Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 184 (2021) 156–163

Procedia Computer Science

www.elsevier.com/locate/procedia

The 12th International Conference on Ambient Systems, Networks and Technologies (ANT)
March 23 - 26, 2021, Warsaw, Poland

Conceptual design of a trust model for perceptual sensor data of autonomous vehicles

Lauri Halla-aho*, Ethiopia Nigussie, Jouni Isoaho

University of Turku, Vesilinnantie 5, 20014 Turun yliopisto, Finland

Abstract

This paper presents a conceptual trust model for the perceptual sensor data of autonomous vehicles to improve their reliability and safety of operation. In particular, the model aims to ensure the trustworthiness of the data used in the automated decision-making processes of vehicles. The presented model forms a comprehensive view of factors that affect trust in the perceptual sensor data. These factors, namely environment, operation, security, and technical limitations, further cover a number of related trust parameters used to evaluate trust values. Each parameter is evaluated using Dempster-Shafer theory using a trust-distrust frame. Mass values are based on instantaneous sensor data and sensor behaviour tested under similar circumstances. As a result, this model is viable for use in conjunction with data fusion and decision-making to improve their reliability by enabling the tracking of the development of sensor trustworthiness.

Keywords: Trust model; autonomous vehicle; perceptual sensor; data reliability; Dempster-Shafer theory

1. Introduction

Autonomous driving is getting closer to reality thanks to technological advancements on various fronts. Accurate perception of the surrounding environment, through the use of camera, radar, lidar, and other sensors, is one of the key requirements for safe and reliable autonomous driving. Based on perception, path planning and appropriate actuation are done to steer the car safely without endangering other actors in traffic. Faults and errors in perceptual sensors, as well as their sub-standard operation due to unfavourable environmental conditions, may affect the reliability of their data, impacting the accuracy of object detection, which may result in collisions. To minimise such a risk, various hardware- and software-based solutions are under development by the scientific and industrial communities [3, 9, 10]. Evaluating the trustworthiness of the data of perceptual sensors is among the solutions that allow enforcing proactive

* Corresponding author.
E-mail address: lauri.m.halla-aho@utu.fi

10.1016/j.procs.2021.04.002

measures for mitigating the consequences of data uncertainties. In this work, the conceptual design of a trust model for evaluating the trustworthiness of perceptual sensors data at real-time is presented.

Previous research into the topic of data trust in autonomous vehicles (AVs), while limited, has focused on vehicular ad hoc networks (VANETs), and the trust associated with vehicle-to-vehicle communication. The model discussed by Sun, Li, and Gerdes [8] accounts for potentially malicious peers in a VANET. In their model, the behaviour of other vehicles is compared to how they report themselves to be acting. They assume the ego vehicle, alongside at least a single neighbouring vehicle, to be trustworthy. They use an extended Kalman filter to predict the movement of the vehicles using local measurements and received state information to detect falsified inputs. Rosenstatter and Englund [5] proposed a method for modelling trust in the ego vehicle and its peers in traffic using a limited set of variables, focusing on position, distance, and movement. They identified sensor quality, environment, and vehicle behaviour as the main factors which affect the decision-making process of a vehicle. These factors are represented by trust indices, which are combined into an overall trust index.

The focus of this work is on determining the trustworthiness of onboard perceptual sensors such as radars, lidars, and cameras, during the operation of a heavy-duty autonomous vehicle. In particular, our interest lies on accounting for all factors that can affect the reliability of sensor data. The resulting model is currently conceptual and is built for compatibility with utilised hardware. Consequently, the main contributions of this paper are:

- A holistic approach to understanding factors, which impact the trustworthiness of data of vehicular perceptual sensors, and
- A novel conceptual trust model for perceptual sensor data.

This paper is organised as follows: the motivation behind and context of this paper is described in section 2, followed by term definitions and detail for the trust model in section 3. Use of the model in conjunction with autonomous vehicle decision-making is discussed in section 4, and finally the concluding remarks are given in section 5.

