# Augmented Perception by V2X Cooperation (PAC-V2X): Security issues and misbehavior detection solutions

Shagdar † Oyunchimeg, Pierre Merdrignac, Mohamed Hadded

# Augmented Perception by V2X Cooperation (PAC-V2X): Security issues and misbehavior detection solutions

Mohamed Hadded, Oyunchimeg Shagdar and Pierre Merdrignac
Institut VEDECOM, 23 bis Allée des Marronniers, 78000 Versailles, France
{mohamed.elhadad, oyunchimeg.shagdar, pierre.merdrignac}@vedecom.fr

***Abstract*— Cooperative Intelligent Transport System (C-ITS) also known as connected vehicle technology uses wireless technologies to enable real-time communication between vehicles moving along roads, traffic signals, infrastructure and other mobile devices. In order to boost the role of C-ITS in the domain of autonomous driving and smart mobility, the FUI French project PAC V2X (Perception Augmented by V2X Cooperation) proposes to enhance the vehicles perception in safety critical zones via a cooperation between the roadside infrastructure and the vehicles by relying on V2X communication and sensors. Several applications are considered in this project which require fundamentally new solutions for security, that differ from traditional security mechanisms such as PKI, signatures, encryption, etc. Indeed, a certified vehicle in PAC V2X can easily send false location information, alert incorrect event or report a bogus object. Therefore, new and innovative security approaches are needed to detect and report malicious activities, identify the misbehaving vehicles as well as react either by dropping the incorrect information or excluding the misbehaving vehicles from the network. In this paper, we target the PAC V2X use cases, we present attacker models and potential misbehavior detection mechanisms and a classification of these mechanisms.**

***Index Terms*— PAC V2X, C-ITS, vehicular networks, security attacks, misbehavior, detection solution.**

## I. Introduction

C-ITS rely on Vehicular Ad hoc NETwork (VANET) architecture where road network and vehicles are equipped with communication devices serve to exchange information about current vehicles position, speed and the state of roads. As cooperative and connected vehicles are equipped with new communication interfaces and embedded electronics, they can be threatened by the unwanted malicious attacks [1]. These C-ITS communication devices not only suffer from classical IT attacks such as Spoofing, Denial of Services (DoS) and Black hole attacks, but they also suffer from new security threats. For example, a malicious vehicle can broadcast falsified information with wrong identification to get the attention of its neighboring vehicles and act as police or an emergency vehicle. In addition, connected vehicle broadcasts periodically its geographic position to its neighboring [2]. Therefore, position information can be used by an attacker to track the driver.

Basic IT security mechanisms such as PKI, signatures, encryption, are not sufficient to ensure security [3]. Indeed, a certified vehicle can easily send false location information, alert incorrect event, modify/delay/drop packets (forwarding attack) [4]. Note that the vehicle can send false information to act as misbehaving vehicle for malicious or selfish reasons or due to faulty hardware [6]. As a result, new security approaches that can detect and report malicious activities are necessary to keep overall C-ITS communications functionality. A local misbehavior detection mechanism is able to detect data inconsistency and implausibility (i.e. false position, speed, heading) by applying consistency and plausibility check techniques. However, this detection suffers from pseudonym changes of attackers. Hence, locally misbehavior reports created by vehicles should be transmitted to a central entity for evaluation. This permits to identify the misbehaving vehicles with higher probability, and react either by filtering out the incorrect information or excluding the misbehaving vehicles from the network.

The French FUI PAC V2X project (Perception Augmented by V2X cooperation) [5] propose to augment the vehicles perception of their environment via a cooperation between the infrastructure and the vehicles themselves. In such context, the vehicles will fuse collected data by means of their own sensors and with data received by I2V (Infrastructure to Vehicle) and V2V (Vehicle to Vehicle) local telecommunication. Road Side Unit will use also sensors (cameras, radars) to build their own perception which will be then shared with equipped vehicles. Different levels of misbehaviour detection are made in PAC V2X particularly at the data fusion level and at the application level. The misbehaviour detection at the data fusion level detects misbehaviour from the raw data so that mitigating to write a wrong data in the Local Dynamic Map (LDM) [8], where misbehaviour detection at the application level tracks LDM histories and provides a high level analysis to recognize patterns that are corresponding to abnormal situations. This work investigates cyber-security related aspect in the context of PAC V2X. In this paper, we present the PAC V2X project and its related applications and we identify and describe the attacker models that can threaten the PAC V2X applications and then we give an overview regrading misbehavior detection mechanisms and we present a classification of these mechanisms based on [7].

