The road forward for securely connected cars

This paper basically deals with self-driven cars and their vehicle to environment connection to provide low carbon dioxide emission, avoid accidents. Since the car is evolving with time in today’s world ninety percent of car innovation is in electronics. Vehicles are transformed into a mobile personalized information. Advanced Driver Assistance System permits the security and safety of drivers and passengers and enhances automation in driving. Self-driven cars will bring a heterogeneity of wireless connections for the exchange of data with other vehicles and the surrounding environment all this will aim at understanding the world around it in a way to reduces accidents and give passengers confidence in using these new secure self-driven cars. In this paper, we will be presenting an idea for decreasing the data storage problem in self-driven car and method for handling such enormous amount of data.

The solution is to not store any data in the car apart from it download everything from the cloud as per the need of a vehicle, surrounding and driver. In this, we are relying on cloud infrastructure for the cloud. Capable of reliable wireless and wired communication technologies together with powerful data-processing system, at the peak levels of privacy and system security, are analytical. This paper gives an idea of what it takes to really believe the securely connected car of the future.

In today’s world wired communication in the car is influence by Local Interconnect Network(LIN) and Controller Area Network(CAN). LIN is a serial network protocol (protocols are basically some set of defined rules for transmission of data between deferent devices) used for transferring information between a variable component in the vehicle. CAN is basically a

bus designed in such a way to permit microcontroller and various devices to share information with each other. the the the the bandwidth of LIN is up to 20kbps and CAN is up to 1mbps each of these is cost effective we can achieve high bandwidth link using point-to-point links (shielded cables). There is a demand for a system with higher bandwidth and for this, we required a new communication technology for avoiding the increasing cost and weight of copper cable in the car. The application which required higher bandwidth includes V2X, ADAS, Car radar. For this automotive ethernet is a new point-to-point network communication technology that is based on an unshielded twisted paper (UTP). It gives us an increase in bandwidth, increased data capacity, cost-efficient, reducing weight but it leads in toughness of design. this is because of switches, transceivers, and controllers used in it. Deterministic Ethernet points to a technology which uses the time to schedule for bringing deterministic real-time communication to a predefined IEEE 802 ethernet. It operates using a global sense of time.

Detection will be the most significant application for Ethernet since it requires much higher bandwidth for video transportation.

Ease of Use

A. VEHICLE-TO-EVERYTHING(V2X) COMMUNICATION It basically involves the sharing of information of vehicle and traffic related data between cars and different frames. The main aim for this is safety with energy saving. It is based on WLAN technology. Examples of V2X messages are warning about hazardous location, emergency braking, time of traffic lights. This technology is highly recommended for reducing road accident, decreasing carbon

dioxide emission, improving the flow of traffic, enabling autonomous driving. This technology enables a car to trace more than 300 objects and respond size is less than 20ms and it has a very low latency. Challenges are penetration level of V2X. For having effective network of cars at least 10% of them must have ITS module.

B. Car radar

Basically, a radar is used to detect if the speed is being observed by cops using a radar gun they are generally used so that the driver can decrease the cars speed before being caught by the police. It uses the Doppler effect to masseur the relative speed of the vehicle. New Car Assessment Program (NCAP) demands self-sufficient emergency braking system and pedestrian protection system. Radar provides range, velocity information to different sensors such as a camera. Nowadays reducing power consumption or increasing power efficiency can be achieved by reducing sensor size. The radar IC is used for covering 76-81GHz bandwidth for high range resolution. It is being verified by RFCMOS radars are used for operating in micrometer Wave band and by this, we can use the system on chip automotive radar including processors on a monolithic die.

C. Automotive Quality

Devices in Self-driven cars must withstand difficult environmental condition there for it requires rigorous packaging, circuit design, control of processing technologies. It will have various constraints, Stricter rules on device size. As a consequence, this leads to design consuming high power in order to full fill this robustness requirement.

D. Near area information exchange

It is commonly known as near field communication (NFC). It connects devices over the smaller range and high-frequency wireless communication technology can be achieved. It enables the transfer of data between devices about a distance of 10cm. It interfaces a smart card and a reader into one device it permits the exchange of data between digital devices like using a cell phone for booking online tickets. As it’s range is very less it gives a higher degree of security than commonly use Bluetooth it can also work if power is not being supplied in the device. The most important thing is that the tree operation modes are supported that is read/write, card emulation and device-to-device communication.

