**3GPP TSG-RAN WG2 Meeting #113 electronic R2-21xxxxx**

**Online, January 25th – February 5th 2021**

**Agenda Item: X.X.X**

**Source: Sharp**

**Title: [Post112-e][254][R16 MOB] Issue on failure handling of handover without key change for the UE configured with attemptCondReconfig (Sharp)**

**Document for: Discussion, Decision**

# 1 Introduction

This document is to collect companies comment in the following email discussion:

* [Post112-e][254][R16 MOB] Issue on failure handling of handover without key change for the UE configured with attemptCondReconfig (Sharp)

Scope: Discuss issues raised by [R2-2010205](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_112-e/Docs/R2-2010205.zip) and discussed in email [AT112-e][211][MOB] as per [R2-2010719](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_112-e/Docs/R2-2010719.zip) to understand whether there are security issues and if there are, what can be done to mitigate them.

Intended outcome: Summary + agreeable CRs (if any)

Deadline: Long

For this email discussion, it is proposed to have the following two phases:

Phase 1: Discuss whether there are security issues on handover failure handling for the UE configured with *attemptCondReconfig*. (Deadline: Jan 04, 23:59UTC)

Phase 2: If the issue is confirmed in Phase 1, discuss detailed specification changes to solve the issue and prepare agreeable CR. (Deadline: Jan 12, 23:59UTC)

# 2 Discussion

## 2.1 Phase 1

In Phase 1, an example scenario which would cause a security issue (reuse of the same key stream) is introduced in the subclause 2.1.1, and it is discussed whether the example scenario is valid and the security issue is caused in the subclause 2.1.2.

### 2.1.1 Background

In the AS security section (subclause 5.3.1.2) in TS 38.331 [1], it is explained that using the same COUNT value for the same security key (at the same radio bearer), i.e. the same keystream, is not allowed.

|  |
| --- |
| 5.3.1.2 AS Security  …  For each radio bearer an independent counter (*COUNT*, as specified in TS 38.323 [5]) is maintained for each direction. For each radio bearer, the *COUNT* is used as input for ciphering and integrity protection.  It is not allowed to use the same *COUNT* value more than once for a given security key. As specified in TS 33.501 subclause 6.9.4.1 [11], the network is responsible for avoiding reuse of the *COUNT* with the same RB identity and with the same key, e.g. due to the transfer of large volumes of data, release and establishment of new RBs, and multiple termination point changes for RLC-UM bearers and multiple termination point changes for RLC-AM bearer with SN terminated PDCP re-establishment (COUNT reset) due to SN only full configuration whilst the key stream inputs (i.e. bearer ID, security key) at MN have not been updated. In order to avoid such re-use, the network may e.g. use different RB identities for RB establishments, change the AS security key, or an RRC\_CONNECTED to RRC\_IDLE/RRC\_INACTIVE and then to RRC\_CONNECTED transition.  … |

However in the following example scenario (illustrated in Figure 1), the same key stream may be used by SRB1 (which was also introduced in [2][3]).



**Figure 1: Example scenario 1**

Step 1. The UE is configured with CHO candidate cells: Cell X and Cell Y which are both not configured with key change (i.e., *masterKeyUpdate)*. Also, the UE is configured with *attemptCondReconfig*. The UE holds COUNT value 'N' and security key A in source cell just before performing CHO in the step 2.

Step 2. CHO condition to Cell X is met and the UE performs CHO to the candidate Cell X without key change. If contention based random access is applied, COUNT value 'N' with key A is used for transmitting *RRCReconfigurationComplete* message as Msg3 by SRB1, and COUNT value is incremented to 'N+1'.

Step 3. However if the handover fails, the UE reverts back to the source configuration that was used just before the handover execution and performs the RRC re-establishment procedure. According to NOTE 1 of 5.3.5.8.3, all state variables, i.e. including COUNT value, are reverted. This means COUNT value becomes 'N' again.

