RAN-R18-WS-eMBB-Xiaomi - Version 0.0.3
RAN

3GPP TSG-RAN Rel-18 Workshop RWS-210547

Electronic Meeting, June 28 - July 2, 2021

Agenda item: 4.1

Source: Xiaomi

Title: Email discussion summary for [RAN-R18-WS-eMBB-Xiaomi]

Document for: Discussion

General Comm

1 General Comments

This email discussion provides details regarding Xiaomi's proposals for eMBB enhancements proposed for adoption by 3GPP RAN for REL-18. In accordance with direction provided by the RAN chair this email is intended to run from 14 June to 24 June and serves the purpose to help with companies understanding of the proposals ahead of the RAN REL-18 Workshop, June 28th – July 2nd 2021.

This email discussion summary covers the following documents:

- RWS-210090 NR security enhancement considering car communication

- RWS-210114 Work Item on enhanced in-device coexistence for NR

1 areas for consideration are proposed in this discussion.

- Security enhancement covering motivation document RWS-210090.

- eIDC covering motivation document RWS-210114

1.1 Question:

Feedback Form 1: The answers are provided under the section for RWS-210090 Security enhancements

1 – Spreadtrum Communications

Thanks for the proposal.

The security requirement for car communication is indeed higher than nomral UE communication, for some

special scenario. But, maybe we should check with SA3 for their plan on false basestation topic, actually, this topic has beend discussed for a long time. and we suggest to identify the specially scenarios of car communicaiton using Uu or SL, in which the security requirement is higher.

2 – Xiaomi Communications

The answers are provided under section 2.1.

2 eMBB Proposals for Rel-18

2.1 RWS-210090 Security enhancement

2.1.1 Introduction

The following is a summary of contributions RWS-210090 (motivation), which by reference are included in their entirety to this discussion and specifically to facilitate the questions in the following related sections.

The paper represents the security requirements on the car communication and lists the following areas which requires some RAN work in Rel-18:

- False base station as given in 3GPP TR 33.809

- User Plane Integrity Protection as given in 3GPP TR 33.853

- Attacker tracking

The requirement of attacker tracking for car cyber-security requires the standard work in both SA3 and RAN in Rel-18. In order to facilitate the design of the solutions on the enhanced security, RAN should allocate some time units to study and standardize the security enhancement solutions as identified by SA3.

2.1.2 Round 1 Questions

Based on the summary presented above and specifically the details of the contribution in RWS-210090, please submit below your questions for clarification or understanding according to the RAN chair guidelines, including those given in RWS-210002.

Feedback Form 2: Questions/comments on RWS-210090 Security enhancement

1 – Intel Corporation (UK) Ltd

Q1) Is the intention only to address specific issue and solution from SA3?
Q2) Do you foresee any additional stage 3 specification work from UPIP, given that LTE UPIP is also likely to be specified in Rel-17?

2 – Samsung Electronics Co.

does Xiaomi only have interest on the V2X-specific security (e.g. PC5 link only) or want to look into the

Uu link aspectes (which is mainly being discussed in SA3) as well?

3 – Xiaomi Communications

@Intel,

Answer to Q1: We think that the issues and solutions provided by SA3 should be considered in the first place. However we also discover other security issues (i.e. attacker tracking), which are critical for car communication. We think some coordination between SA3 and RAN (especially RAN2/3) is needed to address all security issues and solutions.

Answer to Q2: If LTE UPIP is specified in Rel-17, maybe no additional stage-3 specificaiton work for UPIP support in LTE. We need to double check whether all UPIP issues as discussed in SA3 are covered. For example, the UPIP impacts on the transmission bit rate may also require some RAN work. For example, due to the UE processing capability for decoding integrity protected PDCP PDU, the UE or the gNB need to consider which traffic transmission has more strict requirement on UPIP.

@Samsung,

For car communication, both PC5 and Uu are important. We think that the security issues related to both PC5 and Uu should be addressed in both RAN and SA3.

2.1.3 Round 1 Answers

@Spreadtrum,

Answer: The topic of false base station is just one topic for enhancing the car communication. If companies have concerns on the workload in RAN, the "Key Issue #2: Security protection of system information" should be prioritized. However we think all security issues related to the false base station are critical.

@Intel,

Answer to Q1: We think that the issues and solutions provided by SA3 should be considered in the first place. However we also discover other security issues (i.e. attacker tracking), which are critical for car communication. We think some coordination between SA3 and RAN (especially RAN2/3) is needed to address all security issues and solutions.

