An Overview of Security Ongoing Work in Cooperative ITS

Ines Ben Jemaa, Pierpaolo Cincilla, Arnaud Kaiser, Brigitte Lonc

Paper ID TP0960

An Overview of Security Ongoing Work in Cooperative ITS

Ines Ben Jemaa[1*], Pierpaolo Cincilla[1], Arnaud Kaiser[1], Brigitte Lonc[2]

1{ines.benjemaa, pierpaolo.cincilla, arnaud.kaiser }@irt-systemx.fr

2 brigitte.lonc@renault.com

1. IRT SystemX Paris-Saclay, France
2. Renault SAS, France

Abstract

Cooperative Intelligent Transport Systems (C-ITS) open the way to a large set of new applications that improve road safety and traffic and energy efficiency. However, this exposes vehicles to new security threats. Therefore, securing communication is paramount for ITS deployment that is why several research works are now focusing on emerging threats and countermeasures.

This paper overviews the current state of security standards, research projects and existing security evaluation frameworks. The paper gives a qualitative comparison of the different project solutions, details the current security mechanisms integrated in the simulation platforms and discusses the open research challenges.

Keywords:

Cooperative ITS, security projects, simulation platforms

Introduction

Intelligent Transport Systems (ITS) is a hot research topic from many years and is now close to become an everyday reality. Standardization efforts and pre-deployment projects pave the way for the new smart mobility. Both the European Telecommunications Standards Institute (ETSI) in Europe and the Institute of Electrical and Electronics Engineers (IEEE) in United States define a set of standards for ITS [1] and several pre-deployment projects are now testing related technologies in the field [2]. In addition to embedded sensors, ITS Stations receive (and send) relevant information such as position, speed, and heading from their neighbours, enhancing their capacity to understand and react properly to their environment as shown in figure1. Cooperative aspects of autonomous driving are collecting increasing attention because it has several potentials to improve safety and traffic efficiency.

The AutoNet2030 European project[1], for instance, has been working on developing cooperative autonomous vehicles by testing some use cases such as lane changing and platoon forming. The SARTRE project[2] was focusing also on developing platoon services using ITS-G5/IEEE 802.11p and has showed that platoons reduce considerably the fuel consumption.

Cooperative platoon is one example of autonomous driving use cases where vehicles cooperate to build a platoon of vehicles, to merge with other platoons or to split in several platoons. Vehicles exchange periodically messages about velocity, acceleration, positions, etc to maintain the platoon stability. This promotes an enhancement of traffic fluency and thus decreasing road congestions.

Security mechanisms are one of the major communication requirements for new ITS services. Indeed, detecting and prohibiting malicious behaviours such as message alteration, message spoofing or even track vehicles by eavesdropping their locations, in such networks is compulsory to prevent safety damages and to ensure ITS service reliability and continuity. A malicious user can take the control of a vehicle and modify its behaviour. Changing the manoeuvers of a vehicle may lead to fatal damages and to serious safety risks.

