Strategic Interactions in Multi-Sensor Networks Against False Data Injection

Valeria Bonagura
University Roma Tre, 00146 Rome, Italy
Polytechnic of Bari, 70125 Bari, Italy
Email: valeria.bonagura@uniroma3.it

Chiara Foglietta, Stefano Panzieri,
Federica Pascucci
University Roma Tre, 00146 Rome, Italy
Email: {chiara.foglietta, stefano.panzieri,
federica.pascucci}@uniroma3.it

Leonardo Badia
University of Padova,
35131 Padova, Italy
Email: leonardo.badia@unipd.it

***Abstract*—Ensuring secure and efficient data transmission in large-scale remote sensing is a critical challenge. We employ game theory to model the strategic interaction between multiple sensors, which independently optimize their data transmission, and an attacker seeking to maximize disruption. Each agent shapes its strategy through resource allocation constraints and cost functions associated with transmission and attack efforts. We seek to derive a Nash equilibrium that characterizes the optimal strategies of both transmitters and attacker. By solving Karush-Kuhn-Tucker (KKT) conditions, we obtain analytical equilibrium solutions between transmission efficiency and attack resilience. Our analysis highlights key trade-offs: increasing a sensor transmission cost reduces its activity rate but makes it a more attractive target for attacks, leading to a redistribution of adversarial efforts. Conversely, higher attack costs discourage malicious interference, prompting strategic adjustments in both transmission and defense mechanisms. These findings provide insights to enhance network resilience against strategic adversaries.**

I. Introduction

Cyber-Physical Systems (CPS) depend heavily on efficient data acquisition for effective monitoring, utilizing remote sensing technologies like satellites, drones, and ground-based sensors to gather large-scale data.[1], [2], [3]. However, the vulnerability of these systems to cyber threats such as data breaches and jamming necessitates robust security measures to safeguard data integrity[4], [5].

A critical metric in CPS is the *Age of Information* (AoI) [6], [7], [8], which quantifies the freshness of received updates. Recognizing that AoI lacks consideration for data accuracy, the Age of Incorrect Information (AoII)[9], [10] metric has been introduced to evaluate both data freshness and accuracy. High AoII levels can impair decision-making, underlining the importance of minimizing AoII in maintaining system reliability.

In complex CPS environments, data from multiple sources is transmitted over shared channels, necessitating policies that balance update frequencies to prevent network congestion while ensuring data freshness[11]. Optimization of these policies is essential for prioritizing critical information and maximizing system efficiency[12].

Prior research has explored AoI in scenarios with multiple competing sources. Initial studies [13] employed a game-theoretic approach to model these interactions, identifying less efficient Nash equilibriums compared to optimal strategies. Subsequent research corrected earlier AoI formulations,[7], [8], integrating more variables and extending the game-theoretic framework to encompass strategic decisions by different agents.

While existing studies consider environments where multiple sources aim to optimize their AoI by adjusting transmission frequencies independently, they often focus on competitive yet non-adversarial settings, emphasizing resource allocation challenges among competing interests [14], [15]. Furthermore, other research shifts focus to scenarios with redundant simultaneous updates from different sources providing identical content, revealing systemic inefficiencies and management complexities in distributed systems [16].

In recent research, innovative strategies to enhance CPS' efficiency are explored. [17] introduces a collaborative framework where nodes share correlated information to reduce redundancy and enhance efficiency, deviating from traditional game-theoretic approaches. Complementing this, [18] provides a game-theoretic analysis on similar collaborative behaviors, demonstrating significant reductions in inefficiencies typically associated with decentralized systems. These studies underscore the benefits of collaborative strategies in minimizing system overhead and boosting performance in CPS environments.

In contrast to these approaches, our study specifically addresses adversarial threats in CPS, particularly from entities like jammers. Previous research, such as [19], explored power control games where an agent minimizes AoI while an adversary aims to maximize it through targeted disruptions. However, our work uniquely integrates the concept of AoII to address both the timeliness and accuracy of information, which is crucial for scenarios vulnerable to false data injection [10].

Moreover, while foundational game-theoretic studies such as [20] and [21] focused on throughput objectives in network communications, our research shifts the focus specifically to the interplay between sensor updates and adversarial interference. We utilize a game-theoretic framework to model the strategic interactions between sensors and the adversary, emphasizing the minimization of AoII through strategic transmission adjustments. This approach diverges from traditional metrics by incorporating transmission costs to curb excessive actions, enabling the identification of optimal transmission policies that mitigate adversarial impacts while maintaining operational efficiency and security.

