ETSI TR 103 460 V2.1.1 (2020-10)

Intelligent Transport Systems (ITS);
Security;
Pre-standardization study on Misbehaviour Detection;
Release 2

Reference
DTR/ITS-00539

Keywords
ITS, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document provides an overview of the relevant misbehaviour detection mechanisms suitable for C-ITS and provides comments on performance and applicability of different misbehaviour detection mechanisms. The present document provides also hints on potential minimum requirements for the security architecture and misbehaviour detection distribution mechanisms, i.e. misbehaviour reporting.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 101 539-1: "Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification".

[i.2] ETSI TS 101 539-2: "Intelligent Transport Systems (ITS); V2X Applications; Part 2: Intersection Collision Risk Warning (ICRW) application requirements specification".

[i.3] ETSI TS 101 539-3: "Intelligent Transport Systems (ITS); V2X Applications; Part 3: Longitudinal Collision Risk Warning (LCRW) application requirements specification".

[i.4] ETSI TS 102 637-1: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements".

[i.5] ETSI EN 302 637-2: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[i.6] ETSI TS 102 894-2: "Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary".

[i.7] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

[i.8] ETSI TS 103 096-2: "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP)".

[i.9] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

[i.10] ETSI TR 103 562: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Analysis of the Collective Perception Service (CPS); Release 2".

[i.11] ETSI TR 102 893: "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)".

[i.12] Recommendation ITU-T X.696 (08/2014): "Information Technology-Specification of Octet Encoding Rules (OER)".

[i.13] European Commission: "Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1", June 2017.

NOTE: Available at https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf.

[i.14] European Commission: "Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)".

NOTE: Available at https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf.

[i.15] C-ITS Platform WG5: "Security & Certification Final Report Annex II Revocation of trust in Cooperative Intelligent Transport Systems (C-ITS)".

NOTE: Available at https://ec.europa.eu/transport/themes/its/c-its_en.

[i.16] EU-US ITS Task Force - Standard harmonization Task Group 6: "Cooperative-ITS Security Policy Framework".

NOTE: Available at https://ec.europa.eu/digital-single-market/en/news/harmonized-security-policies-cooperative-intelligent-transport-systems-create-international.

[i.17] US-DOT, CVRIA: "Connected Vehicle Reference Implementation Architecture".

[i.18] US-DOT, ARC-IT: "The National ITS Reference architecture - Cooperative ITS Credentials Management System".

NOTE: Available at https://local.iteris.com/arc-it/html/physobjects/physobj86.html.

[i.19] FHWA-JPO-16-312: "Security Management Operational Concept - Tampa (THEA)".

NOTE: Available at https://rosap.ntl.bts.gov/view/dot/30827.

[i.20] 2016-31059 National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT): "Federal Motor Vehicle Safety - V2V communications, Notice of Proposed Rulemaking (NPRM)".

[i.21] V. Mahieu, G. Baldini: "Harmonization Task Group 6 Cooperative ITS Security Policy", ITS World Congress 2015.

[i.22] T. Leinmüller, R. K. Schmidt and A. Held: "Cooperative position verification - defending against roadside attackers 2.0", Proceedings of 17th ITS World Congress, 2010.

[i.23] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan and M. Rajarajan: "Host-based intrusion detection for vanets: A statistical approach to rogue node detection", IEEE Transactions on Vehicular Technology, vol. 65, no. 8, pp. 6703-6714, Aug 2016.

[i.24] S. Chang, Y. Qi, H. Zhu, J. Zhao and X. Shen: "Footprint: Detecting sybil attacks in urban vehicular networks", IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp. 1103-1114, June 2012.

[i.25] A. Vora and M. Nesterenko: "Secure location verification using radio broadcast", IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 4, pp. 377-385, Oct 2006.

[i.26] R. W. van der Heijden, A. Al-Momani, F. Kargl and O. M. F. Abu-Sharkh: "Enhanced position verification for vanets using subjective logic", IEEE 84th Vehicular Technology Conference (VTC-Fall), Sept 2016, pp. 1-7.

[i.27] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak and I. Stojmenovic: "On data-centric misbehavior detection in vanets", 2011 IEEE Vehicular Technology Conference (VTC Fall), Sept 2011, pp. 1-5.

[i.28] Joseph Kamel, Arnaud Kaiser, Ines Jemaa, Pierpaolo Cincilla, Pascal Urien: "Feasibility Study of Misbehavior Detection Mechanisms in Cooperative Intelligent Transport Systems (C-ITS)", 2018 IEEE 87th Vehicular Technology Conference: VTC2018-Spring, Jun 2018, Porto, Portugal.

NOTE: Available at https://hal.archives-ouvertes.fr/hal-01779985.

[i.29] J. P. Hubaux, S. Capkun and J. Luo: "The security and privacy of smart vehicles", IEEE Security Privacy, vol. 2, no. 3, pp. 49-55, May 2004.

[i.30] Moreno Ambrosin, Lily L Yang, Xiruo Liu, Manoj R Sastry, Ignacio J Alvarez: "Design of a Misbehavior Detection System for Objects Based Shared Perception V2X Applications", to appear in 2019 IEEE Intelligent Transportation Systems Conference (ITSC19), October 27-30, 2019.

[i.31] Joseph Kamel, Ines Jemaa, Arnaud Kaiser, Loic Cantat, Pascal Urien: "Misbehavior Detection in C-ITS: A comparative approach of local detection mechanisms", Vehicular Networking Conference (VNC), Dec 2019, Los Angeles, California, United States.

[i.32] C. Allig, T. Leinmuller, P. Mittal and G. Wanielik: "Trustworthiness Estimation of Entities within Collective Perception", IEEE Vehicular Networking Conference (VNC), Dec 2019.

[i.33] J. Kamel, I. B. Jemaa, A. Kaiser and P. Urien: "Misbehavior Reporting Protocol for C-ITS", IEEE Vehicular Networking Conference (VNC), Taipei, Taiwan, Dec. 2018.

[i.34] N. Bimeyer, C. Stresing and K. M. Bayarou: "Intrusion detection in vanets through verification of vehicle movement data", IEEE Vehicular Networking Conference, Dec 2010, pp. 166-173.

[i.35] C. Chen, X. Wang, W. Han and B. Zang: "A robust detection of the Sybil attack in urban vanets", 29th IEEE International Conference on Distributed Computing Systems Workshops, June 2009, pp. 270-276.

[i.36] Y. Hao, J. Tang, and Y. Cheng: "Cooperative sybil attack detection for position based applications in privacy preserved vanets", in 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, Dec 2011, pp. 1-5.

[i.37] S. Park, B. Aslam, D. Turgut, and C. C. Zou: "Defense against Sybil attack in vehicular ad hoc network based on roadside unit support", MILCOM 2009 - 2009 IEEE Military Communications Conference, Oct 2009, pp. 1-7.

[i.38] M. Raya, P. Papadimitratos, V. D. Gligor and J. P. Hubaux: "On datacentric trust establishment in ephemeral ad hoc networks", IEEE INFOCOM 2008 - The 27th Conference on Computer Communications, April 2008.

[i.39] Z. Cao, J. Kong, U. Lee, M. Gerla and Z. Chen: "Proof-of-relevance: Filtering false data via authentic consensus in vehicle ad-hoc networks", IEEE INFOCOM Workshops 2008, April 2008, pp. 1-6.

[i.40] M. Sun, M. Li and R. Gerdes: "A data trust framework for VANETs enabling false data detection and secure vehicle tracking", IEEE Conference on Communications and Network Security (CNS), October 2017, pp. 1-9.

NOTE: Available at https://doi.org/10.1109/CNS.2017.8228654.

[i.41] S. So, P. Sharma and J. Petit: "Integrating plausibility checks and machine learning for misbehavior detection in vanet", 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 564-571, 2018.

[i.42] J. Kamel, I. B. Jemaa, A. Kaiser, P. Cincilla and P. Urien: "CaTch: A Confidence Range Tolerant Misbehavior Detection Approach", IEEE Wireless Communications and Networking Conference, Apr 2019.

[i.43] M. Raya, P. Papadimitratos, I. Aad, D. Jungels and J. P. Hubaux: "Eviction of misbehaving and faulty nodes in vehicular networks", IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1557- 1568, Oct 2007.

[i.44] Rens W. van der Heijden, Stefan Dietzel, Tim Leinmüller, Frank Kargl: "Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems", IEEE Communications Surveys & Tutorials 2016 (arXiv:1610.06810v2 [cs.CR] 29 Nov 2018).

[i.45] Q. Xu, R. Zheng, W. Saad and Z. Han: "Device fingerprinting in wireless networks: Challenges and opportunities", IEEE Communications Surveys Tutorials, Volume: 18, Issue: 1, First quarter 2016.

[i.46] T. Zhou, R. R. Choudhury, P. Ning and K. Chakrabarty: "Privacy preserving detection of sybil attacks in vehicular ad hoc networks", Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking Services (MobiQuitous), Aug 2007, pp. 1-8.

[i.47] T. H.-J. Kim, A. Studer, R. Dubey, X. Zhang, A. Perrig, F. Bai, B. Bellur and A. Iyer: "Vanet alert endorsement using multi-source filters", Conference MOBICOM - Proceedings of the Seventh ACM International Workshop on VehiculArInterNETworking, ser. VANET '10. New York, NY, USA: ACM, 2010, pp. 51-60.

[i.48] H.-C. Hsiao, A. Studer, R. Dubey, E. Shi and A. Perrig: "Efficient and secure threshold-based event validation for vanets", Proceedings of the Fourth ACM Conference on Wireless Network Security, ser. WiSec'11. New York, NY, USA: ACM, 2011, pp. 163-174.

[i.49] X. Zhuo, J. Hao, D. Liu and Y. Dai: "Removal of misbehaving insiders in anonymous vanets", Proceedings of the 12th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, ser. MSWiM '09. New York, NY, USA: ACM, 2009, pp. 106-115.

[i.50] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held and G. Schaefer: "Vehicle behavior analysis to enhance security in vanets", TU Ilmenau, Proceedings of 4th Workshop on Vehicle to Vehicle Communications (V2VCOM 2008), 2008, pp. 1-8.

[i.51] B. Xiao, B. Yu and C. Gao: "Detection and localization of sybil nodes in vanets", Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, ser. DIWANS '06. New York, NY, USA: ACM, 2006, pp. 1-8.

[i.52] I. J. Byung Kwan Lee, EunHee Jeong: "A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET", International Journal of Security and ITS Applications, vol. 7, pp. 1-10, 2013.

