3GPP TSG-RAN3 #113-e R3-214224

16th – 26th Aug 2021

Online

Agenda Item: 18.5

Source: ZTE (moderator)

Title: SoD on CB #AIRAN6\_DataSecandTrans

Document for: Approval

# Introduction

**CB: # AIRAN6\_DataSecandTrans**

**- Data transmission via control plane could be reasonable way for huge quantity of AI data transmission?**

**- Security address, e.g., IP-Sec or DTLS address, carried in interface setup procedure can be used to guarantee the security of data transmission?**

**- Provide TP if agreeable**

**- Capture agreements and open issues**

(ZTE - moderator)

Summary of offline disc in [R3-214224](https://ericsson-my.sharepoint.com/personal/angelo_centonza_ericsson_com/Documents/Local%20Documents/3GPP_ETSI/RAN3/RAN3-113/EmailDiscussions/CB%20%23%20AIRAN6_DataSecandTrans/Inbox/R3-214224.zip)

Two phases of this email discussion:

**Phase 1 email discussion deadline:12am UTC, Friday, Aug 20th**

**Phase 2 email discussion deadline:4am UTC, Tuesday, Aug 24th, try to come up with TP if agreeable in the 2nd discussion.**

# For the Chairman’s Notes

Propose the following:

**Proposal 1: The size of AI data (e.g., inputs/outputs, model related data) transmission are large that depends on the specific use case solutions.**

**Proposal 2: Security address (e.g., IP sec or DTLS address) could be support and guarantee the security of AI data transmission, which could be discussed later involving SA3.**

# Background

At the latest RAN3#112e meeting, security related issue on AI RAN has been discussed, and it was agreed below:

**Security aspects should be considered and coordinated with other working groups later if needed.**

Currently, three prioritized use case (e.g., energy saving, mobility optimization and load balancing) were agreed to discuss the solution and standard impacts first. Regardless of which AI-based use case, decision or prediction will be generated by analysis large quantity of required data. So how to support AI data transmission in an existing RAN network, and how to guarantee the security of transmission shall be solved.

In this CB, we focus on discussing the data security and transmission for AI RAN, see [1].

# Discussion

[1] mentioned that in order to enable AI functionality into the RAN network, the current open standardized backhaul interface should be enhanced to support AI function, e.g., AI function start/stop, AI measurement configuration/collection, AI model deployment/distribution/update, etc. However, AI data (e.g., training data, inference data, or model related information, etc.) perhaps are very large, so RAN3 needs to consider and discuss how to support the large size data transmission in the existing RAN network.

**Question 1:** **Companies are invited to provide their views on whether the size of AI data transmission over current network interface is huge and large？**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Comments** |
| Ericsson |  | This problem, if at all confirmed, should be discussed once we converge more on use case solutions |
| Deutsche Telekom | Perhaps | The final objective of this question is somehow unclear. The data volume required is strongly dependent on the use cases under consideration. There is also the need to separate between the types of interface, i.e., CP, UP, or MP (Management Plane). We see e.g. AI model deployment/update etc. under MP domain.  |
| Huawei | Clarifications needed | Not sure the intention of this question. We think for offline training, large amount of data is foreseen, but these data are collected and reported to OAM through an accumulated process following timing being, and this doesn’t impact Uu interface. Then, for the input and output of online training or inference, we don’t think the data amount is large. |
| Intel |  | That depends on how we transmit data from one node to another, either in a large data size packet or through multiple packets. The extensive data request by AI/ML can be accumulated, rather than transmit all historical information at once. |
| Lenovo, Motorola Mobility | Probably Yes | In SA1 study, the bitrate of model should be large e.g. 100Mbps. We think it is worth to study the size of AI data. One example is distributed AI, in which case different AI functionalities are deployed in different nodes. But we are not sure we have enough time to have a study in this release. If not, we support to have a study on next release. |
| ZTE | Yes | The AI data we mentioned here includes not only inputs/outputs but also ML model related data. For inputs data/outputs data for training/inference, all historical data may be in a large size, but how to transmit these large quantities of data shall be discussed. And for ML model related data, ML model related information may be different according to different AI models, sometimes is also in a large size.Hence, how to transmit these AI data needs to discussed. |

**Moderator’s summary:**

**The size of AI data (e.g., inputs/outputs, model related data) transmission are large that depends on the specific use case solutions.**

Considering the ML model and AI measurements for various use cases may be huge, while SCTP has the benefits to guarantee the robustness and reliability, it also supports data fragmentation, so the AI data transmission via control plane seems a reasonable way.

[1] proposed to support huge quantity of AI data transmission via control plane.

