Enhanced V2X communication

Vignesh Somasundaram 7206904
Mangal Deep Balasubramani Marutha Babu 7206937
Mukesh Channarayapatna Nanjegowda 7206931
Swathi Sudeendra Rao 7207100

ESM, FH Dortmund

February 28, 2020

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Project Mission

To develop a fully functional subsystem, which can secure the vehicle from all forms of security breach in a commercial automobile encompassing all, the below domains:

The infrastructure domain includes vehicle manufacturers (supply chain), service providers (emergency services, billing, etc.), and trust authorities (TA). Attacks applied at this domain may be platform integrity, data analysis, denial of service (DoS) against functionality, etc.

The V2X domain is representing all the V2X communications, such as the communication between vehicle on-board unit (OBU) and roadside units (RSU) as well as the communication between neighbouring vehicles (V2V) or even V2P. Types of attacks, which applied at this domain, include Black hole, Flooding, Sybil attack, and jamming.

The in-vehicle domain consists of the trusted platform modules (TPM), application units (AU), and electronic control units (ECU). Examples of attacks at this domain may be tampering or physically damage units, manipulating the in-vehicle communications, etc.

1.2 Project Vision

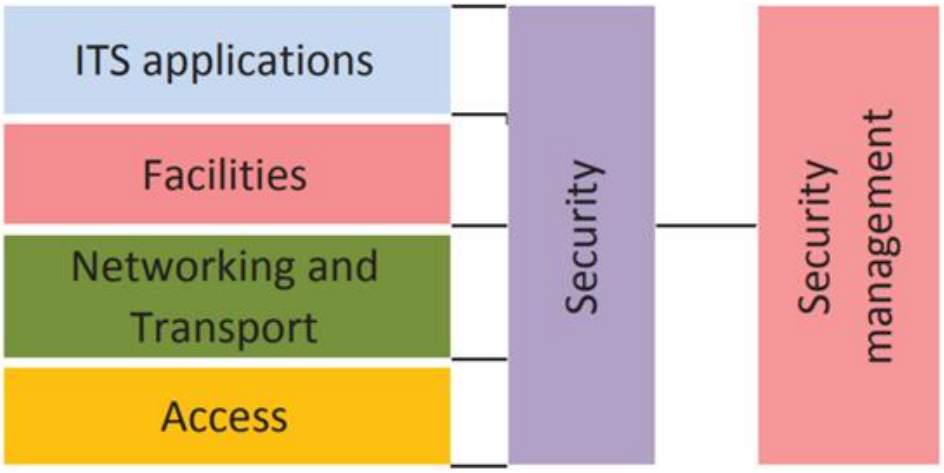

Figure 1 Enhanced V2X communication Overview

- This system aims at reduction of foreign intrusion there by securing the vehicle and the system from any hacking.
- The customer is seldom provided decision of the faulty message or the corrupted one, but with the improved computational understanding, more autonomy can be given to the system itself.
- Manages all incoming and messages from external environment, verifies the genuinely of the message and corrects if identified as faulty/intrusion/alarming then cascades to the main system for deployment.
- The algorithm depends on statistical data stored, adaptive and mutable data change identification, error comparison etc.
- Provision to go into idle mode if messages are under huge traffic and priority inversion takes a toll.

1.3 Abbreviation

OTA	Over the Air
TCU	Telematics Control unit
DoS	Denial of Service
TA	Trust Authority
V2V	Vehicle to Vehicle
V2X	Vehicle to anything
ECU	Electronic Control Unit
RSU	Road Side Unit
OBU	On Board Unit
AU	Application Unit
TPM	Trusted Platform Module
V2P	vehicle to Pedestrian
SDR	Software Defined Radio
GPS	Global Positioning System
DSRC	Dedicated Short-Range Communication
BCM	Body Control Module
PCM	Powertrain Control Module

Table 1 Abbreviations

1.4 References

- **IEEE SRS Format.**
- 1st IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES-2016) - Car Security using the Internet of Things by Vivek Kumar Sehgal), Soumitra Mehrotra2, and Harshit Marwah3
- Trends in Automotive Communication Systems by NICOLAS NAVET, YEQIONG SONG, FRANÇOISE SIMONOT-LION, AND CÉDRIC WILWERT (Invited Paper)
- Security requirements for automotive on-board networks by Olaf Henniger, Ludovic Apvrilley, Andreas Fuchs, Yves Roudierx, Alastair Ruddle, and Benjamin Weylk ,Fraunhofer Institute for Secure Information Technology, Darmstadt
- https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/
- https://web.stanford.edu/class/ee26n/Assignments/Assignment5.html

1.5 Overview

The system must serve as a fool proof medium for the message interactions between the various physical entities surrounding the car.

2. Overall Description

2.1 Situation Model

2.1.1 Situation Name: GPS Spoofing

Information Source: In the last 3 years over 600 incidents of spoofing have been recorded in the seas near the Russian border. These ships appeared to be “transported” to nearby airports (3). This type of spoofing might have been introduced as a defense mechanism to ground spy drones. Most semi-professional drones on the market have a built-in geo-fencing mechanism, which lands them automatically if they come close to airports or other restricted areas (4).

