Quality and Trust Indicators of Digital Road Infrastructure Data Are Essential to Improve Its Usability: An Intelligent Speed Assist (ISA) Study

Jacco van de Sluis[1][a], Daniel Altgassen[2][b] and Peter-Paul Schackmann[1]
[1]*Networks department, TNO - ICT, Strategy & Policy, The Hague, The Netherlands*
[2]*Integrated Vehicle Safety Department, TNO - Mobility & Build Environment, Helmond, The Netherlands*

Keywords: Intelligent Speed Assist (ISA), Misbehaviour Detection and Reporting (MBD&R), Digital Road Infrastructure (DRI), Vehicle-to-Everything (V2X) Communication, Intelligent Transport Systems (ITS), Data Trust, Data Quality, Cooperative Connected and Automated Mobility (CCAM), Advanced Driver Assistance System (ADAS), Automated Driving System (ADS).

Abstract: The promise of a Digital Road Infrastructure (DRI) is to improve both road and vehicle safety. ADAS/ADS with DRI support, can help vehicles in overcoming certain sensor limitations, handle more complex operational situations and offer additional situational awareness. An effective DRI must be trusted and must offer the required data quality, both are currently lacking. Intelligent Speed Assist (ISA) is an interesting show case for the added value of DRI. In our approach camera-based traffic sign detections and map-based speed limit information, both occasionally wrong, are augmented with actual speed limit and road layout information coming from DRI. A Misbehaviour Detection and Reporting (MBD&R) concept tailored to the ISA sources is deployed in the vehicle to detect and report ISA related misbehaviour. Trust and quality indicators are calculated for data coming from camera, map and DRI, which are used to verify and compare theses sources and make improved ISA speed limit decisions. The vehicle implementation is tested under real-life traffic conditions. Our work is a first step in realizing a trusted DRI. The long-term goal is collaboration among all stakeholders to implement mechanisms that improve trust and the quality of shared data sources for use in traffic safety applications.

1 INTRODUCTION

Connected, Cooperative, and Automated Mobility (CCAM) applications can improve the performance of existing Advanced Driver Assistance Systems (ADAS) / Automated Driving Systems (ADS). These new data-driven services enabled by connectivity can increase vehicle intelligence, achieve higher levels of automation and improve safety, see reports from (Farah et al., 2018) and (OECD, 2023). But to work in practice, a trusted and shared Digital Road Infrastructure (DRI) is essential. With numerous components required to make this possible, it is crucial that vehicle OEMs, industry partners, service providers, and road operators collaborate to enhance both road and vehicle safety. An effective DRI offers trusted sources and offers the required data quality, both of which are currently lacking. As our mobility system prepares for vehicles with higher levels of automation, the need for a reliable DRI increases. Information generated by road operators, road users or other data providers - and shared with specific road users - can greatly contribute to that goal. From a vehicle perspective, using external data, on top of the vehicles' own sensor data can significantly extend the vehicle operational horizon and thereby improve vehicle safety (Zhang et al., 2022). Despite DRI potential benefits, the usability of external digital data for safety applications is low, due to concerns about reliability (quality and trust) and possible misbehaviours, see (van der Heijden et al., 2019) and (Kamel et al., 2020). Also road operators and data providers are unsure of the specific data requirements needed and how to provide these. To move forward, cross-chain collaboration between all stakeholders is required, as well as proof that quality and trust issues can be resolved. This paper uses the Intelligent Speed Assist (ISA) as study case to fur-

[a] https://orcid.org/0000-0002-7162-6014
[b] https://orcid.org/0009-0003-2813-0499

van de Sluis, J., Altgassen, D. and Schackmann, P.-P.
Quality and Trust Indicators of Digital Road Infrastructure Data Are Essential to Improve Its Usability: An Intelligent Speed Assist (ISA) Study.
DOI: 10.5220/0013470100003941

In *Proceedings of the 11th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2025)*, pages 631-637
ISBN: 978-989-758-745-0; ISSN: 2184-495X

ther describe the challenges and to introduce possible solutions.