In this study, we investigate a scenario where multiple sensors transmit updates to a remote station, contending with interference from a malicious adversary that compromises data by injecting false information[13], [22]. Sensors monitor various aspects of a dynamic physical process, requiring careful management of transmission rates to balance freshness of information, channel capacity, and processing demands. Adversarial interference exacerbates these challenges, escalating the AoII and reducing system performance [19].

Our aim is to identify and protect the most vulnerable sensors to optimize resource allocation and enhance system robustness against attacks. We apply a game-theoretic framework to model the strategic interactions between sensors and the adversary, focusing on minimizing AoII through strategic transmission adjustments while the adversary attempts to maximize it [15], [20]. A non-zero-sum static game with complete information is formulated, including transmission costs to curb excessive actions. This model enables the identification of optimal transmission policies that mitigate adversarial impacts while maintaining operational efficiency and security.

II. System Model

In this section, we present the mathematical framework describing the dynamics of the system under consideration. The system's behavior is governed by the following equations:

$$\begin{cases} \dot{x}(t) &= f(x(t), u(t)), \\ y(t) &= h(x(t)), \end{cases} \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state vector, and $y(t) \in \mathbb{R}^m$ is the output vector at time t.

Sensor information is transmitted to a remote station, such as a supervisory control and data acquisition (SCADA) system, at discrete intervals. This discrete communication enables efficient data handling and timely decision-making. Each sensor $i = 1, \dots, m$ transmits its output $y_i(t)$ at specific time instances t_i^k, where k indexes the sequence of measurements for that sensor. The transmission intervals are modeled as

$$t_i^k = t_i^{k-1} + 1/p_i, \quad k = 1, 2, \dots$$

where $1/p_i$ denotes the average transmission interval for sensor i. This ensures that the networked control system can continuously update inputs $u(t)$ based on the most recent sensor measurements.

Each sensor measures a dynamic quantity that evolves over time. If the information acquisition rate is insufficient, the available readings may become outdated. We define d_i as the *drift rate* of sensor i, indicating that, on average, a reading becomes outdated after $1/d_i$ seconds. Additionally, the presence of a malicious agent capable of compromising the communication is considered through a *false data injection* attack, with the attack rate denoted as q_i. In such case, the rate at which sensor i readings become outdated is $d_i + q_i$.

To quantify the penalty of outdated or incorrect information from a sensor, we employ AoII, defined for sensor i as

$$\delta_i(t) = \ell_i(t) \cdot g_i(y_i(t), y_i(t_u)),$$

where $\ell_i(t)$ is the time elapsed since the last update, and $g_i(y_i(t), y_i(t_u))$ is an information penalty function capturing the discrepancy between the actual system output $y_i(t)$ and the last update $y_i(t_u)$, which may be malicious or legitimate. The penalty function $g_i(\cdot)$ equals 1 if the discrepancy exceeds a predefined threshold, and 0 otherwise. On average, $g_i(\cdot) = 1$ after $\frac{1}{d_i + q_i}$ seconds.

We take the *system AoII* as its average across all sensors

$$\delta(t) = \frac{1}{m} \sum_{i=1}^{m} \delta_i(t), \tag{2}$$

which is zero only when all sensors have AoII equal to 0. Monitoring the freshness of information from each sensor is crucial for making optimal control decisions.

To model the aging and updating process, we employ a two-state Markov chain model. Each sensor can be in one of two states: Right (R_i) or Wrong (W_i). The R_i state indicates that the information from sensor i is accurate, while the W_i state reflects outdated or incorrect information due to drift or malicious updates.

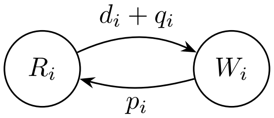

Fig. 1: Continuous-time Markov process illustrating transitions between states for sensor i.

The overall system state $S(t)$ is a tuple

$$S(t) = (S_1(t), S_2(t), \dots, S_m(t)),$$

where $S_i(t)$ denotes the state of sensor i at time t. Our objective is to minimize the time the system spends outside the desirable state:

$$S(t) = (R_1, R_2, \dots, R_m) = R,$$

where R signifies that all sensors are in the correct and timely state. Given the assumption that at any time only one sensor's state can change, the system state evolves as a continuous time Markov-Chain with 2^m states. The analysis begins by computing the average return time to the state R.