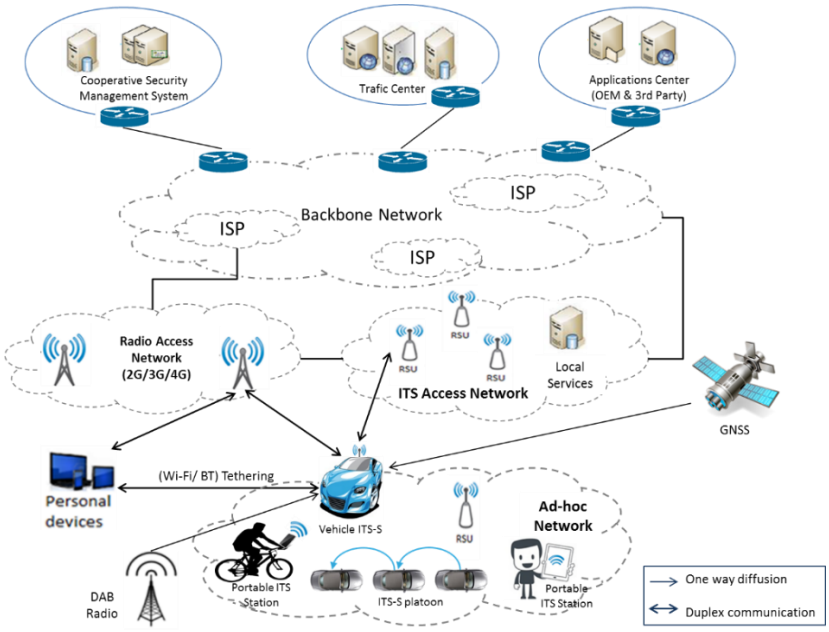

Figure 1 Cooperative ITS architecture

Many efforts have been conducted in the standardization and research community to tackle the problems of security in V2X (Vehicle to Anything) communications with regard to the ITS services. The main methods to investigate security mechanisms' effectiveness are roads tests and simulation. Road experiments permit to test ITS technologies and interoperability in real settings to validate security mechanisms performances on an empiric basis. On the other hand, simulation is useful to investigate ITS stations interactions and behaviour in large-scale scenarios that cannot be tested at this stage. Thanks to simulation, we can investigate emerging phenomena due to complex interactions of a large number

[1] http://www.autonet2030.eu/

[2] http://www.sartre-project.eu/en/Sidor/default.aspx

of vehicles at a city scale.

In this paper, we first survey the ongoing security standardization work in Europe. Second, we compare various research projects and proposed solutions to tackle the ITS communication security. Third, we give the state of the art of the integrated security mechanisms in the simulation platforms. Finally, we discuss the open security research axes.

Overview of current state of security standards, projects and simulation platforms

While Computational performance of cryptographic algorithms or cryptographic attacks are validated and evaluated using real testbeds, many distributed security features such as performance of privacy algorithms or misbehaviour detection strategies are validated and evaluated using simulation.

Besides simulation of security modules, simulators integrate several features, which add more realism and effectiveness to the simulation results. For instance, many simulators integrate ETSI compliant communication protocols or micro and macro traffic models. In the following, we will list the existing simulation and explain their characteristics.

Security standards current state in Europe

ITS need standard message format and communications protocols in order to communicate and cooperate. Both the ETSI TC ITS WG5 working group[3] in Europe and the IEEE 1609.2 working group[4] in U.S are advancing in the standardization effort. [1] presents the standards and implementations progress in Europe.

Table 1 summarizes the existing ETSI security standards and their current state.

Standard Reference	Title	Status
TR 102 893	Threat, Vulnerability and Risk Analysis (TVRA) technical report	v1.1.1 Published, updated with GeoNet risk analysis
TS 102 731	Security services and architecture	v1.1.1 Published
TS 103 097	Security header and certificate formats	v1.2.1 Published under revision and extensions to support requirements of european C-ITS Platform
TS 102 940	ITS communications security architecture and security management	v1.2.1 Published under revision for extensions
TS 102 941	Trust and privacy management	v1.1.1 Published under revision and extensions to support requirements of european C-ITS Platform
TS 102 942	Access Control	v1.1.1 Published
TS 102 943	Confidentiality services	v1.1.1 Published

Table 1 - ETSI ITS Security Standards

[3] http://www.etsi.org/technologies-clusters/technologies/intelligenttransport/cooperative-its

