Filtering distributed information to build a plausible scene for autonomous and connected vehicles

Guillaume Hutzler, Hanna Klaudel, Abderrahmane Sali

Filtering distributed information to build a plausible scene for autonomous and connected vehicles

Guillaume Hutzler[1], Hanna Klaudel[1], and Abderrahmane Sali[1]

Université Paris-Saclay, Univ Evry, IBISC, 91020, Evry, France
{guillaume.hutzler,hanna.klaudel}@ibisc.univ-evry.fr

Abstract. To make their decisions, autonomous vehicles need to build a reliable representation of their environment. In the presence of sensors that are redundant, but not necessarily equivalent, that may get unreliable, unavailable or faulty, or that may get attacked, it is of fundamental importance to assess the plausibility of each information at hand. To this end, we propose a model that combines four criteria (relevance, trust, freshness and consistency) in order to assess the confidence in the value of a feature, and to select the values that are most plausible. We show that it enables to handle various difficult situations (attacks, failures, etc.), by maintaining a coherent scene at any time despite possibly major defects.

Keywords: autonomous vehicles, plausibility, confidence, sensor fusion

1 Introduction

Driving autonomy promises many benefits such as facilitating travel by reducing traffic jams and the number of accidents for which man is mainly responsible, or improving the comfort of the users during their travels. The control of autonomous vehicles is carried out in three stages: perception, decision, action. The perception stage corresponds to the acquisition of data by sensors, coupled to the analysis of these data to build the scene (integrated view of the environment). The decision stage corresponds to the selection of actions to be performed by the vehicle based on the scene, the state of the vehicle and its "intentions" (current maneuver, mission to perform). The action stage corresponds to the realization of the actions chosen based on the various actuators of the vehicle.

In a man-controlled vehicle, none of the sensors and features that they measure (speed, engine rpm, position, etc.) are crucial to the driving activity, they are only an assistance to help the driver in smoothly conducting his vehicle. In that case, the perception is mainly achieved by the senses of the driver. In an autonomous vehicle however, the relevance and reliability of environmental information are crucial to the decision-making process: a noisy perception or a rough reconstruction of the scene can lead to a bad decision and therefore a higher risk of accident. To tackle this issue, manufacturers use various and multiple sensors to obtain some redundancy in order to have more certainty about the environment. A problem arises when one has to choose between various values, measured by different sensors or combinations of sensors, for the same physical measure (position, speed, etc.). Sensors may have different margins of errors, or may be weather sensitive, and they may be subject to malfunctions, faults, or even attacks, that may lead to the production of erroneous values. Filtering the values in order to identify the most plausible one in the present context is thus a major stake in building (iteratively and in real-time) a reliable scene and therefore to increase the robustness of the system. This task is very similar to what happens in avionics where integrating data from different sources is necessary in order to build a view of the environment and create so-called *situational awareness* [9].

In this paper, we first specify the context and related works in section 2. We then define some terminology, explain the criteria used to evaluate the plausibility, and present our algorithm in section 3. We finally explain in section 4 how it was implemented and comment about a selection of results that we obtained.

2 Context and related work

An autonomous vehicle is a vehicle that has the capability to perceive the surrounding environment, and to make decisions that are transmitted to actuators, so as to drive without human intervention [12]. To this end, it is equipped, among other things, with a set of sensors allowing to analyze the current situation with sufficient accuracy to make a good decision. Sensors may be divided into categories relative to their ranges [21]: proximity sensors (e.g. ultrasounds), short-range sensors (e.g. cameras, short-range radars), medium range sensors (e.g. LiDARs, medium range radars), long Range Sensors (e.g. long-range radars) and location sensors (e.g. GPS). Autonomous vehicle manufacturers offer a wide range of sensors in order to respect a cost/accuracy/range compromise.

Communicating vehicles are vehicles that use communication technologies to exchange data (e.g. position, speed, intent) with each other [2]. Transmissions travel either directly between vehicles (Vehicle to Vehicle or V2V communication), or through an infrastructure (Vehicle to Infrastructure or V2I communication). Since vehicles may exchange information about their position, speed, steering wheel angle, etc., we may consider the reception of messages from other vehicles as an additional sensor, whose information can be shared with other sensors.

