FIG.1A

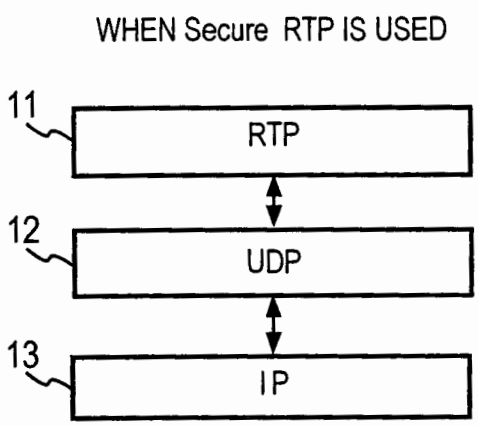


FIG.1B

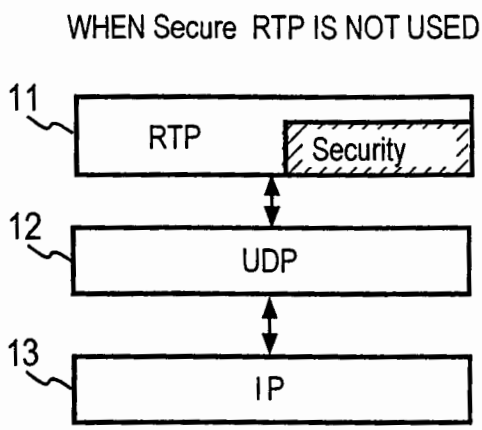


FIG.2

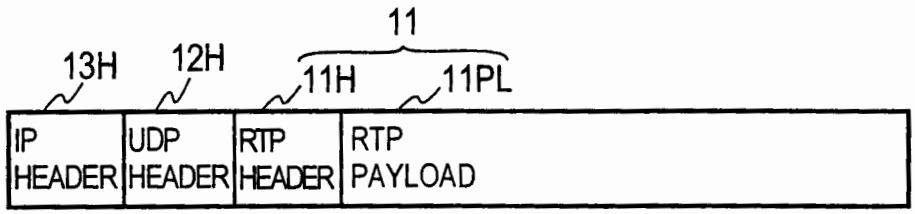


FIG.3

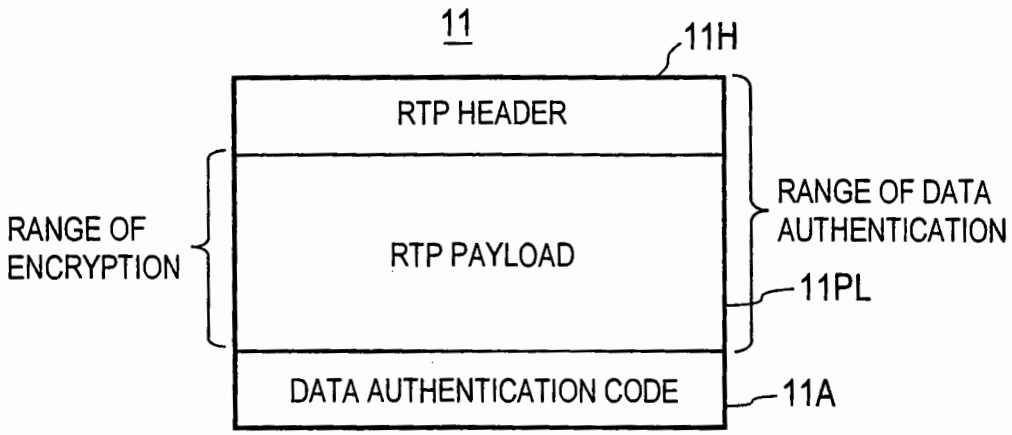


FIG.4A

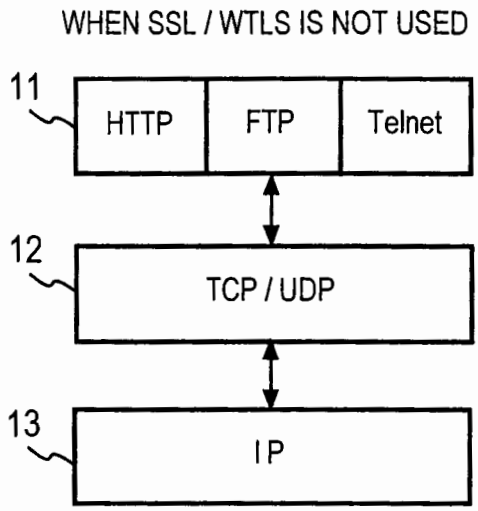

WHEN SSL / WTLS IS NOT USED
11
HTTP
FTP
Telnet
12
TCP / UDP
13
IP

FIG.4B

