C-ITS use cases: study, extension and classification methodology

Farah Haidar, Arnaud Kaiser, Brigitte Lonc, Pascal Urien, Richard Denis

C-ITS use cases: study, extension and classification methodology

Farah HAIDAR[1,2,3], Arnaud KAISER[2], Brigitte LONC[1], Pascal URIEN[3], and Richard DENIS[4]

[1]*Renault*, Guyancourt, France, Email: name.surname@renault.com
[2]*IRT SystemX*, Palaiseau, France, Email: name.surname@irt-systemx.fr
[3]*Telecom ParisTech*, Paris, France, Email: name.surname@telecom-paristech.com
[4]*Valeo*, Creteil, France, Email: name.surname@valeo.com

***Abstract*—In the near future vehicles will be connected and able to communicate with their environment. Such technologies – commonly called Cooperative Intelligent Transportation Systems (C-ITS) – aim at improving road safety, traffic efficiency and drivers comfort. To this end the C-ITS community has proposed many different use cases. In this paper, we start by making an inventory of C-ITS use cases. We then extend this list by proposing new use cases mostly related to security and privacy aspects. Finally we propose a classification methodology based on K-means algorithm to classify the use cases according to criteria we defined. We apply the proposed methodology on our use cases list using security and technical criteria. The obtained results enable to extract a subset of representative use cases from the initial list. Such subset can then be used to apply any process/method (e.g. risk analysis) on it.**

***Keywords*—C-ITS use cases, classification, K-means.**

I. Introduction

C-ITS have gained much attention in the recent years due to the large number of applications/use cases that can improve future driving experience. These applications are based on vehicular communications (V2X). The kind of information exchanged and processed by vehicles can be critical and directly linked to drivers privacy. Therefore security and privacy of C-ITS communications must be taken into account. To this end a risk analysis should be done on the use cases.

However due to the very large number of existing use cases, treating individually each use case is a tedious task. By reducing the list of use cases the treatment can be speeded up. This can be achieved by classifying the use cases into clusters that share common properties and then select a representative subset of them. The risk analysis can then be done on this subset.

In this paper, we first make an inventory of the existing use cases specified by european and american standardization bodies, the cellular community and european projects. We then propose new use cases, mostly related to security and privacy aspects, that are not considered yet. Finally we propose a classification methodology based on the K-means clustering method to classify those use cases. We then use the methodology on the use cases list by using security and technical criteria for classification.

This paper is organised as follows. Section II presents the related works. In section III we detail the new use cases we propose. Our classification methodology is presented in section IV and the obtained results are discussed in section V Finally, section VI concludes the paper and presents future works.

II. Related works

The first step of our work is to make an inventory of existing C-ITS use cases. To this end, we study use cases proposed by European (EU) and American (US) standard institutes, the cellular community, use cases proposed by C-ITS European projects and propositions from the literature.

A. EU standards

In Europe, the European Telecommunication Standard Institute (ETSI) is in charge of standardization activities related to C-ITS. In [1] they detail the Basic Set of Applications (BSA) which consists of a list of use cases they consider for Day-1 deployment (i.e. use cases that may be deployed simultaneously at a targeted time). The selection of use cases to be included in the BSA is made subjectively. ETSI distributed a questionnaire to active stakeholders in ETSI, ISO and European ITS projects. The following criteria were used:

- Strategic requirements
- Economical requirements
- System Capabilities requirements
- System Performances requirements
- Organizational requirements
- Legal requirements
- Standardization and certification requirements

Details of the questionnaire and the critera can be found in annex A and B of [1].

B. US standards

In the US, standardization also specifies use cases related to security and privacy. Authors of [2] present the US security system for C-ITS, namely Security Credential Management System (SCMS). SCMS defines the following four classes of use cases related to security:

- Device bootstrapping
- Pseudonym certificate provisioning
- Misbehavior reporting
- Global misbehavior detection and revocation.

