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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights 4

Foreword....4

Modal verbs terminology....4

1 Scope 5

2 References 5
2.1 Normative references 5
2.2 Informative references....5

3 Definition of terms, symbols and abbreviations....9
3.1 Terms....9
3.2 Symbols....9
3.3 Abbreviations 9

4 Background 10
4.1 General 10
4.2 European C-ITS trust system and revocation of trust....11
4.3 Misbehaviour detection, analysis and response in the US Connected Vehicle project....12
4.3.1 Context of SCMS design and harmonization US-EU-Australia task-group 12
4.3.2 Functional architecture of CCMS 12

5 State-of-the-art 14
5.1 Detection approaches 14
5.1.1 General....14
5.1.2 False beacon information detection 14
5.1.3 False warning detection 16
5.1.4 Node trust evaluation....16
5.1.5 Feasibility assessment....17
5.2 Reporting approaches 17
5.2.1 General....17
5.2.2 Unicast MR to the misbehaviour authority....18
5.2.3 Broadcast MR to neighbours: pros, cons and alternatives 18

6 MD and MR - use cases and scenarios....19
6.1 Use case 1: Plausibility checks on access layer measurements on periodic broadcast messages (CAMs)....19
6.2 Use case 2: Plausibility checks on periodic broadcast messages (CAMs) 20
6.3 Use case 3: Security level local checks on received C-ITS messages....21
6.4 Use case 4: Misbehaviour detection on the DENM messages signalling a traffic event....22

7 Misbehaviour detection and reporting architecture....23
7.1 General 23
7.2 Misbehaviour report message format....25

8 Misbehaviour detection standard recommendations 27

Annex A: Potential misbehaviour detection mechanisms for "Cooperative Awareness Messages" (CAMs)....29

Annex B: Example of an ASN.1 MR specification....31

Annex C: Misbehaviour detection with " Collective Perception Messages" (CPMs)....33

C.1 General 33

C.2 Overview on collective perception messages....33

C.3 Attack model for misbehaving CPMs 33

C.4 Misbehaviour detection with CPM....34

C.5 An initial list of open issues 34

History 35

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).