

Dynamic Team Formation for Mobile Edge Computing in IoT-Enabled Vehicular Networks.

Fabrizio Messina¹, Domenico Rosaci² and Giuseppe M. L. Sarné^{3,*}

¹*Department of Mathematics and Computer Science, University of Catania, Italy*

²*DIIES, university Mediterranea of Reggio Calabria, Via Graziella snc, 89122 Reggio Calabria, Italy*

³*Department of Psychology, University of Milan Bicocca, Piazza dell'Ateneo Nuovo, 1, 20126 Milan, Italy*

Abstract

We present a cooperative agent-based model to manage task allocation in networks of connected vehicles, which is based on the dynamic formation of temporary groups within a Mobile Edge Computing environment. The trust model integrated in this work combines the Quality of Service (QS) and the Quality of Results (QR) into a single reliability metric, based on a distributed reputation mechanism. The trust model is an updated version of a previous one, where we considered also the freshness of observations gives strong resilience and trustworthiness to the temporary groups. Simulation results show an improvement of this new version, in terms of the resilience of the framework, with respect to specific changes occurring in CVs' behaviors.

Keywords

Connected vehicles, Group Formation, Internet of Things, Mobile edge computing

1. Introduction

Modern vehicles are increasingly enriched with communication, sensing, and computational capabilities to interact with other vehicles, infrastructure elements—e.g., roads, cross lights, etc.—and edge resources. These Connected Vehicles (CVs) are essential to enable real-time smart mobility processes. In particular, CVs can exploit Mobile Edge Computing (MEC) infrastructures to dynamically allocate task offloading. In such a way, CVs transfer computational tasks to nearby edge servers significantly improve performance metrics in terms of latency, energy consumption, and processing efficiency [1, 2, 3] improving quality of service (QS) by minimizing dependence on onboard resources.

For Intelligent Transportation Systems (ITS), where tasks are distributed among connected vehicles, the creation of cooperative transient groups composed of heterogeneous nodes represents a key research area to improve performance, as well as for the Internet of Things (IoT) / Edge computing [4, 5, 6, 7, 8].

However, the creation of robust CV teams should consider the dynamic characteristics of mobility, heterogeneity in computational and communication capabilities, the absence of centralized coordination, and the lack of historical data. This means that decisions should not be based solely on functional similarities but also on factors such as reliability, past interactions, and experience, which can increase the effectiveness of the collaboration. Current trust and reputation mechanisms still have significant limitations when applied to dynamic urban environments. In particular, centralized solutions are vulnerable to single points of failure and characterized by poor scalability, while distributed approaches can be affected by simplified or static trust formulations. Moreover, existing frameworks are often limited in their ability to support adaptive and context-aware decisions when they emphasize objective QS indicators, while largely ignore subjective aspects such as the quality of results (QR). To address

WOA 2026: 27th Workshop "From Objects to Agents", June 17-19, 2026, Salerno, Italy

*Corresponding author.

[†]These authors contributed equally.

✉ messina@dmi.unict.it (F. Messina); domenico.rosaci@unirc.it (D. Rosaci); giuseppe.sarne@unimib.it (G. M. L. Sarné)

🌐 <https://web.dmi.unict.it/docenti/fabrizio.messina> (F. Messina); https://www.unirc.it/scheda_persona.php?id=696

(D. Rosaci); <https://www.unimib.it/giuseppe-maria-luigi-sarne> (G. M. L. Sarné)

🆔 0000-0002-3685-3879 (F. Messina); 0000-0002-9256-9995 (D. Rosaci); 0000-0003-3753-6020 (G. M. L. Sarné)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

these shortcomings, in [9] we presented a framework that combines QS and QR in a score, in a specific trust model, to enhance effective cooperative groups in a scenario enabling MEC.

To this purpose, the integration of CVs and MEC infrastructures allows to the process of large data volumes in real time –particularly useful in areas such as security and cooperative coordination–, perform processing closer to the data sources –reducing latency and the load on centralized cloud systems–, warranty scalability even under heavy traffic conditions, and implement collaboration and trust-based team-building strategies. This approach is characterized by a few relevant advantages, as described in [9], consisting of: (i) a decentralized trust-based strategy to build temporary CV groups in a dynamic way; (ii) each CV is modeled as an autonomous agent assessing trust, selecting partners, and participating to collective decisions; (iii) merging QS and QR into a single trust metric to capture both objective performance and subjective outcomes; (iv) providing a unified perspective to join both heterogeneous vehicles and various types of tasks and supporting those CVs that are the less equipped.

The previous approach in [9] was validated successfully through simulation-based experiments, although some limitations remain, namely: (i) scalability should also be confirmed in large-scale deployments and a high number of concurrent interactions; (ii) communication could represent a bottleneck, which requires that more efficient strategies be implemented; (iii) sharing performance and reliability information may expose to risks which require privacy-preserving techniques to be introduced; (iv) deceptive and malicious CVs' behaviors may compromise both security and effectiveness of the framework, which may require suitable strategies for detecting and mitigating such threats.

In this work, we deal with the latter aspect (iv), by introducing a new mechanism for computing trust scores, which is aimed to limit the risks related to deception or malicious behaviors of CVs. Specifically, we do not consider the whole CV history but only a limited number of recent observations, and to this aim, we have also introduced a parameter to weight their freshness: the more recent the observation, the more relevant is in computing the CV score. Besides demonstrating the effectiveness of the proposed method for computing CV reliability, the approach also addresses a limitation of the stateless strategy introduced in [9], whose overly strict criteria could rapidly exclude a substantial number of CVs from participation in team formation. To this aim, we have considered a simple scenario involving basic attacks and basic defense strategy, where there are no tangible advantages for malicious. The experimental results highlight that the framework is now less sensitive to such undesired events.

The rest of the paper is organized as follows. Section 2 introduces related work reviews. Sections 3 and 4 describe the proposed scenario and the updated trust model, respectively. The experiments are presented and discussed in Section 5 and, finally, Section 6 some conclusions are proposed.

2. Related work

Modern urban transportation networks make available wide forms of connectivity for exchanging data in real-time between various actors (e.g., CVs, personal devices, cloud platforms, route infrastructures, points of interest) to adapt mobility to dynamic traffic conditions, as well as users' interests by following the Cooperative, Connected, and Automated Mobility (CCAM) approach [9, 10]. Communication technologies can be based on *Vehicle-to-Vehicle* (V2V) [11], *Vehicle-to-Infrastructure* (V2I) [12], *Vehicular Ad-hoc Networks* (VANET) [13] or, in an inclusive way, V2X (Vehicle-to-Everything) [14]), and similarly for Wireless Sensor Networks (WSNs) [15]. However, to perform reliable CV interactions over such an communication overlay, it needs to estimate the trustworthiness of potential partners also relying on the adoption of trust and/or reputation systems (TRSs).