The remaining part of this paper is organized as follows. In section 2, we highlight the PAC V2X project and its use cases. In Section 3, we present the attacker motives and PAC V2X security attacks. Section 4 introduces the state of the art regarding misbehavior detection mechanisms. Section 5 gives an overview on bogus object detection framework based on movement analysis, and which also uses further information

978-1-5386-7747-6/19/$31.00 ©2019 IEEE

sources in order to filter out bogus object alerts transmitted by misbehave vehicles and thus improve the misbehavior detection accuracy. Finally, conclusion is given in Section 6.

## II. PAC V2X PROJECT AND APPLICATIONS

### A. Project overview

The project PAC V2X (Augmented Perception by V2X Cooperation) aims to enhance the perception of cooperative vehicles and potentially automated vehicles of their environment especially in safety critical areas (i.e. intersections, roadwork, tolling gate, etc). Such an increased perception is achieved through V2X cooperation between vehicles themselves and roadside units. Road Side Unit uses also sensors (i.e. cameras, radars) to build their own perception which will be shared with equipped vehicles by broadcasting standard messages. The PAC V2X system is composed of various types of vehicles including PAC V2X vehicles equipped with both communication devices which serve as the data I/O interface with the network (ITS G5) and local perception sensors which allow them to detect road marks and objects, PAC V2X vehicles with only the communication capability, and non-equipped vehicles.

PAC V2X has a high number of uses cases and applications such as lane merging assist, intersection crossing assist, lane change assist, which require fundamentally new mechanisms for security, that differ from existing IT security requirements. Classical IT security mechanisms such as PKI, signatures, encryption, are not sufficient to ensure security. Indeed, as a PAC V2X vehicle communicate with external networks, it can be threatened by the unwanted malicious attacks such as bogus location information, false alert, location tracking, etc.

### B. PAC V2X exchanged messages

The PAC V2X RSU and vehicles can send several types of messages on the road, here we mainly deal with three types of messages, namely Cooperative Awareness Messages (CAMs), Decentralized Environmental Notification Message (DENM), and Collective Perception Message (CPM). The CAMs are distributed within the ITS-G5 (802.11p) network and provide information about vehicles presence, position, speed [9]. The DENM messages are triggered by the C-ITS vehicles and RSUs to provide information about a specific traffic or driving event such as an emergency braking or an accident [10].

The PAC V2X applications use new message that is currently under standardization, namely Collective Perception Message (CPM) which is used to provide description about objects (i.e. other road participants, obstacles, etc) detected by the sensors embedded in the PAC V2X stations (vehicles and RSU). CPM is composed of one common ITS PDU header and multiple containers [11]. Moreover, the PAC V2X RSU periodically broadcasts SPaT/MAP messages to announce the traffic light phase, timing, and the intersection layout. Many other messages are used in PAC V2X that are not yet standardized such as Tolling Announcement Message (TAM) which is used by the RSU to announce information about tolling gates (i.e identification, state (closed, free) and their particularities (means of payment, reserved only for trucks, the speed profile, etc.) and the actual and expected waiting time, as well as Manoeuvre Coordination Message (MCM) message which contains a vehicle trajectory guidance, a list of geographical points and corresponding velocity.

### C. PAC V2X applications

The exchange of data via V2X communication such as the position, speed, heading or special incidents like an accident or emergency braking, enables a set of safety and traffic management services. In this section, we present some use cases of PAC V2X project.

*1) Traffic scheduling assist service (ICA-S):* The traffic scheduling assist aims at providing intersection crossing priority to the vehicles with special roles including public transportation and emergency vehicles. While the emergency vehicles, such as fire vehicles, ambulance, and police result in signal preemption (signal interruption), the public transportation results in signal priority. The traffic scheduling assist application will be developed with a strong interest on signal priority control.

*2) Motorway access assist service (LMA-M):* The motorway access assist service provides the vehicle (automated) or the driver (HMI) with the optimal speed and path to adopt to enter the motorway smoothly. Moreover, if vehicles are driving on the motorway, they are also provided with the speed which makes easier the vehicle merging from the access lane.

