Data Injection in a Vehicular Network Framed Within a Game Theoretic Analysis

Laura Crosara, Mattia Brocco, Chiara Cavalagli, Xianlong Wu, Elvina Gindullina, Leonardo Badia
Dept. of Information Engineering (DEI), University of Padova, Italy
email: {laura.crosara.1@phd. , mattia.brocco@studenti. , chiara.cavalagli@studenti. ,
xianlong.wu@studenti. , elvina.gindullina@, leonardo.badia@ }unipd.it

***Abstract*—Vehicular networks involve communications between automobiles and roadside infrastructures, to improve safety, traffic efficiency, and comfort. They require to establish secure and efficient means of communication among smart vehicles exploiting the advantage provided by real time data. Thanks to the flexibility of its architecture, a vehicular network is also prone to abuse by individual users and especially to cyber attacks that can have serious consequences. Hence, the assignment of communication opportunities within the network with the purpose of data injection must be carefully monitored. In this work, we develop a game theoretic model that seeks to obtain the best trade-off solution and perform strategic and dynamic decision-making on the available bandwidth assigned to the vehicles. This can be further expanded to counteracting specific types of threat, such as denial of service, or malicious node detection based on the data sent by a vehicle.**

***Index Terms*—Vehicular ad hoc networks; Vehicle-to-Infrastructure; Denial-of-service attack; Game Theory.**

I. Introduction

A vehicular ad hoc network (VANET) has the objective of interconnecting smart nodes on the road, either moving vehicles or stationary roadside units (RSUs), to efficiently spread information and improve the efficiency of intelligent decision making to ensure the safety of the road through interactions and the infrastructure [1].

These networks are particularly important in light of the future development of smart vehicles (SVs) that, incorporating a rich set of sensors and software components, such as GPS, onboard units to communicate with other vehicles, electronic identity, event data recorder, [2], are capable of autonomous driving as well as decision making [3]–[5].

VANETs operate in a highly dynamic scenario, since SVs can move at different speeds and directions, and require real time processing of a high amount of data, thus making their connections extremely short but with strong requirements in terms of freshness and accuracy [6]. In this context, two problems arise: first of all, SVs need an up-to-date representation of the surrounding environment, which translates into a requirement of low age of information [7]–[10] and forces them to frequently report considerable amount of data. On the other hand, data injection from SVs is also subject to concerns of available bandwidth, and the RSUs ought to avoid that local data sent by vehicles saturate the entire channel available. In a classic context of distributed/selfish management of the agents, each SV would be trying to submit as much data as possible, which is a typical selfish behavior that can lead to a phenomenon known as the tragedy of the commons [11], [12].

Finally, the injection of excessive amount of data by an SV may even raise security concerns. Malicious SVs might disseminate fake messages to disrupt network operation, either by sending false information or just saturating the available bandwidth [13], [14].

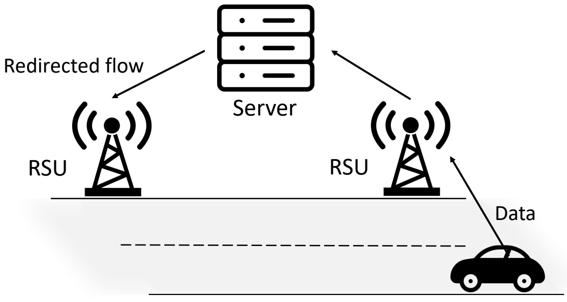

Fig. 1. RSU and SV interaction in a VANET.

We claim that RSUs, being the gateways to the whole data exchange on the VANET, play a critical role in controlling data injection from the SVs, and ought to operate some form of prevention for misuse or DoS attacks. RSUs have the ability to make decisions on resource allocation to balance computational costs, energy consumption and resource requirements [15], while on the other hand the SVs can be aware of this capability and plan their data injection accordingly. All in all, this calls for framing this vehicle-to-infrastructure (V2I) interaction in the context of game theory (GT) [16], [17].

GT allows for modeling, analyzing, and optimizing the behavior of intelligent agents in smart systems such as VANETs, and can be used to design distributed approaches to network cooperation [18]. In this paper, we propose a game theoretic model for the V2I infrastructure taking place between a generic SV and an RSU, as depicted in Fig. 1.