Step 4. If the selected cell during the RRC re-establishment procedure is the candidate Cell Y, the UE initiates CHO because *attemptCondReconfig* is configured as assumed in the step 1. As Cell Y is configured without key change, the UE does not update the key and the same COUNT value 'N' with the same key A to transmit *RRCReconfigurationComplete* massage by SRB1.

Consequently, the same key stream is used.

### 2.1.2 Phase 1 discussion

Regarding the above example scenario:

**Question 1: Do companies agree that the assumed configurations and conditions in the step 1 are valid?**

Step 1. The UE is configured with CHO candidate cells: Cell X and Cell Y which are both not configured with key change (i.e., *masterKeyUpdate)*. Also, the UE is configured with *attemptCondReconfig*. The UE holds COUNT value 'N' and security key A in source cell just before performing CHO in the step 2.

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Ericsson | Yes |  |
| ZTE | Yes |  |
| Intel | Yes |  |
| Nokia | Yes | The procedure for T304 expiry seems to state the UE reverts back to the configuration in the source PCell. This is in principle fine, but maybe it could be considered if the state variables should also be reverted (even though, as per the current NOTE, they are). |
| LG | Yes |  |
| MediaTek | Yes |  |
| ITRI | Yes |  |
| Apple | Yes |  |
| Samsung | Yes |  |
| Huawei, HiSilicon | Yes |  |
| CATT | Yes |  |

**Question 2: Do company agree that the scenario in the step 2 could happen?**

Step 2. CHO condition to Cell X is met and the UE performs CHO to the candidate Cell X without key change. If contention based random access is applied, COUNT value 'N' with key A is used for transmitting *RRCReconfigurationComplete* message as Msg3 by SRB1, and COUNT value is incremented to 'N+1'.

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Ericsson | Yes | Also data could be transmitted on DRBs in MSG3 if the UL grant is large enough and the UE has pending data in its UL buffer. Wouldn’t the same issue then also apply for the DRBs? |
| ZTE | Yes | Agree with Ericsson that the same issue may also apply for DRBs. |
| Intel | Yes | Agree it is applied for both SRB and DRBs. |
| Nokia | Yes |  |
| Sharp | Yes | Agree with Ericsson data could be transmitted on DRBs in Msg3. So this is applied for both SRB and DRB. |
| LG | Yes |  |
| MediaTek | Yes | Agree that this discussion should be applied for both SRB and DRB. |
| ITRI | Yes |  |
| Apple | Yes |  |
| Samsung | Yes |  |
| Huawei, HiSilicon | Yes |  |
| CATT | Yes |  |

**Question 3: Do companies agree that the procedure described in the step 3 will happen according to the current specification [1]?**

Step 3. However if the handover fails, the UE reverts back to the source configuration that was used just before the handover execution and performs the RRC re-establishment procedure. According to NOTE 1 of 5.3.5.8.3, all state variables, i.e. including COUNT value, are reverted. This means COUNT value becomes 'N' again.

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Ericsson | Yes |  |
| ZTE | Yes |  |
| Intel | Yes |  |
| Nokia | Yes | Side comment: we wonder why this important behaviour was captured in the NOTE. |
| LG | Yes |  |
| MediaTek | Yes |  |
| ITRI | Yes |  |
| Apple | Yes |  |
| Samsung | Yes |  |
| Huawei, HiSilicon | Yes |  |
| CATT | Yes |  |

**Question 4: Do companies agree that the procedure described in the step 4 will happen according to the current specification [1]?**

Step 4. If the selected cell during the RRC re-establishment procedure is the candidate Cell Y, the UE initiates CHO because *attemptCondReconfig* is configured as assumed in the step 1. As Cell Y is configured without key change, the UE does not update the key and the same COUNT value 'N' with the same key A to transmit *RRCReconfigurationComplete* massage by SRB1.

