

METHOD AND SYSTEM FOR COLLABORATIVE SECURITY KEY GENERATION FOR AD-HOC INTERNET OF THINGS (IOT) NODES

Field of the Invention

5 This invention relates to a system and a method for generating security key. Particularly, this invention relates to a system and a method for generating security key among a few Internet of Things (IoT) nodes on an ad-hoc basis. In more particular, this invention relates to a system and a method for generating security key collaboratively among a few trusted IoT nodes on an ad-hoc basis.

Prior Art

10 With the proliferation on the use of IoT devices, security of the IoT devices is increasingly becoming an important and critical challenge to solve. In an ad-hoc self-organising IoT network, various IoT nodes are connected to each other and transfer data
15 in a peer-to-peer configuration. In other words, data are transferred among IoT nodes without the need of a router or a network infrastructure. The IoT nodes, which can be wearable nodes, nodes attached to moving vehicles and objects, *etc.*, can be moving around and not necessary fixed at one location. In this case, the IoT nodes regularly connect and disconnect from the ad-hoc network. Hence, maintaining security for an ad-
20 hoc network can be even more challenging.

 Therefore, those skilled in the art are striving to provide an improved apparatus and method that improves the security of an ad-hoc self-organising network among IoT devices.

Summary of the Invention

The above and other problems are solved and an advance in the art is made by a system and method of generating a security key for an ad-hoc network for IoT devices in accordance with this invention. A first advantage of a system and method in accordance with this invention is that the system and method generates a secured master key based on information from a few IoT nodes. This ensures that the master key is secured. A second advantage of a system and method in accordance with this invention is that the system and method generates a master key based on collaboration among a number of trusted IoT devices. In particular, each trusted IoT device is assigned to execute only certain parts of the master key. Hence, the master key cannot be easily replicated by unknown IoT nodes. This further enhances the security of the master key. A third advantage of a system and method in accordance with this invention is that the system and method generates a secured master key with a validity period. This ensures that a new master key is generated after a specified period.

In accordance with an aspect of the invention, a method of establishing a secured ad-hoc network for a plurality of Internet of Things (IoT) nodes is provided in the following manner. The method determines at least four trusted IoT nodes; assigns a master node among the at least four trusted IoT nodes based on information from a security planning template; selects, by the master node, three IoT nodes from the at least four trusted IoT nodes; generates, by the master node, instructions comprising a sequence of actions for each of the three selected IoT nodes; transmits 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 distributes the master key and the expiry time to each of the at least four trusted IoT nodes.

In accordance with an embodiment of the invention, the step of determining the at least four trusted IoT nodes includes 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. In accordance with another embodiment of the invention, the step of determining the at least four trusted IoT nodes includes 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. In accordance with yet another embodiment of the invention, the step of determining the at least four trusted IoT nodes includes 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. In accordance with another embodiment of the invention, the step of determining the at least four trusted IoT nodes includes 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.

In accordance with an embodiment of the invention, the step of determining the at least four trusted IoT nodes further includes 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.

In accordance with an embodiment of the invention, the step of assigning the master node among the trusted IoT nodes includes 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.

In accordance with an embodiment of the invention, the step of assigning the master node among the trusted IoT nodes further includes 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. In accordance with another embodiment of the invention the step of assigning the master node among the trusted IoT nodes further includes in response to condition to qualify as master node being battery power determining the battery power of each of the trusted IoT nodes; and
5 assigning one of the trusted IoT nodes with the highest battery power among the trusted nodes as the master node. In accordance with yet another embodiment of the invention, the step of assigning the master node among the trusted IoT nodes further includes 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
10 one of the trusted IoT nodes with the highest interconnectivity among the trusted nodes as the master node.

In accordance with an embodiment of this invention, the step of generating, by the master node, instructions comprising the sequence of actions for each of the three IoT
15 nodes includes retrieving a master key information from the security planning template; and generating instructions based on the information provided in the master key information.

In accordance with an embodiment of this invention, the instructions based on the
20 information provided in the master key information include 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
25 transmit the stream to the master node.

In accordance with another aspect of the invention, a system of establishing a secured ad-hoc network for a plurality of Internet of Things (IoT) nodes is provided. The system performs the method as described above.