2 IMPROVING SHARED DATA USABILITY FOR ISA

Real-time traffic information data is often only used to inform drivers. In these systems, the driver is responsible for safe driving behavior and occasional misinformation is of lesser criticality, as it is handled by human interpretations. The urgency to decrease misinformation has recently grown, as the same data is now also being used for traffic and road safety applications, such as usage in ADAS. This development increases the importance of the detection of misbehaviour and having a real-time measure for data quality and data trust. To properly scale ADAS and achieve higher levels of automation, relying solely on ego vehicle sensor data is challenging. Especially when operational design domains extend and become more complex, e.g. by covering (sub)urban environments, diverse road and weather conditions. Current ISA vehicle implementations often use a camera to recognize speed limit signs, combined with map data to determine the applicable speed limit. However, camera-based detection can have (limitation) signs that are obstructed, misinterpreted, or affected by weather conditions. Additionally, map data can be inaccurate, insufficiently detailed (e.g. missing information related to: time-of-day, vehicle-type, weather conditions), or outdated. These sensor and map flaws can lead to unsafe situations, such as speeding or unexpected braking, especially when used by automated vehicle systems. The EU 2019/2144 ISA regulation (EC, 2023) makes ISA mandatory in new vehicles. It does not constrain manufacturers by specifying which sources to use for speed limit data, but it outlines performance requirements and implementation possibilities. The additional use of digital road infrastructure (DRI) data can provide the technical solution to achieve the required ISA performance.

2.1 Misbehaviour Detection

But with increased connectivity, cyber-security becomes more apparent. Cyber-attacks and misbehaviour are not limited to the connected vehicles, they need to be considered within the full CCAM ecosystem. The ISA use case is a complex example of a cyber-physical system-of-systems, attacks and misbehaviours can be considered at vehicle level, within the DRI and data sharing environments. For that reason, it is important to have Misbehaviour Detection (MBD) functionalities available at all these levels (5GAA, 2022). For the mitigation strategy, it is necessary to have Misbehaviour Reporting Systems (MRS) to exchange misbehaviour information between relevant entities in the CCAM ecosystem (ETSI, 2023), as part of the response and recovery steps. A basic Misbehaviour Detection and Reporting (MBD&R) setup is illustrated in Fig. 1. This generic architecture is taken from our previous work (Oliveira, 2024), which is also based on the guidelines described in the Misbehaviour Detection white paper from the 5GAA Automotive Association (5GAA, 2022). In-vehicle misbehaviour detectors are deployed to check incoming sensor data and communicated data from DRI, before its usage in ISA. MRS functions are in place to report and share detected misbehaviours across the CCAM ecosystem.

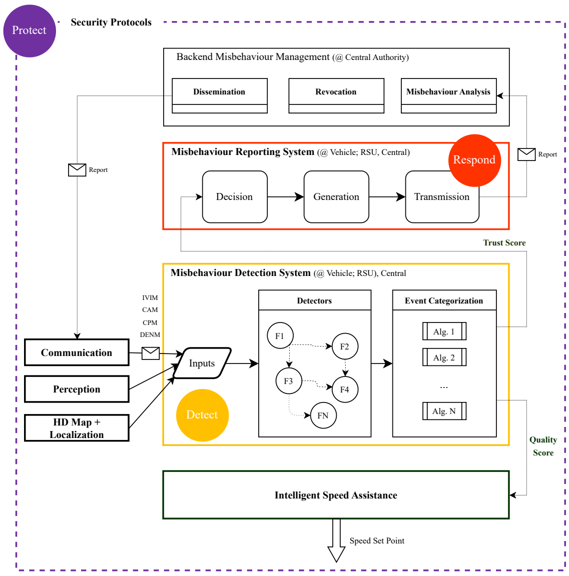

Figure 1: MBD&R high-level architecture.

