**3GPP TSG-RAN WG2 Meeting #113bis-e R2-210xxxx**

**Online, 4 - 12 April, 2021**

**Agenda item:** 8.17

**Source:** Huawei, HiSilicon

**Title:** Summary of [AT113bis-e][026][NR17] SA related (Huawei)

**Document for:** Discussion and Decision

# 1. Introduction

This document attempts to summarize the following offline discussion.

* [AT113bis-e][026][NR17] SA related (Huawei)

Scope: Treat False Base Station Detection and Network Sharing Multiple SSB R2-2102669, R2-2103864, R2-2104134, R2-2104135, R2-2102676, R2-2103221, R2-2104161, R2-2104062, R2-2104102.

Phase 1, determine agreeable parts, Phase 2, for agreeable parts Work on CRs, LS out.

Intended outcome: Report and Agreed-in-principle CRs, Approved LS out, if applicable

Deadline: Schedule A

# 2. Discussion (Phase 1)

## 2.1 False Base Station Detection

The following contributions are discussing false base station according to SA3 LS in R2-2102669. The proposals are copied here.

|  |  |  |
| --- | --- | --- |
|  | [R2-2103864](file:///D:\Documents\3GPP\tsg_ran\WG2\TSGR2_113bis-e\Docs\R2-2103864.zip) RAN impact on the false based station detection Apple | Observation 1: During CGI reporting procedure, the CONNECTED UE acquires the indicated neighbor cell’s MIB/SIB1, report the CGI in SIB1 of the neighbor cell to NW via measurement report.  Observation 2: The SI HASH reporting via logged MDT procedure is feasible from RAN2 perspective.  Observation 3: The SI HASH reporting via CEF reporting procedure is feasible from RAN2 perspective.  Proposal: The SI HASH reporting solution is feasible from RAN2 perspective. |
|  | [R2-2104134](file:///D:\Documents\3GPP\tsg_ran\WG2\TSGR2_113bis-e\Docs\R2-2104134.zip) Discussion on SA3 LS on false base statation detection Huawei, HiSilicon | Proposal 1: To support solution #4, RAN2 needs to specify reporting signalling and procedure for hash value reporting, as well as new UE behaviour of reading SIBs other than MIB/SIB1 in RRC\_CONNECTED mode.  Proposal 2: Current RAN2 specifications support the reporting of RSRP/RSRQ/RSSI/beam level information of SSB or CSI-RS, radio link failure information in *RLF-Report-r16* as well as establishment failure related information in *connEstFailReport-r16*. No more RAN2 work is expected to support reporting of reject\_info and signal\_info mentioned by SA3.  Proposal 3: RAN2 to reply to SA3 including proposal 1 and proposal 2. |
|  | [R2-2104135](file:///D:\Documents\3GPP\tsg_ran\WG2\TSGR2_113bis-e\Docs\R2-2104135.zip) Draft reply LS to SA3 on FBS detection Huawei, HiSilicon | RAN2 would like to thank SA3 for their further clarifications and feedback in the reply LS on false base station detection. Regarding SA3’s question on the feasibility, from RAN2’s perspective there is no showstopper identified to support an enriched measurement reports with a list of MIB/SIBs hashes but additional RAN2 work would be required.  Regarding hash value reporting   * To report hashes of system information is not supported in Rel-15 and Rel-16, therefore the new functionality needs to be specified in RAN2 to enable UE to report the hashes to the network.   Regarding reporting reject\_info and signal\_info mentioned by SA3   * The reporting RSRP/RSRQ/RSSI/beam level information of SSB or CSI-RS is supported since Rel-15. And reporting connection establishment failure and radio link failure is supported in Rel-16. RAN2 see no issue to reuse these existing information reporting procedure for false base station detection if needed. |

Since SA3 requests RAN2 to make evaluations on the feasibility of the solution #4, [1][2] discuss the RAN2 impact to support the solution. Basically, both contributions find the solution is feasible. In details,

* Regarding hash reporting, it is feasible from RAN2 perspective that a UE can report Hash of MIB and SIBs via CGI reporting and logged MDT procedure.
* Regarding UE reporting reject\_info and signal\_info, both contributions think Connection Establishment Failure report and existing RRM measurement reporting could be reused for this FBS detection purpose, no new RAN2 procedure is needed.