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Ericsson | Yes |  |
| ZTE | Yes |  |
| Intel | Yes |  |
| Nokia | Yes | If the COUNT is not reset but reverted. |
| LG | Yes |  |
| MediaTek | Yes |  |
| ITRI | Yes |  |
| Apple | Yes |  |
| Samsung | Yes |  |
| Huawei, HiSilicon | Yes |  |
| CATT | Yes |  |

**Question 5: Do companies agree that there is the security issue (reuse of key stream) in the example scenario?**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Ericsson | Yes | Today the security may not be that severe but if more information gets added to the *RRCReconfigurationComplete* in the future it could be a problem. So we think this issue should be fixed.  If data can be sent in MSG3 as noted in our answer to question 2 the problem would be worse. |
| ZTE | Yes |  |
| Intel | Yes |  |
| Nokia | Yes, but | we do not think the scenario would be very common, but agree that it may occur, according to the current specification |
| LG | Yes, but | We think that this issue can be avoided by network implementation. For example, if the network always changes the security key for CHO, this issue does not happen.  Considering above, if the spec change is needed, we can add a note that the network always changes the security key for CHO. |
| MediaTek | Yes | This may not be a very common case but we should try to fix the problem. Also, we think CHO without security key change should be supported.  One simple way is that the network never set *attemptCondReconfig* for handover without key change. This prohibits “CHO recoverd by CHO” witout key change, but should be fine since CHO is more robust and rarely fails. But for scenario 2 below, there may be concern to prohibit “HO recovered by CHO” if security key is not changed. |
| ITRI | Yes, but | Agree with LG that the reuse of key stream can be avoided by network implementation. |
| Apple | Yes, but | We also agree with LG that the problem could be avoided by NW implementation. |
| Samsung | Yes | We agree with LG’s observation that it can be handled by NW implementation. The problem could be avoided by changing the security key for CHO if configured together with attemptCondReconfig. |
| Huawei, HiSilicon | Yes, but | We share the same view as LG that the problem can be solved if the network always includes the *masterKeyUpdate* for the CHO candidate cell. |
| CATT | Yes | Agree with LG that the issue can be avoided if the network always change the security key for CHO. |

The example scenario in Figure 1 only focuses on CHO failure case. However the same key stream reuse issue may also occur in normal handover failure case as illustrated in Figure 2 below.



**Figure 2: Example scenario 2**

The difference between Figure 1 and Figure 2 is the UE receives *RRCReconfiguration* message with *reconfigurationWithSync* (without *masterKeyUpdate*) in the step 2 and performs normal handover without key change to Cell Z which may or may not a CHO candidate cell. And the other assumptions from the step 1 to the step 4 are the same with the example in Figure 1 (including contention based random access is applied in the step 2).

**Question 6: Do companies agree that there is also the security issue (reuse of key stream) in the example scenario in Figure 2?**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Ericsson | Yes |  |
| ZTE | Yes |  |
| Intel | Yes |  |
| Nokia | Yes | This issue does not seem to depend on whether CHO or HO was attempted. |
| LG | Yes but | If the network always changes the security key, the example scenario will not happen. |
| MediaTek | Yes |  |
| ITRI | Yes, but | The reuse of key stream can be avoided by network implementation. |
| Apple | Yes, but | Agree with LG. |
| Samsung | Yes | We have same understanding as LG that it can be avoided by NW like in the previous issue |
| Huawei, HiSilicon | Yes, but | The problem can be solved if the network always includes the *masterKeyUpdate* for the CHO candidate cell. |
| CATT | Yes |  |