[i.53] A. Jøsang: "A logic for uncertain probabilities", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 9, no. 3, pp. 279-311, Jun. 2001.

[i.54] P. K. Singh, M. K. Dash, P. Mittal, S. K. Nandi and S. Nandi: "Misbehavior detection in c-its using deep learning approach", Intelligent Systems Design and Applications, A. Abraham, A. K. Cherukuri, P. Melin, and N. Gandhi, Eds. Cham: Springer International Publishing, 2020, pp. 641-652.

[i.55] P. K. Singh, S. Gupta, R. Vashistha, S. K. Nandi and S. Nandi: "Machine learning based approach to detect position falsification attack in vanets", Security and Privacy, S. Nandi, D. Jinwala, V. Singh, V. Laxmi, M. S. Gaur, and P. Faruki, Eds. Singapore: Springer Singapore, 2019, pp. 166-178.

[i.56] R.W. van der Heijden, T. Lukaseder, F. Kargl., VeReMi: "A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs", Beyah R., Chang B., Li Y., Zhu S. (eds) Security and Privacy in Communication Networks. SecureComm 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 254. Springer, Cham.

[i.57] A. Jaeger, N. Bißmeyer, H. Stubing, and S. A. Huss: "A novel framework for efficient mobility data verification in vehicular ad-hoc networks", International Journal of Intelligent Transportation Systems Research, vol. 10, no. 1, pp. 11-21, Jan 2012.

[i.58] C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano and P. Manzoni: "T-vnets: a novel trust architecture for vehicular networks using the standardized messaging services of etsi its", Elsevier - International Journal Computer Communications, vol. 93, no. C, pp. 68-83, Nov. 2016.

[i.59] M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani and S. N. Muthaiah: "Detecting misbehaviors in vanet with integrated root-cause analysis", Elsevier - Ad Hoc Networks, vol. 8, no. 7, pp. 778 - 790, 2010.

[i.60] T. Leinmüller, E. Schoch, F. Kargl and C. Maihöfer: "Decentralized position verification in geographic ad hoc routing", Wiley - Security and Communication Networks, vol. 3, no. 4, pp. 289-302, 2010.

[i.61] N. Bissmeyer: "Misbehavior Detection and Attacker Identification in Vehicular Ad hoc Networks", Technische Universität Darmstadt, Dissertation, November 2014.

[i.62] Joseph Kamel: "Misbehavior Detection for Cooperative Intelligent Transport Systems (C-ITS)", PhD dissertation, IP Paris, Télécom Paris, July 2020.

[i.63] Abhinav Kamra, Jon Feldman, Vishal Misra and Dan Rubenstein: "Growth codes: Maximizing sensor network data persistence", Proceedings of ACM Sigcomm, Pisa, Italy, September 2006.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

ego vehicle: vehicle embedding the ITS-S being considered

reported ITS station: ITS station that is subject to creation of an MR

reporting ITS station: ITS station sending an MR

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 102 940 [i.7] and the following apply:

AoA	Angle of Arrival
ART	Acceptance Range Threshold
AT	Authorization Ticket
CAM	Co-operative Awareness Message
C-ITS	Cooperative Intelligent Transport System
CCMS	Cooperative-ITS Credential Management System
CoE	Certainty of Event
CP	Collective Perception
CPM	Collective Perception Message
CRL	Certificate Revocation List
DENM	Decentralized Environment Notification Message
DTSA	Detection Technique against a Sybil Attack
eART	enhanced Acceptance Range Threshold
EWMA	Exponentially Weighted Moving Average
ID	IDentity
ITS	Intelligent Transport System
ITS-S	ITS Station
K-NN	K-Nearest Neighbours
LEAVE	Local Eviction of Attackers by Voting Evaluators
LSTM	Long Short-Term Memory
MA	Misbehaviour Authority
MB	MisBehaviour
MBR	MisBehaviour Reporting
MD	MisBehaviour Detection
MDM	Minimum Distance Moved
MLP	Multi-Layer Perceptron
MPP	Map-Proofed Position
MR	Misbehaviour Report
OBU	On-Board Unit

PKI	Public Key Infrastructure
PRP	Permanent Revocation Protocol
P2DAP	Privacy-Preserving Detection of Abuses of Pseudonyms
RSSI	Received Signal Strength Indicator
RSU	Road Side Unit
SAW	Sudden Appearance Warning
SLEP	Suicide-based Local Eviction Protocol
SVM	Support Vector Machine
T-VNets	Trust architecture for Vehicular Networks
VEBAS	Vehicle Behaviour Analysis and Evaluation Scheme
VeReMi	Vehicular Reference Misbehavior Dataset

4 Background

4.1 General

The main purpose of a "Public Key Infrastructure" (PKI) in a C-ITS trust system, also referred to as "Cooperative-ITS Credential Management System" (CCMS), is to provide a certificate management system that supports secure distribution, use and revocation of certificates to ITS stations (ITS-Ss). Revocation of trust credentials may be needed, under different situations, e.g. for the following reasons:

- The CCMS detects a malicious ITS station and decides to evict it from the network.
- During the ITS-S life-cycle management, the certificates issued to an ITS station will be revoked at the "ITS-S end of life", e.g. the ITS station is decommissioned or the ITS station failed and thus is replaced by a spare part.

Misbehaviour detection and reporting is a main issue in a CCMS and has not been specified in details in the first pre-deployment phases due to the following reasons:

- Algorithms for misbehaviour detection applicable in an ad-hoc network (i.e. local detection on vehicles and roadside stations) as well as in a PKI are not sufficiently defined and seem to be not trivial. Denigration of benign ITS stations cannot be circumvented (risk of false positive).
- Misbehaviour detection requires a network connection to the PKI backend server. It cannot be assumed that a constant communication link is always available. As there are no real-time requirements on the transmission of "Misbehaviour Reports" (MRs), ITS stations may buffer information on detected misbehaviours or suspicious messages, and submit them to the PKI server, i.e. to a misbehaviour evaluation entity also called "Misbehaviour Authority" (MA), when there is a communication link available.

Nevertheless, misbehaviour detection and reporting should be considered from the start of the design of ITS stations.

Also, reactions on reception of an MR taken by the MA can combine various solutions including revocation mechanisms, such as:

- **Passive revocation** (or revocation by expiry): deactivation of the long-term certificate which is also called Enrolment Certificate; subsequently new pseudonym requests are no more allowed.
- **Active revocation**: creation of a "Certificate Revocation List" (CRL) entry and active distribution of the CRL in the applicable ad-hoc network.

The detection of misbehaviour can be implemented in an ITS station operating on the ad-hoc network as a local feature, using e.g.:

- some checks for information correctness on the received (safety) messages; and
- optionally the vehicle sensors' information.

Abnormal behaviour of a faulty or malicious ITS station may also be detected via other types of communication (rather than localized communications, i.e. in an ad-hoc network), e.g. involving networked communications such as Internet, and web services/remote services/applications in a central ITS station. The misbehaviour may also be detected by a CCMS entity if it receives abnormal solicitations from an ITS station.

For flexibility reasons and to enable continuous improvements, without disturbing already deployed ITS stations, detection algorithms should be updateable.

As local detection only provides limited information in time and space, this may be insufficient to identify an attack or an attacker in a reliable manner, and global detection that relies on the back-end systems/backbone infrastructure, i.e. the MA, can be needed.

The MA will be needed in the PKI design from an early stage on.

Misbehaviour detection raises privacy issues:

- when sending an MR, the privacy of the reporter and the reported ITS station should be preserved;
- the MA needs means to either link pseudonym certificates with their real long-term certificate, or use another mechanism for both investigation and revocation purposes.

The management and distribution of revocation information is out of scope of the present document.

4.2 European C-ITS trust system and revocation of trust

In the C-ITS Platform phase 1 report [i.15], the objectives of the revocation of trust have been defined as mechanisms to protect the core security services of authentication-authorization. Revocation of trust applies on a system model where:

- nodes are provisioned with security credentials such that access to security material is restricted to a set of authorized parties (e.g. private key used for signing);
- a node carries out operations where the correct use of security credentials indicates that it holds certain permissions;
- a node operates in a hostile environment where it may at some point stop functioning correctly.

If there are trusted parties that used a node's credentials to trust the node, and if the node meets some conditions for incorrect functioning, those parties are instructed not to trust interactions that are authenticated with these credentials, i.e. not to trust the node. This is known as revocation.

The C-ITS Platform Report [i.15] provides a policy framework for revocation of trust based on three steps:

1) What is to be revoked?
2) How is a revocation decision done?
3) What types of mechanisms are used to communicate information about the node revocation to other parties in the trusted domain (countermeasures)?

With respect to step 3) above (countermeasures), the C-ITS Platform Report [i.15] identifies the following potential solutions:

- **Active deactivation:** via a management/administrative function of the ITS station or application, preventing it from sending messages.
- **Active revocation:** inform all C-ITS parties that the node is to be considered revoked. Also inform all the CAs that the node cannot get new certificates.
- **Passive revocation or revocation by expiry:** do not directly inform the C-ITS parties that the node is to be considered revoked, but inform all the CAs that the node cannot get new certificates (waiting for unauthorized/malicious node credentials to expire).

Recently, the European Commission has published the "C-ITS Certificate Policy" [i.13] and the "Security Policy & Governance Framework for the Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)" [i.14]. These two documents provide the basis for secure and interoperable C-ITS system deployment in Europe. The Release 1 of the certificate policy does not require misbehaviour reporting and evaluation in the PKI and only requires passive revocation for first deployments. The certificate pre-loading period in an ITS station is restricted to maximum 3 months.

4.3 Misbehaviour detection, analysis and response in the US Connected Vehicle project

4.3.1 Context of SCMS design and harmonization US-EU-Australia task-group

In 2013, a team composed of the European Commission (EC), the United States Department of Transportation (US-DOT), and Transport Certification Australia (TCA) gathered to establish harmonized security policies for C-ITS. They compared existing security architectures such as the PRESERVE PKI and CAMP SCMS, and proposed a harmonized policy framework called CCMS ([i.16], [i.21]).

4.3.2 Functional architecture of CCMS

The CCMS is made of five processes:

- **Provisioning:** provides ITS stations with certificates of other CCMS components and policy information so they can start the enrolment process.
- **Enrolment:** issues and manages long-term certificates, including privacy services and policy management.
- **Authorization:** issues and manages short-term certificates, including privacy services and policy management.
- **Misbehaviour:** Receive MRs from ITS stations and process them.
- **Revocation:** Generate CRLs and distribute them to CCMS entities and ITS stations.