Reference: https://www.septentrio.com/en/insights/what-spoofing-and-how-ensure-gps-security

Functional Analysis: Radio interference can overpower weak GNSS signals, causing satellite signal loss and potentially loss of positioning.

Spoofers overpower relatively weak GNSS signals with radio signals carrying false positioning information. There are two ways of spoofing:

- Rebroadcasting GNSS signals recorded at another place or time (so-called meaconing)
- Generating and transmitting modified satellite signals

Short Description: Spoofing is an intelligent form of interference, which makes the receiver, believe it is at a false location. During a spoofing attack, a radio transmitter located nearby sends fake GPS signals into the target receiver. For example, a cheap SDR can make a smartphone believe it is on Mount Everest! Representation of the Environment. External Environment: Faulty antenna or GPS coordinate the broadcaster, Satellite signal blocking Circuits Internal Environment: Telematics Unit, GPS antenna, Vehicle battery, Multimedia system. Driver Constraints: Less secured external systems, weak GNSS signals, inability to have a secured and authenticated signal.

Remedy: With the introduction of the subsystem, the system can be given an intimation on the geninuity of the data after analysis with the static maps, image capturing the external environment, comparing and communicating with other vehicles in a different location (time and place estimate). These algorithms can run after the subsystem learns that there is an underlying threat.

2.1.2 Situation Name: Replicating roller key pattern and disarming the immobiliser

Information Source: The Munich-based automobile club ADAC late last week made public a study it had performed on dozens of cars to test a radio "amplification attack" that silently extends the range of unwitting drivers' wireless key fobs to open cars and even start their ignitions, as first reported by the German business magazine WirtschaftsWoche. The ADAC researchers say that 24 different vehicles from 19 different manufacturers were all vulnerable, allowing them to not only reliably unlock the target vehicles but also immediately drive them away.

Reference: https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/

Reference: https://web.stanford.edu/class/ee26n/Assignments/Assignment5.html

Functional Analysis: The Attack by building a pair of radio devices; one is meant to be held a few feet from the victim's car, while the other is placed near the victim's key fob. The first radio impersonates the car's key and pings the car's wireless entry system, triggering a signal from the vehicle that seeks a radio response from the key. Then that signal is relayed between the

attackers' two radios as far as 300 feet, eliciting the correct response from the key, which is then transmitted back to the car to complete the "handshake." The full attack uses only a few cheap chips, batteries, a radio transmitter, and an antenna. The Roller jam, which can be planted on a car to intercept and replay the “rolling codes” vehicle locking system manufacturers, developed to stay ahead of earlier replay attacks.
Short Description: By this method, the roller key can be recorded and replayed by radio transmitters, which can be used to hack a vehicle.
Representation of the Environment:
External Environment: Multiple radio transmitters, RF recorders and amplifiers.
Internal Environment: TCU, Key Fob, receiving antenna, BCM
Remedy: The enhanced intelligent system will not accept the recorded and replayed roller keys, by considering the place of parking, the presence of the key fob. It would expect a fresh roller key every time there is a request. In addition, the timing and response time is also monitored.

2.1.3 Situation Name: Undesired Vehicle Platooning

Functional Analysis: The attack begins by the intrusion of a malware, which penetrates into the control of the module responsible for directing the slaves. This results in an uncontrolled and undesired command line approach for the slave by the master. The operability of the slave vehicles depends upon the commands of the master vehicle, which can result in catastrophes.
Reference:
https://orfe.princeton.edu/~alaink/SmartDrivingCars/ITFVHA15/ITFVHA15_USA_FutureTruck_ADP_TF_WhitePaper_Draft_Final_TF_Approved_Sept_2015.pdf
Short Description: Platooning is an operation that instructs a group of vehicles to have a certain formation where individual vehicles move in a closely linked manner. To maintain the platoon formation, each vehicle needs to sense the environment, and share the environmental data and critical control information such as route, speed, heading direction and future intentions (braking, acceleration, etc), so that the lead vehicle and other follower vehicles can remain connected with each other. Platooning control helps reduce overall fuel consumption of the platoon, as well as the number of needed drivers.
Representation of the Environment:
External Environment: Telematics Unit from other vehicles.
Internal Environment: TCU, Key Fob, receiving antenna, BCM, PCM
Remedy: Before taking the decision of obeying the master, the slave subsystem needs to ensure the data coming from the master is legitimate. This can be verified with the GPS location, the speed limit of the area, which can be obtained from the cross-traffic alert system, the presence of any obstacle with the help of obstacle detector modules.

2.1.4 Situation Name: Uncontrolled Active braking

Functional Analysis: Certain information originating within a vehicle (such as the vehicle’s environment sensor information, vehicle dynamics sensor information, or position information) when influenced via a malicious entry can lead to hazardous effect.
Representation of the Environment:
External Environment: Multiple radio transmitters, RF recorders and amplifiers, external hardware.
Internal Environment: TCU, BCM, Dynamics sensors, ABS.
Remedy: In such a case the message’s origin, content and time if the vehicle performs actions based on that information needs to be checked and authenticated. Similarly, certain

information that a vehicle receives from other vehicles (such as other vehicles' position information, vehicle-dynamics sensor information, or position information) shall be authentic in terms of origin, content and time if the vehicle performs actions based on that information (such as active braking).