2.2 Data Trust and Data Quality

Standards and trust mechanisms are essential building blocks to fully realize smart mobility benefits. With the European Union C-ITS Security Credential Management System policies (EC, 2018), the EU has established a European Trust Domain that provides electronic signatures to ensure origin and integrity of data (ETSI, 2021). This electronic signature indicates that the shared data has not been changed or tampered with and that it is from a trusted source. With this, vehicles can recognize trusted data *sources* which is crucial in the assessment of the reliability of shared information. This is an important first step, but it is not enough to create a trusted DRI. Ensurance of the right data quality level is crucial as well. Even when data providers are trusted, the data itself can still be flawed, with errors such as incorrect signals or outdated information. Our proposed solution for this is a Misbehaviour Detection (MBD) concept to help identify such issues by comparing multiple data sources and using historical patterns. Data quality from different sources is operationally assessed through data sanity checks and comparisons across these sources. Having both quality and trust metrics enables the ADAS/ADS system to make informed decisions based on the shared data. The Misbehaviour Detection mechanisms can also be used to report suspected faulty data back to the source, allowing that party to make improvements and thus continuously enhance data quality. The requirements and complexity of trust and MBD algorithms depend on the required safety levels. For vehicle systems, increasing levels of automation, means reliability and data quality become more critical.

3 ISA USE CASE WITH DRI SUPPORT

In the Digital Infrastructure for Future-proof Mobility project (DITM, 2022), digital infrastructure for automated transport solutions are being implemented into validation labs. ISA supported by DRI is an important use case of the validation labs. In DITM MBD&R functions are being developed and implemented at vehicle, roadside and central level. The vehicle deployments use TNO carlabs to evaluate the ISA MBD&R system under real-life conditions at public roads. These carlabs are our CCAM research facilities consisting of regular production vehicles equipped with relevant retrofitted hardware and software to enable experimental automated driving applications. The systems and software are under our own control and include sensor-sets (camera, radar, lidar, etc.), wireless communications (ITS-G5, C-V2X, 5G cellular, UWB, etc.), our ADAS/ADS driving stack (perception, localization, sensor-fusion, drive planning, vehicle control, etc.), human-machine interface (HMI, e.g. for warnings, handing over of control). In the remaining part of the paper the focus is on these in-vehicle MBD functions. A generic approach is used that scales with available sensor-suite, supports different data sources as multiple types of applications (traffic safety, ADAS/ADS or other CCAM like applications). Fig. 2 shows a generic sensor set and data sources suitable for use in ISA:

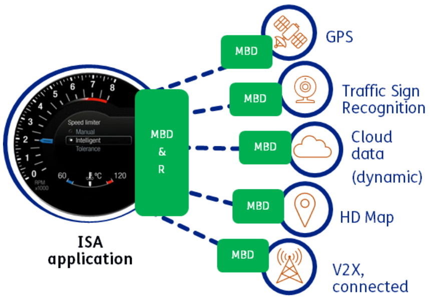

Figure 2: MBD&R example for ISA: vehicle sensors and data sources.

- A GNSS data source used for positioning. The GNSS source can also be used as one of several inputs of a multi-source localization function that enables lane-level accuracy.
- On-board cameras, as part of the perception system, are used for Traffic Sign Recognition (TSR) of (static) traffic signs and possibly overhead variable message signs (VMS). Also other camera image-based functions can be of interest, for example line-detection for lane-level accurate ISA.
- (Dynamic) cloud data is used as a collection term for all kinds of real-time traffic information (RTTI) services, from a multitude of service providers, here specifically those providing speed limits.
- (HD) Map services, next to static (offline) map information, can include real-time map updates, offering new layers of information suited for ADAS/ADS functionality, such as speed limits for ISA.
- V2X communication and connected services related to RTTI-type of data. For ISA the In-Vehicle Information Message (IVIM), (ISO/TC-204, 2020) is of special interest. The IVIM offers speed limit and road layout information and is normally provided by an authorized Road Operator (RO).