**Question 7: Do companies have any other comments?**

|  |  |
| --- | --- |
| Company | Comments |
| Ericsson | Keystream reuse can also occur even if the handover is performed with key change if handover is executed to the same cell twice.   1. UE performs CHO or normal handover to cell X (with key change) and sends the handover complete message in MSG3 using key B and COUNT = 0 2. The first handover fails and the UE performs cell selection 3. In the cell selection, the UE selects the same cell as for which the handover just failed, i.e. cell X. 4. Since X is CHO candidate, the UE performs CHO handover to cell X (with key change) and sends the handover complete message in MSG3 using key B and COUNT = 0.   As the handover complete message in both handovers are encrypted with the same key and COUNT there is keystream reuse. |
| ZTE | We share the same view with Ericsson that keystream reuse issue may also occur in case the handover is executed to the same cell twice. At RAN2#111e meeting, we submitted papers ([R2-2007700](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2007700.zip)) on this issue and proposed to prohibit the UE to attempt a second CHO execution in the same cell failed in the first handover execution. But companies thought it can be up to the UE implementation to handle this. Perhaps we could reconsider the handling of this keystream reuse issue on cell re-selection in this email discussion. |
| Nokia | How likely it is the UE will select again the same cell towards which it has failed to complete the HO? Perhaps the scenario is not the most common one? |
| Sharp | As ZTE explained, the issue raised by Ericsson was already discussed in RAN2#111e meeting and concluded it is up to UE implementation.  For ZTE proposed to reconsider the issue in this email discussion, we (as rapporteur) propose not to re-open the topic here because we have limited time to conclude the original scope. |
| LG | We think that this issue can be avoided by network implementation. |
| MediaTek | The issue raised by Ericsson can be resolved by UE implementation. However, if companies still have concerns, we may add some NOTE, e.g. in this case UE should avoid selecting the same cell for CHO. |
| ITRI | We think the scenarios raised by the rapporteur may happen but can be avoided by network implementation. |
| Apple | We also think the issue can be solved by propoer NW implementation. |
| Samsung | The issue seems not significant. Moreover, security concern arise only if the contents are different (i.e. if ReconfigurationComplete in step 1 and in step 4 are same, there is no security problem) |
| Huawei, HiSilicon | It seems that Ericsson’s scenario has been discussed in previous RAN2 meetings and there was a conclusion, so we may not need to re-open it again. |
| Intel | For the issue mentioned by Ericsson and ZTE, considering the UE sends the same message with same counter, same key stream to the same target cell, Should not it same as retransmission? And therefore should not be security problem. |
| CATT | As this issue was already discussed and there is a conclusion, we think it does not need to be reopened. |

### 2.1.3 Phase 1 summary

In the phase 1 discussion, eleven companies confirmed a keystream reuse issue might happen for both SRB and DRB in the following case.

The UE configured with *attemptCondReconfig* performs normal handover or CHO without *masterKeyUpdate* to Cell X and contention based random access is applied for the handover. After the handover fails, during RRC re-establishment procedure, the UE select one of the CHO candidate cell of which configuration doesn't include *masterKeyUpdate*.

Four companies commented the issue should be solved by network implementation, i.e., *masterKeyUpdate* should be always set in CHO configuration. Two companies commented the issue could be solved if the network never set *attemptCondReconfig* in CHO configuration without *masterKeyUpdate*.

We propose to discuss the solution including the above comments in Phase 2.

Also, one company addressed other keystream reuse issue which was discussed and noted in the RAN2#111e (based on R2-2007700). Eight companies commented it could be solved by implementation, and also in the RAN2#111e some companies commented the same. We propose not to reopen the issue in this email discussion.

**Observation 1: The companies who participated in Phase 1 discussion confirmed a keystream reuse issue might happen for both SRB and DRB in the following case.**

**The UE configured with *attemptCondReconfig* performs normal handover or CHO without *masterKeyUpdate* to Cell X and contention based random access is applied for the handover. After the handover fails, during RRC re-establishment procedure, the UE select one of the CHO candidate cell of which configuration doesn't include *masterKeyUpdate*.**

**Proposal 1: To discuss the solution in Phase 2 including comments (possible solutions) received in Phase 1.**

**Proposal 2: Not to reopen the issue discussed in RAN2#111e based on R2-2007700 in this email discussion.**

## 2.2 Phase 2

### 2.2.1 Phase 2 discussion

During Phase 1 discussion, the following solution to avoid keystream reuse.