Answer to Q2: If LTE UPIP is specified in Rel-17, maybe no additional stage-3 specificaiton work for UPIP support in LTE. We need to double check whether all UPIP issues as discussed in SA3 are covered. For example, the UPIP impacts on the transmission bit rate may also require some RAN work. For example, due to the UE processing capability for decoding integrity protected PDCP PDU, the UE or the gNB need to consider which traffic transmission has more strict requirement on UPIP.

@Samsung,

For car communication, both PC5 and Uu are important. We think that the security issues related to both PC5 and Uu should be addressed in both RAN and SA3.

2.1.4 Round 2 Questions

Feedback Form 3: Any further question on RWS-210090 Security enhancement

1 – Samsung Electronics Co.

Thanks for the reply. If we understand the proposal correctly, to protect system information (i.e. in the Uu interface) would be the essential part for car communication. Do you see any need to enhance PC5 link itself?

2.1.5 Round 2 Answers

@Samsung,

Regarding the enhancement on the PC5 link itselft, we observed that some unecrypted NAS signaling may need further study in SA3. Some rogue UEs abusing the common resource pool of the PC5 link could cause the PC5 jamming. Then we need some solutions to detect/resolve the PC5 jamming caused by rogue UEs.

2.1.6 Summary

In the 1st round QA, 3 companies provided questions. The answers provided above clarified the relation between the RAN security enhancement and the SA3 work including fake gNB, UPIP and potential other security issues (e.g. attacker tracking and radio jamming) in both Uu and PC5.

Regarding the enhancement on the PC5 link itselft, we observed that some unecrypted NAS signaling may need further study in SA3, and no RAN impacts on the PC5 link are observed so far.

In the 2nd round QA, 1 company provided questions. The answers provided above clarified the potential security issues observed for PC5.

2.2 RWS-210114 eIDC

2.2.1 Introduction

The following is a summary of contributions RWS-210114 (motivation), which by reference are included in their entirety to this discussion and specifically to facilitate the questions in the following related sections.

The NR IDC issues include the followings:

- Adjacent frequency interference between 3GPP and other RAT(s)

- Inter-modulation (amongst 3GPP frequencies) interference to other RAT(s)

- Hardware sharing issue between 3GPP and other RAT(s)

- IDC-caused measurement inaccuracy

- Inter-modulation (between 3GPP and other RAT) interference to 3GPP/other RAT(s)

- RLF/HOF caused by the IDC interference

In Rel-15, the IDC FDM solution is introduced to support the EN-DC and the standalone NR. However, the current solutions for NR IDC issues have the following defects:

- Do not support NE-DC.

- Do not support TDM solution (e.g. autonomous deny and UE preferred TDM pattern).

- Only NR-ARFCN can be indicated as the affected frequency.

- Cannot resolve the hardware sharing issue.

- Cannot resolve the measurement inaccuracy issue caused by IDC.

To resolve the above IDC issues, the NR IDC solutions would need the following enhancements:

- Enhanced FDM solution, which allows more flexible indication of affected frequencies (e.g. granularity of BWP or sub-band or PRB level).

- TDM solution (e.g. autonomous deny of UL transmission, indication of UE preferred TDM pattern for UL/DL)

- Hardware sharing indication

- Suspension of IDC-affected measurement

2.2.2 Round 1 Questions

Based on the summary presented above and specifically the details of the contribution RWS-210114, please submit below your questions for clarification or understanding according to the RAN chair guidelines, including those given in RWS-210002.

Feedback Form 4: Questions/comments on RWS-210114 eIDC

1 – ZTE Corporation In LTE, the main intention of IDC is to enable the coexistence of LTE and GNSS/ ISM radio within the same device. In Rel-17 Multi-SIM has been discussed and some enhancement has been proposed in Rel-18 to enable a more flexible UE capabilities coordination between the two active USIM. From our point of view, the two active USIM can be considered as a special case of IDC with two NR radio within the same device. Therefore, to minimize the complexity on both standardization and implementation, we are wondering whether a common framework&solution can be considered for IDC and Multi-SIM to enable the flexible capability coordination&update in NR.
2 – vivo Mobile Communication Co. We are always supportive on this working area from Rel-16. We have two questions on the proposal: 1. What kind of enhanced FDM solution on top of the what we have specified in TEI-16? I assume the motivation is to have more flexibility. Could you please provide more use cases?

2. For 2nd bullet, we understand the example here is to reuse the mechanism in LTE, we would like to check if there is any further enhancement.

3. Regarding the 3rd bullet, I think the same solution could be applicable for hardware sharing and IDC. Is that true?

3 – Lenovo Mobile Com. Technology

Thanks for the interesting proposals! please see our questions for further understanding

1. we would like to further understanding in what case there needs a more flexible frequency indication based on e.g. BWP, sub-band or PRB level?