2.1 Data fusion

Since the same information can be inferred from various sensors, we do have redundancy of information, hence the need to merge the data to increase the robustness of the system, which is called data fusion [5]. There are a lot of different approaches in data fusion, and a lot of different classifications altogether, depending in particular on the type of data that are processed (raw data, features, decisions), and the type of data that are produced.

In our case, we are interested in both redundant and complementary data, that we fuse in a *feature in-feature out* (FEI-FEO) approach (also known as feature fusion, symbolic fusion, information fusion or intermediate level fusion), according to Dasarathy's classification [6]. In this approach, a set of features is processed so as to "improve, refine or obtain new features" [5]. We thus assume that we work with features, i.e., values that have already passed through the data analysis process at the lower level. The vehicle has to make a single decision, and the process is thus centralized.

The main constraints that we have to face are the following: the fusion has to occur in *real-time* since the vehicle does not have the possibility to stop so as to make its next decision; the result of the fusion has to be as precise and *reliable* as possible since the safety issues, for the passengers and the other users of the road are high; the fusion process has to be *fault-tolerant* since sensors may be subject to failures and/or attacks. In addition, we wish the fusion process to be *verifiable*[1] and *explainable*[8].

2.2 Related work

We briefly mention the most popular approaches to data fusion, and how they relate to our case.

Probabilistic models need a priori knowledge (Bayesian inference [15,19]), and are vulnerable to attacks (Dempster-Shafer [7,11]). Artificial intelligence approaches based on neural networks [13] need a large amount of learning data and also lack explainability. This is also the case for other approaches based on genetic programming that tackle the issue of fault tolerance [3]. Similarly, approaches based on fuzzy logic [17,14] are not suitable because the system depends on an inference engine designed by human experts, and thus stability is not guaranteed.

Since part of the information available to the vehicle comes from other vehicles, we may also have to take into account the trust that we have in this data. Trust-based approaches [4,10,22] provide tools primarily applied to multi-agent systems, based on reputation.

3 Proposed approach

In this section, we propose a model allowing to build a coherent scene for the *Ego* vehicle in real-time, enabling it to make well-informed decisions. This vehicle receives features from a set of sensors, and also from other vehicles surrounding it. The model has to take into account the uncertainty of the information related to the environment and the agents, and to withstand possible attacks.

3.1 Terminology and outline of the study

At this point, it is useful to define the terminology that we will use in the remaining of the paper.

- A *feature* is a measure that describes some aspect of an entity in the environment. In the case of autonomous vehicles, features may be the position or speed of the vehicle.
- The *scene* of a vehicle is a set of features that represents both its state and the environment.
- The *Ego* vehicle is the reference vehicle, which tries to build its own scene.
- The features are produced by *information sources*, which may include a variety of elements: it may be a sensor whose raw data are processed to produce the corresponding feature, a collection of complementary features that are combined to produce the target feature, or a prediction about the probable value of a given feature computed from a past scene.

In order to understand the method and algorithm more easily, we will first specify the outline of the study in terms of *sensors*, *features* and *sources of information*.

The reference vehicle, *Ego*, has the following sensors (gathered in Table 1 with their characteristics, as provided by the manufacturers): three ultrasonic sensors: two on the sides and one behind; four cameras: one behind, three forward (one in the middle and two on the mirrors); a LiDAR; a GPS; and a V2V communication sensor. The features that are taken into account are the *Position* (longitudinal and lateral with respect to the road) and *Speed* (longitudinal and lateral with respect to the road). The sources of information can be:

- an individual sensor: each sensor of the *Ego* vehicle (GPS, LiDAR, Camera, Ultrasonic sensors) is considered as a source of information that computes one or several features;
- the V2V communication module: the surrounding vehicles may communicate their features (position, speed) to the *Ego* vehicle;
- complementary features: a feature can be computed from the values of two or more complementary features. For example, in order to have the absolute position of a vehicle V_i, we can combine the relative position of the vehicle V_i, given by a camera of *Ego*, with the absolute position of *Ego* given by the GPS.