Within our generic approach, every relevant ISA sensor can be extended with MBD functionality. In Fig. 2 the green detector blocks are specifically designed for their sensor, i.e. for handling a specific data type. Detector functions perform basic checks on system health and status; data quality and trust validation (consistency, integrity, plausibility, timing, etc.); and expected misbehaviours. These individual MB-detectors are connected to a central in-vehicle MBD&R block that compares sensor data and calculates related trust scores, calculates data quality scores, collects evidence of misbehaviour and uses this information for filing MBD-reports. Based on this central assessment, the speed limit data is used or dismissed by the ISA application and detected misbehaviour is reported back to the providing sources. The latter facilitates the improvement of the data sources and enhances overall system reliability.

4 VEHICLE IMPLEMENTATIONS

This section provides more detailed information on the ISA use case and related vehicle implementations within the DITM project. The developed concept design is being implemented into real vehicles (TNO carlabs) and DRI-elements are deployed and used for ISA testing under real-life conditions.

4.1 Misbehaviour Detectors

The in-vehicle MBD&R functions are depicted in Fig. 3 and are divided into two main blocks:

- On-board Unit (OBU) stack: this is part of the V2X communication system and does checks on the received data. The low-level communication function does security checks (V2X-PKI, credentials, integrity), correct forwarding, data consistency check, timing check etc. It can already filter out untrusted, corrupted messages. Trusted data is forward into specific MBD and AD functions.
- Automated Driving (AD) stack: this part contains all in-vehicle AD related functions like sensors, world model, drive planning and vehicle control. For ISA it has camera and map MB-detectors and uses the output coming from the OBU message detectors. A central function (re-)calculates trust scores and collects evidence to be used in MBD-reports. Quality scores are calculated and are used to determine which speed limit data is used as input for the ISA application.

All received V2X data from DRI elements are processed via the ”communication trust” (blue) block of the OBU stack. This part detects generic communication misbehaviour with checks possible at all communication layers (ETSI, 2010). The security layer is the first layer of this detector in which messages are being assessed based on security-related checks: trusted source, security profiles, integrity checks, etc. If the message is not filtered out at this stage, other checks are performed related to message formats and structure, consistency and timing checks. If messages are discarded at this stage, the collected evidence can be used to file a MB report. For trusted messages, a trust score is calculated, upon which they are forwarded to the ITS message detector (red block). The ITS message detector performs checks based on the type of message received. For ISA the IVIM is assessed and specific checks on message type, expected structure, data elements content checks are executed. Misbehaviour checks are being performed, with specific interest in road layout information and speed limit information at road and lane level, to verify if data are within expected bounds, if data is consistent over time, etc. The ITS message detector filters out irrelevant information (for the ISA application) and forwards the speed limit, road layout information together with a calculated trust score. In the AD stack, all in-vehicle related Misbehaviour Detectors are performing similar specific data checks and calculate individual trust scores. For ISA this are the *Camera Detector* and *Map Detector* (red blocks). First checks are basic system-related checks to validate healthy operation, followed by more specific checks on sensor and system data consistency, plausibility, expected timing of signals, etc. A central block (orange) is processing the output from all detectors to calculate an overall trust score and to collect the evidence for detected misbehaviours, which are being forwarded as input for potential MB-reporting. In addition, quality scores are being calculated based on comparing the different sources (Camera, Map, IVIM) which are used to determine which speed limit to forward to the ISA application. The quality score is, again, built-up of several data-checks (e.g. thresholds), but also based on comparison of sources, and use of confidence values (if available). In Fig. 3 the green Road Model block uses these inputs to determine the applicable speed limit, since ultimately the application needs a single source-of-truth speed limit to act upon.