Let π be the steady-state probability vector of the Markov chain, which satisfies $\pi Q = 0, \sum_i \pi_i = 1$, where Q is the transition rate matrix of the Markov chain. The average return time to state R, denoted as T_R, is expressed as

$$T_R = \frac{1}{\pi_R}.$$

For our scenario, the continuous time Markov chain can be easily shown to be irreducible and recurrent [23], which guarantees that the return time is well-defined and finite.

During the return period T_R, each sensor undergoes multiple update cycles. The number of cycles for sensor i is

$$N_i = \frac{T_R}{1/(d_i+q_i)+1/p_i}. \tag{3}$$

The expected AoII over T_R, denoted as $\Delta_i^{T_R} = \mathbb{E}[\delta_i(t)]$, is computed for each sensor as

$$\Delta_i^{T_R} = N_i \left(\frac{1}{2p_i^2}\right), \tag{4}$$

resulting in an overall average AoII $\Delta = \mathbb{E}[\delta(t)]$ as

$$\Delta = \frac{1/m\sum_{i=1}^{m}\Delta_i^{T_R}}{T_R} = \sum_{i=1}^{m}\frac{1/(2p_i^2)}{1/(d_i+q_i)+1/p_i}. \tag{5}$$

The legitimate agent T seeks to minimize both the AoII Δ and its own transmission costs, while the malicious agent M aims to maximize Δ and simultaneously reduce its injection costs. The utility functions for T and M considering a single sensor i are defined as:

$$u_{\mathrm{T}}^i(p_i,q_i) = -\Delta_i^{T_R} - C_i p_i, \quad u_{\mathrm{M}}^i(p_i,q_i) = \Delta_i^{T_R} - K_i q_i. \tag{6}$$

Defining $p = [p_1,\ldots,p_m]^T$, $q = [q_1,\ldots,q_m]^T$, $C = [C_1,\ldots,C_m]$ and $K = [K_1,\ldots,K_m]$, we can express the overall utility functions for T and M as:

$$\begin{aligned} u_{\mathrm{T}}(p,q) &= \sum_{i=1}^{m} -\frac{1}{m}\Delta_i^{T_R} - C_i p_i = -\Delta - Cp, \\ u_{\mathrm{M}}(p,q) &= \sum_{i=1}^{m} \frac{1}{m}\Delta_i^{T_R} - K_i q_i = \Delta - Kq. \end{aligned} \tag{7}$$

In this context, p_i (for $i = 1,\ldots,m$) represents the transmission rate for each sensor, while q_i denotes the injection rate for each transmission channel. These rates chosen independently by the legitimate transmitter and the malicious agent, respectively, without knowledge of each other's decisions, as both aim to maximize their respective utility functions.

The agents' choices are constrained by the following resource limitations:

$$\sum_{i=1}^{m} p_i \le P_{\max}, \quad \sum_{i=1}^{m} q_i \le Q_{\max}, \tag{8}$$

as well as non-negativity conditions:

$$p_i \ge 0, \quad q_i \ge 0, \quad \forall i = 1,\ldots,m. \tag{9}$$

Here, $P_{\max}$ and $Q_{\max}$ are the maximum allowable total transmission and injection rates, respectively. These constraints ensure that the total rate does not exceeds the system's allowable capacity, reflecting practical limitations in resource allocation.

Under nominal conditions, i.e., with no malicious entities compromising the communications, the transmitter can freely select the transmission rate p_i to minimize AoII, subject to a transmission cost C_i for each sensor. The sensors share a common total transmission budget $P_{\max}$, meaning an increase in p_i for one sensor reduces the available budget for others. Thus, the sensors compete for this limited resource, and the allocation of p_i must be optimized to minimize Δ.

