

Claims:

1. A method of establishing a secured ad-hoc network for a plurality of Internet of Things (IoT) nodes comprising:

- 5 determining at least four trusted IoT nodes;
- assigning a master node among the at least four trusted IoT nodes based on information from a security planning template;
- selecting, by the master node, three IoT nodes from the at least four trusted IoT nodes;
- 10 generating, by the master node, instructions comprising a sequence of actions for each of the three selected IoT nodes;
- transmitting the instructions to each of the three IoT nodes;
- in response to receiving a stream from one of the at least three trusted IoT nodes, the master node generates a master key with an expiry time; and
- 15 distributing the master key and the expiry time to each of the at least four trusted IoT nodes, wherein the step of generating, by the master node, instructions comprising the sequence of actions for each of the three IoT nodes comprises:
- retrieving a master key information from the security planning template; and
- generating instructions based on the information provided in the master key
- 20 information.

2. The method according to claim 1 wherein the step of determining the at least four trusted IoT nodes comprises:

- determining an application layer of each of the plurality of IoT nodes; and
- 25 clustering the IoT nodes with the same application layer as trusted IoT nodes.

3. The method according to claim 1 wherein the step of determining the at least four trusted IoT nodes comprises:

determining a network layer of each of the plurality of IoT nodes; and

clustering the IoT nodes with the same network layer as trusted IoT nodes.

5

4. The method according to claim 1 wherein the step of determining the at least four trusted IoT nodes comprises:

determining a system layer of each of the plurality of IoT nodes; and

clustering the IoT nodes with the same system layer as trusted IoT nodes.

10

5. The method according to claim 1 wherein the step of determining the at least four trusted IoT nodes comprises:

determining an identification data of each of the plurality of IoT nodes; and

clustering the IoT nodes with the same identification data as trusted IoT nodes.

15

6. The method according to any one of claims 2-5 wherein the step of determining the at least four trusted IoT nodes further comprises:

updating a trusted IoT nodes list to include the clustered IoT nodes;

determining if a valid master key is available; and

20

in response to determining a valid master key is available, transmitting the valid master key to trusted IoT nodes that are newly added to the trusted IoT nodes list.

7. The method according to claim 1 wherein the step of assigning the master node among the trusted IoT nodes comprises:

25

retrieving information on the conditions to qualify as master node from security planning template; and

determining the condition to qualify as master node from the security planning template.

8. The method according to claim 7 wherein the step of assigning the master node among the trusted IoT nodes further comprises:

in response to condition to qualify as master node being processor power, determining the processor power of each of the trusted IoT nodes; and

assigning one of the trusted IoT nodes with the highest processor power among the trusted nodes as the master node.

9. The method according to claim 7 wherein the step of assigning the master node among the trusted IoT nodes further comprises:

in response to condition to qualify as master node being battery power determining the battery power of each of the trusted IoT nodes; and

assigning one of the trusted IoT nodes with the highest battery power among the trusted nodes as the master node.

10. The method according to claim 7 wherein the step of assigning the master node among the trusted IoT nodes further comprises:

in response to condition to qualify as master node being highest interconnectivity among the trusted nodes, determining the network topology of the trusted IoT nodes; and

assigning one of the trusted IoT nodes with the highest interconnectivity among the trusted nodes as the master node.

11. The method according to claim 1 wherein the instructions based on the information provided in the master key information comprises:

assigning a first of the three IoT nodes to generate a first portion of a key structure;

assigning a second of the three IoT nodes to generate a second portion of the key structure; and

assigning a third of the three IoT nodes to receive the first and second portions of the key structure, generate a stream comprising the first and second portions of the key structure and dummies, and transmit the stream to the master node.

12. A system for establishing a secured ad-hoc network for a plurality of Internet of Things (IoT) nodes comprising:

a processing unit comprising a processor and a memory; and

instructions stored on the memory executable by the processor to:

determining at least four trusted IoT nodes,

assigning a master node among the at least four trusted IoT nodes based on information from a security planning template,

selecting, by the master node, three IoT nodes from the at least four trusted IoT nodes,

generating, by the master node, instructions comprising a sequence of actions for each of the three selected IoT nodes,

transmitting the instructions to each of the three IoT nodes,

in response to receiving a stream from one of the at least three trusted IoT nodes, the master node generates a master key with an expiry time, and

distributing the master key and the expiry time to each of the at least four trusted IoT nodes, wherein the instruction to generating, by the master node, instructions comprising the sequence of actions for each of the three IoT nodes further comprises instructions to:

retrieving a master key information from the security planning template; and

generating instructions based on the information provided in the master key information.

13. The system according to claim 12 wherein the instruction to determining the at
5 least four trusted IoT nodes further comprises instructions to:

determining an application layer of each of the plurality of IoT nodes; and
clustering the IoT nodes with the same application layer as trusted IoT nodes.

14. The system according to claim 12 wherein the instruction to determining the at
10 least four trusted IoT nodes further comprises instructions to:

determining a network layer of each of the plurality of IoT nodes; and
clustering the IoT nodes with the same network layer as trusted IoT nodes.

15. The system according to claim 12 wherein the instruction to determining the at
15 least four trusted IoT nodes further comprises instructions to:

determining a system layer of each of the plurality of IoT nodes; and
clustering the IoT nodes with the same system layer as trusted IoT nodes.

16. The system according to claim 12 wherein the instruction to determining the at
20 least four trusted IoT nodes further comprises instructions to:

determining an identification data of each of the plurality of IoT nodes; and
clustering the IoT nodes with the same identification data as trusted IoT nodes.

17. The system according to any one of claims 13-16 wherein the instruction to
25 determining the at least four trusted IoT nodes further comprises instructions to:

updating a trusted IoT nodes list to include the clustered IoT nodes;
determining if a valid master key is available; and

in response to determining a valid master key is available, transmitting the valid master key to trusted IoT nodes that are newly added to the trusted IoT nodes list.

18. The system according to claim 12 wherein the instruction to assigning the master node among the trusted IoT nodes further comprises instructions to:

retrieving information on the conditions to qualify as master node from security planning template; and

determining the condition to qualify as master node from the security planning template.

19. The system according to claim 18 wherein the instruction to assigning the master node among the trusted IoT nodes further comprises instructions to:

in response to condition to qualify as master node being processor power, determining the processor power of each of the trusted IoT nodes; and

assigning one of the trusted IoT nodes with the highest processor power among the trusted nodes as the master node.

20. The system according to claim 18 wherein the instruction to assigning the master node among the trusted IoT nodes further comprises instructions to:

in response to condition to qualify as master node being battery power determining the battery power of each of the trusted IoT nodes; and

assigning one of the trusted IoT nodes with the highest battery power among the trusted nodes as the master node.

21. The system according to claim 18 wherein the instruction to assigning the master node among the trusted IoT nodes further comprises instructions to:

in response to condition to qualify as master node being highest interconnectivity among the trusted nodes, determining the network topology of the trusted IoT nodes; and

assigning one of the trusted IoT nodes with the highest interconnectivity among the trusted nodes as the master node.

5

22. The system according to claim 12 wherein the instructions based on the information provided in the master key information comprises:

assigning a first of the three IoT nodes to generate a first portion of a key structure;

assigning a second of the three IoT nodes to generate a second portion of the key

10 structure; and

assigning a third of the three IoT nodes to receive the first and second portions of the key structure, generate a stream comprising the first and second portions of the key structure and dummies, and transmit the stream to the master node.

15