2.2 Stakeholder Analysis

Stakeholder	Communication type (V2V/V2I/ V2N) */ Role played	Interest of the Stakeholder
Pedestrian	V2N	• Risk evaluation • Time management • Risk communication
Customers	Via an Application connecting the driver's smart device to the vehicle	• Risk management • Time management • Improves lifestyle
Engineers and technical support	Installation and maintenance	• Ensuring smooth operation • Evaluating faults • Solution discovery for the challenges • Safety evaluation and compliance
Smart Building owners	V2I	• Easy allocation of Parking Slots • Evaluation of the number of parking slots • Drop and take-off places allocated
Investor/ OEM	Investing upon the firmware	• Risk evaluation • Time management • Capital investment • Safety evaluation and compliance • Delivery of the system

Table 2 Stakeholder analysis

2.3 Target Group

1. Investors
2. Smart Car manufacturers
3. Certification Authority
4. Telematics Unit
5. Web developers
6. Safety engineers
7. V&V team

2.4 Assumptions and Dependencies

1. All the physical entities are connected to the internet.
2. Information from the outside world is transmitted to the modules in the network only by the TCU.

3. Specific Requirements

3.1 Functional Requirements

1. (SRS-001) The system should be able to identify the Impersonation of the sender of V2X messages being sent to the vehicle. (Priority: HIGH)
   Attributes: MessageClass, SenderClass.
2. (SRS-002) The systems should be able to decide the criticality of the message and decide on the imminent step, in case of jamming the channel for V2X control signal, typically that throttles the service availability, viz, the denial of service (DoS) attack. (Priority: MEDIUM)
   Attributes: SystemUnderAttackDetection, HazardPreventionAct.
3. (SRS-003) The System should be able to identify any modification of the V2X message and alert the customer on the tampering. (Priority: LOW)
   Attributes: MessageAuthencity, IntruderAlert.
4. (SRS-004) The System shall monitor the GPS coordinates, which it received from the transmitters and check for the authenticity based on the statistical and past records. (Priority: MEDIUM)
   Attributes: GPSCoordinatesReceived, GPSCoordinateDatabase.
5. (SRS-005) In case of the roller key impersonation, the systems shall monitor the time taken to send the keys from the time of request. In addition, delay and interrupt shall be identified and reported to the owner. (Priority: HIGH)
   Attributes: RollerKeyID, KeyValidationTime.
6. (SRS-006) The system shall detect any foreign connection any hardware connected wirelessly as well as wired in the network (which tries to query it) and report it to the customer. (Priority: HIGH)
   Attributes: SourceIdentifier, SourceValidity.
7. (SRS-007) The system shall support all the Diagnostic requirements of the parent hardware in which it is hosted. (Priority: LOW)
   Attributes: DTC, HWID.
8. (SRS-008) The system shall operate on a common checksum and CRC for sending and receiving signals and authentication of the message. (Priority: MEDIUM)
   Attributes: Checksum, CRCbits
9. (SRS-009) The systems shall validate the checksum value upon failing so shall report the anomaly to the customer. (Priority: LOW)
   Attributes: ChecksumCriteria, ChecksumValidity.
10. (SRS-010) The system shall monitor the time, frames and any intrusion while receiving information from the pedestrian systems. (Priority: LOW)
    Attributes: Time, Frame.
11. (SRS-011) The system shall obey the IEEE standard IEEEP1619 encryption standard for message sending and receiving. (Priority: MEDIUM)
    Attributes: EncryptMsg, MessageFactor.
12. (SRS-012) The system shall detect the obstruction of the visual range of the driver of an individual vehicle by large vehicles (e.g., trucks). (Priority: LOW)
    Attributes: ObstacleDistance, ObstacleType.