2. Motivation

The decision-making process is a critical part of the functionality of autonomous vehicles and ensuring its reliability, trustworthiness, and low latency of operation are thus vital for them to become viable for regular road use. In order to achieve autonomy at levels three or above, an AV requires a suitable perceptual sensor coverage, efficient object classification and tracking solutions, an accurate data fusion method, as well as a robust set of backup systems in cases of malfunction. If the aforementioned requirements are not met, the risk of accidents increases. In the worst-case scenarios, they can even lead to fatalities, such as in the case of the autonomous vehicle tested by Uber [2]. In this case the tested vehicle was not equipped with enough sensors to ensure a full coverage of its surroundings, leaving it with blind angles. Additionally, the object classification systems were unable to accurately determine the type of the object, a pedestrian, and mistook it for a vehicle and a bicyclist.

The model proposed in this paper aims to provide a holistic view of the system and its operation, focusing on factors that can alter it and negatively affect its output. The project uses a heavy-duty truck as the vehicle for which the discussed systems are developed, albeit initially as an aid for the driver. The utilised sensors include radars, lidars, and cameras, which are combined with data fusion to form a unified situational view of the surroundings of the vehicle. In order to evaluate the instantaneous negative effects due to the applicable operational circumstances the system is subjected to, the trust model is used in conjunction with the data fusion to provide additional information about data trustworthiness. In figure 1, the major steps of onboard data processing are shown.

The trust model is meant to act as an aide to the driver, as well as a part of an eventually automated decision-making process, and alert them when the perceptual subsystem is behaving unusually and its output, whether partially or entirely, is subjected to doubt. Additionally, its evaluations are used during data fusion to adjust the influence of individual sensors if they have been deemed to produce unreliable data. Its two main purposes are to perform these trustworthiness evaluations with latencies as low as reasonably achievable, and to enable reliable low-latency decision-making based on incomplete or uncertain information. The former is vital to ensure the decision-making processes and the driver have as up-to-date information available to them as possible, allowing them to react more efficiently to detected issues. On the other hand, the latter emphasises the difficulty in producing an accurate, all-encompassing

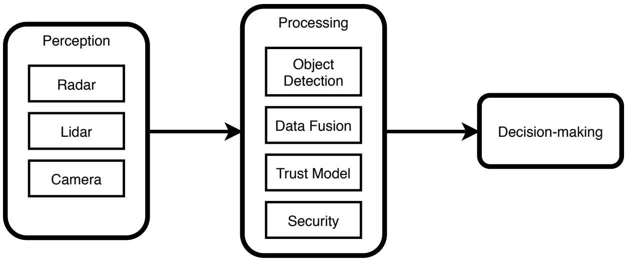

Fig. 1: A simplified representation of the three stages of data management in a heavy-duty truck.

situational view at every instant using available technology. It can be assumed that some information will remain unattainable, e.g. due to a lack of suitable sensors or inaccuracies in measurements, and thus autonomous vehicles must be able to make safe decisions based on partial data.

3. Trust model

3.1. Trust terminology

Trust as a concept has multiple definitions depending on the area of its application. As such, it is important to define the term in the context of this paper. In particular, *trust*, *mistrust*, and *distrust* are key terms and thus require definition. Further, the two main applications for the concept are trust in the data sources and trust in the data received from those sources.

Trust is the belief of a *truster* and expectation of the actions or behaviour of someone or something, a *trustee*, to be truthful or reliable. In particular, the actions of the trustee can be assumed to be intended as benevolent or neutral in nature towards the truster. When used in conjunction with sources and data, this translates to the assumption that they measure their actual environment. Mistrust and distrust, as discussed by Marsh and Dibben [1], are two types of trust that are dependent on the relationship between the truster and the trustee. Mistrust occurs whenever trust in someone or something is betrayed. This betrayal is not necessarily intentional but means that the affected trust was placed on a faulty basis. On the other hand, distrust is a form of negative trust in which the truster believes the trustee to be actively and intentionally acting against the interests of the truster.

