

## Research Article

# Adaptive Fault-Tolerant System and Optimal Power Allocation for Smart Vehicles in Smart Cities Using Controller Area Network

Anil Kumar Biswal <sup>1</sup>, Debabrata Singh <sup>1</sup>, Binod Kumar Pattanayak <sup>1</sup>,  
Debabrata Samanta <sup>2</sup>, Shehzad Ashraf Chaudhry <sup>3</sup>, and Azeem Irshad <sup>4</sup>

<sup>1</sup>Department of CSE, ITER, SOA Deemed to be University, Bhubaneswar, Odisha, India

<sup>2</sup>Department of Computer Science, CHRIST University, Bangalore, Karnataka, India

<sup>3</sup>Department of Computer Engineering, Istanbul Gelisim University, Istanbul, Turkey

<sup>4</sup>Computer Science Software Engineering, International Islamic University, Islamabad, Pakistan

Correspondence should be addressed to Azeem Irshad; azeem.phdcs66@iiu.edu.pk

Received 7 June 2021; Revised 8 September 2021; Accepted 28 September 2021; Published 13 October 2021

Academic Editor: Emanuele Maiorana

Copyright © 2021 Anil Kumar Biswal et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Nowadays, the power consumption and dependable repeated data collection are causing the main issue for fault or collision in controller area network (CAN), which has a great impact for designing autonomous vehicle in smart cities. Whenever a smart vehicle is designed with several sensor nodes, Internet of Things (IoT) modules are linked through CAN for reliable transmission of a message for avoiding collision, but it is failed in communication due to delay and collision in communication of message frame from a source node to the destination. Generally, the emerging role of IoT and vehicles has undoubtedly brought a new path for tomorrow's cities. The method proposed in this paper is used to gain fault-tolerant capability through Probabilistic Automatic Repeat Request (PARQ) and also Probabilistic Automatic Repeat Request (PARQ) with Fault Impact (PARQ-FI), in addition to providing optimal power allocation in CAN sensor nodes for enhancing the performance of the process and also significantly acting a role for making future smart cities. Several message frames are needed to be retransmitted on PARQ and fault impact (PARQ-FI) calculates the message with a response probability of each node.

## 1. Introduction

In recent days, the avoidance of the traffic congestion in smart cities has become a major research trend [1, 2]. The autonomy nature of IoT brings virtual representation and unique identification of devices, applications, and services which helps for building a block of future smart cities [3, 4]. The emerging characteristics of the smart sensing system and vehicles make it possible for its enormous use like huge data collection and processing, transferring of data among the nodes of the network, connectivity of the nodes, decision making, and working accordingly by the devices [5, 6]. Due to that reason, to design a smart vehicle that contains some sensor nodes, Arduino microcontroller and also Controller Area

Network (CAN) can be used. The CAN protocol provides a serial bus communication for a reliable and robust platform to transmit and receives a message from one sensor node to another [7, 8]. Using the CAN bus also provides a backbone for managing smart or automotive vehicle system engine control units (ECUs), brakes, and other components [9]. This CAN protocol is also used to improve the performance through distributed control and monitoring the congestion by virtue of sending priority messages from the various units of the vehicle [9, 10]. In this system, a carrier sense multiple access/collision detection (CSMA/CD) protocol and priority message scheduling are implemented to control overall communication, thereby reducing the cause of delays [11].

The CAN incorporates mechanism to design a real-time system with fault tolerance for communication at the time of occurrence of an error [12]. This system generally works in an electrical environment, whereas the communication is affected by electromagnetic interference (EMI) or any internal/external noise [13]. This noise can lead to reduction of performance of an automotive vehicle [13, 14]. There is a reason for causing an error or fault due to the unintended use of automatic repeat request (ARQ) [15]. Here, the corrupted message frames need to be retransmitted, but in this case, noncorrupted messages are also equally reforwarded, which causes inefficient utilization of the system resources [16]. So, it also takes more time to resend a long message, and thus, the response time of this message can be increased to cause an error. The system efficiency and overall performance are reduced due to the stop-and-wait resending strategy and wrong assigning of message length of the CAN bus [17]. This paper aims at enhancing the performance by adding a single error bit that depends on the impact of a faulty or corrupted message [18]. At the same time, CAN communication process is also improved through the analysis of probability automatic repeat request (PARQ) with its fault impact (PARQ-FI) which can verify the information message priority before retransmission.

This smart vehicle is connected with the Arduino controller to manage the various transmissions of messages from one sensor node to another [19]. When this controller is integrated with the CAN bus, then its transmission method is enhanced. There are also other factors like vehicle cabling pattern, unnecessary retransmission of frame, and poor energy source communication with distinct sensor nodes [20, 21]. Due to collision, data packets are consumed with excess energy which needs to retransmit fault packet for making an error-free system. Energy collection in today's world is being achieved from environmental sources of energy, such as solar, thermal, and vibration, to increase the source of sensor nodes from renewable energy [22–24]. Thus, the CAN protocol uses some fault controlling mechanism such as bit stuffing, acknowledgment verify, cyclic redundancy checking (CRC), and fault signaling, thereby saving power for retransmission of frame [25].

*1.1. Problem Statement.* In recent days, the main cause of road accidents arises very highly due to drowsiness and careless driving. Whenever the vehicle driver suddenly becomes conscious of braking, then the collision happens at the time of message packet communication in various nodes of the existing vehicle system. Generally, the data packets are lost or corrupted and also delayed in response that causes a fault in message transmission. Due to that, it is required to plan a smart autonomous vehicle to avoid a collision which is integrated with IoT modules and CAN serial bus protocol to reduce many road mishaps. So, it is used to implement an efficient fault-tolerant CAN protocol with an energy harvesting method to avoid the cause of the collision at the time of driving. Adding an autonomous movement is highly needed to an existing vehicle system availing for road safety as well as to making future smart cities.

*1.2. Contribution to This Work.* An efficient fault-tolerant and also optimal power allocation system is implemented on the smart autonomous vehicle by IoT modules using the Arduino controller and CAN bus on various sensor nodes of the system. The controlling of fault handling mechanism is applied through PARQ and PARQ-FI for assigning the priority of retransmission of message frames to transmit data to the brake of a vehicle for avoiding the collision. It is also providing an optimal approach to enhancement of power allocation in CAN network by implementing energy cost model with retransmission of data packet. Through effective packet routing and a congestion monitoring approach, the suggested paper optimally decreased power usage and data loss.

The rest of the paper is arranged accordingly. The literature review is discussed in Section 2. Section 3 provides a more detailed overview of the proposed system and the methodology in Section 4. Section 5 describes the tests and interpretation of the results. Section 6 concludes the article together with the likely scope for the future.

## 2. Literature Review

An efficient fault-tolerant algorithm for controller area network (CAN) is discussed in [26] that provides a technique to detect a fault at run time. This diagnosis algorithm is developed for a low-cost integrated system that can detect all defective nodes on CAN. Then, these faulty nodes are repaired during the detection process. So, it provides a single-way communication process with the help of standard CAN protocol with reliable communication of messages. This method only detects all faulty nodes at a particular period. When the testing process is not synchronized in time, then its performance is reduced, so it can be enhanced by a new perceptive of an algorithm for good repairing logic through proper synchronization of timing. Authors in [27] have proposed fault-tolerant convolutional neural networks (CNNs) for correcting serious errors in the real-time system. This technique provides safety for critical soft errors that are caused by an excess of voltage, temperature, and abnormal formation of an energy participle. The main cause of these soft errors is controlled through the implementation of three-way methods like using the technique of checksum, standard matrix-matrix multiplication, and the evaluation way of ImageNet using CNN models (AlexNet, VGG-19, etc.). But these experiments can be tested for soft errors in the restricted situation to minimize the overhead of an execution. That is why it is further planned to extend their work through more implementation of CNN model frameworks.

A novel identification technique is proposed in [28], which runs on the physical layer of the vehicular CAN network. The objective of this paper is to detect the erroneous electrical signaling of electronic control units (ECUs) of CAN messages. This process provides an efficient method for improving the CAN standard network for optimally detecting correct ECUs and improvising the logic for correction and detection of corrupted frame of ECUs, which is a vital requirement for avoiding surface attacks, road safety,

and flexibility to driver. So, it does not provide the optimal frame format of standard CAN without modifying the architecture of ECUs and thus, it can give better performance by enhancing the frame format of CAN. A dynamic energy harvesting torque technique is capable of providing a vector process to control and improve the efficiency of the motor wheel movement as elaborated in [29]. This vector process algorithm is capable of efficiently optimizing power consumption and executive torque of each side of the vehicle, which very swiftly reduces the run-time computation load, thereby allocating reasonable torque space for each side wheel of the vehicle. The nonlinear optimization criticality is swiftly transformed to optimal torque distribution of each side, which provides better optimal reduction of power loss between 13.9% and 18.9%, and also it needs a more advanced method for limiting the range of a torque of the wheels; otherwise, it fails.

