International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor (2018): 7.426

Vehicle to Vehicle Communication- Pothole Detection Application using CAN Protocols and IOT for Safer and Secure City

Snehal Patil

Third Year Electronic and Telecommunication Engineering, Pimpri Chinchwad College of Engineering Pune, India

Abstract: ***Implementation of Controller Area Network (CAN) integrated with IoT for robust communication between two nodes. CAN and IoT are the most versatile and popular technologies of Electronics industry which are used in many practical applications. The Controller Area Network is a serial, asynchronous, multimaster communication protocol for connecting electronic control modules in automotive and industrial applications. Basically IoT is a giant network of connected "things". The combination of CAN and IoT can be the best practice which can improvise the human life more efficiently. Here, we implemented the prototype of vehicle to vehicle communication. For that we have used CAN bus to communicate the two vehicles and a WIFI module to send a warning to the vehicle behind it about its status. The trailing vehicle will receive the message via Wi-Fi and send the data to LPC1768 controller that will notify its user by displaying a message on the LCD.***

Keywords: Wi-Fi Module, CAN, IoT, V2V Communication

1. Introduction

Current Scenario: In busy and heavily trafficked cities especially in India, the roads lose their stiffness resulting in potholes. This loosening of debris can be spotted randomly in any location. The fellow people suffer this dangerous problem almost every day, often resulting in accidents. According to a recent study, the number of deaths has increased to 3597, which is a considerable number of deaths due to potholes. In addition people face high traffic congestion, raising fuel drain and time wastage. This is a critical issue for people in emergency who need immediate conveyance. Moreover, the construction of roads is a tedious process and extremely costly. All this leads to unnecessary frustration to the citizens, so we need to come up with a solution for this issue.

Present Innovation: The idea focuses on implementing a solution by establishing effective communication using CAN protocols. The nexus consist of several ECUs and sensors which with the help of ESP Wi-Fi module conveys caution reports and aware the trailing vehicle well advance in time to prevent any mishap. The time lapse in this process is almost negligible around 0.2 to 0.3 microsec.

2. Assumptions

A. This application is for vehicles travelling in a single lane.
B. All the vehicles are connected to each other through Wi-Fi.
C. The government permits and approves the implementation of the project in full scale.

3. Explanation

The shock absorber of a vehicle experiences mechanical disturbances when the vehicle goes through a pothole. Due to these disturbances the ADC connected to the shock absorber gives high fluctuating output values. The Electronic Control Unit (ECU-1) takes up the ADC data values and transfers it to the ECU-2 through CAN bus which is connected to Wi-Fi module. Two ESP-8266 Wi-Fi modules are interfaced to the respective ECUs of two cars. A giant network connects both the Wi-Fi module through internet. Thus the Wi-Fi module of the former car sends the data to the Wi-Fi module connected to the trailing car. This way, the trailing car will receive the data via Wi-Fi and send to LPC1768 controller through UART protocol. The controller will notify its user by displaying an alert message on the LCD display.

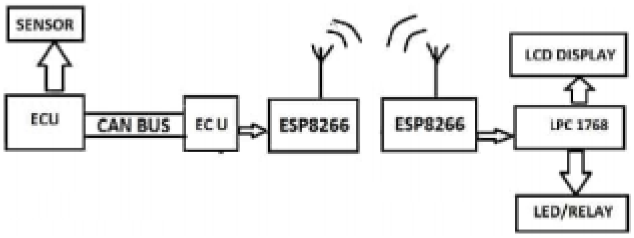


Figure 1: Block Diagram

4. Working

Working of the system is subdivided into following parts:

- Initial data conversion and transfer.
- Communication between controllers using CAN protocols.
- Networking using IoT.
- Data reception and interpretation.

