





Review

# A Survey on Fault Tolerance Techniques for Wireless Vehicular Networks

João Almeida <sup>1,\*</sup> , João Rufino <sup>1</sup> , Muhammad Alam <sup>1</sup>  and Joaquim Ferreira <sup>1,2</sup> 

<sup>1</sup> Instituto de Telecomunicações, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal; joao.rufino@ua.pt (J.R.); alam@ua.pt (M.A.); jjcf@ua.pt (J.F.)

<sup>2</sup> ESTGA—Universidade de Aveiro, 3754-909 Águeda, Portugal

\* Correspondence: jmpa@ua.pt

Received: 7 October 2019; Accepted: 12 November 2019; Published: 16 November 2019



**Abstract:** Future intelligent transportation systems (ITS) hold the promise of supporting the operation of safety-critical applications, such as cooperative self-driving cars. For that purpose, the communications among vehicles and with the road-side infrastructure will need to fulfil the strict real-time guarantees and challenging dependability requirements. These safety requisites are particularly important in wireless vehicular networks, where road traffic presents several threats to human life. This paper presents a systematic survey on fault tolerance techniques in the area of vehicular communications. The work provides a literature review of publications in journals and conferences proceedings, available through a set of different search databases (IEEE Xplore, Web of Science, Scopus and ScienceDirect). A systematic method, based on the preferred reporting items for systematic reviews and meta-analyses (PRISMA) Statement was conducted in order to identify the relevant papers for this survey. After that, the selected articles were analysed and categorised according to the type of redundancy, corresponding to three main groups (temporal, spatial and information redundancy). Finally, a comparison of the core features among the different solutions is presented, together with a brief discussion regarding the main drawbacks of the existing solutions, as well as the necessary steps to provide an integrated fault-tolerant approach to the future vehicular communications systems.

**Keywords:** wireless vehicular communications; systematic review; fault tolerance; dependability

## 1. Introduction

The main motivation behind the development of wireless vehicular communications was based on the need to improve road safety and traffic efficiency. Following previous success cases in the field of intelligent transportation systems (ITS), vehicular networks hold the potential of drastically reducing the number of traffic accidents and road fatalities. For that purpose, international standards have been purposed with the goal of defining how safety messages should be exchanged among vehicles and between vehicles and the roadside infrastructure. IEEE WAVE and ETSI ITS-G5 constitute the most disseminated protocol stacks for vehicular communications in the United States and Europe, respectively. Both of them rely on the IEEE 802.11 standard for the implementation of physical and medium access control (MAC) layers. Recent proposals, such as LTE-V or 5G, are pointed to as possible alternatives to 802.11, since these allow several distinct applications (e.g., mobile broadband, railway systems, etc.) to share the cost of network installation.

Despite the focus on safety, vehicular communications systems by design typically do not take into consideration dependability attributes and the need for hard real-time guarantees. However, this type of safety-critical services demands small end-to-end delays and high levels of reliability and availability. Fault tolerance mechanisms are good candidates to attain such requirements [1].

In this survey, a review of fault tolerance techniques for vehicular networks is presented. A systematic method was followed in order to select the related articles from a set of different search databases.

Fault tolerant methods are sometimes employed in security mechanisms for safety-critical applications in vehicular networks. In fact, the concepts of dependability and security are closely related [2] and in some cases, the proposed solutions aim to increase both the dependability and security attributes of the network. Nevertheless, an effort was made on this survey to avoid the analysis of strategies focusing on the security issues of vehicular communications, since this could be the topic of another review paper, given the large number of threats already identified in the literature [3]. In addition, the search was limited to fault-tolerant techniques specifically addressing vehicular network issues, not broader research topics such as mobile ad-hoc networks (MANETs), or similar fields e.g., mobile sensor networks (MSNs). An example of related work done in fault-tolerant MSNs, which usually take into consideration energy constraints that are not present in vehicular systems, is the mobility-tolerant TDMA-based MAC protocol proposed by Jhumka and Kulkarni [4].

In real-time wireless communication systems such as vehicular communication for safety applications, high availability of the system is very important to guarantee the dissemination of the safely critical messages to the desired destinations in the bounded time. Fault tolerance prevents the connection disruption arising from the system's component failures and therefore, high availability is achieved by ensuring no loss of service. Since fault tolerant systems provide real-time backup and usually depend on the redundant components, they are associated with additional costs. In addition, fault tolerant techniques prevent the failures and therefore restrict the scope of these failures in distributed systems.

The rest of the paper is organized as follows. Section 2 provides some background regarding the topic of fault tolerant communications and the different types of redundancy techniques. Section 3 presents the search method and the paper selection process for this survey based on the discussed criteria. In Section 4, the selected papers are analysed and classified according to the type of redundancy technique used to provide fault-tolerant behaviour. A comparison among some core characteristics of the selected documents is also provided, together with a discussion regarding the relevant findings of this survey. Finally, Section 5 presents the main conclusions of this work.

## 2. Background

Fault tolerant communications aim to guarantee that two or more network nodes can exchange information in spite of faults that may affect the communications link or some of the participating nodes. A communication system providing fault tolerance capabilities typically involves redundancy and diversity techniques. This way, it is possible to avoid the presence of single points of failure in the system and to prevent common failure modes in network nodes or node's components. Communications redundancy corresponds to an increment in resource utilization (mainly replication), in order to provide resilience against faults arising in the system. Traditionally, redundancy techniques can be classified into three main groups:

- **Temporal redundancy** is characterized by the attempt to deliver the same information at multiple moments in time. Retransmission based protocols, such as TCP, are clear examples of this strategy.
- **Information redundancy** corresponds to the use of additional data, so that information can still be retrieved in case of partial data loss. For instance, error correction codes require the transmission of redundant data in order to recover the contents of the exchanged message.
- **Spatial redundancy** refers to the possibility of providing the same information from different sources. Hardware replication constitutes a traditional example of spatial redundancy, where several replicas are able to deliver the same service.

Redundancy may also be categorized in terms of protocol stack layer in which it is applied. For instance, redundant channel links can be classified as physical layer redundancy. As a result, the distinct strategies may be categorized based on the Open Systems Interconnection (OSI) model.

Cross-layer solutions are also possible, covering faults in a set of different layers of the protocol stack. For example, entire node replication, from the RF antenna to the application level, constitutes one of these cases.

Fault-tolerant wireless communications strategies can also be found in other areas of research beyond vehicular networks. For instance, in wireless sensor networks (WSNs) or other types of mobile ad-hoc networks (MANETs), there are also available solutions in the literature to deal with possible faults in the system's operation. However, vehicular communications systems pose specific challenges, ranging from very dynamic network topologies to frequent link disruptions and the Doppler effect. As a result, for this survey, only fault-tolerance techniques particularly targeting vehicular network applications were considered.

### 3. Method

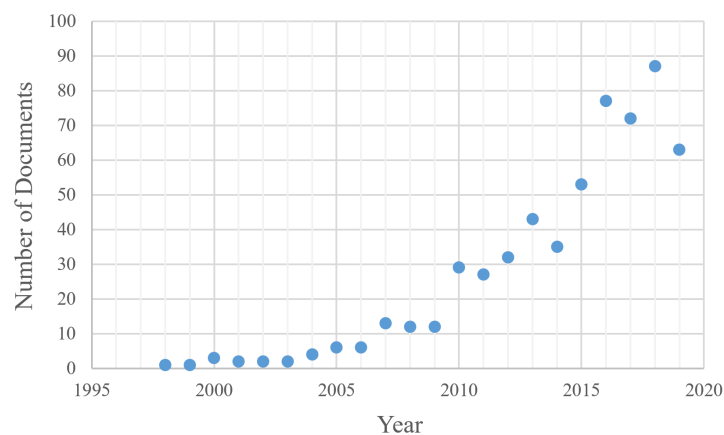
#### 3.1. Search Approach and Groups of Keywords

The search method for this survey was based on a systematic review process according to the preferred reporting items for systematic reviews and meta-analyses (PRISMA) statement [5]. Four different databases were utilized in this search (IEEE Xplore, Web of Science, Scopus and Science Direct), while others, such as Google Scholar, TRID or Academic Search Complete, were also explored but due to several distinct restrictions (e.g., the impossibility to search only on the article's metadata), were not included in the search tools for this review. The approach followed in the paper identification process, required that at least one term from each of two groups of keywords was present in the article's metadata. These two groups of keywords were the following:

- "fault tolerance", "fault tolerant", "fault detection", "dependability", "dependable", "safety critical"
- vehicular network\*, vehicular communication\*, "connected vehicles", "VANET", "cooperative vehicles", "cooperating vehicles", "intervehicle communications", "vehicle to vehicle"

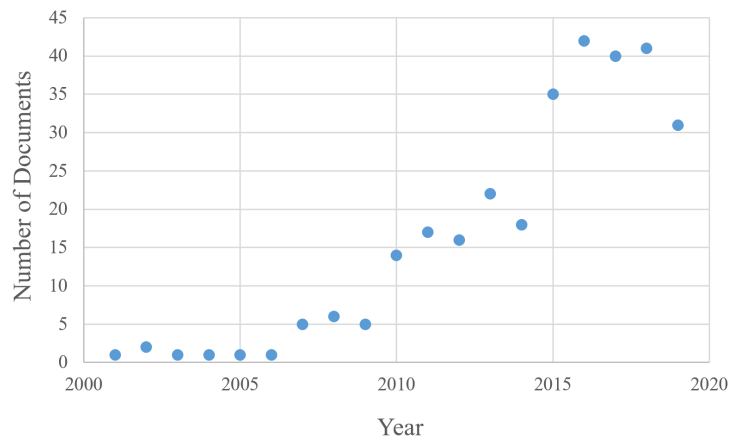
The terms "reliability", "reliable" and "real-time" were also considered for the first group of keywords, however, since these terms are typically employed in a broader sense, it was decided to limit the search to the keywords shown above. By employing these search terms, a total number of 1493 papers were identified (586 from the IEEE Xplore database, 299 from Web of Science, 585 from Scopus and 23 from ScienceDirect).

