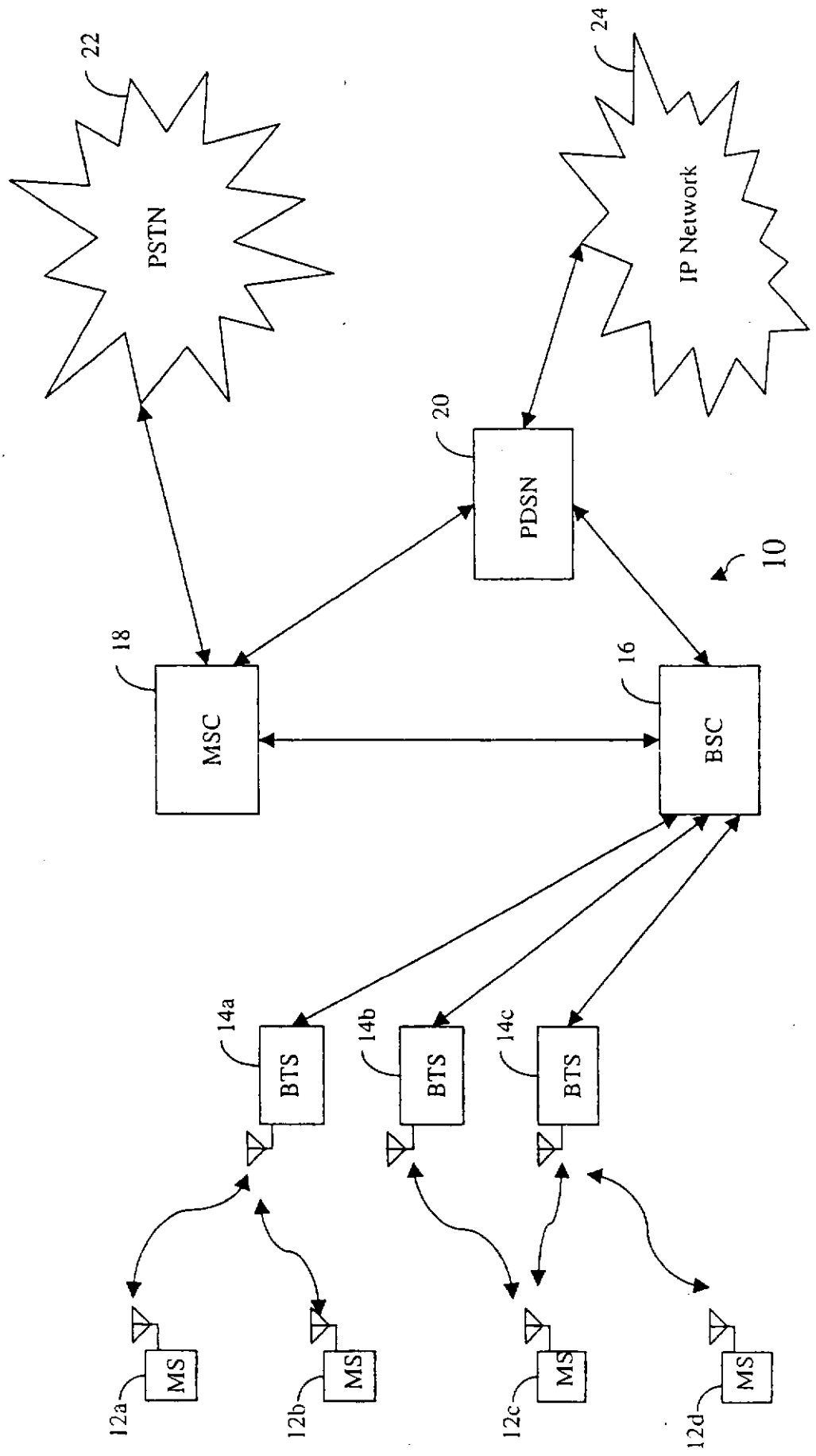

22
PSTN
24
IP Network
20
PDSN
10
18
MSC
16
BSC
14a
BTS
14b
BTS
14c
BTS
12a
MS
12b
MS
12c
MS
12d
MS

FIG. 1

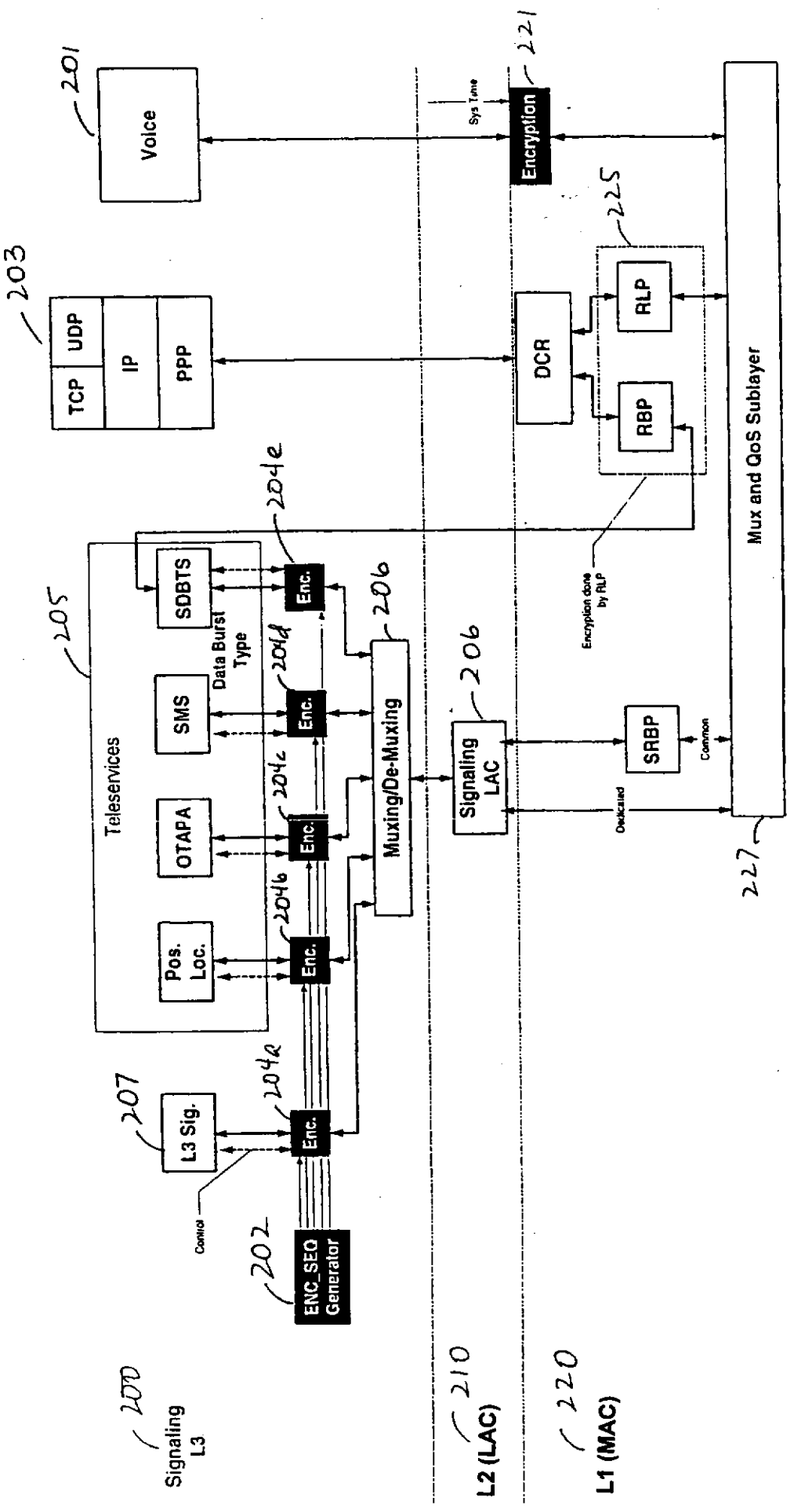

Voice
201
Sys Time
Encryption
221
225
203
UDP
TCP
IP
PPP
DCR
RLP
RBP
Encryption done by RLP
Mux and QoS Sublayer
204e
SDBTS
Enc.
205
Teleservices
Data Burst Type
SMS
204d
Enc.
206
OTAPA
204c
Enc.
Muxing/De-Muxing
Signaling LAC
206
Pos. Loc.
204b
Enc.
SRBP
Common
Dedicated
207
L3 Sig.
204a
Enc.
Control
202
ENC_SEQ Generator
227
200
Signaling L3
210
L2 (LAC)
220
L1 (MAC)

