V2I Cooperation for Traffic Management with SafeCop

Giovanni Agosta, Alessandro Barenghi,
Carlo Brandolese, William Fornaciari,
Gerardo Pelosi
DEIB – Politecnico di Milano
name.surname@polimi.it

Leonardo Napoletani, Luciano Bozzi
RoTechnology
name.surname@rotechnology.it

Carlo Tieri
Thales
carlo.tieri@thalesgroup.com

Stefano Delucchi, Massimo Massa
AITEK
nsurname@aitek.it

Enrico Ferrari
Impara s.r.l.
e.ferrari@impara-ai.com

Maurizio Mongelli
CNR-IEIIT
maurizio.mongelli@ieiit.cnr.it

Dajana Cassioli and Luigi Pomante
Università degli Studi dell'Aquila
name.surname@univaq.it

***Abstract*—The *Safe Cooperating Cyber-Physical Systems using Wireless Communication* (SafeCop) project addresses safety-related issues in cooperating cyber-physical systems. These systems, characterised by wireless communications, multiple stakeholders, and variable operating environments, are called Cooperative Open Cyber-Physical Systems (CO-CPS). CO-CPSs can successfully address several societal challenges – cooperative vehicles have been shown to reduce fuel consumption as well as the number of accidents. A vehicle-to-infrastructure (V2I) cooperation for the traffic management scenario is therefore considered as a key use cases of SafeCop. In this paper, we outline the V2I traffic management scenario, assess the research goals that arise from it, and provide an overview of the architecture of the demonstrator, as well as a roadmap for its development and evaluation.**

1. Introduction

The global Intelligent Transportation Systems (ITS) market, estimated at USD 14.59 billion in 2012, is expected to reach USD 38.68 billion by 2020. A similar trend characterizes the connected-vehicular market which is expected to grow 20% annually in the next years, reaching $46 billion by 2017. In the same year approximately 56 million cars are expected to be equipped with telematics functionality.

Cooperative-Intelligent Transportation Systems (C-ITS) [20] can be very useful when situations such as construction site warnings and traffic congestion in highways caused by an accident or road damage are encountered. According to the U.S. Department of Transportation, up to 80% of automobile accidents can be prevented with improved vehicle connectivity, using Vehicle-to-Anything (*V2X*) communications [22], which are on the verge of commercial deployment. In September 2014 Delphi Automotive PLC announced that it was the first-to-market with Vehicle-to-Vehicle (V2V) and V2I communication technology [1]. Additionally, it is projected that over 10% of time spent driving is wasted in traffic jam, 12% of urban traffic is created by vehicles looking for a parking slot, and up to 17% of urban fuel is wasted at traffic lights when there is no cross-traffic. With vehicles connected together and with roadside infrastructure, all of these problems can be mitigated. It is worth noting that C-ITS require more stringent safety requirements and standardization procedures to enable the cooperation among systems developed by different producers.

Nevertheless, the diffusion of V2X communications and driver assistance platforms can be negatively impacted by security and safety concerns. This consideration arises from a 2014 UMTRI poll [23]: *Some 30% of those questioned said they are 'very concerned' about security breaches from hackers, and about data privacy in tracking speed and location. Another 37% are 'moderately concerned'. In addition, most expressed concern about system failure and performance, and about drivers relying too much on the technology or being distracted by it.* Moreover, it is important to highlight that people percepts the usefulness of V2X and driver assistance services. According to the same poll "*...75% of respondents believe that connected vehicles will reduce the number and severity of crashes, improve emergency response times and result in better fuel economy*". Thus, it clear that the acceptance of V2X technology

This work is supported in part by the European Commission under the H2020 ECSEL program, grant 692529-2 SafeCOP.

[1] http://www.businesswire.com/multimedia/home/20140905005829/en/

is not limited by its perceived value, but by the potential security and safety issues.

Safety assurances for vehicles relying on V2X communications require reliable cooperation among the components of the whole system, as the reliability of the whole system allows both to prevent accidents and to detect malfunctioning subsystems. The problem is twofold: on one hand it is necessary to develop innovative and efficient solutions to increase the security and safetey of these systems; on the other hand it is necessary to standardize the security assurance procedures, and to use prototypes and demonstrator to reassure people about security concerns and foster their wide utilization. A key point is that a fast widespread adoption of V2X technology is crucial for it to provide significant benefits. Indeed, in a context where V2X-equipped vehicles are the norm, any vehicle on the road not V2X-equipped has the potential to increase the risk of accidents, and therefore to decrease the overall impact of V2X technology.