2. for TDM solution, we understand LTE solution could be served as a baseline solution and further enhancement can be FFS?

3. we are wondering if *suspension of IDC-affected measurement* is more relates to RAN4 RRM requirement or there expect some impacts on procedure?

4 – LG Electronics Inc.

1. Regarding enhanced FDM solution, in which scenario you think finer granularity than frequency is needed? For example, BWP or sub-band, they all belong to a frequency, and we think they all experience same or similar interference.

2. Regarding hardware sharing indication, isn't it more like a capability signaling than IDC indication? Do you think hardware sharing is dynamically changed?

5 – Guangdong OPPO Mobile Telecom.

Thanks for the contribution. Some questions for clarification as below:

Q1. R15 and R16 have introduced FDM based IDC solution for EN-DC and NR standalone respectively, it's not clear to us what does "enhanced FDM solution" mean in the first bullet. Would you like to elaborate a bit more on it?
Q2. what does the "Hardware sharing indication" mean in the third bullet?
Q3. In bullet 4, by saying "suspension of IDC-affected measurement", does it mean UE proactively stop the measurement when identifying the IDC issue or something else?

6 – China Mobile Com. Corporation

Thank you for the contribution! The goal of this interference avoidance technology component is to protect the different radios from mutual interferences,e.g. LTE, NR, WiFi and Bluetooth. And in Rel-16, the IDC FDM solution is introduced to support the standalone NR. So, could you clarify what is the deficiency in the exsiting IDC scheme? If the motivation is for bring up more felxibility, could you provide corresponding use cases?

7 – Intel Corporation (UK) Ltd

1) Among the IDC issues raised in the justification, intermodulation to major non 3GPP systems has always been considered, when we specify the RF requirements. And for hardware sharing, it is hugely UE implementation specific. IDC-caused measurement inaccuracy was not identified, when we specified IDC solutions for LTE and no RRM accuracy relaxation was considered. Can you please help to clarify more details on potential RRM measurement inaccuracy

8 – Spreadtrum Communications

Thanks for R18 contribution! We are interested with IDC topic. For enhanced FDM solution and TDM solution from objective, on top of the existing R16 FDM and LTE TDM solution, could you clarify the related use cases and/or motivation, and what additional benefit do you expect? Thanks.

9 – TCL Communication Ltd.

This IDC topic is interesting. What do you think of the advantages and disadvantages respectively comparing TDM and FDM?

10 – China Unicom

Thanks for this contribution.

A clarification question for objective 3, for the ”Hardware sharing indication”, is that meaning of **sharing of physical transmitter and reciever for different (e.g. LTE/NR/WiFi/Bluetooth) technologies**? What is the standard impact?

2.2.3 Round 1 Answers

@ZTE,

Answers: It is not clear to us how to achieve some common solutions for both IDC and multi-SIM. We would expect that the many solutions (e.g. FDM, hardware sharing and measurement inaccuracy) from IDC are anyway independent from multi-SIM. I guess ZTE is assuming that we could try to have some common solutions for the TDM solutions. We are open for such discussion to achieve some commonality for the TDM solution of both IDC and multi-SIM.

@vivo,

Answer to Q1: When the NR UE is configured with a wide bandwidth (e.g. 100MHz between ARFCN-1 and ARFCN-2) of frequency, the UE could have a subset of frequency range (e.g. between AFRCN-3 and ARFCN-4) is impacted by IDC interference. According to the current specification, the UE is only allowed to report the ARFCN. In order to indicate the impacted frequency range, the UE would have to provide a big list of ARFCNs so as to cover all impacted frequencies, which is currently very in-efficient. We are open to the solutions on how to provide more efficient frequency indication for a range of frequencies.

Answer to Q2: The TDM configuration/report is associated with a specific numerology. LTE only support 15KHz numerology, but NR supports many different numerologies. Thus the NR TDM solution should at least consider the numerology impacts on the TDM configuration/report.

Answer to Q3: The suspension of IDC-affected measurement in LTE is not related to RAN4 RRM requirement, but rather to avoid the wrong measurement report for the SON/MDT purpose.

@LG,

Answer to Q1: The IDC interference could impact the whole BWP or a sub-band of a BWP. According to the

testing cases, the RF de-sense caused by IDC inference are quite different from one frequency to another. If possible, we would prefer a more generic framework for the FDM solution to indicate any frequency or any frequency range. We are open to the solutions, as indicating ARFCN definitely causes too much signaling.