FIG. 2

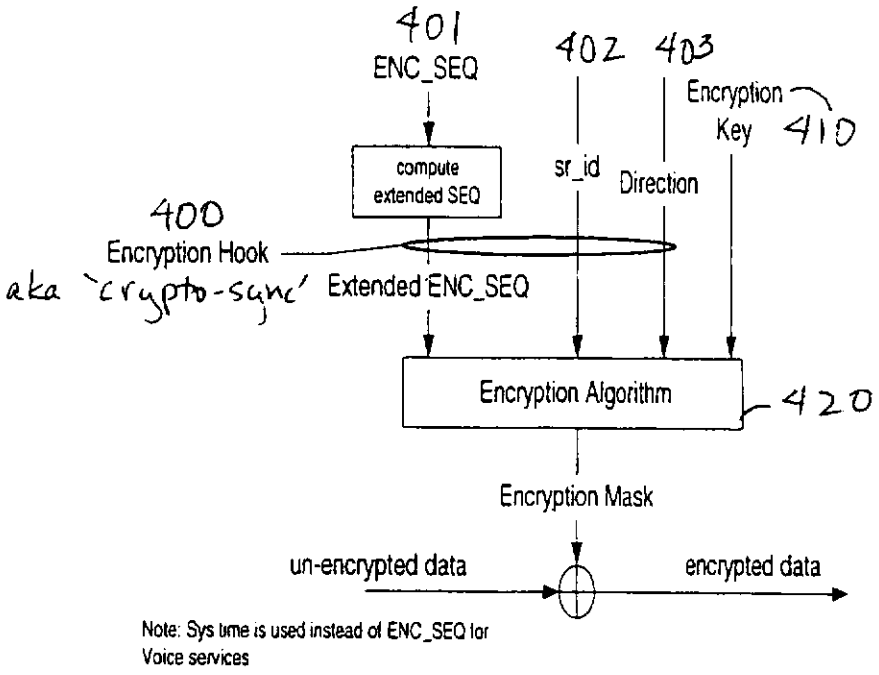
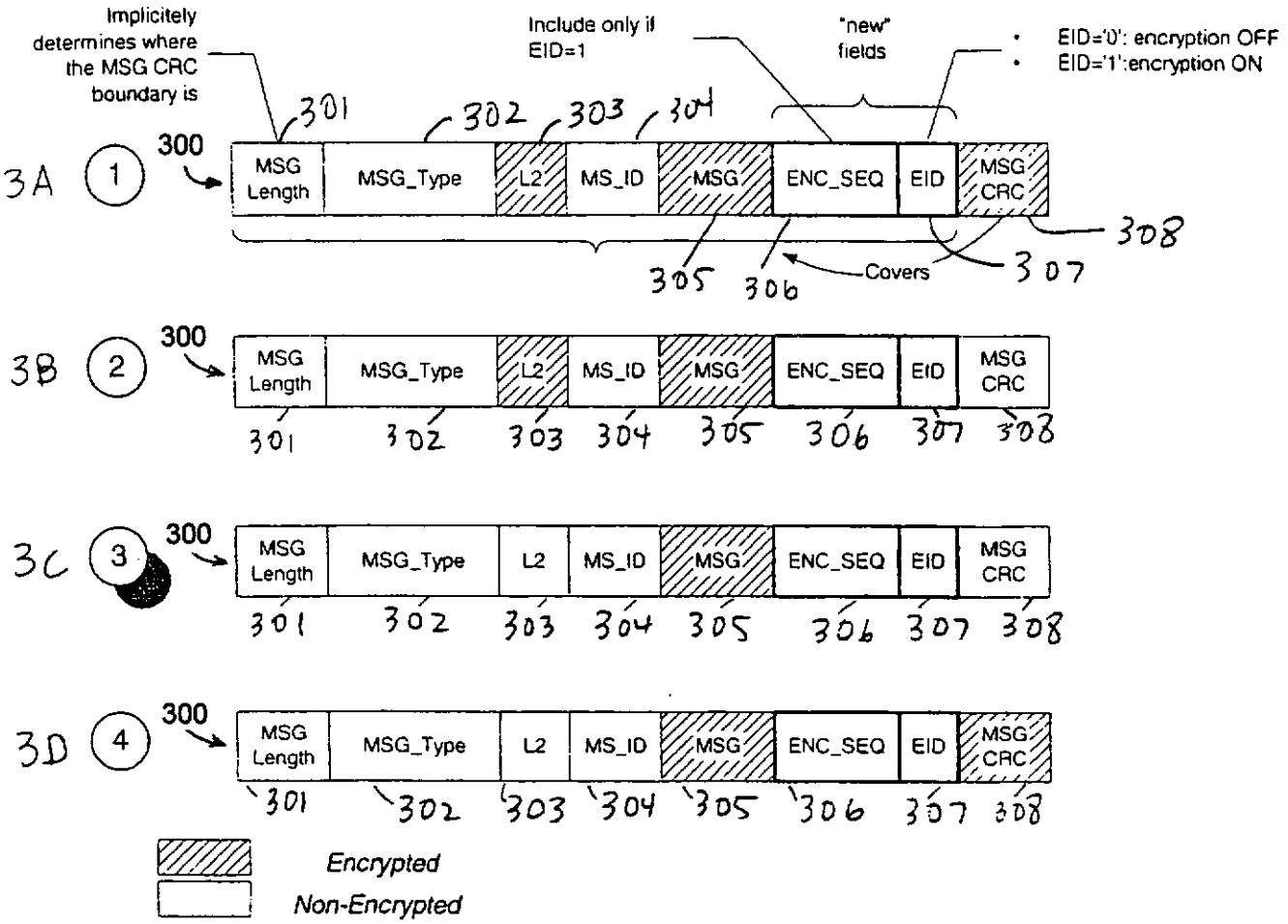

