

# Formal Methods to Verify and Ensure Self-Coordination Abilities in the Internet of Vehicles

Vahid Yazdanpanah\*, Enrico H. Gerding, and Sebastian Stein

Agents, Interaction and Complexity Research Group,  
University of Southampton, Southampton, United Kingdom  
v.yazdanpanah@soton.ac.uk, {eg,ss2}@ecs.soton.ac.uk

**Abstract.** The emerging Internet of Vehicles (IoV) is a distributed multiagent network that utilises the potentials for *collaboration of vehicles* with the aim to improve the reliability and safety of transportation and logistic systems. IoV systems require operational methods to reason about the capacity of the involved (human and artificial) agents to form strategically *capable* coalitions as a means to ensure safety. In this work, we (1) develop a logic-based machinery to represent and reason about strategic abilities in IoV systems, (2) provide a process to verify whether a given IoV system is capable to safely self-coordinate, and (3) introduce a mechanism to ensure such an ability in a *temporal*, *strategic*, and *normative* setting.

**Keywords:** Multiagent Systems · Computational Logic · Smart Logistics · Self-Coordination · Internet of Vehicles · Formal Reasoning.

## 1 Introduction

With the increasing need for safe transportation, the rapid development of communication technologies, and the ongoing race for developing autonomous vehicles, the Internet of Vehicles (IoV) is emerging as one of the hottest topics in the AI research community with high relevance and potential impact in the transportation industry. The IoV is a distributed multiagent network that utilises the potentials for *collaboration of vehicles* (via coalition forming, information sharing, or collaborative task execution) with the overarching aim to improve the reliability and safety of transportation and logistic systems [12, 9]. Realising

---

\* Corresponding Author: v.yazdanpanah@soton.ac.uk

such a form of collaboration can be reduced to classic optimisation problems with standard solution concepts when we deal with obedient non-autonomous vehicles (as tools) that merely follow instructions. However, in IoV systems<sup>1</sup> that involve autonomous (human, vehicular, and infrastructure) agents, it leads to new forms of coordination and control problems. In principle, giving more autonomy raises the challenging problem of *whether* and *to what extent* such autonomous systems are capable of collaboration and self-coordination towards collective-level safety concerns. For instance, in an intersection, it is crucial to realise whether the set of involved IoV agents can collaboratively self-coordinate towards ensuring the safety of the intersection.

To that end, IoV systems require operational methods to reason about the capacity of the involved (human and artificial) agents to form *feasible* and *capable* coalitions as a means to ensure safety. Here, feasibility refers to the absence of potential incompatibilities of involved agents (i.e., their preference to get involved or avoid collaborating with one another) and capability refers to being able to strategically ensure safety (i.e., having a chain of actions—a strategy—to guarantee safety regardless of what agents outside the coalition do). We argue that such methods should satisfy the following desiderata:

- *Expressivity*: to capture the temporal, strategic, and normative aspects of IoV systems in coalitional settings. The behaviour of the IoV evolves over time (temporal dimension) and is a result of the interaction of various agents where the combination of their actions (strategic dimension) may result in desirable outcomes such as safety or undesirable ones such as a collision (normative dimension). A reasonable analysis of whether an IoV system can maintain such desirable outcomes requires modelling what different groups of agents, and not merely individuals, are able to ensure collectively (coalitional dimension). E.g., the collective-level safety is a property that in most

---

<sup>1</sup> We say “*IoV system*” to refer to a particular instance, e.g., a multiagent intersection scenario, in the IoV as a whole (with millions of nodes). In the following, whenever it is clear from the context that we are focused on a specific IoV system, we may simply refer to it as the “*IoV (case/scenario)*”. Indeed, one may approach the IoV in a granular level, with all the nodes and sensors, but this work approaches the topic on a system level and focuses on reasoning about the self-coordination abilities of coalitions in IoV systems.

multiagent IoV cases is achievable not by an individual but is a result of group-level coalitional strategies.

- *Coalitional Feasibility*: it is not realistic to assume that any subset of involved (human, vehicle, and infrastructure) agents in an IoV system can and is willing to collaborate. So, even if a subgroup is theoretically capable of ensuring a desirable outcome, it is crucial to verify whether it is a feasible coalitional collaboration.<sup>2</sup> For instance, two vehicles may be close enough to communicate, share information, and as a coalition find a way to coordinate who goes first in an intersection but not willing to do so due to privacy concerns avoiding them to share information with vehicles from other manufactures. In this case, we say the coalition is not feasible to form. We argue that contextual requirements such as privacy, and in turn the feasibility of coalitions, need to be integrated into smart IoV coordination frameworks.
- *Generality*: to be generic enough for reasoning about various forms of normative outcomes and not hard-wired to a given safety concern. E.g., a safe behaviour in a T-shape intersection may be unsafe in crossroads.

Reviewing the literature on IoV coordination and control, no method capable of capturing all these principles currently exists [24, 22, 8, 14, 16]. In [22], the authors use a graph theoretical representation that is temporally expressive. However, the results are specific to platoon formation cases in a static topology with no room for expressing scenarios in which the set of available actions to each agent varies over time and with respect to the state of the IoV system. The presented approach in [8] removes the need for traffic lights and solves the coordination problem in crossroads but under the strong assumption that the involved vehicles are fully collaborative and that all the potential two-member coalitions are feasible to form in order to avoid pairwise collisions. Finally, in [14, 16], the safety can be guaranteed under the assumption that vehicles share information regardless of their potential incompatibilities, e.g., caused by being designed by different manufacturers with justifiable conflicts of interests.

---

<sup>2</sup> Coalitional *feasibility* is different from stability in cooperative games and coalition structure generation (see e.g., [21, 19]). There, the focus is mainly on post-conditions and what agents gain as a result of coalition formation while what we call coalitional feasibility is about pre-conditions on inherent incompatibilities of agents and verifying whether the formation of a collaborative coalition is feasible.