Moreover, V2X technology acts as a support tool for autonomous vehicles, which are under development and foreseen to reach maturity in the next decade. Google, Nissan, and other companies expect that by 2020 cars on the market will be completely driverless in many situations. These cars will employ sensors to detect other vehicles, pedestrians, and objects around them, but this information can be integrated with additional data coming from roadside monitoring systems, using V2I communication, improving the quality and speed of the detection, as well as providing information that cannot be detected by sensors at all (e.g., the timing of traffic lights ahead).

For more efficient drive assistances and future autonomous vehicles a large amount of information needs to be communicated from roadside monitoring units to the vehicles in transit. At the same time, an efficient monitoring roadside system needs to acquire information from the vehicles in transit. Such information can be obtained in many ways, including Adaptive Traffic Light System (A-TLS) Cooperative Awareness Message (CAM), Green Light Optimal Speed (GLOSA) Cameras, radar, lidar (light detection and ranging) and laser technologies. There are already proposals for combining CAM with automated traffic lights [14].

1.1. Contributions

We propose an holistic approach to integrate the advantages offered by technologies such as CAM, GLOSA and A-TLS, in a Traffic Management Application to enhance road safety via functions such as *traffic condition warning* (rapid traffic evolution), *stationary vehicle warning* (disabled vehicles), and *wrong way driving warning*. To this end, the SafeCop project grounds on a real industrial use case scenario and develops a demonstrator that allows to experiment with different technological solutions.

Specific industrial and research challenges in the above framework deal with the need for a robust approach using *sensor fusion* to ensure reliability for drive assistance (and, in the future, for autonomous vehicles) Sensor fusion allows to rely on multiple, heterogeneous data sources to extract relevant knowledge to take decisions. In the SafeCop Traffic Management scenario, sources are the results of locally-performed analyses on individual sensors, including Video Content Analysis (VCA) on roadside camera feeds, as well as navigation and driver behaviour data from in-vehicle sensors. Machine learning is crucial for performance discovery of autonomous vehicles and driver assistance systems due to the large amount of data and its heterogeneity. The application of machine learning theory to the field of C-ITS represents an innovative contribution.

Moreover, SafeCop will need to guarantee security of communication. While confidentiality of the individual communication link can be guaranteed via encryption, the authenticity and trustworthiness of the endpoints needs to be established [22]. Whether the communication and computation constraints imposed by the scenario are compatible with traditional authentication techniques is a challenge that SafeCop will need to address. Moreover, the Road Side Units (RSU) are, by their very nature, exposed to physical threats. Even On Board Units can be tampered with by maintainance operators, or when parked. The implementations of encryption algorithms must therefore be robust against applied cryptanalysis techniques. In SafeCop, we will investigate the engineering trade-offs between security security level and performance of the cryptographic subsystem included in the RSU and OBU platforms.

2. Industrial Use Case Scenario

Intelligent Transportation Systems (ITS) optimize the efficiency and improve the safety of transportations, exploiting the possibilities offered by the state-of-the-art of Information and Communication Technology (ICT).

- *Active road safety* ITS applications class decreases the probability of traffic accidents by providing assistance to drivers (e.g. in order to avoid collisions with other vehicles).
- *Efficiency and management* ITS applications class optimizes the traffic flow, by coordinating the vehicles kinematics— speed and route—with respect to the traffic flow.[2]

Both classes need a solid (in terms of reliability and response time) communication channel connecting all transportation actors, the vehicles and the infrastructure: wireless vehicular networks are the most important components of ITS enabling technologies. Vehicle to Infrastructure (V2I) communications are part of this use case.

