Joint meeting 3GPP TSG GERAN/S3
Madrid,Spain
27th, April 2001
Source: Nokia

S3z010037

GERAN RRC Messages and Integrity Protection

1. Introduction

The aim of this document is to roughly estimate the typical size of 44.018 based RRC messages, as well as characterise the criticality of those messages with respect to the integrity protection. Also the integrity protected and not integrity protected RRC messages that are adopted from 25.331 are listed. The outcome is captured in the following sections.

2. 44.018 based RRC Messages

Table 9.1/3GPP TS 44.018: Messages for Radio Resources management

Channel establishment messages:	**Applicability**	**Integrity Protection Criticality (Note 1)**	**Message size (min-max) (Note 2) [octets]**
ADDITIONAL ASSIGNMENT	Iu and A/Gb	High	5(11)-18
IMMEDIATE ASSIGNMENT	Iu and A/Gb	High (see Note 3)	12(15)-34
IMMEDIATE ASSIGNMENT EXTENDED	Iu and A/Gb	High (See Note 3)	19(22)-23(26,30)
IMMEDIATE ASSIGNMENT REJECT	Iu and A/Gb	High (see Note 3)	23
DTM ASSIGMENT FAILURE	Iu and A/Gb	High	3
DTM REJECT	Iu and A/Gb	High	3
DTM REQUEST	Iu and A/Gb	High	12-n
PACKET ASSIGNMENT	Iu and A/Gb	High	12-n
RR INITIALISATION REQUEST	Iu and A/Gb	High but IP not possible	18
Ciphering messages:	**Applicability**		
CIPHERING MODE COMMAND	A/Gb	N/A	
CIPHERING MODE COMPLETE	A/Gb	N/A	
Handover messages:	**Applicability**		
ASSIGNMENT COMMAND	Iu and A/Gb	High	9(10,15,31..)-148-331
ASSIGNMENT COMPLETE	Iu and A/Gb	High	3
ASSIGNMENT FAILURE	Iu and A/Gb	High	3
DTM ASSIGMENT COMMAND	Iu and A/Gb	High	13 (39,45) – n
INTER SYSTEM TO UTRAN HANDOVER COMMAND	Iu and A/Gb	High	4 – n
PDCH ASSIGNMENT COMMAND	Iu and A/Gb	High	5 (28,29,46) – n
HANDOVER ACCESS	Iu and A/Gb	Not Applied	
HANDOVER COMMAND	Iu and A/Gb	High	9 (12,13,19,…) – 140…300
HANDOVER COMPLETE	Iu and A/Gb	High	3 – 8
HANDOVER FAILURE	Iu and A/Gb	High	3
RR-CELL CHANGE ORDER	Iu and A/Gb	High	8-11
PHYSICAL INFORMATION	Iu and A/Gb	High	3
INTER SYSTEM TO CDMA2000 HANDOVER COMMAND	FFS	High	6 – n
Channel release messages:	**Applicability**		
CHANNEL RELEASE	Iu and A/Gb	High	3 (8,16,21) – n
PARTIAL RELEASE	Iu and A/Gb	High	5
PARTIAL RELEASE COMPLETE	Iu and A/Gb	High	2
Paging messages:	**Applicability**		
PACKET NOTIFICATION	A/Gb (Iu is FFS)	Not applied	
PAGING REQUEST TYPE 1	Iu and A/Gb	Not applied	
PAGING REQUEST TYPE 2	Iu and A/Gb	Not applied	
PAGING REQUEST TYPE 3	Iu and A/Gb	Not applied	
PAGING RESPONSE	Iu and A/Gb	Not applied	

System information messages:	**Applicability**		
SYSTEM INFORMATION TYPE 1	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 2	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 2bis	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 2ter	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 2quater	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 3	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 4	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 5	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 5bis	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 5ter	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 6	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 7	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 8	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 9	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 13	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 16	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 17	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 18	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 19	Iu and A/Gb	Not applied	
SYSTEM INFORMATION TYPE 20	Iu and A/Gb	Not applied	
Specific messages for VBS/VGCS:	**Applicability**		
NOTIFICATION/FACCH	A/Gb	N/A	
NOTIFICATION/NCH	A/Gb	N/A	
NOTIFICATION RESPONSE	A/Gb	N/A	
TALKER INDICATION	A/Gb	N/A	
UPLINK ACCESS	A/Gb	N/A	
UPLINK BUSY	A/Gb	N/A	
UPLINK FREE	A/Gb	N/A	
UPLINK RELEASE	A/Gb	N/A	
VGCS UPLINK GRANT	A/Gb	N/A	
Measurement specific messages:	**Applicability**		
EXTENDED MEASUREMENT ORDER	Iu and A/Gb	Low	19
EXTENDED MEASUREMENT REPORT	Iu and A/Gb	Low	18
MEASUREMENT REPORT	Iu and A/Gb	Low	18
MEASUREMENT INFORMATION	Iu and A/Gb	Low	TBD
ENHANCED MEASUREMENT REPORT	Iu and A/Gb	Low	TBD
Miscellaneous messages:	**Applicability**		
CHANNEL MODE MODIFY	Iu and A/Gb	High	6 (10,13) – 17
CHANNEL MODE MODIFY ACKNOWLEDGE	Iu and A/Gb	High	6
CHANNEL REQUEST	Iu and A/Gb	Not applied	
CLASSMARK CHANGE	Iu and A/Gb	High	9-20
CLASSMARK ENQUIRY	Iu and A/Gb	High	5
UTRAN CLASSMARK CHANGE	Iu and A/Gb	High	4-n
cdma2000 CLASSMARK CHANGE	A/Gb (Iu is FFS)	High	TBD
	)		
FREQUENCY REDEFINITION	Iu and A/Gb	High	25 – 33
SYNCHRONIZATION CHANNEL INFORMATION	Iu and A/Gb	Not applied	
RR STATUS	A/Gb (Iu is FFS)	Not applied	3
GPRS SUSPENSION REQUEST	A/Gb (Iu is FFS)	High	13
Configuration Change messages:	**Applicability**		
CONFIGURATION CHANGE COMMAND	Iu and A/Gb	High	4 (6) – 15
CONFIGURATION CHANGE ACKNOWLEDGE	Iu and A/Gb	High	2
CONFIGURATION CHANGE REJECT	Iu and A/Gb	High	3
Application messages:	**Applicability**		
APPLICATION INFORMATION	A/Gb (Iu is FFS)	High	TBD (max over 200)