Several security tools are embedded on the Internet for the vehicle which is detailed in [30] that integrates IoT modules with the CAN bus. This paper dynamically detects any malicious attacks and also hacking the control of a vehicle that causes safety issues for drivers and passengers. So, these CAN security measuring tools are used for evaluating the risk zones of a vehicle and major critical situations of passengers. Here, this system consumes more energy for handling their several sensor nodes and ECUs in a vehicle. The adaptable network protocol (CAN) is used in the automobiles communication process for detecting irregular connection fault that is proposed in [31]. The random cable connection in the car generates a communication problem that impairs the network system efficiency. In this paper, the fault detection is effective as well as economically detected by tree-based detection process, which is capable of eminently finding the location of the faulty node in overall communication. When the counter of sending data packet error crosses the threshold value that causes the failure of the system, it is rectified through the tree-based economical cost method. Thus, this tree-based process is required for optimal localization of internal collision, thereby detecting faults in the various critical topological environments.

The autonomous vehicle optimally performs the activity in the complex intersection of roadside mapping problem that is proposed in [32]. This paper claims that the traffic control signals do not efficiently manage and schedule the action of many vehicles in the recent situation; that is why it deigns an effective distributed algorithm and scheduling method that control the intersection of road path by minimizing the possible ratio of intersection delay. So, the case of complicated traffic system and first-in first-out (FIFO) scheduling are observed to have significantly minimized the ratio of the delay. Moreover, performance can be improved by using fault detection techniques. Authors in [33] described a clock synchronization and fault avoidance mechanism in CAN bus. This paper claims to have provided very optimal precision, supporting less transmission and operational overheads at the time of exchange of data packets. In the real-time implementation, this system is archiving better performance without an exchange of components of the CAN system. Then, the influence of

energy consumption in the message packet and several scheduling criteria are not used in the clock synchronization of this CAN system.

An electric vehicle is designed with the integration of the powertrain method that is unswervingly linked with the vehicle motor and gearbox, which is mentioned in [34, 35]. This mechanism is improved through a strong efficiency in the reduction of size and optimal energy harvesting in it. Using this technique, the cause of oscillation damping and also linear matrix inequalities in the vehicle system can be resolved. If the actuator and parameter variability do not work properly, then it needs to be enhanced in the proposed controller. The threat to the CAN network represents the cyber-attacks that are detailed in [36], which can evaluate the ratio of securities of passengers and vehicles. This paper is capable of detecting anomalies and critical message packets through a one-class classification that implements an advanced classifier (image processing) to assign a fault-tolerant handling mechanism to the CAN system, whereas this single-type classifier is only tested in the random parameter of the CAN packet. But it is not tested for a feasible value of the wheel, which is critical to find the fault of the system. Traditional vehicular network suffers various technical issues in implementation and management as technology evolves and the number of smart vehicles grows. These challenges include a lack of flexibility, scalability, poor connectivity, and insufficient intelligence. Due to the huge number of vehicles on the road, traffic accidents, road congestion, fuel consumption, and pollution have all become important global issues.

### 3. Proposed System

This proposed system provides a dynamic and flexible environment to avoid any kind of occurrence of a collision, engine fault, and communication error. The automation is implemented with the use of IoT modules like Arduino controller, motor controller, various sensor nodes, and CAN protocol, in addition to the supply of energy source for improving communication platform in different nodes of the system.

*3.1. Controller Area Network (CAN) for Proposed Architecture.* The IoT-based modules are used to maximize the reconfiguration method and dynamic changes through its hardware and software [37, 38]. So, this is implemented in the CAN bus controller, in addition to the bit-stream controller (BSC) and PARQ/PARQ-FI that are used for retransmission of priority messages in the sub-block of the CAN protocol. This proposed CAN architecture is depicted in Figure 1. This controller controls the transmission, retransmission of error priority messages and reception of frames through various medium access control (MAC) or logical link control (LLC) by adding CRC field and extra control field.

At the time of communication to handle read and write process in configuration buffer which acts as a register, a microcontroller is used. The transmitting end (TE) and receiving end (RE) units are accessed that maintain separate

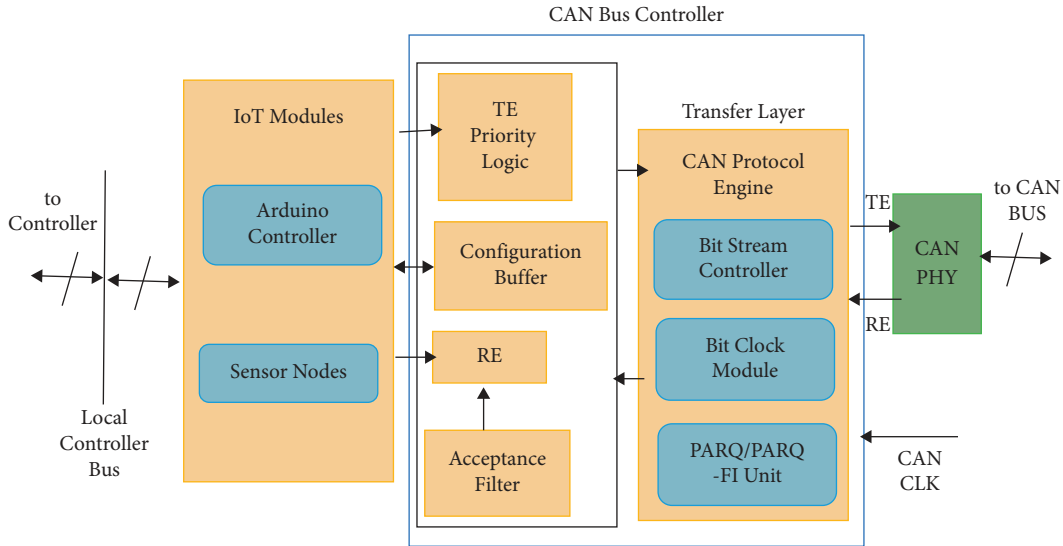


FIGURE 1: Proposed CAN bus block diagram.

buffers for communication of messages with the use of an acceptance filter (AF). The CAN protocol engine synchronizes the transmitted and received messages by using bit clock module and BSC module.

**3.2. Retransmission of CAN Message Frame.** The fault handling technique is effectively used for the communication of messages in CAN through the automatic repeat request (ARQ) method, which is a fault or error handling mechanism of re-sending the error message by proper observation of acknowledgments and timeouts for data transmission [39–41]. The redundant bits and CRC bit are used in the sending message stream for fault or an error detection which ensures reliable data communication link from source to a target node [14].

Whenever a message frame is sent in a noisy environment, then it is divided into tiny data packets with fault detection coding. If an error bit is zero, the packet will be accepted without error by the receiver. This indicates that the receiver is getting positive acknowledgment for the successful receipt of a message. But if there is no acknowledgment received, then the sender waits for a specified amount of time before re-sending the message packet [42, 43]. However, a negative acknowledgment (NACK) will be forwarded to the sender for re-sending the respective packet, if the receiver error bit is not the same as zero. Generally, the receiver node is waiting corrected message packet instead of a corrupted message packet. The acknowledgment feedback is used by the fault or error handling technique to inform whether the communication is correctly accomplished or not.

The message packet-1 is sent, and when the receiver receives it and finds that there is no-fault, then it forwards a positive acknowledgment (ACK) to signal a successful receipt of the packet [43, 44]. So, the communication continues with a message packet-2 which is received with an error and then, it sends a negative acknowledgment (NACK), which is shown in Figure 2.