4.2 Trust and Quality Score Calculations

4.2.1 Trust Score

This is a continuation of our work done in (Oliveira, 2024), which already uses trust and quality scores as part of ISA MBD functionality. A reputation system concept is developed targeting all ISA entities, or nodes (data sources), such as communication channels, perception systems, possibly other vehicles (via V2X communication) etc. The used trust scoring concept is based on the theory of reputation scores from publications of (Michiardi and Molva, 2002), (Leinmuller et al., 2008) and (Bißmeyer et al., 2012). The trust scores are intended to track the occurrence of misbehaviour in each node. A misbehaviour can directly be linked to a check of a detector, with a detector covering multiple checks applied in logical relations. Additionally, the interest is not only in trust at a specific moment, but more in a historical trust over a certain window of time. This ensures that false pos-

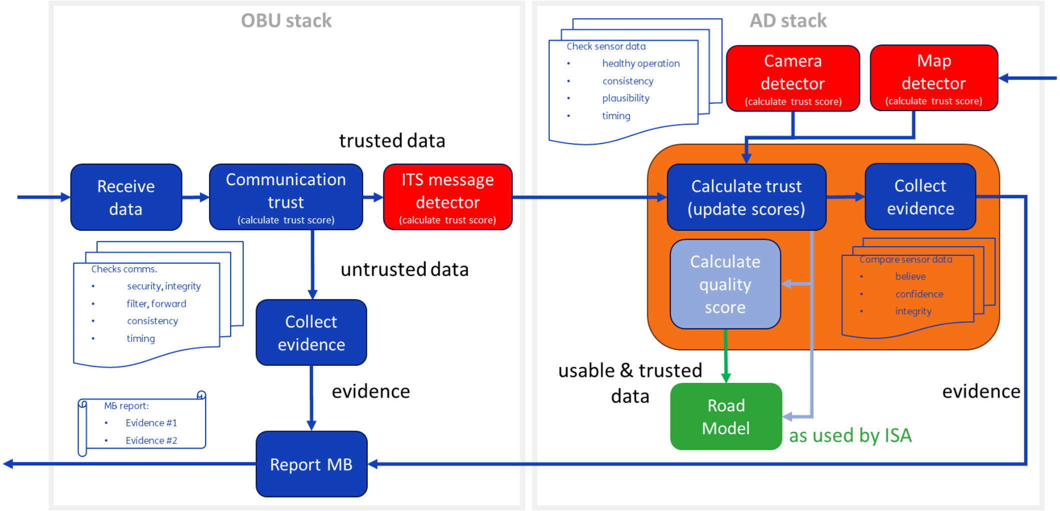

Figure 3: Flow diagram of the in-vehicle MBD&R system.

itives do not suddenly raise the trust value of a node. For a node to become trustworthy, it needs to perform correctly for a certain amount of time. Current extensions also include concepts of the Transferable Belief Model (TBM) (Philippe Smets, 1994). Where TBM provides a mathematical framework for rational and evidence-based decision making under various types of uncertainty. Like for instance inaccurate or distrusted observations, indecisive or missing information, or dealing with conflicts in the evidence. Application of TBM has several features particularly relevant to the detection and handling of anomalies and misbehaviour. Evidence can be provided at different levels, e.g. the evidence that a sensor is working, the evidence that the sensor detected a line, and evidence that the sensor recognized a traffic sign, and a sub-sign, etc. Causality of evidence can be organized and aggregated in a complex belief model as a logical network. Our approach is compatible with ongoing developments covered in (5GAA, 2022) and (5GAA, 2024), which uses concepts like trust relationships, trust referral and trust network analysis with subjective logic (J. Audun and Pope, 2006).