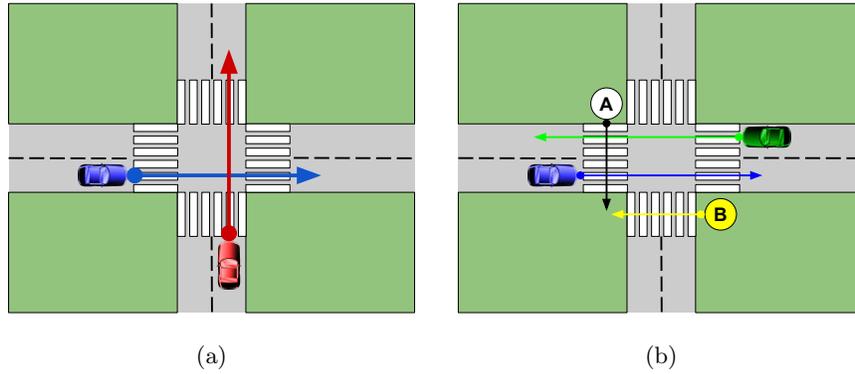
For the first time in this work, we present a formally evaluated methodology to verify the self-coordination capacity of IoV systems using formal strategic reasoning and develop a mechanism to ensure it. We employ the semantic machinery of Alternating-time Temporal Logic (ATL) [1] as the basis for reasoning about strategic abilities in the IoV and employ its coalitional extension [4] to model endogenous and exogenous constraints in terms of argumentative notions of *incompatibility* and *priority*. In practice, this framework can be embedded in the IoV infrastructure as a safety-ensuring coordination service. In IoV scenarios, e.g., in an intersection, it is common that vehicles communicate with a trusted Infrastructure Agent (IA) a short time before reaching the intersection. Using our presented methods, an IA can evaluate the self-coordination ability of the agents and if needed apply the mechanism to ensure it.

## 2 Conceptual Analysis and Game Structures

In the IoV, we encounter situations in which the traditional forms of coordination may be ineffective. For instance, think of an intersection with a fixed interval traffic light. When two vehicles—both travelling from east to west—arrive at the intersection, they have to wait for the green light even if there is no harm if they pass. In the IoV, given the possibility of communication among the involved agents, such inefficiencies can be handled using smart and dynamic forms of self-coordination techniques. Thus, this paper focuses on developing reasoning methods to verify whether self-coordination is feasible in an IoV system and establishing a framework to coordinate IoV scenarios to ensure safety. We later elaborate on safety as a principle to guide the process of designing coordination mechanisms for IoV systems. If one aims to replace static external coordination techniques (e.g., traditional traffic lights) with a dynamic self-coordination mechanism, safety is the main concern. Imagine the simple two-agent scenario in Figure 1(a). Having no external signal, how can they decide to go or to stop? They can stop at the intersection forever or may cause a crash.

Even with full awareness about the environment and observability over the surrounding traffic, ensuring the safety of the intersection requires verifying if the group of vehicles (in this case *blue* and *red*) can come up with a plan to pass the intersection safely. Here, no single one of them is able to ensure that both a crash and a deadlock is avoided. The only safe way is if one goes before the

other—which requires them acting together as a group, i.e., taking a coalitional action. Then it is crucial to consider that, e.g., for privacy concerns, they may avoid sharing information with one another, hence cannot form a coalition and execute a collective plan. This necessitates capturing what we introduced as the *coalitional feasibility* condition while verifying self-ordination abilities in the IoV.



**Fig. 1.** The Intersection Scenario: Vehicles (*red, blue, green*) and pedestrians (*A* and *B*) can form coalitions in order to self-coordinate and ensure safety.

Note that many intersections and traffic junctions currently operate without any traffic light and merely rely on the self-ordination capacity of human-driven vehicles (e.g., in roundabouts). To keep them operational and safe for a mixed group of human-driven and autonomous vehicles, we argue that the IoV infrastructure needs to be enriched with computational methods to (1) *verify* whether—in a given scenario—involved agents are able to safely self-coordinate and (2) when they are not able to do so, to *ensure* safety using verifiably reliable coordination techniques.

Using multiagent strategic reasoning semantics (e.g., [1]), one can evaluate whether an agent or agent group is able to avoid the crash or to ensure that no deadlock takes place. For instance, we can verify whether the coalition of agents  $\{red, blue\}$  is capable of ensuring that neither a crash nor a deadlock takes place. However, such a realisation (that such a group with a successful strategy exists) does not necessarily imply that such a group will form and accordingly will ex-

ecute their collective strategy to avoid undesirable situations. In the context of the IoV—with vehicles from different manufacturers and with different priority levels—it is not a reasonable assumption that all agents can communicate, form such coalitions, and successfully execute actions in a particular order. There might be incompatibilities among agents. These are mostly caused by inherent characteristics of the involved agents (endogenous constraints). E.g., differences in the technologies or manufacturers may prevent agents from forming a collaborative coalition with each other.<sup>3</sup> Moreover, in real-life and physically bounded multiagent systems such as the IoV, there exist external conditions that may require them to do specific actions or to form coalitions (exogenous constraints). For instance, consider regulatory rules and road priorities that expect agents to give way if an ambulance arrives at the intersection.

To model the external as well as internal constraints of coalition formation in real-life applications of the IoV, we capture inherent incompatibilities of agents (e.g., being produced by competing manufacturers) using the argumentative notion of “attack” relations [17]. We follow [4] and consider potential priorities among vehicles (e.g., ambulances, bicycles, or fire trucks over other vehicles) using a preorder on the involved agents. A formal account of these notions will be presented in upcoming sections. These elements act as constraints over the feasibility of coalitions in an IoV system. Then, a feasible coalition that possesses a strategy to ensure safety in an IoV scenario is *realistically able* to self-coordinate the scenario in a safe manner. The first part of work presents logic-based methods to formally verify whether such a coalition exists in a given IoV scenario and the second part provides a mechanism to ensure it. For instance, in Figure 1(a), the coalition  $\{red, blue\}$  is able to self-coordinate only if it is a feasible coalition. Taking feasibility into account distinguishes our work from methods that merely

---

<sup>3</sup> We would like to emphasise that ensuring the safety and reliability of dynamic systems such as the IoV needs to balance the trade-offs between strict, design-time, offline standardisation (e.g., see [20]) and flexible run-time online coordination (e.g., see the interdisciplinary study in [15]). While standardisation is effective for parts of the IoV with less complexity and more predictability, for other parts in which standardisation is out of reach, the IoV requires flexible techniques able to capture the characteristics of specific scenarios and able to be exploited at the run time. This work focuses on such instances where incompatibilities are probable and provides a base for verifying and ensuring self-coordination in the run-time.

focus on the availability of strategies to agent groups. While such a perspective is applicable for closed worlds with benevolent and cooperative agents (e.g., software agent systems in [18]), physically bounded IoV systems demand methods capable of addressing feasibility constraints. Our concern to capture feasibility of coalitions in the IoV relates to the notion of natural abilities in [11], where the authors formalise natural strategies as those with a feasible degree of complexity. Then it is a question whether a feasible coalition to ensure safety necessarily exists. Do we fail to self-coordinate if *red* and *blue* cannot form a feasible coalition? In real-life scenarios, e.g., traffic handling in intersections with no traffic light, priority rules act as predesigned mechanisms for coordination. Inspired by this, we introduce a model-updating mechanism to ensure the existence of a minimal coalition, feasible to be formed and capable of ensuring the safety of an IoV system.