Figure 3 explains the proposed PARQ/PARQ-FI communication technique, which is a combination of automatic error correction (AEC) and ARQ fault handling method to allow a corrupted packet to retransmit to the receiver node. But the corrupted packet is saved in a buffer for re-sending after correction. If an erred packet is received, then it sends the request for a new one, which is checked through AEC and the fault handling ARQ method that allow re-transmitting corrupted packet from a buffer to avoid the collision [45, 46]. This technique conducts the communication in three ways as follows:

- (i) Discarding an erred message packet, after receiving the retransmitted packet.
- (ii) Redundant bits are used for re-sending actual bit message packets with the use of AEC.
- (iii) The process of self-decoding method is used for recovering missing message bits.

Single-ended and differential CAN signals are processed by the CAN transceiver (CANH and CANL). In perfect condition, the CAN High and CAN Low lines are at 2.5 volts. The dominant bit in CAN is logic “zero,” and the recessive bit is logic “one.” When the dominant bit is communicated, CAN High rises to 3.5 volts and CAN Low falls to 1.5 volts, resulting in a 2-volt differential voltage. When the recessive bit is sent, the CAN High and CAN Low lines are both driven to 2.5 volts, indicating that the recessive bit’s differential voltage is 0 volts. To eliminate signal reflections, a 120-ohm CAN bus terminal resistor should be placed to the physical end of the CANH and CANL lines.

## 4. Methodology

A dynamic and adaptive fault-tolerant approach is implemented to avoid the collision at the time of message packet transmission in CAN bus with the implementation of an optimal energy harvesting technique; that is the objective of this paper.

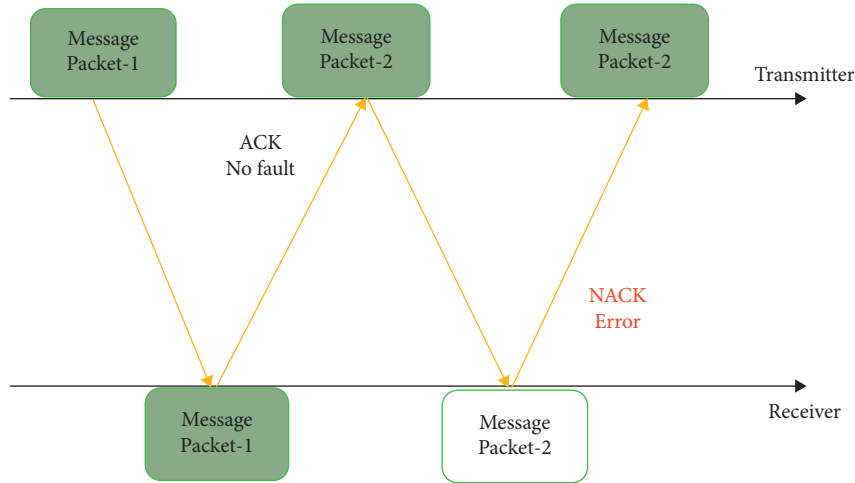


FIGURE 2: ARQ communication technique.

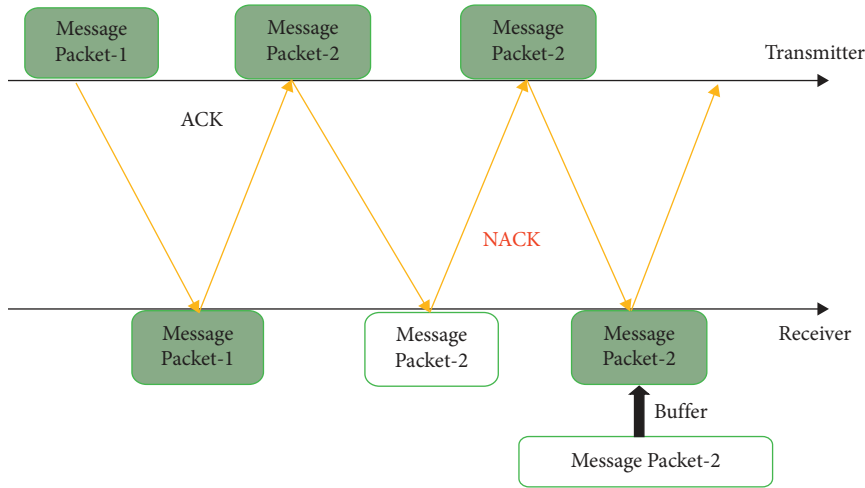


FIGURE 3: Proposed PARQ/PARQ-FI communication technique.

4.1. Fault/Error Handling Methods in CAN. Out of a number of messages transmitted from one node to another, some messages get corrupted in the CAN bus frame due to collision [47, 48]. So, it necessitates the use of fault or error handling technique to find a fault and request for resending of the message packet [39]. So, the CAN protocol is used for fault handling which is detailed below.

- (i) When the bus line signal is varied from the transmitted signal, then the sender forwards an error message packet, which is analyzed by the bit monitoring field.
- (ii) When the five sequential equal bits are found, then the bit stuffing assigns a complementary bit at the 6th bit location of the frame.
- (iii) When a fixed frame format in the received message does not comply with the requirements of the protocol, a corrupted frame is sent by the recipient and the received frame is not accepted. So, it needs to verify the message frame format.

- (iv) The acknowledgment check is checking the dominant bit frame slot for the data and distant frame.
- (v) The cyclic redundancy check (CRC) bit is accessed for fault finding from the beginning of the frame (BOF) to the message packet field.

The standard CAN's message frame format is depicted in Figure 4.

4.1.1. Bit and Cyclic Redundancy Check (CRC) Errors. The analysis of CAN inaccessibility is considered at the time of communication of message bits from a source node to [49]. As soon as the first bit of a dataset is transmitted, bit error detection as per a transmitting node can take place. The corresponding network inaccessibility period is set to the best time required to signal the error:

$$C_{\text{inac-bterr}} = C_{\text{bt}} + C_{\text{err}} + C_{\text{IFS}}, \quad (1)$$

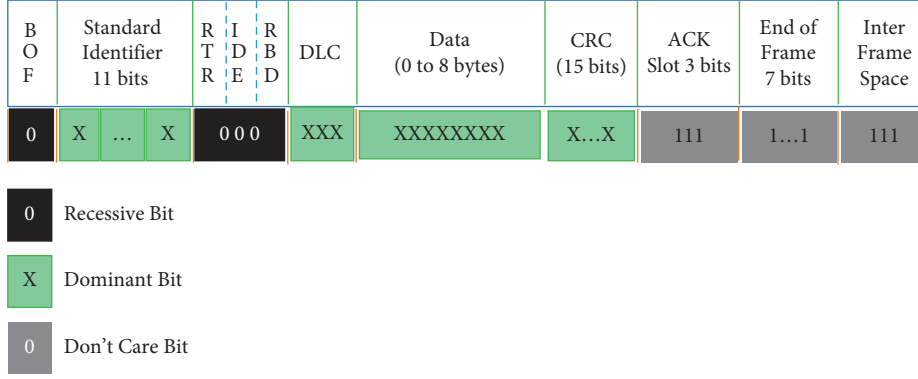


FIGURE 4: Standard message frame format of CAN.

where  $C_{\text{inacbtterr}}$  is denoted as error detection in the duration of communication network inaccessibility,  $C_{\text{bt}}$  confirms the communication of first bit of a bit stream,  $C_{\text{err}}$  is used for finding error at the of communication, and  $C_{\text{IFS}}$  is denoted as intermission field in the communication of message packet.

The CAN bus uses a 15-bit CRC frame with 1-bit delimiter, which is required to check the correctness of data transfer. Then, the inaccessibility time of communication network is expressed as

$$C_{\text{inac-crc}} = C_{\text{data}} - t_{\text{EOF}} + C_{\text{err}} + C_{\text{IFS}}. \quad (2)$$

Here, the actual data frame is represented as  $C_{\text{data}}$  and  $t_{\text{EOF}}$  is denoted as time period of end-of-frame (EOF) field.

