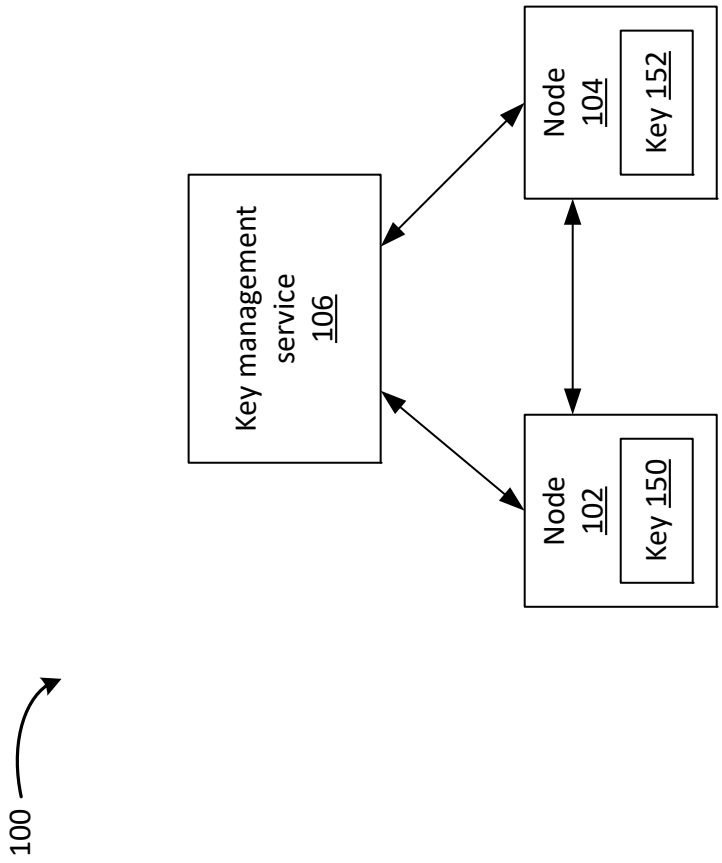
100
Key management service 106
Node 102
Key 150
Node 104
Key 152

FIG. 1

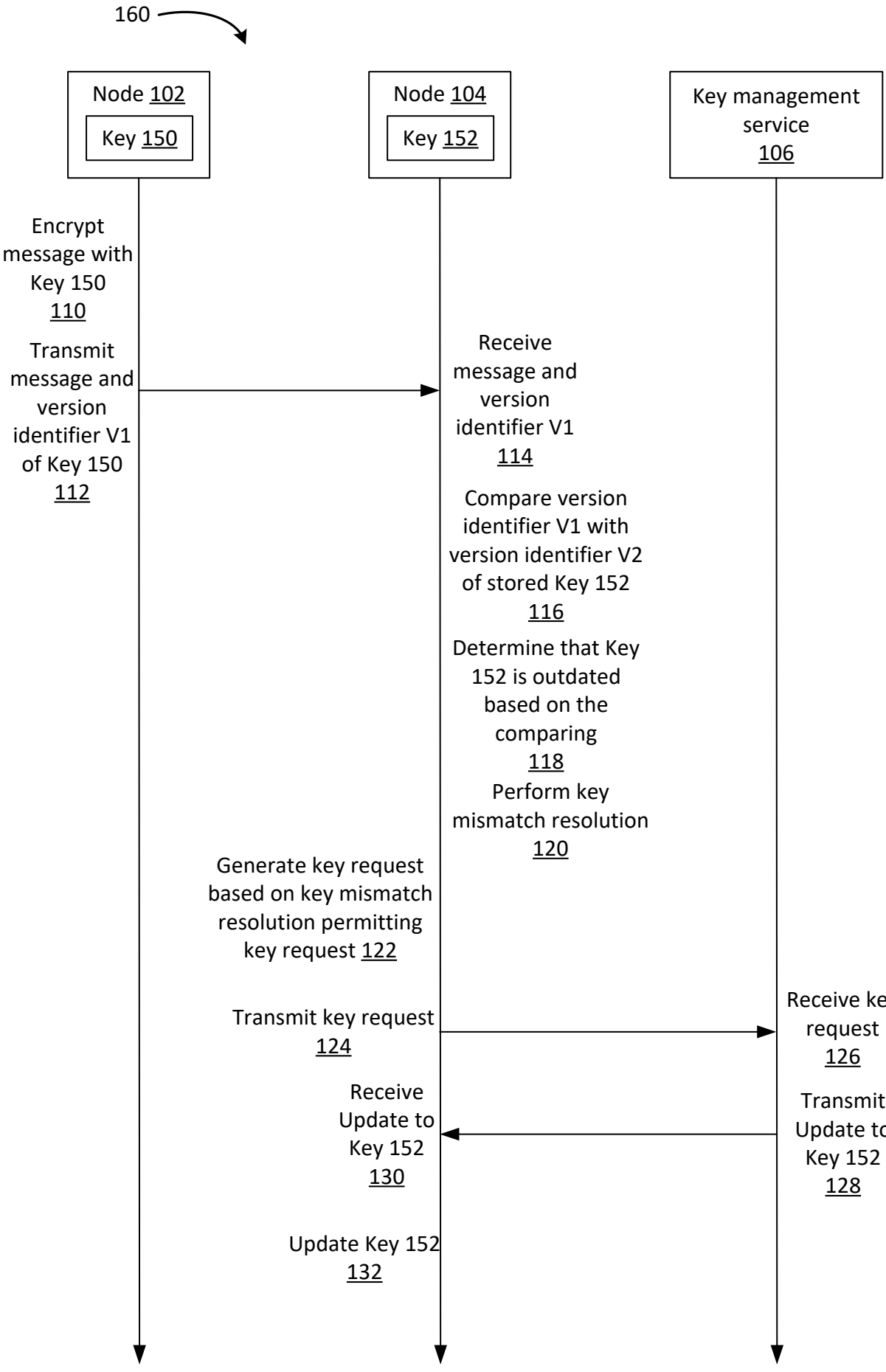
160
Node 102
Key 150
Node 104
Key 152
Key management service 106
Encrypt message with Key 150 110
Transmit message and version identifier V1 of Key 150 112
Receive message and version identifier V1 114
Compare version identifier V1 with version identifier V2 of stored Key 152 116
Determine that Key 152 is outdated based on the comparing 118
Perform key mismatch resolution 120
Generate key request based on key mismatch resolution permitting key request 122
Transmit key request 124
Receive key request 126
Receive Update to Key 152 130
Transmit Update to Key 152 128
Update Key 152 132