In the CVRIA architecture model (see [i.17] and [i.18]), the overall model (enterprise level) shows the main entities, processes and procedures of the CCMS: Provisioning, Enrolment, Authorization, Misbehaviour Reporting, Revocation as presented in Figure 1.

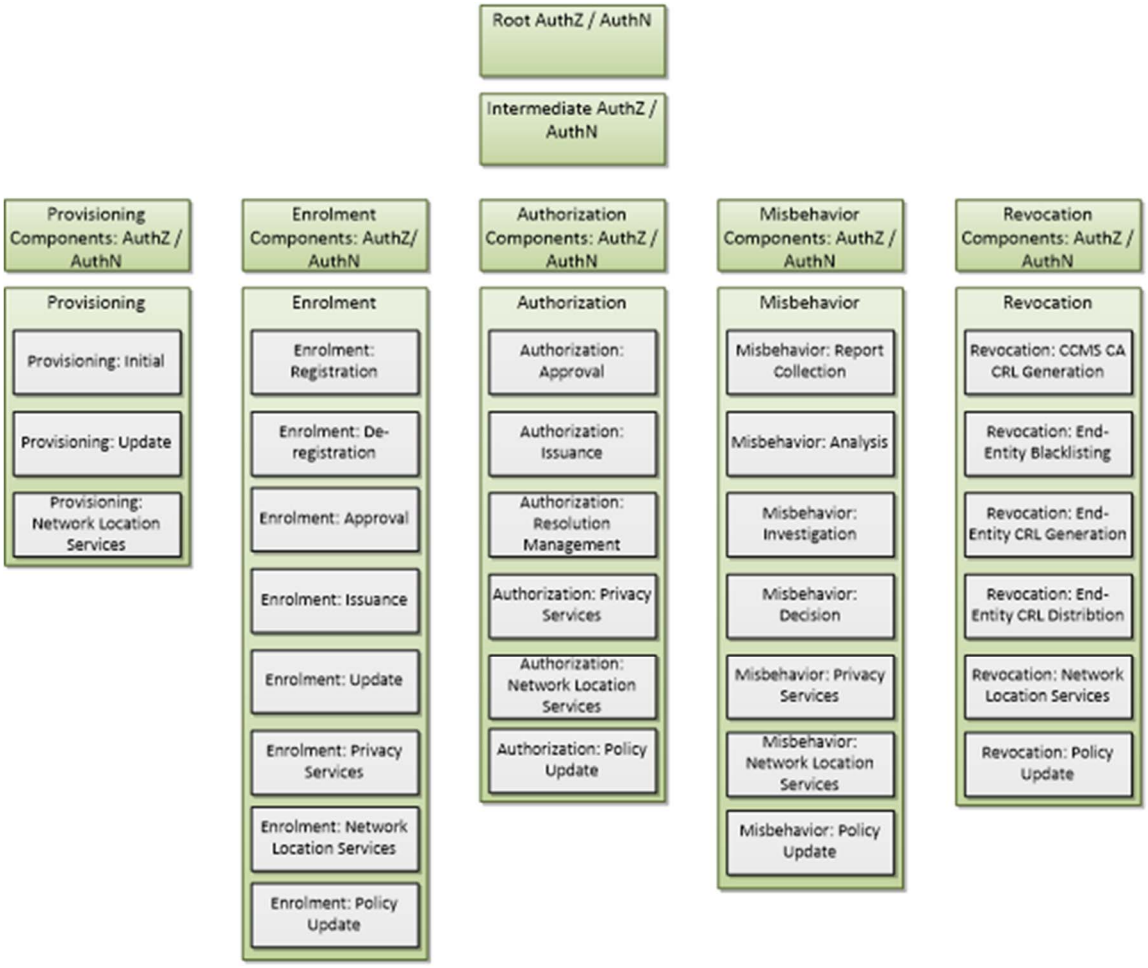


Figure 1: CCMS Entities, Processes and Procedures

The process of misbehaviour reporting/action and of revocation are defined in more details below:

- **"CCMS Misbehaviour"** components process MRs received from end entities. This process analyses each of these incoming MRs. Information is provided to the system operator and identify which issues may warrant additional investigation. This process correlates investigated MRs with end entities in order to identify systemic issues - defects, bad actor, etc. If revocation is warranted, this process provides information to "Authorization Components" or "Revocation Components", either locally or in another CCMS to initiate revocation and/or blacklisting, as appropriate. This process provides the system operator with status information about the transmission of credentials and information about identification and investigation of misbehaving connected vehicle devices.

- **"CCMS Revocation"** components generate the internal blacklist and CRLs, and distribute CRLs to other CCMS components and end entities. Once placed on the CRL, an end entity is in the unauthorized state. Once placed on the blacklist, an end entity is in the unenrolled state.

5 State-of-the-art

5.1 Detection approaches

5.1.1 General

Clause 5.1 presents the current state of the art detection approaches as described in relevant published works. It is worth to be noted that the technical subject presented in the referenced publications can be considered as being at the level of scientific investigations, rather than the result of practical implementations and respective field trials. Some of these publications are based on assumptions, e.g. on the exchange of messages different to CAM or DENM, that might not be directly applicable to current deployment of C-ITS. The present document is not providing any normative requirements on misbehaviour detection and related reporting. However, prior to normatively standardizing methods based on the publications referenced in the present document, feasibility studies are recommended.

In C-ITS, safety services rely on the cooperation of each communicating node in the network, which is supposed to send either beaconing information or warning messages. The present document focuses on misbehaviour that is based on sending false beacon information (e.g. CAM), see clause 5.1.2, and false warning messages (e.g. DENM), see clause 5.1.3. These mechanisms that result from "semantic level attacks" are qualified as message-based detection mechanisms. Misbehaviour detection may also be based on the evaluation of trust on a certain node based on the messages it sends. These mechanisms are known as node trust-based detection mechanisms.

Note that PKI based security would not be able to prevent such data semantic level attacks. Thus, the safety system highly requires the deployment of a mechanism that is able to detect misbehaving entities in the network.

5.1.2 False beacon information detection

Physical layer detection

Multiple studies suggest location verification using physical aspects of the signal. [i.25] proposes a method of triangulation of a node using distributed sensors on the network. The distributed sensors can be "Road-Side Units" (RSUs). [i.29] and [i.27] propose the use of distance-bounding in vehicular networks. This method relies on the speed of light and the message timestamp to verify the distance from the source of the signal. Additionally, [i.51] uses the Received Signal Strength Indicator (RSSI) in its location verification process. [i.40] uses the "Angle of Arrival" (AoA) and Doppler frequency measurement of the received signal to detect false positions and speed by misbehaving vehicle and track it despite the misbehaviour. Due to the nature of propagation of electromagnetic waves, the accuracy of physical layer detection mechanisms can be disputed.

Data-centric detection

This mechanism uses the semantics of the messages to determine its trustworthiness. "Vehicle Behaviour Analysis and Evaluation Scheme" VEBAS [i.50] proposes the use of multiple data-centric mechanisms such as:

- "Acceptance Range Threshold" (ART);
- "Minimum Distance Moved" (MDM);
- "Map-Proofed Position" (MPP); and
- "Sudden Appearance Warning" (SAW).

The multiple methods are combined using "Exponentially Weighted Moving Average" (EWMA). [i.34] proposes a method that combines the mechanism from VEBAS and a plausibility model to check intersection of multiple vehicles. [i.26] improves on the ART by creating "enhanced Acceptance Range Threshold" (eART) where the acceptance range is similar to a Gaussian curve instead of a fixed threshold. The Gaussian approach is better for combining eART with other mechanisms.

Machine-learning based detection

These mechanisms are based on multiple, usually data-centric, basic detectors. These detectors are then fused using machine learning to assess the overall behaviour of a certain neighbouring station. Van der Heijden et al. introduced "Vehicular Reference Misbehavior" (VeReMi) dataset [i.56]; it is a misbehaviour detection dataset created with the VEINS simulator and using the LuST network scenario. VeReMi contains five types of misbehaviour:

- Fixed Position;
- Fixed Position Offset;
- Random Position;
- Random Position Offset; and
- Eventual stop.

So in [i.56], Van der Heijden et al. trained and tested multiple machine learning models using the VeReMi dataset [i.41]. The solution used plausibility checks as an input feature vector for the machine learning models. The study aimed on creating a baseline machine learning solution and tested "K-Nearest Neighbours" (K-NN) and "Support Vector Machine" (SVM). Both algorithms performed similarly with SVM having a slight edge. Singh et al. proposed a similar solution on the VeReMi dataset [i.55]. The study tested SVM and logistic regression with SVM as the better performer. Singh et al. also proposed a deep learning-based solution that tested "Multi-Layer Perceptron" (MLP) and "Long Short-Term Memory" (LSTM) [i.54]. LSTM is the better performer although at the cost of more computational time. Finally, Kamel et al. published a comparison between different local detection mechanisms including the previously discussed machine learning based methods [i.31].

Neighbour list exchange

Studies from [i.51], [i.36] propose a protocol that relies on vehicles broadcasting a list of neighbours. The broadcasted list should include unique identifiers for neighbours such as the hash of the last beacon. Calculation then determines the legitimacy of each node according to the neighbours list and the range of each vehicle. Sybil attackers could then be reported or excluded from the network.

Additional information exchange

Several studies proposed for local misbehaviour detection use a mechanism that requires the exchange of additional information between neighbouring vehicles. [i.60] combines the data-centric methods used in [i.50] and the proactive exchange of neighbour tables. [i.26] combines the eART and the proactive neighbour exchange using subjective logic [i.53]. [i.23] proposes a method that relies on statistical model where vehicles calculate and broadcast a flow parameter. The flow parameter is calculated based on the density and speed of vehicles in a fixed range and thus the flow for neighbouring vehicles has to be within a certain threshold.

Path history detection mechanisms

[i.24], [i.35], [i.37] propose a model where a vehicle with an "On-Board Unit" (OBU) collects signed timestamps from each RSU it encounters. The theory is that these stamps act as proof that a vehicle had passed a certain RSU. Each vehicle is required to broadcast collected stamps. Since a Sybil attacker can only have one physical path, a group of vehicles with a similar collection of stamps is considered suspect of a sybil attack.