C. Cellular

With the ongoing development of 5G and the Device-to-Device (D2D) communication, the cellular technology tends to become a strong candidate for V2X communications. In order to deal with new complex situations and needs, projects and industries introduce the 5G technology on vehicular network, especially to improve performances [3]. The 5G PPP presents in [4] its vision on how 5G will enable the next generation of connected and automated driving and new mobility services. They also provide new use cases on which 5G communication would be required.

- **Automated overtake** Fully-automated vehicles will need to perform overtake maneuver on two-way roads. Such maneuver may be dangerous as a quickly approaching oncoming vehicle may be out-of-range of vehicle sensors. Vehicles thus need to cooperate to allow a safe overtake without a risk of collision.
- **High density platooning** is the creation of closely spaced multiple-vehicle chains on highway. Vehicles in the same platoon will exchange information in real-time to maintain a distance between them down to 1 meter. Vehicles thus need to constantly exchange kinematic state information to allow speeding up and braking while keeping the distance constant.
- **See through sensoring** is the exchange of video information between a vehicle and the one behind it. For instance a vehicle behind a truck receives a video stream coming from the camera at the front of the truck. This will give the driver an extended vision of the environment thus allowing safer decision making (e.g. when the vehicle decides to overtake the truck). Such use case thus requires a high reliability, availability and data rate as well as a low latency.
- **High definition map download (HDMap)** In fully-autonomous driving the use of usual 2D digital roadmaps is not sufficient. Indeed, autonomous vehicle require precise information about their complex environment. HDMap are new generation of maps that could be used for this purpose. Such map have high precision at centimeter level accuracy but require high data rate to be downloaded by vehicles.

D. European projects

Over the last decade many european projects have been conducted (SEVECOM, COMeSafety, EVITA, Drive C2X, PRESERVE, SCOOP@F, ...). These projects contribute to the C-ITS by proposing and studying various use cases. Some of these use cases are already integrated in the European standard whereas others not. Some of the latters are described below.

- **Traffic data collection** This use case has been introduced by SCOOP@F project. The vehicle sends information about position, speed, and direction to a plateform in order to better identify congested zones and react accordingly.
- **Accident zone warning** A driver detects that another vehicle (or himself) has been in an accident and signals it to the operator via his HMI. The operator broadcasts the information to road users, that could be in the relevance area of the road, in ordre to alert them of a potential danger.

E. Literature

In [5], the authors present two classes of applications: *Day one* and *Day two and beyond* applications. The formers are driver support functions that intend to increase information horizon of the driver. On the contrary the latters focus on more advanced applications designed for automated driving. The level of autonomy a use case provides is an interesting criteria that could be used for use cases classification. Thus we consider such criteria in our work.

The work presented in [6] is close to our work. The authors study ETSI use cases and provide their security and technical requirements (type of messages used, type of communication, etc.). We go a step further by extending the list of use cases by considering not only ETSI use cases. We also propose a classification methodology and we base our classification on similar security and technical requirements criterias.

III. New proposed use cases

As presented in section II, the current literature is full of C-ITS use cases that focus on road safety, traffic efficiency and driver experience for either connected and/or fully-automated vehicle. However, the security and privacy aspects of C-ITS communication is much less considered. Security and privacy mechanisms indeed have specific operational requirements. That is why use cases that are oriented to security and privacy needs also have to be defined and considered. This is the purpose of this section. After describing how security and privacy work in C-ITS networks, we propose and describe new use cases that are of paramount importance to ensure that security and privacy functions work properly.

A. Security and Privacy in C-ITS networks

V2X communication security is based on the use of pseudonym certificates. Each entity of the system (i.e. vehicles and roadside units) authenticates itself to a trusted thrid-party called Pulic Key Infrastructure (PKI). In return, authenticated entities get from the PKI a pool of pseudonym certificates. They then use these certificates to digitally sign their outgoing V2X messages.