We discuss a model for their interaction as strategic players, where the SV chooses a data rate and the RSU independently chooses a target for that rate, trying to have the SV staying below that value. This is modeled first as a static game of complete information, where we identify an equilibrium point that allows for some slack in data injection, yet keeping it below the target. Furthermore, we expand the game to a dynamic setup, given the highly time varying nature of VANETs. We consider a repeated game, where the time of the network connection between the RSU and the SV can be related to the discount factor adopted. This generates further possible investigations on collaboration strategies with an implicit agreement between the actors, which is relevant in the context of detecting misbehaviors by the mobile users.

The rest of this paper is organized as follows. In Section II, we review related work. Section III presents the system model and the game theoretic analysis. We show numerical results in Section IV and we conclude in Section V.

II. Related Work

Our setup may be related to a combination of [19] and [4]. The former is interested in capturing VANET interactions through GT, whereas the latter explores security concerns related to data injection, in particular for DoS attacks.

An extended analysis, which does not directly relate to VANETs but include the issue of mobility of players into account, is presented in [14]. In this paper, the behavior of a node entering a network is uncertain between regular or malicious, and this is accounted for through a Bayesian type.

In [5], congestion control in VANETs is investigated from a game theoretic perspective. Differently from our model, where the interaction takes place between an RSU and a single vehicle, in their analysis a non-cooperative game is introduced, where the vehicles act as selfish players. This is compared with the allocation obtained from the Karush-Kuhn-Tucker conditions, and a plain collision detection algorithm.

Another related approach, still considering a wider network scenario, is shown in [20]. While we focus on the interaction between a single RSU and an SV (multiple RSUs are actually present, but just as traffic redirection), that paper considers the choice of the RSU to connect to, in order to achieve a proper traffic balancing, also in consideration of the moving speeds of the vehicles. The solution proposed, based on evolutionary GT, can be seen as an extension for our approach.

A similar scenario to ours can also be found in [2]. Here, the authors consider an opportunistic offloading, also taking place between a SV and a RSU, and model it through GT. However, they consider an auction mechanism, and also pricing and utility shaping considerations are involved [21].

Finally, most of the investigations that employ GT to discuss injection in VANET involve malicious users, for example causing DoS attacks [6], [13], [19], [22]. While intentionally more general, our analysis can be certainly framed into this context. However, the critical point is about the detection of the malicious behavior beforehand, which would be required even for a simple static game of complete information, which assumes that the RSU is informed of the intent of the SV before an attack even takes place. We think that a proper way to frame these investigations is to explore possible strategies that can be chosen by the SVs, which in turn may be used for classification and prevention of misbehaviors [23].

III. System Model

We focus on the atomic interaction between an SV and an RSU. The former is interested in injecting data to a rate r. The latter is able to receive data to communicate with a server, and, if necessary, redirect the data flow to a neighboring RSU. To limit heavy data injection, the RSU sets up a target T. An exaggerated data injection beyond target T can be interpreted as an attempt to monopolize the available bandwidth, or jeopardize the network operation through a DoS attack. We denote with C the total bandwidth capacity of the RSU.

We can further assume that the RSU takes some special action if $r > T$. E.g., the data from the SV can be classified as a DoS attack, and therefore an alarm is raised or the flow is blocked. The purpose of the RSU is to choose T such that $P(r \leq T)$ is low. On the other hand, the SV aims at transmitting with an high rate, but without being blocked by the RSU. In this sense, the objective of the players converge (as long as the intent of the SV is non-malicious).

Moreover, for compliancy with the GT setup and the numerical analysis described later, the RSU is assumed to have complete knowledge of the capabilities of the network. The SV can further infer the probability of its flow to pass, drop or get redirected to another RSU based on a probabilistic framework [19]. Moreover, the capacity C available at the RSU is fixed and it is known to all the actors involved.

The development of the framework and its assumptions lead to a two player game between an SV and an RSU, which have different strategic choices as well as objectives and constraints that influence their strategies. The RSU's objective is to minimize the overall congestion and improve the traffic flow in the network. Conversely, the SV tries to maximize the amount of data that can be injected in the network. At first, we consider a static game where each player chooses to perform an action in order to maximize its payoff. This choice is done once and for all, and without consultation with the other player, i.e., the choice of r for the SV and of T for the RSU occurs without knowing the opponent's choice.

As evolution over time is important for our scenario, a further analysis investigates the repeated game version, discussing the role of the discount factor. For the numerical computations, the support enumeration algorithm [24] has been used to find the NE, as it enables finding all the equilibria of a game, even at the expense of an increased computational effort.