*3) Active roadwork warning service (LMA-R):* In the active roadwork warning applications, the RSU and vehicles are cooperating to avoid a collision with workers / equipment and assist the insertion of a vehicle (automated or human driven) at roadworks area to merge on one of open lanes.

*4) Motorway tolling assist service (LCA-T):* In the motorway tolling assist application of PAC V2X project, the RSU provides information on the tolling station as well as suggests the appropriate tolling gate to pass by taking into account the status of each tolling gate (open/close), speed limit, payment method and the vehicle type.

*5) Wrong way driving warning (WWDW):* The aim of this service is to detect the vehicles circulating in wrong direction (wrong way driving) on a motorway or expressway exit ramp. Upon a detection of a wrong way driving vehicle, a security alert is provided to the driver or the automated vehicle moving on the wrong way. Moreover, the RSU provides alerts to other vehicles for immediate crash avoidance actions.

*6) Traffic Light Violation Warning (ICA-W):* This PAC V2X application alert consists of a signal violation detection at road junction and alerting signal violation. This application involves both the PAC V2X RSU and OBU. Upon detection of the signal violation by the RSU which covers the intersection area, it sends notification of this violation to the surroundings OBU. Each OBU assesses the threat for itself and alerts the driver or automated vehicle as appropriate.

## III. PAC V2X ATTACKERS

In this section, we discuss the attacker motives and the main attacker models that can threaten the PAC V2X applications.

### A. PAC V2X Attacker motives

Various types of attacks can be launched by the vehicles in the network depending on their intention. The PAC V2X attacker motives can be generally classified into three main classes based on [12], [13]: faulty (damaged), selfish and malicious motives.

*1) Selfish attacker:* A selfish attacker exploits all information transmitted and their types that can contribute to an attack with a specific goal [15]. The selfish vehicle does not have malicious intentions of causing accidents or decreasing the network performance, but to gain advantage on the road. For example, a selfish vehicle might simulate fake traffic jams on the road and send false report on congestion to obtain an open road and thus reaching its destination faster.

*2) Faulty vehicle:* Faulty Vehicles can start malfunctioning due to some internal failures (sensors, GNSS, CAN, etc) and give out false location (loss of GPS signal), false alerts and speed. This malfunctioning can happen due to software bugs that cause bogus readings or messages to be generated. As example, consider a vehicle that transmits a CAM message reports its current speed is 0 m/s on a highway, while its speed in its previous CAM message was 60 m/s, then this vehicle may be considered as a faulty vehicle. The question that arises is whether the vehicle misbehave with its second message, or sudden failure in GPS device? Therefore, the misbehavior detection mechanism should be able to identify the causes of abnormal behaviors. From our point of view, we assume that a damaged vehicle will be penalized in a similar way as a misbehaving vehicle. Therefore, it is up to the vehicle owner to maintain and ensure that all vehicles devices at good conditions.

*3) Malicious vehicle:* Malicious vehicle, and in particular the disruptive attacker is the most dangerous type of attack that can have dangerous impact on drivers, passengers and vehicles. In contrast to selfish attacker, the malicious attacker does not necessarily gain on advantage on the road. The goal of a malicious vehicle is to disrupt the PAC V2X applications. The threats can be varied from complex Denial of Service (DoS) to simple signal jamming and attempts to disrupt an assist service. The malicious attack may be directed against the network (denial of service, channel congestion, etc), or against applications and their users.

### B. PAC V2X attacker models

The PAC V2X applications assume that data such as CAM, DENM and CPM messages will be exchanged and disseminated by vehicles in communication. This feature makes PAC V2X applications vulnerable to attack such as bogus information attacks. In fact, a certificated PAC V2X vehicle could generate false information on its own and broadcasts it to the network. Mostly, the vehicles misbehave not to create threats that can involve dangerous consequences on passengers' lives, but rather for selfish reasons e.g. reaching their destinations faster or for gaining access to a particular lane.