Another part of the use case is the Adaptive Traffic Light System (A-TLS), which is an efficiency and management application. A-TLS changes the traffic lights signaling plan (the duration of red, yellow and green phases) at least according the time and the day. A better A-TLS optimizes the signaling plan according to the changing traffic conditions, usually by extending the green phase when vehicles are closely spaced. Currently, the time interval between two

[2] There is a third class of miscellaneous applications (e.g. infotainment), which are not considered here.

consecutive passing vehicles is measured, by inductive loops sensors.[3]

Whilst A-TLS adapts the signaling plan to traffic conditions, another applications considered by the use case, the Green Light Optimal Speed Advisory (GLOSA), tries to adapt the traffic flow to the signaling plan. GLOSA computes the optimal vehicles speeds that minimizes the average (of all vehicles) travel cost (e.g. stop time at traffic lights and total travel time), for a given traffic lights signaling plan. Then GLOSA informs vehicles drivers about the optimal speed they should maintain, using some communications mean that, currently, consists of auxiliary roadside signs.

Figure 1 shows the use case block diagram.

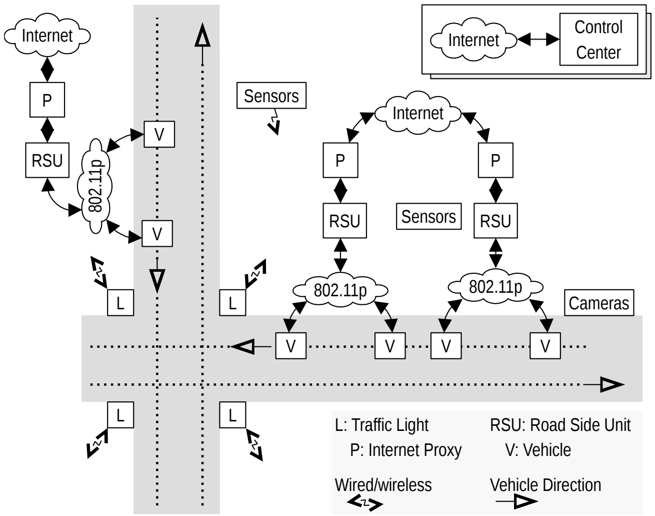


Figure 1. Use Case Block Diagram

It is worth noting that, other than to improve driver comfort, efficiency and management ITS applications bring environmental benefits, because a smooth driving, with limited (de)accelerations and shorter travel time, reduces fuel consumption and CO_2 emissions.

Besides common sensor techniques, such as the use of inductive loop sensors, every vehicle will have V2I communication enabled. Also, by applying Video Content Analysis (VCA) techniques, on the installed video infrastructure, it is possible to detect passing vehicles, and in this manner to contribute to the traffic management. Moreover, VCA is capable of extracting information about dangerous situations, such as vehicle queues or vehicles moving along forbidden directions. Other examples include *traffic condition warning* (rapid traffic evolution), *stationary vehicle warning* (disabled vehicles), and *wrong way driving warning* (forbidden heading). V2I based efficiency and management applications can be extended in order to inform vehicles of such traffic anomalies. In this manner, vehicles cooperate through the infrastructure.

3. SafeCOP Technology Overview

This section explains the technical advances of the SafeCOP V2I experiment.

3.1. On Board and Road Side Units

The SafeCop V2I traffic management system employs a combination of Road Side Units (RSU) and On Board Units (OBU) to collect information about the ongoing traffic at a crossroad.

The RSU has a single sensor, a camera, which is used to provide a video feed to the Control Center.

The OBU constitutes the core system for collecting individual vehicle data, namely dynamic data (accelerations, angular speeds and magnetic field), position data (latitude/-longitude, speed, heading) and — when available — vehicle data (brake, engine rpm, gear, etc.). To this purpose the system is equipped with the following main components: 1) A 9-DOF inertial measurement unit for acceleration, angular speed and magnetic field 2) A high-precision GPS receiver 3) A CAN bus interface to be connected to the OBD vehicle diagnostic interface

In addition to these sensing units, the OBU will host a microcontroller and a 3G/4G module to provide connectivity to the Control Center. The same communication interface is used also for configuration and diagnostic of the device itself. The processing of dynamic, position and diagnostic data will be partitioned into an on-line portion, performed by the OBU itself, and an off-line part performed either in real-time or in batch mode in the Contro Center. The on-line processing is structured according to a synchronous data streaming model and will consist of the following main phases.

Acquisition. Data from all the sensors is acquired at fixed but configurable sampling rates. The accelerometer and the gyroscope will be sampled at a frequency between 1.5kHz and 5kHz, while the magnetometer will be sampled at a much lower rate, typically around 20Hz to 40Hz.

