



МЕЖДУНАРОДНА НАУЧНА КОНФЕРЕНЦИЯ „МЕХАТРОНИКА, ЕКО И ЕНЕРГОСПЕСТЯВАЩИ СИСТЕМИ И ТЕХНОЛОГИИ“ - ПЛОВДИВ' 2026

НАДЕЖДНО СЪБИРАНЕ НА ДАННИ ОТ ПЪТНИ СЕНЗОРИ

RELIABLE DATA COLLECTION FROM ROAD SENSORS

Radoslav Furnadzhiev, Mitko Shopov, Maria Babanova

1) *Technical University of Sofia, Faculty of Electronics and Automation,
Department of Computer Systems and Technologies, Plovdiv, Bulgaria*

2) *Center of Competence "Smart Mechatronic, Eco-and Energy-Saving Systems and Technologies",
4000 Plovdiv, Bulgaria*

Abstract

Intelligent Transportation Systems (ITS) increasingly depend on dense networks of road sensors whose measurements feed traffic management, pavement assessment, and safety applications. The value of these applications is bound by the reliability of the underlying data: sensor faults, environmental noise, intermittent wireless links, node mobility, and malicious interference all degrade the quality of the collected information. This paper surveys and synthesises the mechanisms that make data collection from road sensors reliable, drawing on recent literature spanning sensor infrastructure, multi-sensor data fusion, fault-tolerant networking, distributed fog/edge processing, and distributed-ledger integrity protection. We organise the field around four reliability layers: the sensing layer; the fusion layer; the network and processing layer; and the trust layer and show how techniques at each layer complement one another. Distributed data fusion based on the theory of belief functions, executed through self-stabilising algorithms, tolerates unreliable sources and network failures; fault-tolerant virtual network embedding and hierarchical fog computing preserve data continuity under node and link failures; and lightweight distributed-ledger technologies secure the integrity and provenance of vehicular data. No single mechanism is sufficient in isolation; reliable road-sensor data collection requires their coordinated combination. The paper consolidates design guidelines for laboratory C4.1 of the Center of Competence "Smart Mechatronic, Eco-and Energy-Saving Systems and Technologies".

Keywords: road sensors, reliable data collection, data fusion, belief functions, fault tolerance, fog computing, edge computing, intelligent transportation systems, data integrity.

1. INTRODUCTION

Road infrastructure is one of the most heavily instrumented environments of the modern smart city. Intelligent Transportation Systems (ITS) embed sensors in the pavement, mount them on roadside gantries and smart poles, and increasingly treat moving vehicles as mobile sensing platforms. The resulting data streams drive traffic-state estimation, incident detection, pavement-condition assessment, adaptive signal control, and driver-assistance services. The usefulness of every one of these applications is, however, bounded by a single property of the data on which it operates: reliability. A congestion estimate computed

from a stuck inductive loop, an icy-road warning derived from a miscalibrated thermometer, or a safety message lost to a wireless outage can be worse than no information at all, because it induces misplaced confidence in a wrong decision.

Reliability in the road-sensor context is multi-dimensional. It encompasses the correctness of individual measurements, the continuity of the data flow in the presence of node and link failures, and the integrity and provenance of the data as it traverses an open, frequently wireless, and sometimes adversarial communication medium. These dimensions are attacked by distinct phenomena: sensors drift,



age, and fail; the physical environment introduces noise, occlusion, and in the case of vehicular networks extreme mobility; wireless links suffer interference, fading, and congestion; and exposed media invite spoofing, tampering, and denial-of-service attacks [3, 7].

Because no single technique addresses all of these failure modes, a reliable road-sensor data-collection system is necessarily a layered construction. This paper, prepared within the activities of laboratory C4.1 of the Center of Competence "Smart Mechatronic, Eco-and Energy-Saving Systems and Technologies", surveys the principal mechanisms reported in the recent literature and organises them into the four cooperating: a sensing layer, a fusion layer, a network and processing layer, and a trust layer. Data ascends through the layers from raw, individually unreliable readings at the bottom to trusted, reliable estimates at the top, with each layer countering a distinct class of failure.