FIG. 2A

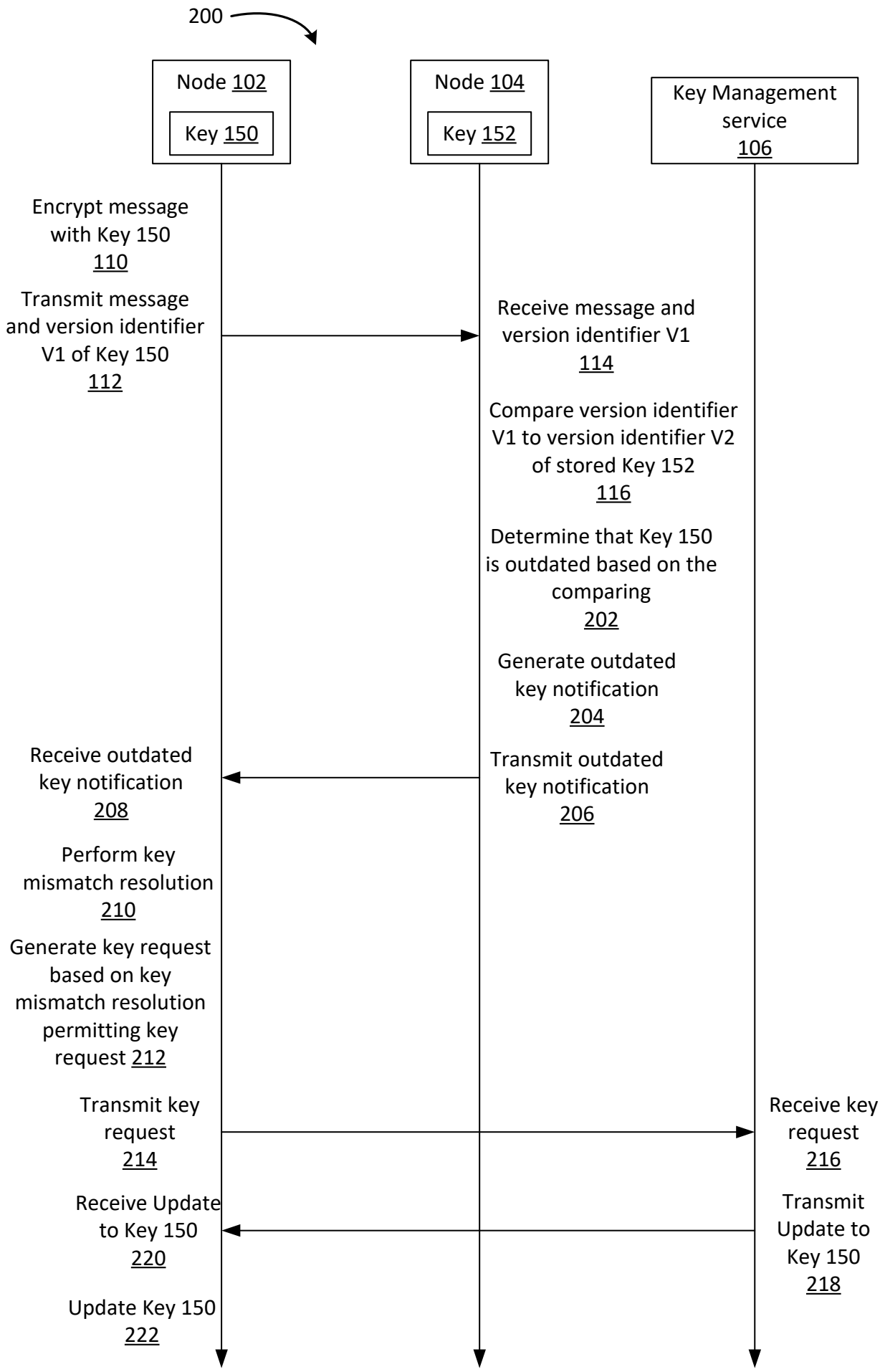
200
Node 102
Key 150
Node 104
Key 152
Key Management service 106
Encrypt message with Key 150 110
Transmit message and version identifier V1 of Key 150 112
Receive message and version identifier V1 114
Compare version identifier V1 to version identifier V2 of stored Key 152 116
Determine that Key 150 is outdated based on the comparing 202
Generate outdated key notification 204
Transmit outdated key notification 206
Receive outdated key notification 208
Perform key mismatch resolution 210
Generate key request based on key mismatch resolution permitting key request 212
Transmit key request 214
Receive key request 216
Transmit Update to Key 150 218
Receive Update to Key 150 220
Update Key 150 222