13. (SRS-013) The system shall support and communicate with other systems so that the message frames sent from other vehicles can help the vehicle to determine whether a potential hazard exists. (Priority: LOW)
    Attributes: MessageValidity, MessageReceived.
14. (SRS-014) The system should broadcast an emergency notification message including position data in order to warn other systems on the impending emergencies examples, imminent stop for a traffic jam stop, accident. (Priority: HIGH)
    Attributes: EmergencyFlag, EmmergencyClass.
15. (SRS-015) The system shall monitor and report the activity of the nomadic devices like USB sticks, or MP3 devices and other aftermarket parts and prevent any security breach. (Priority: HIGH)
    Attributes: DeviceValidity, DeviceAcceptance.
16. (SRS-016) The systems shall be available for continuous updates with Over the Air updates. (Priority: LOW)
    Attributes: UpdateAvailability, AutoUpdateON.
17. (SRS-017) The system shall allow the connection of the known devices upon a secured encrypted key acknowledgement with a time factor and identity factor. (Priority: HIGH)
    Attributes: DeviceID, DeviceType.
18. (SRS-018) The system should act upon the data being received by the TCU and not the intra-communication between the modules. TCU should act as the gateway for the system. (Priority: MEDIUM)
    Attributes: TCURX, TCUTX.
19. (SRS-019) The system shall pass the message as such if the authenticator is not able to complete the process of authentication within the stipulated time. (Priority: LOW)
    Attributes: MessageReceived, CheckTimeout.
20. (SRS-020) A certificate authority (CA) issues certificates for DSRC units. The role might be split into a CA and a registration authority (RA) to introduce an organizational mean of privacy protection. (Priority: HIGH)
    Attributes: Certification, Registration.
21. (SRS-021) Certificates need to be renewed regularly to provide new certificates for the privacy mechanism of changing certificates. New certificates could be requested via DSRC RSU, if available, or large bulks of certificates could be loaded during vehicle service. (Priority: HIGH)
    Attributes: CertUpdateCount
22. (SRS-022) Certificates could be encrypted before loading them to a DSRC unit and only decryption keys could be provided regularly via DSRC RSUs. (Priority: LOW)
    Attributes: CertificateUpdates
23. (SRS-023) Revocation is necessary to remove DSRC units from the system (e.g. after misbehaviour occurs). Revocation can be performed with two mechanisms (Priority: MEDIUM)
    Attributes: RevocationFrequency
    23.1. (SRS-023.1) Distribution of certificate revocation lists (CRL): the CA lists all certificates to be removed in a CRL and distributes the CRL to all DSRC units. DSRC units then do not accept packets anymore from senders that use

revoked certificates. Since each DSRC unit is equipped with multiple certificates, an efficient mechanism is required to identify all certificates of a DSRC unit with a single entry.

Attributes: RevokedCertificatesNum

23.2. (SRS-023.2) Denial renewal of certificates: the CA creates a CRL but does not distribute it to DSRC units. However, if a revoked DSRC unit requests new certificates, the request is denied

Attributes: RevokedCertificatesNum

24. (SRS-024) CA Hierarchy could be highly flexible. For instance, there might be root CAs for Europe and for the US. Sub-CAs might be deployed per state and nation, and there might be sub-CAs per vehicle manufacturer. It is crucial though those minimum requirements for CAs are defined to allow interoperability. A flat hierarchy is superior in terms of performance, especially for V2V safety applications. (Priority: MEDIUM)

    Attributes: CALevel, CA_Authority.

25. (SRS-025) Connectivity between DSRC units and CA shall be needed to enable security. At deployment, this connectivity might be provided by Cellular connection or by DRSC RSUs. In case of RSUs, it is foreseen that a relatively small number of RSUs is sufficient that can then grow with higher OBU penetration rates. (Priority: HIGH)

    Attributes: RSUNum, ConnectivityStratergy.

3.2 System Requirements

1. (SRS-026) The system shall retain its past state even when the power supply to the system is stopped.
2. (SRS-027) The system shall not occupy more than 2MB space in the memory unit.
3. (SRS-028) The system shall have the priority immediately next to safety.
4. (SRS-029) The system shall adhere to hard deadlines.
5. (SRS-030) The system shall be capable of identifying the aged data.