Both Scopus and Web of Science search tools provide charts with the results distribution along the years. These graphs can be observed in Figure 1. From the analysis of both charts, it is possible to derive a clear growth in the number of articles published with the search terms. This trend demonstrates the raising importance given by the scientific community to the topic of fault tolerance and dependability in the field of vehicular networks.



(a) Scopus.

Figure 1. Cont.



(b) Web of Science.

**Figure 1.** Results distribution along the years (adapted from Scopus and Web of Science databases).

### 3.2. Selection Process and Inclusion/Exclusion Criteria

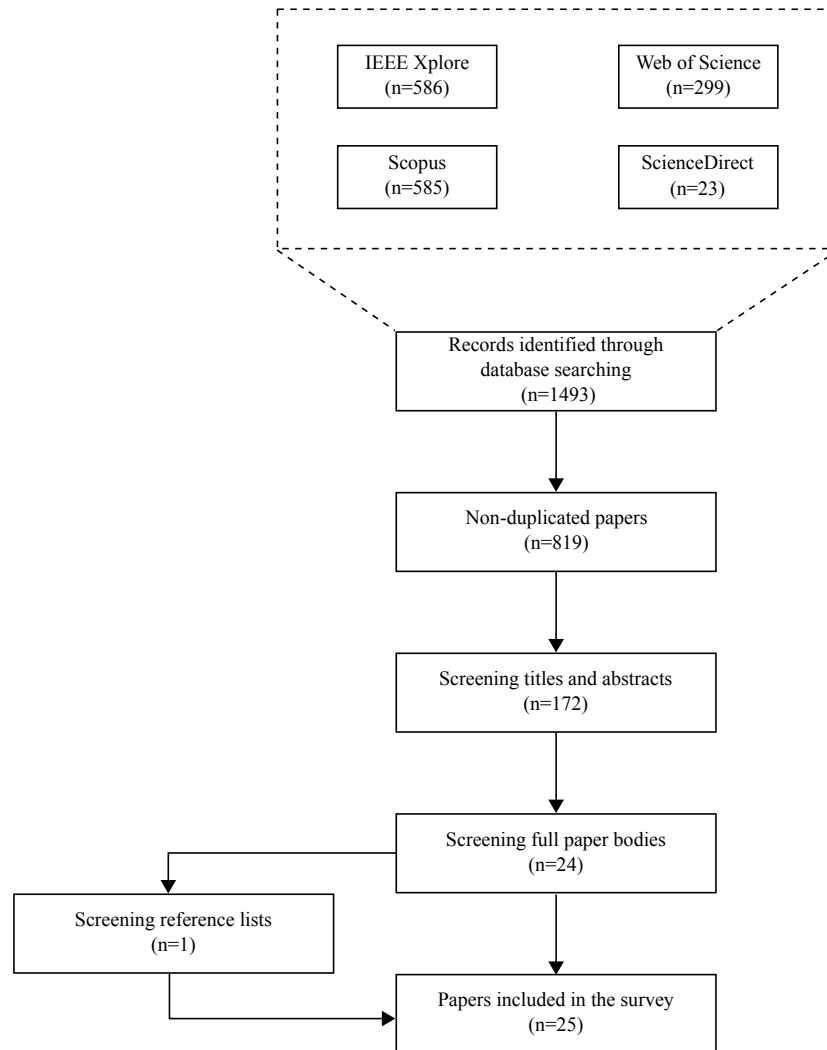
After this initial step, the duplicated entries were removed, as well as standards and other invalid results, such as programs, forewords or table of contents from conference proceedings. A total of 819 papers remained for analysis. Then, the titles and abstracts of the remaining articles were screened to exclude research work outside the scope of this survey, focusing for instance on satellite communications or intra-vehicle networks such as Controller Area Network (CAN) or FlexRay. 172 records were still left for the final selection process, in which not only the metadata (title and abstract) but also the body of the paper was analysed. A set of several criteria was used to ensure the eligibility of the articles to include in this survey:

- be published in English in a peer reviewed journal or conference proceedings;
- be focused on safety applications using wireless vehicular communications;
- including fault tolerance techniques to improve the dependability attributes of vehicular networks.

Complementarily, the following exclusion criteria were utilized in this selection process:

- only the most recent paper from a set of similar articles by the same author was kept (for instance, a paper published in a conference and later extended to a journal or magazine);
- papers not specifically focusing on safety-critical applications (with strict real-time constraints) were excluded;
- articles focusing on security issues of vehicular networks were not selected for the review;
- papers targeting railway, aviation systems, unmanned autonomous vehicle (AUxV), military vehicular clouds (MVC) or wireless sensor networks (WSN) were also considered out of the scope of this analysis;
- research works referring to fault-tolerance techniques designed to alternative technologies for vehicular applications, such as visible light communications (VLC), were not included;
- articles not specifically focusing on vehicular networks were discarded, like the ones with a broader scope (e.g., MANETs).

Following these criteria, 24 papers were selected. An additional record was added after screening the reference lists of this final selection, summing up a total number of 25 articles to be the subject of analysis in this survey. The complete paper selection process can be visualized in Figure 2.



**Figure 2.** Systematic paper review process according to preferred reporting items for systematic reviews and meta-analyses (PRISMA) statement [5].

#### 4. Fault-Tolerance Techniques

The selected publications encompass fault tolerance techniques that can be categorized according to the type of communications redundancy used (temporal, spatial and information). This classification can be visualized in Table 1. This section summarizes the contributions of each one of the selected publications.

**Table 1.** Results classification according to redundancy types.

Temporal	Spatial	Information
Jonsson et al. [6]	Matthiesen et al. [7]	Kumar et al. [8]
Bohm et al. [9]	Cambruzzi et al. [10]	Eze et al. [11]
Savic et al. [12]	Abrougui et al. [13]	Ali et al. [14]
Sawade et al. [15]	Chang et al. [16]	
Nguyen et al. [17]	Lann et al. [18]	
	Sanderson et al. [19]	
	Aljeri et al. [20]	
	Casimiro et al. [21]	
	Worrall et al. [22]	
	Ploeg et al. [23]	

Table 1. Cont.

Temporal	Spatial	Information
	Fathollahnejad et al. [24]	
	Bhoi et al. [25]	
	Elhadeif et al. [26]	
	Almeida et al. [27]	
	Medani et al. [28]	
	Devangavi et al. [29]	
	Younes et al. [30]	

#### 4.1. Temporal Redundancy

Regarding temporal redundancy methods, solutions found in the literature are based on packet retransmission schemes. For instance, the work of Jonsson et al. [6] focuses on increasing MAC protocol reliability for platooning applications. Time is divided into periodic transmission cycles, called superframes, each one including both contention-based phases (CBPs) and contention-free phases (CFPs). Applications with hard real-time constraints utilize the CFPs to transmit information. These CFPs rely on a polling-based mechanism administered by a master vehicle that applies a time division multiple access (TDMA) scheme for nodes' transmissions. Each transmission corresponds to a specific time slot, which are ordered according to the earliest deadline first (EDF) policy and a real-time automatic repeat request (ARQ) scheme. This ARQ scheme allows the retransmission of packets to not be well received and they can still be transmitted before their deadline expires. The performance evaluation of the protocol demonstrates a reduction in message error rate by several orders of magnitude when compared to the case without retransmissions.

Despite the improved reliability provided by the proposed solution, this retransmission scheme requires some modifications to the transport layer of vehicular communications protocol stack, in order to be implemented. This non-compliance with the standards encompasses the addition of a real-time polling-based layer on top IEEE 802.11p MAC, as well as the implementation of the transport layer retransmission scheme over a service channel exclusively dedicated to platooning communications. Another disadvantage is the fact that in highly congested scenarios, the retransmission scheme can lead to some bandwidth reduction for each transmitter, however, the real-time scheduling algorithm (EDF) guarantees the optimization of channel use. Furthermore, nothing is referred about the possibility of master failure, the one responsible for coordinating all the communications in the platoon, and how the proposed scheme reacts to that event. Finally, it should be also pointed out that the evaluation of this work was only performed in a simulation environment, very similarly to a numerical analysis, in which the network parameters were kept very static.