A large number of TRSs were proposed to meet specific peculiarities belonging to different contexts and architectures [16, 17, 18, 19, 20, 21, 22]. Effective trust measures require a TRS well fitting with the context domain [23, 24] –regardless of its centralized or distributed nature¹–, exploiting a significant number of trustworthy sources [25], and aggregating trust (i.e., reputation) score in a global (i.e., local)

¹Centralized approaches are simpler to implement as they maintain trust scores in a centralized repository; differently, distributed solutions are more resilient as they do not have a single point of failure, given that each CV locally calculates and updates the trust scores of other nodes.

way [26].

TRSs enable the prediction of future behaviors and contrast whitewash strategies, but refer to long-lived actors, drive new interactions based on past experiences, and spread trust/reputation measures and feedback throughout the community [27, 28]. Moreover, it is known that the use of trust/reputation measures helps form effective and more stable groups, providing them with reliable suggestions about a potential member and vice versa [29, 30, 31].

The exchange of information within (*temporary*²) CV teams may contribute to managing traffic issues and unexpected road events [33, 34]. A relevant concern for these teams is not-spreading false or malicious data and several studies have highlighted the effectiveness of TRSs in estimating the credibility of a source before its association with a team [35, 36]. TRSs typically leverage time-series data, cross-source correlations, and feedback from previous interactions with other CVs.

In this context [37, 38], a comprehensive overview of TRS systems in VANET-based systems has been provided, highlighting how these systems integrate –and sometimes replace– cryptographic techniques to mitigate threats posed by CVs that seek to cause disruptions or gain undue advantages.

The idea of temporary vehicle groups is exploited in TRIP [39], to identify unreliable participants, taking advantage of both data consistency and vehicle reputation, ensuring robustness against coordinated attacks and maintaining reliable information exchange even in highly dynamic environments. Clustering algorithms, often adopted to form groups in VANET scenarios increasing their stability, are analyzed in [40]. In this area, trust-driven clustering approaches have gained attention; for example, [41] introduces the Trust-based Stable Clustering (TSC) method, enhancing cluster stability, has been shown to outperform alternative solutions in experimental evaluations.

An usual problem in teams or platoon³ is the selection of a leader. In [42] a trust- and privacy-based recommendation scheme, called TPPR, which is resistant to some sophisticated attacks, selects an unmalicious platoon leader by adopting a truth discovery process based on the reputation of each CV. Another reputation-based mechanism to elect the platoon head can be found in [43], which adopts two subsystems, the former saves reputation values on a blockchain, and the second one adopts an incentive mechanism to promote participation to the elections.

Reputation systems can be profitably applied in the traffic management scenario. In [44] they allow only highly reputed CVs to spread traffic information for traffic congestion or accidents to mitigate the diffusion of inaccurate data. Similarly, a reputation system is adopted to set the transmission frequency of messages to rule overload on communication networks [45]. Also edge blockchain and computing technologies are combined with TRS in CVs environments. In particular, trust can be calculated in near real-time at the network edge, improving both latency and responsiveness [46], while the use of blockchain allows for the immutable storage of reputation records over time, adding transparency and resistance to tampering in the system, as in [43].

The issues of preserving privacy, integrity, confidentiality, security and accessibility of data and services generated by an IoT ecosystem by meeting user demands and consuming the lowest amount of resources are focused in [47, 48]. The study in [49] examines the interplay between MAC and IoT of a wireless-powered mobile edge computing system operating in a dynamic setting, featuring multiple Hybrid Access Points (HAPs). In this scenario, wireless devices harvest energy from the radio frequency signals transmitted by HAPs and subsequently either process their tasks locally or offload them to selected HAPs for edge execution.

In summary (see Table 1), the TRSs adopted in vehicular networks share several common traits. Centralized approaches, easier to implement, are limited by scalability constraints and single points of failure [16, 23], while decentralized ones, although more robust, often rely on weak or incomplete reliability indicators [35, 36, 41]. Existing proposals typically focus on objective QS metrics (e.g., latency and/or throughput) [39, 40] or on reputation and clustering mechanisms [44, 45, 40, 43], with limited efforts to integrate both objective and subjective aspects. In contrast, our framework computes reliability,

²The temporary nature relies on the CVs' behavior in entering or leaving a team mainly due to physical proximity, traffic evolution, interests, and reputation [32].

³Connected Automated Vehicles (CAVs) often move in a platoon, where multiple vehicles form an involuntary temporary group traveling in coordinated formation

based on QS and QR measures, combined with distributed reputation exploited in a decentralized team formation process within MEC-enabled vehicular networks. Its novelty compared to existing approaches and highlighted in Table 1.

Approach	Key features	Main limitations	Main differences with our work
Centralized trust and reputation models [16, 23]	Trust with a central manager.	Poor scalability; single point of failure; limited flexibility.	Fully distributed, improving robustness and scalability.
Decentralized and clustering-based solutions [35, 36, 41]	Distributed trust with clustering support.	Static indicators; clustering overhead.	Dynamic trust metric (QS, QR, reputation) without fixed clusters.
QS-centric approaches [39, 40]	Focus on performance metrics (e.g., latency, throughput).	Disregarding the outcomes quality; incomplete evaluation.	QS with QR combined for more reliable measures.
Reputation- or history-based mechanisms [44, 45, 40, 43, 42]	Trust based on past interactions and ratings.	Slow adaptation; requires long-term data.	Reputation integrated with real-time reliability for faster adaptation.
Proposed framework	Unified QS/QR reliability with distributed reputation for team formation.	–	Provides a scalable and adaptive multidimensional trust model.

Table 1

A comparison between some representative TRSs and the proposed framework in vehicular scenarios.

3. The proposed Scenario

We propose a scenario consisting of a fleet of autonomous CVs [50] operating within a transportation network (e.g., in an urban setting) equipped with a series of edge servers. CVs are typically equipped with multiple sensors and advanced communication units, which allows low-latency interactions in offloading tasks processes at the level of edge servers [51]. These edge resources provide substantial computational capacity, allowing faster processing, reduced response times, and improved overall system performance.