4.2.2 Quality Score

The quality scoring is used to evaluate the validity of the speed limit information for use by the ISA application. So, the quality score calculation for a single source or node is not based on a historical evaluation of the data. Instead, quality scoring is based on the belief scores of individual sample values available from individual Misbehaviour Detectors. To recall, for our ISA example the individual speed limit sources are TSR data from camera, received IVIM from DRI and map-based speed limits. The three available isolated belief scores are evaluated and undergo a ”2-out-of-3” real-time comparison of the available speed limit values. Depending on the belief scores, defined thresholds, and applied situational weighting, the most likely speed limit is determined. Situational weighting implies the option to take into account contextual knowledge by the system in computing the belief (e.g. knowledge about the road type the vehicle is currently on, with the assertion that a speed limit sign of 30 km/h on a highway is implausible). The quality score must be recalculated every time one of the independent sources provides a new speed limit value. The trust scores are calculated in real-time and are updated per independent source. For the trust and quality scores, computational loads and times are expected to be within acceptable limits, as the detected speed limit changes over a certain traveled distance are also limited. In addition, depending on individual source trust scores or detected misbehaviours, certain data will be discarded, or an individual source is (temporarily) marked as untrusted.

4.3 Test in Real-Life Conditions

For the ISA use case the MBD&R implementations are being deployed in our experimental carlab and test scenarios are executed at the highways surrounding the city of Eindhoven in The Netherlands. Within the DITM digital data sharing environment, tooling has been deployed to share actual IVIMs that match the local conditions of the roads. It also supports specific predefined misbehaviour into the IVIMs which allows for replicable testing. Testing scenarios cover the local conditions with detected traffic signs, diverse road and lane layouts, active VMS systems and com-

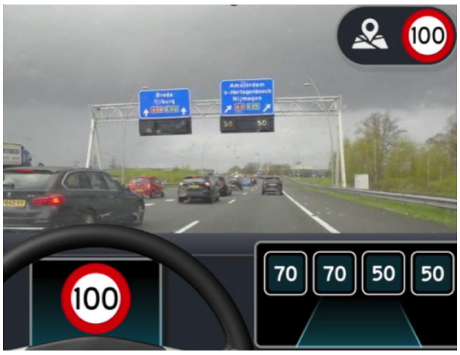

Figure 4: Illustration of ISA MBD&R testing under real-life conditions.

mercial map data (as depicted in Fig. 4). All ISA relevant data is presented to the driver via the vehicle HMI, but the ISA application itself is operated in open loop, without actuation of speed control, as public roads are being used. In addition, all relevant data will be logged (DRI, vehicles) for post-processing and further analysis.

4.4 Expected Results

The ISA MBD&R functions, with trust and quality scoring methods, are currently being implemented into our carlab. Testing for verification at vehicle level is planned for early 2025. Thereafter real-life validation can start at the highways surrounding Eindhoven. Relevant data will be collected for analysis of ISA performance including speed limit information from: maps (static and dynamic); available traffic signs (static signs, VMS); and lane-specific speed limits from IVIMs. The validation data will also be used for further improving the MBD functionality, for example tuning the individual misbehavior detectors and quality and trust scoring methods. Expected is that having our MBD&R implementation deployed will improve the performance of ISA application because of:

- the IVIM exchange via DRI offers an additional source of ISA information.
- certain misbehaviours can now be detected.
- data sources can be identified as trusted.
- data quality and trust scores can improve usability of the data for ISA and thus improve ISA speed limit selections.

5 CONCLUSIONS

Current ADAS/ADS, like an ISA application can be improved with the support of DRI. Concerns about quality and trust in data must be addressed to fully realize the benefits of smart mobility. Our MBD&R implementation for ISA, with cross-verifying data from cameras, maps and extended with DRI sources, can be a first step in realizing such a trusted CCAM environment. This is done with ISA sources and data identified as trusted (or untrusted) and the detection and reporting of misbehaviours. Furthermore, with data quality and trust scores to improve data usability and speed limit selections for ISA. Future work involves the execution of the real-life testing, scaling up with other sensors and including other sources coming from DRI. Doing more specific MBD scenario testing, for instance by incorporating lane-specific rules. The test results and more technical details of the concepts will be published later in a research paper. Our approach is generic and can be used for other ADAS/ADS applications and can even be applied in similar ways at other entities in the CCAM data chain, e.g. at data service providers. The continuation of this work is preferably done with participation of stakeholders such as road operators, data providers and vehicle OEMs, seeking agreements on data quality and trust specifications to ensure effective use of shared data.

