

WHAT IS CLAIMED IS:

1. A method comprising:
while in a key failure detection time period associated with a first key, detecting,
by a node in a mesh network, a decryption failure using the first key;
in response to detecting the decryption failure using the first key, entering, by the
node, a key validating blocking period starting from a time of the
decryption failure using the first key;
incrementing, by the node, a failure count for the first key;
determining, by the node, that the key validating blocking period has elapsed and
a key update time period has been entered; and
in response to determining that the failure count is at least a threshold count and
a key update time period has been entered, transmitting, by the node to a
key management service, a request for an update to the first key.
2. The method of claim 1, wherein the key failure detection time period begins a set
time period after a first failure associated with the first key has been detected.
3. The method of claim 2, wherein a time of the first failure associated with the first
key comprises a time when the first failure is detected while the failure count is zero.
4. The method of claim 1, further comprising, in response to receiving the first key,
resetting, by the node, the failure count to zero.
5. The method of claim 1, wherein the determining that the key validating blocking
period has elapsed and the key update time period has been entered occurs after
receiving, by the node, the first key.
6. The method of claim 1, wherein detecting the decryption failure using the first key
comprises determining that the first key is outdated based on a comparison of a version
identifier of the first key with a version identifier of a second key, wherein the second

key is used to encrypt a message received by the node.

7. The method of claim 1, wherein detecting the decryption failure using the first key comprises determining that the first key is outdated based on an outdated key notification received by the node from a second node.

8. The method of claim 1, further comprising:
receiving, by the node and responsive to the request for the update to the first key, an update to the first key;
replacing, by the node, the first key with the update to the first key; and
based on the update to the first key, resetting, by the node, the failure count to zero.

9. The method of claim 1, further comprising:
determining that a wait period has elapsed without a response to the request for the update to the first key; and
in response to determining that the wait period has elapsed without the response, transmitting a second request for the update to the first key.

10. One or more non-transitory computer-readable media storing instructions which, when executed by one or more processors of a node of a mesh network, cause the one or more processors to perform operations comprising:
determining that a failure counting period associated with a first key has been entered;
while in the failure counting period, identifying a failure associated with use of the first key;
in response to identifying the failure associated with use of the first key,
determining that a key validating blocking period has been entered,
wherein the key validating blocking period starts from a time of the failure;
updating a number of failures associated with the first key;
determining that the key validating blocking period has elapsed and a time period

for requesting updates to the first key has been entered; and
in response to determining that the number of failures associated with the first
key is equal to or greater than a minimum failure count and the time period
for requesting updates to the first key has been entered, transmitting, to a
key management service, a key validation request for the first key.

11. The one or more non-transitory computer-readable media of claim 10, wherein
the failure counting period comprises a set time period before an end of a key rollover
try period, the key rollover try period starting from a time of a first failure associated with
use of the first key.

12. The one or more non-transitory computer-readable media of claim 11, wherein
the time of the first failure associated with use of the first key comprises a time when the
first failure is identified while the number of failures associated with the first key is zero.

13. The one or more non-transitory computer-readable media of claim 12, wherein
the operations further comprise, setting the number of failures associated with the first
key to zero at an update timestamp associated with the first key.

14. The one or more non-transitory computer-readable media of claim 10, wherein
identifying the failure associated with use of the first key comprises determining that the
first key is outdated based on a comparison of a version identifier of the first key with a
version identifier of a second key used to encrypt a message received by the node.

15. The one or more non-transitory computer-readable media of claim 10, wherein
identifying the failure associated with use of the first key comprises receiving an
outdated key notification associated with the first key from a second node.

16. A node device in a wireless mesh network, comprising:
one or more processors; and
memory storing instructions that, when executed by the one or more processors,

cause the one or more processors to:
while in a key failure detection time period associated with a first key,
detecting a failure associated with the first key;
based on the detected failure associated with the first key,
entering a key validating blocking period starting from a time of the
detected failure associated with the first key;
incrementing a failure count for the first key;
determining that the key validating blocking period has elapsed and a key
update time period has been entered; and
based on a determination that the failure count is at least a minimum
failure count and a current time permits requesting updates to the
first key, transmitting to a key management service, a key update
request for the first key.

17. The node device of claim 16, wherein a start of the key failure detection time period is set based on a time of a first failure associated with the first key.

18. The node device of claim 16, wherein detecting the failure associated with the first key comprises:

determining that the first key is outdated based on a comparison of a version identifier of the first key with a version identifier of a second key used to encrypt a first communication received by the node device; or
receiving an outdated key notification from a second node device in response to transmitting a second communication encrypted using the first key to the second node device; or
failing to decrypt a third communication using the first key.