Following a similar approach, Böhm and Kunert [9] propose a retransmission scheme based on the data age of previously received messages. The framework targets intra-platooning communications but also communication between different platoons (inter-platooning). A dedicated service channel is used for intra-platooning communications, while vehicles in distinct platoons exchange information through the control channel. The platoon leader or master is responsible for periodically disseminating beacon messages to all the other vehicles in the platoon. Then during a collection phase, vehicles transmit status updates, which may or may not be well received by the master. In case of unsuccessfully decoded packets, the leader vehicle initiates a retransmission phase by sending individual polling messages to the other nodes, that immediately attempt to retransmit the failed messages. After that, a control phase begins which is used by the master to coordinate the other platoon members based on the retrieved status information. During this window, control packets are transmitted individually to each regular vehicle. In the end, another retransmission phase begins based on acknowledgements returned by the receiving nodes. Moreover, retransmission opportunities are assigned to the nodes, according to the data age of the messages received by the leader vehicle, which keeps a table with the reception time of

the latest status update and acknowledgement frames. From this record, higher transmission priorities are allocated to vehicles with older successfully transmitted messages.

The proposed solution introduces some tweaks at the MAC and transport layers in relation to the standard protocols and requires a significant amount of overhead, with acknowledgment messages, retransmissions packets and individual polling messages, in order to improve the packet delivery ratio, making the available bandwidth smaller for other applications or in case of channel saturation. Moreover, the authors do not take into account the problem of having the platoon coordinator as a single point of failure, holding the table with data age of messages from each vehicle. The protocol evaluation demonstrated the feasibility of the proposed scheme and the ability to maintain a stable data age value for the platoons. Additionally, the simulation analysis compares the proposed protocol with the standard approach and other retransmission schemes, but lacks a close-to-real-world scenario evaluation.

The work of Savic et al. [12] targets a distinct application, in this case, the collision avoidance problem of fully autonomous cars at road intersections. An algorithm for distributed intersection crossing is proposed, being able to cope with an unknown and large number of communications failures. A priority for intersection crossing is assigned to each one of the vehicles based on current position estimates and the cars' dynamics. Three types of packets are exchanged: periodic heartbeat messages and 'ENTER' and 'EXIT' messages immediately before and after crossing the intersection, respectively. In case of receive-omission failures, the 'ENTER' or 'EXIT' packets are retransmitted and the model assumes that at least one heartbeat ('HB') message is received before the intersection crossing (IC) algorithm starts and that vehicles eventually succeed to receive the 'ENTER' and 'EXIT' messages. The numerical results show only a slight increase of the crossing delay in the presence of communications failures.

The limitations of the proposed model include the omission of transmitter faults, messages with erroneous content and the assumptions of receiving at least one 'HB' packet prior to the initialization of the IC algorithm and the eventual successful reception of the sent 'ENTER' and 'EXIT' messages. An advantage of this solution is the fact that there is no centralized entity to control the intersection crossing, avoiding single point of failures in the system. Regarding the evaluation process, the numerical analysis is very limited since it only considers two vehicles and consecutive receive-omission failures. Further testing with a high number of vehicles and with more arbitrary conditions in common traffic simulators and real-world implementations is necessary, in order to better evaluate the proposed algorithm.

Sawade et al. [15] propose a protocol for cooperative maneuvers under adverse conditions. The proposed solution relies on bidirectional stateful communication, i.e., an established session link connecting two or more participants on a collaborative driving maneuver. A synchronization layer is added on top of the bi-directional negotiation of collaborative maneuvers, through the utilization of the Turquoise algorithm for attaining distributed consensus under byzantine conditions. Participants must send heartbeat periodic messages in order to keep the session open. Once a predefined number of consecutive missed messages from a vehicle, the session is called unstable and can be terminated. Once in a session, any vehicle broadcasts the current session state in a hashed value. The session state must be consensual across the party of vehicles, so each bit of the hash is individually synchronized between stations. A parameter is used to control the robustness of the sessions against packet loss. This factor is a tradeoff between packets lost consecutively before a failure state is requested and the assurance of consensus among vehicles.

This work adds missing capabilities to the existing vehicular communications standards, through the integration of a collaborative maneuver protocol in the ETSI ITS-G5 protocol stack. The proposal has the advantage of introducing new features on the message-layer only, thus being backwards-compatible to current standard implementations. The main drawback of the work, however, is on the evaluation part, since only simulation results are provided for the specific case of a platoon with just two vehicles. Nevertheless, the conducted experiments show that a session would be stable 99% of the time for reasonable tradeoff values and environments with less than 20% of packet loss.

Nguyen et al. [17] also propose a protocol that encompasses the retransmission of safety messages that failed to broadcast. The protocol takes into account the presence of hidden nodes and their effect on communications faults. The proposed multi-channel MAC scheme (RAM) divides the control channel cycle in three main intervals: the safety interval, the response interval and the contention-based interval. Any collided safety packets can be retransmitted in the contention-based interval. Whenever a vehicle does not receive any safety packet within a time window from its neighbours, it will request an RSU to send one. The RSUs behave as a central authority inside a given area, being responsible for managing the duration of each cycle, tracking the exchanged messages and advertising the vehicles what packets were successfully received. Based on vehicle density and data traffic conditions, the RSU optimizes the length of the contention-based interval, by also taking into consideration the hidden terminal problem. A Markov chain model is used to analyze the reliability of the real-time transmission of safety packets and to provide information for the computation of the optimized control channel intervals. Simulation results show the improved performance of the proposed RAM protocol in terms of packet delivery ratio in comparison with two other related works.

Despite the increased reliability in the transmission of safety packets, the proposed RAM scheme cannot be directly applied using current vehicular communications equipment, since it requires some modifications to the standard MAC layer, due to the division of the control channel interval into three distinct phases: one congestion-based period (as the standard MAC protocol operates) and two congestion-free intervals. The protocol also introduces some additional overhead in the communications, as a result of the need to transmit acknowledgment messages and retransmission packets. Moreover, the solution has the drawback of assuming that vehicles are distributed along a straight line, in order to simplify the hidden terminal problem, which is typically not the case in real world conditions, where several roads interconnect with a lot of physical obstacles in the middle, either in urban or highway environments. The simulation results lack the implementation in standard traffic and network simulators software and the diversity of simulated traffic environments.

#### 4.2. Spatial Redundancy

In [7], Matthiesen et al. investigate the utilization of replicated application services in dynamic clusters of vehicles. The goal is to increase the reliability and availability of safety-critical applications in ad-hoc vehicular networks. The example of a distributed shared memory, which supports the operation of a stateful road-traffic information service, is presented in this work. Several metrics are analysed and evaluated for different cluster dimensions, such as data consistency, response time and application availability. A Replication Manager is employed in order to achieve stable clusters, by selecting replicas with good communication metrics that minimize service response time and reconfiguration overhead in case of faulty behaviour. These faults can be due for instance to excessive delay or high packet loss, which may affect timeliness and correctness of the service, thus leading to inconsistent application states.

The proposed fault-tolerant model has the advantage of not requiring any changes in the protocol stack, since the replication model is fully deployed at the application layer. On the other hand, however, overhead of replica selection and exchanging servers in case of failure is not taken into account and may have a significant impact in real-world operation, due to the topology changes and very dynamic environments in which vehicular networks operate. The model also does not consider network congestion scenarios, where the proposed solution may not operate as expected. With simulation results or real test-case measurements, these last points could be better evaluated, not being limited to the numerical analysis provided to validate only some parameters of the replication service.

The work of Cambruzzi et al. [10] proposes a failure detection scheme based on a protocol that detects both link and system failures. It employs a heartbeat mechanism in which all roadside units and vehicles transmit a beacon message periodically to their single-hop neighbours. When a beacon packet reaches its destination, the receiving node adds or updates its neighbours' list with the received information together with a timestamp of the packet. If no message is received from that neighbour



during a predefined time interval, the node is considered to be faulty and is inserted into a list of suspects. The algorithm uses adaptive timeouts in order to cope with the dynamic conditions of vehicular communication networks. In this model, only two types of faults are assumed. Those caused by a system crash and the ones caused by a vehicle exiting the road. Malicious or Byzantine faults are not considered in this study.

The fault model considered in the design of this failure detection scheme is very limited, since it only takes into account two type of faults, namely crash-faults (in case of equipment crash) and exit-faults (when a vehicle exits the road). For instance, babbling idiot failures are not analysed, which restricts the validity of the proposed model. Moreover, the impact of the exchange of tables, with the list of neighbours and their perceived status, in the communications overhead is neither discussed nor analysed. Finally, the simulation experiments consider only a simplified scenario with a straight road segment where all vehicles move in the same direction. In practice, this scenario may only happen in very few cases and, therefore, more complex environments should be evaluated, since the model depends significantly on the variation of network topology and link stability.