3.3 Goal Model

3.3.1 SDM

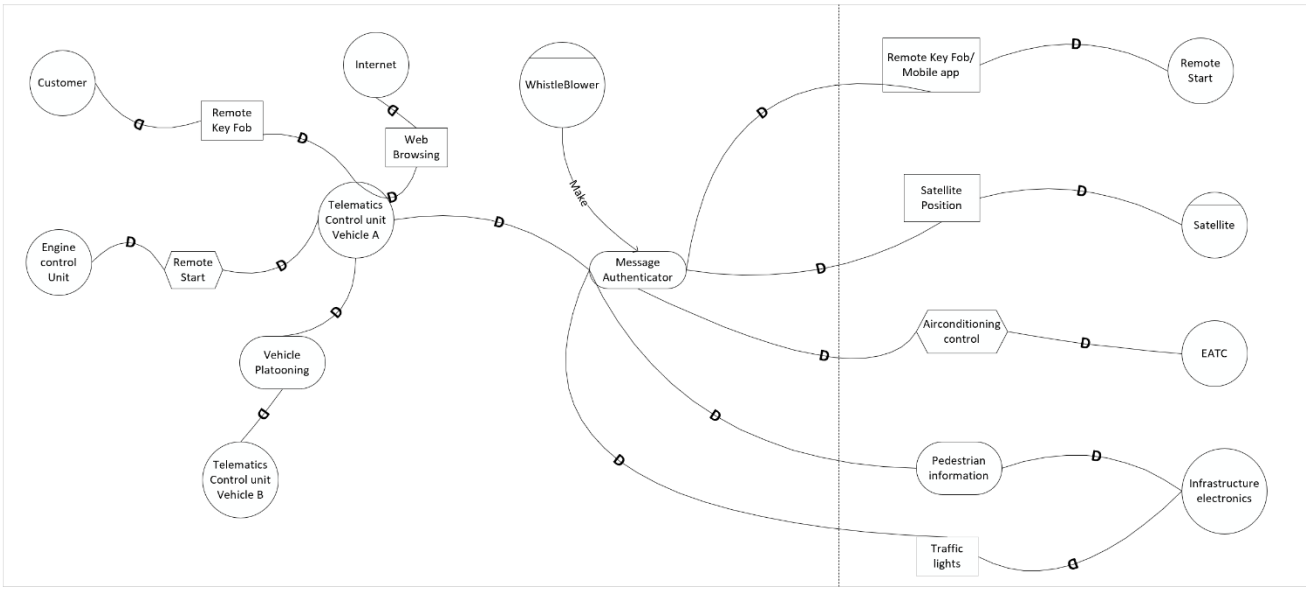

Figure 2 SDM

3.3.2 SRM

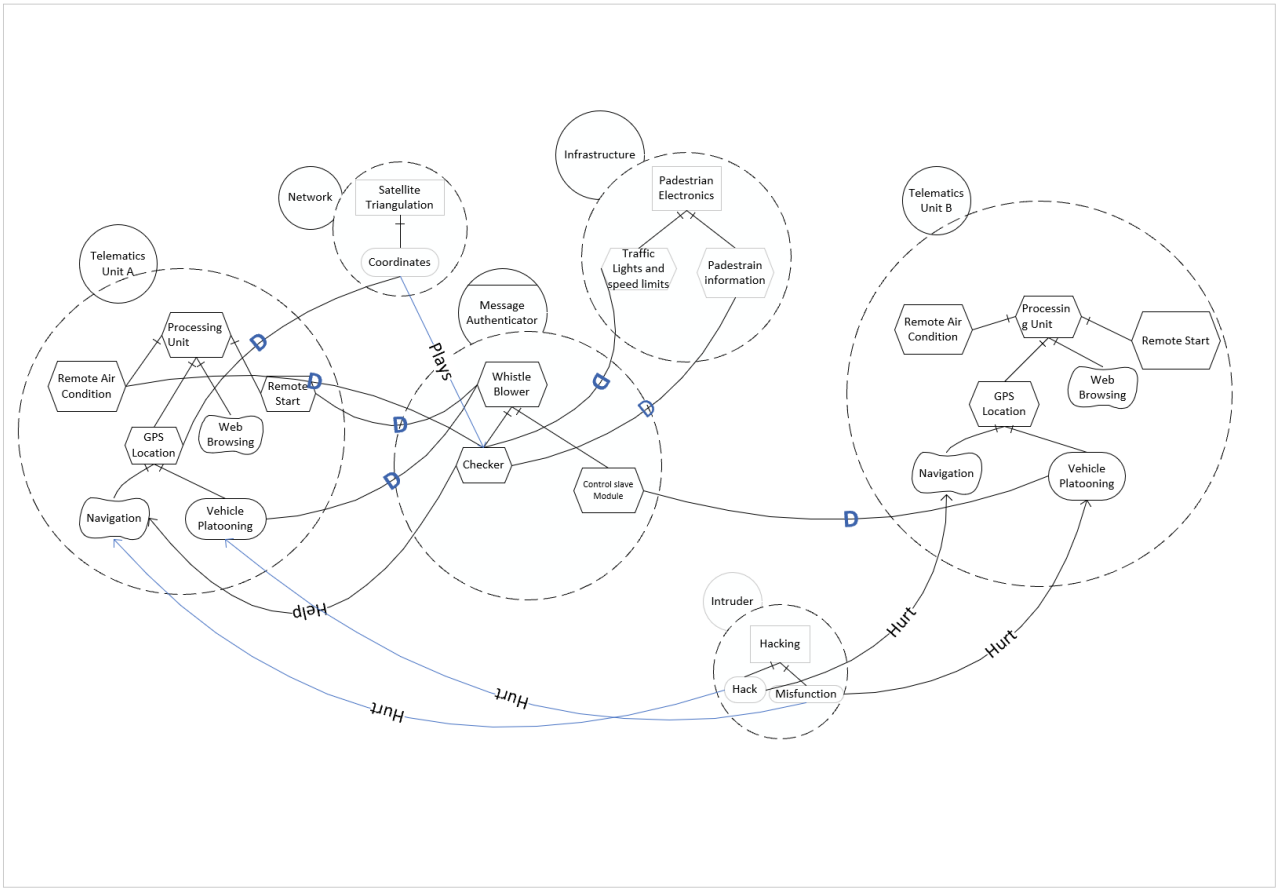

Figure 3 SRM

3.4 Context Model

The following context diagram provides an idea about the overall system and their interactions between the modules.