401
ENC_SEQ
402
403
Encryption Key
410
compute extended SEQ
sr_id
Direction
400
Encryption Hook
aka 'crypto-sync'
Extended ENC_SEQ
Encryption Algorithm
420
Encryption Mask
un-encrypted data
encrypted data
Note: Sys time is used instead of ENC_SEQ for Voice services

FIG. 4



Note: L2 fields represents all the fields that are added by cdma2000 LAC and are not explicitely shown in this figure as a separate field (e.g., ARQ, Auth., etc.)

FIG. 3

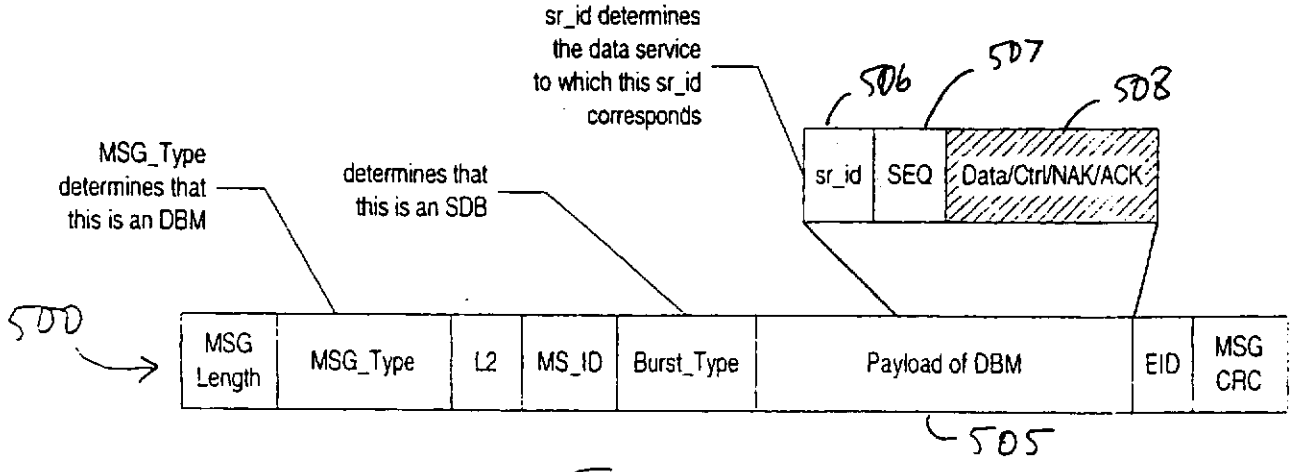


FIG. 5

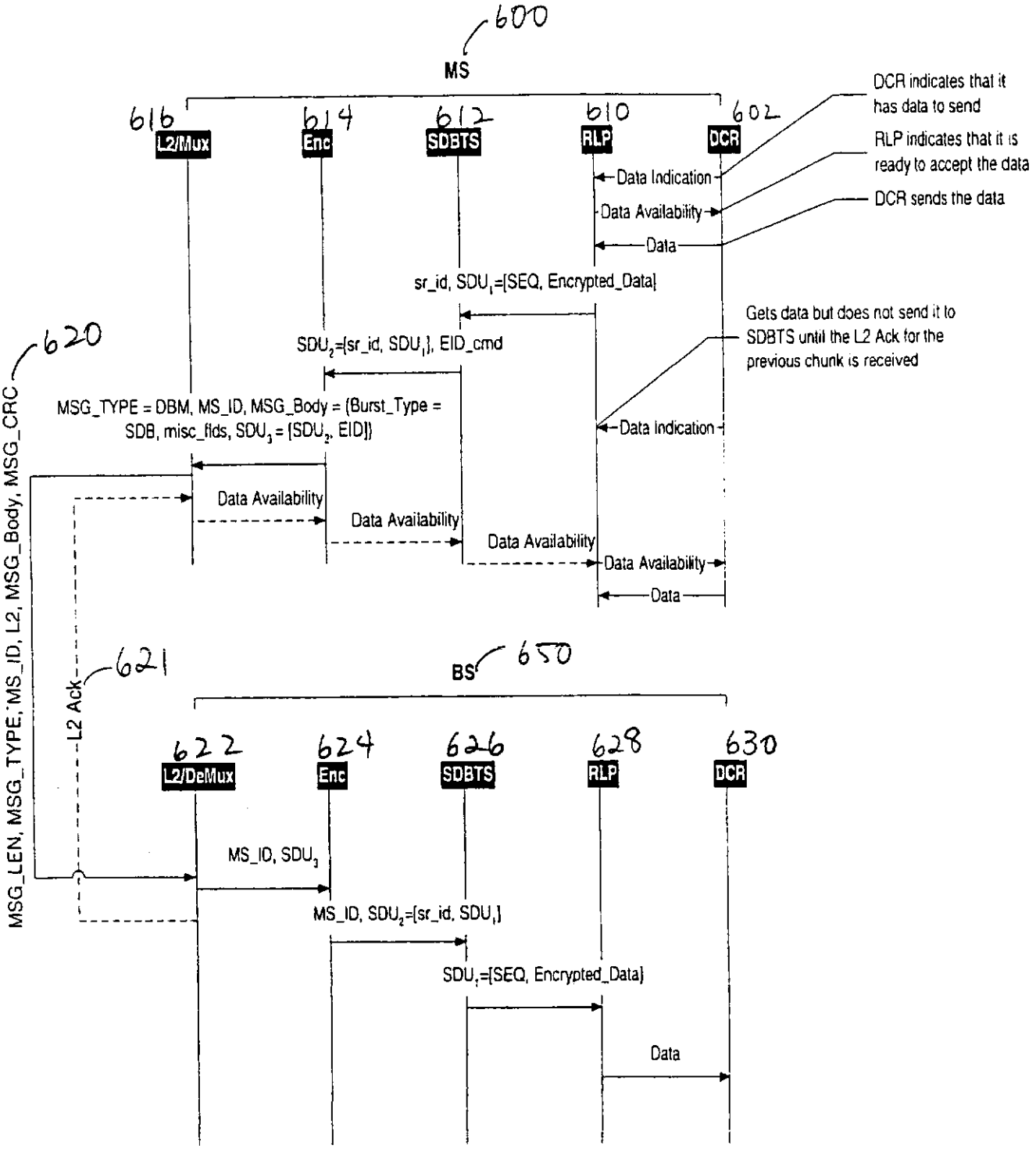

600
MS
616
L2/Mux
614
Enc
612
SDBTS
610
RLP
602
DCR
DCR indicates that it has data to send
RLP indicates that it is ready to accept the data
DCR sends the data
Data Indication
Data Availability
Data
sr_id, SDU1={SEQ, Encrypted_Data}
Gets data but does not send it to SDBTS until the L2 Ack for the previous chunk is received
620
SDU2={sr_id, SDU1}, EID_cmd
MSG_TYPE = DBM, MS_ID, MSG_Body = {Burst_Type = SDB, misc_flds, SDU3 = {SDU2, EID}}
Data Indication
Data Availability
Data Availability
Data Availability
Data Availability
Data
MSG_LEN, MSG_TYPE, MS_ID, L2, MSG_Body, MSG_CRC
621
L2 Ack
650
BS
622
L2/DeMux
624
Enc
626
SDBTS
628
RLP
630
DCR
MS_ID, SDU3
MS_ID, SDU2={sr_id, SDU1}
SDU1={SEQ, Encrypted_Data}
Data