We need to define proper payoff functions of the players involved that are functions of both of their actions, i.e., r and T for the SV and the RSU, respectively. The choices that makes the problem worth of analysis are those where the payoff of an individual player jointly depends on both values [21].

The goal of the SV is to inject as much data as possible. Notably, this hold true regardless of the nature of this data, i.e., whether they are just regular data exchanged or even contain malicious attacks. A possible extension, left for future work, involves the study of this feature through a Bayesian type of the player [14]. Thus, the payoff of the SV is directly proportional to the rate, and we insert a direct proportionality also with term T, since a higher target allows to inject more data. Finally, we normalize the utility to the bandwidth C. So, the utility $u_{\mathrm{V}}(r,T)$ of the SV is computed as

$$u_{\mathrm{V}}(r,T) = \frac{T\,r}{C^2} \tag{1}$$

For the RSU, the payoff is inversely proportional to the rate injected, since the main goal is to avoid bandwidth saturation. At the same time, the RSU should also choose not too low a target, to ease the communications in the VANET. All of this is modeled via a quadratic function whose minimum is located at half of the capacity C. This results in [19]

$$u_{\mathrm{R}}(r,T) = 1 - \frac{T\,r}{C^2} - \left(\frac{T}{C} - \frac{1}{2}\right)^2 \tag{2}$$

A static game of complete information corresponds to both players looking for a local maximum of their utilities with full knowledge of the utilities of both players, and also being aware that the other player is seeking a maximization as well.

This can be extended to a further variation of the interaction between the SV and the RSU, namely, a repeated game played over multiple rounds, with the RSU and the SV interacting with each other every time, dynamically choosing

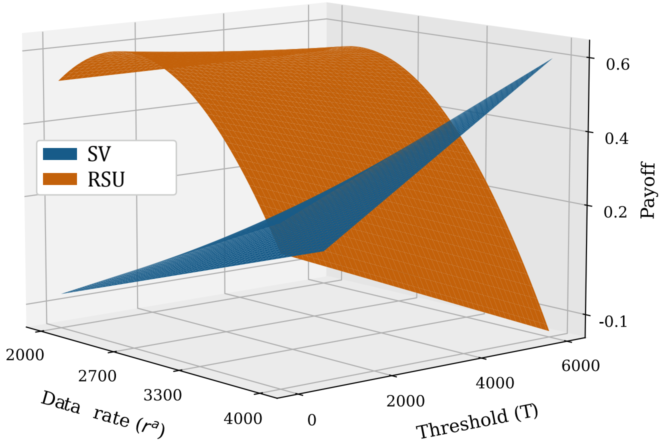

Fig. 2. Payoff surfaces.

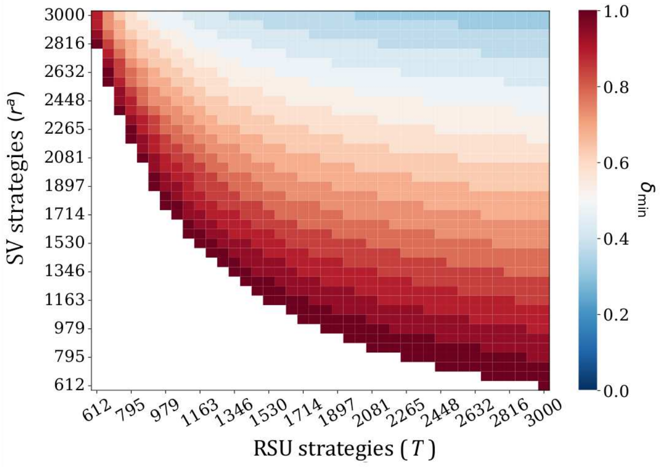

Fig. 3. Discount $\delta_{\min}$ as (r, T) vary.

T and r, respectively, using strategies that are contingent on past actions and outcomes. For example, the RSU can adjust the target based on the SV's response to its previous choices.

In this context, the setup of the discount factor $\delta \in (0,1)$ becomes key. In repeated games, the discount factor represents the importance of future payoffs relative to current payoffs, since players make decisions based not only on the current round but also on the potential future interactions. Thus, the discount factor is an exponential multiplicative weight of future payoffs against current payoffs [25].