As V2X messages include mobility information such as the geolocation, speed and heading of the vehicle, is it very easy for an eavesdropper to link V2X messages coming from a same vehicle (e.g. by looking at the pseudonym certificate used for signature) and thus track that vehicle. Therefore, in order to preserve drivers privacy, vehicles frequently change pseudonym in such a way that it becomes much harder to track a vehicle. As pseudonym certificates are frequently changed, vehicles need to communicate sometimes with the PKI to reload their pseudonym pool.

B. Pseudonym change

Pseudonym change is the mechanism used to preserve drivers privacy. However doing an *efficient* pseudonym change is not an easy task. Indeed if a vehicle is alone on the road and changes pseudonym, it is very easy to link the previous pseudonym with the new one, thus breaking all privacy. Moreover changing of pseudonym too frequently may disturb safety applications [7] [8] which is in direct contradiction with the main objective of C-ITS (improving road safety). Therefore finding the best pseudonym change strategy is not easy task as many parameters are involved.

C. Lack of pseudonym

It remains possible that a vehicle has no more pseudonym certificate left and no connectivity to the PKI is possible (e.g. because of the lack of network infrastructure). In such scenario two modes are possible for the vehicle.

The first one is the *fail safe* mode. The vehicle is not authorized anymore to send V2X messages as it cannot sign them. The vehicle thus should park in the best safe way by the side of the road.

The second one is the *fail operational* mode. The vehicle has one backup pseudonym certificate with a higher validity period than the usual pseudonym certificates. It uses that certificate to continue sending V2X messages until it can reach again the PKI. However during this period of time it remains vulnerable to tracking attacks.

D. Pseudonym reloading

When a vehicle is low on pseudonym certificates it should be able to communicate with the PKI to request new certificates. This use case is all about informing vehicles about their possibility to access the PKI and how to handle it. For instance not all roadside units may provide an access to the Internet. Using cellular network or Wi-Fi hotspots may also be a possibility for a vehicle to reach the PKI in the case of lack of roadside infrastructure.

E. Distribution of CTL and CRL

Certificate Trust List (CTL) and Certificate Revocation List (CRL) are lists that gives information to the vehicles and roadside units about trusted PKI entites. Basically speaking the CTL contains the list of URLs of trusted PKI entites. The CRL contains the list of PKI entities that have been revoked. Both lists thus enable vehicles and roadside units to be informed if a PKI entity has been compromised or not. This use case focus on the distribution of CTL and CRL to vehicles and roadside units.

F. Cryptografic Agility

Crypto-agility is the ability to migrate from a cryptographic algorithm to another one over the time. In the context of C-ITS the following two use cases are defined.

- **Capacity to support cryptographic algorithms** It is the capacity of the hardware to support cryptographic operations. For instance a change of the signature algorithm should still work without requiring hardware upgrade. Device should therefore implement a mechanism to communicate their capability of supporting such operations.
- **Verification of software authenticity and integrity** The equipment should not allow malicious software installation. To this end each software should be digitally signed in order to authorize installation of only truted software.

IV. Use cases classification

Due to the large number of use cases present in the literature, it is obvious that applying any process/method (e.g risk analysis) on them is a tough task. Therefore, there is a need to classify the use cases in clusters that share similar characteristics. Then the extraction of representative use cases from each cluster enables to get a subset of use cases to work with. In this section we describe our classification methodology.

A. Classification methodology

The proposed methodology is depicted in figure 1. It consists of the six following steps.

1) We make an inventory of C-ITS use cases. We end up with a list of 182 use cases.
2) We pre-filter the list by removing redundant or similar use cases. We end up with the reduced list of 65 use cases presented in table I.
3) In order to reduce even more this list, we classify use cases that share similar characteristics into clusters. To this end we first define the classification criteria. Similarly to [6] we focus on criteria related to security and technical requirements. The criteria we consider are presented in table II.
4) We then pre-analyze each use case by assigning them a corresponding value for each criteria. We end up with a 65x24 matrix (65 use cases with 24 ceriteria).
5) We apply the K-means algorithm (see section IV-B) on the matrix to classify the use cases into clusters.
6) Finally, for each cluster we select a representative use case, ending up with a final list of 10 use cases.

