**3GPP TSG-RAN WG2 Meeting #126 \_R2-2405950**

**Fukuoka, Japan, 20th May – 24th May, 2024**

**Agenda Item: 8.2.5**

**Source: Huawei, HiSilicon**

**Title: Report of [AT126][022][AIoT] CB on 4 step RA**

**Document for: Discussion and Decision**

# 1 Introduction

**[AT126][022][AIoT] CB on 4 step RA (Huawei)**

 Intended outcome: Discuss msg 4 details and contention resolution.

 Deadline: 05-24-24

# 2 Discussion

***4-step CBRA procedure***

[R2-2404926](file:///C%3A%5CUsers%5Cpanidx%5COneDrive%20-%20InterDigital%20Communications%2C%20Inc%5CDocuments%5C3GPP%20RAN%5CTSGR2_126%5CDocs%5CR2-2404926.zip) Discussion on random access of Ambient IOT Spreadtrum Communications discussion Rel-19

[R2-2404811](file:///C%3A%5CUsers%5Cpanidx%5COneDrive%20-%20InterDigital%20Communications%2C%20Inc%5CDocuments%5C3GPP%20RAN%5CTSGR2_126%5CDocs%5CR2-2404811.zip) Discussion on random access for Ambient IoT Lenovo discussion Rel-19

[R2-2405107](file:///C%3A%5CUsers%5Cpanidx%5COneDrive%20-%20InterDigital%20Communications%2C%20Inc%5CDocuments%5C3GPP%20RAN%5CTSGR2_126%5CDocs%5CR2-2405107.zip) Further on AIoT random access Nokia discussion FS\_Ambient\_IoT\_solutions

***Agreements for 4-step CB RACH***

**1 A-IoT Msg1: the device sends an ID to the reader. ID is a random ID generated by device (FFS how it is generated, e.g. randomly generated or generated based on Device ID). FFS on ID size**

**2 A-IoT Msg2: the reader echos the ID received in Msg1. Further information may be included in mgs2 based on RAN1 agreements**

**3 *A-IoT Msg3: device sends Device ID and/or any other upper layer data (depending on upper layer request)***

***FFS on contention resolution based on step 4***

***4 A-IoT Msg4: FFS on the need and presence for this***

Discussion for contention resolution and Msg4

Comparison:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Broadcast message before | Msg1 | Msg2 | Msg3 | Msg4 |
| NR 4-step RACH | RACH configuration | Time/ frequency/ Preamble sequence | UL TA, UL grant | CCCH (e.g. ue-Identity) | UE Contention Resolution Identity (part of the CCCH SDU) |
| A-IoT 4-step CBRA | Parameters for Msg1 PDRCH transmission | Time/ frequency domain access opportunities, Random ID | Echo the random ID | upper layer data | ? |

Calculation: A-IoT Msg3 collision of one specific A-IoT device:

, N is device number to access, Q is number of access opportunities.

Question 1: The device considers the contention resolution as successful, if the Msg2 including the same random ID in Msg1 is received?

* Assuming the size of random ID in Msg1 is at least 16-bits. FFS more bits are needed.
* Msg4 will not be used mainly for contention resolution. We can discuss the Msg4 details in another discussion (for Msg3 transmission).

QC: Agree with the equation with 16 bit assumption. It depends on the N. CATT: agree with the calculation. Consider Msg2 can address the contention. Xiaomi: 4-step like? Intel: We ignore the terms for now. The Msg3 collision is already low enough. Lenovo: Has doubt on the difference between A-IoT and NR RACH. In A-IoT, even there is the contention still in Msg3, we can ignore the issue if probability is low. VDF: NR use about 40bits for contention resolution. It is related to fast access, unlike A-IoT. Intel claims understanding to VDF. For latency, the Msg4 increase the latency for inventory a lot. There is no requirement for reliability. Vivo: 1) reader cannot detect the collision. The trigger can be re-tran. 2) Collision is very low after Msg2. 3) Even if the Msg3 collision happens, CN can address the issues. Therefore, there is no need of Msg4. Interdigital: Even 16bits is to be discussed, as long as the Q is suitable, Msg4 is not used for contention. Msg4 is another discussion. ZTE: Agree. Msg4 for acknowledgement for Msg3. Msg4 can do both ACK and contention resolution. Samsung: Agree Msg2 can address the contention if 16bit is used in Msg1. FW: Msg3 is actually not mainly for the AS layer contention, more like the upper layer ID purpose. LG: Prefer Msg4 but OK with Msg2 for contention resolution. We can even consider the Msg3 is already out of the RA procedure. MTK: This is just modelling issue for LG comments. Agree with FW see the need of temp ID somehow. OPPO: Compare to the limited RO in NR, A-IoT has this sufficient 16 bits random ID in Msg1. Apple: Msg2 can be used for contention resolution. This depends on the number of devices. Msg3 is still RA. Ericsson: Agree with the calculation, with the reasonable number of ID bits, Q, N. Then, the collision probability of Msg3 is extremely low. RFID use this without any issue. CMCC: Agree with Apple. If the N is too large, the collision could be still there. Prefer Msg4, but can understand the concern of Msg4 from other companies.