Pre-filtering. Previous experience in the specific domain shows that acceleration and angular speed data have a significant bandwidth between 40Hz and 100Hz, while magnetometer data has a bandwidth around 10Hz. The pre-filtering phase is constituted by a low-pass anti-alias digital filter followed by suitable decimation.

Synchronization. The sensor fusion algorithms that follow this phase need to operate on synchronized data, which is not necessarily guaranteed by the sensors themselves due to clock frequency differences between the sensors. The synchronization phase has the purpose of guaranteeing that the ratio between sampling frequencies of the different source — inertial unit, GPS and CAN bus — are constant over time.

Sensor fusion. Raw dynamic and position data are the combined with a filtering scheme still to be defined in detail. Typical solutions are based on Kalman filters or AHRS (Attitude and Heading Reference System) filters to produce derived measures, namely yaw, pitch, roll and speed.

[3] An inductive loop is a wire, of square, circle or rectangle shape, that is installed into or under the surface of the road.

On-line processing. Using the data produced by sensor fusion, this phase executes a set of algorithms that need to process the data in real-time. The main purpose of such algorithms is to compute a set of *features* with a much slower rate of change. As an example, maximum positive/negative acceleration, average acceleration and average speed will typically be computed over a 1 second period. Such features constitute the final output of the OBU.

Data produced by the OBU is then transmitted via the 3G/4G module to the Control Center for further processing.

Planned extensions to the RSU and OBU units in SafeCop include the possibility of leveraging vehicular networks based, e.g., on the IEEE 802.11p protocol, to support direct communication between OBU and RSU, as well as the construction of safety functions (see Section 3.3). Moreover, to support functions such as slow vehicle warning or traffic jam ahead warning, the OBU will be extended from sensor-only to include actuators, typically based on a buzzer or, possibly, a remote display.

3.2. Hazard Detection Functions

The understanding of the security risks involved in connected vehicle streams through V2V/V2I communication is an hot topic of research [7]. Hazard detection presents a scientific challenge as the inference of anomalies may be derived in the absence of a-priori knowledge about how such abnormalities can be realized and how they can be measured through the available sensors. The concept of anomalies not only include cyber-attacks, but also fault events (e.g., string instability of the vehicle platoon) or unexpected network congestion to be prevented. The proposed approach involves the use of innovative machine learning models [18], [19]. Even the *feature extraction* phase (i.e., the processing of the raw data before the application of machine learning algorithms) may include advanced statistical methods, such as spectral analysis and advanced statistics, such as the *mutual information* metric [17]. The most difficult task is the lack of a-priori knowledge of the anomalies (known in the literature as *unsupervised learning*) [21]. In order to identify anomalies, a “clustering” processing of data [13], [24] is performed. Roughly speaking, the process “brings together” all the data which can be considered as a regular, except for the few samples that could be linked to abnormalities. Clustering can be achieved through traditional algorithms such as *k-mean* or be flanked by newer methods, such as *one- class classification* [15]. If, on the other hand, data can be a-priori characterized (*labelled*) as regular or anomalous, the process can be empowered by supervised learning that exploits the a-priori knowledge of the data. The aggregation of data through clustering is then processed to classify the aggregations (*clusters*) according intelligible rules. To do so, the *Switching Neural Network* (SNN) is used [19], [9]. It creates intelligible rules with an accuracy comparable to traditional black box techniques, such as neural networks. Intelligible rules means a sequence of Boolean functions that link the data collected, their values and the fulfillment of certain conditions. For example, a rule may state the following:

```
if
   (level of congestion > threshold_1)
  and
   (frequency of specific flags in the
     packet headers > threshold_2)
  and
   (number of open sockets > threshold_3)
then
   (risk alert is above the acceptable
    threshold)
```

The interested reader finds in [12] a detailed comparison between the SNN and traditional classification methods. Models based on intelligible rules and high accuracy are of main interest in this context because they drive effective actions by human operators, for example, by setting certain operational conditions in order to maintain a desired security level. The rules and the inherent actions may be easily integrated within the cyber-physical system as well. Since intelligible rules are expressed in terms of boolean functions, their application requires a very small amount of computational resources and therefore allows its efficient implementation even on simple hardware devices, such as an FPGA or an 8-bit microcontroller. The study is carried out through the Rulex platform [11]. Rulex contains an implementation of the SNN, with focus on both reliability (test extended on numerous case studies) and computational efficiency (speed calculation , memory optimization). The following figure shows all the elements that make Rulex a machine learning platform over the state of the art. Once the model has been derived from historical data, one can update it with new data (*re-training*). Depending on the impact on quality of the processing steps from feature extraction to the derivation of rules, the re- training stage may involve the intervention of an analyst who oversees the accuracy of the updated model or be fully automated.