Edge servers accept requests from autonomous CVs, for example, when a CV needs to calculate an urban route. If this task is assigned to an edge server, the calculation can leverage on a large amount of data and computational resources with minimal processing latency.

The outcome of offloading tasks is valuable in terms of “*service quality*” and “*results quality*”. In other words, the former refers to processing delays, latency, and so on, while the second one depends on the quality of the generated recommendations, which in turn are linked to data available at the edge server generated them.

In such a scenario, a collaboration model, shown in Figure 1, assumes that CVs can cooperate by recommending strategies computed by offloading tasks on edge servers. In fact, in some situations, a vehicle may also handle a request on behalf of another, although this option can be constrained by security and privacy issues.⁴

More formally, this collaborative process relies on two key metrics:

⁴This modality may be restricted due to security and privacy concerns.

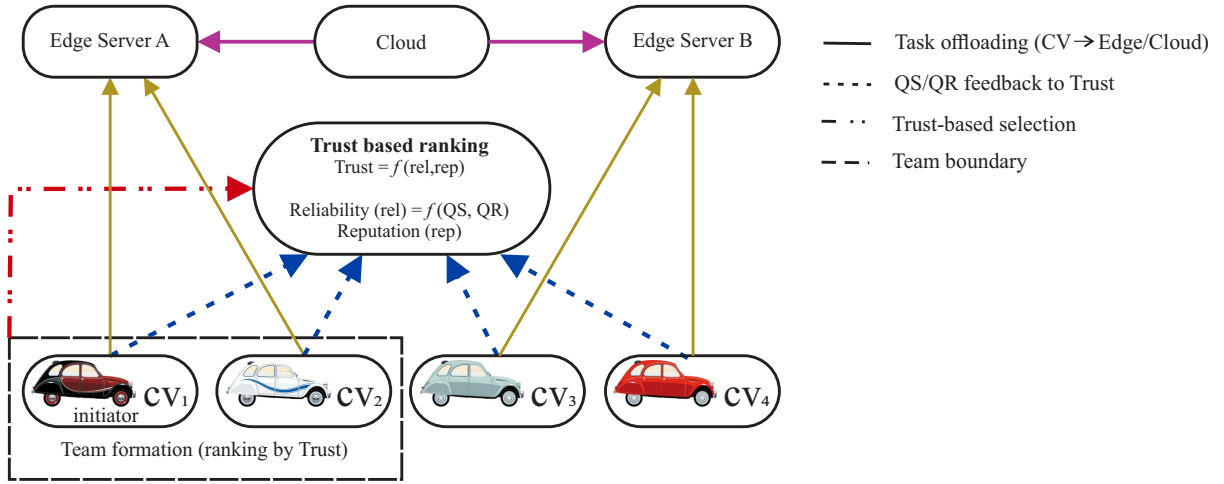


Figure 1: The proposed framework.

- *Quality of Service (QS)*: it reflects the satisfaction of non-functional requirements, such as latency, bandwidth usage, and processing time;
- *Quality of Results (QR)*: it measures how effectively a vehicle satisfies functional requirements for a given task category for its offloading strategy.

In a team, a CV has the opportunity to gain the trust of its peers and may interact to retrieve information for a given category of interest. As we will see in the next section, this will involve a given vehicle selecting the most appropriate suggestion in order to delegate a specific activity.

4. The Updated Trust Model

The trust model proposed in [9] is designed to represent in a single score the performance of a CV. The CV provides, within a MEC environment, offloading tasks that fall into a category (i.e., t) for free in a collaborative and benevolent perspective. In particular, qualitative measures, previously introduced, are mapped into quantitative ones.

In our framework CVs can exploit offloading tasks made available by other CVs. Such offloading tasks are denoted by both (i) a score representing the degree of satisfaction it meets with respect to latency and/or processing delay, denoted as *Quality of Service (QS)*, and (ii) a score representing the degree of satisfaction it meets with respect to its quality in terms of results, denoted as *Quality of Result (QR)*.

Moreover, let CV *reliability (rel)* be a performance score referring to the ability of a generic CV (i.e., x) to provide a given performance level in MEC offloading for a given category t . To compute a measure *rel*, we will consider that for the category t both *QS* and *QR* can be measured and combined linearly as in Equation 1:

$$rel_x^t = \gamma_t \cdot QS_x^t + (1 - \gamma_t) \cdot QR_x^t \quad (1)$$

where the system parameter γ_t^5 is a system parameter belonging to $[0, 1] \subset \mathbb{R}$ that in computing rel_x^t on s weights the relevance of *QS* with respect to *QR* as perceived by a CV that is client of x . Besides, note that (i) any CV agent can provide *QS* and *QR* measures, both ranging in $[0, 1] \subset \mathbb{R}$ –respectively, referring to processing delay, latency, etc.–, and the quality of the result of the offloading tasks, and (ii) for sake of simplicity we assume that *rel* is stateless measure, which does not directly consider the high variability of the urban mobility.

⁵Currently, γ_t is set in an empirical way making attention that Equation 1 balances the mutual relevance between objective network performance and the subjective outcome quality measures. This does not preclude the possibility that other adaptive mechanisms may be adopted in the future to calculate γ_t (i.e., infrastructure conditions, traffic conditions, or other requirements).

The *reputation* measure (*rep*), belonging to $[0, 1] \subset \mathbb{R}$, refers to the perception that the other members of a team T have for a given CV x about its reliability in terms of performance in a given category t . More formally, for T and for a given time, the reputation of x is computed as in Equation 2:

$$rep_x^t = \frac{\sum_{m=1}^{N_T-1} rel_{x,m}^s}{N_T - 1} \quad \forall \quad CV \in T \neq x \quad (2)$$

where N_T is the number of CVs in T .

Then we can compute the (stateless) measure of trust in the performance of x in the category t within T by combining *reputation* and *reliability* as in Equation 3:

$$trust_x^t = \epsilon \cdot rel_x^t + (1 - \epsilon) \cdot rep_x^t \quad (3)$$

where $\epsilon \in [0, 1] \subset \mathbb{R}$ is another parameter of the system, balancing the weight of *rel* with respect to *rep*.

Moreover, we have reasonably postulated that the increasing percentages of reliability *rel* and reputation *rep* with respect to the measure of *trust* are the same (i.e., $\frac{\Delta trust}{\Delta rel} = \frac{\Delta trust}{\Delta rep}$) and set the system parameters γ and ϵ , based on the specific domain, to optimize performance. Observe also that the choice of using a linear approach allows us to make clear the mapping between the single measures involved in Equations 1 and 3 and, at the same time, provides a linear complexity without compromising their capability to express the mutual dependencies involved in our framework.