RSU pseudonym linkability

Some studies rely on a system where in some way pseudonyms have to be linked. Linking pseudonyms would enable the detection of a sybil attacker using the certificates issued for the same vehicle. [i.46] introduced "Privacy-Preserving Detection of Abuses of Pseudonyms" (P2DAP), a method which enables linkability at RSU level by using pseudonyms which hash a common value. Similarly, "Detection Technique against a Sybil Attack" (DTSA) [i.52] suggests that each vehicle verifies the identity of neighbouring vehicles with the help of a server, accessible via RSUs.

5.1.3 False warning detection

Data-centric detection

[i.59] and [i.27] rely on the assumption that a vehicle emitting a warning event should behave accordingly. For example, a vehicle issuing a blocked road warning needs to be on a proximity of the event and needs to change its path accordingly to avoid the obstacle. A vehicle issuing a warning event is thus monitored by receiving vehicles to determine the message authenticity.

Voting-based detection

Some studies have proposed voting or cooperative validation of an event to ensure integrity. This mechanism proved effectiveness in a densely populated network with an honest majority. [i.39] proposes the validation of an event based on signatures, the signatures are collected and distributed using Growth Code [i.63]. [i.47] proposes a method with a "Certainty of Event" (CoE) curve. The CoE is calculated using a combination of mechanisms, one of which is the reports from other vehicles. [i.48] considers a system where an event becomes valid if the number of witnesses exceeds a certain threshold, then proceeds to evaluate multiple threshold-based event validation algorithms.

5.1.4 Node trust evaluation

In this clause detection methods estimating trust in the vehicle rather than the correctness of messages separately are evaluated. Therefore, each message from a corresponding node (i.e. beacon and warning messages) will be evaluated according to its trust level.

Reputation-based methods

Reputation is the trust built in a vehicle over time. [i.47] presents a mechanism to assess the trustworthiness of an incoming message based on multiple factors, one of which is the reputation of the vehicle issuing the message. A vehicle's trust increases if it reports a true alert and decreases otherwise. It is worth noting that, although the combination of different mechanisms increases the efficiency of the method, it inherits all the feasibility challenges.

Cooperative trust establishment

The two main methods to cooperative trust are voting and consensus mechanisms, see e.g. "Local Eviction of Attackers by Voting Evaluators" (LEAVE) [i.43], and "Suicide-based Local Eviction Protocol" (SLEP) and "Permanent Revocation Protocol" (PRP) [i.49]. Consensus mechanisms have also been studied. [i.22] proposes a method that builds trust using data centric mechanisms (like the MDM) then exchanges trust scores with neighbouring vehicles to help them build transitive trust relations. [i.58] introduces a novel "Trust architecture for Vehicular Networks (T-VNets) using the standardized messaging services of ETSI ITS", a method that proposes to build trust on using a combination of different mechanisms: data-centric, event-based, watchdog, RSU-based trust. The trust level is shared between nodes using "Cooperative Awareness Messages" (CAMs) and regularly updated.

Data-centric trust evaluation

Data-centric methods evaluate trust without using cooperation between vehicles. This approach would reduce the risk of a sybil attack. [i.38] proposes a method that evaluates trust based on:

- the type of the vehicle (police vehicle, emergency vehicle, etc.);
- the event-specific trustworthiness (trust based on the relation of the event to the emitting vehicle);
- the dynamic trustworthiness (based on the revocation status); and
- the time and location indicators such as the proximity to the event.

Local pseudonym linking

In order to circumvent the issue of pseudonymity for the trust establishing mechanisms, some methods propose solutions to achieve an implicit linkability between pseudonyms. The main idea is to analyse the beacon messages to estimate the trajectory of a vehicle. [i.57] proposes a method that uses Kalman filters for trajectory prediction and vehicle tracking; therefore, implicitly linking the pseudonyms. [i.45] discusses the opportunities of wireless fingerprinting for node identification. The result of the simulations claims a high success rate in the detection of sybil attacks. Both methods could be used with any node-based detector to increase the integrity of honest nodes.

5.1.5 Feasibility assessment

Table 1 presents a feasibility assessment of the techniques introduced in clause 5.1 within the constraints imposed by cost, regulation and current state of the standardization process. In detail, the three considered criteria are:

- **Standard:** does the method conform with current standards? (yes, no, partially)
- **Privacy:** is the method likely compliant with current privacy-related regulations? (i.e. in the European Union compliant with the GDPR) (yes, no, partially)
- **Equipment:** does the method work with equipment compatible (in cost and complexity) with the deployment on a vehicle? (yes, no, partially)

Details on the assessment methodology may be found in [i.28] and [i.62].

It is important to underline that this does not constitute in any form an assessment or a comparison of the performance of the different methods.

Table 1: Feasibility assessment of techniques

	Method	References	Standard	Privacy	Equipment
False beacon information detection (clause 5.1.2)	Physical layer: RSU triangulation	[i.25], [i.29]	yes	yes	partially
	Physical layer: signal properties	[i.51], [i.27], [i.29], [i.40]	yes	yes	partially
	Data-centric	[i.50], [i.34], [i.26]	yes	yes	yes
	Machine learning based	[i.56], [i.41], [i.55], [i.54], [i.31]	yes	yes	partially
	Neighbour list exchange	[i.36], [i.51]	partially	partially	yes
	Additional information exchange	[i.26], [i.60], [i.23], [i.50], [i.53]	partially	partially	yes
	Path history detection mechanisms	[i.24], [i.35], [i.37]	no	no	partially
	RSU pseudonym linkability	[i.46], [i.52]	partially	partially	partially
False warning detection (clause 5.1.3)	Data-centric	[i.59], [i.27]	yes	yes	yes
	Voting-based	[i.39], [i.47], [i.48], [i.63]	partially	yes	yes
Node trust evaluation (clause 5.1.4)	Reputation-based	[i.47]	no	no	yes
	Cooperative	[i.43], [i.49], [i.22], [i.58]	no	partially	yes
	Data-centric	[i.38]	partially	yes	yes
	Pseudonym linking	[i.57], [i.45]	yes	partially	yes

5.2 Reporting approaches

5.2.1 General

After a "Misbehaviour" (MB) is detected, "Misbehaviour Reporting" (MBR) addresses the question of:

- what should be the content of an MR;
- using which (communication) protocol; and
- to whom such MR should be communicated.

In the literature, attention is mostly given to misbehaviour detection, so MB reporting is often implicitly or offhanded discussed. Nevertheless, [i.61] and [i.33] have investigated carefully what to be included in MB reports.

On the question of what should be included in an MR, there is general agreement in principle that an MR should include sufficient evidence of the misbehaviour to establish the credibility of the report so that the receiving party is able to verify the misbehaviour independently. This should include the original message, the specific parts of the messages that is believed to be incorrect (i.e. misbehaving), and on what basis such determination is made, i.e. the specific detection scheme employed by the ego vehicle. [i.33] specifically calls out "reliability and proof-based" as one of the requirements for an MR, specifically such that the MA is able to recompute the same misbehaviour checks and get the same reported results using the input data from the report. Similarly, [i.56] proposes "*every report contains an evidence of the observed event. For example, in the case of an observed relevant position overlap two signed CAMs are added proving the overlap of vehicle polygons*". In addition to the pseudonym of the reporter node and a list of suspected nodes, [i.56] also proposes to include a subset of the one-hop neighbours surrounding the reporter in its MR, prioritized by the distance between the respective neighbour and the location of the misbehaviour. The author argues that the list of neighbours is relevant for the central MA in order to decide a misbehaviour event has really happened or an attacker is just using received messages from benign nodes to discredit them. The MA may corroborate reports from the neighbours who may be able to witness or refute the same misbehaviour.

Given the variety of detection mechanisms described in clause 5.1, it seems to be necessary to standardize a set of related detection algorithms or at least categories of promising algorithms with sufficient detail, such that an MR can be specified based on the algorithm that detected the MB. [i.33] points out that flexibility and extensibility is also important so that the MR can be extended in order to integrate new misbehaviour checks and new data proofs.

Clauses 5.2.2 and 5.2.3 discuss the state of the art in answering the question of what protocol and to whom an MR should be communicated with. One complicating factor is that some of the cooperative detection mechanisms proposed in the literature rely on MRs shared among participants. However, MR sharing incur additional security and privacy challenges, and an alternative approach that relies on collective perception may achieve the similar intent but avoids the potential pitfall better.

5.2.2 Unicast MR to the misbehaviour authority

After a misbehaviour is detected, the vehicle should generate an MR and submit it to the MA at the backend, more specifically, to CCMS misbehaviour reporting and action components (see Figure 1), via unicast mechanism which may require networked communications including nodes in the infrastructure. Such messages should be integrity and confidentiality protected. Once the misbehaviour is confirmed, CCMS revocation components (see Figure 1) can decide to revoke the misbehaving stations system-wide and hence remove the potential harm such stations may impose to the ITS.

With roadside ITS stations having reliable connectivity to the backend, vehicles can submit MRs to the MA at the backend via such roadside ITS stations. In [i.56], the MA sends to the reporting vehicle an acknowledgement when receiving the MR successfully. The vehicle may buffer its MR until it receives the acknowledgement from the MA. Then the vehicle may delete the local copy of the MR.

NOTE: An acknowledgement, as presented in [i.56], may not reach the destination ITS station via the same roadside ITS station due to the movement of the destination ITS station

If a reporting vehicle has no direct communication connectivity to RSUs or base stations, it may use other vehicles to relay an MR to the MA. This can help reduce the latency of misbehaviour reporting due to intermittent connectivity to the backend and increase the chance for an MR to reach the MA before it is dropped from the local buffer.

5.2.3 Broadcast MR to neighbours: pros, cons and alternatives

[i.44] catalogues and analyses over 40 different MB detection mechanisms in the literature and there are about 19 local detection mechanisms and 19 cooperative additional ones. Sharing of MRs with neighbours via broadcast is either implicitly or explicitly required by some of the cooperative detection mechanisms proposed in the literature.

For example, VEBAS [i.50] as summarized in clause 5.1.2 is a cooperative reputation system that is built on local ratings which in turn are based on the use of multiple data-centric mechanisms. By combining the output of these mechanisms, each vehicle is assigned a trustworthiness value which may be additionally exchanged among all vehicles, building up reputation. Based on this information, vehicles are classified into trustworthy, untrustworthy or neutral. The authors recognize the danger of "Trust Distribution Loops", and specifically stated that "*the exchange of reputation should be limited to local ratings. The aggregation of local and cooperative ratings should not be sent out to prevent falsely increased trust values caused by loops. Hence, a one-level reputation system is required*". Mechanisms that involve MR sharing with neighbours face two major challenges:

- First of all, an MR reflects an opinion of the sender. MRs are susceptible to Sybil attacks. Multiple fake MRs can be generated even if the attackers compromise only a single station. For example, a sybil attack may easily compromise the cooperative reputation scheme in [i.50].
- Secondly, there may be additional privacy concern as the observed original message (e.g. CAM or DENM) is likely to be included as part of the evidence in an MR and hence rebroadcast.

