3GPP TSG-RAN WG2 Meeting #109bis-e R2-2004078

Electronic, 20 April – 30 April 2020

Source: CATT (rapporteur)

Title: Summary of offline discussion for PDCP remaining issues (CATT)

Agenda Item: 6.4.3.2

Document for: Discussion and Decision

# Introduction

This document is to kick off the offline discussion #705 to discuss the PDCP remaining issues which include the issues and proposals in the V2X PDCP summary document [1]. The scope of this offline discussion in the chairman notes is as following.

* [AT109bis-e][705][V2X] PDCP issues (CATT)

Scope: To discuss summary of PDCP remaining issues

Expected outputs: Proposals and summary in R2-2004078

Deadline: 4/24 10:00 for companies’ feedback and 4/27 10:00 for rapporteur version (UTC)

# Discussion

## Issue 1: LCID usage for integrity and ciphering algorithms

In SA3 reply LS [2], SA3 confirmed that there shall be a 5-bit input for the security algorithms and the triple (Key, Bearer, Counter) are only used once in order to avoid key stream reuse. SA3 ask RAN2 to decide how 5-bit input is derived from a particular LCID.

In 38.321, the values of LCID for SL SRBs and DRBs are from 0 to 19. Thus, using the 5 least significant bits of LCID can differentiate the SL SRBs and DRBs which can satisfy the SA3 properties. Therefore, most companies propose to use the 5 least significant bits of LCID as input to the ciphering/integrity algorithms and reply LS to inform SA3 ([3]- [9]).

**Question 1: Does company agree, from RAN2 perspective, the 5 least significant bits of LCID can be used as 5-bit input to the ciphering/integrity algorithms?**

* **Yes. If Yes is selected, please further clarify whether is it necessary to reply LS to SA3 to inform RAN2 preference;**
* **No. If No is selected, please further clarify the preferred solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | Yes |  |
| OPPO | Yes |  |
| HW, HiSi | Yes | It is necessary to reply LS to SA3, to make sure the 5 least significant bits of LCID is used. |
| MediaTek | Yes | Send LS to SA3 about RAN2 agreements. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

According to the answer on Q1, no matter what solution we prefer, rapporteur suggests we need reply SA3 LS to inform our preferred solution.

**Question 2: Does company agree whether it is necessary to reply SA3 LS to inform RAN2 preferred solution based on companies answer to Q1?**

* **Yes;**
* **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | Yes | We are fine with reply LS to SA3 to inform the decision. |
| OPPO | Yes |  |
| HW, HiSi | Yes |  |
| MediaTek | Yes |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Issue 2: Whether D/C filed and SDU type are necessary for SL SRB?

According to the OPPO’s draft CR [6], the SDU type is unnecessary for SL SRB for unicast and broadcast. Thus, some clarifications need to be captured in the Data PDU format for SLRBs for broadcast, i.e., the unprotected PC5-S message (e.g. Direct Communication Request). Moreover, similar as Uu, D/C filed is also unnecessary for SL SRB. Thus, a separate Date PDU format for SL SRB in unicast is necessary to be added in spec. Rapporteur suggests we can agree D/C filed and SDU type are unnecessary for SL SRBs for unicast and broadcast.

**Question 3: Does company agree D/C filed and SDU type are unnecessary for all SL SRBs for unicast and broadcast messages?**

* **Yes;**
* **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | Yes |  |
| OPPO | Yes |  |
| MediaTek | Yes |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Issue 3: Data PDU formats for SL unicast

Several companies provide contributions to discuss the Data PDU formats for SL unicast ([1]- [6] and [8]-[12]). Companies have different views on the design of Data PDU formats for SL unicast. Regarding to the Data PDU formats, there are several issues should be discussed as following:

* Issue 3.1: Whether is it necessary to design separate Data PDU formats for SL SRBs and SL DRBs?
* Issue 3.2: Whether is it necessary to carry Key ID in the PDCP PDU header?