A potential drawback of our framework is that a newcomer CV will not be provided with a trust score, and, therefore, it really risks to never be selected for temporary teams. To avoid this situation, the new arrival CV will be provided with a first trust score set to 0.5 – an intermediate value suitable to not penalize much the newcomer – until the first interaction, after which its trustworthiness will be determined as described above.

In the scenario presented in [9], CVs are assumed to be benevolent; however, this represents an idealized condition that rarely holds in real-world environments. Although malicious or improper behaviors typically arise when tangible benefits –generally economic– are involved, they must be considered also in our framework to limit the introduction of deceptive information in the system. Other undesired malicious behaviors, like collusion and similar, represent improbable events and can be ignored. Differently, note that in the case of real advantages, then further countermeasures should be introduced into the framework.

To improve resilience against such behaviors, this paper revises the modality with which CVs compute reliability measures. In detail, instead of adopting the stateless formulation used in [9], we introduce a short interaction history to capture recent behavior. From a practical perspective, each CV is treated as a long-lived entity, in line with the assumptions in [27]. Given the temporary nature of the groups, this history is intentionally limited to a small horizon (e.g., 3–5 interactions).

Furthermore, in incentivizing correct behaviors, the more recent the observation, the more relevant contribution in calculating the CV reliability measure. Formally, the reliability of each CV will be computed as follows:

$$rel_x^t = \frac{\sum_{k=1}^h \sigma_k \cdot rel_k^t}{\sum_{k=1}^h \sigma_k} \quad (4)$$

where h is the maximum number of reliability measures rel^t –having the form described in Equation 1– considered in computing the updated reliability measure.

In other words, the horizon adopted to calculate the new reliability measures varies from 0, when there are no previous interactions with a given CV, to h . The weight σ accounts for the freshness of rel^t and is defined as $\sigma = 1/(1 + h - k)$, where $k = h$ corresponds to the most recent observation and $k = 0$ to the oldest of the observations considered h . Consider that when a CV has fewer than h prior interactions (e.g., at initialization), in Equation 4 the value of k is set to the number of available observations.

Moreover, to penalize improper behavior and make it harder to restore reliability after misconduct, when $rel^t < 0.5$ the parameter σ is set to 1, thereby enforcing a stronger incentive toward correct behavior.

4.1. Temporary teams formation algorithm

The updated trust model only marginally affects the original temporary teams formation algorithm, which here is summarized.

The formation of teams allows to each CV of requiring to the other CV members of the same team to support, at any CV, for assigning and executing a given offloading task at the edge. Note that the original proposal for such a cooperation relies only on the benevolence of the other CVs, while the updated trust model provides further support in the selection of the best performing CVs for a given category of tasks.

This algorithm supports the building of CV teams by selecting the most trustworthy CV, based on the computed trust scores, to perform a collaborative task. The main characteristics of this algorithm can be summarized in: (i) a fully decentralized architecture; (ii) adaptive traffic conditions and CVs' behaviors and capabilities; (iii) providing support less equipped CV.

In detail, at time t_0 , when a CV –denoted as a_0 – initiates the team formation process for a group A , the selection procedure begins by identifying the most trustworthy vehicles based on their current trust rating. Now suppose that within the communication range of a_0 there are at least k candidate CVs, from which n are selected to form the team, with $n \leq k + 1$ and $A = \{a_0, a_1, \dots, a_n\}$.

The team formation algorithm, shown in Figure 2, consists of five stages, namely:

1. **Starting** - a_0 decides to form a team to perform a task for the category t . In the communication range of a_0 there are at least k CVs that can receive its broadcast message, which consists of the tuple $\langle mx, mn, T, trust_{min} \rangle$, where: (i) mx is the maximum number of CV in A , with $mx \leq k$; (ii) mn is the minimum number of CV in A , with $mn \geq 1$; (iii) T is a time threshold that CVs have to answer to a_0 ; (iv) $trust_{min}$ the minimum trust score value required from a_0 to enter in A .
2. **Request** - the a_0 message is sent to the k CVs belonging to its communication range to collect: (i) their availability to join with A , and (ii) the most recent reliability score (if any) for each CV j –one agent of the $k - 1$ potential members of A – i.e., $rel_{j,m}^t$. In other words, a_0 gathers the information required to compute the reputation of each of the k candidate vehicles and, consequently, their trust values (see Equations. 2, 3, and 4).
3. **Answer** - after that, a potential member of A received the a_0 's request if: (i) it does not respond to the a_0 's request, which means that it does not want to join with A ; (ii) it computes the values of rel_j^t , $\forall j \neq 0, j$ and sent them to a_0 .
4. **Select** - once the time threshold T elapsed and a_0 received at least z responses, with $z \leq k$, then a_0 will compute the trust scores $trust_j$, with $j = 1, \dots, z$ based on the reliability values sent by the other potential members of A . Agents and their respective trust scores greater than $trust_{min}$, will be inserted in a list L of agents eligible for the temporary team A . Finally, L will be ordered in an increasing way according to the trust values.
5. **Forming** - to form A , a_0 will select $\min(mx, length(L)) \geq mn$ CVs, having the highest trust scores, from L and an acceptance message will be sent to them from a_0 .

The formation of the temporary team, executed in a fully distributed manner, ends.

5. Experiments

In this section, we present the experiments that were performed to evaluate our approach. We have simulated the cooperation of the connected vehicles, implementing the algorithm described in the previous Section 4. Our goal is to verify if the updated trust model improves the performance of the original algorithm in accurately identifying and excluding from the formation of temporary teams only

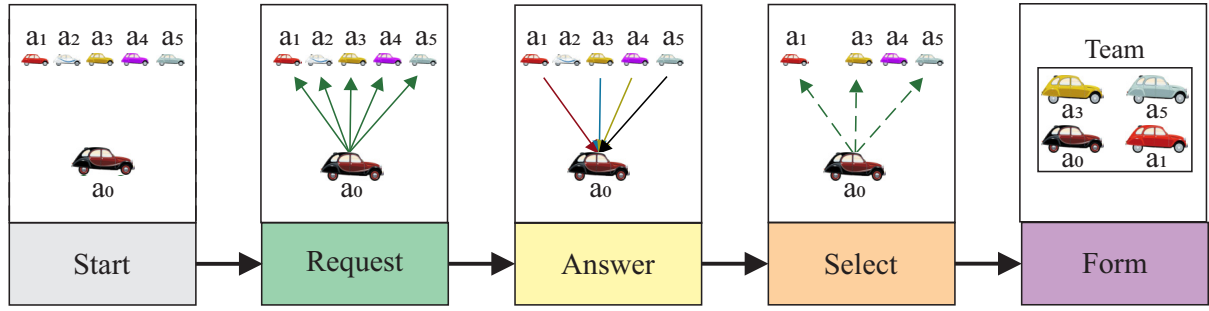


Figure 2: Temporary Team formation

those CVs that are engaged in improper or malicious behaviors, without inadvertently penalizing honest and well-behaved CVs as a side effect. This latter issue is similar to the one present in the well-known EigenTrust model [52] and addressed in [53, 54].