Section 2 describes the road-sensor infrastructure and its intrinsic reliability characteristics. Section 3 analyses the sources of unreliability. Section 4 examines multi-sensor data fusion as the primary means of extracting reliable estimates from imperfect sources. Section 5 reviews fault-tolerant networking and distributed fog/edge processing, which preserve data continuity. Section 6 considers data integrity and trust through distributed-ledger technologies. Section 7 discusses the findings and Section 8 concludes.

2. ROAD SENSOR INFRASTRUCTURE

The starting point for reliable data collection is the sensing layer itself. In their paper the authors [1] provide a comprehensive taxonomy of the IoT sensor systems used to monitor road infrastructure, dividing them into

two broad classes according to their relationship with the pavement.

Intrusive sensors are installed on or within the pavement surface. The class includes inductive loop detectors, magnetometers, and piezoelectric sensors. Piezoelectric elements generate an electrical impulse when mechanically stressed by a passing axle, enabling vehicle classification, weigh-in-motion, and speed estimation [1]. Intrusive sensors deliver accurate, low-latency measurements but are costly to install and maintain because deployment and replacement require interrupting traffic and cutting into the road surface, an operation that itself shortens pavement service life. Their physical exposure also makes them a frequent source of faults, which directly motivates the reliability mechanisms discussed in later sections.

Non-intrusive sensors observe the road from a distance and include acoustic sensors, radar, LiDAR, passive infrared sensors, and camera systems [1]. Cameras provide the richest semantic data and can even be combined for example, two co-located cameras used for stereovision act as a virtual sensor that transforms image pixels into spatial voxels for distance measurement [1]. The price of this richness is high bandwidth and sensitivity to illumination and weather, which translate into data-quality variability that downstream fusion must absorb.

A defining feature of the modern road-sensor stack is that processing is distributed across the edge, fog, and cloud layers [1, 6]. The authors [1] distinguish edge computing, which runs on edge devices such as single-board computers close to the sensor, from fog computing, in which more capable devices exercise decentralised control and perform complex analysis over a group of edge devices in the same local network, reserving the centralised cloud for heavy, latency-tolerant analytics. In their work the authors [6] surveyed precisely this intersection



of ITS sensing and edge computing, arguing that moving computation toward the sensor is essential to meet the latency, bandwidth, and critically for this paper reliability requirements of ITS, because local processing reduces the volume of data exposed to the unreliable wide-area links and shortens the control loop for time-critical reactions.

3. SOURCES OF UNRELIABILITY

Before reliability mechanisms can be designed, the failure modes they counter must be made explicit. Four recurring sources of unreliability emerge from the literature.

Source-level imperfection. Individual sensors produce low-quality, redundant, or simply erroneous readings due to calibration drift, ageing, environmental interference, and outright hardware failure. The elimination of low-quality, redundant, and conflicting data as a critical task of data-fusion preprocessing, confirming that imperfect sources are the rule rather than the exception [2]. Different studies [3] frame the same problem as the "data source inaccuracy and unreliability problem", noting that classical fusion assumes homogeneous, reliable sources giving similar readings an assumption that road environments routinely violate.

Network-level failure. Wireless links between sensors, roadside units, and gateways suffer interference, fading, congestion, and topology changes. In vehicular ad hoc networks the situation is aggravated by high mobility, which causes frequent route breakage and message loss [7]. A reliable system must therefore tolerate not only bad data but a network that intermittently fails to deliver good data [3].

Node and embedding failure. In a wireless sensor network the failure of a relay node or the depletion of its battery can sever the only path between a source and the gateway. In their study the authors [4] treat this as a virtual-network-embedding problem in which

the survival of at least one source-to-destination path after a failure is the quantity to be maximised.

Adversarial interference. Because vehicles and roadside units communicate over unrestrained, exposed wireless media, they are visible to security threats; data may be intercepted, spoofed, or modified for unauthorised use [7]. Reliability here merges with security: data that cannot be trusted is, for decision-making purposes, unreliable [8, 9].