For Issue 3.1, based on the discussion in issue 2, for SL SRBs, it is unnecessary to carry D/C field and SDU type field in the PDU header and the MAC-I is always present. Thus, it’s better to have a separate Data PDU format design for SL SRBs [4][6].

**Question 4: Does company agree to adopt separate Date PDU formats for SL SRBs and SL DRBs for unicast?**

* **Yes;**
* **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | Yes |  |
| OPPO | Yes |  |
| HW, HiSi | Yes |  |
| MediaTek | Yes |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

For Issue 3.2, Huawei mentioned that security context confusion duration is very short, in comparison to the total communication duration of the two UEs. So if 16-bit Key ID is always carried in the SLRB PDCP header, it will result in significant radio resource waste, because most of the time the Key ID is not useful for the pair of UEs at all. In addition, it is unfriendly for UE processing to carry 16-bit Key ID in the NR V2X SLRB PDCP header, as this enforces the UE to implement different PDCP header processing mechanisms for SLRB and Uu DRB respectively, which significantly increases UE implementation complexity [10].

Although the Key ID should indeed be concluded by SA3 from a security perspective, SA3 should have taken no consideration on radio resource efficiency as well as the AS implementation complexity when they made the decision, as these are within the expertise of RAN2. Therefore, RAN2 may also need to have a check on whether the 16-bit Key ID concluded by SA3 is acceptable from an AS perspective. Also, an enquiry with SA3 is possible, as the next SA3 meeting is before next RAN2 meeting, giving sufficient time from RAN2 to receive firm conclusion from SA3.

**Question 5: If 16-bit Key ID is always carried in the SLRB PDCP header, does company agree that the above drawbacks which are mentioned in the Huawei’s contribution [10] should be addressed?**

* **Yes;**
* **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | No | We are fine with SA3 decision. This is not new for PC5 since PGK/PTK fields are carried in the PDCP header in LTE-V2X. |
| OPPO | No | We think this is a SA3 issue hence we respect SA3’s decision to keep the key id in the PDCP PDU header as LTE does. |
| HW, HiSi | Yes | 16-bit Key ID in SLRB PDCP header is not necessary, considering the radio resource efficiency and implementation complexity. |
| MediaTek | No |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

According to the preference of Q5, since SA3 already agree the 16-bit Key ID is always carried in the SLRB PDCP header, we need to discuss whether we should follow SA3 guideline or not.

**Question 6: Which following option does company prefer, based on companies answer to Q5?**

* **Option a): Follow the SA3 guideline, which is the 16-bit Key ID is always carried in the SLRB PDCP header for unicast;**
* **Option b): 16-bit Key ID is not carried in the SLRB PDCP header as Huawei’s proposal in [10];**
* **Option c): Send LS to SA3 to ask them for potential guideline.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Samsung | Option a) |  |
| OPPO | Option a) |  |
| HW, HiSi | Option b) or c) | We need to send LS to SA3, to show RAN2 strong concern, and ask SA3 to re-estimate the necessary to carry 16-bit Key ID in PDCP header from security perspective.  It is also OK for us to send LS to SA3 for potential guidance, if companies think SA3’s help from security’s perspective is needed. |
| MediaTek | Option a) | We are also OK to send LS to SA3. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

If option b) is selected in Q6, we need to further discuss how to address the issue on security context confusion in rekeying procedure. In Huawei’s contribution [10], there are two options to address this issue as follows.

* Option 1: No Key ID is carried in NR V2X SLRB PDCP header;
  + In this option, the security context confusion in rekeying procedure is resolved up to UE implementation.
* Option 2: 1 bit indicator is carried in NR V2X SLRB PDCP header to distinguish the old or new security context.