[4] https://standards.ieee.org/develop/wg/1609_WG.html

Overview of security projects in C-ITS

During the ten last years, several research and development projects focusing on security for vehicular communication were launched. Their main interest is to design and test suitable security mechanisms. The **EVITA**[5] project for instance aims at securing the internal on-board system in order to prevent, or at least detect, illegal tampering. Attacks on V2X communication can only be averted if trustworthy V2X communication is combined with on-board security avoiding the transmission of manipulated messages to the external communication pairs. It also considered legal requirements on privacy and data protection and liability issues. The **Oversee**[6] project considers the use cases of "Parking lot reservation" and "Emergency vehicle warning". It provides protected runtime environments for the simultaneous and secure execution of applications. It provides also secured access to the internal network of the vehicle. **SIM-TD**[7] is a German project, which was focusing on real experimentation tests and simulation of security mechanisms for vehicular communications. However, it used non-standardized security mechanisms. **PRESERVE**[8] was one of the main European project that experimented security and privacy solutions. Preserve used existing security components from other R&D projects. The security design and implementation efforts of the project are proposed to the standardization bodies. **SystemX ISE** is a French project aiming at developing security and privacy aspects for C-ITS. The main contribution of the project is to design and implement a proof of concept of an ITS European PKI that has been proposed as a standard at ETSI. Moreover, ISE implemented the security layer as specified by ETSI and experimented it on a real testbed.

Table 2 shows a comparative study of the already listed projects and their main security concerns.

	Evita	**SimTD**	**Oversee**	**Preserve**	**ISE**
Start date	**2008 - 2011**	**2008-2013**	**2010 - 2012**	**2011 - 2015**	**2014 - present**
Real testbeds	X			X	X
Simulations		X		X	X
Evaluation of security	X			X	X
Evaluation of privacy	X			X	X
Inter-vehicle security	X	X	X	X	X
Intra-vehicle security	X				
Reuse of existing project components			X	X	
Use of real PKI				X	X

Table 2 - Qualitative comparison of the security projects

[5] http://www.evita-project.org/

[6] https://www.oversee-project.com/

[7] http://www.simtd.de/index.dhtml/enEN/index.html

[8] https://www.preserve-project.eu/

Overview of security simulation studies in ITS

Packet level simulation

The OMNet++[9] simulator is integrated in several vehicular simulation platforms such as Veins. Veins (Vehicles in network simulation) is an open source simulation platform, which couples OMNeT++ with the SUMO simulator. OMNeT ++ is a widely used simulator within the community working on the vehicular networks. Veins implements both the American and the European communication standards. Recently, several research works focusing on security in the vehicular networks have used Veins to validate and evaluate their proposed techniques such as [12] and [13]. In [12], security attacks such as message falsification and network jamming in a CACC network are simulated and their effects on the string stability are studied. In [14], vehicular misbehavior is simulated and misbehavior detection is tested and implemented.

NS3[10] (Network Simulator 3) is a widely used simulator in the research community. From version 20, NS3 integrates the wave and the IEEE 802.11 p access protocols dedicated for vehicular communication. NS3 is also integrted to the Itetris simulation framework that combines the network simulator, NS3, with the traffic simulator, SUMO (Simulator for Urban MObility). A third entity called ICS is responsible for coordinating both simulators' interaction in real or virtual time. [11] uses NS3 to develop new pseudonym changes techniques in vehicular communication to protect users privacy. However, efforts to integrate security modules for inter-vehicle communication in NS3 remain limited.

Application-level simulation

VanetSim[11] [8], [9] is a java simulator focusing mainly on simulating and testing privacy techniques in vehicular netwoks. VanetSim exports map layouts from Openstreet map and is able to generate microscopic traffic flows. In [4], several pseudonym change techniques, security attacks such as sending fake application messages and various vehicular applications are implemented. However, VanetSim does not implement. Moreover, logging system for performance evaluation purposes are limited.

Several works use vehicle traces to evaluate security performance. Even if this kind of simulation lacks considering communication impacts on the studied security mechanisms, analyzing vehicular traces remain simple and straightforward to characterize the proposed strategy. [15] uses the TAPAS vehicular realistic traces to evaluate their proposed privacy protecting technique. It also uses Matlab[12] processing to evaluate the QoS of forward collision warning (FCW) application when using their pseudonym change technique. [17] uses several configurations of vehicular mobility models and several road scenarios to evaluate their privacy techniques against attacks.