3.3. Safety functions

Wireless cooperative systems in vehicular application scenarios enable a set of *traffic management* applications, including the above mentioned A-TLS, for the adaptation of signal plan to the instantaneous traffic conditions, and the GLOSA, which shapes the vehicles traffic by suggesting the optimal speed to reduce (de)acceleration and stopping time, aiming to reach the green light on time. Traditionally, this information is derived from sensors mounted under or above the road surface (referred to as the Infrastructure), and auxiliary roadside signs may be used to inform the drivers. These systems are currently developed independently; however, changes in the dynamic signal plan according to the instantaneous traffic conditions impose the selection of a different speed optimal value, i.e. the integration of these two systems will strongly improve the effectiveness of this traffic management function [10]. In this context, SafeCOP will design and demonstrate an integrated A-TLS and GLOSA system based on Cooperative Awareness Message (CAM) that a vehicle periodically transmits on the V2I network, to inform the *infrastructure* of its position and speed (as well as other status information).

Road safety applications aim at providing drivers with information about critical situations in order to prevent accidents; these include Cooperative Forward Collision Warning, Approaching Emergency Vehicle, Emergency Electronic Brake Lights, Pre-crash Sensing Warning. Among these, the most advanced are the *active road safety* applications, which include the detection of dangerous road event/situations, in order to assist the vehicle driver. All *road safety functions* rely on Vehicle-to-Infrastructure (V2I) communications, i.e. vehicles are equipped with short range wireless communication capabilities which collaborate to form a temporary distributed network enabling communications with road infrastructure nodes (or other vehicles) located in line of sight or even out of radio range (if a multi-hop network is built among vehicles). Possible dangerous road events/situations, such as vehicles slowing down, vehicles queue, motionless objects, etc., can be detected through a specific platform for the acquisition from video cameras and elaboration algorithms, which is called the Video Content Analysis (VCA) platform [16]. SafeCOP will contribute to the active road safety by exploring the integration, on the V2I network, of the traffic management application and a VCA platform, in order to alert drivers of emerging traffic anomalies. SafeCOP V2I networks will support communications for both management and safety information.

Furthermore, starting from the available standards from IEEE 802.11p, ITS-G5 and CEN, SafeCOP will develop new mechanisms for safe wireless communications between cooperative embedded systems in vehicles and for V2I communications, in order to enhance the automotive functional safety. This include a revision of the messages that enable the V2x applications, e.g. the CAMs (Cooperative Awareness Messages) and DENMs (Decentralized Environmental Notification Messages), transmitted by vehicles and infrastructure periodically. These messages, which contain status information about vehicles (e.g. position, speed, heading, etc.) and information about certain events (e.g. event type, scope, validity, etc.), respectively, are collected by the Local Dynamic Map (LDM) entity, which describes the position and movement of the vehicle within its environment and the spatial relationship to other vehicles and roadside units in the surrounding.

3.4. Security

Cryptographic primitives are the foundational building-blocks to provide security and privacy assurances in complex computational and communication systems, and V2X communications are no exception. When the device is exposed to physical threats, cryptographic primivites may be subject to applied cryptanalysis techniques, i.e. implementation attacks. The largest class of implementation attacks is represented by *side-channel attacks* (SCAs), where the attacker exploits the information leakage happening on an unintended channel, typically an environmental parameter of the computation which is dependent on the computed data. Instances of such side-channels include energy consumption, execution timing or electro-magnetic (EM) emanations: all these environmental parameters provide enough information to infer the value of secret data intended to be stored within the device in an otherwise un-accessible way.

Designing efficient and effective countermeasures against side-channel attacks is a topic which has received warm attention by the research community. Typically, countermeasures against the aforementioned threats involve modifying the cipher at either the algorithmic or the implementation level [3], [4], [5], [6], [8], or changing the underlying hardware architecture so to suppress the side-channel leakage. In SafeCop, we will investigate the engineering trade-offs between security security level and performance of the cryptographic subsystem included in the RSU and OBU platforms [2].

