Informatics Journal, 17(1), 5–14. https://doi.org/10.1177/1460458210393914

[9] Angst, & Agarwal. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. MIS Quarterly, 33(2), 339. https://doi.org/10.2307/20650295

[10] AlOmrani, E. N., & Humayun, M. (2023). Securing Electronic Health Records (EHR) from tampering using blockchain. Advances in Systems Engineering, 397–410. https://doi.org/10.1007/978-3-031-40579-2_38

[11] A. Maatouk, S. Kriouile, M. Assaad, and A. Ephremides, "The age of incorrect information: A new performance metric for status updates," IEEE/ACM Trans. Netw., vol. 28, no. 5, pp. 2215–2228, May 2020

[12] L. Badia, "A Markov analysis of selective repeat ARQ with variable round trip time," IEEE Commun. Lett., vol. 17, no. 11, pp. 2184–87, Nov. 2013.

[13] L. Badia, A. Zanella, and M. Zorzi, "Game theoretic analysis of age of information for slotted ALOHA access with capture," in Proc. IEEE Infocom Wkshps, 2022

[14] K. Saurav and R. Vaze, "Game of ages in a distributed network," IEEE J. Sel. Areas Commun., vol. 39, no. 5, pp. 1240–1249, May 2021.

[15] G. D. Nguyen, S. Kompella, C. Kam, J. E. Wieselthier, and A. Ephremides, "Impact of hostile interference on information freshness: A game approach," in Proc. WiOpt, 2017.

[16] A game of age of incorrect information against an adversary injecting . (n.d.-a). https://www.dei.unipd.it/ badia/papers/202307C_S_R