In the absence of attackers and assuming $P_{\max}$ is large enough to render the budget constraint inactive, the problem simplifies to finding the optimal p_i for each sensor independently. The optimal p_i is found by solving the fourth-degree polynomial equation obtained from $\partial u_T(p)/\partial p_i = 0$, i.e.,

$$2C_i p_i^4 + 4C_i d_i p_i^3 + 2C_i d_i^2 p_i^2 - 2d_i p_i - d_i^2 = 0. \tag{10}$$

for all i. This equation has a single positive real root, which represents the optimal transmission rate:

$$p_i = \frac{1}{6}\left(-3d + \sqrt{3}\sqrt{s} + \frac{3\sqrt{\frac{d_i^2}{3} + \frac{1}{3}s + \frac{2\sqrt{3}d_i}{C_i\sqrt{s}}}}{C_i}\right) \tag{11}$$

where: $s = d_i^2 + \frac{d_i^4 C_i}{r} + \frac{r}{C_i}$, and:

$$r = \left(\frac{27d_i^2C_i}{2} + d_i^6C_i^3 + \frac{3}{2}\sqrt{3}\sqrt{d_i^4C_i^2(27+4d_i^4C_i^2)}\right)^{\frac{1}{3}}.$$

In this case, each sensor's transmission rate is computed independently, providing a direct relationship between the cost parameter C_i and d_i and the optimal allocation strategy.

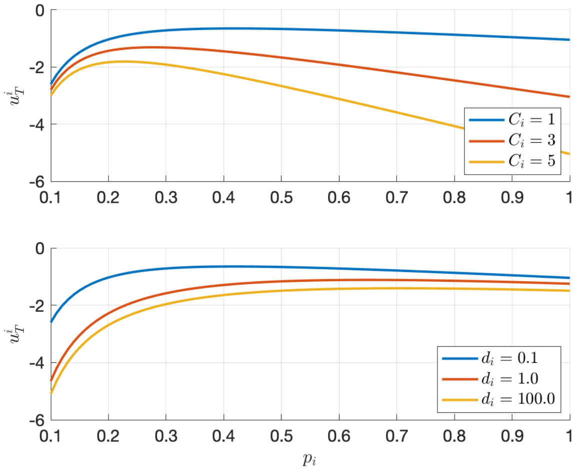

Fig. 2: Utility function $u_T^i(p)$ for a single sensor.

To better clarify, we consider a scenario with three sensors that must select their transmission rate p_i under nominal conditions. Specifically, we analyze the utility function $u_{\mathrm{T}}^i(p_i)$ as a function of p_i for each sensor $i = 1,2,3$, considering distinct drift rates and transmission costs. The drift rates are given by $d_i = [0.1, 1.0, 100]$, and the transmission costs are $C_i = [1,3,5]$, respectively. Fig. 2 shows that when the drift rate d_i is higher, the utility function becomes less sensitive to changes in p_i, with the curve flattening for larger values of d_i. This behavior indicates that the sensor's utility stabilizes and becomes less dependent on power allocation as d_i grows. Conversely, a higher transmission cost C_i results in a downward shift of the utility curve, with higher C_i values leading to lower utility. This highlights that higher transmission costs reduce the overall utility of the sensor, emphasizing the importance of optimizing power allocation to maintain system performance.

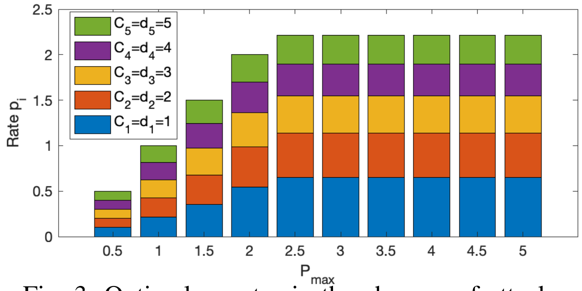

Fig. 3: Optimal p_i rates in the absence of attackers.

Fig. 3 demonstrates that as $P_{\max}$ increases, the values of p_i stabilize. This behavior suggests that when $P_{\max}$ is large enough, the system effectively operates without a total power constraint, resembling the water-filling problem described in [24].

III. Game-Theoretic Analysis

The interaction between the transmitter T and the adversary M is formalized as a game $\mathcal{G} = (\mathcal{P}, \mathcal{A}, \mathcal{U})$, where $\mathcal{P}$ is the set of players, $\mathcal{A}$ denotes their possible actions, and $\mathcal{U}$ corresponds to their utility functions. In this context, the set of players $\mathcal{P}$ consists of the transmitter T and the adversary M.