4. Demonstrator

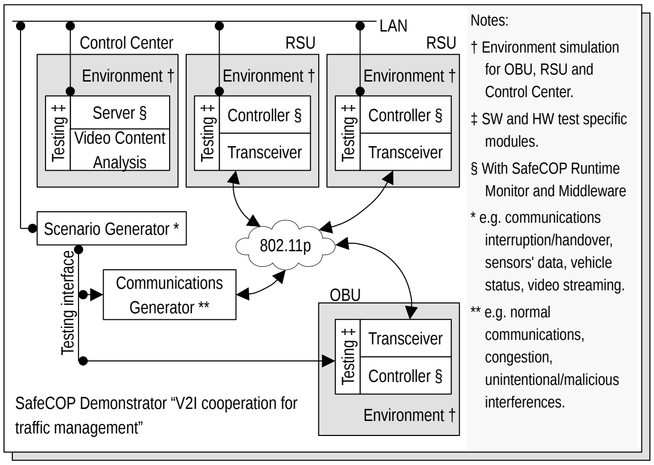
Our *demonstrator* is a medium fidelity system operated in a laboratory simulated environment. The related activities are estimated to have their center of gravity at Technology Readiness Level [1] 5 (technology validated in relevant environment) for the framework components and 4 (technology validated in laboratory) for the integrated demonstrator. The purpose of the demonstrator is to act as a proof-of-concept for SafeCOP concepts, as well as a means for validation and verification of SafeCOP framework components.

Proof-of concept. The demonstrator exploits the integration of Cooperative Awareness Messages (CAM), which are periodically sent by vehicles on the V2I wireless network, with the Green Light Optimal Speed Advisory (GLOSA) and the Adaptive Traffic Light System (A-TLS) in a traffic efficiency and management application, hereafter referred to as the *Traffic Management Application*. The application explores the fusion of road-side sensor data with vehicles' CAM; moreover it uses such awareness messages in order to offer an early warning service for traffic anomalies. The demonstrator functionalities and experimental evaluation thus serve as use case proof-of-concept.

Validation & verification. Demonstrator development is based on the SafeCOP framework components: safety assurance methodology and tools, secure wireless cooperation, platforms (HW, operating system, and middleware), and Runtime Monitor. Demonstrator development activities by themselves are part of the component *validation*, and the experiences which are gained during the demonstrator realization are fed back to the work packages that provide the framework. The component *verification* includes the integration tests needed to cover all the functional and non-functional properties in an integrated configuration.

4.1. System Architecture

Figure 2 shows the intended demonstrator architecture. The demonstrator integrates several *SafeCOP framework* *components*, including runtime mechanisms for safety assurance and distributed safety-critical cooperation techniques (based on extensions to IEEE 802.11p), into a *Traffic Management Application*, which runs in a distributed way on the demonstrator system parts. The demonstrator system is composed of on-board (OBU) and road side (RSU) units, as well as a server-based *Control Center*. Communications between the parts of the demonstrator system are performed through radio frequency front-ends which transmit and receive on-the-air, or through attenuators and noise generators for testing purposes. The Control Center and the OBUs are connected through Internet over a LAN.



Notes:
† Environment simulation for OBU, RSU and Control Center.
‡ SW and HW test specific modules.
§ With SafeCOP Runtime Monitor and Middleware
* e.g. communications interruption/handover, sensors' data, vehicle status, video streaming.
** e.g. normal communications, congestion, unintentional/malicious interferences.

Figure 2. Block diagram of the components of the V2I cooperation for traffic management prototype system

These systems are supported by a simulation environment composed of a *Scenario Generator*, a *Communication Generator*, and a set of *Testing Modules* which interface the Scenario Generator to the Control Center, OBUs, and RSUs. The *Scenario Generator* executes a given *test pattern* – it establishes when communication interruptions/handovers must happen, generates vehicle status and sensor data, and *plays back* video streaming analysed by the Video Content Analysis. Tests patterns that are *played-back* by Scenario Generator can be derived from the simulations and from the module tests carried on in WP3 and WP4, or from those executed during the implementation of the algorithmic part of the Traffic Management Application. The *Communication Generator* includes wireless transceivers connected to the IEEE 802.11p network and simulates a variable number of wireless nodes originating normal communications or unintentional/malicious interferences.

