PRISSMA Project
Plateforme de Recherche et d'Investissement pour la Sûreté
et la Sécurité de la Mobilité Autonome
04/2021 - 04/2024

[L5.1] REPORT ON CONNECTIVITY PERFORMANCES CONSTRAINTS IN AUTONOMOUS VEHICULES ENVIRONMENT

RAPPORT SUR ANALYSE DES CONTRAINTES DE PERFORMANCE DE LA CONNECTIVITE DANS LES ECOSYSTEMES VEHICULAIRES AUTONOMES

Main authors: Sammy HADDAD (Oppida) and G. Perrin (Université Gustave Eiffel)

Reviewers or second authors: Jean CASSOU-MOUNAT (Transpolis)

Keywords: Connectivity, KPI

Abstract. This deliverable aims at presenting a state of the art for Key Performance Indicators (KPI) for both Information Technologies (IT) connectivity in general and Communicating Intelligent Transport Systems (C-ITS) in particular. In the context of PRISSMA, we extracted from this state of the art a set of KPI to be evaluated in Autonomous Vehicles (AV) ecosystems. The goal of these selected KPI is to guarantee the correct behavior of AVs.

Résumé. Ce livrable présente un état de l'art des métriques de performance (ou KPI) pour les systèmes IT (Information Technology) de manière générale puis pour les systèmes C-ITS (Communicating Intelligent Transport Systems) en particulier. Dans le contexte du projet PRISSMA, nous avons extrait de l'état de l'art les métriques qui nous permettrons de d'évaluer et de qualifier les performances des communications des systèmes de transport autonomes à bases d'IA.

Table of contents

1 INTRODUCTION

This deliverable aims at presenting a state of the art for Key Performance Indicators (KPI) for both Information Technologies (IT) connectivity in general (section 2) and Communicating Intelligent Transport Systems (C-ITS) in particular (section 3). In the context of PRISSMA, we extracted from this state of the art a set of KPI (section 4) to be evaluated in Autonomous Vehicles (AV) ecosystems. The goal of these selected KPI is to guarantee the correct behavior of AVs.

2 IT CONNECTIVITY KPIS - NETWORK INTERCONNECT DEVICES PERFORMANCES

To our knowledge very few publications proposed KPIs for communication performances. One of the few references we have found has been defined by the IETF and is mostly reused by other approaches (cf. sections 5, 7 and 8).
The IETF started its standardization activities on benchmarking of network devices in 1989 when they started the activities of the benchmarking methodology working group (bmwg). Performance indicators were fist defined in RFC 1242 [1] in 1991 for Network Interconnection Devices. The document provides both terminology definition for network performance and descriptions, defining such elements as: Back-to-back, Bridge, Data link frame size, Frame Loss Rate, Latency, Overhead behavior, Throughput, etc. For each of those entry it provides a definition of the element, discuss how to measure, or evaluate it when meaningful together with proposed measurement units and potential issues for measurement.
This group published in 1999 the RFC 2544 [2] which defines tests set up including devices under test (DUT) set up, frames format and sizes, broadcast frames, routing frames, filters, protocol addresses, etc.
They present a total of 7 metrics, that are still heavily used in the domain:

- **Throughput** which determines the device under test DUT's maximum rate at which none of the offered frames are dropped by the device, as defined by [1].
- **Latency** (for store and forward devices) determines the time interval starting when the last bit of the input frame reaches the input port and ending when the first bit of the output frame is seen on the output port as defined by [1].
- **Loss rate** determines the Percentage of frames that should have been forwarded by a network device under steady state (constant) load that were not forwarded due to lack of resources of a DUT throughout the entire range of input data rates and frame sizes as defined by [1].
- **Back-to-back frames** which characterize the ability of a DUT to process back-to-back frames, i.e. fixed length frames presented at a rate such that there is the minimum legal separation for a given medium between frames over a short to medium period of time, starting from an idle state as defined by [1].
- **System recovery** which characterizes the speed at which a DUT recovers from an overload condition.
- **Reset** which characterizes the speed at which a DUT recovers from a device or software reset.