Prescan[13] is a proprietary software that was firstly developed to simulate Advanced Driver Assistance Systems (ADAS) for driving systems. Prescan integrated first, statistical V2X models and it was

[9] https://omnetpp.org/

[10] https://www.nsnam.org/

[11] http://svs.informatik.uni-hamburg.de/vanet/

[12] https://mathworks.com/products/matlab.html

[13] https://www.tassinternational.com/prescan

extended lately to support V2X communication protocols as defined by the ETSI standard but it does not integrate security simulation modules. It is largely used by the community working on ADAS but its use for V2X communication simulation remains limited. [10] used PreScan to simulate intersection collision scenarios and to compare different strategies of changing pseudonyms and their impact on the safety in intersections. Table 3 shows a qualitative comparison between the already cited simulators.

	VanetSim	**OMNet++**	**NS3**	**Prescan**	**Vehicle traces**
V2X com. stack	No	Yes	yes	yes	No
Privacy modules	Mix Zones, Silent Periods, SLOW and Pro-Mix	Mix Zones, Silent Periods	No	No	Yes
Simulation of security attacks	Application layer attacks	Application layer attacks	No	No	Application layer attacks Network layer attacks
Traffic simulation	Microscopic	Micro (Veins)	Micro (Itetris)	Macro	Microscopic
ADAS simulation	No	No	No	yes	No
Application integration	EEBL, RHCN, EVA, SVA	CACC	yes	No	forward collision warning

Table 3 - Qualitative comparison of simulators

Discussion

Both simulations and Field Operational Tests (FOT) allow validating and evaluating C-ITS protocols. Security aspects are evaluated in several levels. Real implementations are essential to evaluate the cryptographic performance of specific algorithms on specific hardware such as benchmarking the cryptographic performances of a HSM. However, as large-scale testbeds are time and resource consuming, the use of simulation is intuitive to evaluate the performances of a protocol especially in a large-scale scenario. However, its main drawback is that physical channels are modelled and thus not accurate and does not reflect real environments. Rreal implementations are usually deployed on a small scale scenarios to get empirical results that may (in)validate results from simulations.

If we have a look at Table 2, we can observe that recent projects focus on security real implementations. Indeed, as standards maturate over time, it is usually not worth to implement the protocols that are not stable yet. Therefore, to speed up the standardization process, ETSI encourages the real implementation of Proof-Of-Concept (PoC) through the organization of Plug tests events. The main objective of such events is to bring together all actors of the C-ITS domain (OEM, manufacturers, road operators, etc.) that own a real implementation of the ETSI ITS protocol stack. Several test sessions are organized to evaluate each implementation on conformance, validation and interoperability.

At the standardization level, the specification of mechanisms such as misbehaviour detection are still lacking. At the time of writing this paper, there is no standardized solution to detect and revoke malicious vehicles in the network at the authority level.

New security open challenges in C-ITS

Requirements for generic security mechanisms in hybrid communications

The current security mechanisms in the ITS communication are designed to operate well over the ITS-G5 designed to fulfil the requirements of road safety applications. Security mechanisms for vehicular communication do not ensure data confidentiality as vehicles join freely the ad-hoc network to transmit and receive alerts. Moreover, each vehicle receiving a message in the network performs message integrity and authentication check. On the other hand, cellular networks are often used to ensure user access to usual Internet-based services thanks to their wide coverage and availability. Lately, the new generation of cellular technologies promotes novel services in the automotive field through direct communication between devices known as Device-to-Device (D2D).

Security mechanisms in cellular technologies are different from the current design of security for V2X communication. In cellular technology, it is the network, which controls the communication among User Equipments (UE). The core network authenticates each UE through periodic signalling and all sent data have to be encrypted using a pre-shared secret key.

New vehicular applications require using multiple access technologies to guarantee the best data delivery performance. In the same idea, security requirements have to be guaranteed for vehicular communication and should be agnostic from the used media and technology. Security mechanisms for V2X communication in D2D are not yet completely designed. Generic security mechanisms that do not depend on the access technology architecture have to be integrated to the ITS communication stack. Security mechanisms for hybrid architecture have to be also compliant with the new autonomous driving service requirements such as real time communication and high data reliability. They have also to rely on a generic security management system that is independent form the carrier to deliver and manage long-term certificates and short-term certificates.