4.2. Functional Specification

The narrative description of our demonstrator functions as follows. The demonstrator (hardware and software) operates in a simulated environment and its evolution is triggered by the *Scenario Generator* component that generates a sequence of events, according to which the environment simulation evolves, and to which the systems under test (OBU, RSU, Control Centre, Traffic Management Application) react.

OBU periodically transmit CAM that are received by RSUs; legacy sensors detect passing vehicles. Traffic Management Application *basic functions*: 1) collect these data, perform data fusion and determine vehicle types and their kinematics; 2) optimize and actuate the traffic light signalling plan, and in a coordinated manner; 3) compute and distribute to vehicles their optimal speeds. Traffic Management Application ***hazards detection** functions*: 1) check for malicious attack to the wireless network; 2) monitor communication congestion or interruption: packet drop due to shadowing or out-of-range, delayed handover, etc.; 3) detect dangerous traffic conditions: rapid evolution, stationary vehicle, wrong way driving warning, etc.

The road-side monitoring system is equipped with video cameras and communicates the acquired information to the vehicles in transit. This system is mainly composed of a *Video Content Analysis* (VCA) platform running on the Control Center serve in charge of monitoring the roads, and elaboration algorithms which generate warning messages. In more detail, this system is able to extract the following information about potentially dangerous situations, analysing the images acquired by video cameras opportunely installed along the roads: 1) presence of objects moving inside the reference area; 2) presence of motionless objects in the reference area for longer than a minimum time threshold; 3) detection of vehicles slowing down inside the scene; 4) presence of vehicle queues in the video camera scene; 5) detection of objects moving along a reference direction (e.g. vehicles moving in forbidden directions); 6) presence of people inside sensitive areas; 7) detection of smoke or fog in sensitive areas.

4.3. Development and Evaluation Roadmap

The demonstrator will be developed incrementally, starting from an initial version of the Communication Generator and the Traffic Management Application, which will be initially developed separately to provide two simulation environments to integrate in the early demonstrator. The initial Communication Generator will support the basic communication functions, including the relevant SafeCOP components, whereas the Traffic Management Application will be initially developed on top of consumer hardware using an initial version of the Scenario Generator to drive the simulation. This incremental development aims at an early stable demonstrator that is free of module and integration tests issues.

5. Conclusions

SafeCOP is an upcoming ECSEL project, funded by the European Commission and several EU national governments, aiming at the definition of a framework for cooperating cyber-physical systems with safety and security concerns. Within SafeCOP, a relevant goal is to support V2X applications, which impose significant safety and security constraints. In this paper, we have provided an overview of the V2I cooperation for traffic management industrial use case, which will drive the development of the SafeCOP framework and serve as a benchmark for the validation and verification of several of its components.

References

[1] Technology readiness levels (TRL). HORIZON 2020 WORK PROGRAMME 2014-2015 General Annexes, Section G, 2014.

[2] Giovanni Agosta, Alessandro Barenghi, M. Maggi, and Gerardo Pelosi. Design space extension for secure implementation of block ciphers. *IET Computers & Digital Techniques*, 8(6):256–263, 2014.

[3] Giovanni Agosta, Alessandro Barenghi, and Gerardo Pelosi. A code morphing methodology to automate power analysis countermeasures. In Patrick Groeneveld, Donatella Sciuto, and Soha Hassoun, editors, *The 49th Annual Design Automation Conference 2012, DAC '12, San Francisco, CA, USA, June 3-7, 2012*, pages 77–82. ACM, 2012.

[4] Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi, and Michele Scandale. Enhancing Passive Side-Channel Attack Resilience through Schedulability Analysis of Data-Dependency Graphs. In *Network and System Security - 7th International Conference, NSS 2013, Madrid, Spain, June 3-4, 2013. Proceedings*, pages 692–698. 2013.

[5] Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi, and Michele Scandale. A multiple equivalent execution trace approach to secure cryptographic embedded software. In *The 51st Annual Design Automation Conference 2014, DAC '14, San Francisco, CA, USA, June 1-5, 2014*, pages 210:1–210:6. ACM, 2014.