Sensor	**Feature**	**Sampling**	**Angle**	**Range**	δ
GPS	Pos_{abs}, $Speed_{abs}$	25 Hz	-	-	$1m$
LiDAR	Pos_{rel}, $Speed_{rel}$	20 Hz	360°	150 m	1%
Camera	Pos_{rel} , $Speed_{rel}$	20 Hz	120°	200 m	0.5%
Ultrasound	Pos_{rel}	20 Hz	120°	4 m	0.05%
V2V	Pos_{abs}, $Speed_{abs}$	1 Hz	360°	1 km	$1m$

Table 1. Ego's sensors with their respective tolerances δ.

Source of information	$Pos_{abs}Ego$	Pos_{abs} V_i	Pos_{rel} V_i	δ
GPS	✓			$1m$
V2V Communications		✓		$1m$
LiDAR			✓	1%
Camera			✓	0.5%
Ultrasound			✓	0.05%
(GPS, V2V communications)			✓	$1m + 1m$
(GPS, LiDAR)		✓		$1m + 1\%$
(GPS, Camera)		✓		$1m + 0.5\%$
(GPS, Ultrasound)		✓		$1m + 0.05\%$
(V2V Communications, LiDAR)	✓			$1m + 1\%$
(V2V Communications, Camera)	✓			$1m + 0.5\%$
(V2V Communications, Ultrasound)	✓			$1m + 0.05\%$
Prediction	✓	✓	✓	0

Table 2. Sources of information to calculate the *Position* features of *Ego* and vehicles V_i.

– the prediction module: the value of the features may be estimated thanks to the information in the previous scene(s).

Table 2 presents the sources of information to be taken into consideration when calculating the *Position* features. The checked boxes indicate that the corresponding source of information is to be considered for the calculation of this feature, while δ represents the margin of error of the source.

3.2 Criteria for selecting sources

Since we have, potentially, lots of different ways to compute the same feature, the problem consists in selecting, at any time, the most reliable and plausible source of information. To this end, we define criteria that characterize both the quality of the source in general (relevance and trust), and the quality of a given information in particular (freshness and consistency). These criteria are used to compute a global *Confidence* for each information:

– **Relevance**: Is a given source of information well suited to measure a given feature?
– **Trust**: Did the source provide information that was considered as correct in a recent past?
– **Freshness**: Is the information considered as recent or out of date?
– **Consistency**: Is the information consistent with the previous values of the same source?

Relevance of the source Each sensor has been designed for a given purpose. But one sensor, which is very relevant to measure a given feature and used mainly in this way, may also be used, although in a less relevant manner, to measure another feature. This relevance is represented by a static percentage defined beforehand for each information source and each feature.

For example, to define the position of Ego, we can use either the GPS or the combination of values coming from a LiDAR (which provides the relative position of a vehicle A with respect to vehicle Ego) with the absolute position communicated by A, or make a prediction based on the last known position and speed of Ego. We can consider that the GPS is perfectly suited to the measurement of this feature, since it has been designed to this end. It can also be assumed that the combination of the relative and absolute positions of A is less suitable because of the potential errors during communication, and also because information received from A may be considered as less trustworthy. Finally, the prediction is a default choice when other sources of information are considered as faulty and should be rated as the least relevant source of information.

Relevance thus defines a partial order between the sources of information for each feature (100% being the most relevant) to favor specific sources of information with respect to others.

Trust in the source Trust in the source is a percentage that reflects the quality of the measurements provided by the source during a limited time window corresponding to a near past. When a source provides a measure that is considered as correct, the trust increases, and conversely it diminishes if the measure is considered incorrect, according to equation (1).