Not all cooperative detection mechanisms require MR sharing with neighbours. Instead of sharing the result of local MB detection, the other approach is to exchange additional information between the vehicles that is helpful to the MB detection. For example, [i.60] and [i.22] position verification against falsified position data is based on network logical structure information shared in the form of neighbour tables by each vehicle. Each vehicle checks logical consistency of the neighbour tables received from different neighbours and perceived by the ego vehicle.

Along the same line, recently ETSI started the effort to define "Collective Perception" (CP) [i.10], the concept to share the perceived environment of an ITS station based on perception sensors. While CP is envisioned primarily to benefit safety applications, CP also can benefit MB detection because it mitigates a fundamental limitation in CAM that is lack of redundancy as each CAM only contains information about the ego vehicle. Misbehaviour detection relies on redundancy of information and so the addition of CP should help misbehaviour detection to look for data inconsistency more effectively. In [i.30] a generic perception model is assumed where vehicles periodically exchange lists of perceived objects and techniques for object tracking, association and fusion can be used to not only merge consistent observations from different witnesses, but also detect where inconsistency happens as evidence for misbehaviours. [i.32] introduces a probabilistic model using Bayes theorem to recursively estimate a belief that a pair of entities, e.g. two remote vehicles or the ego vehicle and a remote vehicle, are both trustworthy. The method updates the belief based on the consistency of the data that both entities provide. These early works show promising results in misbehaviour detection by leveraging the collective perception shared among the neighbours.

6 MD and MR - use cases and scenarios

6.1 Use case 1: Plausibility checks on access layer measurements on periodic broadcast messages (CAMs)

The ITS access layer can collect various types of data upon packet reception. Data derived from RF signals provide a view of the physical connection between the transmitter and the receiver. This data can be used for security analysis by comparing the measurements with models of expected communication for identifying anomalies which may be analysed to isolate misbehaving stations in the V2X system.

Several access layer properties can be measured, such as

- "Receive Signal Strength Indicator" (RSSI);
- Doppler shift; and
- "Angle-of-Arrival" (AoA).

RSSI represents the power present in the radio signals during reception of packets. The RSSI data may be correlated with the distance from the transmitter based on assumptions of transmit power, directivity of the transmitter antenna, path loss (dependent on propagation model), and receiver directivity. The signal level could match expected ranges for the distance; an abnormally high signal level (in related to measured distance from the transmitter) may be a sign of a misbehaving entity.

Doppler shift depends on the relative speed between transmitter and receiver, the carrier frequency and Line-of-Sight condition. For speed validation, the measured Doppler shift can be compared with the expected one based on the relative speed and heading between the ego vehicle and the transmitting vehicle.

The AoA gives the direction of the transmitter from where the signal arrived at the receiving antenna. RSSI and AoA could be jointly used for location verification.

This self-analysis can help to monitor and detect discrepancies between the location reported by the transmitting vehicle and a possible location based on access layer measurements.

6.2 Use case 2: Plausibility checks on periodic broadcast messages (CAMs)

Any ITS station (fixed or mobile) which receives periodic broadcast messages (CAMs) from a given "Vehicle ITS-S" (V-ITS-S) identified by its *StationID* should perform simple plausibility checks on the received CAMs to detect suspicions on a misbehaving vehicle, and should report the detected abnormal behaviour of the ITS-S transmitting the suspicious messages to a global misbehaviour authority (running on a central back-end server). As presented in ETSI TR 102 893 [i.11] (threat analysis), the global misbehaviour detection uses the received reports containing direct or probabilistic evidences to recognize the type of misbehaviour and makes the decision about misbehaving ITS-S, e.g. to revoke the certificates (ATs) of misbehaving ITS-Ss.

Many basic plausibility checks use the vehicle movement information that is provided in each incoming CAM. At least, the ITS station should perform basic checks using the CAM movement data (such as the vehicle position, heading and speed, etc.): these CAM parameters are contained in the *BasicContainer* and in the *BasicVehicleContainerHighFrequency* as specified in ETSI EN 302 637-2 [i.5]).

Table 2 shows minimum data elements used for these basic plausibility checks. Other data elements may also be necessary for some of the detection mechanisms included in this use case such as: *VehicleLength, VehicleWidth, StationType*.

Table 2: CAM data frames/data elements as specified in ETSI TS 102 894-2 [i.6]

	Included in	Contains data elements
DF ReferencePosition	BasicContainer	
DF Heading	BasicVehicleContainerHighFrequency	HeadingValue, HeadingConfidence
DF Speed	BasicVehicleContainerHighFrequency	SpeedValue, SpeedConfidence
DF DriveDirection	BasicVehicleContainerHighFrequency	-
DF LongitudinalAcceleration	BasicVehicleContainerHighFrequency	LongitudinalAccelerationValue AccelerationConfidence
DF Curvature	BasicVehicleContainerHighFrequency	CurvatureValue CurvatureConfidence CurvatureCalculationMode
DF YawRate	BasicVehicleContainerHighFrequency	YawRateValue YawRateConfidence

The following basic detection methods should be performed in receiving ITS stations (see the state-of-the art analysis in clause 5):

Maximum beaconing frequency: Detects violations of common maximum beaconing frequencies.

CAM generation frequency rules are specified in ETSI EN 302 637-2 [i.5]. CAM transmission frequencies as specified by current ETSI application requirements standards (ETSI TS 101 539-1 [i.1], ETSI TS 101 539-2 [i.2] or ETSI TS 101 539-3 [i.3]) are allowed to vary between 100 ms and 1 000 ms. This corresponds to a transmission rate between 1 Hz and 10 Hz.

The CAM transmission frequency is varying, for instance depending on the channel usage requirements of DCC for ITS-G5 channels, and on the vehicle kinematics. A new CAM is generated once one of the following conditions is satisfied since the previously sent CAM:

- the vehicle orientation (heading) has changed by more than 4 degrees;
- the position of the vehicle has changed by more than 4 m;

- the vehicle speed has varied by more than 0,5 m/s (1,8 Km/h).

The previous verifications are done every 100 ms.

As an example, a vehicle traveling at a speed higher than 180 km/h would send 10 CAMs per second (it will have moved more than 5 m at each check). Similarly, a vehicle traveling in a straight line at 50 km/h will send just under 2 CAMs per second, and at 90 km/h, it will send 5 CAMs per second.

Message Content Verification: A preliminary list of plausibility checks try to categorize CAMs as suspicious by checking the physical implausibility of mobility data in received messages such as position, heading, speed, acceleration.

If the station type is a passenger car, the preliminary plausibility checks should identify as implausible any received CAM for which the vehicle mobility data are outside the values as specified in Table 3.

Table 3: CAM data field values (passenger vehicles)

DF Speed	Speed greater than 70 m/s (252 km/h)
DF LongitudinalAcceleration (positive LongitudinalAccelerationValue)	Longitudinal acceleration of 0-100 km/h in fewer than 2,3 seconds (greater than 12 m/ s²)
DF LongitudinalAcceleration (negative LongitudinalAccelerationValue)	Longitudinal deceleration of 100-0 km/h in fewer than 28,95 m (greater than 12 m/s²)
DF Curvature	Curvature radius of smaller than 3,9 m
DF YawRate	Yaw rate of greater than 1,5 radian/s

The plausibility checks depend of the type of vehicle: for different types of vehicles specified in `DE_StationType` in [i.6] such as motorbikes, bus, trucks, other values for the plausibility checks on above data should be defined.

As introduced in the US NPRM [i.20] and evaluated in the CV Deployment program's test sites e.g. in Tampa [i.19], the detection mechanisms can be split as level 1 or level 2 checks. The basic plausibility checks above are consisting of level 1 plausibility checks. They can be complemented by level 2 consistency checks which make use of multiple, successive CAMs received from the same neighbour ITS station. E.g. in [i.20], the following level 2 checks are specified:

- motion validation; and
- proximity plausibility.

Table A.1 presents level 1 and level 2 misbehaviour detectors specified on CAMs using the list of minimum data frames/data elements of the CAMs defined in Table 2.

More complex plausibility checks may also be provided. They are categorized as:

- level 3 (map based), e.g. the plausibility of vehicle data may depend on the type of road or driving conditions (e.g. drive on a curvy road which does not allow to drive over a certain speed);
- level 4 (combining with the on-board sensors data).

These level 3/4 detection methods are not considered in this clause.

6.3 Use case 3: Security level local checks on received C-ITS messages

In this use case, the detection of misbehaving ITS stations is performed by using security checks on messages received from neighbouring ITS stations.

NOTE 1: Since the check of coherence of SSP permissions and message content is optional, it might be possible for non-genuine messages to pass the security checks without being rejected. Moreover, this type of misbehavior reporting is advocated in the TVR analysis ETSI TR 102 893 [i.11].

Any ITS station (fixed or mobile) which receives secured broadcast messages from a neighbouring station performs the local security checks as specified in ETSI TS 103 097 [i.9]: all the incoming secured messages should only be accepted if all of the secured message consistency validation steps and cryptographic checks as specified in [i.9] are successful.

NOTE 2: The incoming secured message should only be accepted by the receiver if the security level checks are successful and if the payload of the secured message is consistent with the ITS-AID and SSP in the certificate and with the security profile as defined in the application or service specification standard.

The receiver ITS station can report the detected failed security checks using its security processing services and sends these reports to the MA.

Table 4 shows a list of security tests based on ETSI TS 103 097 [i.9] and ETSI TS 103 096-2 [i.8] for CAM, DENM, or generic security profile (e.g. used for infrastructure messages).

NOTE 3: C-ITS services have associated security profiles and define appropriate application-level permissions, using the corresponding ITS-AID/SSP. The process for checking the message payload consistency with the certificate's application permissions is specified in each application/facilities message standard. These checks are not covered in Table 4.