Based on a similar failure detection mechanism, Abrougui et al. [13] introduce a fault-tolerance location-based service discovery protocol for vehicular networks. This protocol handles the discovery procedure of different types of both safety and infotainment services and it was designed to perform well even in the presence of service provider failures, communication link failures and roadside units failures. The proposal relies on a cluster-based infrastructure, where roadside units are clustered around service providers, the congested areas of the vehicular network and the intermittent areas to improve the connectivity of the network. The proposed fault-tolerance mechanisms were introduced at the network level, in order to cope with several types of failures in the connection between the service provider and the service requester. Essentially, in case of link or system failure, an algorithm is employed to designate alternative nodes that will supply or forward the information missed in the faulty nodes/links. Simulation results showed an improvement in the success rate of discovery queries of approximately 50% and 30%, in case of a roadside router and link failure scenarios, respectively, when compared with a simplified version of the protocol without fault tolerance techniques.

However, this fault-tolerance scheme presents some disadvantages, such as the fact that the routing protocol is based on a non-standard solution (CLA-S), which requires some modifications in the protocol stack. Additionally, it introduces overhead in the communications protocol, by requiring mechanisms such as the leader election for the roadside routers. Despite the fact that the proposed fault detection mechanism is also able to detect intermittent failures, only permanent ones are considered in the simulation experiments. Moreover, no measurements of the time to recover from failures, e.g., including failure detection time and leader reelection phase, are presented.

Chang and Wang [16] propose a fault-tolerant protocol for a reliable broadcast of alert messages in vehicular ad-hoc networks. The goal of this protocol is to reduce the total number of messages needed to disseminate the alert message along the road. The proposed method designates the two farthest vehicles in the radio range of the source vehicle to act as candidate relay nodes of the message to be broadcast. This selection is performed by the source vehicle and it is based on the GPS coordinates provided by all vehicles in the transmission range. If the farthest vehicle from the source node does not transmit the safety message within a maximum time interval, the sub-farthest will assume that there was a system failure and will disseminate the intended message. The results show that the penetration rate of the fault-tolerant scheme is very satisfactory even for low traffic densities, providing advantages in relation to the simple flooding method in terms of transmission delay and total number of messages exchanged in the wireless medium.

The proposed protocol has the limitation of being specifically designed for network topologies typically found in the highway scenarios. For instance, in urban environments with a lot of road intersections, it could be important to disseminate warning messages in different directions. In such context, this solution with only one farthest and one sub-farthest vehicles can no longer be applied. In addition to this, the protocol requires some modifications both to the standard MAC and transport

layers, which means that it cannot be directly deployed using commercial off-the-shelf (COTS) components. Furthermore, the simulation experiments could include not only the testing of natural communications link limitations, but also communications faults and equipment crashes, in order to broaden the scope of the fault model analysis.

The work of Gérard Le Lann [18] deals with omission failures originated by a transient fault in the transmitter, receiver or in the communications channel. High reliability and strict timeliness properties are achieved through group dissemination protocols so that every message can be delivered to a given set of vehicles within a worst-case deadline. A Zebra protocol suite which comprises geocast, convergecast, multicast and the Altruistic protocol is employed to guarantee the timely delivery of messages. The proposed fault-tolerant strategy relies on the spatial redundancy provided by the multiple copies of information kept in the different vehicles. This approach would typically lead to high overhead, however, the notion of proxy sets is introduced in order to limit the scope size of the global dissemination protocol.

The proposed scheme has the main drawbacks of not considering permanent failures, i.e., equipment crashes, but only transient faults, and the fact that it specifically targets platooning applications, not being designed as a more generic solution for other safety-critical vehicular applications. It also requires changes to the standard protocol stack, namely at the MAC, routing and transport layers, by employing a suite of protocols (Zebra), specifically designed for time-critical single hop multipoint communications. Besides, it needs a more thoughtful evaluation, since neither simulation nor real test-case experiments were conducted.

Sanderson and Pitt [19] propose an adaptation of the *Paxos* algorithm [31] to implement consensus formation in self-organizing vehicular networks. The proposed algorithm (*IPcon*) handles institutionalized consensus in spite of faults occurring in the dynamic clusters of vehicles. The protocol tolerates faults caused by nodes that fail by permanently stopping or later restarting, delayed, lost or duplicated messages, however, malicious vehicles and corrupted packets are not considered. The evaluation of the algorithm demonstrates the resilience against role failures (nodes may play four different roles in the *IPcon* protocol) and cluster fragmentation and aggregation.

One of the limitations of the proposed solution is that it does not take into account all faults in the value domain, e.g., corrupted message content. Moreover, the communications overhead of the consensus algorithm (*IPCon*) may have some negative impact on the timeliness of safety-critical applications running on top of vehicular networks. Similarly, the leader election and conflict resolution processes could also consume a considerable amount of time to be executed. Practical evaluation regarding these time measurements should be carried out, in order to assess the validity of the proposed scheme under dynamic real-world scenarios.

A fault detection protocol is introduced in [20] by Aljeri et al. in order to mitigate communications problems in vehicular networks. Fault diagnosis is performed by comparing the output messages from a group of vehicles. This way, it is possible to identify faulty vehicular nodes. The process is initiated by an RSU, which attributes the same task to a group of vehicles. Then, the results are computed by each node and the answers are transmitted back to the initiator. If the results are identical, it is assumed that there are no faults in the network. On the other hand, if different results are yielded, faulty road components can be detected. Additionally, a more efficient implementation of the protocol is proposed that relies on regional RSUs, which decreases the total number of packets transmitted and the diagnosis latency of this method.

The proposed fault detection mechanism implies additional network resource usage, in order to identify faulty nodes. The tasks assigned to pairs of vehicles, with the goal of verifying disagreements and diagnosing faults, introduce some communications rounds and consume processing time. It is not a transparent solution that takes advantage of the messages already exchanged inside the vehicular network. Additionally, it is assumed that two faulty vehicles always give different outputs, which may not always be the case, e.g., in common failure mode. Another drawback relies on the fact that the fault detection scheme only targets networks where roadside units are present. There is no alternative

framework devised for communications solely among clusters of vehicles, or for the specific case when there is a permanent failure in the gateway node, which behaves as a single point of failure in the network.

In [21], Casimiro et al. develop a kernel-based architecture (KARYON) for safety-critical coordination in vehicular systems. Besides dealing with sensor faults and real-time properties of the wireless communications (e.g., self-stabilizing protocol), the proposed architecture also introduces extra components to the standard MAC layer. According to the followed subsystem isolation, the authors assume in the fault model that communication components can experience crash or timing faults, however, data cannot be corrupted, i.e., faults may occur in the time domain, but not in the value one. In addition to the standard MAC layer, two extra elements are introduced: the mediator Layer (MLA) and the Channel Control Layer. For example, the MLA is responsible for node failure detection and membership and control of temporary network partitions. On the other hand, the channel control layer supervises the channel state and enhances the network resilience by taking advantage of the diversity of radio channels available for vehicular communications purposes.

The main disadvantage of the devised architecture is the need for introducing several changes in the protocol stack, especially at the MAC layer level, so that some extra functionalities that are not present in current COTS components become available. As already mentioned, in the communications modules of the system, not all types of faults are covered, since crash or timing faults are tolerated, but not data corrupted messages. Finally, no evaluation is performed in this publication, that is part of the future work, so there is no way to validate the performance of the proposed fault-tolerant solution.

The work of Worrall et al. [22] deals not only with the complete loss of radio communications but also with partial degradation of the wireless link. In some cases, the communications performance is affected in an intermittent way or behaves poorly after a certain distance, due e.g., to damages in the external cables, antennas or connector. The proposed method utilizes data gathered during normal operation so that the antenna behaviour can be modelled and used in future fault detection. This model is derived by analysing and learning the properties of wireless communications in a fleet of vehicles, taking into account parameters such as relative orientation, bearing and range between vehicles. The detailed knowledge about the communications performance is then utilized to detect partial antennas faults or permanent link failures, which are identified by observing when the RF communications deviate from the expected operation. Additional computational resources are required in order to allow online execution of the mathematical model and appropriate comparison with the run-time results of the antenna performance.

The proposed fault detection mechanism is not suitable for a large number of vehicular communications applications, which are based on broadcast messages, since this solution is specifically designed for point-to-point radio links. The scheme only covers faults in the physical air interface, namely cable and antenna performance degradation, not detecting any time and value issues in the exchanged messages. Furthermore, the real test case results show that the settling time for statistically detecting healthy antenna behaviour may be relatively long, which may be critical in constantly changing network topologies with frequent communications links disruption.