A high discount factor places greater emphasis on future payoffs, whereas a low discount factor implies that players will be more focused on maximizing their immediate gains. For our problem at hand, since we involve a highly variable network dynamics, the discount factor can be put in relationship with the time that the SV is expected to stay in the network, after which the interaction ceases to exist. Thus, the desire for the SV to collaborate over present interaction may be a sign that it expects to stay connected for a long time. Conversely, a fast moving SV, or a malicious node injecting false data, may exhibit a very low discount factor [26], [27].

IV. Numerical Results

We considered the GT setup defined in the previous sections. Python package `nashpy` [28] is used for the numerical computation of NEs, through the support enumeration algorithm [24]. The capacity of the RSU C is set at 6000 Mbps [22]. Due to the computational power required to compute all the NEs involved given the size of the strategic spaces, we limited the numerical choices for the action parameters, still retaining enough complexity for them to be representative. The strategic space of the SV was discretized into an array of 8 equally-spaced values ranging from $\frac{C}{3}$ to $\frac{2C}{3}$. Similarly, for the RSU we set up an array of 8 equally-spaced values ranging from $C/8$ to C.

Fig. 2 shows the payoff obtained as functions of T and r. For the SV, it increases linearly in either T or r, when the other is kept constant. This happens, as the objective of the SV is to exchange the highest possible amount of data with the VANET, which becomes increasingly feasible as the RSU adjusts the target for traffic at higher levels. The NE yielded by the SE algorithm is unique, and it is ($r^* = 4000$, $T^* = 858$).

Because the target set by the RSU is lower than the rate that the SV chooses, the connection may be blocked to a point to which all the traffic generated by the SV is dropped and connection is lost. Throughout the study, it has been empirically proven that this consideration is not influenced by changes in the intervals selected, provided that the strategic space for the defender includes values lower than $C/2$. When this is not satisfied, the optimal strategy for the RSU becomes merely choosing the lowest possible target among those available.

Taking into account the results of the static game, where the NE is unique, we can extend the analysis by taking it as a stage of a repeated version over an infinite horizon. This new game is subject to discounting for the utilities to converge, so that a multiplicative discount factor $\delta \in (0,1)$ is defined and the utilities over the jth repetition are weighted through δ^j.

In a dynamic game where nodes join and leave a network, as is the case for a VANET, the numerical setup of δ can be connected to the expected duration of their stay in the system. Indeed, it is logical to assume that the SV is connected to the RSU for a variable time that implies it to play for an expected number of slots equal to $(1-\delta)^{-1}$ [25].

In this setting, the direction of analysis is assessing whether, with this type of GT framework, there exists another equilibrium that arises from players' agreement that deviates from the unique NE found for the static game. To do so, a strategic space is defined for both players so that they are both arrays of fifty even-spaced values (of r and T) between 0 and $\frac{C}{2} = 3000$. Furthermore, an array of twenty values for the discount factor $0 < \delta < 1$ is generated.

The development exploits the concept of the Carrot-and-stick approach [29]. In the first stage the RSU selects $T > T^*$. If the SV chooses any $r < r^\star$, then the agreement is kept. Otherwise, the SV is punished by selecting a new $T = \frac{T^*}{2}$ Next, it is required to check the condition that makes the cooperation to be feasible. This needs to be done for the SV only, as it is the one that can deviate, and translates into

$$u_{\mathrm{V}}(r,T) + \sum_{t=0}^{\infty} \delta^t > u_{\mathrm{V}}(r^\star,T) + u_{\mathrm{V}}\left(r^\star, \frac{T^*}{2}\right) \sum_{t=1}^{\infty} \delta^t \quad (3)$$

The results shown in Fig. 3 clarify that it is more likely to find an agreement as both r and T increase, meaning that

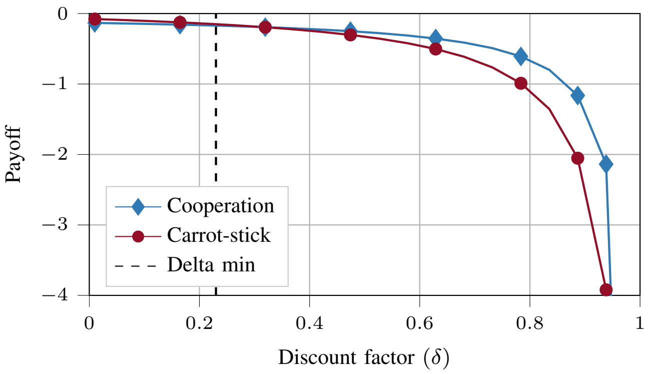

Fig. 4. SV payoff at ($r = 3000$, $T = 2020$) with $\delta_{\min}$.