- The network always sets *masterKeyUpdate* in *condRRCReconfig*.

- The network never sets *attemptCondReconfig* in *ConditionalReconfiguration* if any of *condRRCReconfig* doesn't include *masterKeyUpdate*.

In addition, we propose that the state variables for radio bearers are maintained (not reverted) when the UE configured with *attemptCondReconfig* reverts back to the source configuration if the previous handover was not required key change.

**Question 1: Which solution(s) do companies support to solve the keystream reuse issue confirmed in Phase 1?**

**Solution A. The network always sets *masterKeyUpdate* in *condRRCReconfig*.**

**Solution B. The network never sets *attemptCondReconfig* in *ConditionalReconfiguration* if any of *condRRCReconfig* doesn't include *masterKeyUpdate*.**

**Solution C. The state variables for radio bearers are maintained (not reverted) when the UE configured with *attemptCondReconfig* reverts back to the source configuration if the previous handover was not required key change.**

**Solution D: Other**

|  |  |  |
| --- | --- | --- |
| Company | Solution(s) | Comments |
| LG | Solution A |  |
| CATT | Solution A |  |
| Qualcomm | Solution B | Solution A is not preferable since there is no reason to restrict the case when *attemptCondReconfig* is not used. |
| Ericsson | Solution D | Solution A is far too restrictive. Solution C is similar to how the PDCP COUNT for SRB1 is handled during fallback to source cell in case of failed DAPS handover. One problem with this solution though is that it will create a “hole” in the PDCP COUNT sequence. Referring to the example scenario in Figure 1, if the COUNT is maintained the UE will send the RRCReconfigurationComplete message in cell B in a PDCP PDU with COUNT = N+1. But the gNB is expecting COUNT = N and will therefore treat the PDCP PDU as arriving out of order and will not the deliver the PDCP SDU (i.e. the RRC message) to higher layers until the reordering timer has expired. This problem can be solved through implementation but would likely require some cross-layer interaction and that the PDCP layer peeks into the PDCP SDU.  Considering the above solution B might be a better option. However, B is not optimal either, as it is also too restrictive, same to A if the network wants to set *attemptCondReconfig*. A solution with less impact is preferred, see a proposal in Q3. |
| Apple | Solution B |  |
| ZTE | Solution D | Share the same view with Ericsson. Solution A and B is too restrictive, which limits the benefit of CHO and CHO based recovery in some cases. For solution C, if in sequence delivery of RLC and/or PDCP packets is used in the NW, the target cell may also be not able to receive the *RRCReconfigurationComplete* message since the PDCP reordering is blocked to wait the packet with COUN N. So we can consider to just add an additional condition to restrict the use scenario of CHO based recovery, e.g. the CHO based recovery can be used only if the failed handover is with key change (i.e. *masterKeyUpdate* was included in the *RRCReconfiguration* for the previous reconfiguration with sync) or only if the selected cell is a CHO candidate cell with key change (i.e. *masterKeyUpdate* is included in the *RRCReconfiguration* contained in *condRRCReconfig*). |
| Nokia | Solution B | We think Solution B has the lowest impact on the existing specification and does not constrain the network’s behaviour too much, unlike Solution A which completely disables the CHO without security key update. Solution C may result in more changes to the specification, perhaps not limited to RRC/Stage 2, if we are to change the behaviour concerning the PDCP state variables. |