To reason about the abilities of agents and agent coalitions in a multiagent system such as the IoV, we employ Concurrent Game Structures (CGS). CGS, as the semantics machinery of Alternating-time Temporal Logic (ATL) [1], enables modelling the behaviour of IoV systems over time (capturing temporality) and is expressive for representing the ability of individual agents as well as coalitions to ensure/avoid a given situation (strategic abilities). Moreover, CGS-based notions can be implemented using established model-checking tools [5, 13]. Using CGS, we reason about coalitional aspects of the IoV and model the temporal and strategic aspects of IoV scenarios.

*Concurrent Game Structures:* Formally, a *Concurrent Game Structure* (CGS) is a tuple  $\mathcal{M} = \langle \Sigma, Q, \Pi, \pi, Act, d, o \rangle$  where:  $\Sigma = \{a_1, \dots, a_n\}$  is a finite, non-empty set of *agents*;  $Q$  is a finite, non-empty set of *states*;  $\Pi$  is a set of atomic propositions;  $\pi : Q \mapsto \mathcal{P}(\Pi)$  is a valuation of propositions;  $Act$  is a finite set of atomic *actions*; function  $d : \Sigma \times Q \mapsto \mathcal{P}(Act)$  specifies the sets of actions available to agents at each state; and  $o$  is a transition function<sup>4</sup> that assigns the outcome state  $q' = o(q, \alpha_1, \dots, \alpha_n)$  to state  $q$  and a tuple of actions  $\alpha_i \in d(a_i, q)$  that can be executed by  $\Sigma$  in  $q$ . To represent *strategies* and *outcomes* we make use of the following auxiliary notions.

---

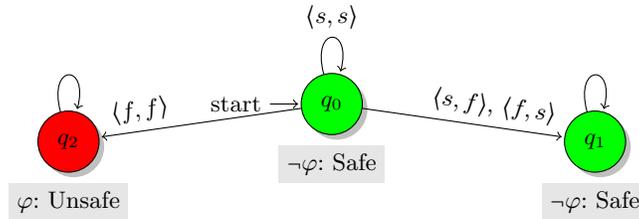
<sup>4</sup> CGS can be extended to probabilistic forms by adding probabilities to transitions.

For the purpose of this work, our approach can be applied after a standard determinisation procedure [23]. If one focuses on finite traces (as argued for in [2, 7]), a probabilistic automaton can be reduced to a deterministic one.

*Successors and Computations:* For two states  $q$  and  $q'$ , we say  $q'$  is a *successor* of  $q$  if there exist actions  $\alpha_i \in d(a_i, q)$  for  $a_i \in \{1, \dots, n\}$  in  $q$  such that  $q' = o(q, \alpha_1, \dots, \alpha_n)$ , i.e., agents in  $\Sigma$  can collectively guarantee in  $q$  that  $q'$  will be the next system state. A *computation* of a CGS  $\mathcal{M}$  is an infinite sequence of states  $\lambda = q_0, q_1, \dots$  such that, for all  $i > 0$ , we have that  $q_i$  is a successor of  $q_{i-1}$ . We refer to a computation that starts in  $q$  as a *q-computation*. For  $k \in \{0, 1, \dots\}$ , we denote the  $k$ 'th state in  $\lambda$  by  $\lambda[k]$ .

*Strategies and Outcomes:* A *memoryless strategy*<sup>5</sup> for an agent  $a \in \Sigma$  is a function  $\zeta_a : Q \mapsto Act$  such that, for all  $q \in Q$ ,  $\zeta_a(q) \in d(a, q)$ . For a coalition of agents  $C \subseteq \Sigma$ , a *collective strategy*  $Z_C = \{\zeta_a \mid a \in C\}$  is an indexed set of strategies, one for every  $a \in C$ . Then,  $out(q, Z_C)$  is defined as the set of potential  $q$ -computations that agents in  $C$  can enforce by following their corresponding strategies in  $Z_C$ .

CGS is expressive to capture complex scenarios where we are interested in a combination of temporal, coalitional, and strategic properties. Note that reasoning about normative (*un*)desirable properties in IoV scenarios, e.g., to verify whether a crash is possible, avoidable, or inevitable, requires going beyond single-shot properties in contrast to merely analysing whether a crash happens in the immediate next state of the system. For instance, our running example with two vehicles can be modelled as a 3-state CGS (Figure 2).



**Fig. 2.** We model the scenario presented in Figure 1(a) as  $\mathcal{M} = \langle \Sigma, Q, \Pi, \pi, Act, d, o \rangle$  where:  $\Sigma = \{red, blue\}$ ;  $Q = \{q_0, q_1, q_2\}$ ;  $\Pi = \{\varphi\}$  ( $\varphi$  represents the breach of safety, i.e., the crash, in the intersection);  $Act = \{f, s\}$  to represent going forward “ $f$ ” and stopping “ $s$ ”;  $d(a_i, q) = Act$  for all  $a_i \in \Sigma$  and  $q \in Q$ ; and  $\pi$  and  $o$  are represented in the automaton.

<sup>5</sup> We focus on memoryless strategies to avoid the strong assumption that agents necessarily recall the evolution of the IoV system.

Being concerned about the occurrence of a crash or passing safely, we use the unique proposition  $\varphi$  to represent a crash (in general, we can represent a finite set of propositions, relevant to our scenario, in  $\Pi$ ). Then, we are interested in verifying if individual agents or coalitions of agents are capable of avoiding such a crash using their available actions or sequences of actions. To reason about agents' potentials, we have that in  $q_0$ , *red* and *blue* may each stop or go forward. With no communication, hence no coordination, the two vehicles may remain in a deadlock situation in  $q_0$  or cause a crash in  $q_2$ . However, coalition  $\{\textit{red}, \textit{blue}\}$  has a strategy to avoid this (e.g., *red* goes first and *blue* second). But the question is whether such a coalition is a reasonable one to form in the context of IoV systems and given potential incompatibilities among the involved agents. In real-life IoV scenarios, we cannot assume benevolent agents but need to restrict theoretically formable coalitions to a subset of feasible ones.