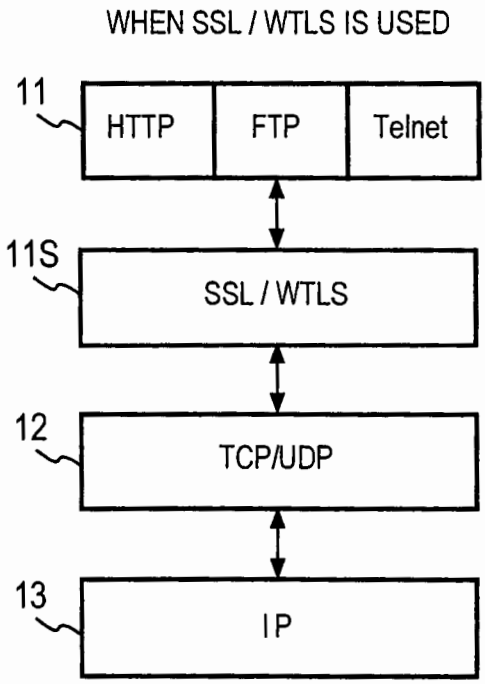

WHEN SSL / WTLS IS USED
11
HTTP
FTP
Telnet
11S
SSL / WTLS
12
TCP/UDP
13
IP

FIG.5

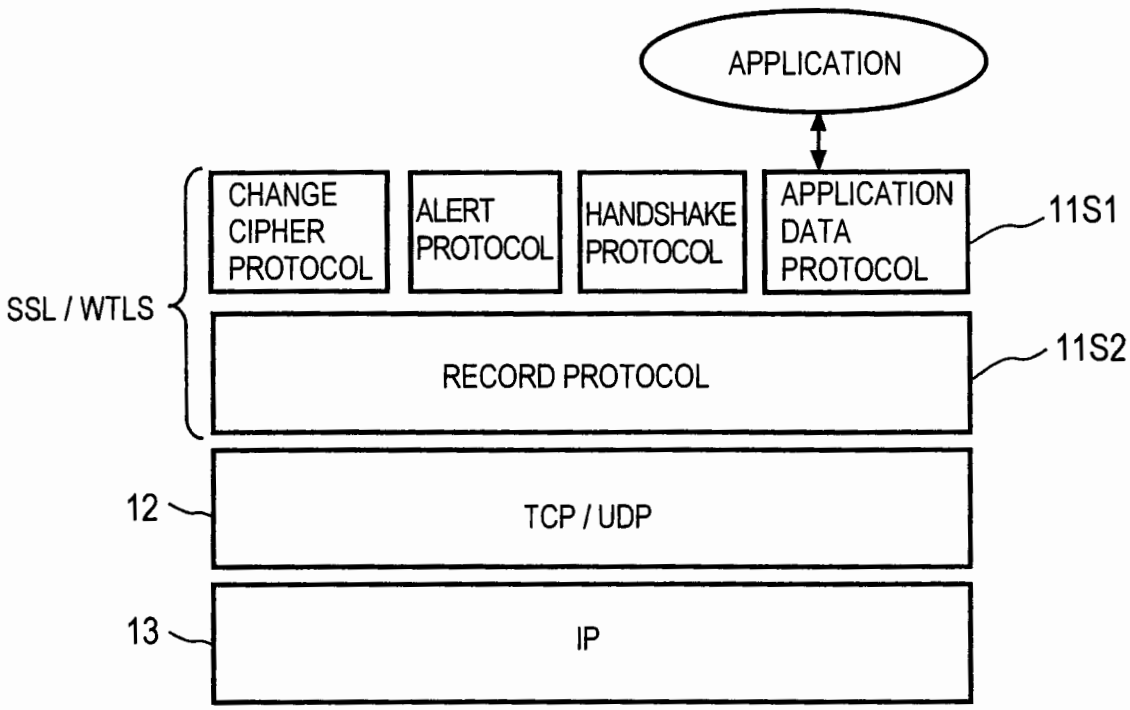
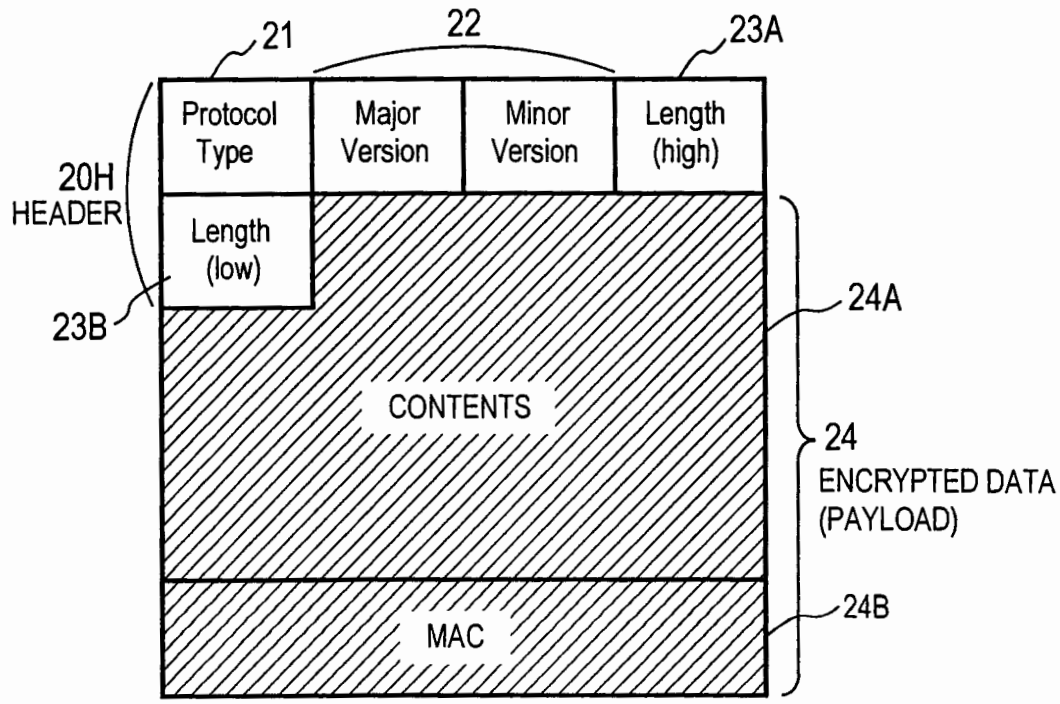

APPLICATION
CHANGE CIPHER PROTOCOL
ALERT PROTOCOL
HANDSHAKE PROTOCOL
APPLICATION DATA PROTOCOL
11S1
SSL / WTLS
RECORD PROTOCOL
11S2
12
TCP / UDP
13
IP

