|  |
| --- |
| 3GPP TR 33.877 V0.3.0 (2022-10) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on the security aspects of Artificial Intelligence (AI)/Machine Learning (ML) for the NG-RAN(Release 18) |
|   |
|  |  |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 7

4 Background 7

4.1 General 7

4.2 NG-RAN use cases 7

5 Key Issues 7

5.1 Key Issue #1: User Privacy of the RAN AI/ML framework 8

5.1.1 Key issue details 8

5.1.2 Security threats 8

5.1.3 Potential security requirements 8

5.2 Key Issue #2: Robustness of the RAN AI/ML framework against data poisoning attacks 8

5.2.1 Key issue details 8

5.2.2 Security threats 9

5.2.3 Potential security requirements 9

6 Solutions 9

6.0 Mapping between key issues and solutions 9

6.Y Solution #Y: <Solution Name> 9

6.Y.1 Introduction 9

6.Y.2 Solution details 9

6.Y.3 Evaluation 9

7 Conclusions 9

Annex <X> (informative): Change history 10

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The study aims at identifying key issues and solutions in order to address the security aspects of employing AI/ML techniques in RAN. The motivation of this study is to provide potential security handling for the procedures of the NG-RAN AI/ML framework [2]. The NG-RAN AI/ML framework includes functional entities and information flows between functions in order to realize an AI/ML architecture for data collection, model training, data inference and actions/feedback for the NG-RAN and UEs. The NG-RAN AI/ML framework is also accompanied by three RAN-related use cases.

The study aims at studying the following aspects:

 - The applicability of existing security mechanisms for the NG-RAN AI/ML framework.

- Whether user privacy issues exist for the selected use cases in the related RAN group studies, not disrupting the current system designs. Use cases not selected in AI/ML for NG RAN by RAN groups are out of scope of this study. The need for alignment with the study of privacy of identifiers over radio access would also be assessed.

- Security aspects of the RAN use cases from the point of view of AI/ML robustness in the face of AI/ML adversaries in AI/ML for NG-RAN.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 37.817: "Study on enhancement for data collection for NR and ENDC"

[3] 3GPP TS 38.423: "NG-RAN; Xn Application Protocol (XnAP)"

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

AI Artificial Intelligence

CHO Conditional Handover

ML Machine Learning

RLF Radio Link Failure

QoE Quality of Experience

# 4 Background

## 4.1 General

The NG-RAN AI/ML framework has been described in clause 4.2 of 3GPP TR 37.817 [2] and the related use cases which are captured in clause 5 of 3GPP TR 37.817 [2]. This document aims at studying the potential security handling of the NG-RAN AI/ML framework and the selected use cases.

The selected use cases in 3GPP TR 37.817 [2] are briefly described below.

## 4.2 NG-RAN use cases

Clause 5 of 3GPP TR 37.817 [2] includes the following use cases:

- Network Energy Saving: This use case is about cell activation/deactivation which is an energy saving scheme in the spatial domain that exploits traffic offloading in a layered structure to reduce the energy consumption of the whole radio access network (RAN). When the expected traffic volume is lower than a fixed threshold, the cells may be switched off, and the served UEs may be offloaded to a new target cell.

- Load Balancing: The use case is to distribute the load evenly among cells and among areas of cells, or to transfer part of the traffic from congested cells or from congested areas of cells, or to offload users from one cell, cell area, carrier or RAT to improve network performance. This can be done by means of optimization of handover parameters and handover actions.

- Mobility Optimization: The use case is to minimize performance loss due to unsuccessful or erroneous mobility management events. Mobility management is expected to guarantee the service-continuity during the mobility by minimizing the call drops, Radio Link Failures (RLFs), unnecessary handovers, and ping-pong. In the future, it is expected that handovers will be increasing in numbers as the coverage of a single node decreases and UE mobility gets higher and higher. In addition, for the applications characterized with the stringent QoS requirements such as reliability, latency etc., the Quality of Experience (QoE) is sensitive to the handover performance, so that mobility management should avoid unsuccessful handovers and reduce the latency during the handover procedures.

# 5 Key Issues

Editor's Note: This clause contains all the key issues identified during the study.

## 5.1 Key Issue #1: User Privacy of the RAN AI/ML framework

### 5.1.1 Key issue details

The RAN AI/ML framework studied in TR 37.817 [2] and specified in RAN specifications (e.g., TS 38.423 [3]) includes several network entities exchanging AI/ML related information for the purposes of data collection, data inference, output and feedback. These network entities are UEs, RAN nodes and potentially OAM nodes depending on the architecture. The RAN AI/ML framework specifies three use cases, namely Network Energy Saving, Load Balancing and Mobility Optimization for which the UEs and RAN nodes provide input and inference data and the RAN AI/ML framework on RAN and potentially OAM nodes provides output and feedback data to relevant nodes.

An OAM and /or NG-RAN node may train a model or perform inference using UE related information acquired by the RAN node (e.g., UE location information and UE trajectory prediction), and the information obtained from neighbouring RAN nodes (e.g., UE mobility history information).

The RAN AI/ML framework includes information transfer procedures from UEs and RAN nodes. UE-related data are annotated with temporary UE identifiers or UE measurement identifiers. Moreover, the UE and RAN node generated information stays within the 3GPP network and is not exposed to third parties.

### 5.1.2 Security threats

The source, inferred, output and feedback data used for RAN AI/ML use cases can contain UE related information such as UE location information, UE trajectory predictions, etc. which may compromise user privacy.

### 5.1.3 Potential security requirements

Editor's Note: The UE related information transmitted in the RAN AI/ML framework is determined by RAN WG3. Depending on the RAN WG3 progress it is FFS whether the specification of the RAN AI/ML framework needs any solution for addressing user privacy for the RAN AI/ML framework.

## 5.2 Key Issue #2: Robustness of the RAN AI/ML framework against data poisoning attacks

### 5.2.1 Key issue details

The RAN AI/ML framework studied in TR 37.817 [2] and specified in RAN specifications (e.g., TS 38.423 [3]) includes several network entities exchanging AI/ML related information for the purposes of data collection, data inference, output and feedback. These network entities are UEs, RAN nodes and potentially OAM nodes depending on the architecture.

The input data from UEs and RAN nodes are used to train AI/ML models which are in turn used to generate inferred data and actions on the behaviour of the RAN. As a result, there is a potential information path from an adversary to network entities. Moreover, specifically since the RAN AI/ML framework includes the realization of three use cases (Energy Saving. Load Balancing, Mobility Optimization) an attacker has a potential control knob to affect the energy consumption of a network, the load distribution across the network and mobility performance.

The AI/ML model or algorithm is out of scope of 3GPP, only the inputs, outputs, inferred data and feedback information is standardized and the types of data provided by the UE and RAN node, assuming an attacker can eavesdrop (and deduce the type of data) is generic and based on existing specifications. Therefore, an attacker does not have any knowledge of the use case or cases that the network has decided to support. As a result, the adversary operates with the black box assumption with respect to data poisoning. In other words, the adversary does not have the knowledge of the specific use case, the specific AI/ML algorithm used in each use case and the adversary may not have any information on the effectiveness of its attacks, i.e., there may not be a way for the attacker to estimate the level of success of the attacks.

### 5.2.2 Security threats

The RAN AI/ML framework uses input and inference data from network entities, some of which may be under the control of adversaries which could disrupt the AI/ML model and potentially cause network outages (availability attacks), denial of service and poor performance (resource consumption) to the network depending on the use case.

### 5.2.3 Potential security requirements

N/A

NOTE: The effect of data poisoning depends on the ML algorithm/model for the use cases considered in the Technical Report. There could be multiple ML algorithms/models for one specific use case. Hence countermeasures to such attacks that affect the integrity of the ML model are left to the implementation.

# 6 Solutions

Editor's Note: This clause contains the proposed solutions addressing the identified key issues.

## 6.0 Mapping between key issues and solutions

Editor's Note: This clause contains a table mapping between key issues and solutions.

## 6.Y Solution #Y: <Solution Name>

### 6.Y.1 Introduction

Editor's Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

Editor's Note: Each solution should list the impacts to the system.

# 7 Conclusions

Editor's Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-06 | SA3#107Adhoc-e | S3-221573 |  |  |  | TR skeleton | 0.0.0 |
| 2022-07 | SA3#107Adhoc-e | S3-221650 |  |  |  | Version after incorporating changes in S3-221649. | 0.1.0 |
| 2022-09 | SA3#108-e | S3-222405 |  |  |  | Version after incorporating changes in S3-221957, S3-222404.  | 0.2.0 |
| 2022-10 | SA3#108Adhoc-e | S3-223074 |  |  |  | Version after incorporating changes in S3-222912, S3-223067, S3-223068.  | 0.3.0 |