**Q1: Do companies agree the above views?**

|  |  |  |
| --- | --- | --- |
| Company | Agree(Yes/No) | Comments |
| Ericsson | Yes (but see comments) | We agree that reporting of hash of MIB and SIBs is feasible   * For UEs in RRC\_CONNECTED it should at least be possible to report hash of MIB and SIB1 of neighbour cells since UEs are already required to read MIB and SIB1 for CGI reporting. How to report hash of other SIBs is FFS. * For UEs in RRC\_IDLE/RRC\_INACTIVE it should be possible to report hash of MIB and SIBs for all cells that the UE is camping in. The UE should at least be able to report the hash of MIB and the SIBs that it normally reads, i.e. we may not want to force the UE to read additional SIBs. * We may want to reconsider using logged MDT for the hash reporting since logged MDT requires user consent and is a quite heavy feature that few UEs implement. A better option would be to extend the Mobility History Information (MHI) reporting or define a new procedure for this purpose.   For the other info requested by SA3, reject\_info and signal\_info, we think the description was somewhat vague in the the SA3 LS and SA3 report. It is correct that Connection Establishment Failure (CEF) report and existing RRM measurement reporting provides some information and can be re-used but we are not sure whether the information in these reports is sufficient for the purpose SA3 has in mind. For example, the CEF report can be used to count the number of connection establishment failures but it cannot provide the number of rejects since reject is not counted as failure. So we are not sure that no new RAN2 procedure would be needed. |
| Qualcomm | Yes (mostly) | From signaling point of view, reporting HASH is obviously feasible. However, we have concerns on introducing new procedures and UE power consumption. Therefore, we should only use the existing procedures/measurements where the UE already reads MIB/SIB1. For such cases, calculating the HASH and including in a report is relatively minimal impact to the UE. For Connected mode, CGI reporting is acceptable but only for reading SIB1 as in legacy reporting; there is no need for the UE to read other SIBs. Otherwise, CGI reporting will take a longer time and consumer more UE power. Reading other SIBs and MIB is not needed from security point of view as well. For Idle/Inactive, we would also prefer logged MDT. Agree with the rapporteur on reject info and signal info; existing procedures are sufficient. |
| ZTE(Zhihong) | Yes from signalling point of view | Report HASHs of SIBs is feasible from signalling point of view, but how to calculate this hash value needs further discussion.   * For signalling:   For connected mode reporting, we tends to agree with QC that for FBS detection, it is sufficient to read SIB1 as supported by current CGI report procedure and no further enhancements is need. For idle/inactive UEs, it is feasible to report HASH value in logged MDT.   * For HASH calculation   We think it needs to be clarify how to compute the HASH values to avoid complexity in implementation. Based on the method proposed in TR 33809, it is suggested to use SHA256 for HASH value computation, which means different SIB strings will lead to different HASH values. During reporting period, SIB content might be changing, e.g., SFNs, si-BroadcastStatus,valueTags..., which will lead to different HASH outputs. Therefore it needs to be further discussed how to do the calculation to mitigate the implementation complexity. |
| Huawei, HiSilicon | Yes | About reject\_info and signal\_info, we agree the description in SA3 LS is vague, so we also checked their TR, based on which we do not see new requirement not satisfied by current CEF. And since we could mention the CEF in our reply LS, SA3 can be aware what is supported already, and if they figure out new things to be supported by RAN2, we can still work on that.  About Hash reporting, we agree with Qualcomm, it is not supported right now that a UE in RRC\_CONNECTED mode to read SIBs other than SIB1, which may cause extra stand effort, we can mention it in response LS, and let SA3 to discuss if it is really necessary for FBS detection.  About Hash calculation, generally we understand it is in SA3 scope, SA3 will discuss the UE behaviour of Hash calculation similar as other key/security related information derivation approach. |
| OPPO | Yes | It is possible from signalling point of view to report the HASH of MIB/SIB for RRC\_CONNECTED mode UE via CGI reporting and for RRC\_IDLE/INACTIVE mode UE via logged MDT in RAN2.  However, RAN2 should consider the power saving to enable UE to do it. |
| MediaTek (Nathan) | Yes (with comments) | We generally agree with Qualcomm and Ericsson’s comments above. The request from SA3 was clear that they are interested in having the UE report the hash when it is already available; the UE should not be required to read additional SI for this. From the signalling point of view we see no obstacle to having a UE in RRC\_CONNECTED report SI hashes of which it is already aware.  Regarding reject\_info, we have the same comment as raised by Ericsson that the current failure count does not include reject events, and SA3 are probably interested in logging rejects as well, since a false base station could send an RRCReject. We should be clear about this distinction in any response to SA3, and allow them to indicate clearly if there is a requirement to enhance the information that the UE currently logs.  We should also be clear about what we understand signal\_info to comprise, so we don’t give any false impressions about what signal information the UE can recognise. The draft response from Huawei seems accurate in this respect.  Finally, we have some concern about reusing CGI reporting as suggested by some companies, because it seems disruptive for the UE in terms of interruption and power consumption if CGI reading were to become more frequently triggered. In our understanding, SA3 only asked about reporting hash values that the UE already holds, and we want to avoid the scenario that the gNB goes “hunting” for false base stations by triggering frequent CGI reading from a UE that would otherwise not be doing it. |
| Intel | Yes with comments | From the signalling perspective, it is feasible. However, as others also commented, having to perform SI reading for this purpose can be disruptive and power consuming.  Regarding Reject, we can provide details of what we currently include so that SA3 can evaluate if that is sufficient to meet their requirements. |