**Question 2:** **If you agree that the quantity of AI data transmission is huge, companies are invited to provide their views on which could be a reasonable way for huge quantity of AI data transmission, via control plane or user plane?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Control plane, or user plane?** | **Comments** |
| Ericsson |  | As commented above, it is not possible to answer these sort of questions without knowing which solutions RAN3 will promote per use case |
| Deutsche Telekom |  | Similar understanding as E///. As stated under Q1, MP is missing here, that could be related to model deployment aspects. |
| Huawei | Not sure | As commented, we are trying to understand how this large amount of data would come, and are required to transmit over a very short period of time? |
| Intel |  | We may revisit the AI management aspects after understanding more about the solution. |
| Lenovo, Motorola Mobility |  | We are positive to study these aspects e.g. for distributed AI. If these parts can not be studied in R17 due to time limit, we would prefer to have a study in R18. |
| ZTE | Control plane | As we said, SCTP has the benefits to guarantee the robustness and reliability, and it supports the data fragmentation so that AI data in a large size will not be transmitted at once. Hence, the AI data transmission via control plane seems a reasonable way |

**Moderator’s summary:**

**No consensus on how to support huge quantity of AI data transmission, via CP, UP, or MP.**

Besides solving huge data transmission issues, security of data transmission should also be considered because some AI data per UE basis and then ML model per UE basis are privacy. [1] also proposed that security address, e.g., IP-Sec or DTLS address, can be used to guarantee the security of AI data transmission.

**Question 3:** **Companies are invited to provide comments on whether security address (e.g., IP sec or DTLS address), or other methods to support and guarantee the security of AI data transmission?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Comments** |
| Ericsson |  | It is already possible to date to secure interface traffic with IPSec and other security techniques. It is not clear what else RAN3 should do in this respect. |
| Deutsche Telekom |  | W.r.t. security techniques we should involve SA3, especially if we go beyond features already defined on RAN interfaces. |
| Huawei | Not sure | In our understanding, the security of data should be guaranteed in a secure place (e.g. data center under the full control by operators); regarding the transmission, yes, we have IP sec or DTLS mechanism, but this should not be discussed in RAN3, and we think this is current mechanism. |
| Intel |  | Share the same view with Ericsson. |
| Lenovo, Motorola Mobility |  | More study is needed before we can have a clear answer. Not only security issue but also privacy issue should be taken into account. |
| ZTE | Yes | Security of data transmission should be considered because some AI data per UE basis and then ML model per UE basis are privacy. Hence, security address (e.g. IP-Sec or DTLS address) can be carried for control plane security protection to exchange or transfer different measurements or ML models information during the interface setup/modify procedure between NG-RAN nodes. The encrypted and encapsulated data can achieve the purpose of integrity protection, replay protection and confidentiality protection. |

**Moderator’s summary:**

**Security address (e.g., IP sec or DTLS address) could be support and guarantee the security of AI data transmission, which could be discussed later involving SA3.**

Moreover, [1] proposed that security address (e.g., IP-Sec or DTLS address) can be carried to exchange or transfer different measurements or ML models related information during the interface setup/modify procedure, as shown below. The encrypted and encapsulated data can achieve the purpose of integrity protection, replay protection and confidentiality protection.

**

Figure 1. Interface security setup procedure between NG-RAN nodes

**Question 4:** **Companies are invited to provide their views on whether security address (e.g., IP-Sec or DTLS address) can be carried to exchange or transfer different measurements or ML models related information during the interface setup/modify procedure?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Yes/No** | **Comments** |
| Ericsson |  | This work is based on current architecture and interfaces. Current interfaces already provide the possibility of being security protected. We do not see the reason for this discussion right now |
| Deutsche Telekom |  | Same view as E///.  |
| Huawei | Clarifications needed | No problem with the above signaling follow, but not sure if we should discuss this in RAN3 or not. Seems to us, this is similar with what transmission layer should do before setting up an interface, not sure if we misunderstood anything. |
| Intel |  | Share the same view with Ericsson. |
| Lenovo, Motorola Mobility |  | More study is needed before we can have a clear answer. Not only security issue but also privacy issue should be taken into account. |
| ZTE | Yes | Security address (IP-Sec and DTLS address) can be carried in the interface setup/modify procedure for AI functionality if we agree to use these security address to guarantee the security of the AI data transmission. |

**Moderator’s summary:**

**Security address (e.g., IP sec or DTLS address) could be support and guarantee the security of AI data transmission, which could be discussed later involving SA3.**

# Conclusion, Recommendations [if needed]

If needed

# References

1. R3-213760, Analysis on data transmission for RAN AI (ZTE Corporation, China Unicom)