FIG. 6

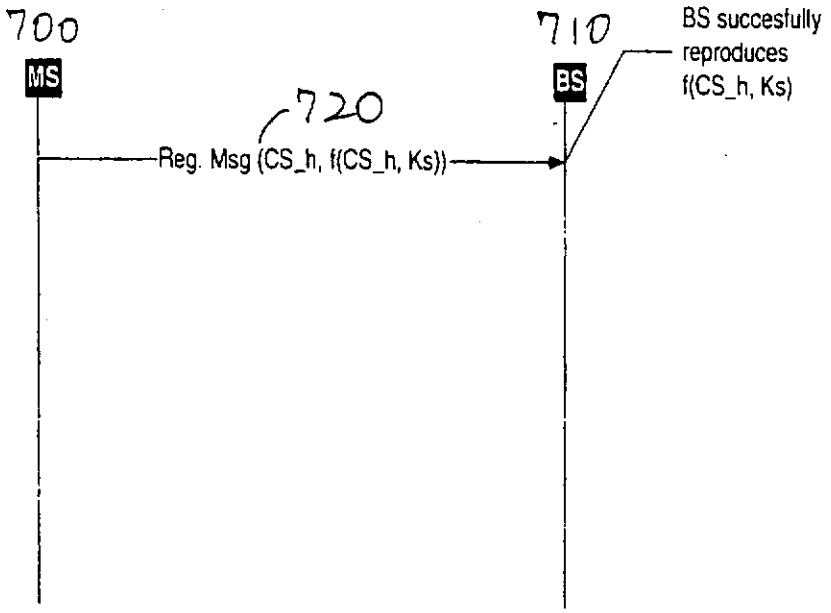

700
MS
710
BS
BS succesfully reproduces f(CS_h, Ks)
720
Reg. Msg (CS_h, f(CS_h, Ks))

FIG. 7

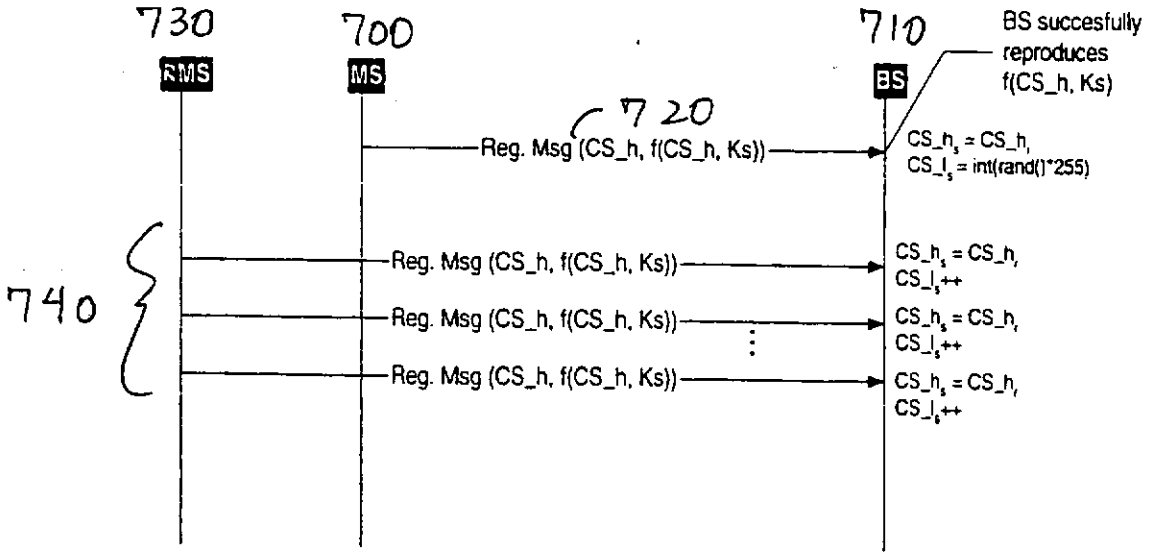

730
RMS
700
MS
710
BS
BS succesfully reproduces f(CS_h, Ks)
720
Reg. Msg (CS_h, f(CS_h, Ks))
CS_h_s = CS_h, CS_l_s = int(rand()*255)
740
Reg. Msg (CS_h, f(CS_h, Ks))
CS_h_s = CS_h, CS_l_s++
Reg. Msg (CS_h, f(CS_h, Ks))
CS_h_s = CS_h, CS_l_s++
Reg. Msg (CS_h, f(CS_h, Ks))
CS_h_s = CS_h, CS_l_s++