As such, a *trusted source* is one that has not been negatively influenced by malicious actors or the environment. It can then be assumed to produce detections which are as close to the objective truth as technically attainable. The aforementioned data sources, in the scope of this paper, include the perceptual sensors discussed previously; environmental sensors, such as thermometers and GPS; as well as external sources including roadside units and other vehicles. In particular, the proposed model focuses on the internal sources and disregards the potential external nature of some sources. A vehicle uses the data from its sensors to plan its route by predicting the behaviours of the surrounding objects and attempting to avoid collisions. In certain scenarios, the vehicles are capable of forming VANETs and share their information with neighbouring vehicles to mutually improve the reliability and accuracy of their decision-making. Such information can contain, inter alia, sudden changes in the flow of traffic and upcoming obstructions. When partaking in VANET communication, be it between vehicles or with a roadside unit, the trustworthiness of the communication partners should also be evaluated through applicable means [12].

Trusted data, on the other hand, are detections or measurements perceived to highly likely be accurate and have retained their integrity. They can be safely used in decision-making without risking the safety of the vehicle. For a detection to be classified as trustworthy, its source must be trusted and known to produce reliable detections in identical conditions. Additionally, the data are more trustworthy if neighbouring trusted sources are able to confirm the presence of the detected objects. *Mistrusted data* are data that were initially estimated to be trustworthy but, with later detections or analysis, are found to have been incorrect. These data could have been received from a source that has degraded during operation or the operational environment of which has become sub-optimal. Alternatively, a malicious third party could have modified or forged the data in an attempt to compromise the safety of the vehicle. If a data source repeatedly outputs mistrusted data or is detected to be an active attacker, it is classified as a distrusted source. Additionally, a source that systematically produces uncorroborated data can be assumed to be an untrustworthy source. Such sources are assumed to only produce unreliable or corrupted data. As a result, one of the goals to achieve reliable autonomous decision-making is to minimise the number of mistrust events.

3.2. Factors affecting sensor data trustworthiness

In order to determine the state of the trustworthiness of the vehicle, this model assumes each sensor can be compromised and produce unreliable data. They are subjected to their environment as well as external factors that affect their performance and the data they output. The primary factors identified in this model are *environment*, *operation*, *security*, and *technical limitation*. It is important to map the effects of these factors on the data and develop a reliable method of evaluating trust in them based on that knowledge.

The sensors are directly affected by their operating environment. This covers the amount of available light, the external temperature, and the various types of weather capable of hindering their performance. While some sensors are not susceptible to changes in the lighting conditions, lidars and cameras, especially, are reliant on the amount of background light or the overall brightness of the environment in order to produce reliable and high-resolution images. For lidars, negative effects are caused by false positive detections due to light pollution that overlaps with the portion of the light spectrum they use. Cameras, on the other hand, require an adequate amount of light to produce good quality images that can be used for object detections. This applies, albeit to a lesser extent, also to cameras utilising light outside the visible spectrum, such as infrared cameras. Temperature and weather can be interpreted as two intertwined parameters but here the latter focuses solely on the effects on visibility. These effects can be physically direct, e.g. lens obstruction via snow, mud, or frost, or indirect, i.e., reduced viewable area without direct contact, as is the case during foggy conditions or rain. Due to the complexity of different weather conditions, and limitations on available onboard weather sensors, an approximation based on the information obtainable from these sensors has to be used. Temperature considerations account for both internal, where allowed by the utilised equipment, and external temperatures. Operating outside of the nominal temperature range of a sensor can affect the performance of its onboard processing as well as its detector components.

The operational factor encompasses three aspects of the operation of the sensors that are important for trust evaluation. They are object continuity, supporting detections, and component wear. Object continuity is a measure of the accuracy of the previous detections of a sensor. If the actual future position of a tracked object continuously differs significantly from its predicted position based on the prior detection, the sensor is likely to suffer from a systematic error or be compromised. In the cases of vehicles equipped with sensors with at least partially overlapping fields of view, detections from such sensors can benefit from the support of shared detections. In this manner, detections of a sensor can be confirmed to be trustworthy even if their continuity is found wanting. The sensors wear down slowly during their lifetime, increasing the likelihood of mechanical failure and unreliable detections. This occurs e.g., due to their exposure to the elements, vibrations from the road, and regular use. Component wear can then occur both gradually and spontaneously, making modelling it accurately challenging. In practice, it is a function of a number of factors, including total usage time and environments in which the device has been used. However, due to the slow pace at which the state of wear of the sensor changes, when a suitable model has been developed for the wear, it is enough to only evaluate the state for the sensors periodically.