### 3 Coalitional IoV Systems

Inspired by the presented approach in [4], we build on the CGS machinery, adopt elements from the literature on formal argumentation theory [17], and model coalitional IoV systems in Definition 1. The first element, adopted from argumentation theory, is a relation to represent potential incompatibilities between agents (known in the formal argumentation community as the *attack* relation). Furthermore, the second adopted element is a preorder to represent priorities among agents in the IoV context, e.g., an ambulance has priority over a truck. Note that notions of computation and strategy are syntactic elements of CGS and do not capture the feasibility of coalitions. In a CGS, a group  $C$  may have a collective strategy to enforce a particular form of computation. This merely means that there exists a chain of collective actions to do so and disregards that some agents in  $C$  may hesitate to (form a collaborative coalition and) execute the collective strategy. By adding new elements to CGS, we can distinguish groups with a strategy from feasible groups with a strategy. This allows capturing, not only the existence of a collective strategy but also, the feasibility of forming a coalition to execute the strategy.

**Definition 1 (Coalitional IoV).** *A coalitional IoV is given by a tuple  $\mathcal{I} = \langle \Sigma, Q, \Pi, \pi, Act, d, o, \mathfrak{J}, \prec \rangle$  where  $\langle \Sigma, Q, \Pi, \pi, Act, d, o \rangle$  is a CGS modelling the behaviour of the IoV,  $\mathfrak{J} \subseteq \Sigma \times \Sigma$  is an antireflexive relation representing the*

*potential incompatibilities between agents, and  $<$  is a preorder on  $\Sigma$  representing priorities between agents.*

Here, relation  $\mathfrak{I}$  reflects potential incompatibilities not as misalignment in goals but in terms of inherent characteristics, e.g., competing manufacturers of vehicles. Making incompatibilities explicit in the modelling relaxes the common assumption that IoV systems are operating either in a cooperative or fully non-cooperative setting and enables modelling realistic scenarios, where some agent groups (but not necessarily all) may be able to form coalitions. Furthermore, the ordering  $<$  is a contextual element in the IoV system that models priorities. In real-life cases—e.g., in applying our method to traffic coordination scenarios—priorities act as regulatory norms and override potential incompatibilities. For instance, regardless of the brand of an ambulance, other vehicles collaborate with it as it has a higher priority. Using CGS for specifying IoV systems enables capturing the temporal, strategic, and normative aspects. In addition, it is implementable using computationally affordable model-checking tools, e.g., [5, 13].

**Definition 2 (Feasibility).** *Let  $\mathcal{I}$  be a coalitional IoV and  $C \subseteq \Sigma$  an agent group in  $\mathcal{I}$ . We say  $C$  is a feasible coalition if and only if for all  $a_i, a_j \in C$  we have that  $(a_i, a_j) \in \mathfrak{I} \Rightarrow a_i < a_j$ . The set of all feasible coalitions is denoted with  $\mathfrak{F}$ .*

Notice that the feasibility of a coalition is defined in terms of incompatibilities that are not overruled by priorities. Moreover, note that we do not assume symmetry on the incompatibility relation  $\mathfrak{I}$ . This reflects the reality of the IoV context. For instance, vehicles from a manufacturer  $A$  may avoid forming coalitions with others from  $B$  while vehicles from  $B$  are not necessarily concerned with being in a coalition with vehicles from  $A$ . This is also the case when we consider vehicle-human or vehicle-infrastructure relations. For instance, imagine extending our two-vehicle scenario with  $\mathfrak{I} = \{(red, blue)\}$  and  $red < blue$ . Then we have an incompatibility but it is “overruled” by the priority preorder. Thus, the grand coalition is feasible and able to safely self-coordinate towards  $q_1$ . By the corollary to Definition 2, we have:

**Corollary 1.** *Let  $\mathcal{I}$  be a coalitional IoV. Then we have: 1. (conflict-freeness) Any  $C \subseteq \Sigma$  is a feasible coalition (i.e., a member of  $\mathfrak{F}$ ) if  $\mathfrak{I} = \emptyset$ ; and 2. (maximality) If  $C$  is a feasible coalition ( $C \in \mathfrak{F}$ ), then any  $C' \subseteq C$  is a feasible coalition.*

The first point shows that in a conflict-free IoV—i.e., with no incompatibility among the agents—all potential coalitions are feasible. Then the second point shows that being feasible is a maximal quality for a coalition. The latter is crucial to presenting the first main result of our work on the ability of an IoV to safely self-coordinate (Theorem 1). The former point relates to what we later discuss as *weak homogeneity* in IoV systems. Note that the feasibility of coalitions does *not* reflect the post-conditions in the IoV (i.e., what they can ensure via their actions) but is defined with respect to their inherent characteristics (e.g., potential manufacturer differences and type of the vehicle) and the context of the IoV (i.e., what priorities and codes of conduct are in place). Next, we move to our focal question on “whether agents in an IoV system can safely self-coordinate”. This is to verify if agents can *feasibly* ensure a given  $S$  that represent safe states and *maintain* it over time. In a CGS, the capacity of a set of agents  $C$  to ensure a subset of states  $S$  from a state  $q$  requires  $C$  to have a strategy  $Z_C$  such that all  $q$ -computations in  $out(q, Z_C)$  include a state in  $S$ . In other words, all such computations should meet a state in  $S$  at least once. Then, maintaining  $S$  is a specific form of ensuring as it requires that all such computations consist of states in  $S$  and only states in  $S$ . Note that it is not necessary that computations  $C$  enforces (using  $Z_C$ ) consist of identical states but any state in  $S$ . In other words, even if  $q \in S$ , group  $C$  does not need to enforce the system to remain in  $q$  but can enforce computations that go through other states in  $S$ . In the following, we use the term “*to ensure and maintain*” to convey the point that maintaining  $S$  (even from a  $q \in S$ ) can be achieved by ensuring other states in  $S$  and not necessarily by remaining in  $q$ .