**Question 7: If option b) is selected in Q6, which following option does company prefer to address the issue on security context confusion in rekeying procedure?**

* **Option a): No Key ID is carried in NR V2X SLRB PDCP header;**
* **Option b): 1 bit indicator is carried in NR V2X SLRB PDCP header to distinguish the old or new security context;**
* **Option c): Other solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| HW, HiSi | Option b) | 1 bit is enough to distinguish the old or new security context. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Issue 4: Solution for PDCP COUNT wrap around

For NR SL, whether PDCP re-establishment should be supported was discussed in the last meeting during the offline discussion. Some companies thought PDCP re-establishment is needed for security key refresh, and LS was sent to SA3 to ask whether the re-keying procedure should be introduced for NR V2X unicast.

In SA3 TS 33.536 [17], the re-keying procedure is specified in Section 5.3.3.1.4.4. The re-keying operation shall be done before the counter for a PDCP bearer repeats with the current keys. A re-keying operation shall refresh the KNRP-sess and NRPEK and NRPIK. The KNRP-sess ID is carried in the PDCP header. NRPEK and NRPIK are used in the integrity and ciphering algorithms. According to companies’ contributions, there are two options to address the PDCP COUNT wrap around issue.

* Option 1: SLRB release and addition procedures;
* Option 2: PDCP re-establishment procedure.

Only one company support Option 1 [14], while other four companies prefer Option 2 ([5]- [9] and [13]).

**Question 8: Which following option does company prefer to address the PDCP COUNT wrap around issue in rekeying procedure?**

* **Option a): SLRB release and addition procedures;**
* **Option b): PDCP re-establishment procedure;**
* **Option c): Other solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Samsung | Option a) | We prefer to use SLRB release and addition procedures to avoid PDCP COUNT wrap around which is same as Uu (i.e., gNB can initiate release/add or full config). From procedure point of view, there is nothing to change in SLRB release and add procedures for this purpose. About triggering this is a separate discussion.  The use of existing Uu PDCP reestablishment has a problem for AM DRB since the COUNT value is not reset to the initial value in the PDCP reestablishment. So, option b) works only for UM DRB and SRB. If we use PDCP reestablishment for RLC AM, then we need to modify the current PDCP reestablishment procedure. |
| OPPO | Option b) | Rekeying procedure itself makes it unnecessary to either change LCID or reset COUNT. Hence PDCP re-establishment is sufficient. Plus Option a) cause more user plane interruption and packet drop. Please note PDCP SN wrap round doesn’t mean PDCP COUNT wrap round i.e. it is different from Uu wrap round issue at all. |
| HW, HiSi | Option c) | Left to UE implementation. |
| MediaTek | Option b) | Agree with OPPO. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

If option a) is selected in Q8, Samsung propose that SL DRB release and addition can be triggered by UE’s lower layer, e.g., PDCP layer. The TX UE checks whether TX\_NEXT is approaching to the large COUNT value or not. If so, UE’s PDCP layer indicates it to RRC layer to perform SLRB release and addition procedures.

**Question 9: If option a) is selected in Q8, does company agree that SL DRB release and addition can be triggered by UE’s lower layer, e.g., PDCP layer?**

* **Yes;**
* **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | Yes | We are not that strong in PDCP layer. This can be triggered either PDCP layer or RRC layer.  About V2X layer, unless SA3 defines any requirements, e.g., TX\_NEXT is approaching to the maximum COUNT, it can be up to RAN2. |
| HW, HiSi | No | Refer to Q8 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

If option b) is selected in Q8, whether the PDCP re-establishment trigger is captured in RRC or V2X layer should be discussed. Over Uu interface, the trigger of PDCP re-establishment is captured in RRC spec. While over PC5 interface, PDCP re-establishment is only triggered by rekeying procedure which is in V2X layer but not RRC layer. Thus, OPPO suggest to send LS to SA3 to capture the PDCP re-establishment trigger due to re-keying operation in V2X layer.