*1) Jamming attack:* Denial of service, especially jamming is one of the serious threats in vehicular networks. The aim is to prevent the legitimate vehicles to access the network services by increasing the signal to noise ratio (SNR). For example, in motorway tolling assist service, the attackers may broadcast frequently dummy messages to flood the transmission channel and thus prevent the PAC V2X RSU to provide tolling assistance service to the vehicles or to prevent the Dispatcher to communicate with the PAC V2X RSU. Jamming attack can be either constant or reactive [13]. Constant jamming continuously sends radio signals that not follow any rule of the WAVE communication stack to make the channel always busy. In reactive way, the jammer transmits signals upon detecting a radio activity on the communication channel.

*2) False location information:* The attacker tries to affect the network performance by disseminating false and wrong position information to other vehicles. In fact, the attacker can create and broadcast valid digital signature CAM messages but with false position information. Consequently, a ghost vehicle can be created that does not exist in the reality. Figure 1 shows an example of location-based attacks in the case of motorway tolling assist application, where the PAC V2X RSUs are used to determine the appropriate tolling gate for each vehicle in the tolling area. The vehicle C tries to get the attention of the RSU in order to be served faster (before the vehicle A, B and D) by creating a ghost vehicle C1 in the tolling area.

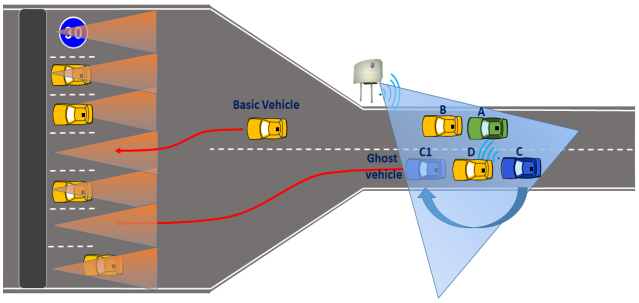


Fig. 1. Location based attack in motorway tolling assist application

*3) Bogus object attack:* The PAC V2X RSUs and the vehicles can broadcast CPMs (Collective Perception messages) when road objects are detected by their sensors, Lidar or cameras. Therefore, an attacker can disseminate a false CPM message informing the detection of a bogus object in order to force other vehicles to take incorrect decisions or to gain access to a particular tolling lane. As shown in Figure 2, a selfish vehicle A will try to get the tolling gate reserved by the PAC V2X RSU to vehicle B by broadcasting a false CPM message to signal the detection of a bogus object in front of the vehicle B. Upon reception of the CPM message, the vehicle B will turn right and realize the tolling gate.

*4) False alert information:* The alert messages are important to send safety information in order to prevent other vehicles about an abnormal traffic conditions such as an accident, traffic signal violation, emergency braking, traffic

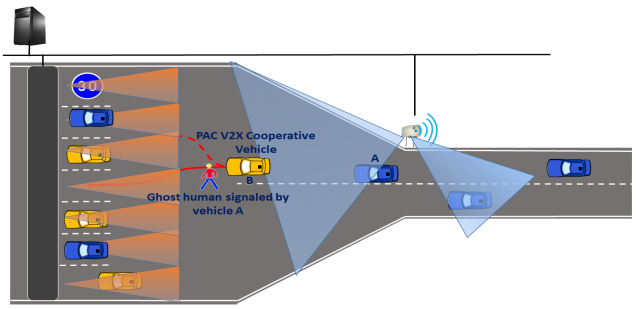


Fig. 2. Ghost human detected by vehicle A in front of the vehicle B

congestion, etc. The Decentralized Environmental Notification Message (DENM) is a facilities layer message that is mainly used by ITS applications in order to alert road users of a detected event using ITS communication technologies [10]. Thus, an attacker could report a false emergency situation by broadcasting a fake DENM message intentionally for selfish reasons (e.g. better driving conditions, getting easier and faster access to the road, etc.). For example, as shown in Figure 3 a misbehave vehicle might send DENM message to alert traffic signal violation to the neighboring vehicles, even when there is no such event on the road. In this case, the misbehave vehicle wants to convince the vehicle B that a traffic signal violation event has occurred in order to clear the junction and turning right faster.