**Theorem 1.** *Let  $\mathcal{I}$  be a coalitional IoV and  $S \subseteq Q$  a safety state of affairs represented by a set of states in the IoV. From a safe state  $q \in S$ , the IoV  $\mathcal{I}$  can safely self-coordinate w.r.t.  $S$  if (1) there exists a  $C \subseteq \Sigma$  with a collective strategy  $Z_C$  to ensure and maintain  $S$ , (2)  $C$  is a feasible coalition, and (3) no  $C' \subset C$  satisfies both (1) and (2).*

*Proof.* To guarantee that  $\mathcal{I}$  can ensure and maintain  $S$ , agents in  $\Sigma$  should have the capacity to do so. A minimal (part 3) and feasible (part 2) sup-group of agents  $C \subseteq \Sigma$  with a collective strategy  $Z_C$  (part 1) is capable of forming  $C$  (thanks to its feasibility) and ensuring that all the  $q$ -computations  $\lambda$  in  $out(q, Z_C)$  are merely composed of states that are in  $S$ . This is thanks to its capacity to ensure

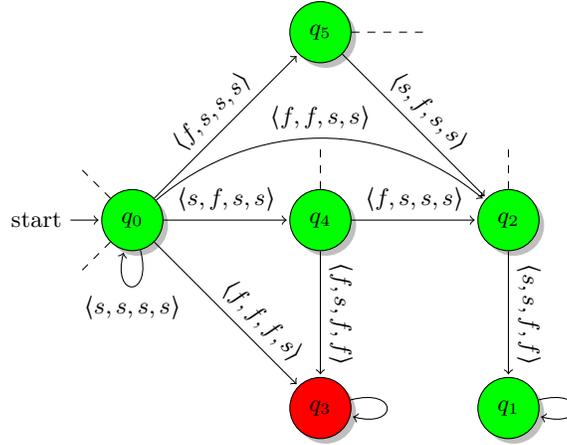
and in addition maintain (i.e., remaining in)  $S$ . As  $\mathcal{I}$  is safe in the first place (in  $q$ ) and any potential  $q$ -computation remains in  $S$  if  $C$  executes  $Z_C$ , we have the coordination capacity within  $\mathcal{I}$ .  $\square$

From an implementability point of view, note that the problem to verify whether an IoV is capable of self-coordination in a safe manner reduces to a model-checking problem, that takes the set of feasible coalitions as its input, and hence is implementable using standard tools (e.g., using [5, 13]). First, any state of affairs  $S$  translates to a valid proposition in  $\varphi \in \mathcal{L}_{ATL}$  (see [25] for a similar approach). Basically,  $S$  consists of those states in  $Q$  that satisfy  $\varphi$ . Then we have a straightforward process to verify if in  $q$ , any feasible coalition has a strategy to minimally ensure  $S$ . As shown in Corollary 1, subsets of a feasible coalition preserve the feasibility. Hence, instead of model-checking on possible coalitions in  $\Sigma$ , we only consider feasible coalitions.

Based on Theorem 1, the presented 2-vehicle IoV can safely self-coordinate as the grand coalition is feasible and is the only minimal coalition capable of ensuring and maintaining  $q_1$ . In the scenario displayed in Figure 1-b, we have vehicles *blue* and *green*; pedestrians Alice ( $A$ ) and Bob ( $B$ ); and the following action space, incompatibilities, and priorities:  $d(a, q) = \{s, f\}$  meaning that any agent  $a$  can either stop ( $s$ ) or go forward ( $f$ ) in any state  $q$ ;  $\mathfrak{I} = \{(green, blue)\}$  meaning that *green* is incompatible with *blue*;  $green < blue, green < A, blue < A$  meaning that *blue* has priority over *green* and Alice has priority over both the vehicles. The partial CGS in Figure 3 models this scenario. Here, the three-member coalition of Alice, *green*, and *blue* satisfies the conditions of Theorem 1. Their coalition is feasible thanks to the priority of *green* over *blue* and minimal as no member can be excluded.

Building feasible coalitions (i.e., expecting to collaborate with others) is not necessarily required in all the IoV cases. Our framework can capture such cases too. For instance, imagine Figure 1-(b) with only the two vehicles *green* and *blue*—with neither Alice nor Bob. Then all the potential outcomes are safe, hence the empty set is the feasible and minimal coalition capable of ensuring a safe state. In general:

**Proposition 1.** *For any incompatibility relation  $\mathfrak{I}$  and priority  $<$ ,  $\mathcal{I}$  can safely self-coordinate w.r.t.  $S$  if  $S = Q$ .*



**Fig. 3.** This CGS represents various paths which the coalition composed by  $A$ ,  $green$ , and  $blue$  can ensure and maintain safety in  $q_1$ . E.g.,  $q_0, q_4, q_2, q_1, \dots$ . Action profiles on each arrow are actions for  $A$ ,  $B$ ,  $blue$ , and  $green$ , respectively. Dashed lines represent other paths that may result from unrepresented actions.

*Proof.* If all states are in  $S$ , any successor of any  $q \in Q$  is a safe state. Formally, for any strategy  $Z_\emptyset$ , all the states in  $out(q, Z_\emptyset)$  are in  $S$ . Hence the empty set is the unique minimal coalition capable of ensuring safety from any  $q$ .  $\square$

While we use a state-based formalisation of safety in the IoV, our approach is not limited to state-based normativity and safety on the state level but has behavioural connotations. Basically, a state of affairs in  $Q$  represents all the states that satisfy a  $\varphi \in \mathcal{L}_{ATL}$  (e.g., see Figure 2). Using the state-based notation is more intuitive and enables colour-based visual labelling. To see the behavioural aspect, notice that our notion of strategy is a multi-step temporal notion as it involves chains of actions to reach a  $q \in S$ . Moreover, verifying if such a strategy is available to a group requires model-checking the potential evolution/behaviour of the MAS using the semantic notion of path/computation (in contrast with the purely syntactic notions of action and state). As observed, adding agents to an IoV does not preserve the self-coordination ability.

