WHAT IS CLAIMED IS:

1. A computer-implemented method of transmitting messages within a mesh network, the method comprising:

receiving at a first node included within the mesh network a network message that is to be broadcast within the mesh network;

determining a security key type based on at least one of a resource parameter associated with at least one neighbor node included in the mesh network or an attribute of the network message;

securing the network message with a security key of the security key type to generate n secured network message; and

broadcasting the secured network message to one or more other nodes included in the mesh network that are directly connected to the first node.

2. The computer-implemented method of claim 1, wherein the security key is stored at the first node.

3. The computer-implemented method of claim 1, wherein the security key type is one of an asymmetric encryption key, a symmetric encryption key, an asymmetric authentication key, or a symmetric encryption key.

4. The computer-implemented method of claim 1, wherein broadcasting the secured network message to the one or more other nodes included in the mesh network comprises broadcasting the network message to a second node included in the mesh network that is not directly connected to the first node.

5. The computer-implemented method of claim 1, wherein the resource parameter associated with the at least one node comprises at least one of a computational cost of encrypting the network message at the first node, an amount of time needed for the first node to encrypt the network message, an amount of memory used to encrypt the network message at the first node, an amount of power used to encrypt the network message at the first node, or an indication of an amount of power remaining at the first

node.

6. The computer-implemented method of claim 1, wherein the resource parameter associated with the at least one node comprises at least one of a number of resource-limited nodes that are directly connected to the first node or an indication of the availability of an asymmetric encryption key at the first node.

7. The computer-implemented method of claim 1, wherein the one or more other nodes include at least a second node, and further comprising:

determining from the network message that a trust level associated with the second node has changed from a first trust level to a second trust level; and

in response, broadcasting a new network message to a third node included in the mesh network , wherein the new network message indicates that the second node has changed from the first trust level to the second trust level.

8. The computer-implemented method of claim 7, wherein the second trust level comprises a higher trust level than the first trust level.

9. The computer-implemented method of claim 1, wherein the attribute of the network message comprises at least one of a trust level associated with the network message or a forwarding status associated with the network message.

10. The computer-implemented method of claim 9, wherein the trust level associated with the network message comprises one of a manufacturing trust level, a vendor trust level, or a customer trust level.

11. A non-transitory computer-readable storage medium including instructions that, when executed by one or more processors, configure the one or more processors to perform the steps of:

receiving at a first node included within a mesh network a network message that is to be broadcast within the mesh network;

determining a security key type based on at least one of a resource parameter associated with at least one neighbor node included in the mesh network or an attribute of the network message;

securing the network message with a security key of the security key type to generate a secured network message, and

broadcasting the secured network message to one or more other nodes included in the mesh network that are directly connected to the first node.

12. The non-transitory computer-readable storage medium of claim 11, wherein the security key type is one of an asymmetric encryption key, a symmetric encryption key, an asymmetric authentication key, or a symmetric encryption key.

13. The non-transitory computer-readable storage medium of claim 11, wherein broadcasting the secured network message to the one or more other nodes included in the mesh network comprises broadcasting the network message to a second node included in the mesh network that is not directly connected to the first node.

14. The non-transitory computer-readable storage medium of claim 11, wherein the resource parameter associated with the at least one node comprises at least one of a computational cost of encrypting the network message at the first node, an amount of time needed for the first node to encrypt the network message, an amount of memory used to encrypt the network message at the first node, an amount of power used to encrypt the network message at the first node, or an indication of an amount of power remaining at the first node.

15. The non-transitory computer-readable storage medium of claim 11, wherein the resource parameter associated with the at least one node comprises at least one of a number of resource-limited nodes that are directly connected to the first node or an indication of the availability of an asymmetric encryption key at the first node.

16. The non-transitory computer-readable storage medium of claim 11, wherein the one or more other nodes include at least a second node, and further comprising instructions that, when executed by one or more processors, configure the one or more processors to perform the steps of:

determining from the network message that a trust level associated with the second node has changed from a first trust level to a second trust level; and

in response, broadcasting a new network message to a third node included in the mesh network , wherein the new network message indicates that the second node has changed from the first trust level to the second trust level.

17. The non-transitory computer-readable storage medium of claim 16, wherein the second trust level comprises a higher trust level than the first trust level.

18. The non-transitory computer-readable storage medium of claim 1, wherein the attribute of the network message comprises at least one of a trust level associated with the network message or a forwarding status associated with the network message.

19. The non-transitory computer-readable storage medium of claim18, wherein the trust level associated with the network message comprises one of a manufacturing trust level, a vendor trust level, or a customer trust level.

20. A system, comprising:

a processor; and

a memory storing instructions that, when executed by the processor, cause the processor to perform the steps of:

receiving at a first node included within the mesh network a network message that is to be broadcast within the mesh network;

determining an encryption key type based on at least one of a resource

parameter associated with at least one neighbor node included in the mesh network or an attribute of the network message;

encrypting the network message with an encryption key of the encryption key type to generate an encrypted network message; and

broadcasting the encrypted network message to one or more other nodes included in the mesh network that are directly connected to the first node.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, at a first node included within a mesh network, a network message that is to be broadcast within the mesh network;

determining, at the first node, a security key type based on at least one of a resource usage parameter associated with at least one neighbor node included in the mesh network or a resource usage parameter associated with the first node;

securing, at the first node, the network message with a security key of the security key type to generate a secured network message; and

broadcasting, at the first node, the secured network message to one or more other nodes included in the mesh network that are directly connected to the first node;

wherein the resource usage parameter associated with the at least one neighbor node comprises at least one of an amount of memory used to decrypt the network message at the at least one neighbor node, an amount of power used to decrypt the network message at the at least one neighbor node, or an indication of an amount of power remaining at the at least one neighbor node; and

wherein the resource usage parameter associated with the first node comprises at least one of an amount of memory used to encrypt the network message at the first node, an amount of power used to encrypt the network message at the first node, or an indication of an amount of power remaining at the first node.