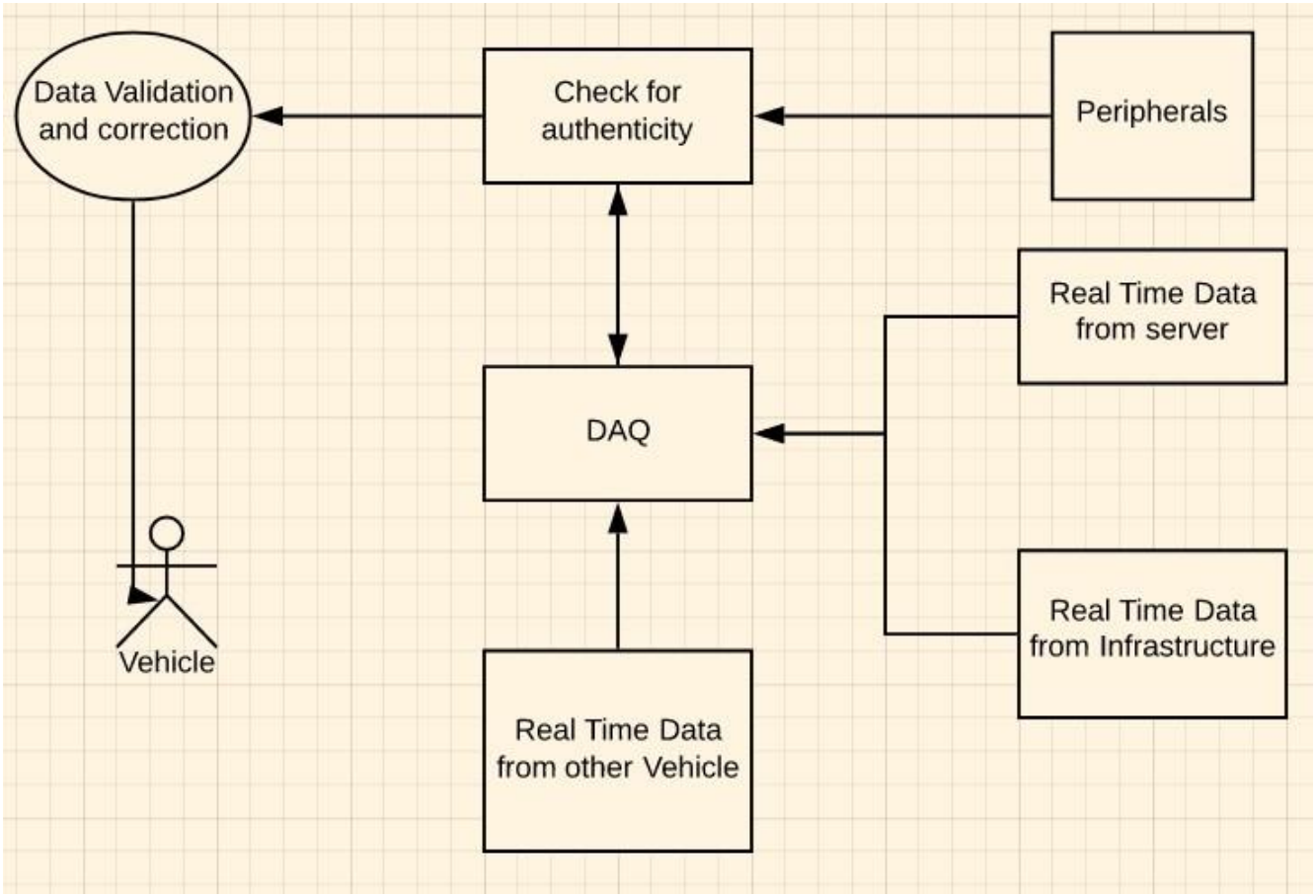

Figure 4 Context Model

3.5 Data Model

The following Data Model provides information on the overall V2X system and the exchange of messages between the various physical entities depicted through a class diagram.