FIG. 2B

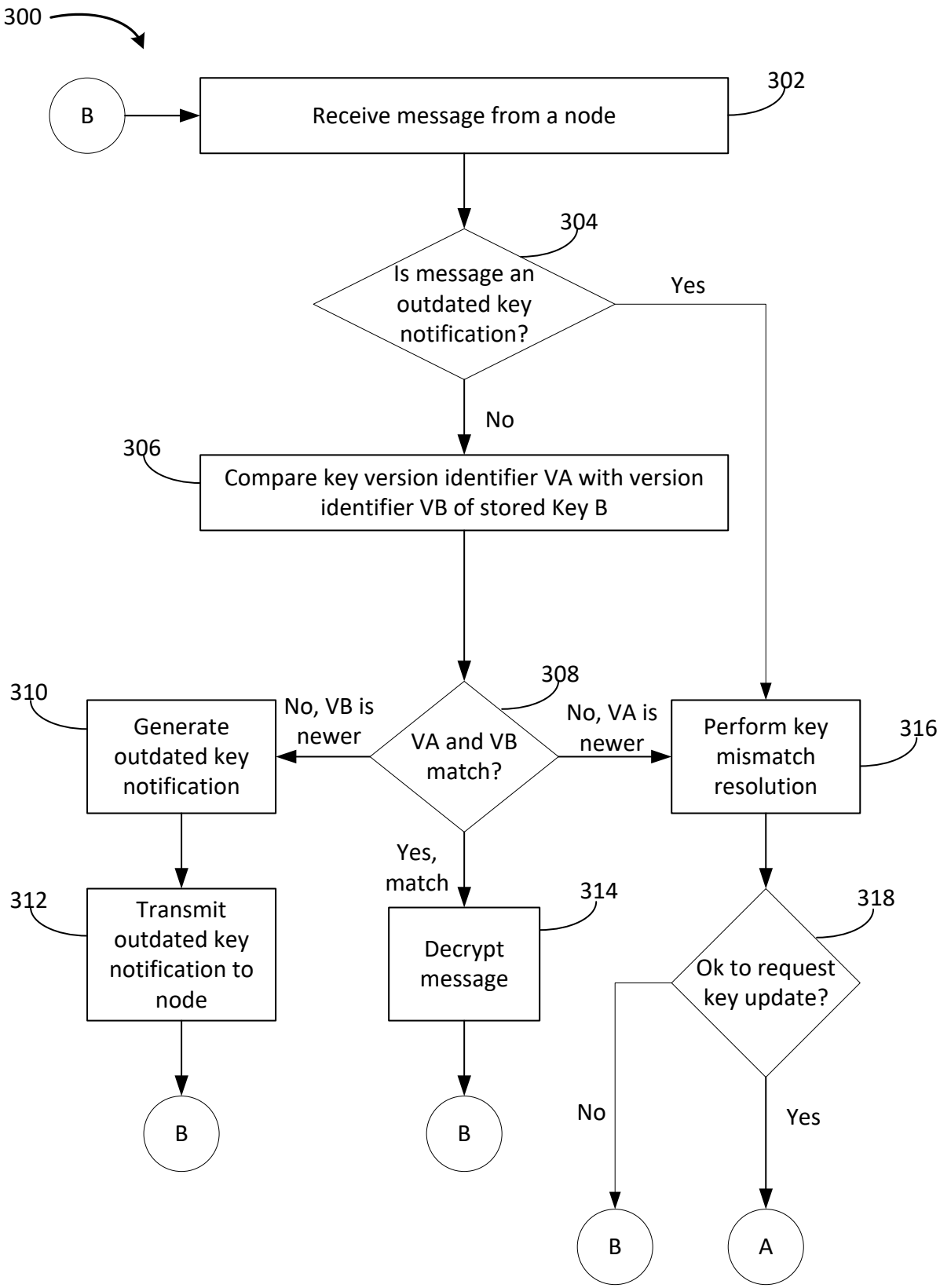
300
B
Receive message from a node
302
304
Is message an outdated key notification?
Yes
No
306
Compare key version identifier VA with version identifier VB of stored Key B
308
VA and VB match?
No, VB is newer
No, VA is newer
310
Generate outdated key notification
316
Perform key mismatch resolution
Yes, match
312
Transmit outdated key notification to node
314
Decrypt message
318
Ok to request key update?
No
Yes
B
B
B
A