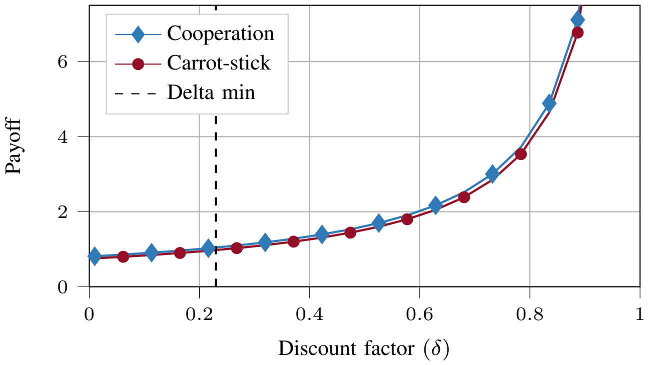

Fig. 5. RSU payoff at ($r = 3000$, $T = 2020$) with $\delta_{\min}$.

the discount factor has a smaller lower bound. Instead, for the combinations of low values for both r and T (bottom left corner in the plot), there is no δ giving cooperation, and the SV always deviates. The non-linear pattern of the minimum discount factor yields that the lowest $\delta_{\min} = 0.32$ occurs for $r = 3000$ Mbit/s (i.e. the maximum rate considered) and $T = 2020$ Mbit/s, as shown for the SV in Fig. 4 and for the RSU in Fig. 5. It is worth noting that this operating point, while still skewed since the SV attempts an overly aggressive allocation that may cause some of its data injections to be discarded, is more balanced than the previous static allocation.

Overall, repeated games are a promising approach to address data injection and additional security and authentication challenges faced by vehicular networks [15], enabling AVs to maintain safe and secure communication channels while navigating complex and dynamic traffic environments.

V. Conclusions

The use of GT to analyze data injection in VANETs can provide insights into the strategies and interactions of smart vehicles and the network, and help design more robust and secure VANET systems. Static games can be used to model the interactions between agents choosing their strategies simultaneously. This can provide insights into the NEs that are likely to arise in a one-shot interaction and lead to identify anomalies and attacks when the SV inject malicious data [14].

Dynamic games are an interesting extension, as they allow to keep movement of the SVs into account. This aspect is introduced through the discount factor [25], [26], modeling the expectations about the persisting presence of an SV in the VANET over future instants and can be combined with a possible Bayesian [12] or evolutionary analysis [20] about the malicious character that an SV may have, and the countermeasures for the network.

References

[1] R. Gasmi and M. Aliouat, “Vehicular Ad hoc NETworks versus Internet of vehicles – a comparative view,” in *Proc. ICNAS*, 2019.

[2] N. Cheng, N. Lu, N. Zhang, X. Zhang, X. S. Shen, and J. W. Mark, “Opportunistic WiFi offloading in vehicular environment: A game-theory approach,” *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 7, pp. 1944–1955, 2016.

[3] U. Michieli and L. Badia, “Game theoretic analysis of road user safety scenarios involving autonomous vehicles,” in *Proc. IEEE PIMRC*, 2018, pp. 1377–1381.

[4] H. Sedjelmaci, T. Bouali, and S. M. Senouci, “Detection and prevention from misbehaving intruders in vehicular networks,” in *Proc. IEEE Globecom*, 2014, pp. 39–44.

[5] H. M. Amer, C. Tsotskas, M. Hawes, P. Franco, and L. Mihaylova, “A game theory approach for congestion control in vehicular ad hoc networks,” in *Proc. IEEE SDF*, 2017.

[6] K. D. Thilak and A. Amuthan, “DoS attack on VANET routing and possible defending solutions - a survey,” in *Proc. ICICES*, 2016.

[7] S. Kaul, M. Gruteser, V. Rai, and J. Kenney, “Minimizing age of information in vehicular networks,” in *Proc. IEEE SAHCN*. IEEE, 2011, pp. 350–358.

[8] L. Badia, “Age of information from two strategic sources analyzed via game theory,” in *Proc. IEEE CAMAD*, 2021.