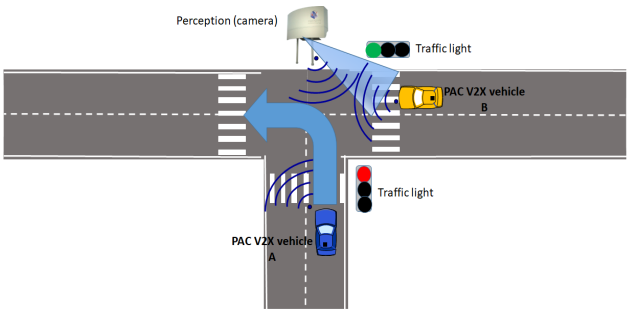


Fig. 3. Vehicle A broadcasts a false traffic alert violation message (DENM) to gain access to the junction

*5) Messages forwarding attack:* Securing alert messages forwarding and broadcasting is a critical issue in. An attacker can be seen as an entity who wants to change, drop and delay the received alert messages unnecessarily for some amount of time before forwarding. This attack type is called black whole attack.

*6) Location tracking:* The attacker can locate and track vehicle movement through the CAM message which it broadcasts periodically. By tracking a vehicle, it becomes possible to build vehicles profile; in this way, the privacy of the driver of vehicle is breached. In addition, the attacker can record and use the information about vehicles without owner's consent. Table I show some attacks that can threat the applications of PAC V2X and their damage rating.

TABLE I

*PAC V2X attacks and their motivations*

| Attack | Messages | Layer | Motivation |
|---|---|---|---|
| Jamming | Signal jammer | Physical | Malicious |
| False location | CAM/CPM | Facility | Faulty, Selfish |
| Bogus object | CAM/CPM | Facility | Selfish |
| False alert | DENM | Facility | Selfish |
| Black whole | DENM | Routing | Malicious |
| Tracking | CAM | Application | Malicious |

### C. Impact of different attacks on PAC V2X use cases

This section covers the damage of attacks against PAC V2X use cases. In fact, a successful attack can cause major damage on PAC V2X applications, and potentially has disastrous impact on the vehicles and passengers safety. The impact of different attacks on PAC V2X uses cases can be centered on three main risk levels (Low, Medium, High). As shown in Table II, the damage rating for each attack can be evaluated by asking the following questions: How easy is it to produce the attack ? How great is the impact of the attack ? and How easy is it to detect the attack ? The Table III shows the damage rate of each attack on the PAC V2X applications obtained based the second question. For instance, the impact of the jamming attack on LMA-R use case is considered high because this attack causes permanent or temporary suspension of DENM message reception by the vehicles moving at high speed on highway which can lead to dangerous consequences for the drivers and the vehicles.

TABLE II

*Damage rate levels*

| Question | High | Medium | Low |
|---|---|---|---|
| Attack producibility | The attack can be easily produced and at every time | The attack can be produced but with some limitations | The attack is not easy to be produced |
| Attack impact | The attacker infects the system and can lead to catastrophic damage (i.e. an accident) | The attacker infect the system and can lead to moderate damage (i.e. traffic jam) | The attack have no impact on the system but can inflict minor harm to the road users. |
| Attack detectability | Broadcasted information readily explains the misbehavior | Attack is not common and it produces only in certain applications | Extremely difficult to detect attack |

## IV. Misbehavior Detection Mechanisms

Several solutions have been proposed in the literature to detect misbehavior and malicious nodes in vehicular ad hoc networks. Generally, the misbehavior detection mechanisms

TABLE III

*PAC V2X attacks and their potential damage rates*

| Attack | ICAS | LMAM | LMAR | LCAT | WWDW | ICAW |
|---|---|---|---|---|---|---|
| Jamming | Low | High | High | Medium | High | High |
| False location | Medium | High | High | Medium | High | High |
| Bogus object | Medium | Medium | Medium | Medium | Low | Low |
| False alert | Medium | Medium | High | Medium | High | High |
| Black whole | Low | Low | Medium | Low | High | Low |
| Tracking | Low | Low | Low | Low | Low | Low |

fall into one of two broad categories, namely Node-Centric and Data-Centric misbehavior detection schemes.

### A. Data-centric based MDB

The concept of data-centric misbehavior detection is based on the different data exchanged between vehicles in the network such as received messages through wireless communication, local sensors measurement or reported messages to perform data plausibility and data consistency checks control. In fact, the messages transmitted by the vehicles are observed and compared with the information reported or received by the other vehicles. When inconsistencies or implausible information is detected such fake emergency alerts or false information fake, the suspicious vehicle is observed and its trustworthiness will be locally evaluated. Most existing solutions in the context of misbehavior detection in VANETs are based on data-centric plausibility and consistency checks.