[6] Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi, and Michele Scandale. The MEET approach: Securing cryptographic embedded software against side channel attacks. *IEEE Trans. on CAD of Integrated Circuits and Systems*, 34(8):1320–1333, 2015.

[7] M. Amoozadeh, A. Raghuramu, C. n. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, 53(6):126–132, June 2015.

[8] Alessandro Barenghi, Gerardo Pelosi, and Yannick Teglia. Information Leakage Discovery Techniques to Enhance Secure Chip Design. In Claudio Agostino Ardagna and Jianying Zhou, editors, *Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication - 5th IFIP WG 11.2 Int.'l Workshop, WISTP 2011, Heraklion, Crete, Greece, June 1-3, 2011. Proceedings*, volume 6633 of *LNCS*, pages 128–143. Springer, 2011.

[9] Davide Cangelosi, Fabiola Blengio, Rogier Versteeg, Angelika Eggert, Alberto Garaventa, Claudio Gambini, Massimo Conte, Alessandra Eva, Marco Muselli, and Luigi Varesio. Logic learning machine creates explicit and stable rules stratifying neuroblastoma patients. *BMC Bioinformatics*, 14(7):1–20, 2013.

[10] Soufiene Djahe, Nafaa Jabeur, Robert Barrett, and John Murphy. Toward V2I Communication Technology-based Solution for Reducing Road Traffic Congestion in Smart Cities. In *International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6, May 2015.

[11] Rulex Inc. Rulex website.

[12] Rulex Inc. Technology comparison.

[13] A. K. Jain, M. N. Murty, and P. J. Flynn. Data clustering: A review. *ACM Comput. Surv.*, 31(3):264–323, September 1999.

[14] Daniel Krajzewicz, Andreas Leich, Robbin Blokpoel, Michela Milano, and Thomas Stützle. COLOMBO: Exploiting Vehicular Communications at Low Equipment Rates for Traffic Management Purposes. In *Advanced Microsystems for Automotive Applications 2015*, pages 117–130. Springer, 2016.

[15] L. Livi, A. Sadeghian, and W. Pedrycz. Entropic one-class classifiers. *IEEE Transactions on Neural Networks and Learning Systems*, 26(12):3187–3200, Dec 2015.

[16] C. Machy, C. Carincotte, and X. Desurmont. On the use of Video Content Analysis in ITS : A review from academic to commercial applications. In *9th International Conference on Intelligent Transport Systems Telecommunications (ITST)*, pages 574–579, Oct. 2009.

[17] M Mongelli, M Aiello, E Cambiaso, and G Papaleo. Detection of dos attacks through fourier transform and mutual information. In *Communications (ICC), 2015 IEEE International Conference on*, pages 7204–7209. IEEE, 2015.

[18] M Mongelli, T De Cola, M Cello, M Marchese, and F Davoli. Feederlink outage prediction algorithms for sdn-based high-throughput satellite systems. In *Communications (ICC), 2016 IEEE International Conference on*. IEEE, in press.

[19] M. Muselli and E. Ferrari. Coupling logical analysis of data and shadow clustering for partially defined positive boolean function reconstruction. *IEEE Transactions on Knowledge and Data Engineering*, 23(1):37–50, Jan 2011.

[20] P. Pagano, M. Petracca, D. Alessandrelli, and C. Salvadori. Is ict mature for an eu-wide intelligent transport system? *IET Intelligent Transport Systems*, 7(1):151–159, March 2013.

[21] Animesh Patcha and Jung-Min Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 51(12):3448 – 3470, 2007.

[22] Mukesh Saini, Abdulhameed Alelaiwi, and Abdulmotaleb El Saddik. How close are we to realizing a pragmatic vanet solution? a meta-survey. *ACM Comput. Surv.*, 48(2):29:1–29:40, November 2015.

[23] Brandon Schoettle and Michael Sivak. A survey of public opinion about autonomous and self-driving vehicles in the US, the UK, and Australia. Technical Report UMTRI-2014-21, University of Michigan, Ann Arbor, Transportation Research Institute, 2014.

[24] J. Xie and S. Jiang. A simple and fast algorithm for global k-means clustering. In *Education Technology and Computer Science (ETCS), 2010 Second International Workshop on*, volume 2, pages 36–40, March 2010.