1) Initial data conversion and transfer Initial data conversion takes place with the help of an Analog to Digital Converter. When the car passes through a pothole the ADC connected to the shock absorber of the car receives a high signal and thus converts the analog signal into high digital values due to sudden disturbance. This high data values are further transmitted to the respective connected ECU and then transferred further.
2) Communication between controllers using CAN protocols. Controller area network bus is serial communication bus originally developed for automotive

industry to replace complex wiring harness with two-wired bus which allows devices and microcontrollers to communicate with each other without host computers. So we use CAN buses to communicate between different ECU's in a car. When the data values from one ECU enter the CAN bus then data frames of CAN bus starts working as follows

Figure 2: Structure of CAN data frame-

1 bit	29 bit	1 bit	6 bit	0-64 bit	16 bit	2 bit	7 bit
SOF	CAN ID	RTR	CONTROL	DATA	CRC	ACK	EOF

- SOF: Start of Frame is 'dominant 0' to tell other ECU's that a message is coming.
- CANID: Contains message identifier and priorities. Lower values have high priority.
- RTR: Remote Transmission Request allows ECU's to request message from other ECU's .
- CONTROL: Informs the length of data in bytes (0-8) bytes.
- DATA: Contains the actual data values which need to be 'scaled' or converted to be readable and ready for analysis.
- CRC: Cyclic Redundancy Check is used to ensure data integrity.
- ACK: The Acknowledgment slot indicates if the CRC process is working well or not.
- EOF: End Of Frame indicates that the CAN message is transferred further. In this way the data values from one ECU is transferred to the second ECU using Can protocols.

3) Networking using IoT

IoT is simply the network of interconnected things/devices which are embedded with sensors, software, network connectivity and necessary electronics that enables to collect and exchange data making them responsive.

More than a concept internet of things is essentially an architectural framework which allows integration and data exchange between the physical world and computer systems over existing network infrastructure.

The fundamental components that make internet of things a reality are:

Hardware- Making physical objects responsive and giving them capability to retrieve data and respond to instructions. Here we use two Wi-Fi modules to connect two respective cars over Internet. The Wi-Fi module used is ESP 8266.

ESP 8266 (Wi-Fi Module)

ESP 8266 offers a complete and self-contained Wi-Fi networking solution, allowing it to either host the application or to offload all Wi-Fi networking functions from another application processor. When ESP 8266 hosts the application, and when it is the only application processor in the device, it is able to boot up directly from an external flash. It has integrated cache to improve the performance of the system. In such applications and to minimize the memory requirements. Alternately, serving as a Wi-Fi adapter, wireless internet access can be added to any microcontroller based design with simple connectivity through UART interface. ESP 8266 on-board processing and storage capabilities allow it to be integrated with the sensors and other application specific devices through its GPIOs with minimal development upfront and minimal loading during runtime. With its high degree of on-chip integration which includes the antenna switch, power management convertors, it requires minimal external circuitary and the entire solution, including front-end module is designed to occupy minimal PCB area.

- Software- Enabling the data collection, storage, processing, manipulating and instructing.
- Communication Infrastructure- Most important of all is the communication infrastructure which consist of protocols and technologies which enable 2 physical objects to exchange data.

Architecture of IOT

IoT system consists of three main parts viz. sensors, network connectivity and data storage applications. The same has been depicted in figure-1. As shown in the figure, Sensors in the IoT devices either communicate directly with the central server for data storage or communicate via gateway devices.

