Project-1 Computer Networks

AIM: To create a design and specification document for a concept for a decentralised, distributed data fabric provider for intermittent communication, that will be used to link together fragmented silos of data/communication requirements.

Name: Vanshika Sinha

Student ID: 21355135

Preferred focus and use case

The automotive industry is now advancing towards building more safer and feature-rich vehicles. This is the focus of emerging trends in the industry such as connected cars and self-driving cars. In particular, self-driving cars can greatly improve the safety of everyone on the road by eliminating human error and other factors such as latency in action. A major impact that networking and communication technology can have on self-driving cars is through vehicle-to-vehicle (V2V) communication. V2V communication can greatly improve the safety and convenience provided by self-driving cars. For example, consider a scenario when two cars are turning at the same time on a narrow road with a blind turn. If none of the cars are visible to each other, it greatly increases the possibility of a collision. If the V2V communication is possible, the cars can transmit their locations and other necessary information to nearby vehicles to alert them of their speed and direction of approach. Depending on this, both cars can then slow down or change their trajectory to avoid collision with advance warning. There can be several other possible use cases of V2V communication such as transmitting a distress or SOS signal to nearby vehicles in case a vehicle meets with an accident or the passengers need assistance in case of emergency. V2V communication in this case is effective as it will reduce latency and dependency on any centralized server. It can even scale with more capacity as more and more vehicles come into the network.

This project proposes a V2V communication system where vehicles can transmit data between each other in the format of messages. The key features and requirements of this V2V communication system will be:

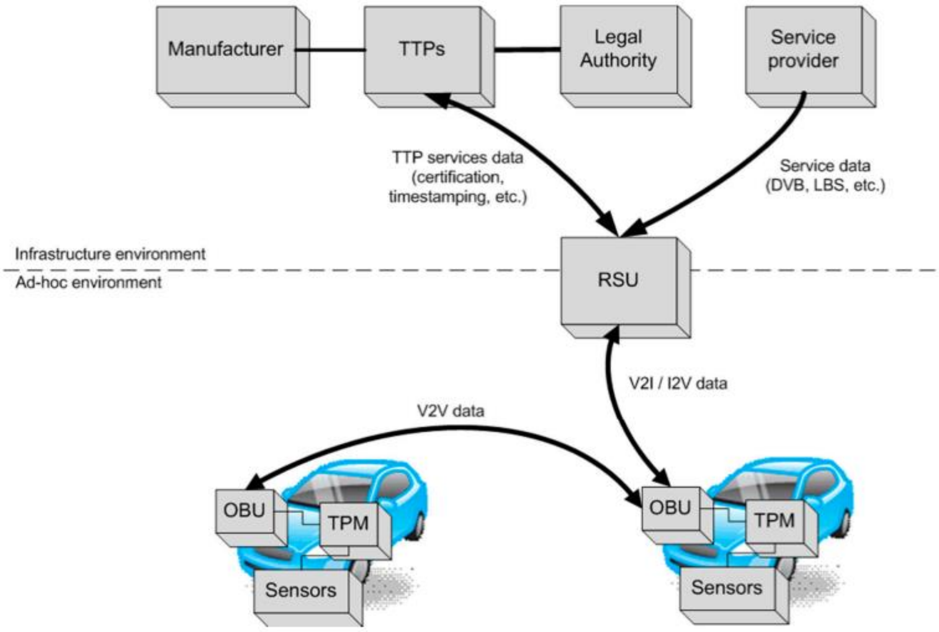
- Different criticality levels of message transmission. (For eg: In case of a blind turn or emergency, the message needs to transmitted quickly with a priority in queueing)
- Messages between vehicles should be transmitted based on the criticality and use case to the appropriate radius. For eg: The precise location of a vehicle would only need to be transmitted to the vehicles in close proximity while in case of an emergency, all vehicles within the locality may be alerted.
- In case of a full buffer, messages with low priority can be dropped but those with higher priority should be allowed to be communicated.
- The communication should be secure. The data transmitted between vehicles can be sensitive information and should not be readable by untrusted agents.
- The throughput of the messaging system can be low as only critical messages with few vital pieces of information such as the location and speed of vehicle is sent. But the throughput is not elastic as messages need to be transmitted quickly.
- Message integrity should be verified to safeguard against unwanted messages sent by malicious sources.

- On the application layer, messages should be access controlled and users should only be authorized to send messages only according to their permissions. For example, in the event of an accident, if a user is incapacitated, or if the car has some fault, the message should be sent automatically and a user should not be able to send such a message voluntarily.

The key constraints of the solution are as follows:

- The communication should be with latency less than the human reaction time to be sufficient in case of an emergency.
- The communication hardware should be lightweight and portable to be installed on the vehicles.
- The number of hops for messages should be minimum.

The solution can later be extended to communication between other agents as well such as vehicle to pedestrians (V2P) and vehicle to surrounding infrastructure (V2I). An example fo such an architecture is shown in the figure below:



Protocol Overview:

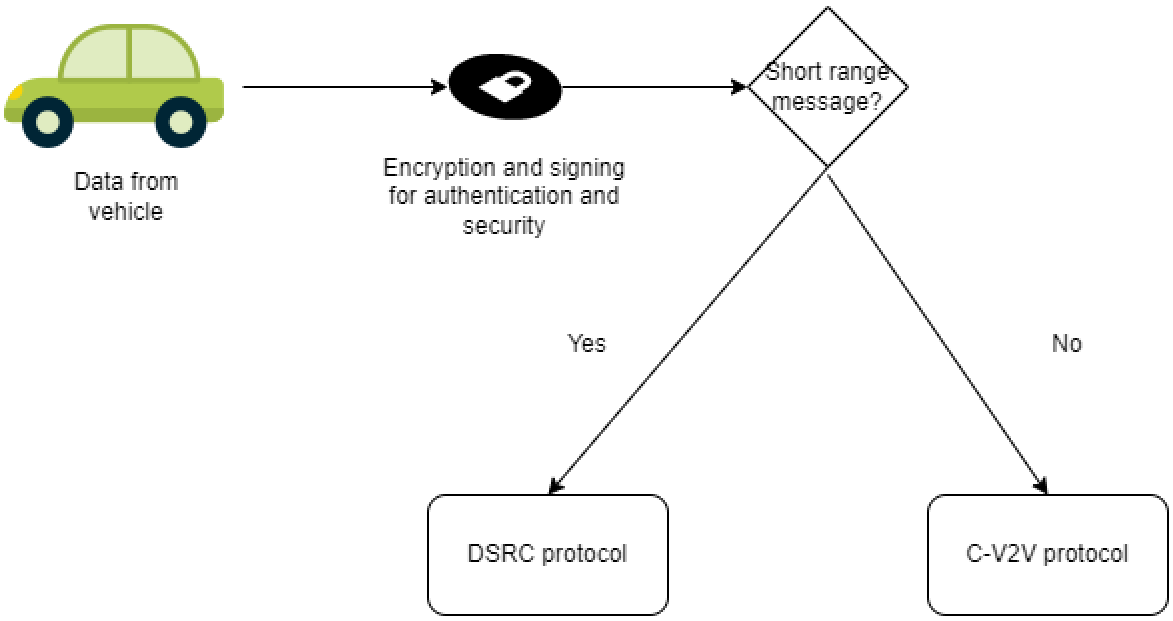
The vehicles require a communication protocol which enables the transmission of data securely between vehicles with authentication.

- **(Dedicated Short Range Communication) DSRC protocol:** This protocol enables direct communication between two compatible devices in a short range (1 km) without relying on an intermediary such as cellular network. It operates in the 75MHz band, with low latency in establishing connections. It is robust and susceptible to interference. In addition, it performs good even in extreme weather conditions. However, it is less accurate when two vehicles are speeding and out of the network range.
- **(Cellular Vehicle-to-vehicle) C-V2V protocol:** This protocol uses a cellular connection to transmit data between vehicles. It uses the cellular network as an intermediary between vehicles. It covers a wide area of communication where-ever the cellular signal is available. It works well even in communication between fast moving vehicles.

For optimizing both short and medium range communication between vehicles according to the use cases described above, the proposed design will use both DSRC and C-V2V protocol to transmit data. In case of short-range communication use case where the vehicle needs to alert other vehicles about its location and speed, it will use the DSRC protocol and otherwise, in case of emergency scenarios and to alert nearby vehicles in the locality, it will use C-V2V protocol. The messaging would be on a mesh network P2P based mechanism similar to BitTorrent. All vehicles would be automatically logged into the network if they are turned on. When the vehicle is parked or off, it will be logged off from the network.

Communication Model:

The communication model is described in the figure shown:



The data from the vehicle is first sent to a encryption and signing module to encode the data to prevent manipulation and unauthorized interception of data by malicious actors. After this, a decision module can look at the type of message classification that needs to be transmitted, and depending on the range required, it will transport the message using DSRC or C-V2V protocol.

On the receiving side, the process would occur in reverse. The decision module would not have a role to play in while receiving a message. After receiving a message on any of the protocol, the message would be authenticated and decrypted for subsequent actions to be performed.

Module Descriptions

The vehicles interact using a P2P framework where each vehicle signs the data sent using a certificate or cryptographic techniques to ensure the integrity of the message. In addition, the message transmission will be encrypted to prevent data manipulation and sniffing. For encryption, state of the art algorithms such as AES256 or RSA can be used. The trade-offs are involved in the protocols selected. DSRC protocol works even in low network areas, where there is no cellular reception, but it has its some shortcomings as described above. While C-V2V protocol is used for communication over a wider range.

Summary of Algorithms

The overall communication algorithm is explained in the communication model diagram above. To achieve the required functionalities of different modules , the following libraries will be used in Python:

1. Encryption:
   a. Cryptography (https://pypi.org/project/cryptography/): This open source library provides encryption based on all major state of the art algorithms such as AES-256. It is portable across a wide range of environments.
2. Wireless connection:
   a. Wireless (https://pypi.org/project/wireless/): This python library offers cross-platform support for implementing wireless communication using simple interfaces in code.

Software Development Practices

The communication module will be designed with security and reliability in mind. The development will be done in test-driven fashion where each module will be unit-tested after implementation to ensure that the module performs well in all use cases. After individual module testing, the module can be tested as a whole system in the integration testing stage to ensure that all modules interact and are compatible with each other. This will also help to track and observe the overall metrics of the system such as latency.

References:

1. https://journals.sagepub.com/doi/10.1155/2013/676850
2. https://innovationatwork.ieee.org/autonomous-vehicles-standards-need-greater-focus-on-vehicle-to-vehicle-v2v-communications/
3. file:///C:/Users/hp/Downloads/preprints201706.0001.v1.pdf
4. https://arxiv.org/ftp/arxiv/papers/2102/2102.07306.pdf
5. https://www.information-age.com/need-know-vehicle-vehicle-communication-123465752/
6. https://connectedvehicle.devpost.com/details/understanding-dsrc
7. https://www.sciencedirect.com/science/article/pii/S2590005621000321?dgcid=rss_sd_all