FIG. 3A

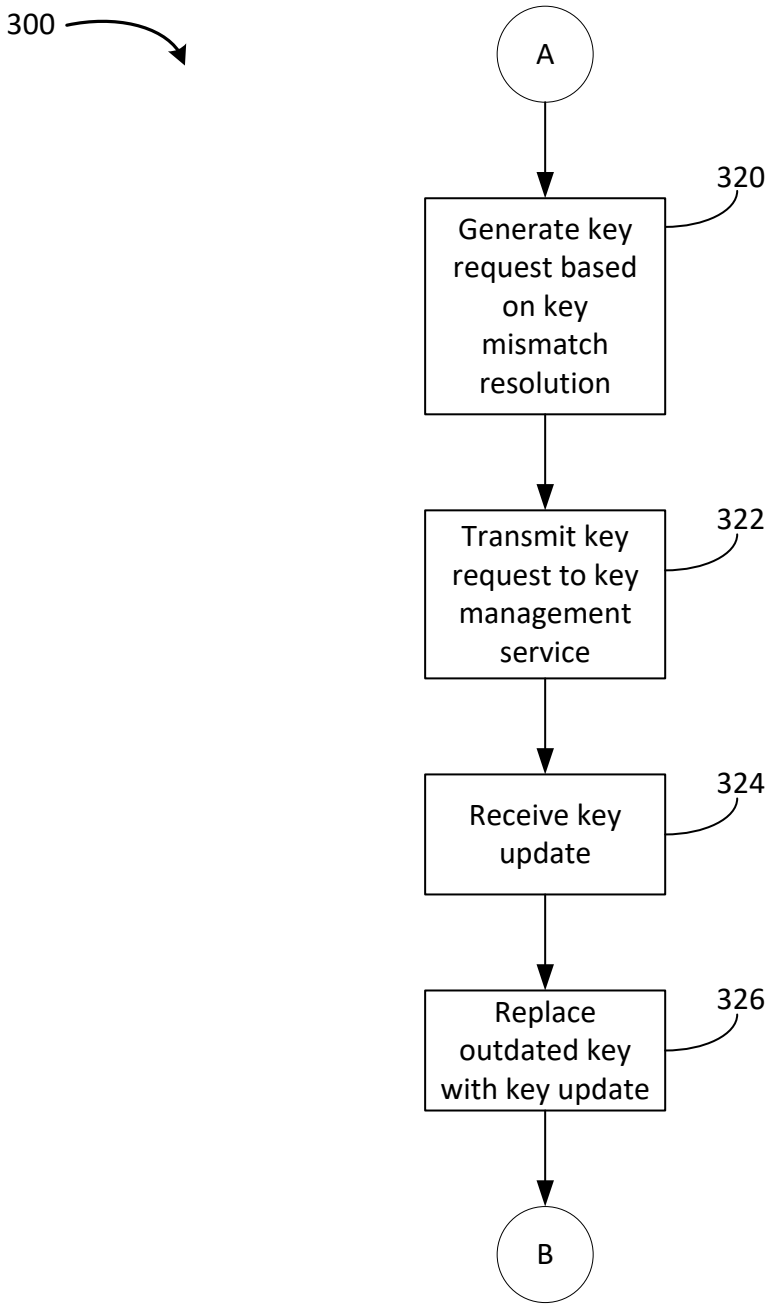
300
A
320
Generate key request based on key mismatch resolution
322
Transmit key request to key management service
324
Receive key update
326
Replace outdated key with key update
B

FIG. 3B

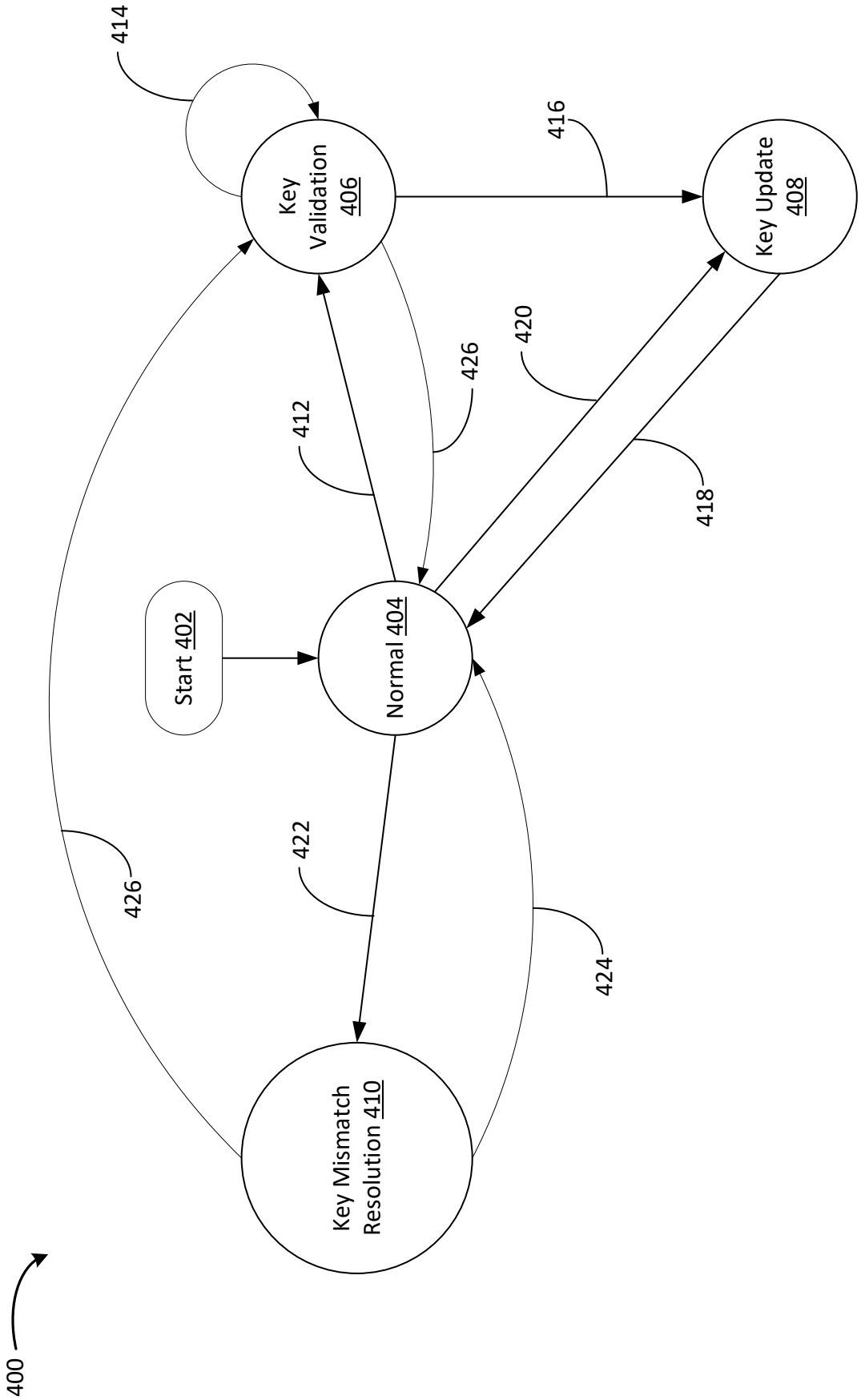
400
414
Key Validation 406
416
Key Update 408
426
420
412
418
Start 402
Normal 404
422
426
424
Key Mismatch Resolution 410