FIG. 8

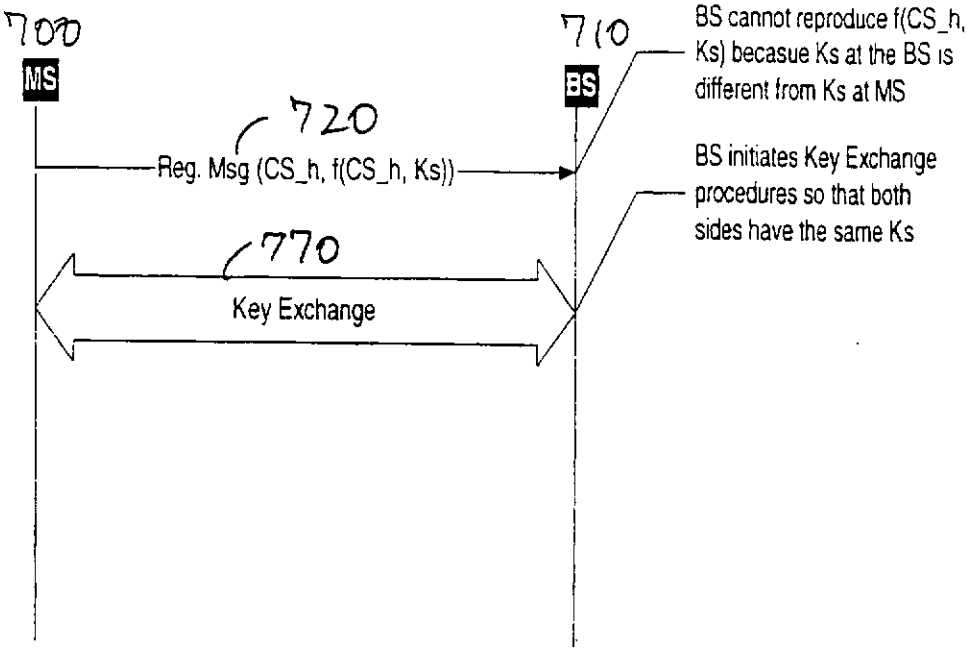
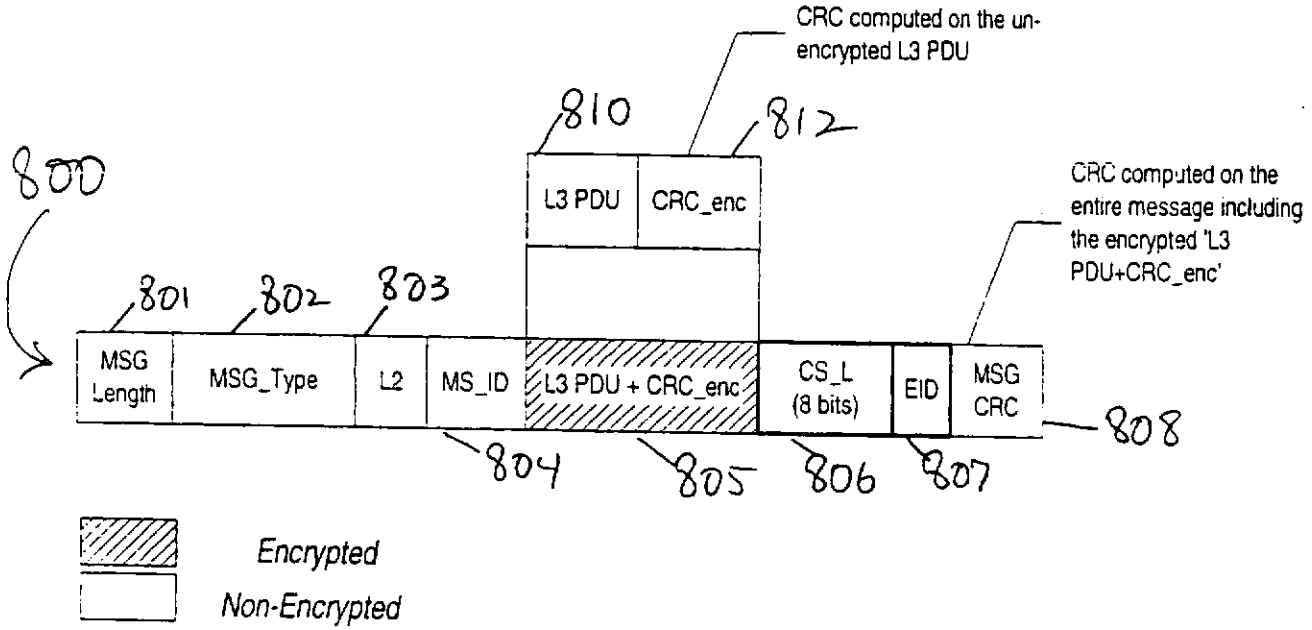


FIG. 9



Note: L2 fields represents all the fields that are added by cdma2000 LAC and are not explicitely shown in this figure as a separate field (e.g., ARQ, Auth., etc.)