Similarly to [9], simulations were performed using the same software –a script in the Octave language [55] to guaranty a correct comparison between experiments–, and the same parameters and setting previously adopted, while the horizon h , required in the calculation of the reliability in the updated trust model, was set to 3 and the percentage of malicious CVs was set to 5%. The complete simulation setting adopted in the experiments is reported in Table 2.

Parameter	Value/range
Simulated time	60 hours
CVs	1000
No. of task category	5
Max no. of CVs per group	50
Horizon h	3
Malicious percentage	5%
$Rel^{(0)}$	0.5
$Rep^{(0)}$	0.5
γ	0.5
ϵ	0.4
CV requests per hours	Poisson distribution, $\lambda = 20$
QS	Normal Distribution
QR	Normal Distribution
QS $\{(v, \sigma^2)\}$	$(v, \sigma^2) = \{p_1 : (0.9, 1.0), p_2 : (0.7, 1.0), p_3 : (0.5, 2.0)\}$
QR $\{(v, \sigma^2)\}$	$(v, \sigma^2) = \{p_1 : (0.9, 1.0), p_2 : (0.7, 1.0), p_3 : (0.5, 2.0)\}$
Ratio of $p_1/p_2/p_3$ CVs in the simulated scenario	$\frac{1}{3} / \frac{1}{3} / \frac{1}{3}$

Table 2
Simulation parameters

We recall that the experiments simulated a time period of 60 hours, involving 1000 CVs, for 5 task categories⁶ –consistently with prior studies [56]–, a maximum of 50 CVs per group, and the parameters γ and ϵ , after preliminary tests, were set respectively to 0.5 and 0.4 for assigning equal relevance to QR with respect to QS in the calculation of the reliability measure and to weight reputation with respect to reliability in the calculation of the trust measure –in line with common choices adopted in trust modeling [18, 19, 20]. The value of 0.5 for both the initial reliability ($rel^{(0)}$) and the initial reputation ($rep^{(0)}$) for newcomers is a compromise that allows them operability and hinders whitewashing strategies, as specified in Section 4.

Moreover, the simulated dataset is consistent with a metropolitan traffic scenario, the heterogeneous

⁶For our purpose, since team formation is always related to a specific category of task, we have analyzed the experimental results for a single category of task; indeed, as expected, the results for all categories of task were very similar.

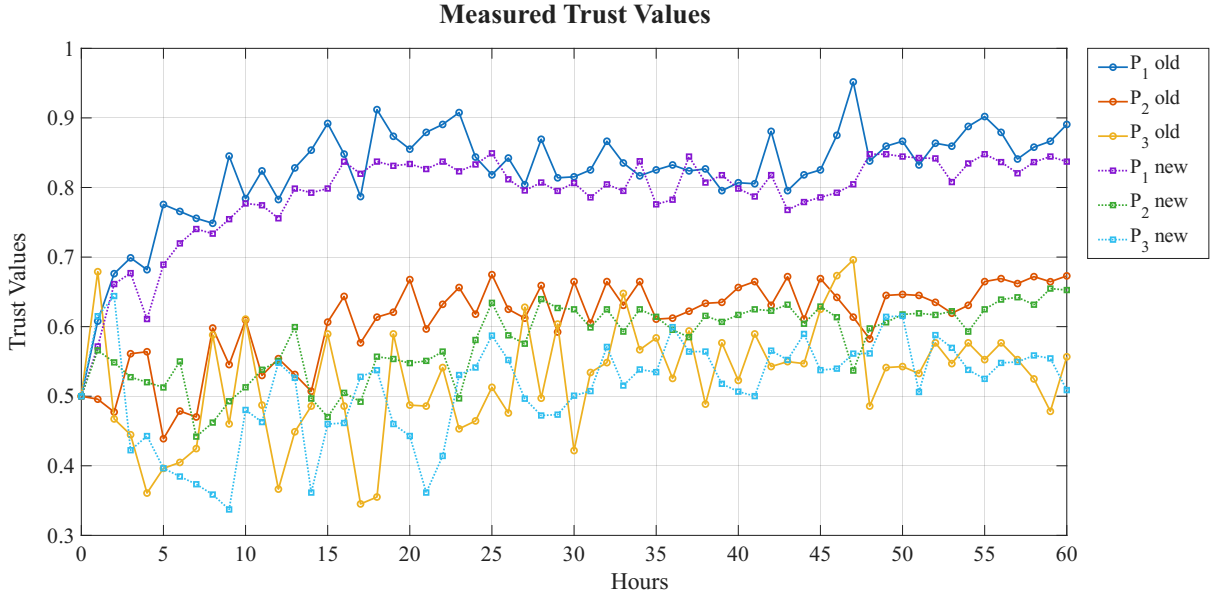


Figure 3: Measured trust values for the profile

vehicle profiles ensure both variability in task demands and interaction opportunities, while the number of CVs and the simulation time ensure that the dynamics of temporary team formation can be observed for an adequate time. The average number of task requests per hour was modeled by adopting a Poisson distribution with λ set to 20, while the QS and QR distributions were parameterized by a normal distribution, with ν and σ^2 set as in Table 2, to form vehicle profiles p_1 , p_2 and p_3 , characterizing high, medium and low performance and variability, respectively. This abstraction ensures that the trust model clearly captures system heterogeneity: vehicles with stronger MEC capabilities consistently achieve higher QS and QR scores, thereby attaining higher trust values and being preferentially selected during team formation.

Let us now provide some considerations on the choice of the parameter h , which should be set according to the complexity of the simulated scenario, balancing effectiveness and computational cost. In this regard, the scenario under study is rather basic, does not involve tangible benefits (e.g., economic interests), and is of limited scale (e.g., network size, number of CVs). These aspects do not currently justify the adoption of more sophisticated trust models for CVs or the use of large values of h . It is also worth noting that for values of h lower than 3 the effectiveness of the model decreases due to the presence of many false positives, while larger values of h become appropriate in more complex scenarios.