FIG. 4

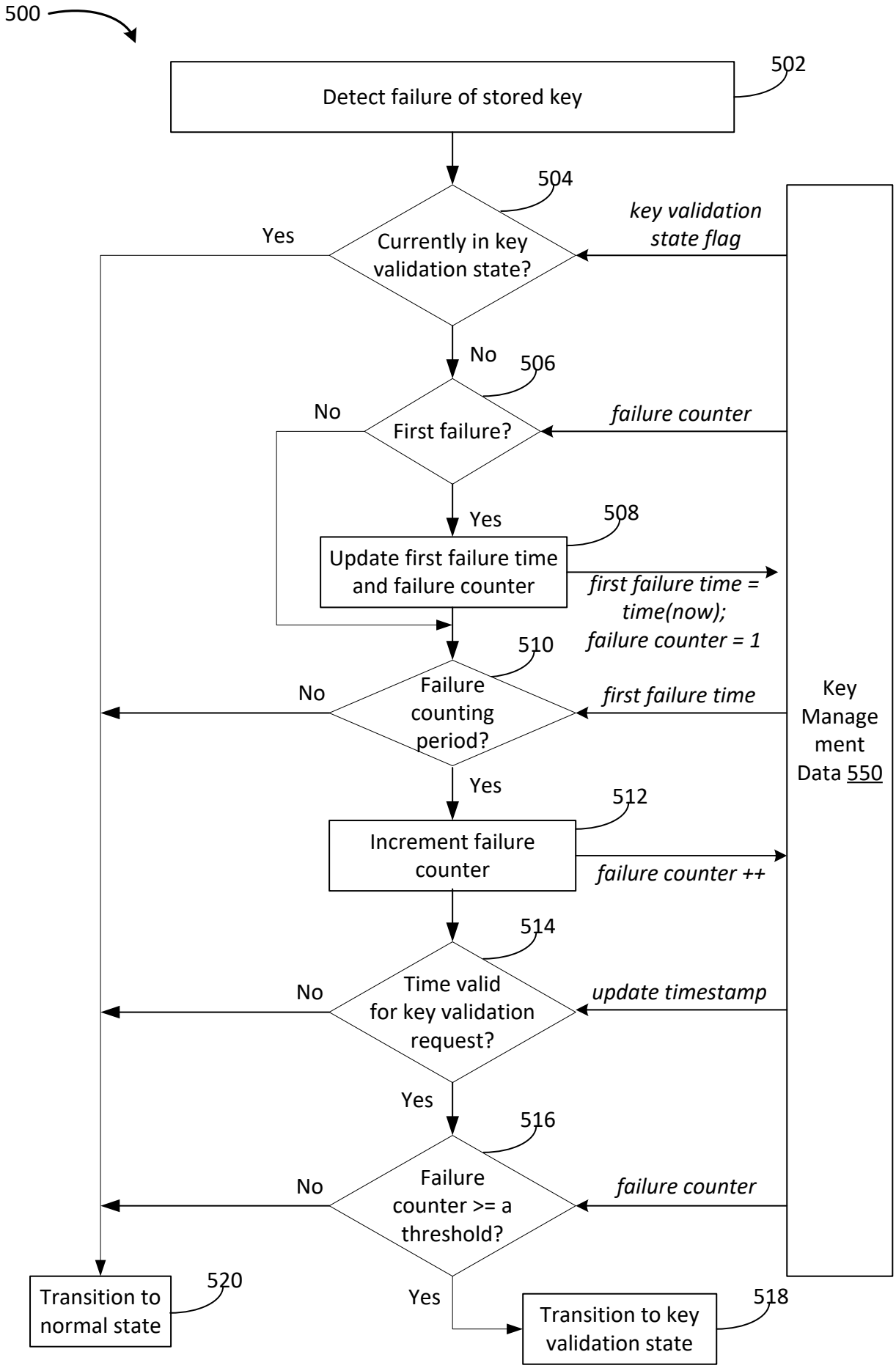
500
Detect failure of stored key
502
504
Currently in key validation state?
Yes
key validation state flag
No
506
First failure?
No
failure counter
Yes
508
Update first failure time and failure counter
first failure time = time(now); failure counter = 1
510
Failure counting period?
No
first failure time
Yes
512
Increment failure counter
failure counter ++
514
Time valid for key validation request?
No
update timestamp
Yes
516
Failure counter >= a threshold?
No
failure counter
Yes
Transition to normal state
520
Transition to key validation state
518
Key Management Data 550