As the vehicles in question in this paper are designed to operate autonomously, their cyber security should be among the topmost concerns. As a result, the integrity of the systems and data should be ensured. In order to sufficiently secure the vehicle, attacks should be reliably detected and prevented, and the used data should only be modified by authorised processes. As previously discussed, novel networked vehicles are susceptible to a plethora of new types of vulnerabilities that conventional vehicles did not have to account for in their design. It is then advisable to incorporate defensive systems, such as firewalls and intrusion detection systems, against these cyber security threats onboard autonomous vehicles. These systems can be used to signal the trust model whenever the trustworthiness of a data source could be affected by a detected attack or issue.

Finally, technical limitations of the sensors must be considered when the trustworthiness of their data is evaluated. Common limitations across the sensors used in this project have been identified as the tracking capacity, field of view, and object motion detection. Sensors operating within object-rich environments can reach the limit of their object tracking capacity. In these cases, the probability of failing to detect a vital piece of information increases as the maximum tracking capability decreases. In addition to the tracking of the locations of objects, their detected speeds can be erroneous if the relative velocity of the vehicle and the object exceeds the maximum measurement of the sensor.

Similarly, the reliability of detections within certain sections of its field of view, e.g. close to the sensor or near the extremities of the view, can be lower. Information about the above technical limitations are ideally provided by the manufacturer but can be empirically tested for each sensor model.

The previous limitations are based on the design of the components and, as such, can be assumed to be identical across components of the same model and manufacturer. However, these limitations do not account for variations in each individual component caused e.g. by minor defects in the silicon or changes in the quality of their parts. These fluctuations are unpredictable and, due to their randomness, practically irreproducible. To counter their effects on the reliability of specific instances of equipment, they must be individually tested and calibrated to perform as expected. These factors and their respective parameters are enumerated in table 1. A summarised rationale is provided for each of the parameters as well as a distrust mass (DM). The DM values are used as a measure of distrust in the measurements and are consequently used in the trust evaluation of the sensors and data, as discussed in 3.3. The p-values under the DM-column represent parameter-specific distrust constants.

Table 1: A summary of trust parameters used in this model. Distrust masses determined through empirical testing are given a list of their factors.

Factor	Parameter	Rationale	Distrust mass
Environment	Luminosity	The performance of some sensors, e.g. cameras, is affected by the amount of available light.	p_L if $L \notin [L_{min}, L_{max}]$
	Temperature	Sensors are not guaranteed to operate nominally outside their designed environmental temperature range, reducing the reliability of their detections.	p_T if $T \notin [T_{min}, T_{max}]$
	Weather	Various weather types affect the performance of sensors by impairing their vision or reducing the visibility.	$f(sensor, weather)$
Operation	Continuity	Reliable prediction of the future positions of objects rely on accurate detections.	$Err(r_{pred}) + Err(\theta_{pred})$
	Support	Detections supported by other sensors can be deemed more reliable than those only detected by a single sensor.	$\frac{supporting\ sensors}{neighbouring\ sensors}$
	Wear	Prolonged use and exposure to environment gradually degrades sensors, increasing their probability of malfunctioning and producing unreliable detections.	$f(time, environment)$
Security	Integrity	Sources and data can be subjected to e.g. tampering or interference, reducing data reliability. Decision-making can be also affected by interference in communication between sensors and onboard processing.	$f(severity)$
	Detected attacks	Information about attacks against the system or specific sensors can be used to refine the trust in the affected components. This requires onboard security solutions to act as a source of information about suspicious behaviour.	$f(attack\,type)$
Technical limitations	Capacity	Sensors operating at their maximum tracking capacity are capable of failing to detect important objects.	p_{TC} if $n_{max} < n$
	Field of view	Certain types of sensors have blind sections or less reliable areas in their field of view. This usually affects detections close to the sensor or close to the edge of its view.	$p_{FoV,r}$ if $r \notin [r_{min}, r_{max}]$, $p_{FoV,\theta}$ if $\theta \notin [\theta_{min}, \theta_{max}]$
	Motion	Measuring the movement of objects is often restricted e.g. by limits on the byte sizes of data points, lowering their maximum magnitude and resolution.	$\Delta r + \Delta\theta + \Delta v$