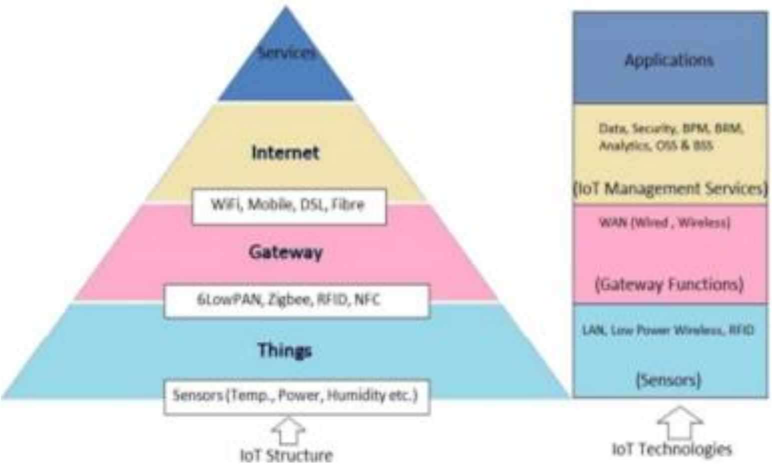


Figure 3: Architecture of IoT

Sensors for various applications are used in different IoT devices as per different applications such as temperature, power, humidity, proximity, force etc. Gateway takes care of various wireless standard interfaces and hence one gateway can handle multiple technologies and multiple sensors. The typical wireless technologies used widely are 6LoWPAN, Zigbee, Z-wave, RFID, NFC etc. Gateway interfaces with cloud using backbone wireless or wired technologies such as Wi-Fi, Mobile, DSL or Fibre. As shown IoT supports both IPv4 and IPv6 protocols. Due to support of IPv6 which has about 128 bit long IP address length, there are enough addresses available to growing demand of IoT devices. DTN (Delay Tolerant Networks) is the unique feature of IoT which takes care of large variable delay requirement of IoT based networks compare to traditional computer networks.

4) Reception and Interpretation of data.
Reception is done by the UART embedded in the ARM Cortex M3 Board and later on it interprets the data and displays the alert message on the LCD screen.

UART
UART is usually individual (or part of an) integrated circuit used for serial communications over computer or a peripheral device serial port. UARTs are now commonly included in microcontrollers. The Universal Asynchronous Receiver Transmitter (UART) takes bytes of data and transmits the individual bits in a sequential fashion. At the destination, a second UART re-assembles the bits into complete bytes. Each UART contains a shift register which is fundamental method of conversion between serial and parallel forms. Serial transmission of digital information (bits) through single wire or other medium is less costly than parallel transmission through multiple wires.

UART main features –
a) A clock generator, usually a multiple of the bit to allow sampling in the middle of a bit period.
b) Input and output shift registers
c) Transmits/ receives control
d) Read/write control logic
e) Transmit/receive buffer (Optional)
f) System data bus buffer (Optional)
g) First In First Out (FIFO) Buffer memory (Optional)

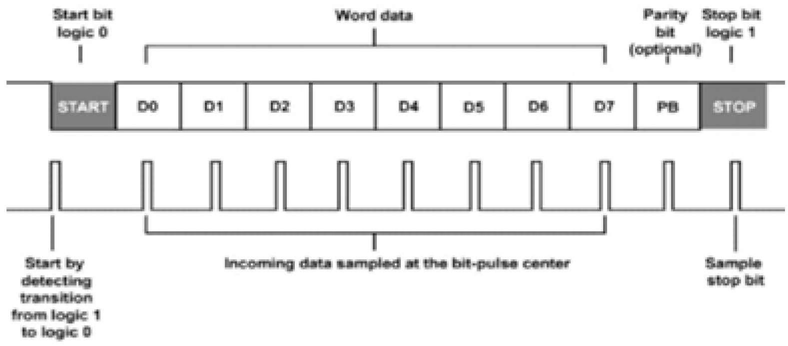


Figure 4: Frame structure of UART

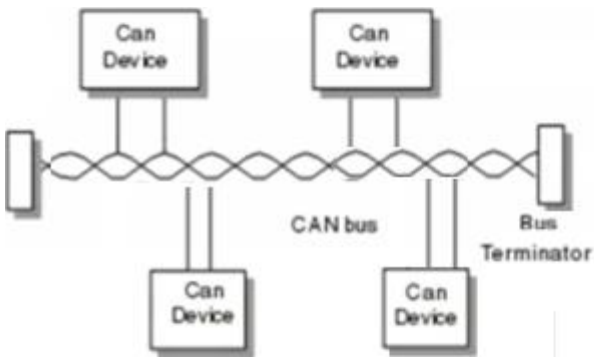
5. Features

CAN
- Prioritization of messages.
- Guarantee of latency times.
- Configuration flexibility
- Multicast reception with time synchronization.
- Multi-master
- System wide data consistency.
- Error detection and signalling.
- Automatic retransmission of corrupted messages as soon as buses idle again.