Note 1: "N/A" means that integrity protection is not at all applicable to this message (i.e. A/Gb mode messages). "Not applied" means that it clear that this message does not need to be integrity protected, or it is sensible at all (e.g. channel access). "Low" means that the need for integrity is considered to be low. "High" means that the need for integrity protection is considered to be high, i.e. these message, if tampered, could cause major problems, e.g. loss of connection.

Note 2: A (B,C,D) – E…F means that absolute minimum size of message is A, and other minimum sizes with different configurations are B, C and D. The maximum size of message is between E and F with different configurations.

Note 3: The initial Immediate Assignment procedure, which is used when moving from RRC Idle mode to RRC Connected mode, cannot be integrity protected. While in RRC Connected mode, the integrity protection of Immediated Assignment is possible in case of MT terminating traffic, but not in case of MO traffic (MS's identity is not known). Also in this case, the size of the message transferred to the lower layers may cause problems. Thus it is proposed that Immediate assignment is never integrity protected, except when used for TBF establishment (two-message assignment procedure available), see s3z010016.

3. 25.331 based RRC Messages

The integrity protection applicability for these messages is directly based on UTRAN.

Table 9.1b/3GPP TS 44.018: Additional 25.331 based Messages for Radio Resources management (these messages are applicable only in Iu mode)

Messages:	Integrity Protection
RRC connection request, setup and release	
RRC CONNECTION RELEASE COMPLETE	Required
RRC CONNECTION REJECT	Not applied
RRC CONNECTION RELEASE	Required
RRC CONNECTION SETUP	Not applied
RRC CONNECTION REQUEST	Not applied
RRC CONNECTION SETUP COMPLETE	Not applied
RRC connection mobility	
CELL UPDATE	Required
CELL UPDATE CONFIRM	Required
GRA UPDATE	Required
GRA UPDATE CONFIRM	Required
GERAN MOBILITY INFORMATION	Required
GERAN MOBILITY INFORMATION CONFIRM	Required
GERAN MOBILITY INFORMATION FAILURE	Required
HANDOVER TO UTRAN COMMAND	Required
HANDOVER FROM UTRAN COMMAND COMPLETE	Required
Radio bearer control procedures	

RADIO BEARER RECONFIGURATION	Required
RADIO BEARER RELEASE	Required
RADIO BEARER SETUP	Required
RADIO BEARER RECONFIGURATION COMPLETE	Required
RADIO BEARER RECONFIGURATION FAILURE	Required
RADIO BEARER RELEASE COMPLETE	Required
RADIO BEARER SETUP COMPLETE	Required
RADIO BEARER RELEASE FAILURE	Required
RADIO BEARER SETUP FAILURE	Required
Signaling flow procedures	
SIGNALLING CONNECTION RELEASE	Required
SIGNALLING CONNECTION RELEASE REQUEST	Required
INITIAL DIRECT TRANSFER	Required
DOWNLINK DIRECT TRANSFER	Required
UPLINK DIRECT TRANSFER	Required
Security mode control	
SECURITY MODE COMMAND	Required
SECURITY MODE COMPLETE	Required
SECURITY MODE FAILURE	Required

4. Summary

4.1.RRC messages not to be integrity protected

The list with all RRC messages applicable to Iu mode, which are not integrity protected, is presented below.

Channel establishment messages:
IMMEDIATE ASSIGNMENT (*)
IMMEDIATE ASSIGNMENT EXTENDED
IMMEDIATE ASSIGNMENT REJECT
RR INITIALISATION REQUEST
Handover messages:
HANDOVER ACCESS
Paging messages:
PACKET NOTIFICATION
PAGING REQUEST TYPE 1
PAGING REQUEST TYPE 2
PAGING REQUEST TYPE 3
PAGING RESPONSE
System information messages:
SYSTEM INFORMATION TYPE 1 – 20
Miscellaneous messages:
CHANNEL REQUEST
SYNCHRONIZATION CHANNEL INFORMATION
RR STATUS
Measurement specific messages:
EXTENDED MEASUREMENT ORDER
EXTENDED MEASUREMENT REPORT
MEASURMENT REPORT
MEASUREMENT INFORMATION
ENHANCED MEASUREMENT REPORT
RRC connection request, setup and release
RRC CONNECTION REJECT RRC CONNECTION SETUP RRC CONNECTION REQUEST RRC CONNECTION SETUP COMPLETE

(*) Except when TBF establishment is performed.