Answer to Q2: This is actually depending on how companies interpret the hardware sharing issue. According to the current UE implementation, the RF chain of 3GPP could be temporarily occupied by the WiFi when the user switches on the WiFi module. For some UE implementations, when the 3GPP RF module has multiple RF chains, the WiFi may only occupy one of them when the WiFi module is on.

@OPPO,

Answer to Q1: When the NR UE is configured with a wide bandwidth (e.g. 100MHz between ARFCN-1 and ARFCN-2) of frequency, the UE could have a subset of frequency range (e.g. between AFRCN-3 and ARFCN-4) is impacted by IDC interference. According to the current specification, the UE is only allowed to report the ARFCN. In order to indicate the impacted frequency range, the UE would have to provide a big list of ARFCNs so as to cover all impacted frequencies, which is currently very in-efficient. We are open to the solutions on how to provide more efficient frequency indication for a range of frequencies.

Answer to Q2: According to 36.300, the hardware sharing problem means that "IDC problem can happen when the UE (intends to) uses WLAN on the overlapped carrier/band or adjacent carrier/band to the unlicensed carrier used for LAA operation, e.g. when related UE hardware components, such as antennas, are shared between LAA and WLAN operations.". According to the current UE implementation, the RF chain of 3GPP could be temporarily occupied by the WiFi when the user switches on the WiFi module. For some UE implementations, when the 3GPP RF module has multiple RF chains, the WiFi may only occupy one of them when the WiFi module is on. When a 3GPP RF chain is occupied by the WiFi, the 3GPP transmission is not able to use the same RF chain. However we are also open to discuss other hardware sharing issues, as the hardware sharing may happen not just for the overlapping NR-U band, but also for some licensed band. In some cases, the UE could even have inter-modulation between WiFi and 3GPP frequency using the same antenna, which makes the IDC issue even more complicated.

Answer to Q3: In LTE, the suspension of IDC-affected measurement means the UE suspend the report of the measurement result which is affected by the IDC interference. We understand that we could have other ways for suspension, and we are open to all solutions.

@China Mobile,

Answers: NR currently only support FDM solution which only allows the UE to indicate ARFCN. Firstly, when the gNB receives the frequency indication from the UE, the gNB would have to remove the frequency if the gNB wants to alleviate the IDC issue in the UE. This makes the frequency utilization very in-efficient. Then a TDM solution would allow the UE still works in the IDC-impacted NR frequency in a TDM manner without changing its serving frequency.

One another issue which is critical for the operator is that the SON/MDT measurement is anyway reported by the UE even though the measurement result is affected by the IDC interference. This makes the SON/MDT function unable to work properly.

@Intel,

Answer: Regarding the RRM measurement inaccuracy, the main intention is to avoid miss-interpretation of the logged/immediate MDT measurement report due to the IDC interference. However as NR introduced many different measurement configurations (e.g. early measurement configuration), we consider that the IDC impacts on other measurement configurations should also be considered. Regarding the NR measurement relaxation, we consider that the IDC interference may cause the measurement even more inaccurate when the measurement relaxation is allowed by the gNB. Then when gNB configures the measurement relaxation, the gNB needs to be very careful when the relaxed measurement is also impacted by IDC inference.

@Spreadtrum,

Answer to FDM solution: For FDM solution, when the NR UE is configured with a wide bandwidth (e.g. 100MHz between ARFCN-1 and ARFCN-2) of frequency, the UE could have a subset of frequency range (e.g. between AFRCN-3 and ARFCN-4) is impacted by IDC interference. According to the current specification, the UE is only allowed to report the ARFCN. In order to indicate the impacted frequency range, the UE would have to provide a big list of ARFCNs so as to cover all impacted frequencies, which is currently very in-efficient. We are open to the solutions on how to provide more efficient frequency indication for a range of frequencies.

Answer to TDM solution: The TDM configuration/report is associated with a specific numerology. LTE only support 15KHz numerology, but NR supports many different numerologies. Thus the NR TDM solution should at least consider the numerology impacts on the TDM configuration/report.

@TCL,

Answer: The FDM solution is simpler for implementation of the UE and the gNB. The UE needs to indicate its impacted frequency, and the gNB could simply remove the impacted frequency. However the FDM solution is very in-efficient for the frequency utilization, as the impacted frequency has to be removed in order to resolve the IDC issue in the UE. The TDM solution is allows the UE working in the IDC-impacted frequency in a TDM manner. However this is more complex for the implementation of both the UE and the gNB. The UE implementation needs to provide a proper TDM report to the network by considering its transmission/reception pattern in different RAT. The gNB would have to avoid schedule the IDC impacted time slot and this makes the gNB scheduler more complex.