**Question 10: If option b) is selected in Q8, does company agree the PDCP re-establishment trigger should be captured in V2X layer?**

* **Yes. If Yes is selected, please further clarify whether is it necessary to send LS to SA3 to ask them to capture the PDCP re-establishment trigger due to re-keying operation;**
* **No. If No is selected, please further clarify how to capture the PDCP re-establishment trigger.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | No | It can be up to RAN2 unless SA3 defines any requirements, e.g. TX\_NEXT is approaching to the maximum COUNT. |
| OPPO | Yes | A LS to SA3 is needed to introduce a PDCP reestablishment trigger in V2X layer. |
| HW, HiSi | No | Refer to Q8 |
| MediaTek | Yes |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Issue 5: PDCP status report

Regarding to the status report, if PDCP re-establishment is supported, it’s better to support status report to maintain loss-less and in-order delivery [8][9].

Therefore, rapporteur suggests RAN2 to discuss whether the status report is necessary to be supported for SL unicast.

**Question 11: Does company agree to support the status report for SL unicast?**

* **Yes;**
* **No.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s) (Yes/No)** | **Comments if any** |
| Samsung | Yes | If PDCP status report is introduced, status report can be used for retransmission. |
| OPPO | No | Since key ID always exists in the PDCP PDU header it is likely that PDCP PDU will not be dropped. Hence PDCP status report doesn’t help too much in this case. |
| HW, HiSi | No | Not necessary if PDCP re-establishment is not supported. |
| MediaTek | Yes |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Issue 6: Length of bits for PDU type

According to OPPO and CATT’s contributions ([6] and [8]), there are two options for the length of bits for PDU type:

* Option 1: 3 bits.
* Option 2: 2 bits.

If status report is supported, for SL unicast, there are two types of control PDUs, one is PDCP status report and the other is interspersed ROHC feedback. Thus, similar as Uu, using 3-bits PDU type, i.e., Option 1, is preferred in order to reuse the Uu control PDU formats for SL unicast ([8] and [9]).

2-bits PDU type, i.e., Option 2, is suggested in OPPO’s contribution and a new control PDU format is design for interspersed ROHC feedback for SL unicast [6].

**Question 12: Which following option does company prefer on the length of bits for PDU type?**

* **Option a): 3 bits;**
* **Option b): 2 bits;**
* **Option c): Other solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Samsung | Option a) | We are fine to follow Uu format |
| OPPO | Option b) | If status report is not introduced then one code point will be wasted if Uu format is to be reused. |
| HW, HiSi | Option a) | 3 bits is better for future extension. |
| MediaTek | Option a) |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Issue 7: Initial value of RX\_DELIV

In current 38.323, the initial value of SN part of RX\_DELIV is specified as (x – 0.5 × 2[*sl-PDCP-SN-Size*–1]) modulo (2[*sl-PDCP-SN-Size*]), where x is the SN of the first received PDCP Data PDU. The HFN part is not specified at all and it shall be determined automatically by RX\_NEXT.

Considering the relation with SN of first received PDCP data PDU and RX\_NEXT, Samsung proposes the initial value of RX\_DELIV shall be RX\_NEXT - 0.5 × 2[*sl-PDCP-SN-Size*–1] – 1 [14].

**Question 13: Which following option does company prefer on initial value of RX\_DELIV?**

* **Option a): Keep the current specification in 38.323, i.e., the initial value of SN part of RX\_DELIV is specified as (x – 0.5 × 2[*sl-PDCP-SN-Size*–1]) modulo (2[*sl-PDCP-SN-Size*]);**
* **Option b): The initial value of RX\_DELIV shall be specified as RX\_NEXT - 0.5 × 2[*sl-PDCP-SN-Size*–1] – 1.** Note this option b) will update the current specification;
* **Option c): Other solution(s).**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Samsung | Option b) | The initial value of HFN part is not specified at all, but it shall be determined automatically by RX\_NEXT. The text proposal is very simple: “**as RX\_NEXT - 0.5 × 2[*sl-PDCP-SN-Size*–1] – 1”**  Note that there is no room for UE implementation. |
| OPPO | Option a) | Nots sure what’s problem of current initial value |
| HW, HiSi | Option b) | Option b) is ok for broadcast and group broadcast. To clarify this question is not related with unicast. |
| MediaTek | Option a) |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Issue 8: Need of counter-check procedure in PC5