**Proposition 2.** *Coalitional IoV systems are non-monotonic regarding their ability to safely self-coordinate.*

*Proof.* We show that given an IoV  $\mathcal{I}$  capable of self-coordination w.r.t. to  $S$ , adding a new agent  $a_i$  does not preserve the self-coordination ability of the newly

formed  $\mathcal{I}'$ . Basically, there exists a feasible coalition  $C$  in  $\mathcal{I}$  with a strategy  $Z_C$  to ensure and maintain  $S$ . To be able to ensure  $S$  in  $\mathcal{I}'$ ,  $C \cup \{a_i\}$  should be feasible, which is not the case in general due to potential incompatibilities. As a counterexample, imagine adding a new vehicle *brown* (going from east to west) to Figure 1. If *brown* is incompatible with both *red* and *blue*, and we have that  $red < brown$  and  $blue < brown$ , then the IoV system will be unable to safely self-coordinate.  $\square$

## 4 Self-Coordinating IoV Classes

The IoV has the potential to be deployed in various contexts with domain-specific characteristics. For instance, in the context of rail freight transport, one may face a homogeneous set of autonomous train vehicles operating with no incompatibility. This form of context-dependent homogeneity arises when we deal with collaborative agents with negligible incompatibilities. E.g., when we are dealing with a set of vehicles from the same manufacturer. This translates into having  $\mathcal{J} = \emptyset$  in our formalisation. In this section, we focus on the ability of such sub-classes to safely self-coordinate. This has direct implications for deployability of real-life IoV systems.

**Proposition 3.** *Let  $\mathcal{I}$  be an IoV with  $\mathcal{J} = \emptyset$ ,  $S \subseteq Q$  be a non-empty safety state of affairs, and  $q$  be a state in  $S$ .  $\mathcal{I}$  can safely self-coordinate from  $q$  if there is a safe path in  $S$  that contains a loop.*

*Proof.* The antecedent is identical to saying that  $S$  is reachable from  $q$  and maintainable; formally, that for a  $q$ -computation  $\lambda$ , there exists a finite prefix  $\lambda[j] = q_0, \dots, q_i, \dots, q_j$  s.t. all the states in the prefix are in  $S$  and  $q_i = q_j$ . To prove, we show how such an IoV satisfies the three conditions of Theorem 1 on: (1)  $S$ -ensuring and maintenance ability, (2) coalitional feasibility, and (3) minimality. For part one, the existence of safe finite prefix implies that  $\Sigma$  can ensure  $q_i$  in the non-empty  $S$ . Given that  $S$  has a loop,  $\Sigma$  can maintain  $S$  by ensuring that  $\mathcal{I}$  loops back to  $q_i$ . Then, for part two, relying on the conflict-freeness of  $\mathcal{I}$  (see Corollary 1), we have that  $\Sigma$  is feasible. Finally, for part three, either  $\Sigma$  is minimal or by excluding excess agents, we reach to a minimal subset  $C$  where we have that  $C$  necessarily preserve the feasibility condition (maximality term in Corollary 1).  $\square$

Having no incompatibility relaxes the feasibility check, but observe that the ability to ensure and to maintain  $S$  are independent. For instance, in Figure 3,  $\{Bob\}$  can ensure  $S$  but has no strategy to maintain it. Moreover, a group may be capable of maintaining  $S$  in a state  $q'$  but not in a different state  $q$ , e.g., the empty set can preserve  $S$  in  $q_1$  but has no strategy to ensure it from  $q_0$ . Our notion of self-coordination in the IoV is essentially a *local* notion as it is about the ability of the IoV to remain safe from a given safe state. In the context of the IoV, we deem that safety is a requirement that is necessary to be respected in all the possible outcomes. In IoVs, one cannot be satisfied with a path of states that reaches a safe state via unsafe states. For instance, in the intersection scenario, given that  $q_0$  is a safe state itself, we are interested to see if agents can self-coordinate towards  $q_1$  via a safe path. One may argue that *Alice* can stop and individually avoid going into a red state. Note that she can only ensure that the next state after  $q_0$  is either  $q_0$  or  $q_4$  but cannot maintain remaining in a safe state. We need to consider that the capacity to self-coordinate (Theorem 1) is in terms of and bounded to a given set of states, without imposing any requirements on these states, and here we are focused on  $q_1$ . Next, we focus on how the global self-coordination capacity (in contrast to a state-bounded local capacity) can be verified.

**Theorem 2.** *IoV  $\mathcal{I}$  can safely self-coordinate w.r.t.  $S \subseteq Q$  if in all  $q \in S$ , there is a coalition  $C \in \mathfrak{F}$  with a strategy  $Z_C$  such that in any  $\lambda \in out(q, Z_C)$ , we have that  $\lambda[1]$  is in  $S$ .*

*Proof.* To prove, we show how such an IoV satisfies the local conditions of Theorem 1 in any  $q \in S$ . In any  $q$ , if a feasible coalition  $C$  with such a  $S$ -ensuring strategy exists, then the set of possible next immediate states that  $C$  can ensure consists of either only  $q$  itself or has other states  $q' \neq q$  in  $S$ . In the former case,  $C$  can make a loop in  $S$  that satisfies the maintaining condition. Such a  $C$  is either minimal or by excluding excess members we reach to a minimal subset. In the later case, when we may have  $q' \neq q$  in the set of possible next immediate states that  $C$  can ensure, we have a coalition  $C'$  to ensure  $S$  by looping on  $q'$  or by reaching another state in  $S$ . Note that we are not extending  $C$  to  $C \cup C'$  hence coalitional feasibility is not an issue. Intuitively, each  $C, C', \dots \in \mathfrak{F}$  is responsible just to ensure that the next state is in  $S$ . The antecedent indicates that in all  $q \in S$ , such a coalition exists. This ensures the maintenance condition.  $\square$

In this class of IoVs,  $\mathcal{I}$  is capable of self-coordination globally only if in every safe state, there exists at least a feasible coalition capable of ensuring at least an immediate safe state. For instance, imagine the scenario in Figure 1-b but without  $green < blue$ . Then,  $blue$  has no priority over  $green$  and their incompatibility results in the infeasibility of their coalition with  $Alice$ . Such practical concerns in the context of the IoV make self-coordination in coalitional IoVs distinguishable from strategic reasoning in software systems, with fully-collaborative agents, and motivates using mechanisms to update priority rules in order to ensure safety properties.

## 5 A Safety-Ensuring Mechanism

In cases where the conditions of Theorem 1 are not satisfied, the IoV is incapable of self-coordination in a safe manner, thus requires intervening mechanisms to ensure safety. Next, we show that in our formalisation of IoV systems, this can be ensured using a mechanism that minimally introduces priority rules. In this context, minimality refers to the introduction of  $l$  new priority rules such that the IoV is incapable of safe self-coordination under any  $k < l$  added rules. Mechanism  $\mathfrak{M}^S$  (Algorithm 1) is designed to ensure safety concern  $S$  as a function that takes  $\mathcal{I}$  and updates it to  $\mathcal{I}'$  capable of self-coordination with respect to  $S$ .