FIG.6


21
22
23A
Protocol Type
Major Version
Minor Version
Length (high)
20H HEADER
Length (low)
23B
24A
CONTENTS
24
ENCRYPTED DATA (PAYLOAD)
MAC
24B

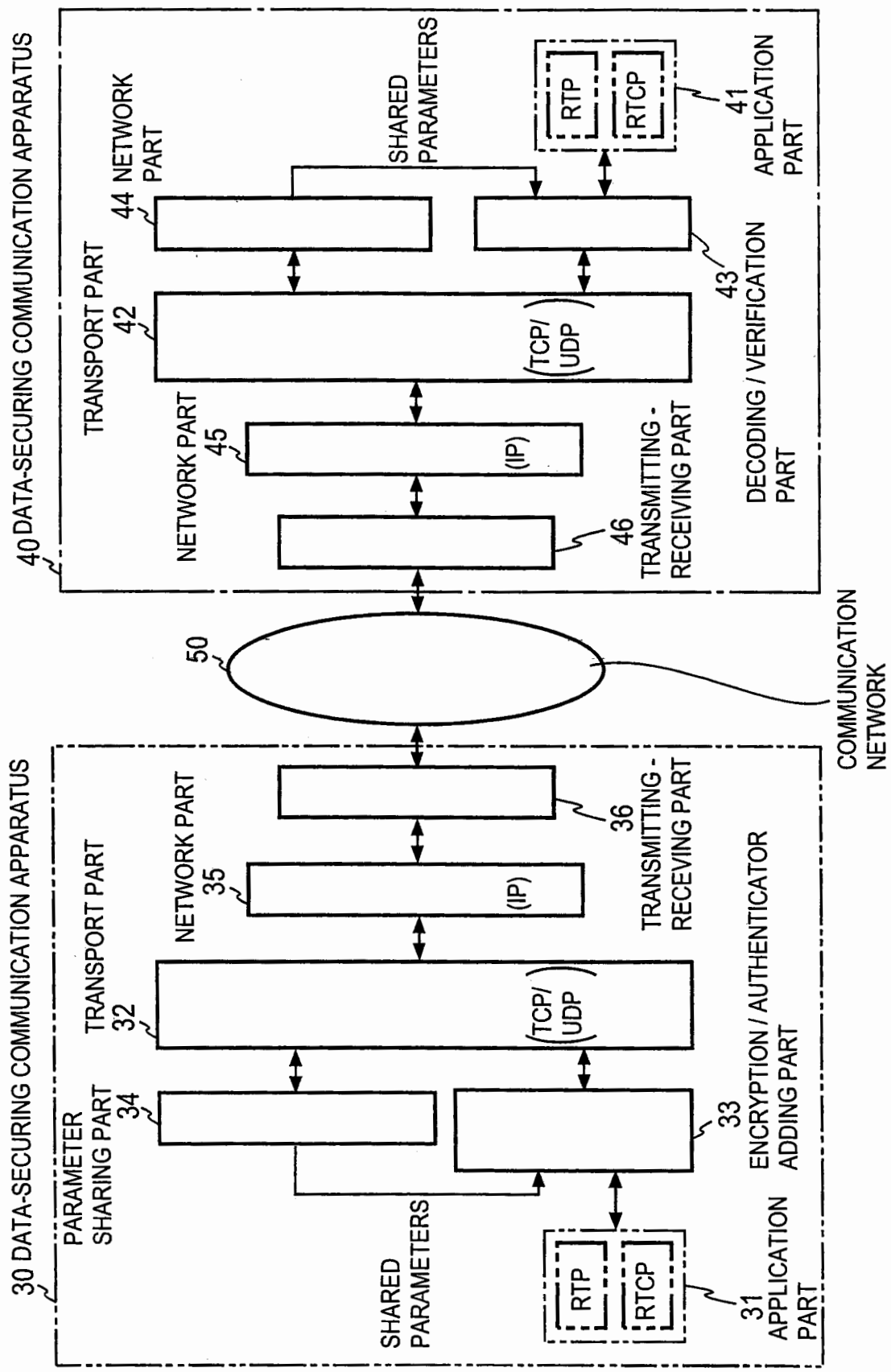

30 DATA-SECURING COMMUNICATION APPARATUS
PARAMETER SHARING PART
34
TRANSPORT PART
32
NETWORK PART
35
(IP)
36
TRANSMITTING - RECEVING PART
ENCRYPTION / AUTHENTICATOR ADDING PART
33
SHARED PARAMETERS
RTP
RTCP
31
APPLICATION PART
50
COMMUNICATION NETWORK
40 DATA-SECURING COMMUNICATION APPARATUS
44 NETWORK PART
SHARED PARAMETERS
RTP
RTCP
41
APPLICATION PART
TRANSPORT PART
42
(TCP/UDP)
43
DECODING / VERIFICATION PART
NETWORK PART
45
(IP)
46
TRANSMITTING - RECEIVING PART

FIG.7

FIG.8

- ENCRYPTIO ALGORITHM
  - Null, DES, 3DES, RC4, etc...
- DATA AUTHENTICATOR GENERATING ALGORITHM
  - MD5, SHA, etc...
- SECRET INFORMATION
- RANDOM VALUE
  - SERVER
  - CLIENT
- RANGE OF ENCRYPTION
- RANGE OF DATA AUTHENTICATION