3.3. Trust evaluation for sensor and data

This model covers the data available from radars, lidars, and cameras, such as object locations and relative radial speeds. Additional, model- and make-dependent information such as signal strength or confidence can be used to further refine the evaluation. As discussed in section 2, the camera feed is pre-processed, e.g. with YOLOv3 [4], to extract appropriate visual information. As a result, the attributes of interest in the detections are the locations and velocities of the objects relative to the vehicle.

The Dempster-Shafer Theory (DST) [6] is used as tool to evaluate the trustworthiness of the system and data by treating each parameter as a piece of evidence. DST provides a method for representing different degrees of belief and plausibility for sets of possible options, contained in a superset called a *frame of discernment* Θ. A collection of subjective probabilities, known as *masses* m, assigned for each of the subsets of the superset is called a piece of *evidence*. Via a combination of these pieces of evidence, DST enables the discernment of the most likely correct option. The theory is augmented with the second Proportional Conflict Redistribution (PCR2) -combination rule introduced by Dezert and Smarandache [7]. PCR2 was chosen due to its perceived accuracy in redistributing conflicted weight, as well as its low impact on overall system latency. This rule removes the counter-intuitive behaviour of DST when heavily conflicting evidence are combined [11]. Using PCR2, the combination of two pieces of evidence occurs as follows for each of the masses:

$$m_{PCR2}(X) = m_{12}(X) + C(X)\frac{c_{12}(X)}{e_{12}}, X \in \Theta, \tag{1}$$

where $m_{12}(X)$ is the conjunction sum for the subset of Θ denoted X; $C(X)$ is 1 if X is participating in a conflict, i.e. there is another subset Y with a non-zero mass such that $X \cap Y = \emptyset$ and $m(X \cap Y) > 0$ and 0 otherwise; $c_{12}(X)$ the sum of the masses corresponding to X in the two original pieces of evidence; and e_{12} the sum of the masses of all conflicted subsets. The used frame of discernment is $\Theta = \{T, D\}$, where T and D denote trust and distrust values, respectively. Distrust, as defined in subsection 3.1, is a form of negative trust and thus D is a notation for $\neg T$. When used as a term for the calculation of the masses of belief assignments, Θ can be used as a substitute for untrust.

The system starts in complete untrust, i.e. initially $m(\Theta) = 1$. Each consecutive message received by the trust model module is evaluated against applicable trust parameters, as listed in table 1. For each evaluated parameter, an applicable piece of trust evidence, as shown in table 2, is used. In the table, the τ constant represents the trust mass given to data that is assumed to be trustworthy.

Table 2: Pieces of evidence used with evaluated parameters.

	$m(T)$	$m(D)$	$m(\Theta)$
Trustworthy	τ	0	$1 - \tau$
Untrustworthy	0	DM	1 – DM

If the data contained in a message is found untrustworthy for a parameter, the latter evidence is used. The DM specified for each affected parameter is used. It estimates the increased probability of data being erroneous based on the operating conditions. As an example, for location and velocity information received from radars a DM could be, as suggested in table 1, DM(motion) = $\Delta r + \Delta\theta + \Delta v$, where Δr, $\Delta\theta$, and Δv_r stand for the relative changes in detected distance, angle, and radial velocity, respectively, between consecutive detections. These are chosen to reflect the expectation of the objects to retain most of their momentum. However, this approach can produce misleading results e.g. if the preceding vehicle brakes unexpectedly, causing a large change in the velocity. This could be mitigated by, for example, the detection of brake lights on the preceding vehicle during the camera feed processing. Detected brake lights can then be included in the distrust mass by adding a Boolean coefficient to the velocity change component. Step functions are recommended for use with distrust masses for parameters which have well-defined limits, such as operating temperatures or sensor detection capabilities.