**Theorem 3.** *Let  $\mathcal{I}$  be an IoV and non-empty  $S \subseteq Q$  a safety state of affairs. If  $S$  is reachable and maintainable from  $q \in Q$  (in the sense of Proposition 3), mechanism  $\mathfrak{M}^S$  ensures the self-coordinating capacity of the updated IoV  $\mathcal{I}'$  to ensure  $S$  via minimal priority updates.*

*Proof.* To prove, we show the correctness of Algorithm 1 using the following lemmas. In Lemma 1 and 2, we respectively establish the non-emptiness of  $\hat{C}_q^S$  and that  $\mathcal{I}'$  satisfies the self-coordinating conditions of Theorem 1.  $\square$

**Lemma 1.** *If  $S$  is reachable and maintainable from  $q \in Q$  (in the sense of Proposition 3), then  $\hat{C}_q^S \neq \emptyset$ .*

*Proof.* Building on Proposition 3, we have that for such a  $S$ , the grand coalition  $\Sigma$  is a member of  $\hat{C}_q^S$  as it is necessarily capable of ensuring and maintaining  $S$ . Note that in this stage, the mechanism is merely focused on the strategic ability of groups regardless of their coalitional feasibility.  $\square$

---

**Algorithm 1:** Safety Ensuring Mechanism  $\mathfrak{M}^S$ 


---

**Input:** IoV  $\mathcal{I}$ ; state  $q \in Q$ ; state of affairs  $S \subseteq Q$ .  
**Result:**  $\mathcal{I}'$  capable of safe self-coordination w.r.t.  $S$ .

- 1 **Initialisation:**  $\varphi \leftarrow$  ATL formula (from  $\mathcal{L}_{ATL}$ ) corresponding to  $S$ ;
- 2  $\hat{C}_q^S \leftarrow$  indexed set of groups  $C_k$  able to ensure and maintain  $\varphi$  from  $q$   
 (standard ATL model-checking [3]);
- 3  $index \leftarrow 0$ ;
- 4  $u \leftarrow |\mathcal{I}|$ ;
- 5 **forall**  $C_k \in \hat{C}_q^S$  **do**
- 6  $u_k \leftarrow 0$ ;  $U_k \leftarrow \emptyset$ ;
- 7 **forall**  $(i, j) \in \mathcal{I}$  **do**
- 8 **if**  $i \in C_k$  **and**  $j \in C_k$  **and**  $j \neq i$  **then**
- 9  $u_k \leftarrow u_k + 1$ ;
- 10  $U_k \leftarrow U_k \cup \{(i, j)\}$ ;
- 11 **if**  $u_k = 0$  **then**
- 12 **return**  $\mathcal{I}$ ;
- 13 **else**
- 14 **if**  $u_k \leq u$  **then**
- 15  $u \leftarrow u_k$ ;
- 16  $index \leftarrow k$ ;
- 17  $\prec' \leftarrow \prec$ ;
- 18 **forall**  $(i, j) \in U_{index}$  **do**
- 19 **if**  $j < i \notin \prec'$  **then**
- 20  $\prec' \leftarrow \prec' \cup \{k < j : k < i \in \prec'\}$ ;
- 21 **return**  $\mathcal{I}' = \langle \Sigma, Q, \Pi, \pi, Act, d, o, \mathcal{I}, \prec' \rangle$ ;

---

By focusing on the class of reachable and maintainable  $S$  from  $q$ , we are making the assumption that it is not reasonable to specify an inevitable situation with  $S$ . An IoV neither can nor is expected to avoid inevitable situations. Moreover, for generating  $\hat{C}_q^S$ , using standard model-checking tools, we highlight that the notion of state of affairs in terms of a subset of  $Q$  is translatable to an ATL-based verifiable proposition.  $\varphi$  corresponds to a fixed set of states  $S \subseteq Q$ . From a computational complexity point of view, verifying whether a group is able to ensure a  $\varphi$  is  $P$ -complete w.r.t. the size of  $\mathcal{I}$  and  $\varphi$  [3].

**Lemma 2.** *From  $q$ , IoV  $\mathcal{I}'$  generated by  $\mathfrak{M}^S$ , can safely self-coordinate w.r.t.  $S$ .*

*Proof.* We show that  $\mathcal{I}'$  satisfies the conditions of Theorem 1. The first condition is fulfilled because  $\hat{C}_q^S$  is non-empty (Lemma 1). For the second condition, Algorithm 1 finds  $C_{index} \in \hat{C}_q^S$  with the least number of unresolved intra-group incompatibilities and introduces the required priorities. For the third condition, as coalitional feasibility is a maximal notion (Corollary 1), excluding excess members leads to the minimal group without harming the feasibility.  $\square$

As presented, this approach aims at intervening as little as possible as we focus on the coalition in  $\hat{C}_q^S$  with the smallest number of incompatibilities. If there exists a feasible group to form a coalition (that is capable of ensuring safety), we say the IoV system is capable of safe self-coordination without any external intervention. This is a crucial background for reasoning about (1) whether intervention, and applying the presented mechanism, is necessary (i.e., by introducing external rules) and (2) as a secondary outcome, whether we can see agents responsible for an unsafe behaviour, i.e., we can justifiably see them responsible if they could ensure safety but failed to do so [26].

## 6 Conclusions

We proposed a coalitional representation of IoV systems rooted in a logic for strategic reasoning in multiagent systems. In our approach, integrating elements from formal argumentation theory resulted in a contextual representation and reasoning framework that captures key aspects of the IoV. For the first time, this work enables automated reasoning about the temporal, strategic, and normative aspects of the IoV using logic-based methods. Specifically, it enables verifying whether a given IoV system is capable of self-coordination with respect to a safety concern. We designed an algorithmic mechanism that guarantees this ability in IoV systems and formally evaluated our results. In this work, we focused on the availability of strategies to coalitions. An interesting extension is to rank groups based on the hardness of their strategy. E.g., in some traffic contexts, a strategy is useful only if it can be executed fast. We aim to integrate the notion of “*natural strategy*” [11] to address this in terms of the number of state transitions. Another direction is to formulate agents’ *responsibility* for an undesirable situation, e.g., a crash. We aim to link our approach to epistemic strategic logics [10] and integrate it with multiagent responsibility reasoning tools [6, 25].