**4.1.2. Bit Stuff Errors.** The CAN access protocol, data transfer, and remote frames bit streams are carried out by means of a bit stuffing system until the end of their CRC 15-bit sequence. Frame receiving entities must therefore monitor this bit stream and provide bit reception decoding and error detection [50]. When a receiving node monitors  $l_{\text{stff}}$  consecutive bits of the same level, the next received (stuff) bit is automatically deleted. The deleted bit shows a polarity opposite to the above under error-free operation, and if this condition is violated, an error will be reported on the auto bus when an error frame is initiated. It is required to find communication duration of inaccessibility, due to stuff error that is expressed as

$$C_{\text{inac-stuff}} = (l_{\text{stff}} + 1) \cdot C_{\text{bt}} + C_{\text{err}} + C_{\text{IFS}}. \quad (3)$$

#### 4.2. Optimal Power Allocation Model for Sensor Node.

The individual sensor node needs transmission and receiving energy. The initial energy ( $E$ ) is also available for each sensor node [51]. Each node requires a low level of energy for sensing and computing so that we can ignore them. We need to take into consideration energy consumption across the nodes, as in the Load Balancing Network [52]. A sensor node of the smart vehicle with  $l_b$ -bit message packet received as

$RP_x = E_{\text{pow}} \cdot l_b$  that represents the consumed power through the first-order radio model. Here, the symbol  $E_{\text{pow}}$  stands for the necessary power to transmit all  $l_b$ -bit message packets for the transmitter or receiver sensor nodes. The communication energy consumed is thus indicated in the following equation:

$$CP_x = RP_x + E_{\text{pow}} * l_b * T_R^\alpha, \quad (4)$$

where  $E_{\text{pow}}$  is utilized for signaling a bit of power and the radius of transmission is indicated by  $T_R$ , and the propagation loss component is represented by  $\alpha$ , where  $2 \leq \alpha \leq 6$ . This model incorporates uniform sensor nodes with the length of the data packet  $l_b$  and is then required to transmit the same power range for each message packet.

**4.2.1. CAN Message Flow Conservation of Sensor Nodes.** Here, the data transfer rates and how to send in the network via the flow conservation equation are discussed.

$$\sum_{j \in M_i} (D_{ij}(t) - D_{ji}(t)) = R_{ij}(t), \quad \forall i \in M, j \in M_i, \quad (5)$$

where the above equation is expressed as follows:

- (i)  $D_{ij}$  refers to the flow rate of messages from the node of the sensor.
- (ii)  $R_{ij}$  represents the information rate of each sensor node acquired at the transmitter node (TR)  $i$  and to the recipient node (RN)  $j \in M$ .
- (iii)  $M$  stands for all sets of sensor nodes,  $i =$  transmitting TR and  $j =$  receiving RN.

**4.2.2. Estimation of Energy Cost System.** The network life is dependent on the sensor node  $S_i$  energy consumption and active node scheduling time  $T_{S_i}$ . The energy communicated per scheduled time  $E_{\text{com}}(t)$  contains  $E_{\text{RE}}(t)$  and  $E_{\text{TE}}(t)$ . The computed energy consists of  $E_{\text{PE}}(t)$  and  $E_{\text{SE}}(t)$ .

Assuming the residual energy is represented by  $E_B(t) \geq 0$ , therefore,  $t$ 's power consumption is defined as



$$PC_i(t) = \sum_{ieN_j, jeN_i} D_{ij}E_{TE}(t) + \sum_{ieN_j, jeN_i} D_{ij}E_{RE}(t) + \sum_{ieN_j, jeN_j} R_{ij}E_{PE}(t) + \sum_{ieN_j, jeN_i} R_{ij}E_{SE}(t), \quad (6)$$

where  $PC_i(t)$  = power consumption in  $(t)$ ,  $E_{RE}(t)$  = receiver energy  $(t)$ ,  $E_{SE}(t)$  = sensing energy  $(t)$ ,  $E_{TE}(t)$  = transmitted energy  $(t)$ , and  $E_{PE}(t)$  = processing energy  $(t)$ .

For the transmission of one bit of data, the power transmitter from  $ieS$  to  $jeS_i$  over a distance  $(dt)$  is

$$E_{TE} = c_1 + c_2 * dt_{ij}^k, \quad (7)$$

where  $k$  = the transmission loss of path exponent,  $dt$  = interval of transmission, and  $c_1$  and  $c_2$  = constants according to  $T_i$ .

**4.3. Corrupted Packet and Retransmission (PARQ/PARQ-FI) of CAN Message.** Here, message analysis implements message error without fault (PARQ scheme), where the message is decoded by a technique as cyclic redundancy check (CRC) as

$$MP_e^{PARQ} = 1 - (1 - MP_b)^{L_{mp}}, \quad (8)$$

where  $MP_e^{PARQ}$  = probability of on event without fault impact,  $L_{mp}$  = message range,  $MP_e$  = messages loss rate, and  $MP_b$  = error bit rate (EBR). Similarly, the evaluation of message packet interference with the impact of fault (PARQ-FI scheme) is carried out, where the message communication is between the smart vehicle's sink node and sensor node. The loss rate of the sink node is

$$MP_e^{PARQ-FI} = 1 - \left( 1 - \sum_{i=e+1}^n \binom{n}{i} (1 - MP_b)^{n-i} \right)^{(L_{mp}/k)}. \quad (9)$$

Then,  $MP_e^{PARQ-FI}$  is the probability of on event with fault impact and here, the number of retransmission is given by

$$EX(Tr) = \frac{1}{(1 - MP_e)}. \quad (10)$$

Here,  $EX(Tr)$  = denotes the expected number of repeated messages. For Hp-hop scenario, the data loss rate is examined when each node transmission is taken independently.

$$EX(Tr, Hp) = \frac{Hp}{(1 - MP_e)}, \quad (11)$$

where Hp = set of hops. The fact that the values for signals  $u_{k-4}$ ,  $u_{k-3}$ ,  $u_{k-2}$ ,  $u_{k-1}$ ,  $v_{k-4}$ ,  $v_{k-3}$ ,  $v_{k-2}$ ,  $v_{k-1}$  required for the controller are not defined during start-up is primarily the reason for the slow convergence to the constant status value. We then develop a heuristic process to identify appropriate values for a maximum of four periodic retransmitted message (RTM) periods as illustrated in Algorithm 1.

This algorithm can record a fault value from the beginning of the RTM received at  $k = 1$ . There will be no fault

correction while waiting for four RTM (steps 3 and 5). The third RTM (step 6) is used to determine the input signal  $u_k$  and the clock error  $\hat{v}$  at  $e_k$  as a result of a clock error difference between  $v_{k-1}$  and  $v_{k-2}$  (step 7). The timestamp and logical clock (LC) at  $e_4$  will then be updated with  $n$ . The proposed correction of the fault is used in (step 9) after  $e_4$  (step 11). One of the main advantages is that less clock variance is attained after four RTMs have been received when a CAN node is initiated.

Whenever all faults or corrupted message frame packets are collected at the period of transmission, each erroneous bit of message frame can be easily traced and also the parity bit correction can be achieved through the proposed algorithmic technique before transmission, which is shown in Figure 5. If the message frame is removed from an error or fault, then it is readily attached with the remaining bits of the frame before transmission. Otherwise, it is retransmitted for avoiding the cause of an erroneous situation.

**4.4. Probability of CAN Message Packet.** A transmitter node utilizes the following node to transmit message and the chance that a packet will receive the data for the other nodes [25]. It also specifies the time for the message to be sent after transferring information opportunities between nodes. The probabilities of their nearby nodes being received are modified. For the whole of the CAN bus node, the energy is adequate to transfer the message for the sake of energy harvesting with the probability of receiving the packet [53].

The performance of the system must be considered in view of the delivery ratio (DR) and delay. The expected count of the data packet is measured by dividing the sink node with a packet node that is needed to define the delivery ratio. The delay is the time taken to produce all the instances with the waiting time period to complete the entire pervious task. We must simulate and compare the PARQ and PARQ-FI methods of CAN to find the performance of the entire process.

## 5. Simulation Setup and Results Analysis

A smart fault-tolerant and optimal energy harvesting method are used to design a vehicle through CAN bus that is dynamically avoiding the cause of an internal message communication error of several sensor nodes, which is depicted in Figures 6(a) and 6(b). Due to this, dynamism is allowed to robustly detect and reduce the collision that occurs due to drowsiness or careless driving.