Platooning applications constitute a particular use case scenario of vehicular communications. Ploeg et al. [23] address the problem of faulty links in a platoon of vehicles. A safe distance between the members of the platoon is continuously computed by taking into consideration the availability of sensor data and the communications link performance. This safe distance is employed by the cooperative adaptive cruise control (CACC) system according to a graceful degradation scheme that adjusts the settings of CACC to keep as much functionality as possible, even in the presence of faults, but always guaranteeing string stability in the platoon. Moreover, two different network topologies can be applied, depending on the time delay of the communications link. If this delay exceeds a predefined threshold value, the platoon service switches from a one-vehicle look-ahead topology to a two-vehicle look-ahead configuration. This fault-tolerance strategy can only be applied if the delay time is not excessively large, otherwise, wireless communications should not be employed in order to preserve string stability.

The described fault-tolerant scheme targets only a particular application, i.e., vehicle platooning, being tied to a concrete network topology and thus not very useful to other use case scenarios. The fault model only takes into account large delay values that may affect the timeliness of the communications links, not considering faults in the value domain of the transmitted packets. Additionally, only numerical results are provided, which makes it difficult to evaluate the performance of the system under real environments with adverse conditions.

In [24], Fathollahnejad et al. propose a synchronous group formation (GF) algorithm to enhance self-organizing vehicular applications under the presence of an unbounded number of asymmetric communication failures. The main goal of the GF algorithm is to achieve agreement, or at least to reduce the probability of unsafe disagreement, on the membership of a cooperative ITS application, e.g., virtual traffic light (VTL) systems. A decision mechanism is employed by each member node (vehicle) to identify the other nodes in the group at each moment in time. The mechanism relies on the utilization of an extra component, designated as *oracle*. These *oracles* are local devices present in each node and are responsible for detecting the remaining participants in the group. The obtained simulation results show that when the local *oracles* provide a correct estimate of the group formation, only safe disagreement scenarios may occur. However, when the *oracles* underestimate the total number of nodes, unsafe disagreement situations may happen and the likelihood of such scenarios increases with the probability of receive omissions in the communications channel.

This work excludes process failures, only dealing with faults in the communications links and more specifically just receive omissions faults, so faults in the value domain are also outside of the scope of the fault model. Moreover, communications overhead for leader election, leader handover or VTL group formation protocol is not discussed and analysed, and the leader election and leader handover mechanism are not yet designed, being part of future work. Finally, the evaluation section only presents numerical results, there are no experiments conducted in more realistic traffic/network simulation or test case environments.

Bhoi and Khilar [25] introduce a fault-tolerant routing protocol for vehicular ad-hoc communications in urban environments. A fault detection technique is used by the vehicle itself to detect if its own operation is fault free or not. If a faulty behaviour is identified, the on-board unit (OBU) does not participate any longer in the routing process. The fault detection mechanism targets soft faults, i.e., erroneous behaviour in the OBU devices causing the generation of incorrect data for a long period of time. This may be caused by high noise affecting the node's operation, making it still able to compute, send and receive information. However, beaconing data transmitted by the vehicle cannot be considered valid, being that this information (position, speed, etc.) is indispensable for hop selection in the routing algorithm. For that reason, these nodes are automatically excluded from the routing process by self-detecting these soft faults, through the analysis of the RSSI values from the received messages and the location coordinates provided by the neighbouring nodes. The proposed protocol provides good results in terms of end-to-end delay, path length and false alarm rate.

The proposed routing protocol just takes into account faults in the value domain, e.g., incorrect data in the position or speed information, not considering the possibility of nodes introducing timing faults, such as large delay values. It is also assumed that the faulty vehicles always provide incorrect data and only by accident the information may be correct. This simplifies the fault detection mechanism but could be a not very realistic situation, since nodes may present intermittent faults that only arise in some occasions. The overhead of exchanging decision messages regarding the state (soft faulty or fault free) of neighbouring vehicles is neither discussed nor analysed. Furthermore, despite the decentralized fault detection scheme, the routing and path value calculation algorithm depends on RSU nodes, which are single points of failure in this forwarding scheme.

The work of Mourad Elhadef [26] suggests the utilization of a primary-backup approach for the design of a fault-tolerant intersection control algorithm. The VTL system is based on a centralized solution, with an RSU controller responsible for coordinating all traffic crossing the intersection. The controller manages the vehicles approaching the site, by granting or denying access to the

intersection, in order to guarantee safety, liveness and fairness, while at the same time maximizing traffic throughput. Both the primary and the backup controllers are constantly synchronizing with each other, so that the backup unit can always be kept updated with all the necessary traffic information. Only permanent crash failures are considered in the fault model. Whenever the main controller stops sending and receiving messages (a keep alive timer is used to detect if the primary node is down), the backup unit takes control of the intersection.

This fault-tolerant intersection control algorithm has the drawback of not dealing with intermittent faults and message errors in the value domain, by only considering permanent crash failures. Besides that, it focus on a specific application (intersection management), while a more generic solution could be devised with the same primary-backup approach for master nodes of vehicular networks that rely on centralized or hybrid architectures. Furthermore, no evaluation of the proposed scheme is carried out, namely in terms of recovery delay after primary replica failure.

An RSU-backup replication scheme is proposed by Almeida et al. [27] in the scope of a fault-tolerant infrastructure-based architecture for vehicular networks. In this framework, the RSUs behave as the masters of the network, controlling time slot scheduling of the OBUs and admission control policies. They have a crucial role in the network operation, acting as single point of failure, and therefore, any fault affecting these nodes may cause a disruption in the time-sensitive communications for safety-critical applications. The work introduces a full replication scheme, where a backup node executes the exact same processes as the primary fail-silent replica. This parallel operation allows the system to perform a very fast recovery procedure in case of failure of the primary node. As a result, the real-time communications protocol does not suffer any discontinuity even in the presence of network faults, thus enhancing the overall dependability of vehicular system.

The replication mechanism proposed in this work consists in a cross-layer approach, since it requires the duplication of the entire RSU node from the physical up to the application layer. Unfortunately, there is no cost-benefit analysis for this solution, since the complete replication of hardware and software parts is expensive and could be compared against other possibilities, such as the option for non fail-silent RSUs and the use of backup ones operating in another channel frequency. Moreover, the deterministic MAC protocol that is on the basis of this architecture also needs some changes to the standard vehicular communications protocols, so the solution cannot be seamlessly implemented on COTS components. Finally, the fault-tolerant system was only tested in a controlled laboratory environment. Some testing in close-to-real world scenarios could give an improved understanding of system's reliability under the presence of hardware, software or communications channel faults.

In [28], Medani et al. develop a time synchronization strategy for the nodes of vehicular networks. Clock synchronization is essential to support the correct operation of safety-critical applications in road traffic environments (e.g., for event causality, medium access control or security purposes). The proposed method, named Offset Table Robust Broadcasting, attains high accuracy and presents fault-tolerant capabilities so that every node is aware of neighbouring clock times and is able to synchronize its communications with other nodes. The clock offsets among several nodes are computed using a round-trip time mechanism and acknowledgement messages are exchanged to ensure that the offset table delivery reaches all nodes.

In order to achieve higher clock synchronization, the proposed scheme introduces some communications overhead, both for the transporter node selection and cluster formation but also for the entire synchronization process that involves collecting timing information, calculate offsets table and disseminate the computed data. Additionally, it requires the modification of the clock synchronization source in the node, which may be sometimes difficult to implement in COTS components. Finally, it would be interesting to perform some field trials evaluation, in order to have real GPS errors and uncertainties in the synchronization process.

A multipath routing protocol is proposed by Devangavi et al. [29], in order to enhance reliability and fault tolerance. Multiple paths are computed from source to the destination node based on Bezier curves. These curves are traced by the parent RSU according to the geographical location of the different nodes in the network on a multi-hop coverage area. The calculation of these paths is also based on several parameters, such as the available bandwidth in the network, the data size to be transmitted and the distances from source to destination. The distinct paths are then prioritized and utilized to forward the information to the destination vehicle, introducing a flexible degree of redundancy in message transmission. The proposed solution was evaluated taking as example the city of Bangalore and the simulation results obtained in NS-2 proved the superior performance of the protocol in comparison with other solutions in the literature and with respect to transmission time and packet delivery ratio.

The proposed protocol is based on a centralized architecture, where RSU nodes are responsible for multipath finding process and network management tasks. However, these nodes are single point failures that in case of permanent crash, disrupt network operation. Furthermore, it is assumed that every vehicle is always connected to at least one RSU, which limits the applicability of the proposed solution in real-world scenarios. It should also be noted that a prioritized path list must be computed for every source-destination pair of vehicles involved in message exchange, which introduces a significant amount of communications overhead that is not evaluated in the simulation experiments.

In [30], Younes et al. propose the FT-PR protocol, a fault-tolerant path recommendation system. In this work, vehicles within a reporting area are responsible for disseminating the traffic characteristics of a road segment. The process is cumulative, since a road segment can have multiple reporting areas. Transmitting vehicles gather information on surrounding clusters and a report is completed as soon as it encompasses the entire road segment. Road-side units (RSUs), assumed to be located at each road intersection, exchange information with each other and calculate the best road segments for specific destinations. RSUs start broadcasting destinations and the best turn towards them. From this part forward, the process is iterative, vehicles entering a road segment receive the path recommendation information and may progress towards the road network. Different techniques are used to improve the robustness of the system, For instance, in order to enhance the traffic collection phase, vehicles can request updates by disseminating vehicles missing in the report description. Furthermore, in case of an RSU error, the nearby RSUs can assume their roles and transmit their information. Additionally a vehicle can retransmit messages from an RSU, in order to increase the RSU communication radius.