*Ethical Statement.* For an effective deployment of trustworthy IoV systems, verifiable computational models to capture and preserve social values, safety concerns, and ethical norms play a key role. The results of this study can be embedded in the IoV infrastructure as a safety-ensuring coordination service and are adaptable for preserving social values and ethical norms in human-centred AI systems.

*Acknowledgements.* This work is supported by the UK Engineering and Physical Sciences Research Council (EPSRC) through the Trustworthy Autonomous Systems Hub (EP/V00784X/1), the platform grant entitled “AutoTrust: Designing a Human-Centred Trusted, Secure, Intelligent and Usable Internet of Vehicles” (EP/R029563/1), and the Turing AI Fellowship on Citizen-Centric AI Systems (EP/V022067/1).

## References

1. Alur, R., Henzinger, T.A., Kupferman, O.: Alternating-time temporal logic. *J. ACM* **49**(5), 672–713 (2002)
2. Brafman, R.I., Giacomo, G.D.: Planning for ltlf /ldlf goals in non-markovian fully observable nondeterministic domains. In: *Proceedings of IJCAI 2019*. pp. 1602–1608 (2019)
3. Bulling, N., Dix, J., Jamroga, W.: *Model Checking Logics of Strategic Ability: Complexity*, pp. 125–159. Springer US, Boston, MA (2010)
4. Bulling, N., Dix, J., Chesñevar, C.I.: Modelling coalitions: ATL + argumentation. In: *Proceedings of AAMAS’08*. pp. 681–688 (2008)
5. Cermák, P., Lomuscio, A., Mogavero, F., Murano, A.: MCMAS-SLK: A model checker for the verification of strategy logic specifications. In: *Proceedings of the 26th International Conference on Computer Aided Verification*. pp. 525–532 (2014)
6. Chockler, H., Halpern, J.Y.: Responsibility and blame: A structural-model approach. *Journal of Artificial Intelligence Research* **22**, 93–115 (2004)
7. Fogarty, S., Kupferman, O., Vardi, M.Y., Wilke, T.: Profile trees for büchi word automata, with application to determinization. *Inf. Comput.* **245**, 136–151 (2015)
8. Ghaffarian, H., Fathy, M., Soryani, M.: Vehicular ad hoc networks enabled traffic controller for removing traffic lights in isolated intersections based on integer linear programming. *IET intelligent transport systems* **6**(2), 115–123 (2012)
9. Hammoud, A., Sami, H., Mourad, A., Otrok, H., Mizouni, R., Bentahar, J.: Ai, blockchain, and vehicular edge computing for smart and secure iov: Challenges and directions. *IEEE Internet of Things Magazine* **3**(2), 68–73 (2020)
10. van der Hoek, W., Wooldridge, M.J.: Cooperation, knowledge, and time: Alternating-time temporal epistemic logic and its applications. *Studia Logica* **75**(1), 125–157 (2003)

11. Jamroga, W., Malvone, V., Murano, A.: Natural strategic ability. *Artif. Intell.* **277** (2019)
12. Kaiwartya, O., Abdullah, A.H., Cao, Y., Altameem, A., Prasad, M., Lin, C.T., Liu, X.: Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. *IEEE Access* **4**, 5356–5373 (2016)
13. Kurpiewski, D., Jamroga, W., Knapik, M.: STV: model checking for strategies under imperfect information. In: *Proceedings of AAMAS'19*. pp. 2372–2374 (2019)
14. Lee, J., Park, B.: Development and evaluation of a cooperative vehicle intersection control algorithm under the connected vehicles environment. *IEEE Transactions on Intelligent Transportation Systems* **13**(1), 81–90 (2012)
15. Malone, T.W., Crowston, K.: The interdisciplinary study of coordination. *ACM Computing Surveys (CSUR)* **26**(1), 87–119 (1994)
16. Milanés, V., Alonso, J., Bouraoui, L., Ploeg, J.: Cooperative maneuvering in close environments among cybercars and dual-mode cars. *IEEE Transactions on Intelligent Transportation Systems* **12**(1), 15–24 (2011)
17. Modgil, S., Prakken, H.: A general account of argumentation with preferences. *Artificial Intelligence* **195**, 361–397 (2013)
18. Mohamed, A.M., Huhns, M.N.: Benevolent agents in multiagent systems. In: *Proceedings Fourth International Conference on MultiAgent Systems*. pp. 419–420. IEEE (2000)
19. Perez-Diaz, A., Gerding, E., McGroarty, F.: Coordination of electric vehicle aggregators: A coalitional approach. In: *Proceedings of AAMAS'18*. pp. 676–684 (2018)
20. Priyan, M., Devi, G.U.: A survey on internet of vehicles: applications, technologies, challenges and opportunities. *International Journal of Advanced Intelligence Paradigms* **12**(1-2), 98–119 (2019)
21. Rahwan, T., Michalak, T.P., Wooldridge, M., Jennings, N.R.: Coalition structure generation: A survey. *Artificial Intelligence* **229**, 139–174 (2015)
22. Santini, S., Salvi, A., Valente, A.S., Pescapè, A., Segata, M., Cigno, R.L.: A consensus-based approach for platooning with inter-vehicular communications. In: *2015 IEEE Conference on Computer Communications*. pp. 1158–1166 (2015)
23. Vardi, M.Y.: Automatic verification of probabilistic concurrent finite-state programs. In: *26th Annual Symposium on Foundations of Computer Science, Portland, Oregon, USA, 21-23 October 1985*. pp. 327–338 (1985)
24. Yang, F., Li, J., Lei, T., Wang, S.: Architecture and key technologies for internet of vehicles: a survey. *J. Comm. Inform. Networks* **2**(2), 1–17 (2017)
25. Yazdanpanah, V., Dastani, M., Jamroga, W., Alechina, N., Logan, B.: Strategic responsibility under imperfect information. In: *Proceedings of AAMAS '19*. pp. 592–600 (2019)
26. Yazdanpanah, V., Gerding, E.H., Stein, S., Dastani, M., Jonker, C.M., Norman, T.J.: Responsibility research for trustworthy autonomous systems. In: *Proceedings of AAMAS'21*. p. 57–62 (2021)