This proposed system is tested through the simulation setup which consists of 500 nodes and 1000 nodes. So, this setup is prepared with deployment area of 500 m × 600 m size where these two distinct ranges of nodes are implemented. Through the center of the implementation zone, the sink node is allocated which optimally provides energy and facilitates an exchange of message packets. We presume that

```

Step 1: InsertParameter:  $v_{k-1}, v_{k-2}, v_{k-3}, v_{k-4}, T$ 
Step 2: Result:  $u_k$ 
Step 3: Init:  $u_{k-1} = 0; u_{k-2} = 0; u_{k-3} = 0; u_{k-4} = 0; k = 0$ 
Step 4: if RTM is accepted then
Step 5:  $k = k + 1; n_{k-1} = e_{k-1,u} - e_{k-1,s}$ 
Step 6: if  $k = 4$  (4th RTM is received at  $e_4$ ) then
Step 7:  $u_k = (v_{k-1} - v_{k-2})/T; \hat{v}_k = v_{k-2} + (2.T.u_k)$ 
Step 8:  $c_i(e_k) = c_i(e_k) + \hat{v}_k$  (clock update)
Step 9:  $e_{k-1,s} = e_{k,s} + \hat{v}_k$  (timestamp overwrite)
Step 10: else if  $k > 4$  then
Step 11: Find  $u_k$  according to (step 9)

```

ALGORITHM 1: Fault correction with initialization.

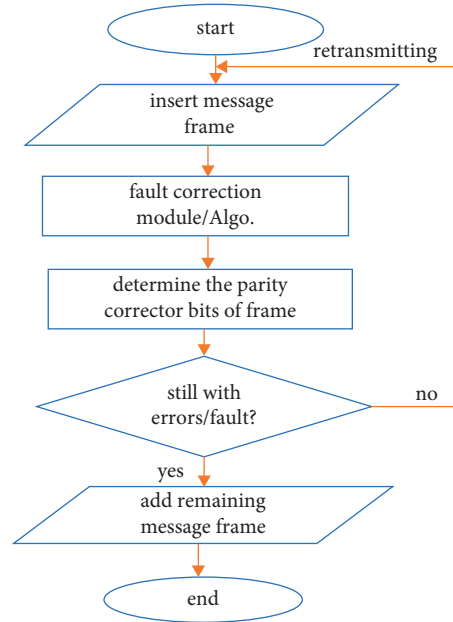


FIGURE 5: Flowchart of proposed fault handling (PARQ/PARQ-FI).

no packets can be received when the collision happens and data packet losses are not permitted in the entire network. This setup is set with the reliability threshold  $T_h = 0.9$  for 500 nodes and  $1.9 T_h$  value for 1000 nodes, as well as that, have to set the time depth to be 0 to  $\Theta$  in a channel where the sink node in the center is located. Suppose that during the simulation phase, no message loss is feasible within the transmission range, but the lack of a precise message is a network collision, which means no correct packet could be accepted. As per the consideration, the communication power consumption is assigned as transmitting end  $P_{te} = 77.1$  MW and receiving end  $P_{re} = 84.2$  MW, message packet sending energy  $E_s = -3.2$  dbm, and message packet receiving energy  $E_r = -84.7$  dbm. To set other parameters are the simulation period = 1000 s, data packet size set to 900 bits, rate of communication  $R_c = 255$  kbps, and in addition, the frequency  $(f) = 2.5$  GHz. These parameters are used for simulation result analysis, but this process also depends on several factors which are discussed below.

**5.1. Analysis of Number of Sensor Nodes in CAN Bus versus Delivery Ratio (DR).** When the number of sensors inside the CAN bus system varies, the delivery ratio is modified. Each node alters its density when it achieves the optimum amount of data transfer via PARQ and PARQ-FI. Figures 7(a) and 7(b) show that the PARQ-FI performs better than PARQ in 500 nos and 1000 nos of a sensor; if the fault does not occur frequently, then the collision is not considered to be successful. But the delivery ratio (DR) also decreases by raising the CAN message packet size.

**5.2. Analysis of Delivery Ratio (DR) versus Charging Rate (Ch) of Nodes in CAN Bus.** The system efficiency of the CAN bus is shown by the charge rate as shown in Figures 8(a) and 8(b). So, the PARQ performs better than PARQ-FI in 500 nos and 1000 nos of a sensor; if any protocol reaches a greater charge rate, the delivery ratio also rises, but the delivery ratio decreases for the charge time after some time.



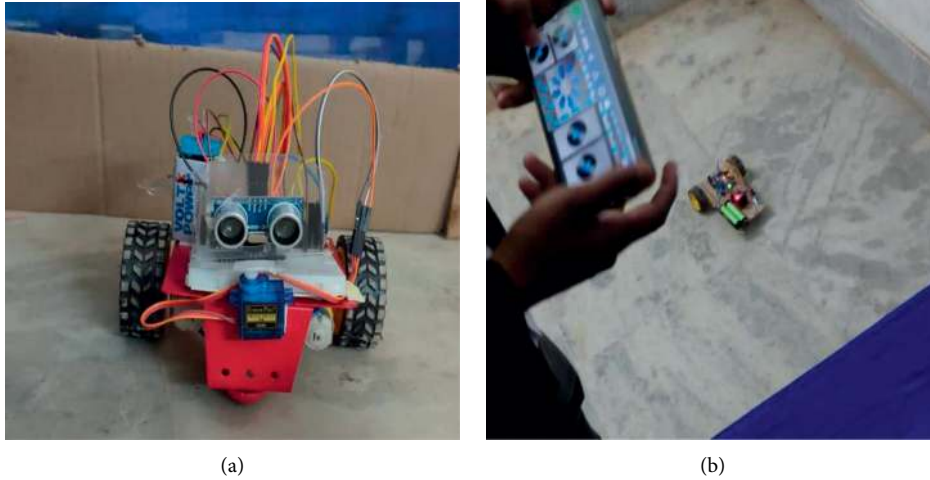


FIGURE 6: (a) Front view. (b) Test view of fault-tolerant smart vehicle.

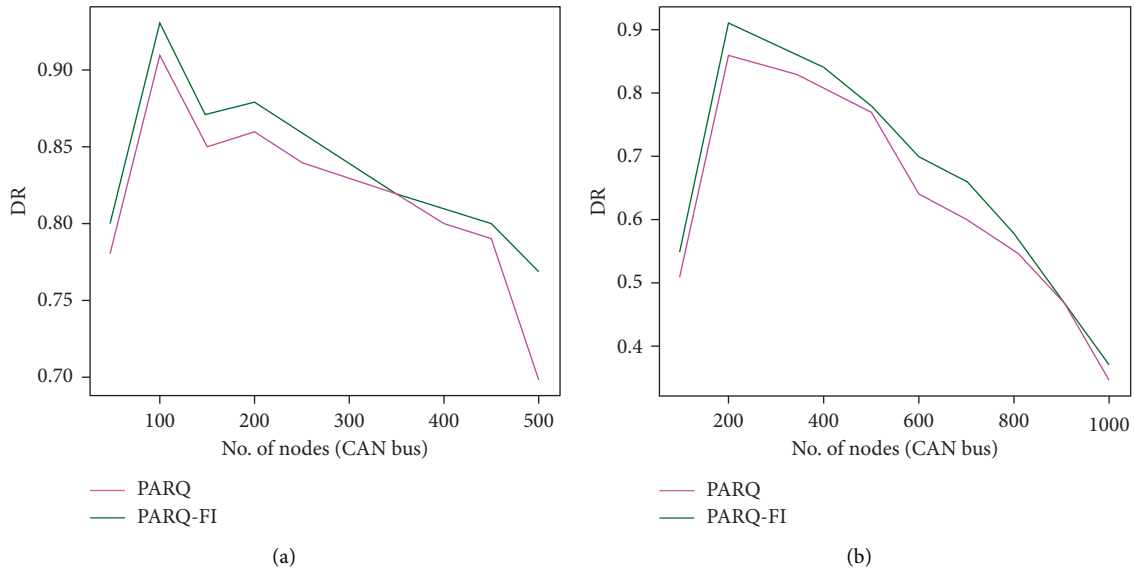


FIGURE 7: (a) 500 sensor nodes ( $n$ ) versus delivery comparison ratio (DR) at PARQ and PARQ-FI. (b) 1000 sensor nodes ( $n$ ) versus delivery comparison ratio (DR) at PARQ and PARQ-FI.

With a higher operating cycle, the sensor nodes charge quickly while the charge rate is increased and more packets are transmitted to the sink.

**5.3. Analysis of Delivery Ratio (DR) versus Delay Factor ( $m$ ) of Nodes in CAN Bus.** In the communication range through PARQ and PARQ-FI, sensors of each node provide their next neighbors with their information as shown in Figures 9(a) and 9(b). Here the PARQ-FI performs better than PARQ in 500 nos and 1000 nos of a sensor which is already shown in the figures. The delivery ratio also decreases, if the protocol provides a higher delay ratio. As delay factor ( $m$ ) is increased, the packets in the protocol are not guaranteed to be sent.