Due to the nature of DST and PCR2 calculations, the fluctuations of trust evaluations are strongly dependent on the number of used sensors. The positive trust introduced by detections supported by multiple sensors is stronger the more the coverage of used sensors overlaps. Additionally, relative changes in motion are exaggerated for objects that are stationary or moving slowly. This effect can be attenuated with the use of minimum thresholds for the changes. For example, setting a minimum multiple of the resolution of the detection capability of the sensor as a requirement would alleviate the fluctuations if the object is barely moving.

Example 1. Let us assume the current state of a trust evaluation of a detection is $m_0 = [0.83, 0.07, 0.10]$ and the evaluation of the motion of the object has resulted in $m_1 = [0, 0.23, 0.77]$. The calculation steps are shown below in table 3, including the conflicted combination and the result after applying PCR2.

Table 3: Example trust evaluation.

	m_0	m_1	$m_0 + m_1$	$(m_0 + m_1)_{PCR2}$
$m(T)$	0.83	0	0.64	0.78
$m(D)$	0.07	0.23	0.09	0.14
$m(\Theta)$	0.10	0.77	0.08	0.08

4. Role of the trust model in decision-making

One of the main benefits of the trust model introduced in this paper is the suitability of its output in multiple different phases of onboard data processing. This benefits the system by allowing its modules to increase redundancy by monitoring and reacting to the trust evaluations at multiple stages, such as data fusion and decision-making, while making it possible to simultaneously track the performance of the model itself and adjust the DMs accordingly. Alternatively, the evaluations could be used for specialised functionalities which do not require the full output of the model. The envisioned system overview of the PRYSTINE truck focused on in this paper is shown below in figure 2. The data flow from perceptual sensors is displayed with a bold arrow.

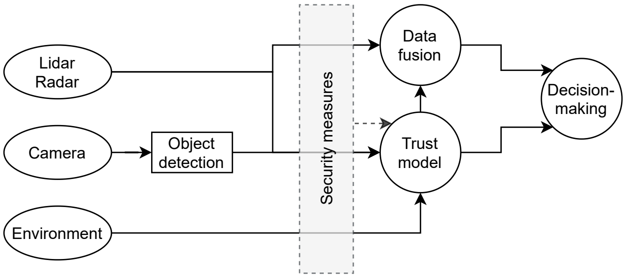

Fig. 2: An illustration of the data flow for the decision-making process on the PRYSTINE truck.

The trust evaluations performed by the trust model can be used to provide warnings to the driver, modify the impact distrusted sensors have on the fused perceptual data, or, if severely distrusted, to directly inform autonomous decision-making processes about potential issues within the system. It can then enhance the decision-making process at multiple stages of the operation of the vehicle. However, in order to use the evaluations in practice, trust thresholds must be defined between trustworthy and untrustworthy operation. The trust ranges corresponding to these modes of operation depend on the used distrust masses. As a result, empirical testing should be done to optimise these ranges corresponding to regular operation, partial unreliability, and likely malfunction, respectively.

Albeit the above three-state approximation lacks the detail of the raw evaluations, it is an easier approach for informing the driver of potential issues in a manner that distracts them as little as possible. It enables active and passive monitoring of the trustworthiness of the vehicle, and aids in the detection of potential issues which could cause a loss of trust. This applies both to strong short-term distrust as well as gradual decrease in trust over longer periods of time. The former case applies e.g. when an important sensor suffers a malfunction that permanently hinders its ability to detect objects while the truck is moving, and the latter is an indicator of gradual component wear.

5. Conclusion

In this work, conceptual design of a trust model of perceptual sensor data was presented. The model expands on earlier trust models proposed for autonomous vehicles. This model is novel in its approach to evaluate trust in the data by forming a holistic view of factors affecting the perceptual subsystem of the vehicle. Through mapping all the major factors that can affect the operation and reliability of perceptual sensors, and consequently tracking them, it is possible to form a comprehensive estimation of the instantaneous trustworthiness of produced data.