Table 4: Security level checks

Octet Position	Bit Position	Security level check	Bit Value
1	0 (80h) (MSBit)	Time stamp (generation_time)	0: passed
			1: failed
1	1 (40h)	Region/Geographic region	0: passed
			1: failed
1	2 (20h)	Certificate validity period	0: passed
			1: failed
1	3 (10h)	Ascending order of header fields	0: passed
			1: failed
1	4 (08h)	Presence of ITS-AID_SSP list	0: passed
			1: failed
1	5 (04h)	No duplicate ITS- AID	0: passed
			1: failed
1	6 (02h)	ITS-AID in certificate are also in the parent certificate	0: passed
			1: failed
1	7 (01h) (LSBit)	Digest will be included	0: passed
			1: failed
2	0 (80h) (MSBit)	Structure of the signature	0: passed
			1: failed
2	1 (40h)	The payload is present and its length is not null	0: passed
			1: failed
2	2 (20h)	reserved for future usage	0: passed
			1: failed
2	3 (10h)	reserved for future usage	not used, set to 0
2	4 (08h)	reserved for future usage	not used, set to 0
2	5 (04h)	reserved for future usage	not used, set to 0
2	6 (02h)	reserved for future usage	not used, set to 0
2	7 (01h) (LSBit)	reserved for future usage	not used, set to 0

6.4 Use case 4: Misbehaviour detection on the DENM messages signalling a traffic event

The Decentralized Environmental Notification (DEN) basic service is part of the basic set of applications of the ITS system as specified in ETSI TS 102 637-1 [i.4]. A DENM (DEN message) is transmitted for various traffic events and road hazard signallings. Three mechanisms have been identified to verify the plausibility of these messages: consensus-based validation, environmental-based validation and behavioural-based validation.

Behavioural-based validation:

This mechanism is based on the fact that a Vehicle ITS-S sending a specific signal is behaving accordingly. The first verification is that the ITS station is within line of sight of the signalled traffic event: the receiver should check the consistency of the detected event location with the location of the ego-vehicle contained in its transmitted CAMs.

Additional verification is based on the behaviour of the vehicle with respect to this specific warning. For instance, a vehicle issuing a road work warning or a traffic congestion warning should decrease its speed accordingly.

Consensus-based validation:

This mechanism validates a certain event, based on a general agreement between neighbouring stations.

This mechanism is generally used by mobile applications providing traffic event warning services. In the case of mobile applications, this mechanism generally works well and is currently largely validated.

However, the ITS privacy protection currently in place would interfere with such a detection mechanism. For instance, in the case of mobile applications, a user misbehaving in the past would affect its ranking in the current consensus. But in this use case, the consensus-based approach is limited due to the pseudonymization mechanism applied in ITS system for the user privacy and data protection. Additionally, using various pseudonym identities a single hacked ITS-station could use multiple identities at once to signal a new warning or to negate an existing one.

This mechanism may be useful in the ITS system when combined with other validation mechanisms, e.g. to detect forged traffic events.

Environmental-based validation:

This mechanism is based on the fact that some warnings are more or less probable depending of the road environment. This validation method is therefore specific to each traffic event/road warning type.

For instance, a warning for an adverse weather condition on visibility or precipitation could be verified using already known local weather information. A traffic congestion warning could be validated by the traffic trends in the region in a particular day or week time. Finally, traffic accidents could be verified by the data trends on a certain portion of road.

NOTE: The previous validation mechanisms may be implemented by R-ITS-S or Central ITS-S when processing e.g. filtering and aggregating information received from DENMs transmitted by vehicles.

If a set of warnings largely deviates from the normal data trends, a human operator in the TCC should be notified. Partly because the warning could be erroneous, and partly because the warning could be due to a change in the local environment that could require servicing.

7 Misbehaviour detection and reporting architecture

7.1 General

The misbehaviour reporting process is illustrated in Figure 2.

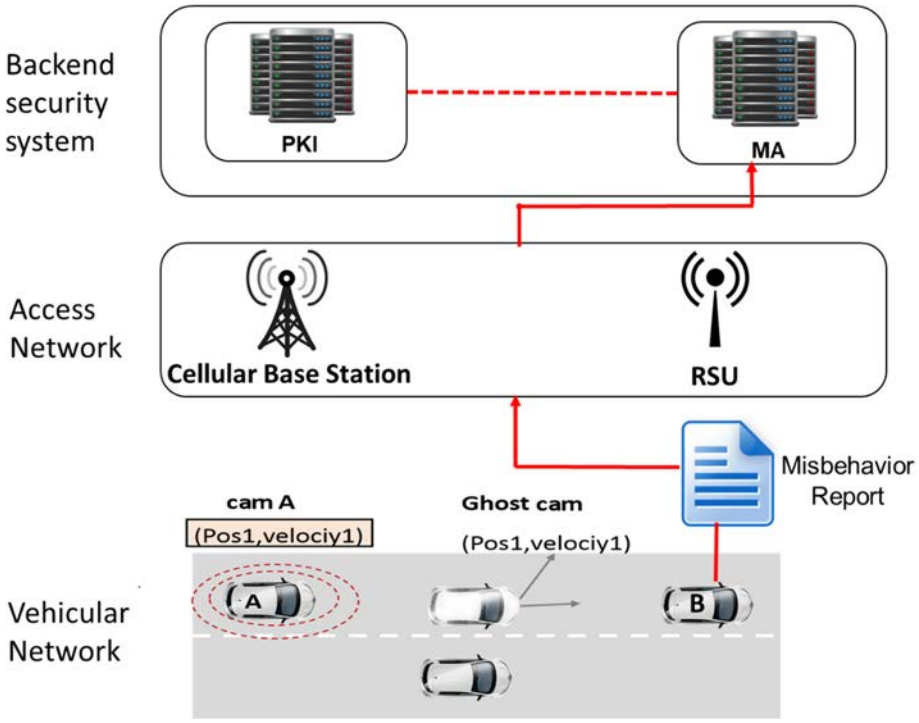


Figure 2: Misbehaviour reporting use case

The misbehaviour detection process is divided into three steps.

Local Misbehaviour Detection

The local misbehaviour detection is performed by every ITS station. The goal is to detect potentially misbehaving neighbouring ITS stations. Every received message should be subject to a set of individual plausibility and consistency inspections (see Table A.1). These detectors are then analysed by a fusion process (application) to decide on the need to send an MR to the MA. The local detection process is illustrated in Figure 3.

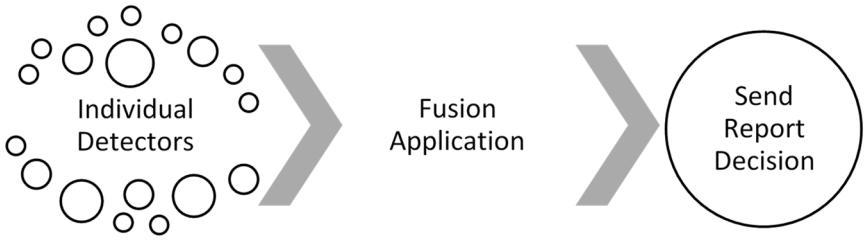


Figure 3: Local Misbehaviour Detection Process

Misbehaviour reporting

The reporting process begins as soon as an ITS station detects an implausibility and the fusion process decides to report it. The ITS station then collects the evidence required to prove and recreate a misbehaviour on the global level. After collecting enough evidence, an MR is created and sent to the MA. Figure 2 shows this action performed by the vehicle B.

Global Misbehaviour detection

The MA has a role of collecting and analysing the received reports. Using the reports, the MA should be able to distinguish between false positive and genuine reports. Moreover, if a misbehaviour is detected, the MA should be able to determine the type of misbehaviour. The severity and type of misbehaviour may be used to determine the suitable reaction required to protect the system and mitigate the misbehaviour effect.

7.2 Misbehaviour report message format

This clause presents basic functionality of the "Misbehaviour Report" (MR) message which should be generated and reported by a reporter ITS station (fixed or mobile) which detects a misbehaving (reported) ITS station. The functional requirements of the misbehaviour reporting mechanism are specified, as well as the security, privacy requirements. The MR message format and its contained data information are exemplified such as to provide reliable evidences for the analysis of the central "Misbehaviour Authority" (MA).

For each detected misbehaviour type, an ITS station should provide the corresponding proofs to be included in the MR. The latter is an indication that enables to differentiate non-forged proofs and self-forged proofs (i.e. if a proof could be forged by the reporting entity).

The "Misbehaviour Detection" (MD) is based on a set of plausibility and consistency checks as shown in Table A.1. This set of checks is performed by a vehicle when receiving a message such as a Cooperative Awareness Message (CAM) or a Decentralized Environmental Notification Message (DENM)). When a vehicle (ego vehicle) detects a misbehaviour, it generates an MR and sends it to the MA. As the reporting is not a real time process, the report is sent to the MA when connectivity is available via a suited network. The MA should perform sufficient data analysis to investigate whether a misbehaviour has occurred or not. A vehicle does not wait for a decision response about the reported node from the MA, but may receive an acknowledgement from the MA upon proper provisioning of an MR.

In Table A.1, the analysis is focusing mainly on the CAM message. However, similar approaches for the misbehaviour evidence could be applied for other types of messages.

The misbehaviour reporting process should fulfil the following requirements:

- **Privacy protection:** The MA should not be able to link the short term and the long-term identity of the reported ITS station as well as the reporter ITS station. The reporter ITS station uses its pseudonym certificates (a.k.a. Authorization Tickets) to communicate with the MA.
- **Confidentiality and authenticity:** MRs sent by a reporting ITS station should be encrypted to protect the confidentiality of the information sent to the MA, which includes the identity of the reported ITS station, the detected misbehaviour type and collected evidences on the detected misbehaviour. MRs sent by an ITS station should be signed with the private key corresponding to the verification public key of the valid "Authorization Ticket" (AT) of the sending ITS station to ensure the integrity and authenticity of the data.
- **Efficiency and minimum resource consumption:** MRs should not overload the communication channel. The reporting process should avoid sending repetitive and redundant information about the same misbehaviour.
- **Reliability and proof-based:** A reporter ITS station should integrate the required proofs of the misbehaviour: using the input data from the reporter ITS station, the MA should be able to recompute the same misbehaviour checks and get the same reported results.
- **Flexibility:** The definition of MRs should be extensible in order to integrate new misbehaviour checks and new data proofs at a later stage without breaking backward compatibility, if needed.