**5.4. Analysis of Delivery Ratio versus Reliability Threshold  $T_h$  of Nodes in CAN Bus.** Increased data delivery in PARQ PARQ-FI in Figures 10(a) and 10(b) depicts that the PARQ-FI performs better than PARQ in 500 nos and 1000 nos of a sensor if the reliability threshold of CAN bus node increases. The sensor sends the identical message back to obtain greater reliability if the reliability threshold ( $T_h$ ) value increases.

**5.5. Analysis of the Number of Sensor Nodes versus Delay in CAN Bus.** If more sensors are placed in the field of a smart vehicle installation, some sensor nodes require quick data recovery from the CAN bus. The time factor likewise grows with the increasing number of sensor nodes. The delay is evaluated with different nodes in Figures 11(a) and 11(b); as shown, the PARQ-FI performs better than PARQ in 500 nos

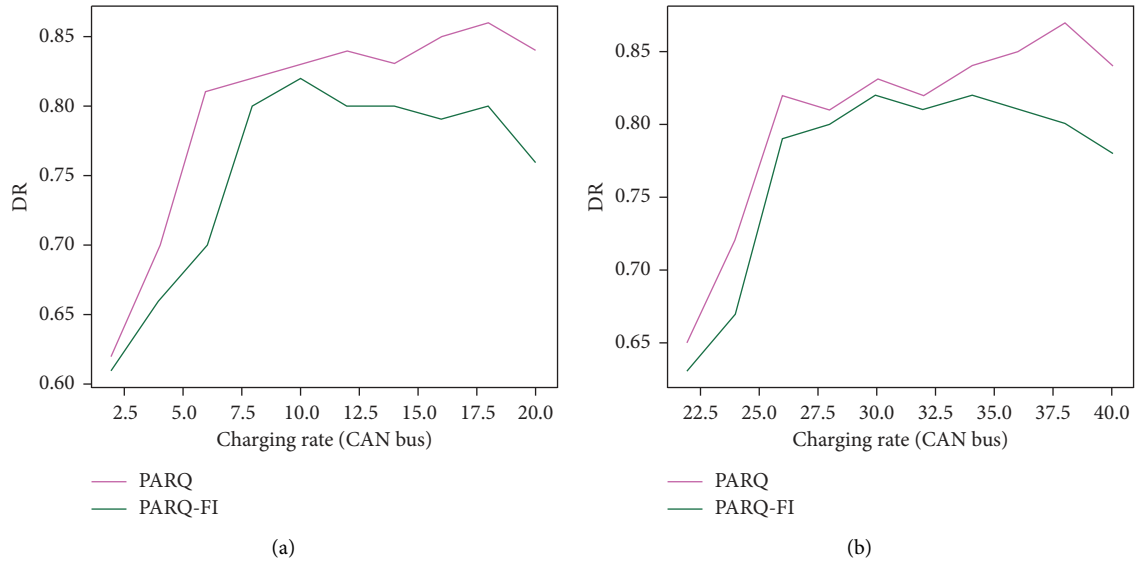


FIGURE 8: (a) Charging rate (Ch) versus delivery comparison ratio (DR) at PARQ and PARQ-FI for  $n = 500$ . (b) Charging rate (Ch) versus delivery comparison ratio (DR) at PARQ and PARQ-FI for  $n = 1000$ .

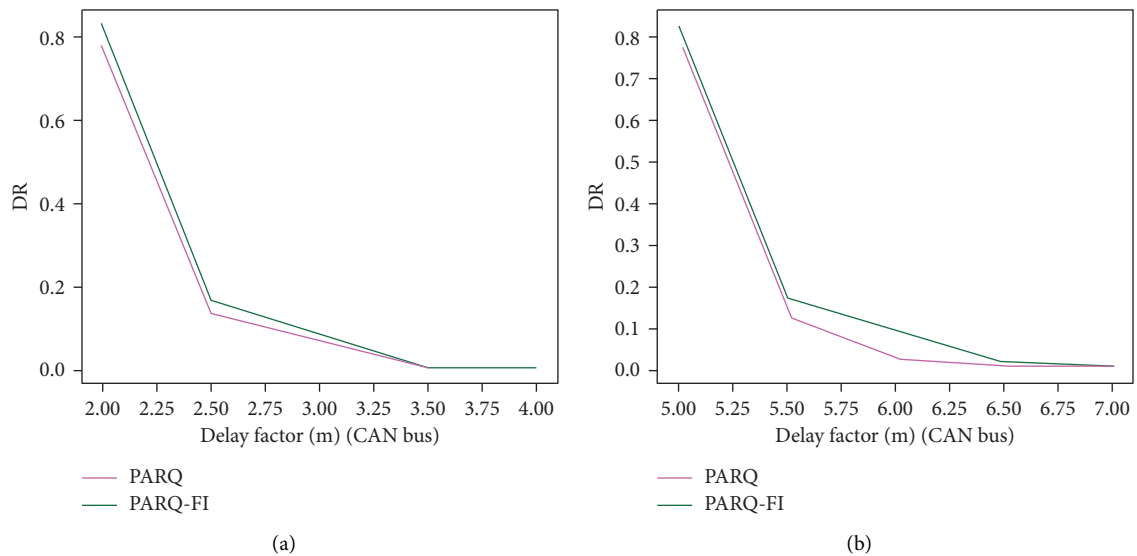


FIGURE 9: (a) Delivery ratio (DR) versus delay factor ( $m$ ) of nodes comparison in PARQ and PARQ-FI for  $n = 500$ . (b) Delivery ratio (DR) versus delay factor ( $m$ ) of nodes comparison in PARQ and PARQ-FI for  $n = 1000$ .

and 1000 nos of a sensor. Due to the limited charge time interval, the delay decreases as the charging rate rises in CAN protocol.

## 6. Discussion

In a test scenario, quite some parameters such as sensor nodes, delivery ratio, charging rate, delay factor, and reliability threshold have to be considered from the above analysis. Using these parameters in PARQ and PARQ-FI improves the fault-tolerant and precise power allocation for building smart vehicles in smart cities. The analysis of

PARQ-FI provides better performance than PARQ as a comparison with sensor nodes versus delivery ratio, delivery ratio versus delay factor, delivery ratio versus reliability threshold, and sensor nodes versus delay in CAN bus. But a single variation consequence is simulated that the PARQ performs better than PARQ-FI in comparison with the sensor nodes versus the charging rate of nodes in the CAN bus. Therefore, we take the two different sets of 500 and 1000 sensor nodes in this paper and check or evaluate the fault-tolerant as well as optimal energy allocation in the vehicles. In order to maintain identification and responsiveness capacity, as well as improve data reliability, transmission, and

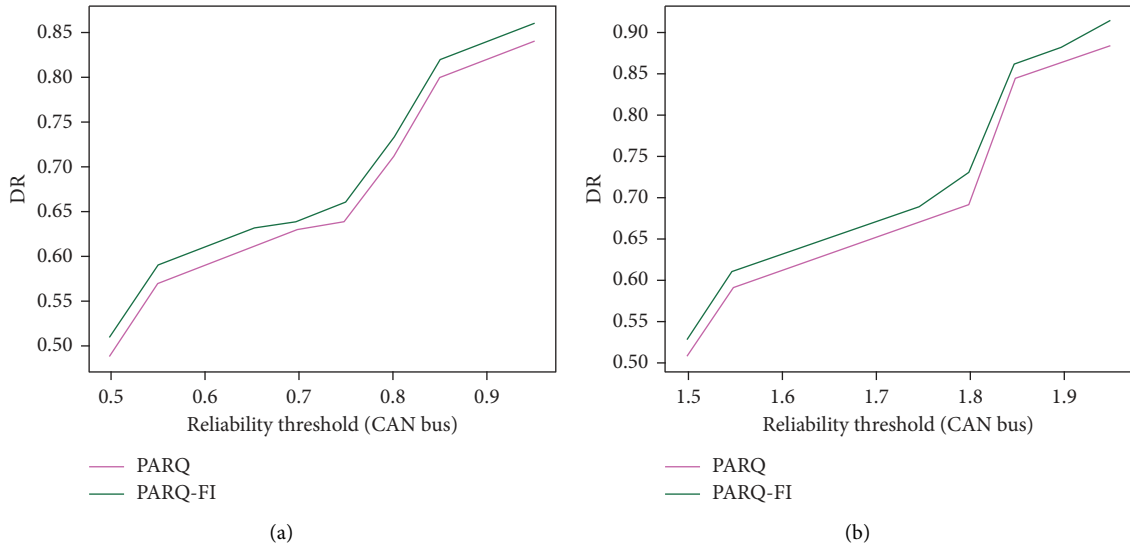


FIGURE 10: (a) Delivery ratio (DR) versus reliability threshold ( $Th=0.9$ ) of nodes comparison in PARQ and PARQ-FI for  $n=500$ . (b) Delivery ratio (DR) versus reliability threshold ( $Th=1.9$ ) of nodes comparison in PARQ and PARQ-FI for  $n=1000$ .