4. DATA FUSION FOR RELIABLE COLLECTION

The single most effective response to source-level imperfection is multi-sensor data fusion, which combines redundant and complementary observations into an estimate more reliable than any constituent measurement. The authors [2] review data-fusion (DF) methods for real-time, multi-sensor traffic-flow analysis and structure the design of any DF method around four core steps preprocessing, filtering, decision, and evaluation operating at three abstraction levels: data-level fusion, which combines raw readings through noise removal, outlier rejection, and denoising (commonly with a Kalman filter); feature-level fusion, which merges extracted features; and decision-level fusion, which reasons over the outputs of multiple classifiers through inference and selection. This hierarchy is the backbone of reliable estimation, because each level removes a distinct class of error: data-level fusion suppresses noise, feature-level fusion exploits complementarity, and decision-level fusion resolves conflicts between sources.

For decision-level fusion under explicitly unreliable sources, the theory of belief functions (Dempster-Shafer evidence theory) is particularly suitable, as it can represent ignorance and conflict directly. The authors [3] build on it to detect dangerous road events, specifically icy roads from distributed



temperature measurements using data from both vehicle on-board sensors and wireless roadside sensors. Their central contribution to reliability is twofold. First, the use of belief functions allows the system to deduce correct conclusions from individually unreliable sources. Second, to cope with network failures, fusion is performed through a self-stabilising distributed algorithm: regardless of transient errors or message loss, the computation converges to a correct global state, preventing a vehicle from converging to an erroneous confidence simply because it missed updates. The combination of independent bodies of evidence is expressed by Dempster's rule of combination,

$$m_{12}(A) = \frac{1}{1-K} \sum_{B \cap C = A} m_1(B) m_2(C), \quad K = \sum_{B \cap C = \emptyset} m_1(B) m_2(C), \quad (1)$$

where m_1 and m_2 are the mass functions of two sources, A is a hypothesis over the frame of discernment (e.g. icy / not icy), and K measures the conflict between the sources. A high conflict K flags disagreement and thereby signals a potentially unreliable source, so the fusion operator both produces an estimate and quantifies its trustworthiness. A proposed approach is validated through in-lab and on-the-road experiments, demonstrating that proper results can be deduced from unreliable data in a real vehicular network [3].

5. FAULT-TOLERANT NETWORKING AND PROCESSING

Fusion improves the correctness of estimates, but it cannot help if the data never arrives. Continuity of the data flow is the responsibility of the network and processing layer.

Fault-tolerant embedding [4] addresses resilience at the level of the sensor network itself through virtualisation. They formulate fault-tolerant virtual network embedding (VNE) in wireless sensor networks as a

bi-objective optimisation solved with an adapted non-dominated sorting genetic algorithm (A-NSGA) that simultaneously maximises fault tolerance the probability that at least one path between source and destination survives a link failure and minimises communication delay. Crucially, the scheme discovers alternative path endpoints when a node or link fails and supports re-embedding without pre-allocating back-up resources, so reliability is achieved without the energy and capacity cost of permanent redundancy.

Distributed fog processing. Pushing analytics toward the data source improves both latency and reliability by reducing dependence on a single central server. The authors [5] propose a hierarchically distributed fog-computing architecture for real-time anomaly detection in smart-meter sensor data; although demonstrated in the smart-grid domain, the architecture transfers directly to road sensing. Machine-learning anomaly-detection models are trained and then executed across intermediate fog nodes rather than in the cloud, overcoming the volume, velocity, bandwidth, and real-time limitations that make a purely cloud-centric pipeline brittle. The same paper notes that reliability is further strengthened by majority voting across three or more nodes when flagging anomalies, a decision-level redundancy mechanism that prevents a single faulty detector from corrupting the result. This hierarchical edge-fog-cloud organisation mirrors the processing model identified in the sensor-infrastructure survey [1, 6] and confirms its generality.

Resilient routing. At the vehicular-network level, it is proposed [7] a resilient and secure cooperative ITS (RS-ITS) that uses the roadside unit as an intelligent agent employing machine learning to predict the best routes and maintain low overhead, while securing the network against vulnerabilities and ensuring



reliable propagation of messages between vehicles and RSUs. Their simulations report improvements over comparable schemes of 17% in delivery ratio, 40% in data delay, 22% in energy consumption, 17% in route discontinuity, 27% in network overhead, and 43% in resistance to malicious attacks quantifying how route reliability and security can be improved jointly rather than traded off.