FIG.9

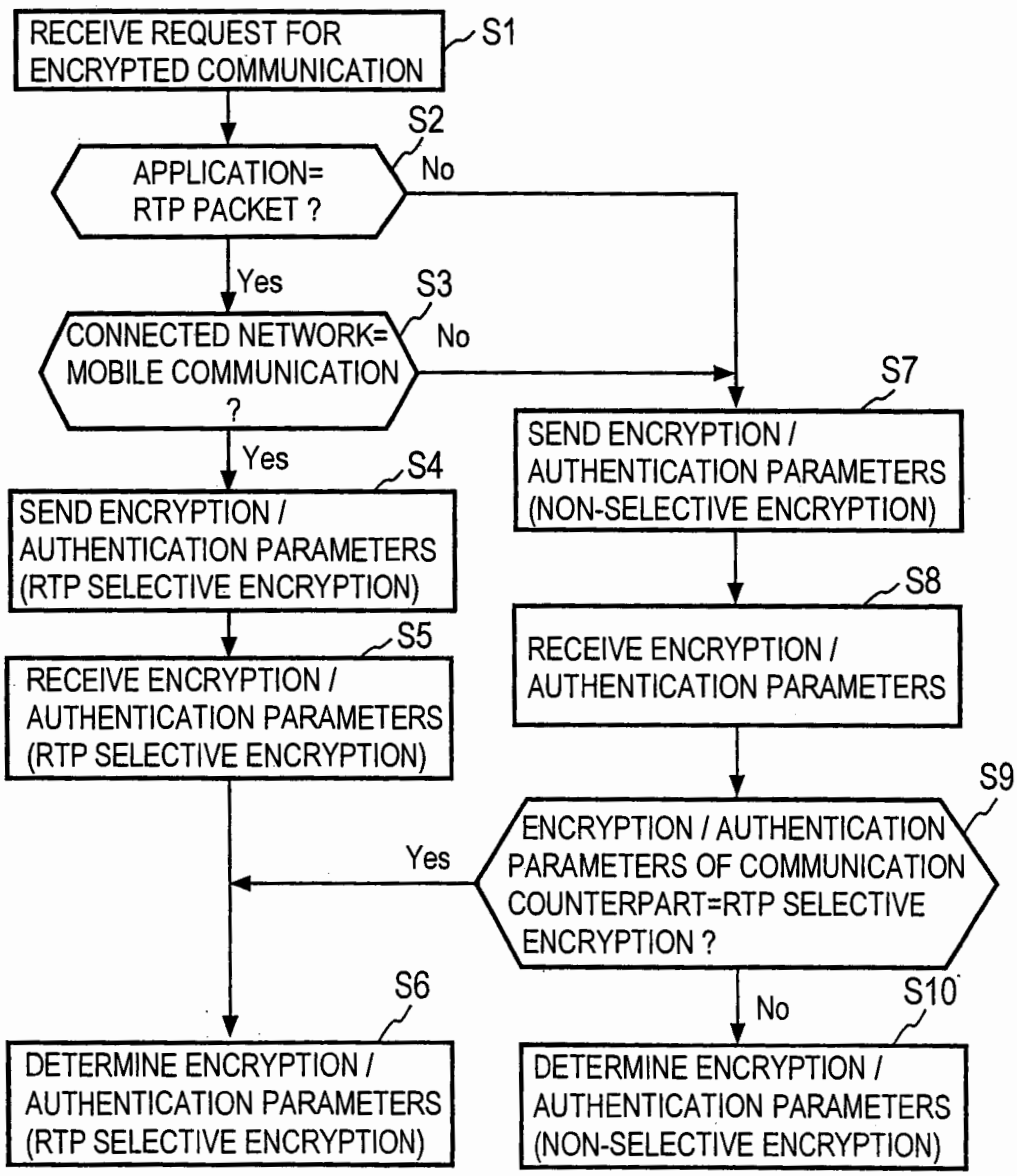


FIG.10

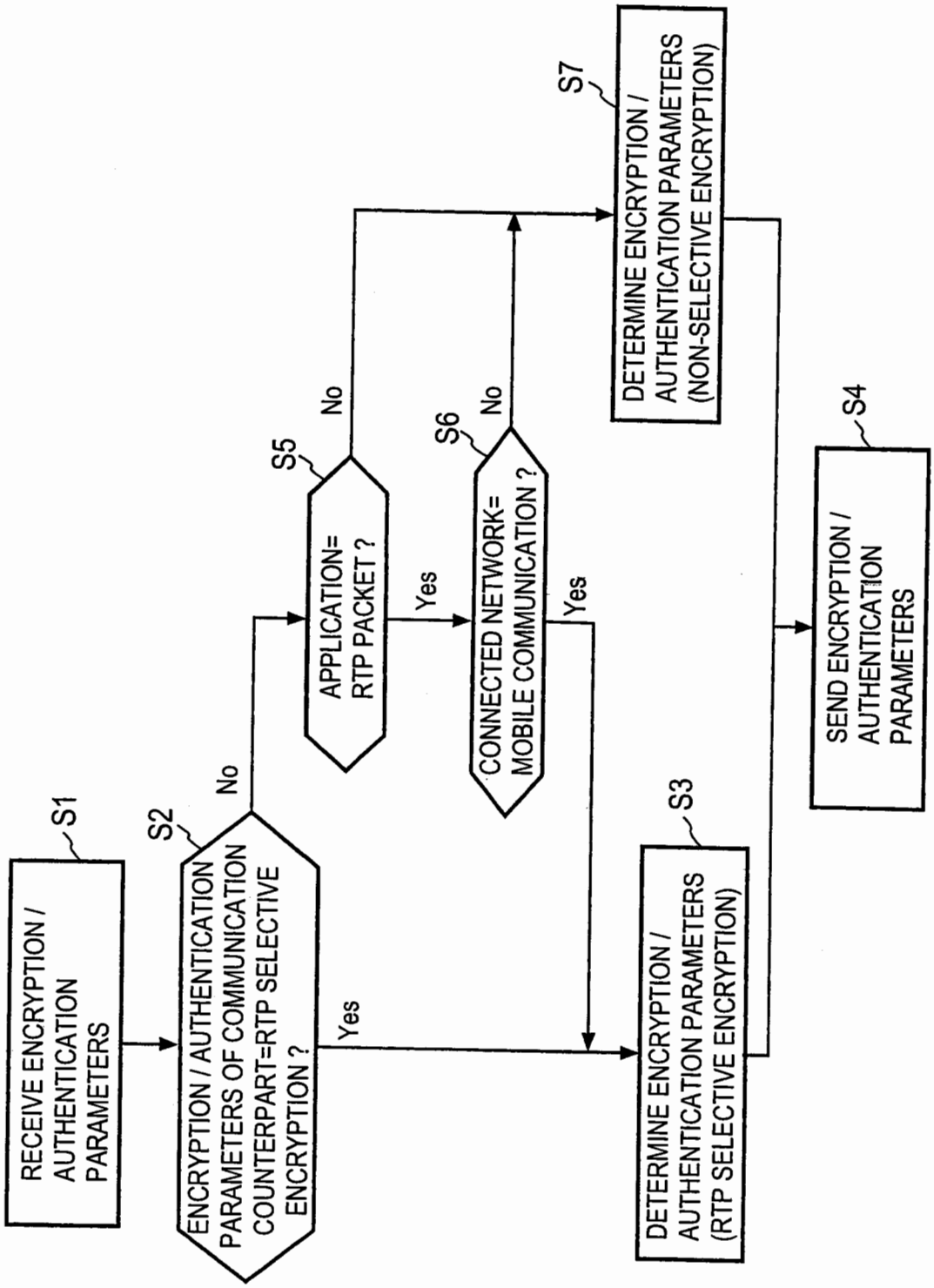

RECEIVE ENCRYPTION / AUTHENTICATION PARAMETERS
S1
ENCRYPTION / AUTHENTICATION PARAMETERS OF COMMUNICATION COUNTERPART=RTP SELECTIVE ENCRYPTION ?
S2
No
Yes
APPLICATION= RTP PACKET ?
S5
No
Yes
CONNECTED NETWORK= MOBILE COMMUNICATION ?
S6
No
Yes
DETERMINE ENCRYPTION / AUTHENTICATION PARAMETERS (RTP SELECTIVE ENCRYPTION)
S3