The urban transportation network that underlies the simulated mobility scenario is constructed using a modular design derived from [57]. In detail, it consists of a 3×3 grid exploiting squared symmetric “module” and simulating only two way roads, to avoid variability for road topologies or traffic traces. The geographical positions of CVs were initially randomly distributed in the urban area, and their positions were revalued minute-by-minute according to a bounded speed range and random direction changes such as [9], while their mobility was simulated using the algorithm presented in [58]. Finally, to simulate variability in task demands and interaction opportunities, vehicle profiles were assumed to be heterogeneous and belonging to five typologies.

Figure 3 reports the evolution of the average trust values measured during the 60-hour simulation for the three profiles p_1 , p_2 , and p_3 and for both original (i.e., old) and updated (i.e., new) trust models. It is possible to note that, in terms of variance, the results of the updated trust model are slightly improved by $-0.093 \div 0.16$ relative to the previous one. Differently, from a quantitative viewpoint, the average trust values are slightly lower for the updated trust model with respect to the first one and over the simulation hours the results of the two trust models tend to converge. This should depend on the higher precision of the new trust model in recognizing malicious CVs, leading to their progressive exclusion

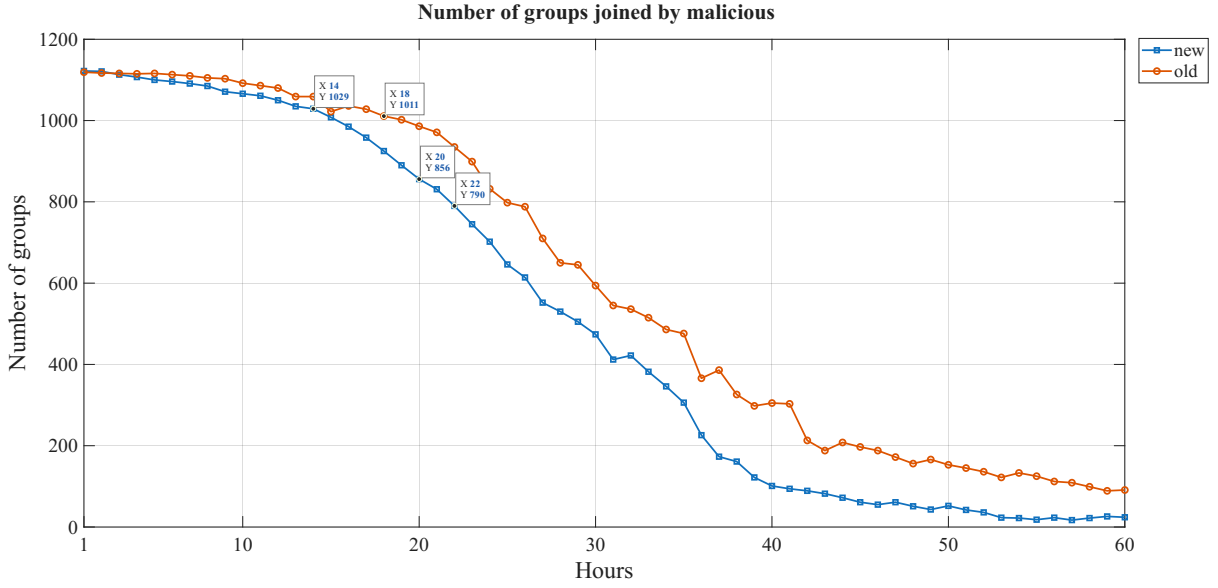


Figure 4: Number of groups joined by malicious along the simulation

from team formation processes more quickly than the other trust model. These results are in line with our expectations.

We also examined the number of malicious CVs joined with groups adopting the two trust models. Simulations considered both the high dynamicity of urban traffic with temporary teams having a short time live. Results are reported in Figure 4. Their analysis shows that, on average, the number of teams involving malicious CVs –after an initial phase, similar for both models and attributable to knowledge spreading– is lower when using the updated trust model. Over time, the baseline model tends to approach similar performance; however, the updated model reaches the target of identifying malicious CVs more rapidly and consistently.

In summary, the experimental results confirm our expectations, demonstrating the greater effectiveness of the updated trust model in mitigating the impact of CVs that exhibit malicious or incorrect behavior, compared to the model presented in [9].

Moreover, consider that an appropriate horizon (see Eq. 4) in calculating reliability introduces only a negligible overhead in terms of computational and memory requirements for CVs when managing the updated trust model.

6. Conclusions

The collaborative framework presented in [9] is focused on supporting by offloading tasks required by CVs, participating in temporary CV teams dynamically formed in a mobility scenario and executed in a MEC environment. Such a framework is characterized from a trust model and a decentralized algorithm, which is designed to form temporary team whose members are selected based on the CVs' trust scores. In particular, the trust model takes into account CVs' reliability –calculated by evaluating both Quality of Service and Quality of Results measures– and reputation scores.

In [9] a fundamental assumption is that CV are always benevolent, although this is justifiable from both the absence of real individual benefits and the high dynamicity that usually characterizes the considered scenario, which is also the reason underlying the temporary nature of teams. However, improper or malicious behaviors are always possible in the scenario described above. To this aim, in this paper an updating of the trust model devoted to provide the system with a greater capability to better characterize not only low-performing vehicles but also those untrustworthy. This update introduces only a slight and not negligible increase in both computational and memory complexity but offers better performance compared to [9].