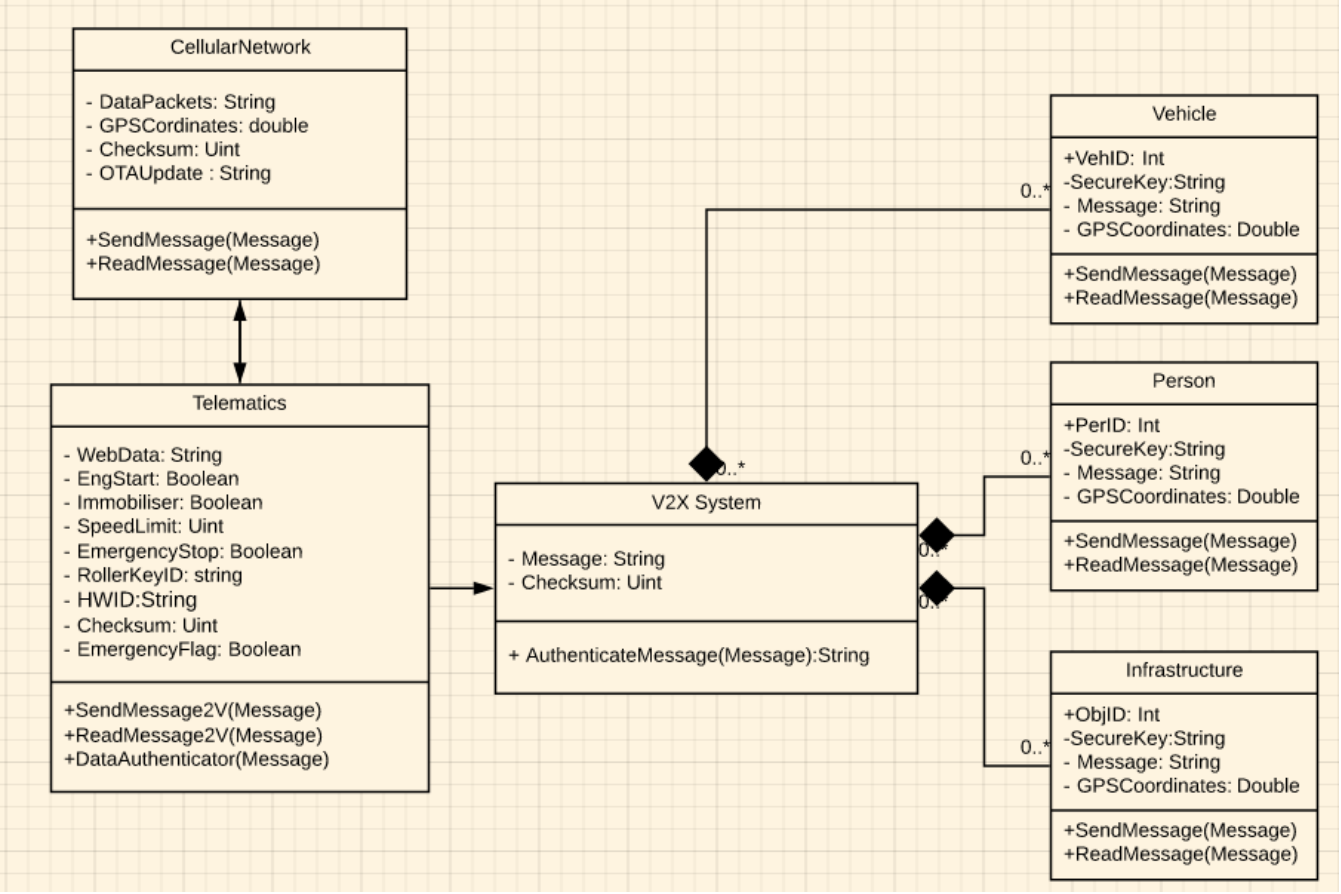

Figure 5 Data Model

3.6 Use Case Diagram

Use case diagrams consist of a set of use cases, actors and their relationships. Each use case represents a particular functionality of use case.
Use case diagrams serves purpose of gathering the requirements of the system. They represent the outside view of the system and helps in identifying the external and internal factors influencing the system.

We have modeled the actor use case relationships of our V2X enhanced communication System with two use-case diagrams.

Functionalities of the system are represented by use cases with their dependency and relationship between other use cases and actors.

1.