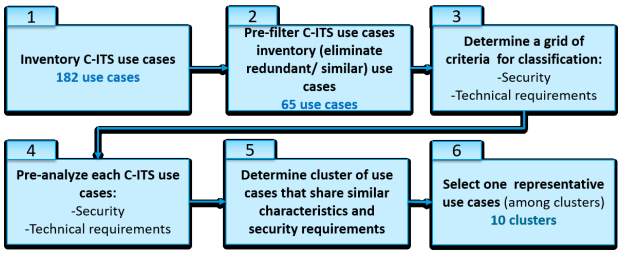

Fig. 1. Use cases classification methodology

B. K-means clustering method

K-means is a statistical method used to automatically partition a data set into K clusters [9], [10]. It proceeds by selecting K initial cluster centroid and then iteratively refine them as follows:

Source	Use case	Number
ETSI	Slow vehicle indication	10
	Emergency vehicle approaching	9
	Across traffic turn collision risk warning	36
	Merging traffic turn collision risk warning	35
	Co-operative merging assistance	37
	Intersection collision warning	54
	Co-operative forward collision warning	48
	Lane change manoeuvre	26
	Emergency electronic brake lights	7
	Wrong way driving warning	14
	Stationary vehicle	11
	Traffic condition warning	1
	Signal violation warning	4
	Roadwork warning	17
	Weather information	24
	Decentralized floating car data	16
	Vulnerable road user warning	2
	Pre-crash sensing warning	6
	Co-operative glare reduction	53
	Motorcycle approaching indication	3
	Safety function out of normal condition warning	5
	SOS service	19
	Car rental/sharing	41
	Overtaking vehicle warning	52
	Co-operative adaptative cruise control	23
	Eco cooperative adaptative cruise control	40
	Traffic light optimal speed advisory	20
	Traffic information and recommended itinerary	39
	Public transport information	30
	In-vehicle signage	28
	Electronic toll collect	49
	Point of interest notification	34
	Stolen vehicle alert	46
	Fleet management	50
	Highway automation system	22
	Regulatory/contextual speed limits notification	27
	Map download and update	42
	Data provisioning	43
	Cooperative perception	62
	Longitudinal collision risk warning	51
	Service advertising	32
	Vehicle and RSU data calibration	44
US	OBE pseudonym certificate provisioning	47
	OBE pseudonym identification certificate provisioning	47
	RSE application certificate provisioning	47
	Misbehavior reporting	55
Cellular	Automated overtake	58
	High density platooning	64
	See through sensoring	57
	HDMap	65
EU projects	Accident zone warning	13
	Human presence on the road	18
	Negation of stationary vehicle DENM	12
	Human problem	25
	In-vehicle variable-message sign	29
	Cooperative positioning improvement	33
	Remote diagnostic and just in time repair notification	45
	Traffic data collection	31
	Consumption/Emission data collection	38
	Collection of event data (by human driver)	8
	Collection of event data (by system)	21
	Adverse weather condition	15
Proposed use cases	Lack of pseudonyms	63
	Cryptoagility and software update	56
	Pseudonym reloading	59
	Distribution of certificate revocation/ trust lists	60
	Pseudonym change	61