DETERMINE ENCRYPTION / AUTHENTICATION PARAMETERS (NON-SELECTIVE ENCRYPTION)
S7
SEND ENCRYPTION / AUTHENTICATION PARAMETERS
S4

FIG.11

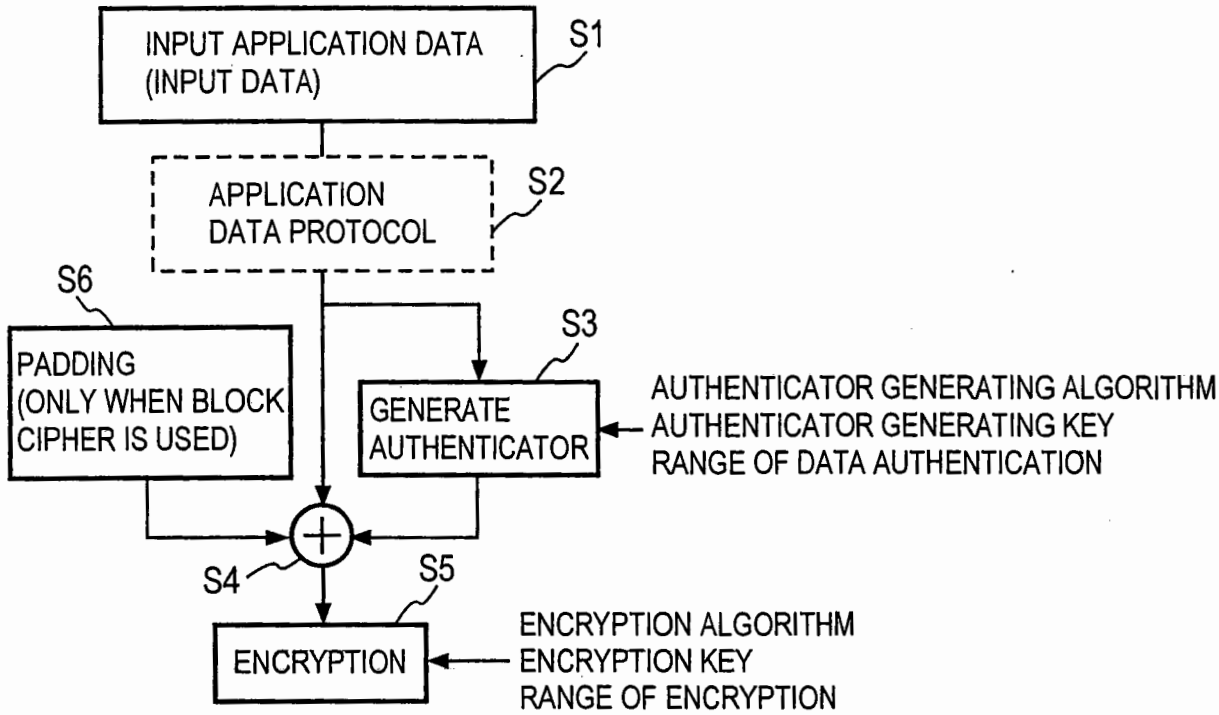

INPUT APPLICATION DATA
(INPUT DATA)
S1
APPLICATION
DATA PROTOCOL
S2
S6
PADDING
(ONLY WHEN BLOCK
CIPHER IS USED)
S3
GENERATE
AUTHENTICATOR
AUTHENTICATOR GENERATING ALGORITHM
AUTHENTICATOR GENERATING KEY
RANGE OF DATA AUTHENTICATION
S4
S5
ENCRYPTION
ENCRYPTION ALGORITHM
ENCRYPTION KEY
RANGE OF ENCRYPTION