5

Brief Description of the Drawings

The above and other features and advantages in accordance with this invention are described in the following detailed description and are shown in the following drawings:

Figure 1 illustrating an ad-hoc network infrastructure for IoT devices;

10

Figure 2 illustrating a block diagram of components in a network interface;

Figure 3 illustrating a flow diagram of generating a master key in accordance with an embodiment of this invention;

Figure 4 illustrating a flow diagram of a process for determining trusted IoT nodes in accordance with an embodiment of this invention;

15

Figure 5 illustrating a flow diagram of a process for determining a master node in accordance with an embodiment of this invention;

Figure 6 illustrating a security key in accordance with an embodiment of this invention;

20

Figure 7 illustrating a flow diagram of a process for generating instructions to respective trusted IoT nodes to perform certain functions in accordance with an embodiment of this invention;

Figure 8 illustrating a timing diagram of the data flow among the four trusted IoT nodes to generate a security key in accordance with an embodiment of this invention;

25

Figure 9 illustrating another timing diagram of the data flow among the four trusted IoT nodes to generate a security key in accordance with another embodiment of this invention; and

Figure 10 illustrating a security planning template in accordance with an embodiment of this invention.

Detailed Description

5 This invention relates to a system and a method for generating security key. Particularly, this invention relates to a system and a method for generating security key among a few Internet of Things (IoT) nodes on an ad-hoc basis. In more particular, this invention relates to a system and a method for generating security key collaboratively among a few trusted IoT nodes on an ad-hoc basis.

10 It is envisioned that a system and a method in accordance with embodiments of this invention may be used for improving the security of an ad-hoc self-organising network among IoT devices. In particular, the system and method generates a security key based on collaboration among a number of IoT devices and hence, provides a higher level of security. In more particular, each trusted IoT device is assigned to execute only certain steps in generating the master/public security key. Hence, the master/public security key cannot be easily replicated by unknown IoT nodes.

Figure 1 illustrates an example of a network infrastructure of a cluster of five IoT nodes. As shown, Node 1 is communicatively connected to Nodes 2, 3 and 4; Node 2 is communicatively connected to Nodes 1 and 3; Node 3 is communicatively connected to Nodes 1, 2, 4 and 5; Node 4 is communicatively connected to Nodes 1, 3 and 5; and Node 5 is communicatively connected to Nodes 3 and 4. Typically in such network infrastructure, Node 3 would be identified as a host or an access point to connect the rest of the nodes. However, since IoT nodes are typically in motion, upon Node 3 moving out of the cluster, a new host has to be identified and repeat the process of connecting the rest of the available nodes.

In accordance with embodiments of this invention, the system and method does not require an IoT node to serve as an access point to connect to the rest of the IoT nodes. Instead, a public key would be generated and distributed among the trusted IoT nodes. Advantageously, should any of the IoT nodes leave the cluster, the rest of the IoT nodes would still be able to communicate among themselves with the public key. Further details of the invention will now be described as follows.

For the purpose of this discussion, the term “Internet of Things” (IoT) device or node refers to any apparatus having a communication interface to allow transferring and receiving of information among the IoT devices over a wired or wireless connection. IoT devices comprise, but not limited to, sensor devices, embedded systems, network-based cameras, gateways, mobile phones, computers, laptops, personal digital assistants (PDAs), white goods, appliances, etc.

For embedded systems, gateways, mobile phones, computers, laptops, PDAs, and mobile devices, such IoT nodes are typically equipped with wireless network interface (e.g. Bluetooth, Wi-Fi, Wi-Fi Direct, Long-Term Evolution (LTE) Direct, RF antenna, etc.) or wired network interface (e.g. an Ethernet connection, a USB or Firewire connection, etc.) to allow transferring and receiving of data.

For white goods such as fridge and washing machine, such appliances may not be equipped with any wired or wireless network interface. Hence, it is common that a network interface module be provided to allow such appliances to be communicatively connected to the Internet so that one is able to control the appliances. Figure 2 illustrates the block diagram of a basic network interface 200. The network interface 200 can

receive and transmit data, execute software applications. Network interface 200 comprises a processor 210, memory 220, transceiver 230 and input/output ports 240.

The processor 210 is a processor, microprocessor, microcontroller, application specific integrated circuit, digital signal processor (DSP), programmable logic circuit, or other data processing device that executes instructions to perform the processes in accordance with the present invention. The processor 210 has the capability to execute various applications that are stored in the memory 220.

The memory 220 may include read-only memory (ROM), random-access memory (RAM), electrically erasable programmable ROM (EEPROM), flash cards, or any memory commonly used for computers.

One or more input/output (I/O) ports 240 can be configured to allow the processor 210 to communicate with and control from various I/O devices for the IoT devices. Peripheral devices that may be connected to network interface 200 via the I/O ports 240 include a USB storage device, an SD card or other storage device for transmitting information to or receiving information from the network interface 200. In addition to updating applications stored on memory 220 or installing new applications onto the memory via the transceiver 230, a user may alternatively install new applications or update applications on the memory 220 through a user interface such as a USB via the I/O ports 240.