ACKNOWLEDGEMENTS

Most of this work is done as part of the DITM project (DITM, 2022), a National Growth Fund project subsidized by the Dutch government. DITM aims to make future mobility safer and more efficient. The project is expected to end in 2026.

REFERENCES

5GAA (2022). Misbehaviour Detection. https://5gaa.org/content/uploads/2022/07/5GAA-Misbehaviour-detection-Final.pdf. Page visit on 18th of February 2025.

5GAA (2024). Creating Trust in Connected and Automated Vehicles. https://5gaa.org/content/uploads/2024/05/5gaa-trust4auto-white-paper-2024.pdf. Page visit on 18th of February 2025.

Bißmeyer, R., Mauthofer, S., Bayarou, K. M., and Kargl, F. (2012). Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters.

DITM (2022). Digital Infrastructure for Future-proof Mobility. https://www.tno.nl/en/digital/smart-traffic-transport/automated-vehicle-technology-public/ditm-digital-infrastructure-future-proof/. 2022 - 2026.

EC (2018). C-ITS Point of Contact (CPOC): European Union C-ITS Security Credential Management System (EU CCMS). https://cpoc.jrc.ec.europa.eu/index.html. Page visit on 18th of February 2025.

EC (2023). Intelligent Speed Assistance (ISA) set to become mandatory across Europe.

ETSI (2010). ETSI EN 302 665: Intelligent Transport System (ITS); Communication Architecture, V1.1.1.

ETSI (2021). ITS; Security; ITS communications security architecture and security management; Release 2. Technical report, ETSI ITS.

ETSI (2023). ITS; Security; Misbehavior Reporting service; Release 2. Technical report, ETSI ITS.

Farah, H., Erkens, S., Alkim, T., and van Arem, B. (2018). Infrastructure for Automated and Connected Driving: State of the art and future research directions. Technical report, Road Vehicle Automation 4. Lecture Notes in Mobility.

ISO/TC-204 (2020). Intelligent Transport Systems, Cooperative ITS, Dictionary of in-vehicle information (IVI) data structures. Technical report, OSI TC-204.

J. Audun, R. H. and Pope, S. (2006). Trust network analysis with subjective logic. in Conference Proceedings of the Twenty-Ninth Australasian Computer Science Conference.

Kamel, J., Ansari, M. R., Petit, J., Kaiser, A., Jemaa, I. B., and Urien, P. (2020). Simulation framework for misbehavior detection in vehicular networks.

Leinmuller, T., Schoch, E., Kargl, F., and Maihofer, C. (2008). Decentralized position verification in geographic ad hoc routing.

Michiardi, P. and Molva, R. (2002). CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks.

OECD (2023). Preparing infrastructure for automated vehicles. Technical report, OECD / International Transport Forum Research Reports.

Oliveira, P. (2024). Misbehaviour Detection System for Intelligent Speed Assistance (ISA). In *Proc. of 2024 IEEE Intelligent Vehicles Symposium (IV)*.

Philippe Smets, R. K. (1994). The Transferable Belief Model. *Artificial Intelligence*.

van der Heijden, R. W., Dietzel, S., Leinmuller, T., and Kargl, F. (2019). Survey on misbehavior detection in cooperative intelligent transportation systems.

Zhang, J., Jemaa, I., and Nashashibi, F. (2022). Trust management framework for misbehavior detection in collective perception services. In *17th International Conference on Control, Automation, Robotics and Vision (ICARCV)*.