Experiments carried out adopting the same modalities and setting as in [9], have validated this new version of the trust model only considering basic attacks, basic defense strategy, and no tangible advantages for malicious. The future evolution of this framework will be addressed to introduce, for instance, mobility patterns, energy availability, dynamic task priorities, and new forms of traffic management make possible from the presence of CVs and MEC infrastructures. Moreover, such new scenarios may require integration of security mechanisms and other countermeasures to protect the trust framework against sophisticated malicious and manipulation behaviors.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] B. Mao, J. Qiu, N. Kato, On an intelligent task offloading model to jointly optimize latency and energy for electric connected vehicles, *IEEE Transactions on Vehicular Technology* 73 (2023) 6024–6028.
- [2] O. Akyıldız, F. Y. Okay, İ. Kök, S. Özdemir, Road to efficiency: Mobility-driven joint task offloading and resource utilization protocol for connected vehicle networks, *Future Generation Computer Systems* 156 (2024) 157–167.
- [3] L. Liu, M. Zhao, M. Yu, M. A. Jan, D. Lan, A. Taherkordi, Mobility-aware multi-hop task offloading for autonomous driving in vehicular edge computing and networks, *IEEE Transactions on Intelligent Transportation Systems* 24 (2022) 2169–2182.
- [4] G. Fortino, C. Savaglio, M. Zhou, Toward opportunistic services for the industrial internet of things, in: *13th IEEE Conf. on Automation Science and Engineering (CASE)*, IEEE, 2017, pp. 825–830.
- [5] G. Fortino, L. Fotia, F. Messina, D. Rosaci, G. M. L. Sarné, Trusted object framework (TOF): a clustering reputation-based approach using edge computing for sharing resources among iot smart objects, *Computers & Electrical Engineering* 96 (2021) 107568.
- [6] G. Fortino, F. Messina, D. Rosaci, G. M. L. Sarné, Using trust measures to optimize neighbor selection for smart blockchain networks in iot, *IEEE Internet of Things Journal* 10 (2023) 21168–21175.
- [7] D. Carnemolla, F. Messina, F. F. Santoro, C. Santoro, An ecosystem to develop multi-agent systems in real-world iot applications, *Software: Practice and Experience* 56 (2026) 339–356.
- [8] F. Messina, D. Rosaci, A cooperative distributed model to evaluate and optimize task offloading in mobile edge computing, *Computer Communications* (2026) 108403.
- [9] F. Messina, D. Rosaci, G. M. L. Sarné, Forming teams of smart objects to support mobile edge computing for iot-based connected vehicles, *Applied Sciences* 15 (2025) 9483.
- [10] E. Y. Bejarbaneh, H. Du, F. Naghdy, Exploring shared perception and control in cooperative vehicle-intersection systems: A review, *IEEE transactions on intelligent transportation systems* 25 (2024) 15247–15272.
- [11] F. Zhang, G. Wang, Context-aware resource allocation for vehicle-to-vehicle communications in cellular-v2x networks, *Ad Hoc Networks* 163 (2024) 103582.
- [12] C. Zhao, D. Ding, Y. Shi, Y. Ji, Y. Du, Graph matching-based spatiotemporal calibration of roadside sensors in cooperative vehicle-infrastructure systems, *IEEE Transactions on Intelligent Transportation Systems* 25 (2024) 9281–9295.
- [13] Y. Asabe, E. Javanmardi, J. Nakazato, M. Tsukada, H. Esaki, Autowarev2x: Reliable v2x communication and collective perception for autonomous driving, in: *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, IEEE, 2023, pp. 1–7.
- [14] A. Hozouri, A. Mirzaei, S. RazaghZadeh, D. Yousefi, An overview of vanet vehicular networks, *arXiv preprint arXiv:2309.06555* (2023).
- [15] K. Nellore, G. P. Hancke, A survey on urban traffic management system using wireless sensor networks, *Sensors* 16 (2016) 157.

- [16] R. Govindaraj, P. Govindaraj, S. Chowdhury, et al., A review on various applications of reputation based trust management., *International Journal of Interactive Mobile Technologies* 15 (2021) 87–102.
- [17] A. Comi, L. Fotia, F. Messina, G. Pappalardo, D. Rosaci, G. M. L. Sarné, Forming homogeneous classes for e-learning in a social network scenario, in: *Intelligent Distributed Computing IX: Proc. of the 9th Int. Symposium on-IDC'2015*, Guimarães, Portugal, October 2015, Springer, 2015, pp. 131–141.
- [18] H. L. J. Ting, X. Kang, T. Li, H. Wang, C.-K. Chu, On the trust and trust modeling for the future fully-connected digital world: A comprehensive study, *IEEE Access* 9 (2021) 106743–106783.
- [19] D. D. S. Braga, M. Niemann, B. Hellingrath, F. B. D. L. Neto, Survey on computational trust and reputation models, *ACM Computing Surveys (CSUR)* 51 (2018) 1–40.
- [20] A. Comi, L. Fotia, F. Messina, D. Rosaci, G. M. L. Sarné, A partnership-based approach to improve qos on federated computing infrastructures, *Information Sciences* 367 (2016) 246–258.
- [21] J. Heidemann, M. Klier, F. Probst, Online social networks: A survey of a global phenomenon, *Computer Networks* 56 (2012) 3866–3878.
- [22] D. Rosaci, G. M. L. Sarné, S. Garruzzo, Integrating trust measures in multiagent systems, *International Journal of Intelligent Systems* 27 (2012) 1–15.
- [23] G. Fortino, L. Fotia, F. Messina, D. Rosaci, G. M. L. Sarné, Trust and reputation in the internet of things: state-of-the-art and research challenges, *IEEE Access* 8 (2020) 60117–60125.
- [24] G. Fortino, L. Fotia, F. Messina, D. Rosaci, G. M. L. Sarné, A social edge-based iot framework using reputation-based clustering for enhancing competitiveness, *IEEE Transactions on Computational Social Systems* 10 (2022) 2051–2060.
- [25] T. Huynh, N. Jennings, N. Shadbolt, An integrated trust and reputation model for open multi-agent systems, *Autonomous Agents and Multi-Agent Systems* 13 (2006) 119–154.
- [26] Y. Kim, H. Song, Strategies for predicting local trust based on trust propagation in social networks, *Knowledge-Based Systems* 24 (2011) 1360–1371.
- [27] P. Resnick, R. Zeckhauser, F. E., K. Kuwabara, Reputation systems, *Communication of ACM* 43 (2000) 45–48.
- [28] A. Comi, L. Fotia, F. Messina, D. Rosaci, G. M. L. Sarné, A qos-aware, trust-based aggregation model for grid federations, in: *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, Springer, 2014, pp. 277–294.
- [29] A. Comi, L. Fotia, F. Messina, D. Rosaci, G. M. L. Sarné, Grouptrust: Finding trust-based group structures in social communities, in: *International Symposium on Intelligent and Distributed Computing*, Springer, 2016, pp. 143–152.
- [30] P. De Meo, E. Ferrara, D. Rosaci, G. M. L. Sarné, Trust and compactness in social network groups, *ACM Transactions on Cybernetics* 45 (2015) 205–216.
- [31] P. De Meo, F. Messina, M. N. Postorino, D. Rosaci, G. M. L. Sarné, A reputation framework to share resources into iot-based environments, in: *2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC)*, IEEE, 2017, pp. 513–518.
- [32] G. Zai, S. Wu, Y. Zhang, Z. Tian, Trust management of vehicle internet based on non-cooperative game, in: *Proceedings of the 2023 5th International Conference on Internet of Things, Automation and Artificial Intelligence*, 2023, pp. 54–58.
- [33] Z. Deng, K. Yang, W. Shen, Y. Shi, Cooperative platoon formation of connected and autonomous vehicles: Toward efficient merging coordination at unsignalized intersections, *IEEE Transactions on Intelligent Transportation Systems* 24 (2023) 5625–5639.
- [34] Z. H. Khatkhat, J. Rios-Torres, M. D. Fontaine, Impact of communications delay on safety and stability of connected and automated vehicle platoons: Empirical evidence from experimental data, *IEEE access* 11 (2023) 128549–128568.
- [35] G. Fornaro, M. Törngren, Improving road traffic safety and performance—barriers and directions towards cooperative automated vehicles, in: *International Conference on Computer Safety, Reliability, and Security*, Springer, 2023, pp. 283–294.
- [36] M. H. Junejo, A. A.-H. B. Ab Rahman, R. A. Shaikh, K. M. Yusof, S. Sadih, Trust model for