FIG. 5

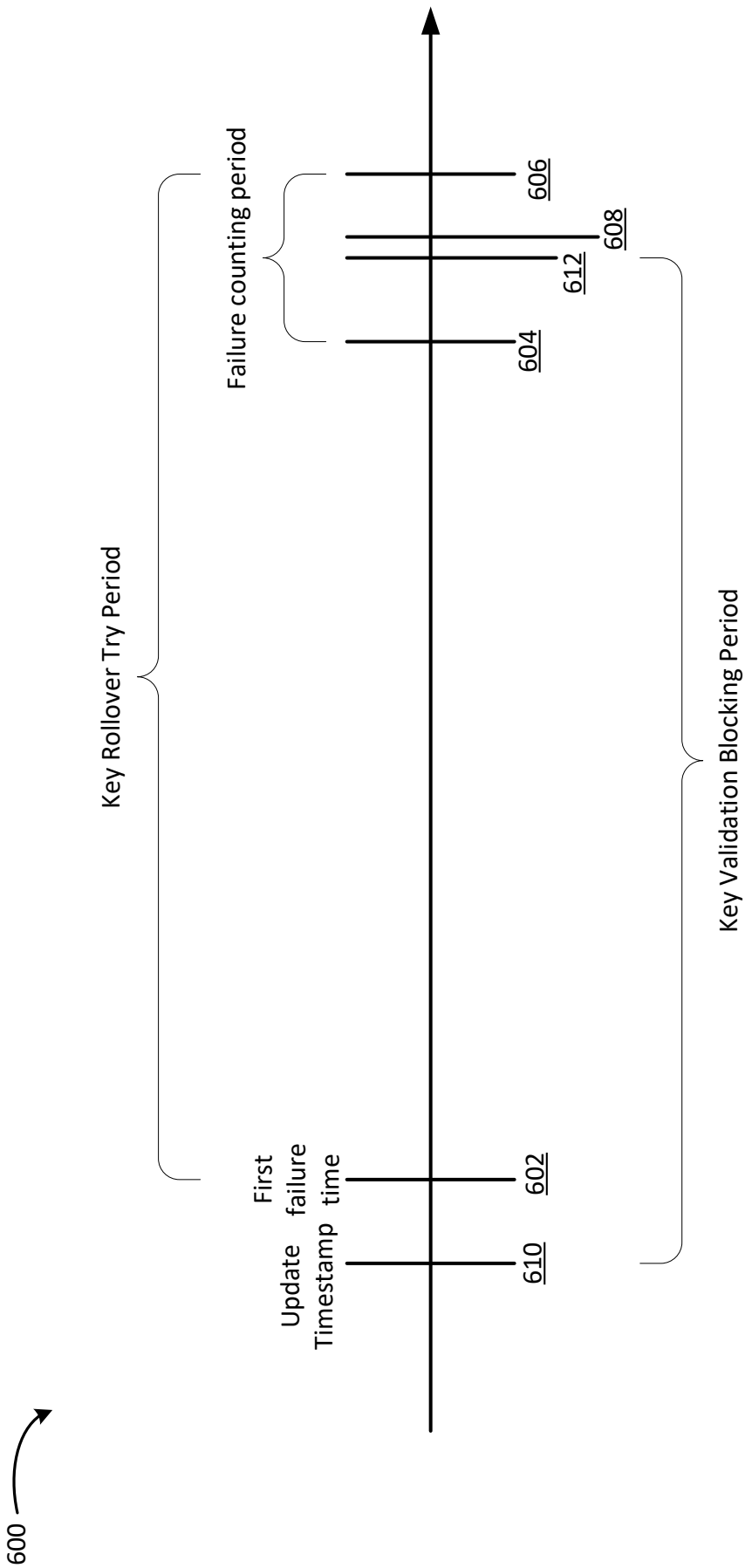
600
Key Rollover Try Period
Failure counting period
Key Validation Blocking Period
606
608
612
604
First failure time
602
Update Timestamp
610