The main contribution of this work consists in the designation of redundant routing paths for multi-hop communications, in order to compensate for RSU failures. The solution does not address the issue of a vehicle reaching a specific RSU node, e.g., one responsible for a safety-critical task, such as controlling a road intersection. If the destination RSU is faulty, no redundant node is available to perform the expected task. Another drawback of the proposed protocol is that the selection of a cluster head for each reported area, a constantly dynamic process, may introduce a significant amount of overhead, which may be critical in terms of delay. Nothing is mentioned in the article about how this selection process is conducted. In terms of results, by using FT-PR protocol, vehicles were able to obtain the optimal path even if 40% of installed RSUs failed to process or forward the advertisement messages. However, the obtained simulation metrics are not generic and were only evaluated for specific layout scenarios. More realistic situations should be considered for further analysis.

#### 4.3. Information Redundancy

Finally, with respect to information redundancy mechanisms, the identified solutions are based on network coding techniques. For instance, the work of Kumar and Dave [8] introduces a decentralized method that provides reliable and scalable vehicular communications, independently of the traffic density level. The solution employs network coding and random walks in order to deal with the constantly changing topologies, varying vehicle density and unreliable channel conditions of vehicular networks. Raptor codes, which are characterized by its low complexity and thus fast decoding, are used

to encode and disseminate information in a completely distributed manner, providing better fault tolerance. In this scheme, a vehicle transmits its data to a random set of neighbouring vehicles and then each vehicle only encodes the information it has received. Posteriorly, a receiving vehicle can efficiently decode the transmitted data by collecting a sufficient amount of data blocks from the network nodes it interacts with while moving. Random walks are utilized to disseminate the data, avoiding the need for supporting a generic layer of routing protocols. The performance evaluation of the proposed scheme is evaluated through simulation and the results are compared against the simple broadcast framework (store and forward strategy) and other related work in the literature. Data overhead and average end-to-end delay are kept low for different traffic densities and data sending rates, while network reachability and packet delivery ratio are improved in comparison with the other analysed solutions.

The suggested scheme requires changes to the standard physical and routing layers, due to encoding/decoding process and data forwarding mechanisms. As a result, it cannot be directly deployed on top of COTS equipment, by just operating at the application level. The method also introduces some communications overhead in exchange for increased redundancy, but completely manageable according to the simulation results. Finally, the performance of the proposed method could be further evaluated by using more realistic traffic models in the simulation tools or by taking results in field trial scenarios.

Eze et al. [11] also propose an innovative communications scheme based on the network coding concept, named Coding Aided Retransmission-Based Error Recovery (CARER). The goal is to improve broadcast reliability and timely delivery of messages with lower number of retransmissions. In this scheme, each node performs an exclusive OR (XOR) operation on a set of both received and generated packets and then send these encoded messages to all the vehicles in a one-hop distance. The advantage of this technique over simply broadcasting the raw packets is that it allows nodes to recover lost frames with low communications overhead. Additionally, the protocol uses a location-aware algorithm that selects an appropriate vehicle for rebroadcasting the encoded packet towards the desired propagation direction. The traditional Request-to-Broadcast/Clear-to-Broadcast (RTB/CTB) handshake is used to overcome hidden node problem and reduce collisions in the wireless medium. An analytical model was developed and simulation tests were performed to evaluate the performance of the protocol. The results show an increased packet recovery probability and a lower packet collision probability when compared to the simple repetition based error recovery scheme with no network coding mechanism involved.

The protocol only takes into consideration faults in the communications links, not dealing with node failures, which may be critical for the operation of the location-aware algorithm that selects a specific node to retransmit the encoded packets. Moreover, the utilization of the RTB/CTB handshake introduces some communications overhead that is analysed but not evaluated in the experimental results section, in terms of total end-to-end delay. Finally, the protocol presents satisfactory results for a straight road scenario with no intersection, which is typically not the case in urban environments, where an inappropriate node can be easily selected to retransmit the encoded packets, i.e., forwarding them in the wrong direction. These more complex and dense topologies must be further evaluated.

Ali et al. [14] addresses one of the main challenges in vehicular communications, the degradation of radio propagation. It proposes a protocol for code-relaying information at road intersections. In the proposed scheme, a station can mediate messages between two other vehicles, B and C, by broadcasting a XOR of the received periodic status messages from both B and C. B and C can retrieve each other's messages by performing the same operation and removing their own messages. The protocol was implemented in NS3 and tested using SUMO, showing that the impact of path loss, fading and shadowing can be highly mitigated by the before-mentioned technique. In particular, it showed that using coded relay, a station could expect higher packet delivery rates and smaller latency (per-instance). Unfortunately, due to the relay mechanism, it takes more time to perform successful reception.

The proposed solution handles communications links faults, such as packet drops, but not node failures or faults in the value domain, e.g., incorrect data messages. This is particularly important for the proposed relaying at road intersection, where a relay node assists the message exchange. These relays

are single point of failures in the communications framework, that in case of faulty behaviour, will compromise the packet forwarding operation. Furthermore, this is even more challenging when the relay node is not an RSU but an opportunistic vehicle that, due to its speed, may only create temporary and unstable connection.

#### 4.4. Discussion

Table 2 provides a comparison among different aspects of the selected documents. A description of the proposed fault-tolerance technique is depicted, including the main applicability, the method used, the target scenario (urban, highway or both) and the structure or architecture of the proposal (centralized, distributed or hybrid). With respect to the fault-tolerance or fault-detection method itself, the technique is classified according to its type, the protocol layer in which operates and the methodology to provide error handling, fault handling or both [2]. Finally, the publications are compared in terms of the evaluation performed, namely the parameters measured, and type of analysis carried out (analytical model, numerical, simulation or real testbed).

Most of the articles provide decentralized solutions, but there are also some hybrid and centralized architectures. Regarding the classification of the protocol stack layer in which the fault-tolerant behaviour is provided, this is not a very straightforward task, since many solutions have an impact at multiple levels. When it is clear that a contribution has a cross-layer approach, the different layers are mentioned, otherwise the most suitable protocol layer is selected for trying to categorize the proposed solution. The protocol layers division is based on the standard protocol stack for wireless vehicular communications [32], namely splitting into the physical, MAC and LLC, network, transport and application layers.

The fault tolerance methods were also analysed in terms of the error handling and fault handling mechanisms used. With respect to the error handling techniques, most of the articles proposed a compensation scheme, in which the erroneous state contains enough redundancy to enable error to be masked, however, in some cases, a rollforward strategy was followed, where the system jumps to a new state without detected errors. For the fault handling part, reconfiguration of the system was typically employed, either switching in spare components or reassigning tasks among non-failed components, while in some solutions isolation and reinitialization mechanisms were also included. Regarding the evaluation process of the proposed solutions, a set of different parameters were evaluated in each case, but most of them relied on analytical models, numerical analysis or simulation results. Only in two articles, a real testbed was used.

In summary, most of the existing fault-tolerance techniques proposed in the literature only take into consideration specific vehicular communications applications, not being designed to support the full range of services enabled by these networks. Moreover, these solutions typically cover just a small number of faults affecting the vehicular communications system, focusing for instance on a particular layer of the protocol stack, e.g., routing protocol. As a result, none of the solutions can fully address the stringent dependability requirements of such safety-critical wireless systems, namely the high reliability and availability levels. For that to happen, an integrated approach of the entire network architecture needs to be taken into account, with an extended fault coverage of the system's operation. In addition to this, more practical implementations of fault-tolerant methods need to be developed, in order to evaluate the proposed mechanisms with field experimental results.



Table 2. Comparison of selected documents.