Trust in the source at iteration t, expressed as a percentage, depends on its value at iteration $t-1$ and on the distance between the tolerance interval of the value coming from the source (IT_s) and the tolerance interval of the value that has been selected (IT_r) from all possible sources for this feature (a tolerance is fixed for each feature). It is assumed that a penalty must be greater than a reward, in order to quickly detect a malfunction of a source or misleading information sent by a malicious vehicle. It is thus not necessary to rely on any reputation system: a new vehicle will be given at first a medium trust; if the information sent by the vehicle is coherent, the trust will quickly increase, but if it is not, the source will be strongly penalised and quickly discarded.

$$\begin{aligned} Trust_0 &= 100 \\ Trust_t &= \begin{cases} \min(100,\, Trust_{t-1} + \sigma^{++}) & \text{if } \; R \in IT_s \\ \min(100,\, Trust_{t-1} + \sigma^{+}) & \text{if } \; R \notin IT_s \text{ and } IT_r \cap IT_s \neq \emptyset \\ \max(0,\, Trust_{t-1} + \sigma^{-}) & \text{otherwise} \end{cases} \end{aligned} \tag{1}$$

with $\sigma^- < 0 < \sigma^+ < \sigma^{++}$ and $|\sigma^-| > |\sigma^{++}|$.

Freshness of information The sources of information are not synchronous. Each source produces features at its own pace, and each value is given a measure of freshness: a value that has just been received at the time of calculation has a freshness of 100%, a value that has an age that exceeds a threshold is considered out of date (see equation 2). We consider a fixed freshness for a time d, before a linear decay, according to a gradient a that may be variable depending on the feature.

$$Freshness(age) = \begin{cases} 100 & \text{if } \; age \leq d \\ 100 - a(age - d) & \text{otherwise} \end{cases} \tag{2}$$

To prevent the system from relying solely on its predictions, especially in the case where no reliable source is available, the prediction value is given a freshness, which is the age of the scene from which the prediction has been computed.

Consistency of information To ensure consistency between the various scenes selected at each moment t, we add a percentage that takes into account the predicted value val_p, the measured value val_m, and the margin of error $toleranceError_m$ associated with val_m. The predicted value is calculated from a bounded time window, using a linear regression over the values measured by a sensor. The distance between val_p and val_m is then calculated. If this distance is less than a certain threshold, a percentage associated with this distance is assigned, otherwise it is considered that this new measured value val_m is not consistent with the predicted value val_p:

$$Consistency = 200 - \frac{|val_p - val_m|}{toleranceError_m + 1} \cdot 100 \quad \text{with} \quad 0 \leq Consistency \leq 100 \tag{3}$$

Confidence Based on the four aforementioned criteria, we calculate a global measure of *Confidence* for each source of information according to the following formula:

$$Confidence = \frac{Relevance \cdot Trust \cdot Freshness \cdot Consistency}{100^4} \cdot 100 \tag{4}$$

3.3 The algorithm

At each iteration and for each feature, given the set of values provided for this feature by all the sources of information, the algorithm selects the unique value R in the following steps:

1. calculate, for each source, the value of the feature and a measure of *Confidence* in the value.
2. select, among all the sources, the one for which the *Confidence* in the value is the best and store the (plausible) value R of the selected source. In case of equality, we choose the source whose value is higher in the following order: *Relevance* > *Trust* > *Freshness*. In case no source of information has a *Confidence* above a predefined threshold ζ, the emergency stop is launched.
3. update the trust in all the sources, by attributing rewards or penalties, according to equation (1). This enables to quickly disregard faulty or malicious sources, but also to allow a source to have temporary failures (e.g. the GPS in a tunnel), without definitely blacklisting it. *Trust* in Prediction is a special case: it is given the trust value of the source selected at this iteration.

One may argue that some sources of information rely, for the calculation of a given feature, on the values of other features, which may create mutual dependencies between the different sources of information. To overcome this problem, if some required feature is not available yet, we can use instead the predicted value for this feature.

4 Implementation and experimentation

We did a large number of simulations using GAMA [18], a free and open-source agent-based simulation environment, with its "vehicleBehaviorExtension" [16], which we have enriched with a set of sensors. Using this framework, we implemented the plausibility algorithm described in this paper, as well as the decision algorithm proposed in [1]. We have also implemented a simplified version of the action module, which makes it possible to obtain flexible longitudinal and lateral trajectories.