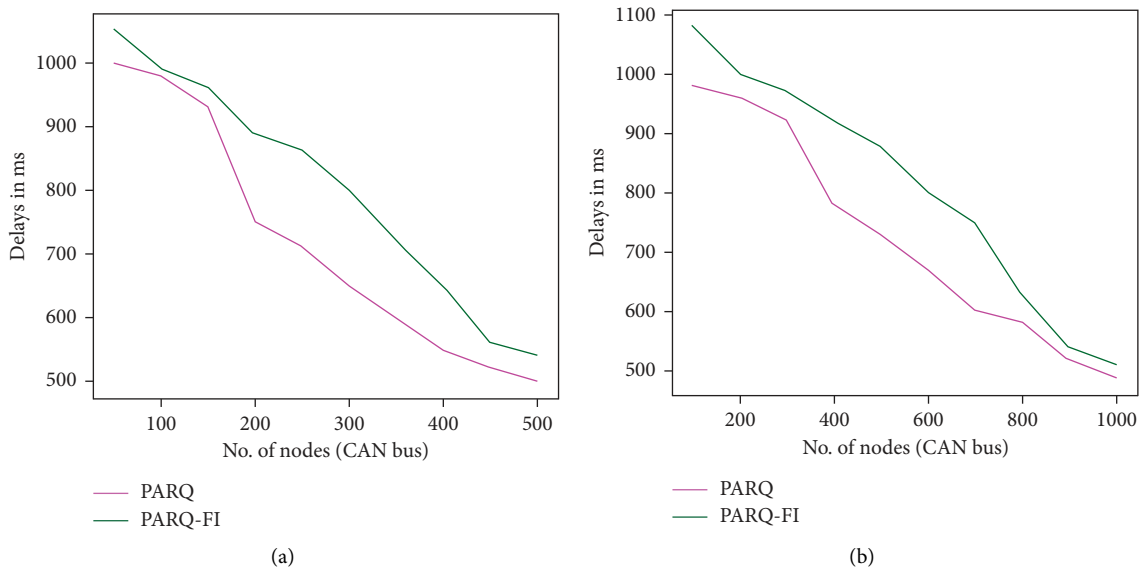


FIGURE 11: (a) 500 sensor node numbers versus delay (ms) comparison in PARQ and PARQ-FI (b) 1000 sensor node numbers versus delay (ms) comparison in PARQ and PARQ-FI.

redundancy, CAN network often requires high data dependability.

### 7. Conclusion

We analyzed the loss of data packet in the smart vehicle of CAN bus sensor nodes as a result of increased energy consumption and transmission collision in the proposed paper. To overcome this problem in future smart cities, the energy efficiency and automotive repeat priority message packet collection among neighboring nodes of a bus should be enhanced. That is why two methods are proposed for collection packets, such as Probabilistic Automatic Repeat Request (PARQ) and Probabilistic Automatic Repeat

Request with Fault Impact (PARQ-FI). Similarly, data packets have not collided due to the adoption of an effective power distribution at the next node. In a sender node, the probability of accepting a message packet from their own enabled or active times and their larger archive delivery ratio are evaluated by simulating the results of each protocol. Thus, it is better usages of the protocol to observing the performance of smart vehicles in smart cities. The future study is focused on how best to identify the prospective threshold value  $T_h$  and the appropriate tracks/updates region for the message request  $\tau$  may be created and the numerical analysis of CAN models and protocols enhanced in smart vehicles for various sensor network regions.

## Data Availability

No data are available for this study.

## Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

## References

- [1] S. S. Shah, M. Ali, A. W. Malik, M. A. Khan, and S. D. Ravana, "vFog: a vehicle-assisted computing framework for delay-sensitive applications in smart cities," *IEEE Access*, vol. 7, Article ID 34900, 2019.
- [2] M. R. Boukhari, A. Chaibet, M. Boukhnifer, and S. Glaser, "A review on fault-tolerant control for vehicle dynamics," *International Journal of Digital Signals and Smart Systems*, vol. 1, no. 3, pp. 181–203, 2017.
- [3] S. Tanwar, A. Popat, P. Bhattacharya, R. Gupta, and N. Kumar, "A taxonomy of energy optimization techniques for smart cities: architecture and future directions," *Expert Systems*, Article ID e12703, 2021.
- [4] F. A. Turjman, "Smart-city medium access for smart mobility applications in internet of things," *Transactions on Emerging Telecommunications Technologies*, Article ID e3723, 2019.
- [5] K. Soomro, M. N. M. Bhutta, Z. Khan, and M. A. Tahir, "Smart city big data analytics: an advanced review," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 9, no. 5, Article ID e1319, 2019.
- [6] F. A. Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' iot communications," *Transactions on Emerging Telecommunications Technologies*, Article ID e3677, 2019.
- [7] Y. Zhang, M. Chen, N. Guizani, D. Wu, and V. C. M. Leung, "SOVCAN: safety-oriented vehicular controller area network," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 94–99, 2017.
- [8] X. Ge, I. Ahmad, Q. L. Han, J. Wang, and X. M. Zhang, "Dynamic event-triggered scheduling and control for vehicle active suspension over controller area network," *Mechanical Systems and Signal Processing*, vol. 152, Article ID 107481, 2021.
- [9] G. I. Mary, Z. C. Alex, and L. Jenkins, "Time analysis of wireless controller area network-based fire and gas safety system," *International Journal of Communication Networks and Distributed Systems*, vol. 18, no. 1, pp. 1–17, 2017.
- [10] M. K. Ishak and F. K. Khan, "Unique message authentication security approach based controller area network (CAN) for anti-lock braking system (ABS) in vehicle network," *Procedia Computer Science*, vol. 160, pp. 93–100, 2019.
- [11] K. W. Schmidt, B. Alkan, E. G. Schmidt, D. C. Karani, and U. Karakaya, "Controller area network with priority queues and FIFO queues: improved schedulability analysis and message set extension," *International Journal of Vehicle Design*, vol. 71, no. 1–4, pp. 335–357, 2016.
- [12] H. Olufowobi, U. Ezeobi, E. Muhati et al., "Anomaly detection approach using adaptive cumulative sum algorithm for controller area network," in *Proceedings of the ACM Workshop On Automotive Cybersecurity*, pp. 25–30, Richardson, TX, USA, March 2019.
- [13] D. Kwon, S. Park, and J.-T. Ryu, "A study on big data thinking of the internet of things-based smart-connected car in conjunction with controller area network bus and 4G-long term evolution," *Symmetry*, vol. 9, no. 8, p. 152, 2017.
- [14] N. M. B. Lakhal, O. Nasri, L. Adouane, and J. B. H. Slama, "Controller area network reliability: overview of design challenges and safety related perspectives of future transportation systems," *IET Intelligent Transport Systems*, vol. 14, no. 13, pp. 1727–1739, 2020.
- [15] M. B. Hassan, E. S. Ali, R. A. Mokhtar, R. A. Saeed, and B. S. Chaudhari, "Nb-iot: concepts, applications, and deployment challenges," in *LPWAN Technologies For IoT and M2M Applications* Elsevier, Amsterdam, Netherlands, 2020.
- [16] R. Kurachi, H. Takada, H. Ueda, and S. Takimoto, "Towards minimizing mac utilization for controller area network," in *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security*, pp. 45–50, New Orleans, LA USA, March 2020.
- [17] M. S. Chen and H. W. Yen, "Online controller area network message scheduling: analysis, implementation and applications," *International Journal of Systems, Control and Communications*, vol. 2, no. 4, pp. 418–430, 2010.
- [18] V. Tanksale, "Anomaly detection for controller area networks using long short-term memory," *IEEE Open Journal of Intelligent Transportation Systems*, vol. 1, pp. 253–265, 2020.
- [19] S. Sicari, A. Rizzardi, and A. C. Porisini, "Smart transport and logistics: a node-red implementation," *Internet Technology Letters*, vol. 2, no. 2, p. e88, 2019.
- [20] G. I. Aswath, S. K. Vasudevan, and R. M. D. Sundaram, "Emerging security concerns for smart vehicles and proposed iot solutions," *International Journal of Vehicle Autonomous Systems*, vol. 14, no. 2, pp. 107–133, 2018.
- [21] A. K. Biswal, D. Singh, and B. K. Pattanayak, "IoT-based voice-controlled energy-efficient intelligent traffic and street light monitoring system," in *Proceedings of the Green Technology For Smart City And Society*, pp. 43–54, Springer, Bhubaneswar, India, August 2021.
- [22] S. Almishari, N. Ababtein, P. Dash, and K. Naik, "An energy efficient real-time vehicle tracking system," in *Proceedings of the 2017 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)*, pp. 1–6, IEEE, Victoria, BC, Canada, August 2017.
- [23] J. Zhang, "Distributed network security framework of energy internet based on internet of things," *Sustainable Energy Technologies and Assessments*, vol. 44, Article ID 101051, 2021.
- [24] N. A. Li, Y. Wei, M. Song, and X. Wang, "Energy-efficiency-aware flow-based access control in HetNets with renewable energy supply," *International Journal of Computational Science and Engineering*, vol. 21, no. 3, pp. 437–445, 2020.
- [25] R. Alaei, P. Moallem, and A. Bohlooli, "Statistical based algorithm for reducing residual error in embedded systems implemented using the controller area network," *IEEE Access*, vol. 8, Article ID 133817, 2020.
- [26] S. Kelkar and R. Kamal, "Adaptive fault diagnosis algorithm for controller area network," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 10, pp. 5527–5537, 2014.
- [27] K. Zhao, S. Di, S. Li et al., "FT-CNN: algorithm-based fault tolerance for convolutional neural networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 7, pp. 1677–1689, 2021.
- [28] W. Choi, H. J. Jo, S. Woo, J. Y. Chun, J. Park, and D. H. Lee, "Identifying ecus using inimitable characteristics of signals in controller area networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 4757–4770, 2018.
- [29] H. Chen, P. Du, Y. Wang, D. Jin, and X. Lian, "Dynamic energy-efficient torque allocation algorithm for in-wheel