	Description			Fault Detection/Fault Tolerance						Evaluation			
	Applicability	Method	Scenario	Structure	Type	Layer	Error Handling	Fault Handling	Parameters	Analytical Model	Numerical Analysis	Simulation	Real Test-Case
Jonsson et al. [6]	Platooning	Message Retransmission	Generic	Centralized	Temporal	Transport	Compensation	—	<ul style="list-style-type: none"> <li>• Message Error Rate</li> <li>• Channel Busy Time</li> </ul>	✓	✗	Matlab	✗
Böhm and Kunert [9]	Platooning	Message Retransmission	Generic	Centralized	Temporal	Transport	Compensation	—	<ul style="list-style-type: none"> <li>• Packet Delivery Ratio</li> <li>• Data Age</li> </ul>	✗	✗	MatLab	✗
Savic et al. [12]	Intersection Control	Message Retransmission	Urban	Decentralized	Temporal	Transport	Compensation	—	<ul style="list-style-type: none"> <li>• Packet Delivery Ratio</li> <li>• Average Delay</li> </ul>	✓	✓	✗	✗
Sawade et al. [15]	Coordinated Maneuvers	Bidirectional Stateful Communication + Distributed Consensus	Highway	Decentralized	Temporal	Transport	Compensation	—	<ul style="list-style-type: none"> <li>• Unstable Session Ratio</li> </ul>	✗	✗	VSimRTI	✗
Nguyen et al. [17]	Distributed ITS Applications	Message Retransmission	Highway	Centralized	Temporal	Transport	Compensation	—	<ul style="list-style-type: none"> <li>• Packet Delivery Ratio</li> </ul>	✓	✓	MatLab	✗
Matthiesen et al. [7]	Service Replication	Petri Networks + Markov Chains	Generic	Decentralized	Spatial	Network	Compensation	Reconfiguration	<ul style="list-style-type: none"> <li>• Service Availability</li> <li>• Group Consistency</li> </ul>	✓	✓	✗	✗
Cambuzzi et al. [10]	Distributed ITS Applications	Failure Detection System	Generic	Decentralized	Spatial	Application	—	—	<ul style="list-style-type: none"> <li>• Percentage of False Suspitions</li> <li>• Average Time of Detection</li> <li>• Average Time of Recovery</li> </ul>	✗	✗	OMNET++	✗
Abrougui et al. [13]	Service Discovery	Spanning Tree Reconstruction	Generic	Centralized	Spatial	Application	Rollforward	Reconfiguration	<ul style="list-style-type: none"> <li>• Recovery Success Rate</li> <li>• Used Bandwidth</li> <li>• Response Time</li> </ul>	✓	✓	✗	✗
Chang and Wang [16]	Message Broadcast	Relay Candidates Selection	Highway	Hybrid	Spatial	Network	Compensation	Reconfiguration	<ul style="list-style-type: none"> <li>• Number of Messages</li> <li>• Transmission Delay</li> <li>• Penetration Rate</li> </ul>	✗	✗	NS-2	✗
Le Lann [18]	Platooning	Cohorts + Proxy Sets + Zebra protocols suite	Generic	Hybrid	Spatial	Network	Compensation	Reconfiguration Reinitialization	<ul style="list-style-type: none"> <li>• Worst Case Termination Time</li> </ul>	✓	✓	✗	✗
Sanderson and Pitt [19]	Distributed Databases	Institutionalised Consensus	Generic	Hybrid	Spatial	Application	Compensation	Reconfiguration Reinitialization	<ul style="list-style-type: none"> <li>• Packet Delivery Ratio</li> <li>• Data Overhead</li> <li>• Average Delay Network</li> <li>• Reachability</li> </ul>	✓	✗	✗	✗
Aljeri et al. [20]	Roadside ITS Applications	Spanning Tree Reconstruction	Generic	Centralized	Spatial	Application	Rollforward	Isolation Reinitialization	<ul style="list-style-type: none"> <li>• Number of Packets</li> <li>• Diagnosis Latency</li> </ul>	✗	✗	NS-2	✗
Casimiro et al. [21]	Vehicle Coordination	Failure Detection System + Graceful Degradation	Generic	Decentralized	Spatial	MAC and Network	Rollforward	Reconfiguration	—	✗	✗	✗	✗
Worrall et al. [22]	Distributed ITS Applications	Radio Redundancy + Machine Learning	Generic	Decentralized	Spatial	Physical	Compensation	Reconfiguration	<ul style="list-style-type: none"> <li>• Antenna Performance</li> </ul>	✗	✗	✗	✓
Ploeg et al. [23]	Platooning	Communication Topology Adaptation	Generic	Decentralized	Spatial	Network	Compensation	Reconfiguration	—	✓	✓	✗	✗

Table 2. Cont.

Description			Fault Detection/Fault Tolerance						Evaluation				
Fathollahnejad et al. [24]	Group Formation	Consensus	Generic	Centralized	Spatial	Application	Rollforward	—	<ul style="list-style-type: none"> <li>• Probability of Safe Disagreement</li> <li>• Probability of Unsafe Disagreement</li> </ul>	✓	✓	✗	✗
Bhoi and Khilar [25]	Multi-hop Routing	Self Soft Fault Detection	Urban	Decentralized	Spatial	Network	Compensation	Isolation Reconfiguration	<ul style="list-style-type: none"> <li>• Fault Detection Rate</li> <li>• False Alarm Rate</li> <li>• End-to-end Delay</li> <li>• Number of gaps</li> <li>• Number of hops</li> </ul>	✓	✗	MatLab	✗
Elhadef [26]	Intersection Control	Controller Redundancy	Urban	Centralized	Spatial	Application	Compensation	Reconfiguration	—	✗	✗	✗	✗
Almeida et al. [27]	Distributed ITS Applications	RSU Replication Scheme	Generic	Centralized	Spatial	Application	Compensation	Isolation	<ul style="list-style-type: none"> <li>• Backup Replica Offset</li> </ul>	✗	✗	✗	✓
Medani et al. [28]	Time Synchronization	Offsets Table Broadcasting Protocol	Generic	Hybrid	Spatial	Network	Rollforward	Reconfiguration Reinitialization	<ul style="list-style-type: none"> <li>• Message Complexity</li> <li>• Convergence Time</li> <li>• Synchronization Rate</li> </ul>	✓	✓	NS-2 VanetMobiSim	✗
Devangavi et al. [29]	Multi-hop Routing	Bezier Curves + Path Redundancy	Generic	Centralized	Spatial	Network	Compensation	—	<ul style="list-style-type: none"> <li>• Transmission Time</li> <li>• Packet Delivery Ratio</li> </ul>	✗	✗	NS-2	✗
Younes et al. [30]	Road Path Recommendation	Path Redundancy	Urban	Decentralized	Spatial	Network	Compensation	—	<ul style="list-style-type: none"> <li>• Average Traveling Time</li> <li>• Average Traveling Distance</li> <li>• Number of Sent Packets</li> <li>• Average Delay Time</li> <li>• Un-tolerated Scenarios</li> <li>• Correctness</li> </ul>	✗	✗	NS-2 + SUMO	✗
Kumar and Dave [8]	Message Broadcast	Network Coding + Raptor Codes + Markov Chains	Generic	Decentralized	Information	Network	Compensation	—	<ul style="list-style-type: none"> <li>• Packet Delivery Ratio</li> <li>• Data Overhead</li> <li>• Average Delay Network Reachability</li> </ul>	✗	✗	NS-2 SUMO MOVE	✗
Eze et al. [11]	Message Broadcast	Network Coding + Message Retransmission	Highway	Decentralized	Information	Network and Transport	Compensation	—	<ul style="list-style-type: none"> <li>• Packet Recovery Probability</li> <li>• Packet Collision Probability</li> </ul>	✓	✗	NS-2 Bonn-Motion tool	✗
Ali et al. [14]	Intersection Control	Network Coding + Message Relaying	Urban	Decentralized	Information	Network	Compensation	—	<ul style="list-style-type: none"> <li>• Expected per-instance latency</li> <li>• Time to successful reception</li> <li>• Packet Delivery Rate</li> </ul>	✓	✗	NS-3 SUMO	✗

## 5. Conclusions

In this work, a systematic and comprehensive survey on fault tolerance techniques for wireless vehicular networks was conducted. In summary, there are not many research works in the area of fault-tolerance specifically focusing on wireless vehicular communications. However, an increasing trend can be observed in the recent years, with more protocols, mechanisms and architectures being proposed in order to enhance the dependability attributes of wireless vehicular networks. A systematic process to select publications from a large dataset was followed, choosing the ones that are more relevant and specifically focused on fault-tolerance in wireless vehicular communications. The analysed papers show that the development of safety-critical applications in such dynamic environments require a careful planning that preserves the system's flexibility and real-time guarantees while providing fault-tolerance capabilities. As a conclusion, there is still a shortage of strategies to completely fulfil the operation of dependable vehicular networks. Nevertheless, this is a crucial requirement of vehicular communications, namely for the safety-critical applications supported by these networks.

**Author Contributions:** Conceptualization and methodology, J.A. and J.F.; formal analysis, investigation, writing—original draft preparation and visualization, J.A. and J.R.; writing—review and editing, M.A. and J.F.; supervision and project administration and funding acquisition, J.F.

**Funding:** This work is supported by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework [Project TRUST with Nr. 037930 (POCI-01-0247-FEDER-037930)].