FIG. 6

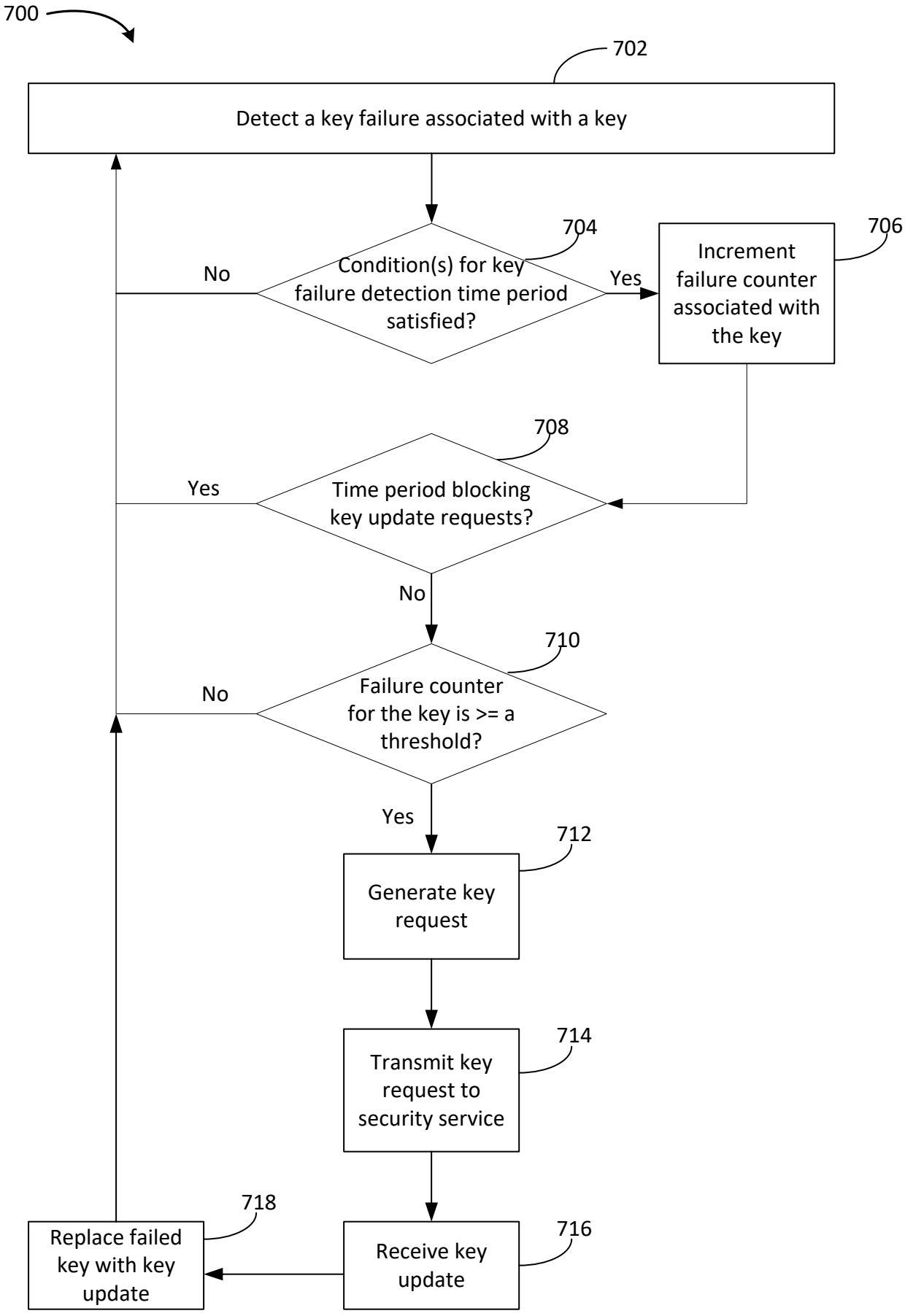
700
702
Detect a key failure associated with a key
704
Condition(s) for key failure detection time period satisfied?
No
Yes
706
Increment failure counter associated with the key
708
Time period blocking key update requests?
Yes
No
710
Failure counter for the key is >= a threshold?
No
Yes
712
Generate key request
714
Transmit key request to security service
716
Receive key update
718
Replace failed key with key update

FIG. 7

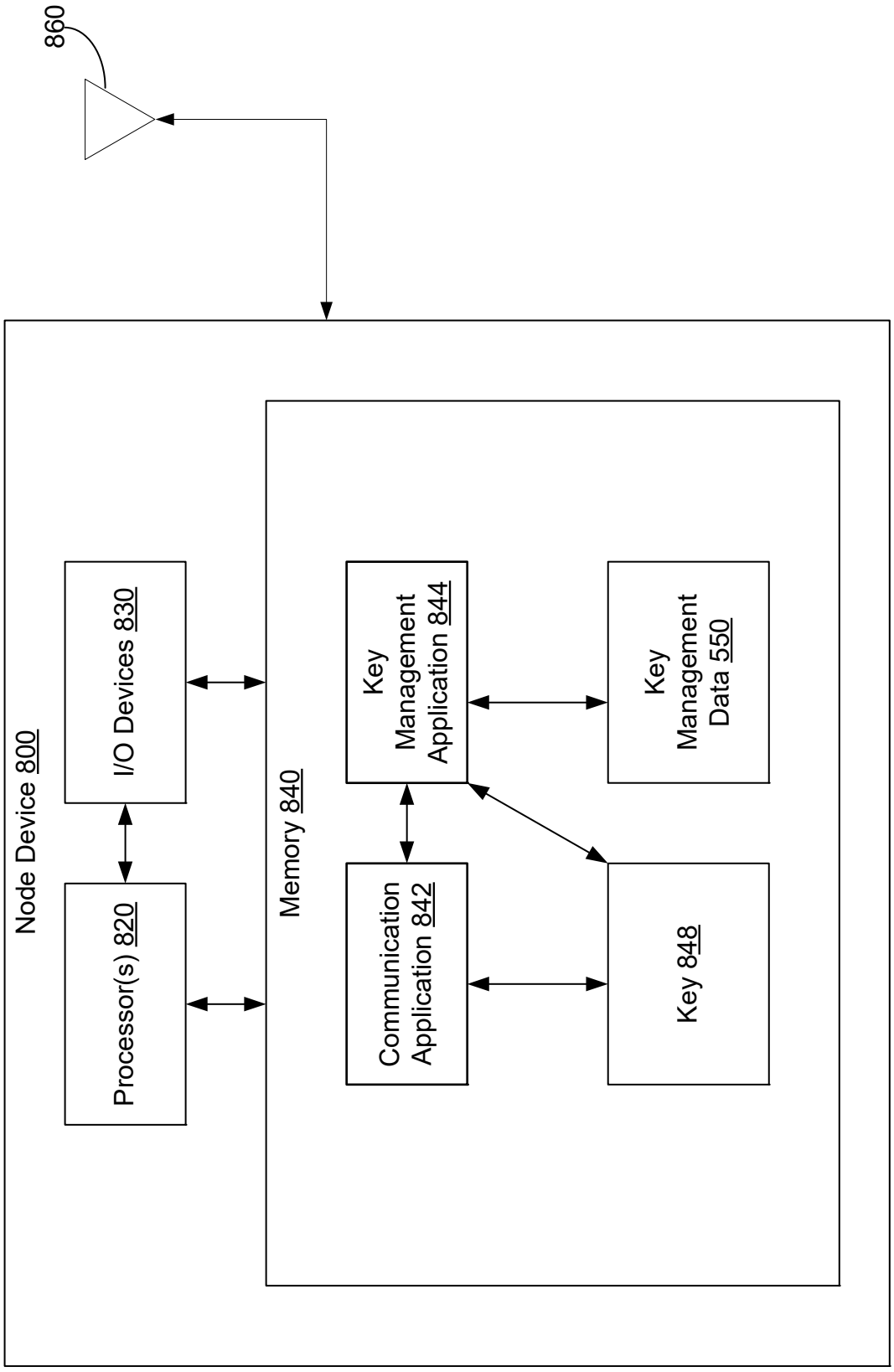
860
Node Device 800
I/O Devices 830
Processor(s) 820
Memory 840
Key Management Application 844
Key Management Data 550
Communication Application 842
Key 848