*1) Data plausibility checks:* Generally, a message-based plausibility mechanisms are based on predefined boundaries and rules [16]. These checks are using both predefined boundaries and the received messages that generally includes the position of the transmitter, its current speed and heading. The velocity values, the position as well as the heading of the sender should follow the domain of definition according to related standardization for CAM and DENM. The domain of definition should be defined for each type of vehicle such as vehicle, bus, trucks, etc.

*2) Data consistency checks:* Consistency-based misbehaviour detection is one of the most used techniques to determine the trustworthiness of vehicles which is based on relations between reported and newly received information [17] as well as the messages received from multiple vehicles. For instance, a vehicle could alert traffic jam situation while other vehicles report fluid traffic flow. A consistency-based detection mechanism would use such information to judge whether there really is a traffic jam and the alert message could be sent by a misbehave vehicle.

### B. Node-centric based MDB

In addition to the data-centric misbehavior detection, a node-based checks are used to establish the trustworthiness of vehicles by using two settings, namely behavioral and trust-based detection. In contrast to data-centric misbehavior detection mechanisms, which focus mainly on the trustworthiness of the received messages, behavioral detection analyzes the observed behaviors of a vehicle and try to derive metrics that measure how well a vehicle behaves. On the other hand, trust-based detection mechanism analyzes the past and present behavior of a vehicle to determine the expected future misbehavior. The mechanism is based on the assumption that a vehicle whose behave correctly in the past is more likely to behave correctly in the future.

## V. CPM VALIDITY CHECK FRAMEWORK

Table IV compares the different misbehavior detection categories. It is clear from this table that while all of these mechanisms can detect certain of attacks, none of them can detect bogus objects. As result, these mechanisms can not ensure network security and makes the PAC V2X applications vulnerable to bogus object attack. Thus, in this section, we propose a CPM validity check framework based on movement analysis and which also uses further information sources in order to detect false CPM messages and thus improve the misbehavior detection accuracy. To the best of our knowledge, this is the first attempt to design a misbehavior detection mechanism for bogus object detection in the context of C-ITS.

### A. CPM validity check based on movement analysis

In this section, we suppose that a vehicle $x$ receives a CPM message from the vehicle $y$ announcing the detection of a bogus object in area $Z$ in order to force it to take incorrect decisions or to gain access to a particular tolling lane. If the area $Z$ is within the PAC V2X RSU observed area, thus it will be able to detect that the vehicle $x$ is lying and it will take action against it. However, the PAC-V2X RSU might not be within the communication range of the malicious vehicle $x$ or it is outside of area $Z$ to analyze the observed misbehavior. In this case, the PAC-V2X vehicles can make a decision on the validity of the CPM message based on the number of neighboring vehicles that report the same object detection or by observing the location and the speed of the vehicle $x$ after announcing the object detection. For example, if vehicle $i$ sends a CPM message to vehicle $j$ at instant $t$ to inform it that " There is an obstacle in location $(x, y)$ " and at instant $t + k$ it is close to location $(x, y)$, then it implies two contradictory statements and the CPM message cannot be trusted.

### B. CPM validity check based on communication and sensors data

Further information sources can be considered in order to improve the misbehavior detection accuracy. Since the number of vehicles equipped with sensors (e.g. cameras, radar and lidar) is growing, the information provided by

| Mechanism | Data plausibility checks | Data consistency checks | Behavior based detection | Trust based detection |
|---|---|---|---|---|
| Jamming | ✔ | | | |
| False location (CAM) | ✔ | ✔ | ✔ | ✔ |
| Bogus object (CPM) | | | | |
| False alert | | ✔ | ✔ | ✔ |
| Black whole | | | ✔ | ✔ |
| Tracking | ✔ | | | |

TABLE IV

*Comparison of misbehavior detection mechanisms*

these devices can be additionally used to verify the validity of objects detected by adjacent vehicles. Each PAC V2X vehicle can accept or refuse a CPM message based on incoming information originating from local environment sensors devices. In fact, these devises are able to provide in real-time information about the environment. For example, two cameras installed side by side or a lidar allow a three-dimensional recognition of the environment.