**Q2: If company’s answer to Q1 is yes, then regarding the response LS if the content in [3] can be agreeable in principle, or any comments.**

|  |  |  |
| --- | --- | --- |
| Company | Agreeable(Yes/No) | Comments |
| Ericsson | Yes | The LS looks fine in principle. For the hash reporting we think it would be good to mention that logged MDT is not the only option that can be used to report the hashes for UEs in RRC\_IDLE/RRC\_INACTIVE. As mentioned in the answer to previous question, it might be better to extend the Mobility History Information reporting or define a completely new procedure for this purpose. Therefore we suggest modifying the text as below.  Regarding hash value reporting   * To report hashes of system information is not supported in Rel-15 and Rel-16, therefore ~~the~~ new functionality needs to be specified in RAN2 to enable UE to report the hashes to the network. Whether this is achieved by extending one of the existing procedures (e.g. logged MDT or mobility history information) or by defining a new procedure requires further study. |
| Qualcomm | Yes (mostly) | We would also prefer to agree and include which procedures will be used. It should be CGI reporting in Connected mode and logged MDT in Idle/Inactive mode. We should also emphasize that no new measurements will be introduced for this purpose, i.e. it will be just HASH calculation and inclusion in the report. |
| ZTE(Zhihong) | Yes | At this stage, the content in LS is sufficient to answer SA3’s questions, detailed design can be discussed further in RAN2. |
| Huawei, HiSilicon | Yes | Regarding the suggestion from Ericsson and Qualcomm, we are fine to mention that the CGI reporting and logged MDT are feasible because these are the procedures SA3 requested RAN2 to evaluate on, and regarding other possible procedures we could further study as per SA3’s request later. |
| OPPO | Yes | The response LS is fine to me. |
| MediaTek (Nathan) | Mostly | What’s included in the reply is fine, but it doesn’t clarify all the potential RAN2 impact. As noted by others, we should indicate which procedures are involved, and that we do not want to introduce new requirements for reading additional SIBs in RRC\_CONNECTED.  We also think it’s important to clarify RAN2 understanding of the current support for reject\_info, as discussed in our comments to Q1: The connection failure information currently logged by RAN2 accounts for failure events but not rejections, and there would be RAN2 impact to add logging of rejection events. |
| Intel | Yes, mostly | In general the LS looks fine to us with a couple of comments.  As others also mentioned, additional information on the consequences should also be included.  The information provided as part of the current procedure must also be included as commented above. |