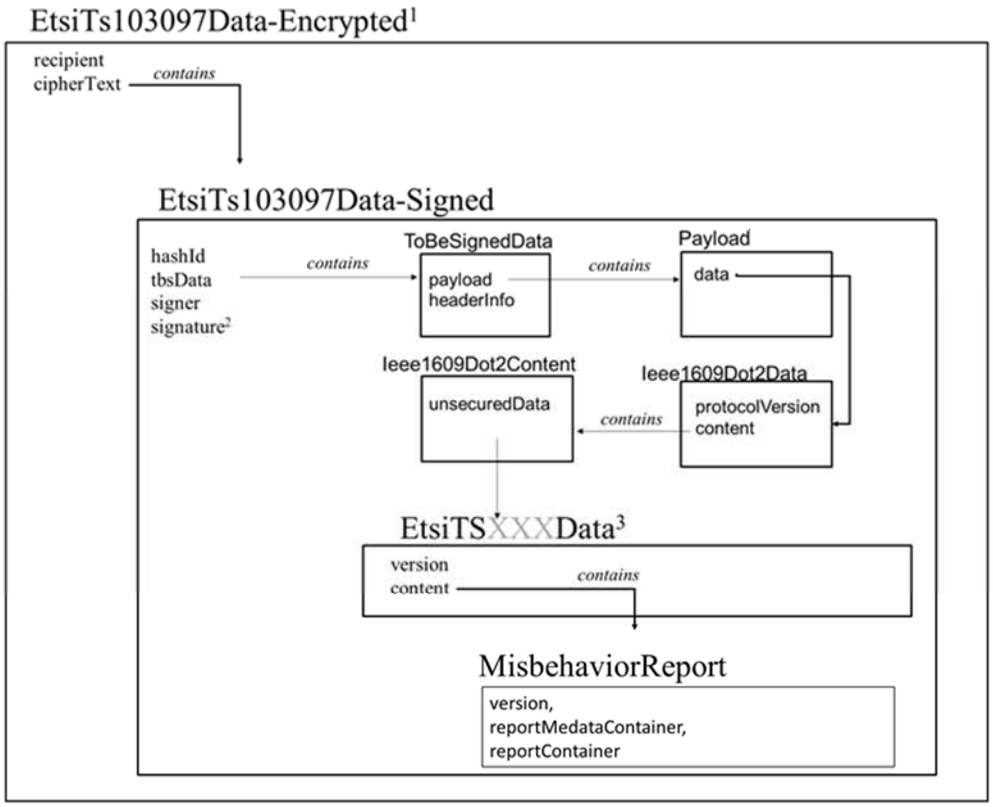
An example report format is provided in Annex B to exemplify basic functionality of an MR message. Its design supports multiple key features:

- reducing overhead by relating messages;
- authenticating the reporter and reported ITS station with their AT;
- specifying the type of misbehaviour;
- specifying the evidences required for each misbehaviour type specified in the present document.

The data structures in the present document are defined using Abstract Syntax Notation 1 (ASN.1). It is recommended to apply Canonical Octet Encoding Rules (COER) as defined in Recommendation ITU-T X.696 [i.12].

The topmost component of an MR message is the MisbehaviorReport data structure presented in the informative Annex B. It should be included in an overall EtsiTs103097 secure data structure as shown in Figure 4.

This example message is composed of two containers: the *reportMetadataContainer* and the *reportContainer*.



[1] Encryption is done with ECIES using the public encryption key of the MA
[2] Signature is computed using the current valid AT verification private key
[3] Depends on the standard where the misbehavior detection protocol will be defined

Figure 4: Example structure of secure misbehaviour report message

A reporter ITS station should refrain from reporting a misbehaving station that is continuously misbehaving. Instead, the ITS station should send an initial report, then wait whilst collecting evidences. After a certain time period, the reporter ITS station sends a new report that includes the information of the *RelatedReportContainer* allocated in the *ReportMetadataContainer*. The *RelatedReportContainer* contains the ID of the initial report and the number of omitted reports.

However, if in the meantime the reporter ITS station changes its pseudonym (AT), the report should not include the initial report ID. This protocol would indeed prevent the linkability of the reporter pseudonyms by the MA thus ensuring the reporter privacy.

Additionally, the report format requires at least one pseudonym certificate (AT) of the reported ITS station in the *ReportedMessageContainer* contained in *ReportContainer* to be valid. The type of misbehaviour is indicated in the *MisbehaviorTypeContainer* contained in *ReportContainer*. The failure may be on a security issue or a semantic issue. In case of failure on the security level, an appropriate error code should be presented; e.g. in the given ASN.1 example presented in an OCTET STRING (Table 5). Every bit set to one identifies a failed security test. This error code should be designed in support of all the security tests specified in the ETSI Technical Specifications ETSI TS 103 097 [i.9] and ETSI TS 103 096-2 [i.8].

Table 5: Description of `securityDetectionErrorCode`

Octet ID	Bit ID	Security Reference
0	0	Time stamp (generation time)
0	1	Region/GeographicRegion
0	2	Certificate validity period
0	3	Ascending order of hearder fields
0	4	Presence of AID (Application-ID) ssp list
0	5	No duplicate AID
0	6	AID in certificate are also in the parent certificate
0	7	Digest will be included
1	0	Structure of the signature
1	1	The payload is present and its length is not null
...	...	...

In case of a failure on a semantic issue, the error code depends on the type of the message included in *ReportedMessageContainer*. In the case of a CAM, the failure is linked to one or more data fields shown in Table A.1. Therefore, in this example, the OCTET STRING containing the error code should point to the relevant data fields (Table 6).

Table 6: Description of `semanticDetectionErrorCodeCAM`

Octet ID	Bit ID	Data Field
0	0	ReferencePosition
0	1	Heading
0	2	Speed
0	3	DriveDirection
0	4	VehicleLength
0	5	VehicleWidth
0	6	LongitudinalAcceleration
0	7	Curvature
1	0	YawRate
...	...	...

Furthermore, Table A.1 includes the required evidences to recreate the misbehaviour checks defined by detection/evidence level. This allows to determine what evidence should be included in the *EvidenceContainer* contained in *ReportContainer* based on the error code and the detection/evidence level.

The *EvidenceContainer* allows for different optional components. It can include a list of ITS messages from the reported vehicle and from neighbouring ITS stations. It can also include the information about the sender of the MR (reporter ITS station), notably in case of a level 4 detection. It is also to be noted that the detection/evidence level is correlated with the reliability of the report. In case of a CAM, the detection levels 1 and 2 entail signed messages of the reported vehicle as evidence. This type of evidence cannot be forged. Consequently, the event should be confidently reproduced by the MA. A level 3 is based on the environment and surrounding messages. The environment information (e.g. map) may be inaccurate and the surrounding messages may be forged with a sybil attack. Finally, a level 4 is based entirely on the reporting of ego vehicle's sensors, thus the evidence may be forged with minimal effort.

8 Misbehaviour detection standard recommendations

The present document recommends considering the following guidelines for the development of an ETSI Technical Specification on MR:

1) The MR design should consider applicable detection means identified in the present document.

2) The first edition of an MR design should be restricted to detection means that are urgently needed for early deployments.

3) The MR design should be restricted to detection means that are sufficiently validated.

4) The MR design should be extendible for future functionality.

5) The MR design should be scalable and future-proof by applying ASN.1 Information Object Classes and Information Object Sets.

6) The MR design should consider the functionality reflected by the ASN.1 example code presented in Annex B.

Annex A:
Potential misbehaviour detection mechanisms for "Cooperative Awareness Messages" (CAMs)

Table A.1 presents potential local misbehaviour detection mechanisms related to the content of the received CAMs, i.e. CAM information components with suspicious values, and related evidence issues for four different evidence levels.

Table A.1: Misbehaviour detection mechanisms for CAMs

CAM Data	Detection mechanisms for different evidence levels			
	Level 1	**Level 2**	**Level 3**	**Level 4**
Reference Position	Data unavailable. Confidence too large. Range plausibility.	Position change (PC) too large. PC *Inc*Φ (see note 1) with Speed. PC *Inc*Φ with Heading.	Position not on a road. Position overlap with other vehicles.	Position *Inc*Φ with relative position (Lidar, Radar, RSSI, AoA). Position *Inc*Φ with maximum plausible range.
Heading	Data unavailable. Confidence too large.	Heading change (HC) too large. HC *Inc*Φ with Speed. HC *Inc*Φ with YawRate.	Heading *Inc*Φ with road heading.	Heading *Inc*Φ with relative heading.
Speed	Data unavailable. Confidence too large. Speed value too high.	Speed change (SC) too large. SC *Inc*Φ with acceleration.	Speed *Inc*Φ with road plausible speed.	Speed *Inc*Φ with relative speed (Doppler).
Drive Direction	Data unavailable.	Direction *Inc*Φ with position change & heading. Direction *Inc*Φ with speed.	Direction *Inc*Φ with road way.	Direction *Inc*Φ with perceived direction.
Vehicle Length/Width	Data unavailable.	Length/width change.	-See note 2	Vehicle length and width *Inc*Φ with perceived dimensions.
Longitudinal Acceleration	Data unavailable. Confidence too large. Acceleration value too high.	Acceleration change too large.	-	Acceleration *Inc*Φ with relative acceleration.
Curvature	Data unavailable. Confidence too large. Curve radius too small.	Curvature change (CC) too large. CC *Inc*Φ with Speed CC *Inc*Φ with HC CC *Inc*Φ with YawRate	Curvature *Inc*Φ with road shape.	Curvature *Inc*Φ with relative curvature.
YawRate	Data unavailable. Confidence too large. YawRate value too high.	YawRate change (YC) too large. YC *Inc*Φ with Speed YC *Inc*Φ with Curvature	-	YawRate *Inc*Φ with perceived YawRate.
	Information related to evidence for different evidence levels			
Evidence Required	One reported CAM (At least including a full certificate).	Multiple reported CAMs (At least one including a full certificate).	One Reported CAM (With a full certificate). CAMs of neighbours (With a full certificate each). Map of the area (Already available for the MA).	One reported CAM (With a full certificate). Sender's sensor information (data).
Evidence Reliability	Total	Total	Partial	Minimal to Partial

NOTE 1: *Inc*Φ: inconsistency symbol.
NOTE 2: '-' means that there is no additional check specified for this level.

Detection levels are defined as follows:

- Level 1: Implausibilities within a single message.
- Level 2: Inconsistencies between successive messages.

- Level 3: Inconsistencies with the local environment.
- Level 4: Inconsistencies with respect to perceived physical attributes (based on-board sensors or V2X physical layer techniques).

Detection levels might also be referred to as "Evidence Levels".

An implementation of a misbehaviour detection framework based on these detection/evidence levels is done in the SCA project ([i.33], [i.42]). The detection mechanisms presented in Table A.1 may also integrate the confidence range of the CAM message field into the calculation of the basic plausibility and consistency checks as presented in [i.42].