TABLE I
LIST OF 65 CONSIDERED USE CASES

Security/Technical requirements	Description *Possible values*
Authentication / Authorization	Verification of the identity of a user or device. *0:Irrelevant 1:Important 2:Very Important*
Confidentiality	Data access and disclosure for authorized users/devices only and privacy protection. *0:Irrelevant 1:Important 2:Very Important*
Integrity	Ensuring that data have not been altered in an unauthorized manner. *0:Irrelevant 1:Important 2:Very Important*
Traceability/ Auditability	Capability of keeping track of a given set or type of information to a given degree. *0:Irrelevant 1:Important 2:Very Important*
Availability	Ensuring timely and reliable access to data. *0:Irrelevant 1:Important 2:Very Important*
Anonymity/privacy	Use of a resource or service without disclosing the user's identity. *0:Irrelevant 1:Important 2:Very Important*
Plausibility	Evaluation of data included in a message. Are they correct and realistic? *0:Irrelevant 1:Important 2:Very Important*
Juridictional Access	Ability to a legal authority to access to the system data in case of dispute. *0:Irrelevant 1:Important 2:Very Important*
Type of use case	*0:Road Safety 1:Traffic Efficiency 2:Other*
Driver's involvement	*0:Irrelevant 1:Awarness 2:Attention 3:Reaction 4:No involvement*
V2V communication	*0:No 1:Yes*
V2I communication	*0:No 1:Yes*
I2V communication	*0:No 1:Yes*
V2D communication	*0:No 1:Yes*
D2V communication	*0:No 1:Yes*
Simplex VS duplex	Session-oriented communication. *0:No 1:Yes*
Use of cellular network	*0:Primary link 1:Secondary link 2:Optional*
Type of routing	*0:Broadcast 1:Multicast 2:Unicast*
Use of LDM	*0:No 1:Yes*
Communication range	*0:Multi-hop 1:Single-hop*
Latency	*0:Highly critical (<300ms) 1:Citical (<5s) 2:Not critical (≥5s)*
Frequency of information sending	*0:High 1:Medium 2:Low*
Volume of exchanged data	*0:High 1:Medium 2:Low*
Quality of information	*0:Not critical 1:Critical 2:Very critical*

TABLE II
CLASSIFICATION CRITERIA

1) Place K points into the space represented by the objects that are being clustered. These points represent initial group centroids.
2) Assign each object to the group that has the closest centroid.
3) When all objects are assigned, recalculate the positions of the K centroids.
4) Repeat steps 2 and 3 until the centroids no longer move. This generates a separation of the objects into groups from which the metric to be minimized can be calculated.

V. RESULTS AND ANALYSIS

A. K-means results

In order to run the K-means algorithm on our list of use cases we first have to set the value of K. We start with an arbitrary value of 6 and run the algorithm. We then evaluate

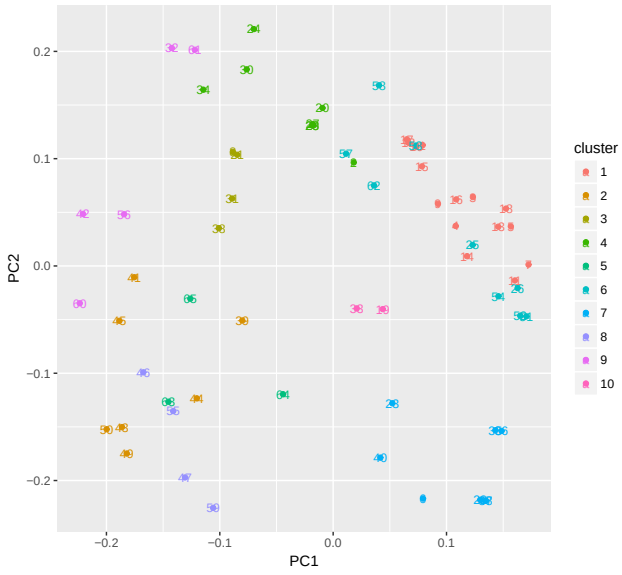

Fig. 2. Clusters after applying PCA

Cluster	Use cases	Main criteria
1	1, 3, 4, 5, 7, 9, 10, 11, 12, 13, 14, **15**, 16, 17, 18	Road safety
2	**39**, 41, 43, 44, 45, 49, 50	Unicast services
3	8, 21, **31**, 38	V2I communication
4	2, **20**, 24, 27, 28, 29, 30, 34	Traffic efficiency
5	**64**, 65	Infotainment services
6	25, 26, 51, 52, 53, 54, **57**, 58, 62	Low latency
7	6, **22**, 23, 35, 36, 37, 40, 48	Warning
8	46, 47, 55, **59**, 63	Autonomous driving
9	32, 42, **56**, 60	I2V communication
10	19, **33**, 61	Miscellanous

TABLE III
USE CASES CLASSIFICATION RESULTS

the obtained 6 clusters by checking if use cases regrouped in a same cluster actually share a majority of similar criteria. If not, we re-run the algorithm by increasing by 1 the K value. Finally, we get a satisfying result for the K value of 10.