Different levels of misbehaviour detection are made in PAC V2X particularly at the data fusion level and at the application level. The misbehaviour detection at the data fusion level detects misbehaviour from the raw data so that mitigating to write a wrong data in the Local Dynamic Map (LDM) [8], in particular, inconsistency between raw data and current state of the objects managed by the augmented perception. On the other hand, misbehaviour detection at the application level tracks LDM histories and provides a high level analysis to recognize patterns that are corresponding to abnormal situations. If an abnormal situation is detected, the corresponding information in the LDM will be marked indicating the detection of a misbehaviour. Specifically, as the input data, the module takes the LDM data history for each C-ITS station (positions, velocities, etc) and the environmental information including the road type, number of lanes, traffic light phase and so on.

## VI. Conclusion

Since connected vehicles are equipped with new communication interfaces, they can be threatened by the unwanted malicious attack such as false information attack, location tracking, etc. Therefore, new security approaches that can detect and report malicious activities are necessary to keep overall PAC V2X applications. Motivated by this observation, in this paper we have presented several PAC V2X attacker models, and we have discussed two main misbehavior detection categories, namely data-centric and node-centric. However, as the number of vehicles equipped with additional information sources such as cameras, radar and lidar is growing, more research should target the misbehavior detection based on communication and sensors data at augmented perception module in order to detect bogus information alerts transmitted by misbehave vehicles and thus improve the misbehavior detection accuracy.

## References


[1] J. Hong, *Cyber Security Issues in Connected Vehicle of Intelligent Transport System* Indian Journal of Science and Technology, vol. 9, no. 3, Jun. 2017.

[2] P. Skorput, H. Vojvodi, S. Manduka, *Cyber security in cooperative intelligent transportation systems*, International Symposium ELMAR, Zadar, Croatia, pp. 35-38, Sept. 2017.

[3] S. Yi and R. Kravets, *Key Management for Heterogeneous Ad Hoc Wireless Networks*, tech. report UIUCDCS-R2002-2290, Dept. Computer Science, Univ. of Illinois at Urbana-Champaign, Jul. 2002.

[4] L. Bysani and A. Turuk, *A survey on selective forwarding attack in wireless sensor networks*, in Proceedings of the International Conference on Devices and Communications (ICDeCom), Mesra, Ranchi, India, pp. 1-5, Feb. 2011.

[5] PACV2X prject,`https://project.inria.fr/pacv2x/`

[6] Z. Huang, *On reputation and data-centric misbehavior detection mechanisms for VANET*, Master's Thesis, School of Electrical Engineering & Computer Science, University of Ottawa, 2011.

[7] R. V. D. Heijden, S. Dietzel, and F. Kargl, *Misbehavior Detection in Vehicular Ad-hoc Networks*, in 1st GI/ITG KuVS Fachgesprch Inter-Vehicle Communication (FG-IVC 2013), Innsbruck, Austria, Feb. 2013.

[8] ETSI TR 102 863, *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization*, tech. report, Jul, 2011.

[9] ETSI TS 102 637-2, *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, 2011.

[10] ETSI EN 302 637, *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*, 2014.

[11] MAVEN Deliverable 5.1, *V2X communications for infrastructure-assisted automated driving*, Feb 2018.

[12] A. Studer, M. Luk and A. Perrig, *Efficient mechanisms to provide convoy member and vehicle sequence authentication in vanets*, In SecureComm, pp. 422-432, 2007.

[13] J. P. Hubaux, S. Capkun and J. Luo, *The security and privacy of smart vehicles, Security*, IEEE Security Privacy, vol. 2, no. 3, pp. 4955, May 2004.

[14] K. Grover, A. Lim, Q. Yang, *Jamming and antijamming techniques in wireless networks: a survey*, Ad Hoc Ubiquitous Computing journal, vol. 17, no. 4, pp. 197-215, 2014.

[15] G. Samara, W. A.H. Al-Salihy, R. Sures, *Security Analysis of Vehicular Ad Hoc Networks (VANET)*, 2010 Second International Conference on Network Applications, Protocols and Services, Kedah, Malaysia, Sept. 2010.

[16] ETSI TS 102 723-8, *Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer*, 2016.

[17] S. Ruj, M.A. Cavenaghi, Z. Huang, A. Nayak, I. Stojmenovic, *On data centric misbehavior detection in VANETs*, IEEE 74th Vehicular Technology Conference, VTC-Fall, San Francisco, USA, 2011.