Misbehaviour detection and certificate revocation

The misbehaviour detection mechanism monitors ITS communications and catch faulty or malicious ITS-Station (ITS-S) to identify and exclude them from the system. In order to enhance cooperative awareness, ITS-S exchange relevant information about their speed, heading, position, etc., as well as emergency messages. Those messages are sensitive for safety and the system must be robust to faulty devices or malicious users that may sent erroneous or tampered information.

To this end, it is essential to have a misbehaviour detection mechanism that permits to monitor the system and exclude misbehaving nodes. The misbehaviour detection system needs two components: one embedded in the ITS-S (e.g. vehicles) that monitor exchanged information plausibility and the other in the cloud that receive misbehaviour reports from ITS-S and analyse them.

The misbehaviour detection arises several privacy issues: to send a misbehaviour report can be threatening for both the reporter and the reported ITS-S. Moreover, the misbehaviour authority needs a means to link pseudonym identities (or another mechanism) for both investigation and revocation purposes. The challenge is to develop misbehaviour detection systems that are effective without harming the privacy of the honest entities. See [18] for a survey.

Privacy threats

V2X messages are exchanged periodically between vehicles and RSU in clear. An entity, that is eavesdropping the exchanged messages on the air interface, could easily track vehicles locations and thus violate their privacy. One solution largely studied in the community to tackle this problem is to change continuously each vehicle's short-term certificate a.k.a pseudonyms, following a specific strategy. Many strategies are proposed in the literature and each strategy has advantages and limitations. A study to evaluate and compare these strategies has been started at ETSI within the ITS Security Working Group (WG5). It is also worth mentioning that such privacy-enhancing system shall enable linkability under some specific circumstances. For instance, if an accident occurs due to a misbehaving vehicle, law enforcement shall be able to find the identity of the driver based on the pseudonymous V2X messages sent by the vehicle.

Yet, legislation and legal efforts in Europe have recently started in the field of ITS privacy. Today there is no standardized and approved privacy protection strategy by the ITS authorities. There are still required interactions between the ITS manufacturer, the transport authorities and the legislative authorities to find an agreement for ITS privacy protection.

Trade-off between security, privacy and safety

The most challenging objective of security mechanisms in vehicular communication is to find an acceptable balance between security, privacy and safety. Today, there are no straightforward solutions and extensive studies on this topic need to be carried out. Indeed, the design of the security mechanisms for vehicular communication has to provide an acceptable level of security and privacy without affecting the vehicular safety. The current system is based on providing long term and short-term certificates (i.e, pseudonyms). Vehicles use certificates to sign V2X messages for integrity and authentication purposes. Message signatures add a security header of about 108 bytes to the CAM (Cooperative Awareness Messages) and DENM (Decentralized Environmental Notification Message) [16]. Moreover, security signature operation and the security signature check may include a considerable processing time at the sender and receiver side respectively. According to [7], the security header creates additional latency and thus has an impact on the timely sensitive applications especially in dense scenarios.

For privacy, the pseudonym change, which leads to changing vehicle's identity temporarily, is a largely accepted solution. It aims at protecting vehicles from being tracked during their journey. However, the frequent change of identity may cause a problem to the whole neighbourhood cooperative awareness and may create phantom entries in the vehicles' neighbourhood database. Moreover, some pseudonym change strategies prohibit vehicles from communicating during a silent period after the change operation. This is not compliant with the real time characteristic of the safety applications where data have to reach target vehicles in a short time frame. New suitable metrics which quantify this trade-offs have to be developed.

Conclusion

In this paper, we presented an overview of the current state of the security research and development

work in cooperative ITS. Several ongoing work either in the standardization bodies or in the R&D projects aim at designing and validating security mechanisms for cooperative ITS. We presented the status of the ongoing security standardization at ETSI and noticed that several security aspects and adaptations have to be designed and integrated to the communication stack.

We then listed the latest security R&D project and identify the main security features that they are working on. We also cited some relevant works that used simulation and highlighted the main simulated security features. We discussed the need to use simulation and field operational tests to validate the security mechanisms and identifies the cases where they are highly recommended.