FIG. 10

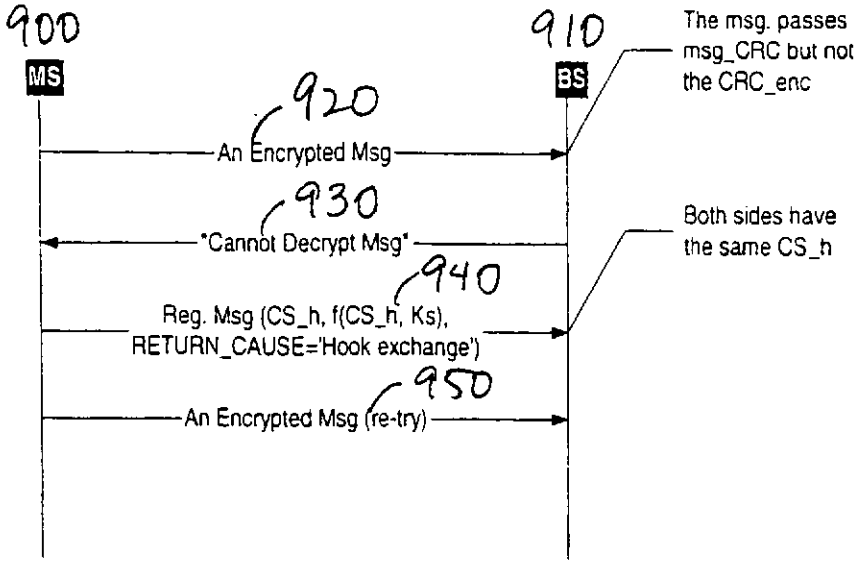

900
MS
910
BS
The msg. passes msg_CRC but not the CRC_enc
920
An Encrypted Msg
930
"Cannot Decrypt Msg"
Both sides have the same CS_h
940
Reg. Msg (CS_h, f(CS_h, Ks), RETURN_CAUSE='Hook exchange')
950
An Encrypted Msg (re-try)

FIG. 11

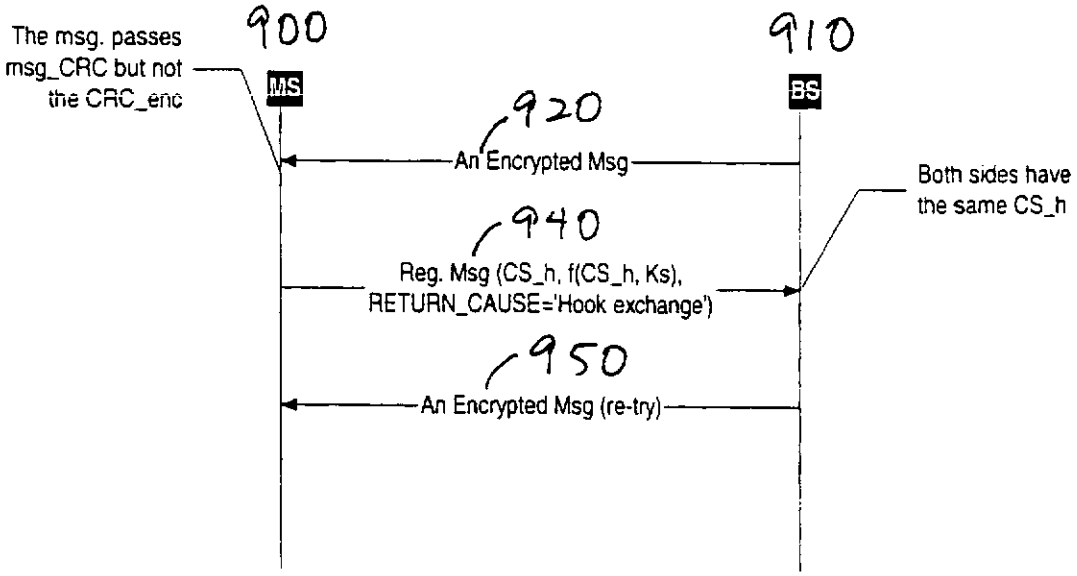

The msg. passes msg_CRC but not the CRC_enc
900
MS
910
BS
920
An Encrypted Msg
Both sides have the same CS_h
940
Reg. Msg (CS_h, f(CS_h, Ks), RETURN_CAUSE='Hook exchange')
950
An Encrypted Msg (re-try)

FIG. 12