The trust-affecting parameters identified in this model were categorised under four major factors: environment, operation, security, and technical limitations. Environmental parameters evaluate the behaviour of the sensors under various visibility and weather conditions. Operational parameters evaluate their performance during normal operation of the vehicle with metrics such as the consistency of detections and support from other sensors. Onboard security measures are used to detect and prevent attacks and to inform the trust model module about potential corruption in the data. Finally, the technical limitations of the used sensors are known and used to evaluate the trustworthiness of the data e.g. with respect to their location and motion.

These parameters are evaluated as distrust masses and used in a trust evaluation based on the Dempster-Shafer theory. The masses of trust and distrust are determined for each parameter based on data points available from sensor detections, previous predictions, or alerts from used security measures. The used approach enables evaluating the trust while ensuring the incurred delay in the data processing remains low. It also allows for estimating system reliability when all of the required information is not readily available, such as in the cases of malfunction or disturbances in operation. Combined, these will enhance the safety and reliability of autonomous vehicles by ensuring continuous trust evaluation for the benefit of onboard decision-making.

Acknowledgements

This work was supported by the PRYSTINE Project, funded by Electronic Components and Systems for European Leadership Joint Undertaking (ECSEL JU) in collaboration with the European Union's H2020 Framework Programme and National Authorities, under grant agreement no. 783190.

References

[1] Marsh, S., Dibben, M.R., 2005. Trust, Untrust, Distrust and Mistrust – An Exploration of the Dark(er) Side, in: Herrmann, P., Issarny, V., Shiu, S. (Eds.), Trust Management, Springer Berlin Heidelberg, Berlin, Heidelberg. pp. 17–33.

[2] Nathional Transportation Safety Board, 2018. Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian, Tempe, Arizona, March 18, 2018. Accident Report NTSB/HAR-19/03, NTSB, Washington, D.C.

[3] Pous, N., Gingras, D., Gruyer, D., 2017. Intelligent vehicle embedded sensors fault detection and isolation using analytical redundancy and nonlinear transformations. Journal of Control Science and Engineering 2017.

[4] Redmon, J., Farhadi, A., 2018. Yolov3: An incremental improvement. arXiv:1804.02767.

[5] Rosenstatter, T., Englund, C., 2018. Modelling the level of trust in a cooperative automated vehicle control system. IEEE Transactions on Intelligent Transportation Systems 19, 1237–1247. doi:10.1109/TITS.2017.2749962.

[6] Shafer, G., 1976. A Mathematical Theory of Evidence. Princeton University Press, Princeton, NJ.

[7] Smarandache, F., Dezert, J., 2005. Information fusion based on new proportional conflict redistribution rules, in: 2005 7th International Conference on Information Fusion, pp. 907–914. doi:10.1109/ICIF.2005.1591955.

[8] Sun, M., Li, M., Gerdes, R., 2017. A data trust framework for VANETs enabling false data detection and secure vehicle tracking, in: 2017 IEEE Conference on Communications and Network Security (CNS), pp. 1–9. doi:10.1109/CNS.2017.8228654.

[9] Van Brummelen, J., O'Brien, M., Gruyer, D., Najjaran, H., 2018. Autonomous vehicle perception: The technology of today and tomorrow. Transportation research part C: emerging technologies 89, 384–406.

[10] Van Wyk, F., Wang, Y., Khojandi, A., Masoud, N., 2019. Real-time sensor anomaly detection and identification in automated vehicles. IEEE Transactions on Intelligent Transportation Systems 21, 1264–1276.

[11] Zadeh, L., 1979. On the validity of Dempster's rule of combination. Memo M 79/24, University of California, Berkeley.

[12] Zeadally, S., Hunt, R., Chen, Y.s., Irwin, A., Hassan, A., 2012. Vehicular ad hoc networks (vanets): status, results, and challenges. Telecommunication Systems 50, 217–241. Copyright - Springer Science+Business Media New York 2012; Last updated - 2020-11-17.