The aim of the experimentation was to validate that the Ego vehicle could always maintain a coherent scene at any time, whatever the perturbations or attacks arising on the sensors. As a first step, we assumed that internal sensors could not be hacked, and that the only attacks could come from communications. We consider in our scenario the following anomalies:

- Noise: a random value in the range of the error margin [-δ,+δ] of the information source is added to the actual value;
- Breakdown: a source of information does not provide information at time t;
- Fault: the actual value is replaced by a random one.

Our test scene contains two vehicles (Ego and A). Ego has an initial speed of 35 m/s and is controlled by our decision algorithm. Vehicle A has only a V2V sensor, has an initial speed of 28 m/s, and is controlled by IDM (intelligent driving model) [20]. The road consists of two lanes with a length of 1 km. Both vehicles are on the same road lane, Ego behind A at some distance, so that Ego has to overtake A before the end of the lane.

Our algorithm uses a set of parameters, which have a direct impact on the performance of the system. For now, we did not achieved any parametric study but selected these values empirically, in order to obtain desired properties (e.g. the time after which a source is disregarded, or considered again after recovering). In the following, we quote the most important ones, with the corresponding values:

- the rewards and penalties σ^{++}, σ^{+}, σ^{-}, are set respectively to 25, 10 and -30. They have an impact on the time the system takes to eliminate a faulty source of information and to reconsider a previously eliminated source;
- the source filter threshold ζ =30%;
- the delay d and the gradient a a in the calculation of freshness: d is equal to the period of the sensor; we assume that this delay remains at 100% as long as the information is available in the period, while beyond this period, it decreases rapidly with gradient $a = 8$.

4.1 Results of experiments and discussion

We first studied the nominal case, i.e., the case with no faults except the noise associated with the sensors. Figure 1 represents the evolution of the selected values of the relative position of vehicle A with respect to Ego. It is very similar to that of actual values, confirming the choices that were made by the algorithm. The change of sources of information around 12k cycles corresponds to the loss of perception of the vehicle A during an overtaking. At first, A is seen by the front camera, then by the right camera, and finally by the rear camera.

We then inject targeted and random faults. Targeted injection aims at analyzing the ability of the solution to withstand potentially critical cases, while random injection tests the solution empirically.

Targeted fault injection Figure 2 shows the impact of fault injection to camera (1) (primary source) and camera (2) (secondary sensor). We injected two faults in each sensor, which consist in random values being provided by the sensors, in the intervals [500ms, 900ms] and [2100ms, 2800ms] for camera (1) and [750ms, 1050ms] and [1900ms, 2400ms] for camera (2). One may observe that the system rejects the faulty source as soon as the error is injected (camera (1) is rejected at time 500ms and camera (2) is rejected at time 750ms). The system selects a third source while waiting for the faulty sources to resume, which is the case for camera (1) at time 1900ms, 1s after the end of the first fault. At time 2100ms, camera (1) is rejected again as a second fault occurs, and since camera (2) is also faulty at that time, camera (3) resumes. Camera (2) resumes at time 3400ms and camera (1) resumes at time 3800ms, 1s after the end of their respective fault interval.

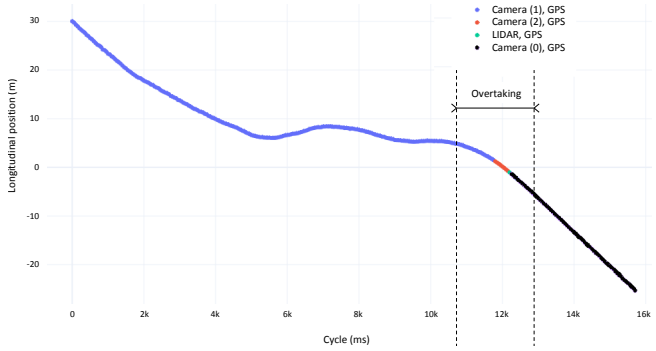

Fig. 1. Selected value R of relative position of vehicle A with respect to Ego: nominal case