FIG.12

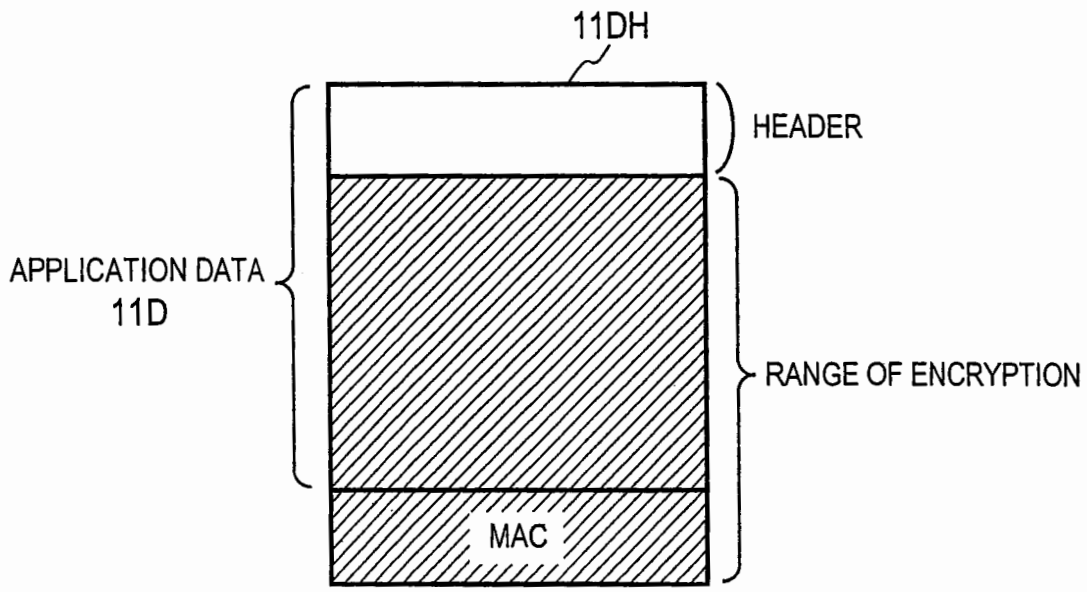

11DH
HEADER
APPLICATION DATA
11D
RANGE OF ENCRYPTION
MAC

FIG.13

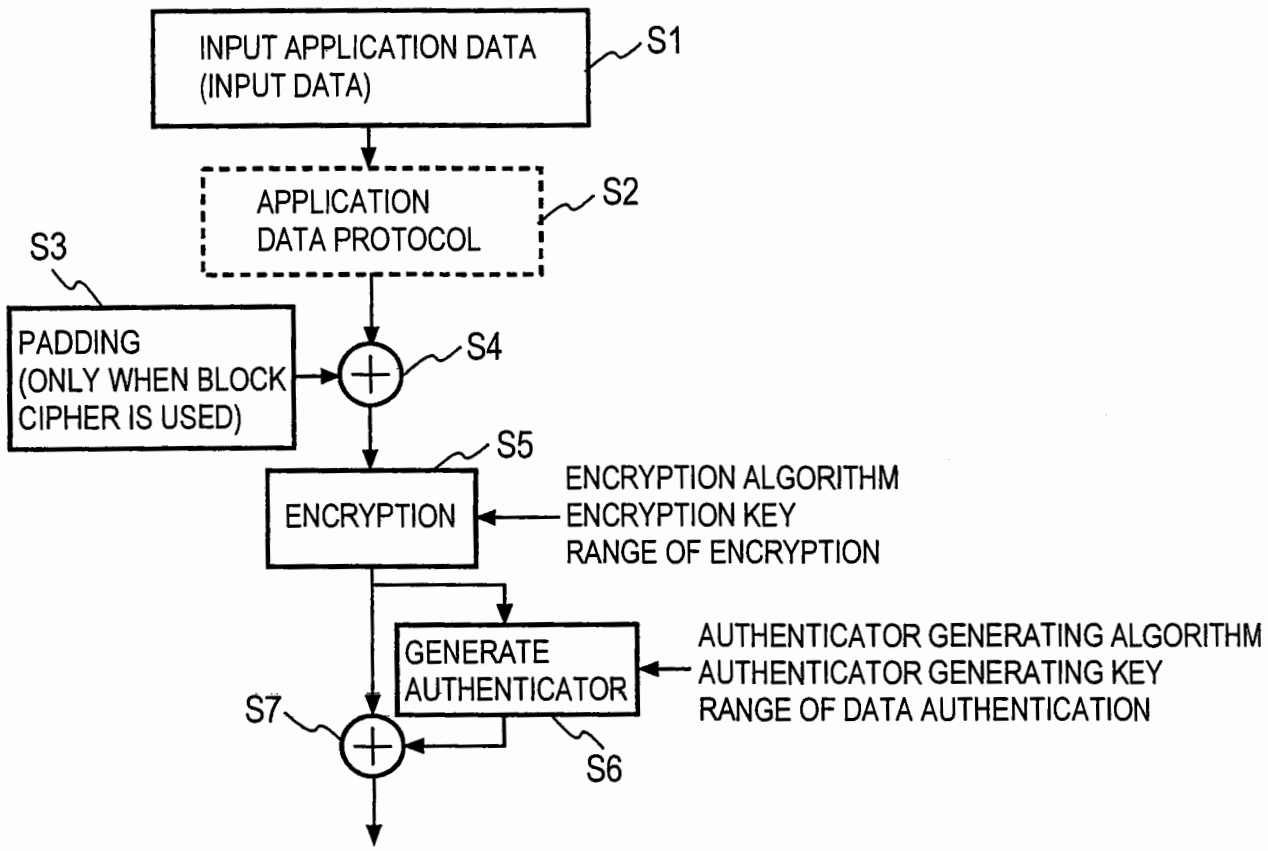

INPUT APPLICATION DATA
(INPUT DATA)
S1
APPLICATION
DATA PROTOCOL
S2
S3
PADDING
(ONLY WHEN BLOCK
CIPHER IS USED)
S4
S5
ENCRYPTION
ENCRYPTION ALGORITHM
ENCRYPTION KEY
RANGE OF ENCRYPTION
GENERATE
AUTHENTICATOR
AUTHENTICATOR GENERATING ALGORITHM
AUTHENTICATOR GENERATING KEY
RANGE OF DATA AUTHENTICATION
S7
S6