Finally, we discussed the new open research challenges in security that have to be taken into consideration in the design of the security standards in the next few years. The next design has to build an efficient and reliable security system that is compliant with the requirements of safety services and low complexity deployment

ACKNOWLEDGEMENT

This research work has been carried out in the framework of the Technological Research Institute SystemX

References

1. Lonc B., Cincilla P. (2016). *Cooperative ITS Security Framework: Standards and Implementations Progress in Europe***.** 3rd International Workshop on Smart Vehicles: Connectivity Technologies and ITS Applications, Portugal.
2. Boudguiga A., Kaiser A., Cincilla P. (2015) *Cooperative-ITS Architecture and Security Challenges: a Survey.* 22th Inteligent Transport System World Congress, France.
3. Panagiotis (Panos) Papadimitratos, Ghita Mezzour, and Jean-Pierre Hubaux. 2008. Certificate revocation list distribution in vehicular communication systems. In *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking* (VANET '08). ACM, New York, NY, USA, 86-87.
4. Jason J. Haas, Yih-Chun Hu, and Kenneth P. Laberteaux. 2009. Design and analysis of a lightweight certificate revocation mechanism for VANET. In *Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking* (VANET '09). ACM, New York, NY, USA, 89-98.
5. J. Petit, F. Schaub, M. Feiri and F. Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 17, no. 1, pp. 228-255, Firstquarter 2015.
6. Pierpaolo Cincilla, Omar Hicham and Benoit Charles Vehicular PKI Scalability-Consistency Trade-Offs in Large Scale Distributed Scenarios, , IEEE Vehicular Networking Conference (VNC) December 8–10, 2016

7. Ben Brahim M, Ben Hamida E, Filali F, Hamdi N. Performance impact of security on cooperative awareness in dense urban vehicular networks. 2015 IEEE 11th Int Conf Wirel Mob Comput Netw Commun WiMob 2015. 2015;(October):268–74.

8. Tomandl A., Herrmann D., Fuchs KP, Federrath H., Scheuer F. VANETsim: An open source simulator for security and privacy concepts in VANETs. **Proc** 2014 Int Conf High Perform Comput Simulation, HPCS 2014. 2014;543–50.

9. Tomandl A, Scheuer F, Federrath H. Simulation-based evaluation of techniques for privacy protection in VANETs. Int Conf Wirel Mob Comput Netw Commun. 2012;165–72.

10. Lefèvre S, Petit J, Bajcsy R, Laugier C, Kargl F. Impact of V2X privacy strategies on Intersection Collision Avoidance systems. IEEE Veh Netw Conf VNC. 2013;71–8.

11. Artail H, Abbani N. A Pseudonym Management System to Achieve Anonymity in Vehicular Ad Hoc Networks. IEEE Trans Dependable Secur Comput. 2016;13(1):106–19.

12. Amoozadeh M, Raghuramu A, Chuah CN, Ghosal D, Michael Zhang H, Rowe J, et al. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Commun Mag. 2015;53(6):126–32.

13. Garip MT, Gursoy ME, Reiher P, Gerla M. Congestion Attacks to Autonomous Cars Using Vehicular Botnets. NDSS Symp 2015

14. Zaidi K, Milojevic M, Rakocevic V, Rajarajan M. Data-centric rogue node detection in VANETs. Proc - 2014 IEEE 13th Int Conf Trust Secur Priv Comput Commun Trust 2014. 2015;(December 2015)

15. Emara K, Woerndl W, Schlichter J. Context-based Pseudonym Changing Scheme for Vehicular Adhoc Networks. 2016

16. “Etsi ts 103 097 v1.2.1 (2015-06) - intelligent transport systems (its); security; security header and certificate formats,”

17. Sampigethaya K, Li M, Huang L, Poovendran R. AMOEBA: Robust location privacy scheme for VANET. IEEE J Sel Areas Commun. 2007;25(8):1569–89.

18. Rens Wouter van der Heijden, Stefan Dietzel, Tim Leinmüller, Frank Kargl: Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems.