**3GPP TSG-SA3 Meeting #106-e *S3-220410-r8***

e-meeting, 14 - 25 February 2022 (revision of S3-yyxxxx)

**Source: Ericsson**

**Title: New SID** **on the security aspects of Artificial Intelligence (AI)/Machine Learning (ML) for the NR Air Interface and NG-RAN**

**Document for: Agreement**

**Agenda Item: 4.18**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: Study on the security aspects of Artificial Intelligence (AI)/Machine Learning (ML) for the NR Air Interface and NG-RAN

Acronym: FS\_RANAIML\_SEC

Unique identifier:

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-18

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  |  | X |  |  |
| No | X |  |  |  |  |
| Don't know |  | X |  | X | X |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
|  | Feature |
|  | Building Block |
|  | *Work Task* |
| X | Study Item |

## 2.2 Parent Work Item

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| N/A | N/A | N/A | N/A |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| 940084 | Study on Artificial Intelligence (AI)/Machine Learning (ML) for NR air interface | RAN1 study item which includes use cases, protocol impacts that may have security impacts |
| 941010 | Artificial Intelligence (AI)/Machine Learning (ML) for NG-RAN | RAN3 work item which specifies the RAN AI/ML framework |

**Dependency on non-3GPP (draft) specification:**

# 3 Justification

RAN3 has been working in Rel-17 on a study (FS\_NR\_ENDC\_data\_collect) for the Artificial Intelligence (AI)/Machine Learning (ML) framework for NG-RAN and the results are currently documented in TR 37.817.

Recently the RAN plenary has approved two items related to AI/ML for NG-RAN. The first is a study item (FS\_NR\_AIML\_air) lead by RAN1 and described in RP-213599 and the second is a work item (NR\_AIML\_NGRAN) lead by RAN3 and described in RP-213602.

The study item FS\_NR\_AIML\_air by RAN1 aims at specifying use cases such as CSI feedback enhancement, beam management, positioning accuracy enhancements for different scenarios. The purpose is to find representative use cases and define the details for AI/ML model specification, model lifecycle, input datasets for training, validation, testing and inference taking into account the framework described in the TR 37.817. Moreover, this study targets investigating the potential specification impact on physical layer aspects (RAN1), protocol aspects (RAN2) and interoperability and testing aspects (RAN4). There are specific notes in the study proposal that user privacy needs to be preserved. Moreover, it is stressed that this study is based on the current RAN architecture and new interfaces shall not be introduced. As a result, the security of communicating entities in the RAN framework may already be covered by current specifications, however this needs to be verified by an SA3 investigation as the study aims at investigating the impact on procedures specified by other working groups. Finally, since the use cases may involve UE-related data collected by UEs or the network, an investigation is needed whether there are any privacy issues due to the selected use cases. In the context of such investigation, the current state of system design should be maintained with respect to the collection of UE-related data.

The work item NR\_AIML\_NGRAN lead by RAN3 focuses on the enhancements of the existing interfaces and architecture for supporting the new identified use cases. More specifically the work item description states that the work focuses on specifying data collection enhancements and signaling support within existing NG-RAN interfaces and architecture (including non-split architecture and split architecture) for AI/ML-based Network Energy Saving, Load Balancing and Mobility Optimization. With respect to transfer of data, models, predictions, between network functions it may be the case that the security aspects are already been taken care of since existing interfaces are assumed to be used. However, if existing security mechanisms are applicable, this needs to be verified by an investigation.

Since the RAN framework described in 37.817 involves actors performing actions that affect other parts of the system, the actions may affect the proper operation of the system. The actions themselves are a result of the collected data and AI/ML models. The collected data and AI/ML models are inputs to the framework and not all these inputs may be under the control of the operator. Some inputs may be under the control of adversaries whose aim is to disrupt the AI/ML model and inference and potentially cause availability attacks to the network. As a result, an investigation about the impact of AI/ML adversaries to the proper operation of the network is imperative.

The use cases studied in RAN groups mainly focus on RAN performance optimization. Assuming the existence of RAN framework described in 37.817, new security related use cases could be proposed to be studied in SA3.

# 4 Objective

The study aims at identifying key issues and solutions in order to address the security aspects of employing AI/ML techniques in RAN. The study aims at studying the following aspects:

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

- 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 by RAN groups are out of scope of this study.

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

# 5 Expected Output and Time scale

|  |
| --- |
| New specifications {One line per specification. Create/delete lines as needed} |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
|  Internal TR | 33.XXX | Study on the security aspects of Artificial Intelligence (AI)/Machine Learning (ML) for the NR Air Interface and NG-RAN | TSG#98 (Dec 2022) | TSG#99 (Mar 2023) | Tsiatsis, Vlasios, Ericsson, vlasios.tsiatsis@ericsson.com |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
|  |  |  |  |

# 6 Work item Rapporteur(s)

Tsiatsis, Vlasios, Ericsson, vlasios.tsiatsis@ericsson.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

RAN1, RAN2, RAN3 may need to be consulted during the SA3 study with respect to the use cases and RAN AI/ML framework.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Ericsson |
| Samsung |
| China Mobile |
| AT&T |
| Nokia  |
| Nokia Shanghai Bell |
| Apple |
| Philips |
| Verizon |
| Interdigital |
| Cable Labs |
|  |