Second round=> QC: This depends on the assumption of Q,N, ID size. It does not matter on the boundary. We may not need to say or not accurate to say “Msg2 address the contention”. Intel: Of course, we don’t need to ensure the 100% contention resolution at all. Msg3 failure has other reason. ZTE want to use the Msg4 for the addressing the following data transmission. MTK: We may end up with many steps. We can somehow use the ID in Msg1 for scheduling. QC want to further discuss how to indicate the Q, ID size.

Rapp: feel companies already discuss the **data transmission function for Msg3 a**nd the one after Msg4. OPPO: If Msg3 includes the device ID, Msg4 is used for ACK. The ID in Msg1 can be used for data transmission purpose.

Rapp: There is another issue for addressing the transmission in layer1. This is still FFS.

* We tend to discuss the modeling of the RA completion later (whether Msg3 is still random access).
* We tend to wait for the PHY design on the addressing of scheduling.

Question 2: Msg4 can be considered to handle the Msg3 transmission failure (due to various reasons). Msg4 does not need to be always sent (at least for inventory only case. FFS for the case with more data transmission)? Msg4 (R2D after D2R transmission) usage/presence can be further discussed.

~~Question 3: Options of the Msg4 content (when needed)?~~

* ~~Option 1: the 1bit NACK;~~
* ~~Option 2a: the 1bit ACK?;~~
* ~~Option 2b: (part) of the Msg3 content?;~~

QC: Agree with the Msg4 can be used to handle the failure. And Msg4 does not have to be always send. Wants to postpone the Msg4 use case/usage. Vivo: There is no Msg4 for inventory. CATT: Agree with FFS for Msg4 usage, OPPO, Intel: Consider the D2R is the feedback for R2D. There is no need of the specific ACK/NACK, Ericsson: No rush to make decision on Msg4. VDF: Msg4 is not random access any more. TCL: agree with VDF. ZTE: Agree somehow Msg4 dose not have to be in random access.

*WF for “4-step” CBRA (consensus):*

* Proposal 1: The device considers the contention resolution as successful, if the Msg2 including the same random ID in Msg1 is received. RAN2 assumes the size of random ID in Msg1 should be sufficient for contention resolution purpose.
* Proposal 2: Msg4 (i.e. the subsequent R2D transmission after D2R transmission) does not need to be always sent in random access. Msg4 can be considered to handle the Msg3 transmission failure (due to various reasons). Msg4 usage/presence can be further discussed.
	+ We will not use “Msg4” for further discussion.

***2-step CBRA procedure***

[R2-2404811](file:///C%3A%5CUsers%5Cpanidx%5COneDrive%20-%20InterDigital%20Communications%2C%20Inc%5CDocuments%5C3GPP%20RAN%5CTSGR2_126%5CDocs%5CR2-2404811.zip) Discussion on random access for Ambient IoT Lenovo discussion Rel-19

Proposal 4: For 2-step A-IoT random access procedure, device includes device id information and data in the very first message to the reader. Detailed steps are as following:

A-IoT Msg0: trigger message from the reader

A-IoT MsgA: the device sends an ID, as well as data (e.g. device ID) to the reader.

A-IoT MsgB: the reader confirm the ID received in MsgA.