The set of actions $\mathcal{A}$ captures the strategic choices available to each player. The transmitter T selects transmission rates $p_i \geq 0$, for $i = 1, \dots, m$, while the adversary M chooses injection rates $q \geq 0$, for the same set of sensors. Although the game involves multiple sensors, we assume that a single legitimate agent (the transmitter) coordinates the transmission across all sensors, while a single malicious agent (the adversary) organizes the distributed attack on these sensors.

The utility functions, $\mathcal{U} = \{u_{\mathrm{T}}, u_{\mathrm{M}}\}$, define the payoffs for both players. The transmitter's utility $u_{\mathrm{T}}(p,q)$ reflects its aim to minimize the AoII while considering its transmission costs. Conversely, the adversary's utility $u_{\mathrm{M}}(p,q)$ represents its objective to maximize the AoII while minimizing its injection costs.

This interaction is modeled as a *static* game, where both players simultaneously select their strategies without knowledge of the other's decisions. The goal is to determine the Nash Equilibrium (NE), a state where neither player can improve their utility by unilaterally changing their strategy.

The utility functions for the transmitter T and the adversary M are defined as follows:

$$\begin{aligned} &\arg\max_{p} \quad u_{\mathrm{T}}(p,q) = -\Delta(p,q) - C^T p \\ &\text{subject to:} \quad \sum_{i=1}^{m} p_i \leq P_{\max}, \quad p_i \geq 0, \quad i = 1, \dots, m. \quad (12) \end{aligned}$$

$$\begin{aligned} &\arg\max_{q} \quad u_{\mathrm{M}}(p,q) = \Delta(p,q) - K^T q \\ &\text{subject to:} \quad \sum_{i=1}^{m} q_i \leq Q_{\max}, \quad q_i \geq 0, \quad i = 1, \dots, m. \quad (13) \end{aligned}$$

Game theory usually aims at finding stable operating points as Nash Equilibria (NEs). An NE represents a state where no player can unilaterally improve their utility by altering their strategy, given the strategies of the others. It can be shown that this game admits a unique Nash equilibrium, which follows directly from continuity and monotonicity of the utility functions. A formal proof is omitted for the sake of brevity.

The associated Lagrangian functions for the transmitter and the adversary are

$$\mathcal{L}_T(p, \lambda_T) = \Delta(p,q) + C^T p - \lambda_T\Big(P_{\max} - \sum_{i=1}^{m} p_i\Big), \quad (14)$$

$$\mathcal{L}_M(q, \lambda_M) = \Delta(p,q) - K^T q + \lambda_M\Big(Q_{\max} - \sum_{i=1}^{m} q_i\Big). \quad (15)$$

To determine the NE, we compute the first-order optimality conditions by taking the partial derivatives with respect to p_i and q_i and solving the stationary equations:

$$-\frac{\partial \Delta(p,q)}{\partial p_i} = C_i + \lambda_T, \quad \frac{\partial \Delta(p,q)}{\partial q_i} = K_i - \lambda_M. \quad (16)$$

For sensor $i = 1, \dots, m$, the equilibrium conditions yield

$$p_i = \big(2(K_i + \lambda_M + C_i + \lambda_T)\big)^{-0.5}, \quad (17)$$

$$q_i = -d_i - p_i + \big(2(K_i + \lambda_M)\big)^{-0.5}. \quad (18)$$

The complementary slackness conditions must hold:

$$\lambda_T\left(P_{\max} - \sum_{i=1}^{m} p_i\right) = 0, \; \lambda_M\left(Q_{\max} - \sum_{i=1}^{m} q_i\right) = 0. \quad (19)$$

If the rate constraint is active, i.e., $\sum_{i=1}^{m} p_i = P_{\max}$, then $\lambda_T > 0$. Otherwise, if $\sum_{i=1}^{m} p_i < P_{\max}$, then $\lambda_T = 0$. The same reasoning applies to the adversary's constraint and λ_M.

When both constraints are binding, the Lagrange multipliers satisfy the following equations:

$$\mathcal{L}_{\lambda_T} : P_{\max} - \sum_{i=1}^{m} (2(K_i + \lambda_M + C_i + \lambda_T))^{-0.5} = 0, \quad (20)$$

$$\mathcal{L}_{\lambda_M} : P_{\max} + Q_{\max} + \sum_{i=1}^{m} \left[d_i - (2(K_i + \lambda_M))^{-0.5}\right] = 0. \quad (21)$$

By solving this system for λ_T and λ_M, we obtain the equilibrium values of the Lagrange multipliers. These are then substituted into (17) and (18), yielding the optimal resource allocation for the transmitter and the adversary.