## 2.2 Network Sharing Multiple SSB

There are three questions from SA5 in R2-2102676. The contributions in R2-2103221/R2-2104061/R2-2104062/R2-2104102 give the analysis and corresponding answers.

|  |  |
| --- | --- |
| SA5’s questions | Answers provided in company contributions |
| 1. Whether the feature multi-SSBs in a carrier is mature and stable in RAN specification? Why the Annex B.2 Multiple SSBs in a carrier in TS 38.331 is informative? | R2-2103221: The feature is mature and stable in RAN specification. Note however, that there is only 1 CD-SSB per cell. Other SSBs (located at different frequencies) would not contain RMSI and can have different PCI than the CD-SSB.  R2-2104062: RAN2 understand the feature multi-SSBs in a carrier is mature and stable in RAN specifications. To avoid unnecessary limitation on implementation, the example of multi-SSB in a carrier has been captured as informative text in Annex B as deployment scenario examples.  R2-2104102: The feature multi-SSBs in a carrier is mature and stable in RAN specification. The Annex B.2 is an example to illustrate the deployment of the feature. |
| 1. Is the feature multiple SSBs in a carrier specific for NG-RAN sharing? | R2-2103221: No, it is more about supporting multiple BWPs (as shown in Annex B.2).  R2-2104102: The feature multiple SSBs in a carrier is not specific for NG-RAN sharing. The feature multiple SSBs in a carrier and the feature PLMN sharing are independent features. |
| 1. Whether the feature multiple SSBs in a carrier can be used to support NG-RAN sharing (i.e. the cell associated to different SSBs can be used by different operators)? | R2-2103221: No, the operator reference (PLMN etc..) is located on CD-SSB only.  R2-2104062: For multi-SSB in a carrier, the PLMNs broadcast in RMSI associated with each CD-SSB can be different to support different operators.  R2-2104102: The feature multiple SSBs in a carrier can be used to support NG-RAN sharing by implementation, e.g. broadcast different PLMNs in the SIB1s associated to different CD-SSBs while the cell channel bandwidths are overlapped or even same. If this is used, it is transparent to the UEs. |

Basically, the feature of multiple SSBs in a carrier is quite clear from RAN2’s perspective, and the company’s answers are similar to some extent. Thus rapporteur suggest to discuss reply LS directly.

Regarding the draft LS provided in R2-2103221/R2-2104062/R2-2104102, the main difference is: in R2-2103221 the answer to 3) is no, but in R2-2104062 and R2-2104102 the answer is kind of yes with more explanations. Rapporteur understands the reason R2-2103221 says no is because the terminology of “RAN sharing” has specific meaning in RAN, which is one physical cell can be shared by multiple operators and a PLMN list containing CGI associated to each PLMN is broadcasted in that cell. However in SA5’s LS the “NG-RAN sharing” is more like a general description as long as different cells/SSBs within the same bandwidth can be used by different operators. In this case, the rapporteur thinks it could be better RAN2 provides more detailed answer to 3) in reply LS to avoid any misalignment between SA5 and RAN2.