Annex B:
Example of an ASN.1 MR specification

The example ASN.1 code presented below aims at clarifying the functionality of an MR. In a future Technical Specification of the MR, the ASN.1 code can be different, e.g. more enabling (e.g. with respect of support of more observed messages than just CAM) and future proof applying the concept of Information Object Classes and Information Object Sets.

```
EtsiTr103460MisbehaviorReportMessage { itu-t(0) identified-organization(4) etsi(0) itsDomain(5)
wg5(5) tr(103460) mrm(0) version(1)}
DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

IMPORTS
TimestampIts, StationType, ReferencePosition, Heading, Speed, DriveDirection, VehicleLength,
VehicleWidth, Curvature, LongitudinalAcceleration, CurvatureCalculationMode, YawRate
FROM
ITS-Container {
itu-t (0) identified-organization (4) etsi (0) itsDomain (5)  wg1 (1) ts (102894) cdd (2) version
(1) }

PerceivedObjectContainer, SensorInformationContainer
FROM
CPM-PDU-Descriptions {
itu-t (0) identified-organization (4) etsi (0) itsDomain (5) wg1 (1) tr (103562) cpm (1) version
(1) }

EtsiTs103097Data, EtsiTs103097Certificate
FROM
EtsiTs103097Module {
itu-t(0) identified-organization(4) etsi(0) itsDomain(5)   wg5(5) ts(103097) v1(0) }

;

-- The root data frame for report messages
Version::=INTEGER(0..255) -- this equals Uint8

MisbehaviorReport::= SEQUENCE {
   version Version, -- use value 1
   reportMetadataContainer ReportMetadataContainer,
   reportContainer ReportContainer
}

ReportMetadataContainer::= SEQUENCE {
   reportID IA5String,
   generationTime TimestampIts,
   relatedReportContainer RelatedReportContainer OPTIONAL
}

RelatedReportContainer::= SEQUENCE {
   relatedReportID IA5String,
   omitedReportsNumber OmitedReportsNumber
}

ReportContainer::= SEQUENCE {
   reportedMessageContainer ReportedMessageContainer,
   misbehaviorTypeContainer MisbehaviorTypeContainer,
   evidenceContainer EvidenceContainer OPTIONAL
}

ReportedMessageContainer::= CHOICE {
   certificateIncludedContainer CertificateIncludedContainer,
   certificateAddedContainer CertificateAddedContainer
}

CertificateIncludedContainer::= SEQUENCE{
   reportedMessage EtsiTs103097Data
}

CertificateAddedContainer::= SEQUENCE{
   reportedMessage EtsiTs103097Data,
   reportedCertificate EtsiTs103097Certificate
}
```

```
MisbehaviorTypeContainer::= CHOICE {
   securityDetection SecurityDetection,
   semanticDetection SemanticDetection,
   ...
}

SecurityDetection::= SEQUENCE {
   securityDetectionErrorCode OCTET STRING (SIZE (0..4)),
   ...
}

SemanticDetection::= CHOICE {
   semanticDetectionReferenceCAM DetectionReferenceCAM,
/*
   semanticDetectionReferenceDENM DetectionReferenceDENM,
   semanticDetectionReferenceCPM DetectionReferenceCPM,
   semanticDetectionReferenceSPAT DetectionReferenceSPAT,
   semanticDetectionReferenceMAP DetectionReferenceMAP,
*/
   ...
}

DetectionReferenceCAM::= SEQUENCE{
   detectionLevelCAM DetectionLevel,
   semanticDetectionErrorCodeCAM OCTET STRING (SIZE (0..2))
}

EvidenceContainer::= SEQUENCE {
   reportedMessageContainer MessageEvidenceContainer OPTIONAL,
   neighbourMessageContainer MessageEvidenceContainer OPTIONAL,
   senderInfoContainer SenderInfoContainer OPTIONAL,
   senderSensorContainer SenderSensorContainer OPTIONAL
}

MessageEvidenceContainer::= SEQUENCE OF EtsiTs103097Data

SenderInfoContainer::= SEQUENCE {
   stationType StationType,
   referencePosition ReferencePosition,
   heading Heading,
   speed Speed,
   driveDirection DriveDirection,
   vehicleLength VehicleLength,
   vehicleWidth VehicleWidth,
   longitudinalAcceleration LongitudinalAcceleration,
   curvature Curvature,
   yawRate YawRate,
   ...
}

SenderSensorContainer::= SEQUENCE OF SenderSensorChoice

SenderSensorChoice::= CHOICE{
   sensorInformationContainer SensorInformationContainer,
   perceivedObjectContainer PerceivedObjectContainer

}

DetectionLevel ::= INTEGER { level(1) } (1..4)
OmitedReportsNumber ::= INTEGER { oneReport(1) } (0..1024)

END
```

Annex C: Misbehaviour detection with " Collective Perception Messages" (CPMs)

C.1 General

While the present document focuses primarily on studying misbehaviour detection based on CAM and DENM messages, ETSI has been specifying the CPM in [i.10]. The goal of this Annex is to give a first hint on challenges and opportunities presented by CPM for misbehaviour detection in general for ITS systems.

C.2 Overview on collective perception messages

CPMs are broadcasted to share information on the presence of road users and other objects that have been detected and recognized by the transmitting ITS station, including information on road users or objects that are not equipped with an ITS station. Such non-ITS-S-equipped objects cannot provide awareness of their existence, dynamics and current state to ITS stations, and cannot contribute individually to the overall cooperative awareness. Moreover, the CPM also includes the detected status information about road users equipped with ITS stations. The general structure of a CPM is shown in Figure C.1.

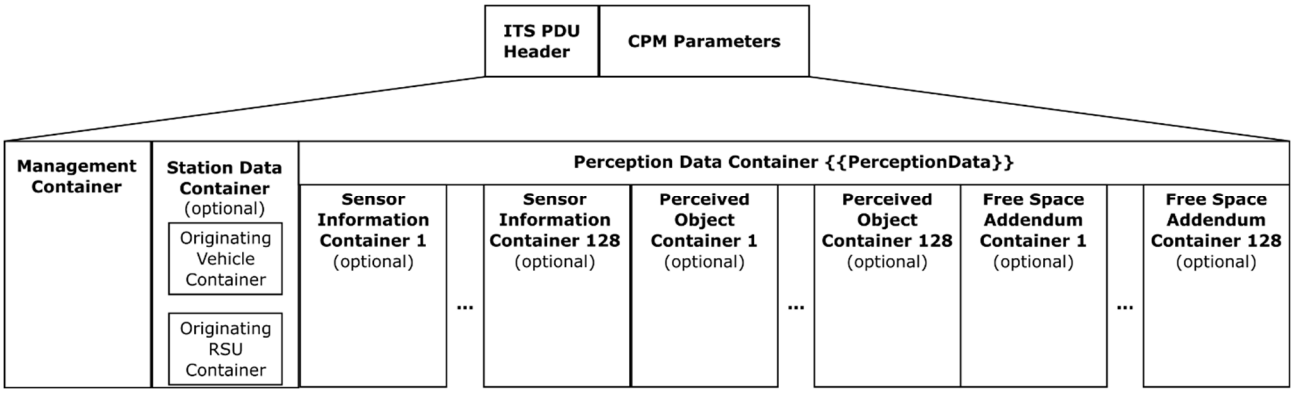


Figure C.1: General Structure of a CPM [i.10], Figure 35

C.3 Attack model for misbehaving CPMs

Similar to the attack model for misbehaving CAM and DENMs, it should be a security concern that any of the data containers in CPM may be misbehaving, carrying incorrect data due to malfunction by a faulty ITS station or completely bogus data due to malicious manipulations by an internal attacker. As a result, CPMs can be used to launch data modification attacks, ghost car attacks, and Sybil attacks.

Note that ghost vehicles could be created by manipulating, for example, the "Originating Vehicle Container" (similar to ghost vehicles created by CAM) or the "Perception Data Container" such as a non-existing "Perceived Object". The Originating Vehicle Container would carry speed, location, heading, acceleration, yaw angle, orientation angles, vehicle dimensions, etc. of the ego-ITS stations. One or multiple of these attributes could be manipulated intentionally or unintentionally, similar to what can be done with the CAM.

In addition, when a perceived object is reported, detected age, confidence, position, speed, heading, acceleration, classification, etc. of the object are also included in the Perceived Object Container. One or multiple of these attributes could also be manipulated intentionally or unintentionally. The same applies to the Free Space Addendum Container.

Sybil attack becomes easier with CPM than CAM, because a single pseudonym certificate can be used to create a fleet of ghost cars by creating multiple "Perceived Objects" in CPM, while in CAM each ghost car requires its own pseudonym certificate. Therefore, it is important to consider how to detect misbehaviour effectively in CPM. This is out of scope of the present document and hence the open issue remains. Studying MD while the CPS is still being specified can be beneficial in case the CPM can be fine-tuned to enable more effective MD.

C.4 Misbehaviour detection with CPM

The attributes of the CAM are subsets of the CPM ones. The techniques used for the CAM MD could be used for the common attributes of the CPM MD. However, additional techniques need to be developed for CPM specific attributes. The CPM presents both opportunities and challenges for MD in general, even for the MD of CAM messages, for example. The opportunities exist because the CPM mitigates a fundamental limitation in CAM that is the lack of redundancy as each CAM only contains information about the ego vehicle. The CPM provides more independent sources (witnesses) of the objects in the common environment. Misbehaviour detection relies on redundancy of information and so the addition of CPM should help the misbehaviour detection engine to look for data inconsistency more effectively. Even when a realistic mixed deployment scenario is considered, where most of the ITS stations broadcast CAM only, and a small fraction of the ITS stations broadcast CAM and CPM, the additional information from the CPM could be used to cross check with the information from the CAMs to detect misbehaviour more readily. This aspect of MD is not included in the present document.

With the deployment of CPS and abundance of redundant information, the computational cost for MD will also increase. The way to do that efficiently in real time may be a potential challenge. Moreover, adopting the CPM in C-ITS may introduce security challenges as it opens another door for attacks as discussed in clause C.3. Therefore, it is necessary to investigate the security implications thoroughly before the deployment of the CPS.

C.5 An initial list of open issues

To help defining the exact scope of a study on MD with CPM, an assessment of the following issues should be performed:

- possible CPM misbehaviour scenarios;
- improve MD on CAM by leveraging the CPM information provided by some ITS-stations;
- detection techniques of misbehaviour in CPM;
- possible ways to make the CPM more robust against manipulations;
- how to provide CPM misbehaviour evidence to the MA;
- are station-internal interfaces to be defined.

History

Document history		
V2.1.1	October 2020	Publication