Fig. 4 illustrate the behavior of the function $\mathcal{L}_{\lambda_M}$ with respect to λ_M under different parameter settings. In both subplots, the function exhibits a strictly increasing and concave shape, ensuring that if a solution exists, it is unique and corresponds to the single point where $\mathcal{L}_{\lambda_M} = 0$.

In Fig. 5, the function starts from a given value at $\lambda_M = 0$ and increases monotonically. However, depending on the fixed parameters, the function may not cross zero, implying the absence of a solution. Specifically, if the function takes positive values for small λ_M, no intersection with the horizontal axis occurs, and thus no valid solution exists.

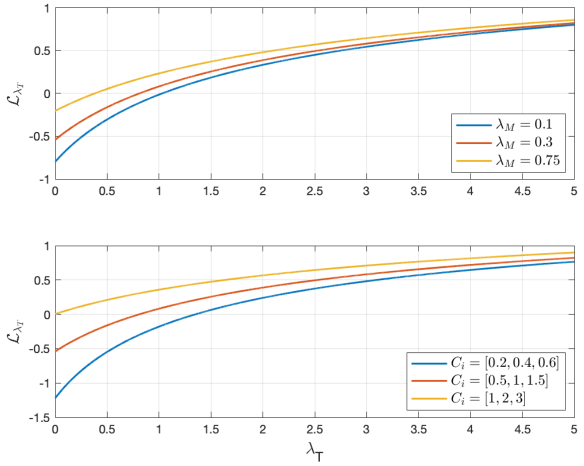

Fig. 4: $\mathcal{L}_{\lambda_T}$ when varying λ_M and C_i.

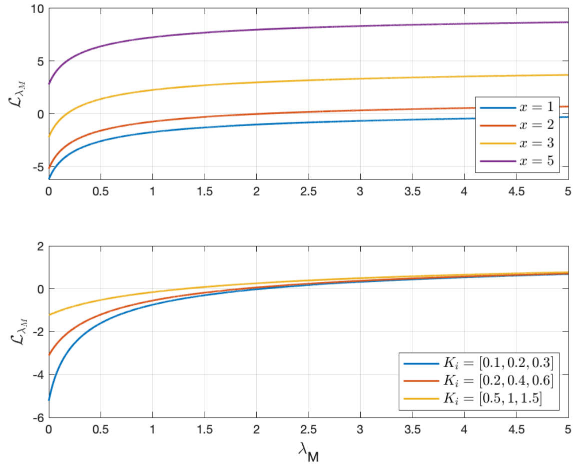

Fig. 5: $\mathcal{L}_{\lambda_M}$ at varying $x = P_{\max} + Q_{\max} + \sum_{i=1}^{m} d_i$ and K_i.

IV. Numerical Results

We consider a system of three sensors, each defined by specific parameters that govern their performance and interactions within the system. This section presents the results for key use cases that illustrate the primary scenarios of interest.

A. Scenario 1: Baseline Case

The first scenario represents a fundamental use case where the resource limitation constraint is inactive. This serves as a reference scenario, allowing us to observe the system's behavior in the absence of external limitations. The parameters for this case are summarized in Table I.

To ensure that the constraints do not influence the results, the values of $P_{\max}$ and $Q_{\max}$ are set sufficiently large.

TABLE I: Parameters and output in Scenario 1.

	d_i	C_i	K_i	p_i	q_i
Sensor 1	0.3	0.3	0.1	1.118	0.818
Sensor 2	0.6	0.6	0.2	0.791	0.190
Sensor 3	0.9	0.9	0.3	0.645	0

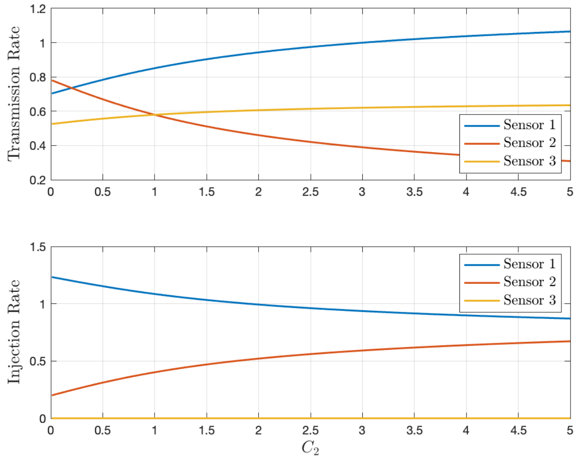

Fig. 6: Transmission and injection rates when C_2 increases.