**Question 2: Do companies agree that the specification change is necessary with the supported solution(s)?**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| LG | No | If the spec change is needed, the NOTE is enough. |
| CATT |  | We also think, a Note is sufficient to clarify this. |
| Qualcomm |  | It can be added as a Note in RRC or captured as the expected NW implementation option in Chair notes. |
| Ericsson | Yes | It is important to avoid key stream reuse and a solution needs to be captured in the specification. |
| Apple | Yes | We prefer to make it clear in spec. |
| ZTE | Yes | We prefer to make it clear in spec. |
| Nokia | Possibly Yes | A simple change to e.g. field description for attemptCondReconfig or to the procedural text in 5.3.7.3 of NR RRC, where the UE behaviour for attemptCondReconfig is described. |

**Question 3: Do companies have any idea for specification change? If yes, please provide the proposed specification change.**

|  |  |
| --- | --- |
| Company | Proposed specification change |
| LG | If the NOTE is needed, we can add it in 38.300 as follows.  RRC managed handovers with and without PDCP entity re-establishment are both supported. For DRBs using RLC AM mode, PDCP can either be re-established together with a security key change or initiate a data recovery procedure without a key change. For DRBs using RLC UM mode and for SRBs, PDCP can either be re-established together with a security key change or remain as it is without a key change. For CHO, a security key is always updated. |
| CATT | LG proposal seems fine to us. |
| Ericsson | TP on 38.331:  5.3.7.3            Actions following cell selection while T311 is running  Upon selecting a suitable NR cell, the UE shall:  1>  ensure having valid and up to date essential system information as specified in clause 5.2.2.2;  1>  stop timer T311;  1>  if T390 is running:  2>  stop timer T390 for all access categories;  2>  perform the actions as specified in 5.3.14.4;  1>  if the cell selection is triggered by detecting radio link failure of the MCG or re-configuration with sync failure of the MCGand *masterKeyUpdate* was included in the failed re-configuration with sync, and  1>  if *attemptCondReconfig* is configured; and  1>  if the selected cell is one of the candidate cells for which the *reconfigurationWithSync* is included in the *masterCellGroup* in *VarConditionalReconfig*:  2>  apply the stored *condRRCReconfig* associated to the selected cell and perform actions as specified in 5.3.5.3;  1>  else:  … |
| Apple | One simple sentence could be added into the field description of attemptCondReconfig that if this field is present, masterKeyUpdate shall be also included. |
| ZTE | Agree with Ericsson. |
| Nokia | As commented in Q2 table. |

**Question 4: Do companies have any other comments?**

|  |  |
| --- | --- |
| Company | Comments |
| Ericsson | Regarding proposal 2, if there is a valid security issue we should try to resolve it and not just ignore it. Future UE implementations may not take the issue into account if nothing is mentioned about it in the specification. It might be that a similar solution that is adopted as outcome of question 2 can be applied also for the security issue in R2-2007700. |
|  |  |
|  |  |
|  |  |
|  |  |

# 3 Conclusion

To be added

# References

[1] TS 38.331 v16.2.0

[2] R2-2010205, "Issue on failure handling of handover without key change for the UE configured with attemptCondReconfig", Sharp

[3] R2-2010719, "Summary of discussion [211][MOB] CHO/CPC RRC corrections (Intel)", Intel

# Annex Contact Information

In order to ease possible offline discussions, all delegates having provided input in this document are requested to fill the following table.

|  |  |  |
| --- | --- | --- |
| Company | Name(s) | Email Address(es) |
| Sharp (Rapp.) | Takako Sanda | sanda.takako@sharp.co.jp |
| ZTE | Mengjie Zhang | zhang.mengjie@zte.com.cn |
| Nokia | Jedrzej Stanczak | jedrzej.stanczak@nokia.com |
| LG | Geumsan Jo | Geumsan.jo@lge.com |
| Apple | Yuqin Chen | [yuqin\_chen@apple.com](mailto:yuqin_chen@apple.com) |
| Huawei | Jun Chen | [jun.chen@huawei.com](mailto:jun.chen@huawei.com) |
| Ericsson | Cecilia Eklöf | cecilia.eklof@ericsson.com |