3GPP TSG RAN Rel-18 workshop
Electronic Meeting, June 28 – July 2, 2021

RWS-210184

Agenda Item: 4.3

Source: Samsung

Title: AS layer Security Enhancement for 5G-Advanced

Document for: Discussion and Decision

SAMSUNG

Motivation

◇ The security is one of the essential part of communication.

However, the basic principles in AS security has not been changed much since LTE time:

- The current AS security protects only L3 (e.g. dedicated RRC messages and user plane data) in RRC_CONNECTED mode, leaving the other parts unprotected, as shown below.

	IDLE/INACTIVE	TRANSITION	CONNECTED
L3 RRC	System Information, Paging	CCCH	DCCH
L3 UP data	N/A	N/A	DTCH
L2 control	N/A	MAC CE	MAC CEs, Control PDU
L2 header	N/A	MAC	PDCP/RLC/MAC
L1 PHY	DCI for SI, Paging	DCI for the initial access	DCI, PUCCH

: Protected

: Unprotected

Fake Base Station attack could lead to ***throughput degradation***

Fake Base Station attack could lead to ***out-of-service***

- Fake base station attack exploiting the unprotected parts could be potential security threats degrading system throughput and QoE.
- Hence, it is time to review the current AS security and potential threats.

©2021 Samsung Electronics Co., Ltd.. All rights reserved.

Potential security threat with the current framework

SAMSUNG

- The following table shows the possible examples of compromised AS information in the current system and corresponding consequences.

Category	Compromised AS information	Consequence
L3 Control	*pagingRecordList* in *Paging* message	Multiple UEs miss their paging.
L3 Control	*masterCellGroup* IE in *RRCSetup* message	A single UE applies wrong configuration resulting in communication broken for the UE.
L3 Control	SIB12 for V2X	V2X UEs apply wrong (not validated) resource configuration for transmission/reception over sidelink leading to V2X service denial.
L2 Header	MAC-I in PDCP PDU	A single UE experiences Integrity Check failure resulting in RLF declaration of the UE.
L2 Control	ACK_SN in RLC STATUS PDU	A single UE experiences data loss from RLC SDUs wrongly discard.
L2 MAC CE	SCS in Guard Symbols MAC CE	A single IAB node applies wrong guard symbols resulting in degradation of IAB operation.
L1 DCI	DCI 1_0 with SI-RNTI	Multiple UEs miss system information blocks.
L1 DCI	DCI 2_0 for Slot Format Indicator	Multiple UEs apply wrong slot format indicator.

Note that 15 types of System Information, 28 types of MAC CE in DL, and 6 types of L2 control SDU are defined in Rel-16 NR specifications.

©2021 Samsung Electronics Co., Ltd.. All rights reserved.

Current status in SA3

SAMSUNG

- SA3 is already discussing the issues under Rel-17 SI "Study on 5G Security Enhancement against False Base Station (FBS)":
  - They have identified and captured the issues as "Key Issues" in their TR 33.809:
    - Key Issue #1: Security of unprotected unicast messages
      - which covers L2 headers & control messages and L3 messages (e.g. CCCH and some of DCCH)
    - Key Issue #2: Security protection of system information
    - Key Issue #7: Protection against Man-in-the-Middle false gNB attacks (e.g. messages in KI#1 + paging)
  - The solutions for the Key Issues might have significant impact to RAN.
    - For instance, SA3 has sent RAN2 the LS S3-212349 about the protection of *RRCResumeRequest* message which addresses *only very small part of Key Issue #1*, but shows several possible RAN2 impacts for the solution (if agreed to introduce):

- UE's capability - gNB/ng-eNB's capability in a SI message - A new procedural text to calculate the enhanced (*short*)*ResumeMAC-I* of the *RRCResumeRequest* message - Enhanced Xn interface - …

  - As of May '21 SA3 meeting, there is no consensus on how to proceed further, and most likely, only few issues (e.g. protection of system information) may be addressed in Rel-17 WI scheduled from 2H 2021 (if a SA3 WI is agreed).
    - Other unprotected parts may not be considered due to lack of time in Rel-17 timeframe and also the impact to RAN WGs.

©2021 Samsung Electronics Co., Ltd.. All rights reserved.

Way forward and proposed objectives

SAMSUNG

- Way forward
  - To initiate Rel-18 SI in RAN, as to aid SA3 in making conclusion.
    - The necessity of AS security enhancement can be evaluated in SA3 (only)
    - However, RAN should get prepared for the corresponding work in RAN side
      - The proposed WI in RAN may NOT be part of the initial Rel-18 package, but the solutions for the issues might have significant impacts to RAN specifications, which may also require several TUs.

- Objectives of the Rel-18 SI, depending on the conclusion in SA3:
  - To study the impact of the potential solutions that provide integrity protection of L1 and/or L2 messages [RAN2-led, RAN1]
    - L2 message includes control PDUs of MAC/RLC/PDCP.
    - L1 message includes DCI and transport block.
  - To study the impact of the potential solutions that provide integrity protection of the system information message [RAN2-led]
    - To generate and include digital signature in the system information message
    - The details on digital signature are defined in SA3.
  - To study the impact of the potential solutions that provide protection of the RRC messages (e.g., in INACTIVE state) [RAN2-led]
    - To protect the *RRCResumeRequest* message
    - To protect the *RRCReject* message

©2021 Samsung Electronics Co., Ltd.. All rights reserved.