For each of them the RFC standardize tests set up and metrics. It defines a first basic test run to be repeated for different frame sizes, "bursty traffic", number of rule entries, etc.
The RFC identifies that security considerations are out of its scope and that it does not address it.
Those metrics have been extensively used and validated over time for the last past 20 years. As defined by the RFC itself they mostly address network component and more specifically routers, but the presented KPI can be applied (with different tests setups of course) to any communication stack of communicating device and thus potentially to C-ITS-S.
Tools exists to perform the RFC tests. They can be divided into two groups: Hardware-based devices, providing efficient but costly approach, and software-based solutions with higher flexibility, lower costs but lower traffic rates and precision.
Some studies have refined or completed this document [4], based on the observation that existing benchmarking approaches often rely on simplistic traffic patterns that do not represent realistic use cases of network interconnect devices, invoking such arguments as basic

interconnect devices such as switches or routers show non-trivial worst-case performance depending on the traffic applied when implemented in software (e.g interarrival times between incoming packets influence the batching behavior, the ordering and diversity of incoming packets stresses the cache and impacts packet processing performance in different ways, complex interconnect devices exhibit non-trivial performance properties using functions with unpredictable side-effects). They propose 4 enhancement axis to be considered for PRISSMA evaluations: (i) extended latency reporting since they demonstrated that average latency as defined by [2] is not always meaningful, (ii) additional test traffic patterns including not only constant-bitrate traffic but also Poisson distribution traffic as it approximates better real world traffic, (iii) defining multiple predefined set of tests per device class since not all device behave the same way with all traffic, and (iv) automated configuration.
This study do not identify the need for nor proposes new KPI, they only propose refinement and further test case definition per KPIs.

3 PREVIOUS ITS PROJECTS KPIS IDENTIFICATIONS

3.1 Secure Cooperative Autonomous systems (SCA) – IRT system

SCA is a collaborative project lead by the IRT Systemx on the definition of security and privacy mechanisms in connected vehicles systems (https://www.irt-systemx.fr/projets/sca/). The project started in 2017 and lasted 3 years. It included most of the main actors of the French automotive industry (Renault, Stellantis, Valéo, Transpolis, Yogoko, etc.).
The results of the project are not fully public and the deliverable providing KPIs for C-ITS is not. However, we can mention that this project studied the following tests categories:

1. Privacy
    a. Anonymity based,
    b. User-centric based,
    c. Traceability,
    d. Pseudonym reuse
2. Safety
    a. Reception rate/packet losses,
    b. Delay/latency,
    c. Wireless channel overhead
    d. Message inter-arrival duration,
    e. Cooperative awareness quality,
    f. Application Reliability
3. Misbehavior management
4. Security performances
    a. Cryptographic operations latency,
    b. Inter-layer processing latency,
    c. Security overhead size,
    d. Packets size,
    e. Certificates provisioning latency,
    f. PKI Scalability,
    g. Cost of an attack (required resources for the attack)

Clearly not all categories studied in this project concern connectivity KPIs. The main group of metrics that can be used as connectivity performance evaluation is the Safety one. It presents some similar metrics to the one defined by [2], i.e. packet losses (loss rate), latency, wireless channel overhead (which actually evaluates indirectly). Interestingly, they propose both network level metrics (reception rate/packet losses, delay/latency, wireless channel overhead)

and application-level metrics (message inter-arrival duration, cooperative awareness quality and application reliability). As identified by the project application-level metrics are not subject to very extensive state of the art.
However, among the KPI they have identified, references can be found such as [6] that defined such metrics as:

- ***neighborhood awareness*** *is a metric which describes the probability that a node v is aware of its neighboring nodes and is calculated with respect to the distance between node v and its neighbors. More specifically, the neighborhood awareness is expressed as the probability of having received at least one beacon message within the past second.*
- ***beacon information age*** *is the average age of received status information and is calculated with respect to the distance between the originator and the receiver. It can also be interpreted as the average inter-reception time between two beacons of the same originator.*

While [7] defines:

- ***awareness quality****, i.e. the awareness of vehicle i at time t and within distance d computed as follows:*

$$Awareness_{d,t}(i) = \frac{\left|N_i^d(t)\right|}{\left|V_i^d(t)\right|}$$

where N_i^d is the set of all discovered neighbors by vehicle i within distance d and V_i^d is the set of all vehicles physically present within distance d.