- reliable grouping-based communications in vehicular ad-hoc networks, *IEEE Access* 11 (2023) 124584–124596.
- [37] I. Souissi, N. B. Azzouna, T. Berradia, Trust management in vehicular ad hoc networks: a survey, *International Journal of Ad Hoc and Ubiquitous Computing* 31 (2019) 230–243.
 - [38] H. Amari, Z. Abou El Houda, L. Khoukhi, L. H. Belguith, Trust management in vehicular ad-hoc networks: Extensive survey, *IEEE Access* 11 (2023) 47659–47680.
 - [39] F. G. Mármol, G. M. Pérez, Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks, *Journal of network and computer applications* 35 (2012) 934–941.
 - [40] M. Ren, J. Zhang, L. Khoukhi, H. Labiod, V. Vèque, A review of clustering algorithms in vanets, *Annals of Telecommunications* 76 (2021) 581–603.
 - [41] D. Singh, A. K. Maurya, Ranvijay, R. S. Yadav, A trust-based clustering approach to form stable clusters in vehicular ad hoc networks, *Journal of Ambient Intelligence and Humanized Computing* 14 (2023) 16209–16228.
 - [42] C. Zhang, L. Zhu, C. Xu, K. Sharif, K. Ding, X. Liu, X. Du, M. Guizani, Tppr: A trust-based and privacy-preserving platoon recommendation scheme in vanet, *IEEE Transactions on Services Computing* 15 (2019) 806–818.
 - [43] Z. Ying, M. Ma, Z. Zhao, X. Liu, J. Ma, A reputation-based leader election scheme for opportunistic autonomous vehicle platoon, *IEEE Transactions on Vehicular Technology* 71 (2021) 3519–3532.
 - [44] H. Che, Y. Duan, C. Li, L. Yu, On trust management in vehicular ad hoc networks: A comprehensive review, *Frontiers in the Internet of Things* 1 (2022) 1–29.
 - [45] V. E. F. Borges, Á. Sobrinho, D. F. Santos, A. Perkusich, A self-sovereign identity-based authentication and reputation protocol for iov applications, *IEEE Access* (2025) 105693–105711.
 - [46] M. Hua, X. Qi, D. Chen, K. Jiang, Z. E. Liu, H. Sun, Q. Zhou, H. Xu, Multi-agent reinforcement learning for connected and automated vehicles control: Recent advancements and future prospects, *IEEE Transactions on Automation Science and Engineering* (2025) 16266 – 16286.
 - [47] I. Ullah, I. Khalil, X. Bai, S. Garg, G. Kaddoum, M. S. Hossain, An ensemble-based hybrid model for the detection of attacks in the internet of vehicular things, *IEEE Transactions on Intelligent Transportation Systems* 26 (2025) 17914–17927.
 - [48] I. Ullah, A. Noor, S. Nazir, F. Ali, Y. Y. Ghadi, N. Aslam, Protecting iot devices from security attacks using effective decision-making strategy of appropriate features, *The Journal of Supercomputing* 80 (2024) 5870–5899.
 - [49] X. Liu, A. Chen, K. Zheng, K. Chi, B. Yang, T. Taleb, Distributed computation offloading for energy provision minimization in wp-mec networks with multiple haps, *IEEE Transactions on Mobile Computing* 24 (2024) 2673–2689.
 - [50] G. Abdelkader, K. Elgazzar, A. Khamis, Connected vehicles: Technology review, state of the art, challenges and opportunities, *Sensors* 21 (2021) 7712.
 - [51] M. J. Alam, M. R. Hossain, S. Azad, R. Chugh, An overview of lte/lte-a heterogeneous networks for 5g and beyond, *Transactions on Emerging Telecommunications Technologies* 34 (2023) e4806.
 - [52] S. D. Kamvar, M. T. Schlosser, H. Garcia-Molina, The Eigentrust Algorithm for Reputation Management in P2P Networks., in: *WWW '03: Proc. of the 12th International Conf. on World Wide Web.*, ACM Press, New York, NY, USA., 2003, pp. 640–651.
 - [53] M. Cotronei, S. Giuffrè, A. Marcianò, D. Rosaci, G. M. L. Sarné, Using trust and reputation for detecting groups of colluded agents in social networks, *IEEE Access* 13 (2024) 1511–1521.
 - [54] M. Cotronei, S. Giuffrè, A. Marcianò, D. Rosaci, G. M. L. Sarné, Improving the effectiveness of eigentrust in computing the reputation of social agents in presence of collusion, *International Journal of Neural Systems* 34 (2024) 2350063–1 – 2350063–16.
 - [55] GNU Octave, <http://www.gnu.org/software/octave/> (2026).
 - [56] J. Lee, B. Park, Development and evaluation of a cooperative vehicle intersection control algorithm under the connected vehicles environment, *IEEE transactions on intelligent transportation systems* 13 (2012) 81–90.
 - [57] M. N. Postorino, G. M. L. Sarné, Reinventing mobility paradigms: Flying car scenarios and challenges for urban mobility, *Sustainability* 12 (2020) 3581.

- [58] M. N. Postorino, G. M. L. Sarné, A reputation-based framework to support dynamic car-pooling, *Intelligenza Artificiale* 14 (2020) 89–102.