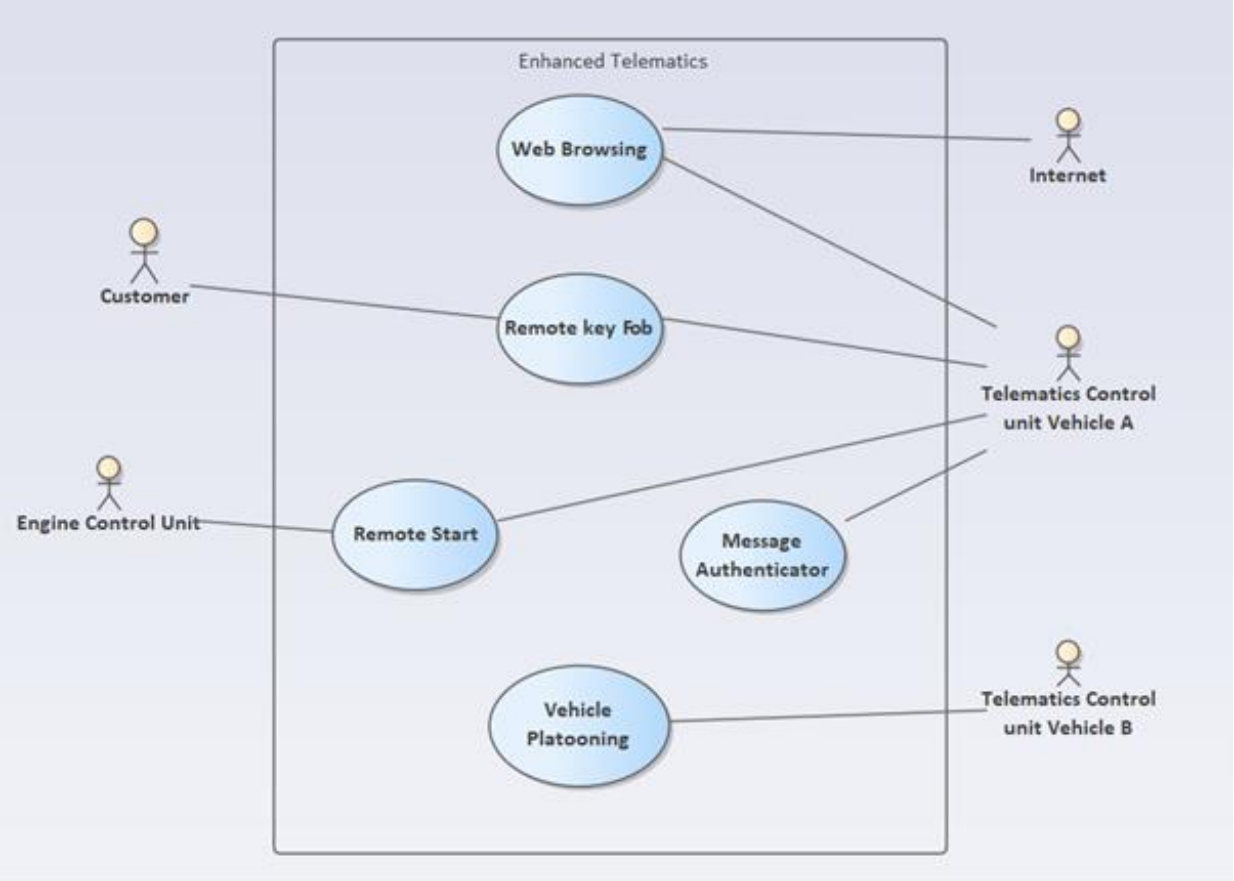

Figure 6 Use Case I

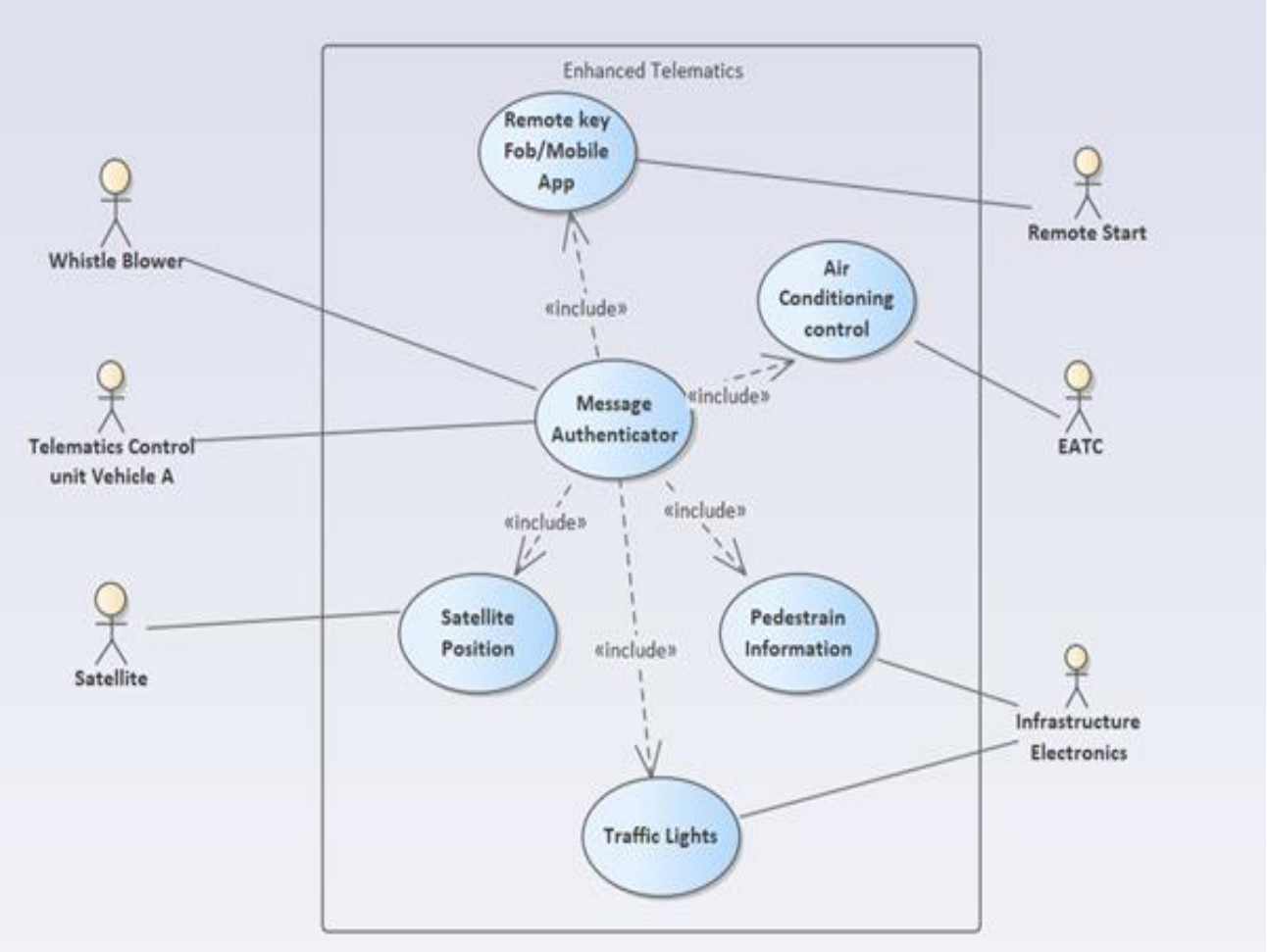

Figure 7 Use Case II