More recent studies like [8] (not mentioned by SCA state of the art) proposed such metrics as Expected Transmission Count (ETX) for link l where pf represents the probability of successful packet transmission, and pr the probability of successful received ACK packet :

$$EXT = \frac{1}{(p_f \,.\, p_r\,)}$$

Together again with more common KPIs already presented in this state of the art, demonstrating once more that the state of the art doesn't provide tens of such KPI, but rather that the core set of them is rather small but sufficient:

- throughput
- packet loss ratio
- number of sent and received packets
- overhead (useful traffic ratio)
- and end-to-end delay statistics
    - minimum, maximum, average, median values, jitter and delay histogram

The privacy KPIs are subject to several research publications such as [9], [10],
[11] and provide such metrics as the *effective anonymity set size S* as a metric. *S* is equal to the entropy of the anonymity set and is computed as follows:

$$S = -\sum_{u \in \Psi} p_u \, log_2(p_u)$$

That is, $0 \leq S \leq log_2|\Psi|$ where:

- $S = 0$ means the system provides no anonymity
- $S = log_2\Psi \vee$ means the system provides maximum anonymity

Or the *degree of anonymity* as a metric. They define the degree of anonymity as a normalized version of the effective anonymity set size, thus bounding its value between 0 and 1. The degree of anonymity *d* is computed as follows:

$$d = 1 - \frac{S_M - S}{S_M} = \frac{S}{S_M}$$

But those metrics are more security related than communication efficiency, so they are out of scope of this deliverable. Which is the same for all the security metrics identified by that project.

3.2 SCOOP-F

SCOOP is a C-ITS deployment project based on a cooperation between road managers and car manufacturers. The project objectives covered “real life” challenges such as : privacy, cybersecurity, industrial processes, calls for tenders, compliance audit, interoperability.
The project is 50% founded by the European Commission, started in 2014 and ended in December 2019.
The deliverable [12] presented a process of the technical evaluation of the SCOOP@F project. Technical evaluation is presented as different from a validation done in real environment by real users. They define validation as the step where the system functions are tested before the experimentation. The validation is meant to verify if the proposed approach achieves its goals while the evaluation is meant to allow to test the system in a real environment to assess its overall performance.
To achieve this evaluation goal, they defined a set of research questions gathered in 3 different groups: common, security and hybrid communication. Then they present scenarios for evaluation for which they define an objective, preconditions, test sequence and comments. Those scenarios are meant to provide answers to previously formalized questions.
The scenarios cover the following evaluation parameters that can be of interest for PRISSMA:

- E2E delay
- ITS-G5 range
- packet error rate
- E2E latency
- loss rate
- security overhead
- Verification if the road operators provide all information for all services to all end users via ITS-G5/cellular and hybrid-communication in the same message formats.
- 4G communication covers all areas between ITS-G5 RSUs
- Congestion problems in one communication channel can be mitigated via alternative communication channel(s)
- Number of created tunnels, number of dropped tunnels, loss of service continuity (for hybrid systems)

Again, we can find the same core KPI that are: E2E delay, packet error rate, E2E latency, loss rate, security overhead.

3.3 5GAA

Finally, we have reviewed a document created by 5GAA regarding "V2X Functional and Performance Test Procedures – Selected Assessment of Device-to-Device Communication Aspects" [10]. The part 5 of the document aims at providing the applicable performance measures to assess the On-Board Units (OBUs) communication and congestion control performance.

- PER (Packet Error Rate), expressed as a percentage, of the number of missed packets at a receiver from a particular transmitter and the total number of packets queued at that transmitter
- IPG (Inter-Packet Gap) as the time, calculated at the receiver and expressed in milliseconds, between successive successful packet receptions from a particular transmitter
- CBP (Channel Busy Percentage), expressed as a percentage, of the time during which the wireless channel is busy
- CBR (Channel Busy Ratio), defined in the document
- IA (Information Age), represents the time interval, expressed in milliseconds, between the current time at a receiver and the time stamp, applied by the transmitter, corresponding to the data contained in the most recently received BSM from the transmitter
- Application E2E Latency, represents the time interval, expressed in milliseconds, between the time instant when the transmitter application delivers the application layer packet (e.g., BSM) to the lower layers, and the time instant when the application layer packet is received by the application layer at the receiver (before payload decoding).
- RSSI (Received Signal Strength Indication) as a measurement of the power present in a received radio signal

These KPIs gives us a complementary analysis regarding the previous KPIs listed.