6. DATA INTEGRITY AND TRUST

The final layer concerns whether collected data can be trusted once it has been delivered. In the open vehicular environment, where the Internet of Vehicles (IoV) interconnects every sensor and actuator, integrity, provenance, and trustworthiness of the data become reliability requirements in their own right [8, 9]. Distributed-ledger technology (DLT) has emerged as the dominant answer.

The authors [8] propose Lightweight-BIoV, a blockchain distributed-ledger scheme for the Internet of Vehicles that addresses the resource constraints of vehicular nodes while providing data integrity, exchange reliability, provenance, and trust for node transactions and communications. The "lightweight" design is essential, because the heavy consensus of general-purpose blockchains is incompatible with the latency and energy budgets of road sensors.

Other studies [9] pursue the same goal at the architectural level with FlexiChain 3.0, a DLT-based Layer-0 network designed specifically for the ITS-IoV setting after an analysis of consensus algorithms and their applicability. They report a throughput of 2.3 transactions per second shown to be acceptable for IoV together with a security level that is largely independent of the number of participating nodes, demonstrating that strong integrity guarantees can be delivered within the timing constraints of fast-moving vehicles.

7. DISCUSSION

The reviewed literature shows that reliable data collection from road sensors is not the property of any single component but an emergent property of cooperating layers. Table 1 summarises the principal mechanisms, the failure mode each one targets, and the representative works.

Reliability layer	Primary mechanism	Failure mode addressed	Ref.
Reference Sensing	Redundant intrusive / non-intrusive sensors; edge pre-processing	Source imperfection, sensor faults	[1], [6]
Fusion	Belief-function fusion; multi-level DF; self-stabilising algorithms	Unreliable / conflicting sources	[2], [3]
Network & processing	Fault-tolerant VNE; hierarchical fog; resilient ML routing	Node / link / network failure	[4], [5], [7]
Trust	Lightweight distributed-ledger technology	Tampering, spoofing, lost provenance	[8], [9]

Table 1. Layered mechanisms for reliable data collection from road sensors.

Three cross-cutting observations follow. First, redundancy is the common currency of reliability, but it appears in different forms at each layer: spatial redundancy of sensors and fusion at the sensing and fusion layers [2, 3], path redundancy at the network layer [4], and



decision redundancy through majority voting at the processing layer [5]. Effective design allocates redundancy where it is cheapest for the dominant failure mode rather than uniformly. Second, reliability and energy are in tension: every redundant sensor, path, or ledger transaction consumes energy, so mechanisms such as adaptive embedding without pre-allocated back-ups [4] and lightweight consensus [8, 9] explicitly seek reliability at minimum cost, a concern of particular relevance to the energy-saving mandate of the Center of Competence. Third, reliability and security converge in the vehicular setting: distributed fusion that detects inconsistent sources [3] and resilient routing that resists malicious attacks [7] protect data correctness and authenticity at the same time, and the trust layer [8, 9] makes this convergence explicit.

The layers are also complementary in time. Belief-function fusion with self-stabilisation [3] and fog-level anomaly detection [5] act in the millisecond-to-second range to keep time-critical reactions correct, while ledger-based integrity protection [8, 9] operates over longer horizons to guarantee auditability and provenance. A complete road-sensor system therefore composes mechanisms across both layers and timescales.

8. CONCLUSION

This paper has surveyed the mechanisms that make data collection from road sensors reliable and has organised them into four cooperating layers: sensing, fusion, network and processing, and trust synthesising findings from nine recent works. At the sensing layer, a taxonomy of intrusive and non-intrusive sensors with edge pre-processing supplies redundant, complementary observations. At the fusion layer, multi-level data fusion and, in particular, belief-function fusion executed through self-stabilising distributed algorithms extract correct estimates from individually

unreliable sources while quantifying conflict. At the network and processing layer, fault-tolerant virtual network embedding, hierarchical fog computing with majority voting, and machine-learning-based resilient routing preserve data continuity under node, link, and network failures. At the trust layer, lightweight distributed-ledger technologies secure the integrity and provenance of vehicular data within strict timing budgets.