E. Ultrawide Band

This technology is used for transmitting processed data over a large bandwidth. A 100 kHz signal is communicated through multiple antennae within the car to make a response in the key, giving information regarding space between the car and the key by calculating the strength of the signal. IEEE suggest a different method by calculating the time of flight(TOF) of RF signal between the source and the destination. The TOF efficiency is directly proposal to signal bandwidth. It can also be used for tracking purpose of wireless monitoring of windows or mirror adjustment.

F. Security

The thing we have discuss like a various electronic function it gives the driver and increases comfort, safety, accuracy, convenient, but it has some

risks with it. This day’s vehicles are turning to (smartphones on whiles) which processes, store, exchange a large amount of data. By using wireless interfaces we can connect to the external network but it increases the probability of being hacked, resulting in the vehicle to be more vulnerable to cyber attacks. Hacker’s can gain complete remote control over the vehicle. This leads to security by design and privacy by design the key objects of security system includes hardware for example(Trust Anchors) which save our data against being hacked. This is the small crypto chips used in various products like ATM cards. passports, visa but safety system may be isolated from the entertainment system present in the car. This architecture needs to be regularly to handle attacks with more efficiency. We should implement multiple security techniques to minimize the risks of electronics devices that are being inside in the car. firstly we need to protect car external interfaces as they are prone for remote and scalable attacks the channel should be secure against data manipulation and unauthorized access by this interfaces. For providing protection in this layers cryptographic technologies must be used for encryption and decryption of data received that the receiver side.

But a securing system with this system is not sufficient. The security implementation should be isolated from deferent not secure code. To secure against side-channel attacks hardware should be designed in such a way that it does not leak unintended information with timing, consumption of power or leakage due to the electromagnetic field that could be an advantage for a hacker to find out information about what hardware is doing or what data store it. This is all about the internal protection but a physical attack requires physical protection. when hackers want to attack IC’s there

should be some tamper resistance for detecting some attacks. For example, people may use integrated sensors and after detection of the attack, it should automatically take appropriate counter masseur like powering of or distorting critical data so that it cannot be stolen.

G. Cloud Storing

We will be assuming that the connectivity of the network is available throughout. The data which we will be receiving from various sources is not necessary to search space to store its cloud is the exact solution for this. If the data is required the software will use it by downloading it. We should take care of some external storage to store the area map so that it can be run even if the network is not available. Now when the driven will be starting the car the computer will get connected to the network which will run web console and asked the user to sign in with username and password which was already registered with the cloud service provider. The user can now input the location where we want to reach, the software will download set of programs to process the data and the data which is already stored in the cloud will be taken by it and it starts processing. And it will act as a learning agent which basically learn from its experiences for example where a particular person goes often which are its favorite routes and it will use this information for the next time. It will also have the privacy which the user wants. Suppose a user wants to go to the place where the network is not available to the vehicle automatically store the data in advance. And if it sea a network issue it will ask the user to drive manually. When the location is reached the software delete all the data thus increase the security . The self-driven car will also spot the mechanical problem in advanced and even

repair it. Self-driving cars use the two-dimensional camera and “ LiDAR” to recognize different objects.

H. Types of Automation

1. No Automation: This is level zero automation in which the driver is the only person who will be having control over vehicle such as break accelerator staring.

2. Function defined automation: This is level one automation in which one or more function will be automated for example a car which has automatic gear will automatically change inside the system. It basically assists the driver.

3. Combine function automation: In this level minimal of two operations should be automatic for example the driver may have his hand and foot at a particular time while which the vehicle will be operating on the car.

Conclusion

This self-driven fully connected cars will only be a reality if they are secure and 100% reliable. The quality and security are the foremost requirements to gain customer confidence in this highly advanced new technology. Functionality like V2X, car radar, ethernet is already available but will continue to increase performance as well as their integration.

Acknowledgment

We would like to show our special thanks of gratitude to our professor Dr. Ramesh Vaddi for providing us this golden opportunity and guiding us. With this project, we came to know