2. The method of claim 1, wherein the security key is stored at the first node.

3. The method of claim 1, wherein the security key type is one of an asymmetric encryption key, a symmetric encryption key, an asymmetric authentication key, or a symmetric authentication key.

4. The method of claim 1, wherein broadcasting the secured network message to the one or more other nodes included in the mesh network comprises broadcasting the network message to a second node included in the mesh network that is not directly connected to the first node.

5. The method of claim 1, wherein the resource usage parameter associated with the first node further comprises at least one of a number of resource-limited nodes that are directly connected to the first node or an indication of an availability of an asymmetric encryption key at the first node.

6. The method of claim 1, wherein the one or more other nodes include at least a second node, and further comprising:

determining from the network message that a trust level associated with the second node has changed from a first trust level to a second trust level; and

in response, broadcasting a new network message to a third node included in the mesh network, wherein the new network message indicates that the second node has changed from the first trust level to the second trust level.

7. The method of claim 6, wherein the second trust level comprises a higher trust level than the first trust level.

8. The method of claim 1, wherein determining the security key type is further based on at least one of a trust level associated with the network message or a forwarding status associated with the network message.

9. The method of claim 8, wherein the trust level associated with the network message comprises one of a manufacturing trust level, a vendor trust level, or a customer trust level.

10. A non-transitory computer-readable storage medium including instructions that, when executed by one or more processors, configure the one or more processors to perform the steps of:

receiving, at a first node included within a mesh network, a network message that is to be broadcast within the mesh network;

determining, at the first node, a security key type based on at least one of a resource usage parameter associated with at least one neighbor node included in the mesh network or a resource usage parameter associated with the first node;

securing, at the first node, the network message with a security key of the security key type to generate a secured network message; and

broadcasting, at the first node, the secured network message to one or more other nodes included in the mesh network that are directly connected to the first node;

wherein the resource usage parameter associated with the at least one neighbor node comprises at least one of an amount of memory used to decrypt the network message at the at least one neighbor node, an amount of power used to decrypt the network message at the at least one neighbor node, or an indication of an amount of power remaining at the at least one neighbor node; and

wherein the resource usage parameter associated with the first node comprises at least one of an amount of memory used to encrypt the network message at the first node, an amount of power used to encrypt the network message at the first node, or an indication of an amount of power remaining at the first node.

11. The non-transitory computer-readable storage medium of claim 10, wherein the security key type is one of an asymmetric encryption key, a symmetric encryption key, an asymmetric authentication key, or a symmetric authentication key.

12. The non-transitory computer-readable storage medium of claim 10, wherein broadcasting the secured network message to the one or more other nodes included in

the mesh network comprises broadcasting the network message to a second node included in the mesh network that is not directly connected to the first node.

13. The non-transitory computer-readable storage medium of claim 10, wherein the resource usage parameter associated with the first node further comprises at least one of a number of resource-limited nodes that are directly connected to the first node or an indication of an availability of an asymmetric encryption key at the first node.

14. The non-transitory computer-readable storage medium of claim 10, wherein the one or more other nodes include at least a second node, and further comprising instructions that, when executed by one or more processors, configure the one or more processors to perform the steps of:

determining from the network message that a trust level associated with the second node has changed from a first trust level to a second trust level; and

in response, broadcasting a new network message to a third node included in the mesh network, wherein the new network message indicates that the second node has changed from the first trust level to the second trust level.

15. The non-transitory computer-readable storage medium of claim 14, wherein the second trust level comprises a higher trust level than the first trust level.

16. The non-transitory computer-readable storage medium of claim 10, wherein determining the security key type is further based on at least one of a trust level associated with the network message or a forwarding status associated with the network message.

17. The non-transitory computer-readable storage medium of claim 16, wherein the trust level associated with the network message comprises one of a manufacturing trust level, a vendor trust level, or a customer trust level.

18. A system, comprising:

a processor; and

a memory storing instructions that, when executed by the processor, cause the processor to perform the steps of:

receiving, at a first node included within a mesh network, a network message that is to be broadcast within the mesh network;

determining, at the first node, an encryption key type based on at least one of a resource usage parameter associated with at least one neighbor node included in the mesh network or a resource usage parameter associated with the first node;

encrypting, at the first node, the network message with an encryption key of the encryption key type to generate an encrypted network message; and

broadcasting, at the first node, the encrypted network message to one or more other nodes included in the mesh network that are directly connected to the first node;

wherein the resource usage parameter associated with the at least one neighbor node comprises at least one of an amount of memory used to decrypt the network message at the at least one neighbor node, an amount of power used to decrypt the network message at the at least one neighbor node, or an indication of an amount of power remaining at the at least one neighbor node; and

wherein the resource usage parameter associated with the first node comprises at least one of an amount of memory used to encrypt the network message at the first node, an amount of power used to encrypt the network message at the first node, or an indication of an amount of power remaining at the first node.