The obtained result of the K-means algorithm is a vector of 24 dimensions (the number of criteria). As it is not possible to visualize a graph with 24 dimensions, we use the Principal Component Analysis (PCA) method to reduce the dimensions to two.

PCA is a statistical procedure that is used to extract the essential part of the data in order to minimize the dimensionality of the data. Each point with n dimensions ($n > 2$) has three or more multiple principal component (PC). In general, PC1 and PC2 represents 80% of the data.

Figure 2 depicts the two-dimensions final clusterization results with $K = 10$. Each point on the graph is a use case (represented by its value from table I) and the color shows the cluster to which it belongs.

B. Representative use cases selection

After applying the K-means algorithm, we made a little adjustment on the resulting classification by moving one use case from one cluster to another one that fits it better. The final result of the classification is presented in table III. The last column shows the main criteria that is shared by all use cases in a cluster. Bold and underligned use cases are the representative use cases we selected in each cluster. They make the final list of 10 use cases.

VI. Conclusion and Future Work

In this paper our first contribution is the inventory of existing C-ITS use cases. We then extend this list by proposing new use cases that are mostly related to security and privacy aspects.

In a second phase we propose a classification methodology that aims at extracting from the original list of use cases a subset of relevant use cases. To this end, we define security and technical criteria and apply the K-means algorithm. The obtained result is a classification of the use cases in 10 clusters. Use cases in a same cluster share similar criteria. We then select one representative use case for each clusters, ending up with a final list of 10 use cases.

The next step of this work mainly consists of doing the risk analysis on these 10 use cases.

Acknowledgments

This research work has been carried out in the framework of the Technological Research Institute SystemX, and therefore granted with public funds within the scope of the French Program *Investissements d'avenir*.

References

[1] ETSI , "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions," June 2009.
[2] William Whyte, Andre Weimerskirch t, Virendra Kumar, Thorsten Hehn+ , "A Security Credential Management System for V2V Communications," in *IEEE Vehicular Networking Conference*, Decembre 2013.
[3] Guillermo Pocovi, Mads Lauridsen, Beatriz Soret, Klaus I. Pedersen, Preben Mogensen, "Automation for On-road Vehicles: Use Cases and Requirements for Radio Design," in *Vehicular Technology Conference (VTC Fall)*, 2015.
[4] , "5G Automotive Vision," in *5GPP white paper*, October 2015.
[5] Katrin Sjoberg, Peter andres, teodor Buburuzan, and achim Brakemeier, "Cooperative Intelligent transport systems in europe Current Deployment Status and Outlook," in *Vehicular Technology Magazine*, June 2017.
[6] Rim MOALLA, Brigitte LONC, Houda LABIOD, Noemie SIMONI, "How to Secure ITS Applications? ," in *Ad Hoc Networking Workshop (Med-Hoc-Net)*, June 2012.
[7] Stephanie Lefevre, Jonathan Petit, Ruzena Bajcsy, Christian Laugier and Frank Kargl, "Impact of V2X privacy strategies on Intersection Collision Avoidance systems," in *IEEE Vehicular Networking Conference (VNC)*, 2013.
[8] Ines Ben Jemaa, Arnaud Kaiser and Brigitte Lonc, "Study of the Impact of Pseudonym Change Mechanisms on Vehicular Safety," in *IEEE Vehicular Networking Conference (VNC)*, 2017.
[9] Kiri Wagsta, Claire Cardie, Seth Rogers, and Stefan Schroedl, "Constrained K-means Clustering with Background Knowledge," in *International Conference on Machine Learning*.
[10] K. A. Abdul Nazeer, M. P. Sebastian , "Imroving the Accurancy and Efficiency of the K-means Clustering Algorithm," in *World Congress on Engineering*, 2009.