One skilled in the art will recognize that other features may be included in the network interface 200. Further, the components in network interface 200 may be replaced by other components that perform similar functions. In brief, the network interface 200 as shown in figure 2 is considered merely illustrative and non-limiting.

In accordance with embodiments of this invention, instructions executable by the processor of network interface 200 or typical network interface provided in IoT nodes are stored in respective memory. One skilled in the art will recognize that the instructions may be stored and/or performed as hardware, firmware, or software without departing from this invention. The instructions will now be described as follows.

A security planning template is pre-installed in the IoT nodes. The security planning template is pre-defined by users and may comprise 1) parameters to be considered a trusted IoT node; 2) attributes for assigning master node; and 3) sequence of actions for each of the nodes.

The security planning template allows a user to define the parameters to qualify IoT nodes as trusted. The parameters can be arbitrary or conditioned based on applications, services or business requirements of the IoT nodes. An example in qualifying an IoT node as a trusted node is as follows:

1. IoT node location is secured?
2. Wireless network security enabled?
3. IoT node owned by operator?
4. Security protection software available?

In the above example, the user can use an IoT gateway located in an enclosed physical area, WPAv2 enabled IoT nodes in the case of WiFi environment, IoT nodes owned by operator, IoT nodes with enhanced security features, etc. as trusted nodes.

A user may also use application(s) or/and operating environment parameters to limit a set of dynamic trusted IoT nodes. The parameters such as energy level of IoT node, distance among each trusted node, the nodes with higher memory and processing power, the nodes with mobility issues or with reliable location, etc. can be used as conditions to re-define a trusted IoT node, hence forming dynamic trusted nodes. Some of the parameters mentioned above may be used as attributes for determining a master node among the identified IoT nodes. Further details on the security planning template will be discussed below.

Figure 3 illustrates a flow diagram of process 300 performed by the processor in network interface 200 or typical network interfaces provided in IoT nodes in accordance with an embodiment of this invention. Process 300 begins with step 305 to determine a number of trusted IoT nodes using the information in the security planning template. Essentially, preferably at least 4 trusted nodes have to be determined. Further details pertaining to this step will be described below with reference to figure 4.

In step 310, process 300 assigns a master node based on certain pre-determined criteria as defined in the security planning template. Further details pertaining to this step will be described below with reference to figure 5.

In step 315, the master node generates a sequence of action for each of the trusted nodes based on the information in the security planning template. The sequence of action is then transmitted to the relevant trusted IoT nodes. Further details pertaining to this step will be described below with reference to figures 6 and 7.

In step 320, the master node receives a stream from one of the trusted nodes. With the stream, the master node generates a master key with an expiry time in step 325

and distributes the master key with the expiry time and a time stamp to each of the trusted nodes in step 330. The master key may be distributed by way of a broadcast to all the trusted IoT nodes in a trusted IoT nodes list. One skilled in the art will recognise that other types of distribution may be implemented without departing from the invention.

5 Process 300 ends after step 330.

Figure 4 illustrates a flow diagram of process 400 performed by the processor in network interface 200 or typical network interfaces provided in IoT nodes in accordance with an embodiment of this invention. Process 400 illustrates the process flow of the step
10 of determining trusted IoT nodes. Essentially, the IoT nodes are considered trusted IoT nodes if they contain the same parameters as set out in the security planning template. The parameters may be the application layer parameter, transport layer parameter, network layer parameter, link layer parameter, physical layer parameter, or ID layer parameter. For example, if the ID layer parameter of the first IoT node contains the same
15 information as the ID layer of the second, third and fourth IoT nodes, the first, second, third and fourth IoT nodes are considered as trusted IoT nodes since they belong to the same user.

For purposes of this discussion, the communication model employed by the
20 network interface 200 or typical network interfaces provided in IoT nodes in accordance with an embodiment of this invention may be based on Internet Protocol Suite (TCP/IP), Open Systems Interconnection (OSI), or any other known network models. Particular, there are multiple layers in the communication stack of the communication interface such as application layer, transport layer, network layer, link layer, physical layer, ID layer, etc.
25 Essentially, at least four IoT nodes need to be determined in order to begin the process of generating a master key. Briefly, the process determines, from the security planning

template, which layer in the communication stack of the communication interface is used, and clusters the IoT nodes having the same layer.

Process 400 begins with step 405 by retrieving and transmitting a parameter to
5 respective IoT nodes. The parameter to be retrieved is based on the parameter set out in the security planning template. One skilled in the art will recognise that more than one parameter may be retrieved and transmitted without departing from the invention.