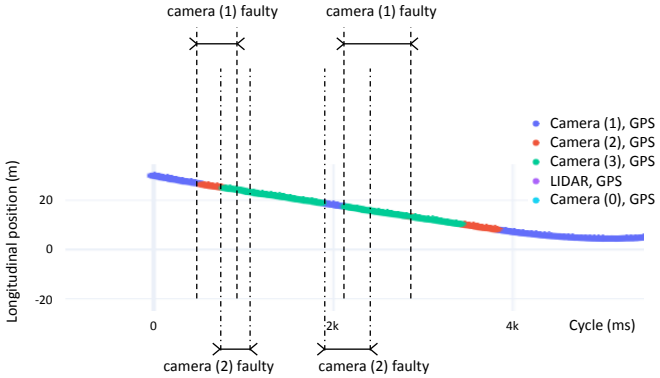

Fig. 2. Relative position of vehicle A wrt Ego: fault injection into camera (1) and camera (2)

Random fault injection In this configuration, we inject faults and failures at random times.

- For failures, which may occur at any time, we observe that if occurrence probability is under 50%, the system always manages to find a reliable source of information and that the number of switches increases proportionally to the probability of failure.
- For faults, which consist in random values appearing at random moments, if probability of occurrence is under 5% for each information source, we observe that the system always finds a reliable source and a value to select. Indeed, the frequency of injection is very low (on average two injections per second), which allows the system to penalize and then reward the source on average in two cycles. Similarly, since injections do not last long, trust is restored very quickly, and the system thus remains operating.

Limitations Although our proposal gives promising results in most situations, its operation is quite sensitive to the choice of parameters. It may happen for example that the system becomes unstable: when an incorrect value has once been selected, the system penalizes all sources of information that are giving correct values; therefore, once the fault injection phase is over, it cannot find a reliable source to select, either because of a low trust, or because of a low consistency.

This issue may be overcome by implementing several improvements to the method: the first one would be to compute the consistency of a feature with more elaborated methods than a simple linear regression. Kalman filters are good candidates since they would allow to take noise and errors into account; a second possible improvement is to also assess the consistency of the value of a feature with respect to the values provided by the other sources of information for the same feature; A third improvement would be, instead of selecting a single value as the most plausible one, to average the values of all the sources of information that appear to be consistent in the measure of the feature, which is common in the field and would limit the impact of incorrect values.

Finally, a parametric study is necessary in order to fine-tune the algorithm. By understanding precisely the role of each parameter, this will enable on the one hand to improve and stabilize the results, and on the other hand to give the user the choice between different driving options, all of which guaranteeing a safe behavior.

5 Conclusion and perspectives

The objective of this project was to design an algorithm to increase the robustness of the decision of an autonomous vehicle, taking into account the redundancy of the information collected by the sensors. To this end, we proposed a mechanism to select in real time, among the values coming from the various sensors, the most plausible ones to be used in the construction of the scene, in order to have the best possible decision making.

The approach is partially inspired by trust-based approaches, and is adapted to the particular context of our project and its constraints. This resulted in a hybrid model that analyzes the operation of sensors (or more generally sources of information), as well as the variation of the measured or computed values. This model takes into account the relevance of a source for a feature, the trust in the source, the freshness of the information and the consistency of the information in time.

In order to assess the validity of the proposal, we conducted an intensive campaign of experiments. Only a few results are presented in this article, but the model has demonstrated a highly satisfying behaviour and has met the expectations in a large range of conditions, either in the nominal case or in the presence of various forms of failures.

Some limitations have clearly been identified, but one of the main strength of the algorithm lies in its modular design, which enables a lot of adaptations and tuning for the computation of each of the four criteria. In the process of developing the algorithm, some parts of the model have deliberately been kept simple (and even naive) in a first step and the parameterization has been done very quickly and empirically. This was to validate the general principle of the computation of a global measure of confidence in the values provided by the various sources of information, and the selection of the most plausible one, without focusing on details of implementation or specific optimizations. Now that the approach has proved to be valid, we will concentrate on these details, notably to improve the computation of the consistency of the values.