- motor-driven vehicle,” *Proceedings of the Institution of Mechanical Engineers-Part D: Journal of Automobile Engineering*, vol. 234, no. 7, pp. 1815–1825, 2020.
- [30] H. Zhang, X. Meng, X. Zhang, and Z. Liu, “CANsec: a practical in-vehicle controller area network security evaluation tool,” *Sensors*, vol. 20, no. 17, p. 4900, 2020.
- [31] L. Zhang, F. Yang, and Y. Lei, “Tree-based intermittent connection fault diagnosis for controller area network,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9151–9161, 2019.
- [32] A. A. Hassan and H. A. Rakha, “A fully-distributed heuristic algorithm for control of autonomous vehicle movements at isolated intersections,” *International Journal of Transportation Science and Technology*, vol. 3, no. 4, pp. 297–309, 2014.
- [33] G. Rodriguez-Navas, S. Roca, and J. Proenza, “Orthogonal, fault-tolerant, and high-precision clock synchronization for the controller area network,” *IEEE Transactions on Industrial Informatics*, vol. 4, no. 2, pp. 92–101, 2008.
- [34] X. Zhu, H. Zhang, D. Cao, and Z. Fang, “Robust control of integrated motor-transmission powertrain system over controller area network for automotive applications,” *Mechanical Systems and Signal Processing*, vol. 58–59, pp. 15–28, 2015.
- [35] K. Jiang, H. Zhang, H. R. Karimi, J. Lin, and L. Song, “Simultaneous input and state estimation for integrated motor-transmission systems in a controller area network environment via an adaptive unscented Kalman filter,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 4, pp. 1570–1579, 2018.
- [36] A. Tomlinson, J. Bryans, and S. A. Shaikh, “Using a one-class compound classifier to detect in-vehicle network attacks,” in *Proceedings of the Genetic And Evolutionary Computation Conference Companion*, pp. 1926–1929, Kyoto Japan, July 2018.
- [37] M. Priyan and G. U. Devi, “A survey on internet of vehicles: applications, technologies, challenges and opportunities,” *International Journal of Advanced Intelligence Paradigms*, vol. 12, no. 1-2, pp. 98–119, 2019.
- [38] A. K. Biswal, D. Singh, B. K. Pattanayak, D. Samanta, and M.-H. Yang, “IoT-based smart alert system for drowsy driver detection,” *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6627217, 13 pages, 2021.
- [39] B. Palaniswamy, S. Camtepe, E. Foo, and J. Pieprzyk, “An efficient authentication scheme for intra-vehicular controller area network,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3107–3122, 2020.
- [40] K. B. Kiadehi, A. M. Rahmani, and A. S. Molahosseini, “A fault-tolerant architecture for internet-of-things based on software-defined networks,” *Telecommunication Systems*, vol. 77, pp. 1–15, 2021.
- [41] A. de Baynast, P. Mähönen, and M. Petrova, “ARQ-based cross-layer optimization for wireless multicarrier transmission on cognitive radio networks,” *Computer Networks*, vol. 52, no. 4, pp. 778–794, 2008.
- [42] S. Garg, D. Mehrotra, H. M. Pandey, and S. Pandey, “Accessible review of internet of vehicle models for intelligent transportation and research gaps for potential future directions,” *Peer-to-Peer Networking and Applications*, vol. 14, no. 1, pp. 1–28, 2021.
- [43] M. Nakamura, M. Ohara, A. Saysanasongkham, M. Arai, K. Sakai, and S. Fukumoto, “Hybrid ARQ for DC-DC converter noise in controller area networks,” in *Proceedings of the 2014 43rd International Conference On Parallel Processing Workshops*, pp. 375–379, IEEE, Minneapolis, MN, USA, September 2014.
- [44] R. Shirai and T. Shimizu, “Failure protection for controller area network against EMI emitted by buck converter,” in *Proceedings of the 2019 IEEE Applied Power Electronics Conference and Exposition (APEC)*, pp. 644–649, IEEE, Anaheim, CA, USA, March 2019.
- [45] G. A. A. Suhail, “Adaptive hybrid ARQ for mode switching receiver in wireless cellular networks,” *International Journal of Reasoning-Based Intelligent Systems*, vol. 4, no. 4, pp. 192–196, 2012.
- [46] M. Nakamura, M. Ohara, A. Saysanasongkham et al., “Testbeds of a hybrid-ARQ-based reliable communication for cans in highly electromagnetic environments,” in *Proceedings of the 2015 IEEE 2nd International Future Energy Electronics Conference (IFEEEC)*, pp. 1–6, IEEE, Taipei, Taiwan, November 2015.
- [47] O. Avatefipour and H. Malik, “State-of-the-art survey on in-vehicle network communication (CAN-bus) security and vulnerabilities,” 2018, <https://arxiv.org/abs/1802.01725>.
- [48] P. S. Murvay, L. Popa, and B. Groza, “Securing the controller area network with covert voltage channels,” *International Journal of Information Security*, pp. 1–15, 2021.
- [49] R. Islam and R. U. D. Refat, “Improving CAN bus security by assigning dynamic arbitration ids,” *Journal of Transportation Security*, vol. 13, no. 1, pp. 19–31, 2020.
- [50] L. M. Zhang, Y. C. Sun, and Y. Lei, “Message delay time distribution analysis for controller area network under errors,” *Frontiers of Information Technology and Electronic Engineering*, vol. 20, no. 6, pp. 760–772, 2019.
- [51] C. Schmutzler, A. Krüger, F. Schuster, and M. Simons, “Energy efficient automotive networks: state of the art and challenges ahead,” *International Journal of Communication Networks and Distributed Systems*, vol. 9, no. 3-4, pp. 266–285, 2012.
- [52] S. S. Thale and V. Agarwal, “Controller area network assisted grid synchronization of a microgrid with renewable energy sources and storage,” *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1442–1452, 2015.
- [53] R. Alaei, P. Moallem, and A. Bohlooli, “Statistical based algorithm for reducing bit stuffing in the controller area networks,” *Microelectronics Journal*, vol. 101, Article ID 104794, 2020.