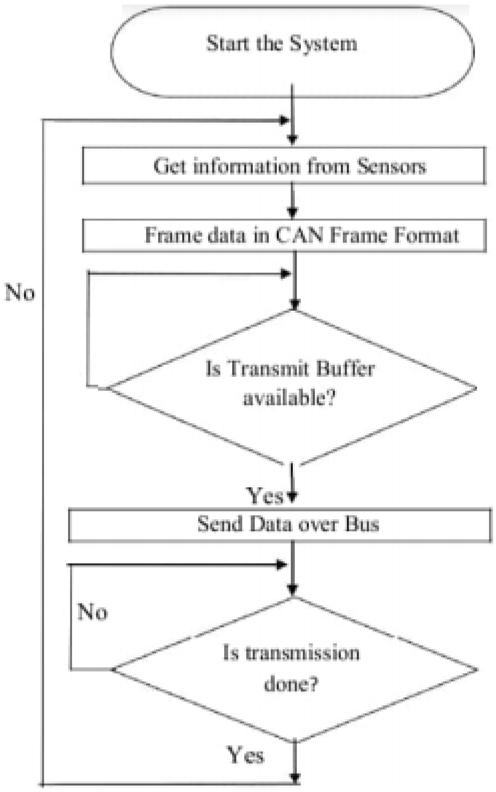
Figure 5- Structure of CAN bus

IOT
- Connectivity enables network accessibility and compatibility.
- Good sensing technology that provides true awareness of the physical world.
- Safety ensures securing of end points, the networks and the data.

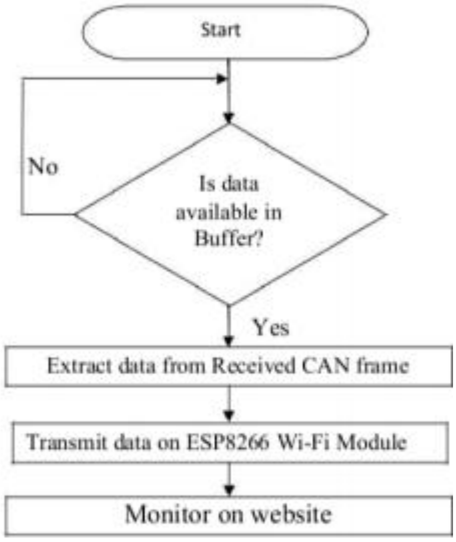
6. Flowcharts



Algorithm 1.1



Algorithm 1.2



7. Comparison

Scenario before implementation:

- Earlier connection of different ECUs used for engine management transmission control, antilock braking system, etc. was done by using point to point wiring.
- The average luxurious car had 30kg of wiring harness over 1km of copper wire and more than 2000 separate connections. This generates problems like heavy weight, increased complexity and size.
- Extremely expensive to manufacture, install and maintain.
- Also failure-prone and unreliable.
- Scenario after implementation:
- During the 1990's the automotive industry begun to use controller area networks, a multiplexed digital communication bus used to connect the ECU's.
- This approach dramatically reduced the size, weight and complexity of wiring harness.
- As the system uses CAN it becomes highly reliable.
- Implementation of this innovation reduces the rate of accidents due to potholes.

References

[1] https://elearning.vector.com/vl_can_introduction_en.html
[2] Renesas CAN pdf
[3] Serial Bus System pdf
[4] CAN primer
[5] LPC 17XX User Manual
[6] ADAFRUIT LIBRARIES
[7] http://nodemcu.com/index_en.html
[8] https://www.arm.com/products/processors/cortex-m/cortex-m4processor.php