3GPP TSG-RAN WG2 #112e R2-20xxxxx

Electronic meeting, November 2nd – 13th 2020

Agenda Item: 8.11.x

Source: Swift Navigation

Title: TP on Integrity Methods for TR 38.857

Document for: Discussion, Decision

# 1 Introduction

This is to provide the text proposal on the Integrity Methods for TR38.857 based on:

* The inputs to email discussion [AT112-e][614][POS] (R2-2010880). The baseline text below is the baseline text that was circulated for feedback in the email discussion. The track changes below represent the edits that were made as a result of the email comments.
* Prior Agreements at RAN2#111-e

This TP should be reviewed alongside the following Tdocs:

* R2-2010877 TP on Integrity KPIs, Concepts, Use Cases
* R2-2010878 TP on Integrity Error Sources

# 2 Text Proposal

*Start of Text Proposal*

9.4 Positioning Integrity Methods

9.4.1 RAT-Independent

error sourcesdescribes how the feared events occurring in different parts of the positioning system can be detected to support the implementation of UE-based and UE-assisted methodologies.

9.4.1.1 UE-Based A-GNSS Integrity Methods

9.4.1.1.1 Detection of Feared Events in the Correction Data

The 3GPP network-assistance data can be used to indicate potential faults in the correction data processing itself, as determined by the corrections service provider systems. If the GNSS correction data processing encounters an error that degrades or impacts the validity of the correction data (e.g. lost, corrupt or invalid observations, software bugs; or external feared events such as satellite failures), and the service provider is capable of monitoring and detecting these feared events, the quality of the correction data can be indicated to the UE. As noted in Table 2, there are no existing IEs corresponding to correction data quality, meaning new assistance data is needed. Signaling the Correction Data quality allows the UE to determine the impact of these events on its computed PL. Note that often the correction data may still be sent even if not indicated as high enough quality for integrity purposes, as it is still of sufficient quality to improve accuracy even though integrity cannot be ensured.

9.4.1.1.2 Detection of Feared Events in Transmitting Data to the UE

Data integrity ensures that the end-to-end data transmission link needed to signal integrity assistance data across the network is secure and free from the possibility of data corruption, including the data link to the corrections service provider. Data integrity algorithms and related security architectures for the 5G system are individual work areas in 3GPP [16].

A related observation in the context of this SI (further addressed in Section ‘9.4.1.1.5 - Data Validation’ below) is that industry-specific functional safety standards (e.g. ISO-26262 for Automotive, IEC 62278 for Rail) are also required to validate integrity compliance for a given implementation. These standards include requirements that may be outside of the current RAN architecture. For example, consider the typical service interface between a corrections service provider sending GNSS assistance data to the UE via the NG-RAN. Both the correction service provider and UE can be designed and qualified with integrity compliance. However, the NG-RAN architecture, although rigorously specified with data security and integrity features in [6], may not comply with industry-specific functional safety standards by default. This implies that the integrity of the data transmission from the correction provider to the UE needs to be trusted and assured without any alterations via the NG-RAN.

One method for achieving this is by providing for the data to be signed by the correction provider and verified by the UE in accordance with the relevant functional standards[[1]](#footnote-1). Once the data has left the correction provider, any changes to the data would invalidate the certificate. This in turn means that, irrespective of whether the 3GPP architecture is compliant to the functional safety standards, appropriate procedures can be implemented to sign and verify the network integrity assistance data with minimal impacts to the NG-RAN – i.e. the NG-RAN can still be leveraged as an efficient data link. Further investigation is required through the SI/WI to determine whether new data integrity IEs are needed for positioning integrity or whether existing data integrity IEs are sufficient (e.g. to carry a data signature from the corrections service provider to the UE).

9.4.1.1.3 Detection of External Feared Events

The correction service provider systems can be used to detect the feared events which occur external to the correction networks and the UE equipment (e.g. GNSS feared events and atmospheric gradients). New assistance data can be defined in LPP to indicate these events to the UE via the NG-RAN, which in turn reduces overhead on the UE by offloading integrity monitoring to the network. It also enables the potential to achieve lower TIRs given the added monitoring and detection capabilities of the network. These methods are further described below.

In practice, feared events detected by the corrections service provider mean that, even outside the probability of a fault occurring (e.g. recognizing these probabilities can be estimated using threat models [5][7]), the correction network itself can be used to detect if the actual event occurs. For example, the correction provider network typically has the benefit of many GNSS reference stations distributed over a wide area. This additional observability can result in more effective detection of these events, removing the burden on the UE to detect them unassisted, and potentially increasing the probability with which these events can be detected (i.e. given the UE alone does not have the benefit of cross-checking data from surrounding GNSS reference stations). Examples of GNSS external feared events include satellite feared events, such as loss of signal, clock errors and constellation failures, and atmospheric feared events, such as large ionospheric and tropospheric gradients.

