**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: Dec 17, 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 11, 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 |  |
|  |  |  |
|  |  |  |
|  |  |  |

**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. |
|  |  |  |
|  |  |  |
|  |  |  |

**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 |  |
|  |  |  |
|  |  |  |
|  |  |  |

**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 |  |
|  |  |  |
|  |  |  |
|  |  |  |

**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 |  |
|  |  |  |
|  |  |  |
|  |  |  |

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 |  |
|  |  |  |
|  |  |  |
|  |  |  |

**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. |
|  |  |
|  |  |
|  |  |

## 2.2 Phase 2

To be added

# 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 |
|  |  |  |
|  |  |  |
|  |  |  |