According to the current SA3 specification, the integrity protection can be optional for SL unicast DRBs. If the SL integrity protection is not used, there may be a need to introduce a counter check procedure in PC5 interface, as proposed in [7].

Therefore, rapporteur suggests RAN2 to discuss whether it is necessary to introduce a counter check procedure in PC5 interface for unicast.

**Question 14: Does company agree to introduce a counter check procedure in PC5 interface for unicast?**

* **Option a): Yes;**
* **Option b): No;**
* **Option c): Send LS to SA3 to ask them about the necessity of introducing SL Counter Check procedure.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Preferred option(s)** | **Comments if any** |
| Samsung | Option a) | It may help to avoid HFN desynchronization problem. |
| OPPO | Option b) | For this release we don’t need it |
| HW, HiSi | Option b) | Prefer integrity check is always used. |
| MediaTek | Option b) |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Other Issues

Regarding to other details editorial issues, e.g., the detail design in PDU format and some clarifications related ciphering and integrity procedure can be further discussed during the PDCP CR discussion. Here, companies are invited to provide other technical remaining issues related V2X PDCP.

|  |  |  |
| --- | --- | --- |
| **Company** | **Issues** | **Comments if any** |
| OPPO | SL SRB PDCP PDU format | Recently CT1 agreed that Direct Communication Request message can be also sent via Unicast. But this message is not protected. So MAC-I should be optional within SL SRB PDCP PDU format which should be also clarified in table 6.3.2-1 |
|  |  |  |
|  |  |  |
|  |  |  |

# Conclusion

This contribution summarizes the offline discussion for open issues on V2X PDCP.

Based on companies’ input, the proposals achieved by this offline discussion are shown as follows.

# Reference

1. R2-2003774, Summary of PDCP remaining issues on NR V2X, CATT
2. R2-2002541, LS reply to RAN WG2 LS on NR V2X Security issue and PDCP SN size (S3-200478; contact: CATT), SA3, LS in, To:RAN2
3. R2-2002566, Discussion on NR V2X remaining user plane issues, ZTE Corporation, Sanechips
4. R2-2002570, (draft)CR on TS 38.323 for NR V2X on miscellaneous issues , ZTE Corporation, Sanechips
5. R2-2002649, Discussion on PDCP open issues, OPPO
6. R2-2002650, 38323\_CRyyyy\_(REL-16)\_Correct on PDCP for NR V2X, OPPO
7. R2-2002810, Remaining issues on NR V2X PDCP Design, Apple
8. R2-2002833, Remaining Issues on PDCP, CATT
9. R2-2002834, 38.323 draftCR for NR V2X, CATT
10. R2-2003510, Discussion on the SLRB PDCP header format, Huawei, HiSilicon
11. R2-2003511, Draft CR on the PDCP format for NR SL unicast, Huawei, HiSilicon
12. R2-2003535, Draft CR to 38.323 for NR PC5-S and PDCP header, Qualcomm
13. R2-2003668, Remaining PDCP issues, Nokia, Nokia Shanghai Bell
14. R2-2003681, Discussion for SL PDCP open issues, Samsung Electronics Co., Ltd
15. R2-2003682, SL PDCP COUNT wrap around avoidance and initial value of RX\_DELIV, Samsung Electronics Co., Ltd, 38.323
16. R2-2003683 , SL PDCP COUNT wrap around avoidance, Samsung Electronics Co., Ltd, 38.331
17. S3-200528 TS 33.536 v0.3.0, Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services