FIG.14

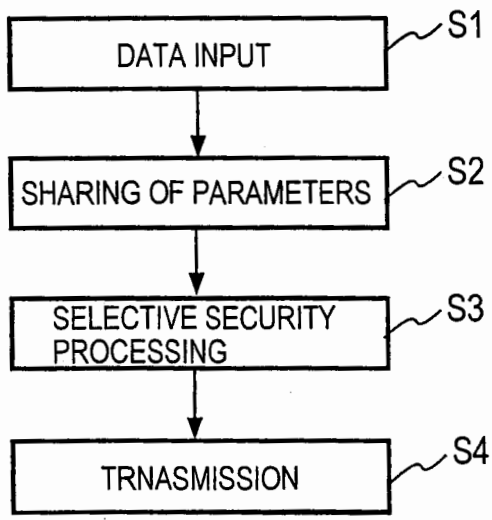

DATA INPUT
S1
SHARING OF PARAMETERS
S2
SELECTIVE SECURITY
PROCESSING
S3
TRNASMISSION
S4

FIG.15

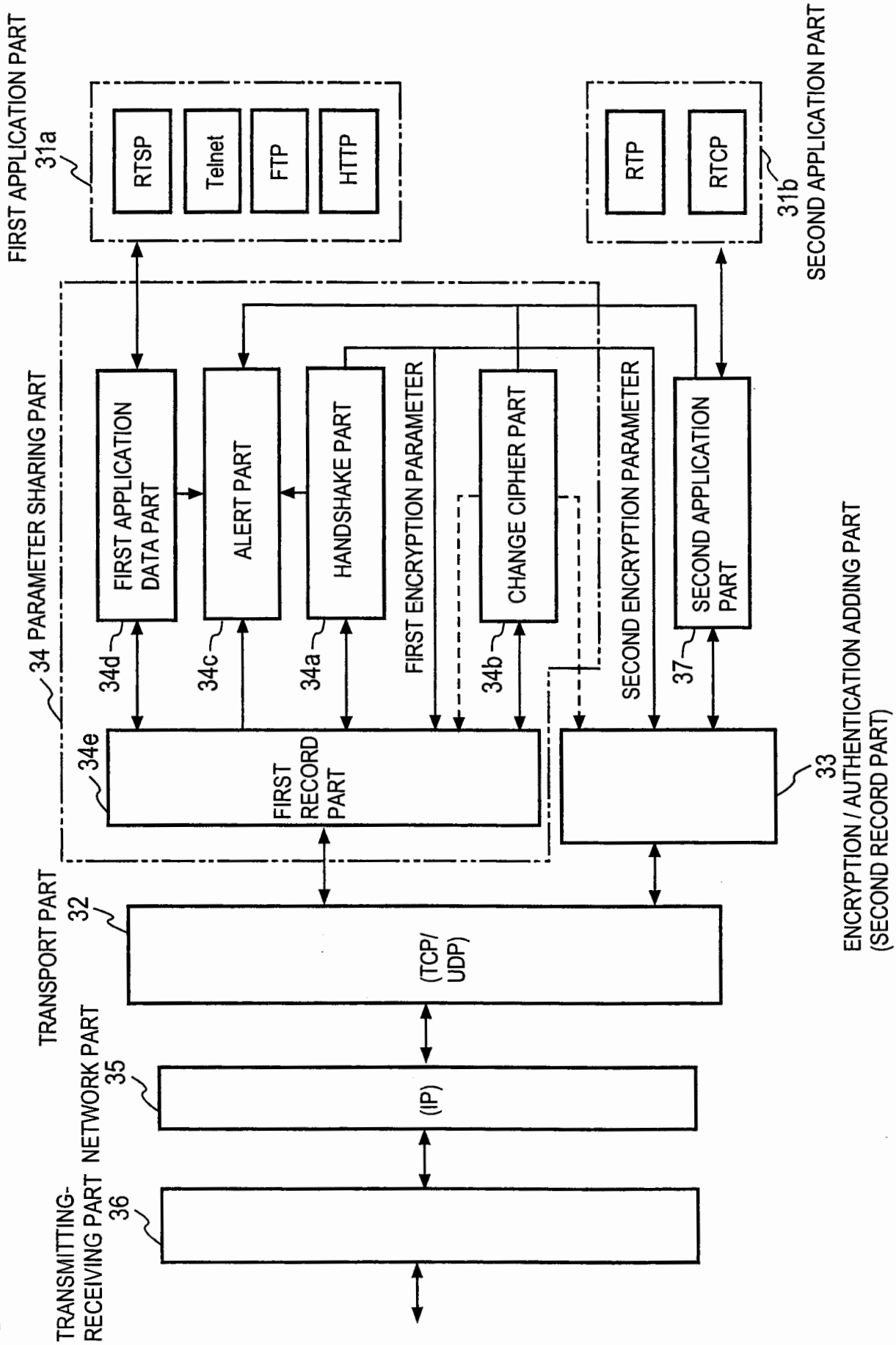
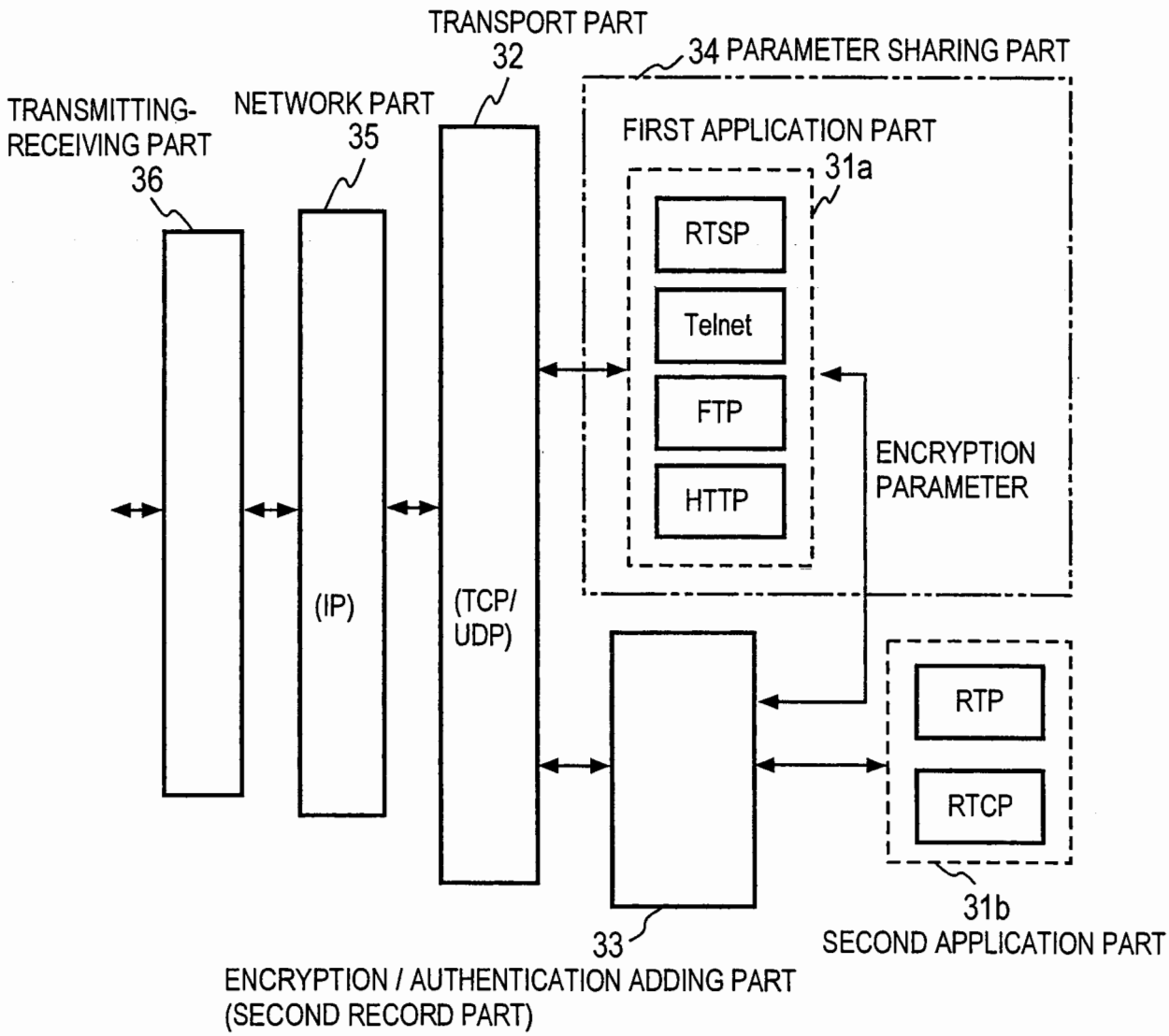

FIRST APPLICATION PART
31a
RTSP
Telnet
FTP
HTTP
RTP
RTCP
31b
SECOND APPLICATION PART
34 PARAMETER SHARING PART
FIRST APPLICATION DATA PART
ALERT PART
HANDSHAKE PART
FIRST ENCRYPTION PARAMETER
CHANGE CIPHER PART
SECOND ENCRYPTION PARAMETER
SECOND APPLICATION PART
34d
34c
34a
34b
37
34e
FIRST RECORD PART
33
ENCRYPTION / AUTHENTICATION ADDING PART
(SECOND RECORD PART)
TRANSPORT PART
32
(TCP/ UDP)
NETWORK PART
35
(IP)
TRANSMITTING-RECEIVING PART
36

FIG.16


TRANSPORT PART
32
34 PARAMETER SHARING PART
TRANSMITTING-
RECEIVING PART
36
NETWORK PART
35
FIRST APPLICATION PART
31a
RTSP
Telnet
FTP
HTTP
ENCRYPTION
PARAMETER
(IP)
(TCP/
UDP)
RTP
RTCP
31b
SECOND APPLICATION PART
33
ENCRYPTION / AUTHENTICATION ADDING PART
(SECOND RECORD PART)