In addition to the network providing integrity assistance data corresponding to the detection of feared events, the network may also provide to the UE certain threat model parameters, allowing them to be updated based on the evolving operational history of the GNSS constellations. An example of this is found in the ARAIM Integrity Support Message (ISM) which contains parameters such as the assumed probability of satellite failure [7]. The scope of this SI is not intended to standardize the integrity algorithms implemented by the corrections service provider to detect the feared events. The study identifies the common set of feared events that can be indicated to the UE by specifying network-assistance data IEs.

9.4.1.1.4 Detection of UE Feared Events

UE-detected feared events depend on the hardware and software capabilities of the equipment and its internal integrity algorithms. This SI does not attempt to standardize the GNSS integrity algorithms at the network or the UE, but rather the network-assistance data needed to transport the integrity indicators derived from the algorithms. The assistance data can then be applied by the UE’s GNSS positioning function (i.e. independent of 3GPP).

This same logic applies to how the RTK and SSR GNSS assistance data has been standardized in previous 3GPP releases – i.e. the RTK and SSR algorithms used to derive GNSS corrections are implementation-defined. The assistance data used to transport the derived corrections are specified in LPP.

9.4.1.1.5 Positioning Integrity Validation

Positioning integrity can only be validated end-to-end, per-implementation. Validation requires a comprehensive Fault-Tree Analysis (as described in [5]) and a complete qualification dossier (e.g. documentation, methodologies, tests and traceability through the entire integrity qualification process).

Integrity validation is particularly crucial for safety-critical applications such as Automotive and Rail. Integrity validation takes into consideration a much wider suite of requirements than the assistance data used to supply the GNSS integrity parameters. For example, this includes the hardware components (e.g. ISO-26262 certified hardware and CPUs), tooling (e.g. ASIL-qualified compilers), software architecture design, safety manuals, test procedures etc, all of which vary for each integrity implementation. While 3GPP integrity assistance data is just one of multiple inputs for integrity validation, defining a standardized set of GNSS integrity assistance data ensures a wider ecosystem of connected devices can readily benefit from knowing what inputs are available from the network to support integrity validation.

9.4.1.2 UE-Assisted A-GNSS Integrity Methods

Editor’s Note: UE-assisted methods are FFS.

9.4.1.3 Summary of A-GNSS Integrity Methods

Table 9.4.1.3 summarizes the network-assisted (UE-Based) and UE-assisted (LMF-Based) methods for determining integrity.

**Table 9.4.1.3: Summary of network assisted (UE-Based) and UE-assisted (LMF-Based) methods for determining Integrity.** NOTE: the details are FFS and to be discussed in WI phase, including the LPP messages and transfer procedures.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Integrity method** | **Location service type** | **Source of KPIs** (e.g. TIR, AL, TTA etc) | **Source of Integrity results**  (e.g. PL, Integrity Availability etc) | **Error source assistance information (FFS)** | **Spec impact (FFS)** |
| Network assisted (for UE-based positioning) | MO-LR | Obtained via UE internal implementation; | Keep inside the UE | From LMF:  - Feared events in the correction data  - Feared events in transmitting the data to the UE  - External feared events  UE internal implementation:  - UE feared events | Procedure to transfer Integrity assistance information from LMF to UE |
| MT-LR | From LMF | From UE | From LMF:  - Feared events in the correction data  - Feared events in transmitting the data to the UE  - External feared events  UE internal implementation:  - UE feared events | Procedure to transfer Integrity assistance information and KPIs from LMF to UE  Procedure to transfer Integrity results from UE |
| UE assisted (for LMF-based positioning) | MO-LR | From UE | From LMF | LMF implementation:  - Feared events in the correction data  - Feared efents in transmitting the data to the UE  - External feared events  From UE:  - UE feared events | Procedure to transfer Integrity assistance information and KPIs from UE to LMF  Procedure to transfer Integrity results from LMF |
| MT-LR | Obtained via LMF implementation | LMF internal implementaiton | LMF implementation:  - Feared events in the correction data  - Feared efents in transmitting the data to the UE  - External feared events  From UE:  - UE feared events | Procedure to transfer Integrity assistance information from UE to LMF |

*End of Text proposal*

# 3 Conclusions

**Proposal 1: Agree to the updated Error Source names:**

1. Feared events in the correction data
2. Feared events in transmitting the data to the UE
3. External Feared Events
4. UE feared events

**Proposal 2: Agree to add Sections 9.4.1.2 (UE-Assisted A-GNSS Integrity Methods) and 9.4.1.3 (Summary of A-GNSS Integrity Methods).**

**Proposal 3: Agree to the updated Table (9.4.1.3) summarizing the integrity methods.**

**Proposal 4: Agree to adopt this TP on Integrity Methods as a baseline for TR 38.857.**

1. Note that the requirements called out by integrity standards such as ISO-26262 can be extremely onerous for any entity that “processes” (i.e. modifies in any way) the data. This possibly includes use of qualified tools such as special compilers, as well as using ISO-26262 certified hardware and CPUs to perform the processing. [↑](#footnote-ref-1)