[9] O. Vikhrova, F. Chiariotti, B. Soret, G. Araniti, A. Molinaro, and P. Popovski, “Age of information in multi-hop networks with priorities,” in *Proc. IEEE Globecom*, 2020.

[10] L. Crosara and L. Badia, “A stochastic model for age-of-information efficiency in ARQ systems with energy harvesting,” in *Proc. Eur. Wirel.*, 2021.

[11] L. M. Feeney and P. Gunningberg, “Avoiding an IoT ’tragedy of the commons’,” in *Proc. ACM MobiSys*, 2018, pp. 495–497.

[12] L. Prospero, R. Costa, and L. Badia, “Resource sharing in the Internet of Things and selfish behaviors of the agents,” *IEEE Trans. Circuits Syst. II*, vol. 68, no. 12, pp. 3488–3492, Dec. 2021.

[13] Y. Kim, I. Kim, and C. Y. Shim, “A taxonomy for DoS attacks in VANET,” in *Proc. ISCIT*, 2014, pp. 26–27.

[14] A. V. Guglielmi and L. Badia, “Analysis of strategic security through game theory for mobile social networks,” in *Proc. IEEE CAMAD*, 2017.

[15] Z. Sun, Y. Liu, J. Wang, G. Li, C. Anil, K. Li, X. Guo, G. Sun, D. Tian, and D. Cao, “Applications of game theory in vehicular networks: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2660–2710, 2021.

[16] Z. Han, Y. Yang, W. Wang, L. Zhou, T. N. Nguyen, and C. Su, “Age efficient optimization in UAV-aided VEC network: A game theory viewpoint,” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 12, pp. 25 287–25 296, 2022.

[17] A. M. Mezher and M. Aguilar Igartua, “G-3MRP: A game-theoretical multimedia multimetric map-aware routing protocol for vehicular ad hoc networks,” *Comp. Netw.*, vol. 213, p. 109086, 2022.

[18] L. Badia, M. Levorato, F. Librino, and M. Zorzi, “Cooperation techniques for wireless systems from a networking perspective,” *IEEE Wireless Commun.*, vol. 17, no. 2, pp. 89–96, 2010.

[19] B. Kumar and B. Bhuyan, “Using game theory to model DoS attack and defence,” *Sādhanā*, vol. 44, no. 12, pp. 1–12, 2019.

[20] D. Wu, Y. Ling, H. Zhu, and J. Liang, “The RSU access problem based on evolutionary game theory for VANET,” *Int. J. Distrib. Sens. Netw.*, 2013.

[21] L. Badia and M. Zorzi, “On utility-based radio resource management with and without service guarantees,” in *Proc. ACM MSWiM*, 2004, pp. 244–251.

[22] M. Clavijo-Herrera, J. Banda-Almeida, and C. Iza, “Performance evaluation in misbehaviour detection techniques for DoS attacks in VANETs,” in *Proc. ACM PE-WASUN*, 2021, pp. 73–80.

[23] F. Ardizzon, L. Crosara, N. Laurenti, S. Tomasin, and N. Montini, “Authenticated timing protocol based on Galileo ACAS,” *Sensors*, vol. 22, no. 16, p. 6298, 2022.

[24] D. Avis, G. D. Rosenberg, R. Savani, and B. von Stengel, “Enumeration of Nash equilibria for two-player games,” *Econ. Th.*, vol. 42, pp. 9–37, 2010.

[25] L. Badia and A. Munari, “Discounted age of information for networks of constrained devices,” in *Proc. IEEE MedComNet*, 2022, pp. 43–46.

[26] M. Estiri and A. Khademzadeh, “A game-theoretical model for intrusion detection in wireless sensor networks,” in *Proc. CCECE*, 2010.

[27] A. Zancanaro, G. Cisotto, and L. Badia, “Modeling value of information in remote sensing from correlated sources,” in *Proc. IEEE MedComNet*, 2022, pp. 47–53.

[28] V. Knight and J. Campbell, “Nashpy: A Python library for the computation of Nash equilibria,” *J. Op. Source Softw.*, vol. 3, no. 30, 2018.

[29] X. Chen, T. Sasaki, Å. Brännström, and U. Dieckmann, “First carrot, then stick: how the adaptive hybridization of incentives promotes cooperation,” *J. Roy. Soc. Interf.*, vol. 12, no. 102, p. 20140935, 2015.