FIG. 8

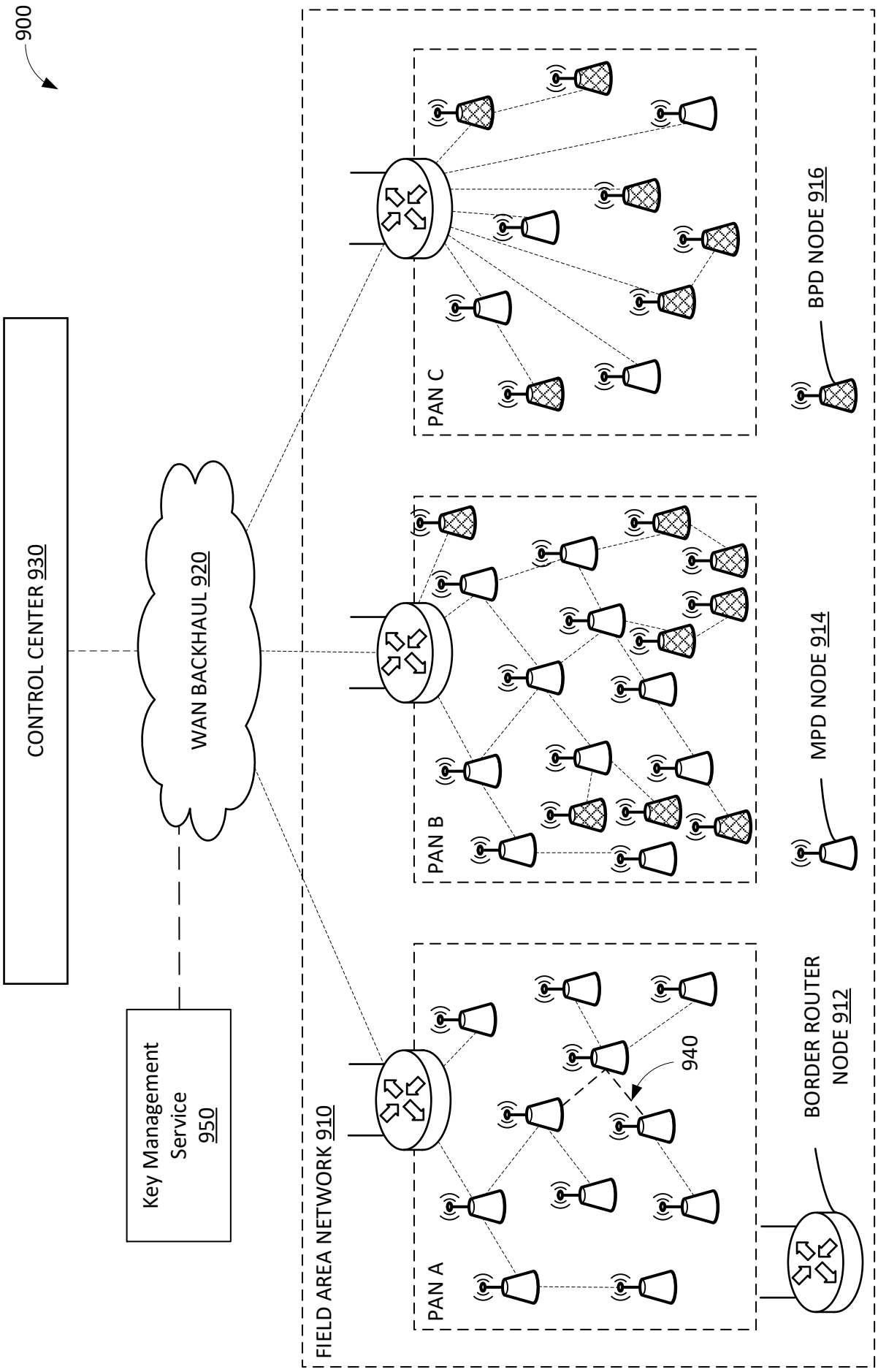
900
CONTROL CENTER 930
WAN BACKHAUL 920
Key Management Service 950
FIELD AREA NETWORK 910
PAN A
PAN B
PAN C
940
BORDER ROUTER NODE 912
MPD NODE 914
BPD NODE 916

FIG. 9