References

1. J. Arcile, R. Devillers, and H. Klaudel. Verifcar: a framework for modeling and model checking communicating autonomous vehicles. *Autonomous Agents and Multi-Agent Systems*, 33(3):353–381, 2019.
2. F. Arena and G. Pau. An overview of vehicular communications. *Future Internet*, 11(2):27, 2019.
3. P. Bentley and S. L. Lim. Fault tolerant fusion of office sensor data using cartesian genetic programming. In *IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1–8, 11 2017.

4. T. Bhuiyan, A. Josang, and Y. Xu. Trust and reputation management in web-based social network. *Web Intelligence and Intelligent Agents*, pages 207–232, 2010.
5. Federico Castanedo. A review of data fusion techniques. *TheScientificWorldJournal*, 2013:704504, 10 2013.
6. B. V. Dasarathy. Sensor fusion potential exploitation-innovative architectures and illustrative applications. *Proceedings of the IEEE*, 85(1):24–38, 1997.
7. A. P. Dempster. A generalization of bayesian inference. *Journal of the Royal Statistical Society: Series B (Methodological)*, 30(2):205–232, 1968.
8. F. Došilović, M. Brcic, and N. Hlupic. Explainable artificial intelligence: A survey. In *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 05 2018.
9. T. Frey, C. Aguilar, K. Engebretson, D. Faulk, and L. Lenning. F-35 information fusion. In *Aviation Technology, Integration, and Operations Conference*, 06 2018.
10. J. Granatyr, V. Botelho, O. R. Lessing, E. E. Scalabrin, J.-P. Barthès, and F. Enembreck. Trust and reputation models for multiagent systems. *ACM Computing Surveys (CSUR)*, 48(2):27, 2015.
11. W. Jiang, B. Wei, X. Qin, J. Zhan, and Y. Tang. Sensor data fusion based on a new conflict measure. *Mathematical Problems in Engineering*, 2016:5769061, 01 2016.
12. K. Jo, J. Kim, D. Kim, C. Jang, and M. Sunwoo. Development of autonomous car—part i: Distributed system architecture and development process. *IEEE Transactions on Industrial Electronics*, 61(12):7131–7140, 2014.
13. K. Kolanowski, A. Świetlicka, R. Kapela, J. Pochmara, and A. Rybarczyk. Multisensor data fusion using elman neural networks. *Applied Mathematics and Computation*, 319:236–244, 2018.
14. S. Majumder and D. K. Pratihar. Multi-sensors data fusion through fuzzy clustering and predictive tools. *Expert Systems with Applications*, 107:165–172, 2018.
15. D. B. Rubin. Bayesian inference for causal effects: The role of randomization. *The Annals of statistics*, 6(1):34–58, 1978.
16. J. Sobieraj. *Méthodes et outils pour la conception de Systèmes de Transport Intelligents Coopératifs*. PhD thesis, Université Paris-Saclay, 2018.
17. S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. K. Khan, and S. Goudarzi. A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. *IEEE Access*, 5:15619–15629, 2017.
18. P. Taillandier, B. Gaudou, A. Grignard, Q. Huynh, N. Marilleau, P. Caillou, D. Philippon, and A. Drogoul. Building, composing and experimenting complex spatial models with the gama platform. *GeoInformatica*, 23(2):299–322, 2019.
19. C. N. Taylor and A. N. Bishop. Homogeneous functionals and bayesian data fusion with unknown correlation. *Information Fusion*, 45:179–189, 2019.
20. M. Treiber, A. Hennecke, and D. Helbing. Congested traffic states in empirical observations and microscopic simulations. *Physical review E*, 62(2):1805, 2000.
21. C. Yan, W. Xu, and J. Liu. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *DEF CON*, 24, 2016.
22. J. Zhang. A survey on trust management for vanets. In *2011 IEEE International Conference on Advanced Information Networking and Applications*, pages 105–112. IEEE, 2011.