@China Unicom,

Answer: According to 36.300, the hardware sharing problem means that “IDC problem can happen when the UE (intends to) uses WLAN on the overlapped carrier/band or adjacent carrier/band to the unlicensed carrier used for LAA operation, e.g. when related UE hardware components, such as antennas, are shared between LAA and WLAN operations.”. According to the current UE implementation, the RF chain of 3GPP could be temporarily occupied by the WiFi when the user switches on the WiFi module. For some UE implementations, when the 3GPP RF module has multiple RF chains, the WiFi may only occupy one of them when the WiFi module is on. When a 3GPP RF chain is occupied by the WiFi, the 3GPP transmission is not able to use the same RF chain. However we are also open to discuss other hardware sharing issues, as the hardware sharing may happen not just for the overlapping NR-U band, but also for some licensed band. In some cases, the UE

could even have inter-modulation between WiFi and 3GPP frequency using the same antenna, which makes the IDC issue even more complicated.

Answer: Regarding the standard impact, the LTE solution is to allow the UE to indicate 1bit hardware sharing indication. For example, when the eNB configures an LAA frequency channel for the UE, the UE could indicate the hardware sharing issue to the eNB. Then the eNB can change the LAA frequency to another one.

2.2.4 Round 2 Questions

Feedback Form 5: Any further question on RWS-2101114 eIDC

1 – Lenovo Mobile Com. Technology for eIDC, seems our comments are missed. Any response would be appreciated
2 – Samsung Electronics Co. Q1: Which working group (e.g. RAN1, 2, 4) consider(s) enhancement(s) mainly? Q2: What is motivation of ”indication of UE preferred TDM pattern for UL/DL” w.r.t. related target scenario?

@Lenovo,

Answer to Q1: When the NR UE is configured with a wide bandwidth (e.g. 100MHz between ARFCN-1 and ARFCN-2) of frequency, the UE could have a subset of frequency range (e.g. between AFRCN-3 and ARFCN-4) is impacted by IDC interference. According to the current specification, the UE is only allowed to report the ARFCN. In order to indicate the impacted frequency range, the UE would have to provide a big list of ARFCNs so as to cover all impacted frequencies, which is currently very in-efficient. We are open to the solutions on how to provide more efficient frequency indication for a range of frequencies.

Answer to Q2: Yes, we consider to use the LTE TDM solution as a baseline, but need to consider at least the NR numerology impacts on the TDM solution, as the time granularity in the TDM solution depends on the numerology.

Answer to Q3: The suspension of IDC-affected measurement does not impact the RAN4 RRM requirements according to the LTE solution. In LTE, the UE suspends the report of the IDC-affected measurement result in the logged MDT and indicates to the network of the IDC issue observed in the logged MDT report. We think the general ideas can be reused for NR. We are open to the solutions to all IDC-affected measurements, as the LTE only considers the solution resolving the logged MDT IDC issue.

@Samsung,

Answers to Q1: RAN2 is the main working group. No RAN1 work is expected. Some new RRM requirements for IDC solutions are required in RAN4.

Answers to Q2: The UE preferred UL is to avoid the IDC interference from 3GPP UL to WiFi DL, as the gNB should avoid schedule the 3GPP UL when the WiFi DL is on-going. However the WiFi DL transmission is more related to the DL traffic pattern of WiFi which is only known by the UE. If the UE reports its preferred

3GPP UL time slots, this means that the transmission those UL time slots will not cause (or cause less) IDC interference to the WiFi. The UE preferred DL is to avoid the IDC interference from WiFi UL to 3GPP DL. Same example as the WiFi DL traffic can be reused also for the WiFi UL traffic.@Lenovo,

2.2.5 Summary

In the 1st round QA, 10 companies provided questions. The answers provided above clarified the following aspects: the relation between IDC and multi-sim, the motivation of introducing more flexible FDM solution, the NR enhancements while reusing the LTE TDM solution, the specification impacts of suspension of IDC-affected measurement, the definition/explanation of the hardware sharing issue, the standard impact of hardware sharing indication, the motivation of introducing TDM solution, the motivation of introducing the suspension of IDC-affected measurement, the relation between IDC issue and the RRM relaxation, and the comparison between FDM solution and TDM solution.

In the 2st round QA, 2 companies provided questions. The answers provided above clarified the following aspects: the motivation of introducing more flexible FDM solution, the NR enhancements while reusing the LTE TDM solution, the specification impacts of suspension of IDC-affected measurement, main working group for the IDC standard work, and the use cases for ”indication of UE preferred TDM pattern for UL/DL”.