4 PRISSMA PROPOSED KPIS

PRISSMA challenge consists in qualifying an AV system and assess it safety, security, and privacy. To do that one of our goals is to assess that AV are able to take the best decision possible to guarantee the passenger safety. This include to ensure that the system can timely and precisely provide information on the vehicle environment to complement its local detection mechanisms (based on its own sensors) or allowing the system to take over the vehicle control in appropriate delays in case of emergency or difficult situations. For that the system needs to provide sufficient communication performance:

1. transmitting and analyzing messages within an appropriate time frame between different component,
2. providing sufficient and accurate information data transfer,

So based on the previous state on the art and to achieve this assessment, we select the following KPIs:

1. Appropriate transmission and packet treatment latencies
    a. **Latency** which measures the amount of time elapsed between the sending of a message by an ITS-S and its reception by another one.
    b. **E2E** delay in milliseconds
    c. **Inter-Packet Gap** as the time, calculated at the receiver, between successive successful packet receptions from a particular transmitter expressed in milliseconds,
    d. **System recovery** which characterizes the speed at which a DUT recovers from an overload condition in milliseconds

   e. **Reset** which characterizes the speed at which a DUT recovers from a device or software reset in milliseconds
   f. **Max number and load of messages** that can be received and treated by the C-ITS-S, i;e. messages per seconds and load (kilo octet) per seconds.
   g. **Throughput of forwarding ITS messages functions** which determines the device under test DUT's maximum rate at which none of the offered frames are dropped by the device both messages per seconds and load (kilo octet) per seconds.

2. Accurate information data transfer
   a. **Loss rate** computed as the ratio of the number of messages received by an ITS-S to the total amount of messages that it should have received in percentage.
   b. **Packet error rate** in percentage
   c. **Cooperative/neighborhood awareness quality** probability [7]
   d. **Delta transmission over different (hybrid case) communication media,** percentage of packets transmitted over only one communication
   e. **IA (Information Age),** represents the time interval, expressed in milliseconds, between the current time at a receiver and the timestamp, applied by the transmitter, corresponding to the data contained in the most recently received BSM from the transmitter

References

[1] S. Bradner, “Benchmarking Terminology for Network Interconnection Devices,” *Internet Engineering Task Force (IETF),* no. RFC 1242, July 1991.

[2] J. M. S. Bradner, “ Benchmarking Methodology for Network Interconnect Devices,” *IETF,* vol. Request for Comments 2544, March 1999.

[3] T. E. A. N. T. C. (EANTC), “Huawei technologies service activation using rfc 2544 tests,” 2008.

[4] S. G. F. W. P. E. P. W. a. G. C. Daniel Raumer, “Revisiting Benchmarking Methodology for Interconnect Devices,” *ANRW ,* July 16, 2016.

[5] C. P. F. C. C. O. R. Asati, “Device Reset Characterization,” *Internet Engineering Task Force (IETF) ,* vol. RFC 6201.

[6] F. T. J. H. H. H. Jens Mittag, “A Comparison of Single- and Multi-hop Beaconing in VANETs,” *VANET’09,* September 25, 2009.

[7] R. L. T. L. C. L.-P. a. G. S. Robert K. Schmidt, “An Approach for Selective Beacon Forwarding to Improve Cooperative Awareness,” *Vehicular Networking Conference (VNC), 2010,* 2010.

[8] N. J. M. Malnar, “A FRAMEWORK FOR PERFORMANCE EVALUATION OF VANETS USING NS-3 SIMULATOR,” *Promet – Traffic & Transportation, Vol. 32,* vol. 32, no. 2, pp. 255-268 , 2020.

[9] G. D. A. Serjantov, “Towards an Information Theoretic Metric for Anonymity,” *Book cover,* p. 41–53, 2003.

[10] S. S. J. C. B. P. C. Díaz, “Towards Measuring Anonymity,” *International Workshop on Privacy Enhancing Technologies,* 2002.

[11] M. M. J. H. D. P. J. Freudiger, “On non-cooperative location privacy: a game-theoretic analysis,” *CCS,* 9 November 2009.

[12] G. evaluation, “Activity 2: Studies - Deliverable 2.3.3.1 Technical Evaluation Methodology - Part 1 : Palier 1 methodology,” *SCOOP@F,* 2019.

[13] A. S. F. J. Santa and Pereniguez-Garcia, “Experimental evaluation of CAM and DENM messaging services in vehicular communications,” *Transportation Research Part C: Emerging Technologies ,* April 2, 2014.