**Q3: Which answer to 3) is agreeable in principle?**

Option 1: The answer in R2-2103221

Option 2: The answer in R2-2104062/R2-2104102

|  |  |  |
| --- | --- | --- |
| Company | Option1/Option2 | Comments |
| Qualcomm | Option 1 | Agree with the analysis in 3221. Using SSBs for different PLMNs as proposed by others is a new scheme and was not discussed/envisioned before, even though it can be done as a NW implementation. More importantly, it is not related to RAN sharing. In RAN2/RAN3 terminology, RAN sharing is for sharing a cell between different PLMNs. We should clarify this point to SA5 so all groups have the same understanding. |
| ZTE(Yuan) | Option 2 | * As explained in R2-2104061, for multi-SSB in a carrier, two CD-SSBs can be associated with different RMSI and the PLMNs broadcast in *SIB1->cellAccessRelatedInfo->plmn-IdentityList* can also be different to support different operators while the cell channel bandwidths are overlapped or even same. * From NW’s perspective, we understand supporting RAN sharing via the multiple SSBs in a carrier can be done in implementation and there is no need to put unnecessary limitation. * There is no need for us to debating on what is RAN sharing as SA5 has explained what exactly they are asking: *Whether the feature multiple SSBs in a carrier can be used to support the case that the cell associated to different SSBs can be used by different operators?* And the answer is obviously Yes. |
| Huawei, HiSilicon | Option 2 | We also prefer to provide more information to SA5 to help they understand how this multi-SSB in a carrier to be used for different PLMNs instead of answering no support of RAN sharing directly. |
| OPPO | Option 2 | It is clearer. |
| MediaTek (Felix) | Option 2 | We prefer to take the reply LS in R2-2104102 as baseline, which explain the view quite clearly.  The key difference between option 1 and 2 is that whether two different CD-SSB within a carrier could be used by different operator. In our view, it is possible. From UE perspective, they are two different intra-band cell and could belong to different PLMN. However, there no such use case in real deployment. |
| Ericsson | Option 2 |  |

If companies choose option2 in Q3, then one of R2-2104062 and R2-2104102 should be chosen as baseline of the response LS. Between R2-2104062 and R2-2104102, in R2-2104062 the answer to 2) is missing, while in R2-2104102 the answers are comprehensive. In addition, the clarification on the 38.300 figure is given in R2-2104102 to help SA5 to understand the feature of multi-SSBs in a carrier.

**Q4: If companies choose option 2 in Q3, which one between R2-2104062 and R2-2104102 is preferred?**

|  |  |  |
| --- | --- | --- |
| Company | R2-2104062/R2-2104102 | Comments |
| ZTE | R2-2104062, as the proponent | * First to clarify that the answer to 2) is not missing in R2-2104062, we understand the answer shown below would be sufficient for both 2) and 3) and that is why we put them together.   *2)Is the feature multiple SSBs in a carrier specific for NG-RAN sharing?*  *3)Whether the feature multiple SSBs in a carrier can be used to support NG-RAN sharing (i.e. the cell associated to different SSBs can be used by different operators)?*  **RAN2 answer**: For multi-SSB in a carrier, the PLMNs broadcast in RMSI associated with each CD-SSB can be different to support different operators.   * We are also open to further discuss and improve the draft LS in the phase 2 discussion if we go for option 2. ^\_^ |
| Huawei, HiSilicon | R2-2104102 | For Q 2), an answer is needed. RAN2 needs to clarify that the multi-SSB in a carrier was not defined for RAN sharing purpose, but it could be used for different PLMNs in an implementation way from network side. (From UE side, it sees multiple cells, no special handling anyway.) |
| OPPO | R2-2104062 | No strong opinion. |
| MediaTek (Felix) | R2-2104102 | We agree with Huawei. |
| Ericsson | R2-2104102 | Gives some more background from our specs to SA5, but no strong view. |

# 3. Conclusion

TBD…

4. Contact information

|  |  |
| --- | --- |
| Company | Email |
| Qualcomm, Ozcan Ozturk | [oozturk@qti.qualcomm.com](mailto:oozturk@qti.qualcomm.com) |
| ZTE(Yuan) | [gao.yuan66@zte.com.cn](mailto:gao.yuan66@zte.com.cn) |
| ZTE(Zhihong) | [qiu.zhihong@zte.com.cn](mailto:qiu.zhihong@zte.com.cn) |
| Huawei, Hisilicon | wangrui46@huawei.com |
| OPPO | wangshukun@oppo.com |
| MediaTek (Felix) | Chun-fan.tsai@mediatek.com |
| MediaTek (Nathan) | [Nathan.Tenny@mediatek.com](mailto:Nathan.Tenny@mediatek.com) |
| Intel | Sudeep.k.palat@intel.com |