The central conclusion is that no single technique suffices: reliable road-sensor data collection emerges only from the coordinated combination of mechanisms, with redundancy as the common currency and energy efficiency and security as the cross-cutting constraints. Future work in laboratory C4.1 will instantiate this layered model on a physical road-sensor testbed, integrating belief-function fusion with a fault-tolerant fog architecture, and will experimentally characterise the reliability-energy trade-off identified throughout this review.

Acknowledgements

This research was funded by the European Regional Development Fund within the OP "Research, Innovation and Digitalization Programme for Intelligent Transformation 2021-2027", Project CoC "Smart Mechatronic, Eco- and Energy-Saving Systems and Technologies", No BG16RFPR002-1.014-0005.

REFERENCES

- [1] Micko K., Papcun P., Zolotova I. Review of IoT Sensor Systems Used for Monitoring the Road Infrastructure. *Sensors*, 23(9), 4469, 2023. doi:10.3390/s23094469. Available at: <https://www.mdpi.com/1424-8220/23/9/4469>.
- [2] Kashinath S. A., Mostafa S. A., Mustapha A., Mahdin H., Lim D., Mahmoud M. A., Mohammed M. A., Al-Rimy B. A. S., Fudzee M. F. M., Yang T. J.



Review of Data Fusion Methods for Real-Time and Multi-Sensor Traffic Flow Analysis. IEEE Access, 9, 51258–51276, 2021. doi: 10.1109/ACCESS.2021.3069770. Available at: <https://ieeexplore.ieee.org/document/9388883>.

[3] Radak J., Ducourthial B., Cherfaoui V., Bonnet S. Detecting Road Events Using Distributed Data Fusion: Experimental Evaluation for the Icy Roads Case. IEEE Transactions on Intelligent Transportation Systems, 17(1), 184–194, 2016. doi: 10.1109/TITS.2015.2464707. Available at: <https://hal.science/hal-01294780>.

[4] Kaiwartya O., Abdullah A. H., Cao Y., Lloret J., Kumar S., Shah R. R., Prasad M., Prakash S. Virtualization in Wireless Sensor Networks: Fault Tolerant Embedding for Internet of Things. IEEE Internet of Things Journal, 5(2), 571–580, 2018. doi: 10.1109/JIOT.2017.2717704. Available at: <https://ieeexplore.ieee.org/document/7950953>.

[5] Jaiswal R., Chakravorty A., Rong C. Distributed Fog Computing Architecture for Real-Time Anomaly Detection in Smart Meter Data. IEEE Sixth International Conference on Big Data Computing Service and Applications (BigDataService), Oxford, UK, 2020, pp. 1–8. doi: 10.1109/BigDataService49289.2020.00009. Available at: <https://ieeexplore.ieee.org/document/9103795>.

[6] Zhou X., Ke R., Yang H., Liu C. When Intelligent Transportation Systems Sensing Meets Edge Computing: Vision and Challenges. Applied Sciences, 11(20), 9680, 2021. doi: 10.3390/app11209680. Available at: <https://www.mdpi.com/2076-3417/11/20/9680>.

[7] Rehman A., Haseeb K., Saba T., Lloret J., Ahmed Z. Towards Resilient and Secure Cooperative Behavior of Intelligent Transportation System

Using Sensor Technologies. IEEE Sensors Journal, 2023. doi: 10.1109/JSEN.2023.3264304. Available at: <https://ieeexplore.ieee.org/document/10093116>.

[8] Laghari A. A., Khan A. A., Alkanhel R., Elmannai H., Bourouis S. Lightweight-BIoV: Blockchain Distributed Ledger Technology (BDLT) for Internet of Vehicles (IoVs). Electronics, 12(3), 677, 2023. doi: 10.3390/electronics12030677. Available at: <https://www.mdpi.com/2079-9292/12/3/677>.

[9] Alkhodair A., Mohanty S. P., Kougianos E. FlexiChain 3.0: Distributed Ledger Technology-Based Intelligent Transportation for Vehicular Digital Asset Exchange in Smart Cities. Sensors, 23(8), 4114, 2023. doi: 10.3390/s23084114. Available at: <https://www.mdpi.com/1424-8220/23/8/4114>