In step 410, each of the IoT nodes receives parameter from respective IoT nodes
10 and compares the received parameter with its parameter in step 415. In step 420, each of the IoT nodes updates its trusted IoT nodes list to include the address of the IoT nodes having similar parameters. The trusted IoT nodes list has to include at least four IoT nodes in order to proceed further to step 425. Four trusted IoT nodes are required to generate a master key.

15 It is noted that a new master key is required to be generated only after the expiry of a current master key. Hence, in step 425, each of the IoT nodes determines whether a valid master key is available based on the information of the master key in the security planning template. Particularly, the IoT nodes check the valid period and the time stamp
20 against the current time. If a valid master key is available, process 400 proceeds to step 430. If a valid master key is not available, process 400 proceeds to step 310 in process 300 to continue with generating a master key.

In step 430, process 400 determines whether a new trusted IoT node has been
25 added. If no new trusted IoT node has been added, process 400 ends. If a new trusted IoT node has been added, the trusted IoT node proceeds to step 435 to transmit the master key and the expiry time to the newly added trusted IoT node.

Figure 5 illustrates a flow diagram of process 500 performed by the processor in network interface 200 or typical network interfaces provided in IoT nodes in accordance with an embodiment of this invention. Process 500 illustrates the process flow of the step of determining a master node among the trusted IoT nodes. This process is triggered only after at least four trusted IoT nodes are identified. Essentially, the master node is selected based on one or more IoT node attributes as set out in the security planning template such as processor power, battery power, memory size, and interconnectivity among the trusted IoT nodes.

Process 500 begins with step 505 by retrieving and transmitting attributes such as processor power, battery power, memory size, interconnectivity among the trusted IoT nodes. The attributes to retrieve are based on the information provided in the security planning template. Upon retrieving the relevant attributes, the trusted IoT nodes forward to the rest of the trusted IoT nodes in the trusted IoT nodes list.

In step 510, each of the IoT nodes receives attributes from respective IoT nodes. Process 500 then retrieve the conditions from security planning template to qualify as master node in step 515.

In step 520, each trusted IoT node would determine whether it is a master node by comparing the attribute with reference to the conditions from the security planning template. Assuming the condition is battery power, the IoT node compares the received attributes to determine which IoT node has the highest battery power value. If a specific IoT node has the highest batter power value, the IoT node is determined as the master node and proceeds with step 315 in process 300. If the IoT node is not a master node, process 500 ends.

Figure 6 illustrates a master key 600 generated by the master node. The master key 600 is valid for a period of time, T. Upon expiry of the master key 600, the process of 300 is repeated to generate a new master key 600 for the ad-hoc network among the trusted IoT nodes.

The master key 600 includes a key structure 610 having 4 cycles namely, C1-C4. One skilled in the art will recognise that other number of cycles may be used without departing from the invention.

Each cycle contains a sequence of security parameters and dummies. For example, the security parameters may be application layer, network layer, or physical layer. The key structure as shown in figure 6 comprises 4 cycles (C1-C4) with sequence being application parameter (A) and physical parameter (P), and dummies (D). One skilled in the art will recognise that the key structure 610 as shown in figure 6 is merely illustrative and other permutations may be implemented.

The key structure 610 is being chained sequentially to form a master key for a period of time, T. Essentially, the master key, K, can be expressed in the following manner:

$$K = (C, \text{Seq}, L) + T$$

Where C is the number of cycle, Seq is the sequence of security parameters and dummies, L is the length of the key structure, and T is the expiry time. This means that the master key 600 as shown in figure 6 can be expressed as $K = (4, A|P, L) + T$. The master key, K, information is stored in the security planning template.

Figure 7 illustrates a flow diagram of process 700 performed by the processor in network interface 200 or typical network interfaces provided in IoT nodes in accordance with an embodiment of this invention. Process 700 illustrates the process flow of the step performed by one of the trusted IoT nodes determined to be the master node to generate a sequence of action in accordance with the master key information stored on the security planning template. The security planning template also includes the sequence of action in order for the master node to generate the relevant instructions to the three IoT nodes.

Process 700 begins with step 705 by selecting 3 trusted IoT nodes from the trusted IoT node list. The 3 trusted IoT nodes may be randomly selected. Alternatively, the 3 trusted IoT nodes may be selected based on the attribute.

In step 710, process 700 assigns the roles of 3 trusted IoT nodes. Particularly, the first trusted IoT node is assigned to generate a first portion of the key structure, the second trusted IoT node is assigned to generate a second portion of the key structure, and the third trusted IoT node is assigned to generate a stream and as a backup master node.