The results for this scenario have been analyzed analytically in [10], but they can also be computed using Eq. 17 and Eq. 18, under the assumption that $\lambda_M = \lambda_T = 0$.

Since the sensors operate independently of one another, the optimization problem for each sensor is solved separately. Each sensor determines its optimal transmission rate (p_i) and the attacker's injection rate (q_i) based on its unique parameters (d_i, C_i, and K_i). This case provides a clear benchmark to compare how different parameter modifications affect the system's dynamics in the subsequent scenarios.

B. Scenario 2: Single Sensor Becomes a Preferred Target for the Attacker

In this scenario, we analyze the effect of increasing the transmission cost C_2 for Sensor 2, while keeping all other parameters unchanged, as listed in Table I.

As shown in Fig. 6, an increase in the transmission cost C_2 leads to a decrease in Sensor 2's transmission rate. This reduction makes Sensor 2 a more attractive target for the attacker, as it becomes easier to compromise. In response, the attacker reallocates its efforts, increasing its injection rate towards Sensor 2 while reducing its focus on the other sensors.

At the same time, the transmitter compensates for the reduced transmission from Sensor 2 by increasing the transmission rates of the other sensors. This balancing effect illustrates the strategic interplay between the attacker and the transmitter: as the cost of transmission for a particular sensor increases, both agents adjust their strategies accordingly. The attacker shifts its focus toward the weaker target, while the transmitter reallocates its resources to maintain overall system performance.

C. Scenario 3: Strengthening the Defense of a Single Sensor

In this scenario, we investigate the impact of increasing the attack cost K_1 for Sensor 1. The other parameters remain unchanged. As depicted in Fig. 7, an increase in K_1 makes attacking Sensor 1 more expensive for the adversary. Consequently, the attacker reduces its injection rate for this sensor. The transmitter follows a similar pattern, decreasing

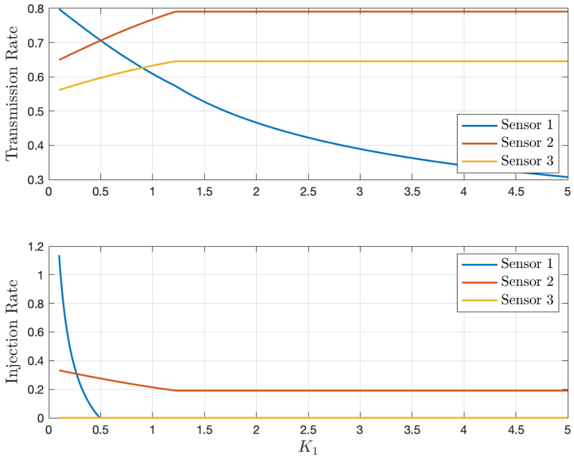

Fig. 7: Transmission and injection rates when K_1 increases.

its transmission rate to avoid unnecessary energy expenditure on a less threatened sensor.

This shift leads to an increase in the transmission rates of the other sensors, as the transmitter reallocates resources to where they are most needed. Similarly, the attacker, facing higher costs to compromise Sensor 1, redirects its efforts toward other sensors that remain more vulnerable. This scenario highlights how increasing the cost of attack for a single sensor can effectively deter adversarial actions, redistributing attack efforts to other parts of the system.

V. Conclusions

This paper investigates the strategic game between transmitters and attackers within a multi-sensor system, focusing on how variations in transmission and attack costs affect their equilibrium strategies. Our analysis reveals that higher transmission costs make sensors more vulnerable to attacks, prompting a strategic redistribution of efforts within the system. Conversely, an increase in attack costs deters aggression towards these sensors, compelling attackers to modify their strategies, while transmitters adjust their defenses accordingly.

The findings suggest methods for enhancing the resilience of multi-sensor networks by strategically manipulating cost parameters to reduce vulnerabilities. The proposed framework has potential applications in areas such as network security and resource allocation in distributed systems. Future work will aim to adapt this strategic framework to dynamic settings, integrating adaptive learning and resource constraints to better counter adversarial threats.