[R2-2404536](file:///C%3A%5CUsers%5Cpanidx%5COneDrive%20-%20InterDigital%20Communications%2C%20Inc%5CDocuments%5C3GPP%20RAN%5CTSGR2_126%5CDocs%5CR2-2404536.zip) Access Procedure for Ambient IOT InterDigital discussion Rel-19 FS\_Ambient\_IoT\_solutions

Proposal 3: Contention-based access procedure using 2-step RACH like procedure consists of the following messages: 1) A first (D2R) message containing at least a data PDU and a device ID (FFS how to determine the ID); 2) A second (R2D) message containing at least the contention resolution ID.

[R2-2405107](file:///C%3A%5CUsers%5Cpanidx%5COneDrive%20-%20InterDigital%20Communications%2C%20Inc%5CDocuments%5C3GPP%20RAN%5CTSGR2_126%5CDocs%5CR2-2405107.zip) Further on AIoT random access Nokia discussion FS\_Ambient\_IoT\_solutions

Proposal 6: For the 2-step contention-based access, the very first D2R transmission in Msg1 consists of a random device identifier generated by the device and the device ID.

Proposal 7: For the 2-step contention-based access, the device considers the contention is resolved and the access procedure is successful when it receives a device ID in Msg2 similar to the device ID it sent in Msg1.

Discussion 2-step CBRA:

***Possible Agreements for 2-step CB RACH***

**1 A-IoT Msg1:the device sends an ID to the reader. ID is a random ID generated by device (FFS how it is generated, e.g. randomly generated or generated based on Device ID). FFS on ID size. The device also sends Device ID and/or any other upper layer data (depending on upper layer request)**

**2 A-IoT Msg2: the reader echos the ID received in Msg1. Further information may be included in mgs2 based on RAN1 agreements**

**3 *~~A-IoT Msg3:~~*** ***~~device sends Device ID and/or any other upper layer data (depending on upper layer request)~~***

Question 4: A-IoT Msg2: the reader echos the random ID received in Msg1?

On the formulation of the 2-step solution:

* Lenovo: Agree with proposal. Apple: Device ID can be used for contention. OPPO: Agree with Apple. MTK: The device ID should not be used for contention resolution. We should further study. Samsung: Think this device ID should be sent. CATT: There should not be large data. Xiaomi: Agree with the formulation. QC: Agree with the formulation. It is beneficial for CFRA only.

Whether we further discuss the 2-step solution:

* Intel: Don’t support this 2-step CBRA at all. It is just the waste of time/resource. Interdigital: RAN2 agree we can study. We may do the decision later. Xiaomi: We should first study and then we decide. LG: With the previous agreements, there is no need of further another 2-step procedure. Vivo see no security concern of Msg1 including device ID. CATT: see the concern of segmentation due to Msg1 including Device ID.
*

*Proposal (not consensus): For the formulation of 2-step CB RACH:*

* A-IoT Msg1:the device sends an ID to the reader. ID is a random ID generated by device (FFS how it is generated, e.g. randomly generated or generated based on Device ID). FFS on ID size. The device also sends Device ID and/or any other upper layer data (depending on upper layer request) FFS on the need of random ID.
* A-IoT Msg2: the reader echos the ID received in Msg1. Further information may be included in mgs2 based on RAN1 agreements.

3 Conclusion

This contribution makes the following proposals:

***“4-step” CBRA procedure***

Proposal 1: The device considers the contention resolution as successful, if the Msg2 including the same random ID in Msg1 is received. RAN2 assumes the size of random ID in Msg1 should be sufficient for contention resolution purpose.

Proposal 2: “Msg4” (i.e. the subsequent R2D transmission after D2R transmission) does not need to be always sent in random access. “Msg4” can be considered to handle the Msg3 transmission failure (due to various reasons). “Msg4” usage/presence can be further discussed.

* RAN2 will not use “Msg4” term for further discussion of the random access.

***“2-step” CBRA procedure***

Proposal 3: For the formulation of “2-step-like” CBRA, if RAN2 intends to further study:

* A-IoT Msg1: The device sends Device ID and/or any other upper layer data (depending on upper layer request). FFS on the need of random ID.
* A-IoT Msg2: the reader echos the ID received in Msg1.