**Conflicts of Interest:** The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

## References

- Gärtner, F.C. Fundamentals of Fault-tolerant Distributed Computing in Asynchronous Environments. *ACM Comput. Surv.* **1999**, *31*, 1–26. doi:10.1145/311531.311532.
- Avizienis, A.; Laprie, J.C.; Randell, B.; Landwehr, C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable Secur. Comput.* **2004**, *1*, 11–33. doi:10.1109/TDSC.2004.2.
- Lima, A.; Rocha, F.; Völöp, M.; Esteves-Verissimo, P. Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, CPS-SPC '16, Vienna, Austria, 28 October 2016; ACM: New York, NY, USA, 2016; pp. 59–70. doi:10.1145/2994487.2994489.
- Jhumka, A.; Kulkarni, S. On the Design of Mobility-Tolerant TDMA-Based Media Access Control (MAC) Protocol for Mobile Sensor Networks. In *Distributed Computing and Internet Technology*; Janowski, T., Mohanty, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2007; pp. 42–53.
- Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *BMJ* **2009**, *339*, doi:10.1136/bmj.b2535.
- Jonsson, M.; Kunert, K.; Böhm, A. Increased Communication Reliability for Delay-Sensitive Platooning Applications on Top of IEEE 802.11p. *Proceedings of the Communication Technologies for Vehicles: 5th International Workshop, Nets4Cars/Nets4Trains 2013, Villeneuve d'Ascq, France, 14–15 May 2013*; Berbineau, M., Jonsson, M., Bonnin, J.M., Cherkaoui, S., Aguado, M., Rico-Garcia, C., Ghannoum, H., Mehmood, R., Vinel, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 121–135. doi:10.1007/978-3-642-37974-1\_10.
- Matthiesen, E.V.; Hamouda, O.; Kaâniche, M.; Schwefel, H.P. Dependability Evaluation of a Replication Service for Mobile Applications in Dynamic Ad-Hoc Networks. In *Service Availability*; Nanya, T., Maruyama, F., Pataricza, A., Malek, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 171–186.
- Kumar, R.; Dave, M. DDDRC: Decentralised data dissemination in VANET using raptor codes. *Int. J. Electron.* **2015**, *102*, 946–966, doi:10.1080/00207217.2014.945193.
- Böhm, A.; Kunert, K. Data age based MAC scheme for fast and reliable communication within and between platoons of vehicles. In Proceedings of the 2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), New York, NY, USA, 17–19 October 2016; pp. 1–9. doi:10.1109/WiMOB.2016.7763224.

10. Cambrozzi, E.; Farines, J.M.; Macedo, R.J.; Kraus, W. An adaptive failure detection system for Vehicular Ad-hoc Networks. In Proceedings of the 2010 IEEE Intelligent Vehicles Symposium, San Diego, CA, USA, 21–24 June 2010; pp. 603–608. doi:10.1109/IVS.2010.5548015.
11. C., E.E.; Zhang, S.; Liu, E. Improving Reliability of Message Broadcast over Internet of Vehicles (IoVs). In Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, UK, 26–28 October 2015; pp. 2321–2328. doi:10.1109/CIT/IUCC/DASC/PICOM.2015.343.
12. Savic, V.; Schiller, E.M.; Papatriantafilou, M. Distributed algorithm for collision avoidance at road intersections in the presence of communication failures. In Proceedings of the 2017 IEEE Intelligent Vehicles Symposium (IV), Los Angeles, CA, USA, 11–14 June 2017; pp. 1005–1012. doi:10.1109/IVS.2017.7995846.
13. Abrougui, K.; Boukerche, A.; Ramadan, H. Performance evaluation of an efficient fault tolerant service discovery protocol for vehicular networks. *J. Netw. Comput. Appl.* **2012**, *35*, 1424–1435. doi:10.1016/j.jnca.2011.10.007.
14. Ali, G.G.M.N.; Noor-A-Rahim, M.; Chong, P.H.J.; Guan, Y.L. Analysis and Improvement of Reliability Through Coding for Safety Message Broadcasting in Urban Vehicular Networks. *IEEE Trans. Veh. Technol.* **2018**, *67*, 6774–6787. doi:10.1109/TVT.2018.2820458.
15. Sawade, O.; Schulze, M.; Radosch, I. Robust Communication for Cooperative Driving Maneuvers. *IEEE Intell. Transp. Syst. Mag.* **2018**, *10*, 159–169.
16. Chang, Y.C.; Wang, T.P. A fault-tolerant broadcast protocol for reliable alert message delivery in vehicular wireless networks. In Proceedings of the 7th International Conference on Communications and Networking in China, Kun Ming, China, 8–10 August 2012; pp. 475–480. doi:10.1109/ChinaCom.2012.6417530.
17. Nguyen, V.; Khanh, T.T.; Oo, T.Z.; Tran, N.H.; Huh, E.; Hong, C.S. A Cooperative and Reliable RSU-Assisted IEEE 802.11P-Based Multi-Channel MAC Protocol for VANETs. *IEEE Access* **2019**, *7*, 107576–107590. doi:10.1109/ACCESS.2019.2933241.
18. Lann, G.L. On the Power of Cohorts—Multipoint Protocols for Fast and Reliable Safety-Critical Communications in Intelligent Vehicular Networks. In Proceedings of the 2012 International Conference on Connected Vehicles and Expo (ICCVEx), Beijing, China, 12–16 December 2012; pp. 35–42. doi:10.1109/ICCVEx.2012.15.
19. Sanderson, D.; Pitt, J. Institutionalised Consensus in Vehicular Networks: Executable Specification and Empirical Validation. In Proceedings of the 2012 IEEE Sixth International Conference on Self-Adaptive and Self-Organizing Systems Workshops, Lyon, France, 10–14 September 2012; pp. 71–76. doi:10.1109/SASOW.2012.21.
20. Aljeri, N.; Almulla, M.; Boukerche, A. An Efficient Fault Detection and Diagnosis Protocol for Vehicular Networks. In Proceedings of the Third ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, Barcelona, Spain, 3–8 November 2013; ACM: New York, NY, USA, 2013; DIVANet '13, pp. 23–30. doi:10.1145/2512921.2512935.
21. Casimiro, A.; Kaiser, J.; Schiller, E.M.; Costa, P.; Parizi, J.; Johansson, R.; Librino, R. The KARYON project: Predictable and safe coordination in cooperative vehicular systems. In Proceedings of the 2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W), Budapest, Hungary, 24–27 June 2013; pp. 1–12. doi:10.1109/DSNW.2013.6615530.
22. Worrall, S.; Agamnoni, G.; Ward, J.; Nebot, E. Fault Detection for Vehicular Ad Hoc Wireless Networks. *IEEE Intell. Transp. Syst. Mag.* **2014**, *6*, 34–44. doi:10.1109/MITS.2014.2304974.
23. Ploeg, J.; van de Wouw, N.; Nijmeijer, H. Fault Tolerance of Cooperative Vehicle Platoons Subject to Communication Delay. *IFAC-PapersOnLine* **2015**, *48*, 352–357.
24. Fathollahnejad, N.; Pathan, R.; Karlsson, J. On the Probability of Unsafe Disagreement in Group Formation Algorithms for Vehicular Ad Hoc Networks. In Proceedings of the 2015 11th European Dependable Computing Conference (EDCC), Paris, France, 7–11 September 2015; pp. 256–267. doi:10.1109/EDCC.2015.29.
25. Bhoi, S.; Khilar, P. Self soft fault detection based routing protocol for vehicular ad hoc network in city environment. *Wirel. Netw.* **2016**, *22*, 285–305. doi:10.1007/s11276-015-0970-8.
26. Elhadeif, M. A Fault-Tolerant Intersection Control Algorithm Under the Connected Intelligent Vehicles Environment. In *Advanced Multimedia and Ubiquitous Engineering*; Park J., Jin H., J.Y.; M., K., Eds.; Lecture Notes in Electrical Engineering; Springer: Singapore, 2016; Volume 393, pp. 243–253. doi:10.1007/978-981-10-1536-6\_33.

27. Almeida, J.; Ferreira, J.; Oliveira, A.S.R. An RSU Replication Scheme for Dependable Wireless Vehicular Networks. In Proceedings of the 2016 12th European Dependable Computing Conference (EDCC), Gothenburg, Sweden, 5–9 September 2016; pp. 229–240. doi:10.1109/EDCC.2016.11.
28. Medani, K.; Aliouat, M.; Aliouat, Z. Fault tolerant time synchronization using offsets table robust broadcasting protocol for vehicular ad hoc networks. *AEU Int. J. Electron. Commun.* **2017**, *81*, 192–204. doi:10.1016/j.aeue.2017.07.026.
29. Devangavi, A.D.; Gupta, R. Bezier Curve based Multipath Routing in VANET. In Proceedings of the 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC), Bangalore, India, 9–10 February 2018; pp. 1–5. doi:10.1109/ICAECC.2018.8479488.
30. Younes, M.B.; Boukerche, A. A performance evaluation of a fault-tolerant path recommendation protocol for smart transportation system. *Wirel. Netw.* **2018**, *24*, 345–360. doi:10.1007/s11276-016-1335-7.
31. Lamport, L. The Part-time Parliament. *ACM Trans. Comput. Syst.* **1998**, *16*, 133–169. doi:10.1145/279227.279229.
32. Kenney, J. Dedicated Short-Range Communications (DSRC) Standards in the United States. *IEEE Proc.* **2011**, *99*, 1162–1182. doi:10.1109/JPROC.2011.2132790.



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).