Acknowledgment

Project co-founded by the European Union - Next Generation Eu - under National Recovery and Resilience Plan (NRRP), Mission 4 Component 2 Incestment 3.3- Decree No. 352 (9^{th} April 2022) of Italian Ministry of University and Research - Concession Decree No. 2153 (28^{th} December 2022) of the Italian Ministry of University and Research, Project code D93D22001390001, within the Italian National Program PhD Programme in Autonomous Systems (DAuSy).

References

[1] B. Dafflon, N. Moalla, and Y. Ouzrout, "The challenges, approaches, and used techniques of cps for manufacturing in industry 4.0: a literature review," *Int. J. Adv. Manuf. Tech.*, vol. 113, pp. 2395–2412, 2021.

[2] E. Camuffo, L. Gorghetto, and L. Badia, "Moving drones for wireless coverage in a three-dimensional grid analyzed via game theory," in *Proc. IEEE APCCAS*, 2021, pp. 41–44.

[3] E. Recayte and A. Munari, "Caching at the edge: Outage probability," in *Proc. IEEE WCNC*, 2021.

[4] M. M. Harb, D. De Vecchi, and F. Dell'Acqua, "Phisical vulnerability proxies from remotes sensing: Reviewing, implementing and disseminating selected techniques," *IEEE Geosc. Remote Sens. Mag.*, vol. 3, no. 1, pp. 20–33, 2015.

[5] V. S. A. Hendrawan and D. Komori, "Developing flood vulnerability curve for rice crop using remote sensing and hydrodynamic modeling," *Int. J. Disast. Risk Red.*, vol. 54, p. 102058, 2021.

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

[7] M. Moltafet, M. Leinonen, and M. Codreanu, "On the age of information in multi-source queueing models," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 5003–5017, 2020.

[8] S. K. Kaul and R. D. Yates, "Timely updates by multiple sources: The M/M/1 queue revisited," in *Proc. Conf. Inf. Sc. Syst. (CISS)*, 2020.

[9] A. Maatouk, M. Assaad, and A. Ephremides, "The age of incorrect information: An enabler of semantics-empowered communication," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 4, pp. 2621–2635, 2022.

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

[11] M. A. Abd-Elmagid and H. S. Dhillon, "Age of information in multi-source updating systems powered by energy harvesting," *IEEE J. Sel. Ar. Inf. Th.*, vol. 3, no. 1, pp. 98–112, 2022.

[12] D. Sinha and R. Roy, "Optimal scheduling for maximizing information freshness and system performance in industrial cyber–physical systems," *Comp. Commun.*, vol. 169, pp. 33–47, 2021.

[13] R. D. Yates and S. K. Kaul, "The age of information: Real-time status updating by multiple sources," *IEEE Trans. Inf. Th.*, vol. 65, no. 3, pp. 1807–1827, 2019.

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

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

[16] Z. Chen, D. Deng, H. H. Yang, N. Pappas, L. Hu, Y. Jia, M. Wang, and T. Q. Quek, "Analysis of age of information in dual updating systems," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 11, pp. 8003–8019, 2023.

[17] A. Buratto, H. Tuwei, and L. Badia, "Optimizing sensor data transmission in collaborative multi-sensor environments," in *Proc. IEEE Int. Conf. Commun. Netw. Satell. (COMNETSAT)*, 2023, pp. 635–639.

[18] L. Badia and L. Crosara, "Correlation of multiple strategic sources decreases their age of information anarchy," *IEEE Trans. Circ. Syst. II*, vol. 71, no. 7, pp. 3403–3407, 2024.

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

[20] G. Thamilarasu and R. Sridhar, "Game theoretic modeling of jamming attacks in ad hoc networks," in *Proc. IEEE ICCCN*, 2009.

[21] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Başar, "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach," in *Proc. IEEE MILCON*, 2011, pp. 119–124.

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

[23] C. G. Cassandras and S. Lafortune, *Introduction to discrete event systems*. Springer, 2008.

[24] O. Elgarhy and L. Reggiani, "Application of the water filling algorithm to the sum rate problem with minimum rate and power constraint," in *Proc. Adv. Wirel. Opt. Commun. (RTUWO)*, 2018, pp. 12–16.