In step 715, process 700 retrieves the master key information from the security planning template.

In step 720, process 700 reads the master key information and generates instructions to each of the selected 3 trusted IoT nodes. Assuming the master key information is $K = (4, A|P, L) + T$, the master node randomly assigns C1, C2, C3 and C4 to both first and second trusted IoT nodes and instructs the first and second trusted IoT nodes to transmit the cycles to the third trusted IoT node. The master node would also

inform the third trusted IoT node on the number of cycle and length so that the third trusted IoT node can insert the correct amount of dummies accordingly upon receiving the correct number of cycles from the relevant trusted IoT nodes. For illustrative purposes, the instructions may be generated as follows:

5

To first trusted IoT node: Generate C1, C3, A|P, Transmit address of third trusted IoT node

To second trusted IoT node: Generate C2, C4, A|P, Transmit address of third trusted IoT node

10

To third trusted IoT node: Receive C1-C4, L, Transmit address of master node

15

Where the first trusted IoT node is required to generate a first portion of the key structure namely, first and third cycles with the sequence being application parameter and physical parameter, and subsequently transmits first and third cycles to the third trusted IoT node; the second trusted IoT node is required to generate a second portion of the key structure namely, second and fourth cycles with the sequence being application parameter and physical parameter, and subsequently transmits second and fourth cycles to the third trusted IoT node; the third trusted IoT node is required to receive total of four cycles from trusted IoT nodes (that is not made known to the third trusted IoT node), arrange the cycles accordingly, insert dummies to fill in the length to form a stream, and subsequently transmit the stream to the master node. Further details on the sequence of action will be described below with reference to figure 8.

20

The above shows a set of instructions that may be generated by the master node.
One skilled in the art will recognise that alternative instructions may be generated without departing from the invention. An alternative set of instructions may be as follows:

25

To first trusted IoT node: Generate C1, C3, A|P; Transmit address of second trusted IoT node

To second trusted IoT node: Receive C1 and C3; Generate C2, C4, A|P; Transmit address of third trusted IoT node

5 To third trusted IoT node: Receive C1-C4; Generate C1-C4, L; Transmit address of master node

Where the first trusted IoT node is required to generate a first portion of the key structure namely, first and third cycles with the sequence being application parameter and physical parameter, and subsequently transmit first and third cycles to the second trusted
10 IoT node; the second trusted IoT node is required to receive first and third cycles, generate a second portion of the key structure namely, second and fourth cycles with the sequence being application parameter and physical parameter, and subsequently transmit first to fourth cycles to the third trusted IoT node; the third trusted IoT node is
15 required to receive total of four cycles from trusted IoT nodes (that is not made known to him), arrange the cycles accordingly, insert correct amount of dummies to fill in the length to form a stream, and subsequently transmit the stream to the master node.

One skilled in the art will recognise that the above illustrated sets of instructions
20 are two possible sequences of actions that may be implemented without departing from the invention.

In step 725, the instructions are transmitted to respective trusted IoT nodes. After step 725, process 700 returns to step 320 in process 300 and await for the stream from
25 the third trusted IoT node.

Figure 8 illustrates a timing diagram 800 of an embodiment of the flow of data among the 4 IoT trusted nodes, namely, master node, first trusted IoT node, second trusted IoT node, and third trusted IoT node. Particularly, figure 8 illustrates a timing diagram of the flow of data based on the set of instructions as illustrated in step 720 of process 700.

Timing diagram 800 begins with sequence 805 where master node transmits the instructions to respective first, second and third IoT nodes. Upon receipt of the instructions from the master node, the first, second and third IoT nodes proceed as follows:

- the first IoT node generates the first and third cycles based on the instructions received,
- the second IoT node generates the second and fourth cycles based on the instructions received, and
- the third IoT node monitors for C1-C4.

In sequence 810, the first IoT node transmits C1 and C3 to the third IoT node upon generating C1 and C3. At the same time or consecutively, the second IoT node transmits C2 and C4 to the third IoT node upon generating C2 and C4. Upon receipt of C1-C4, the third IoT node generates a stream.

In sequence 815, the third IoT node transmits the stream to the master node upon generating the stream. Upon receipt of the stream from the third IoT node, the master node generates a master key with an expiry time. Subsequently, the master node broadcasts the master key with the expiry time and the time stamp to all the trusted IoT nodes in the trusted IoT nodes list. Timing diagram ends after sequence 815.

Figure 9 illustrates a timing diagram 900 of an embodiment of the flow of data among the 4 IoT trusted nodes, namely, master node, first trusted IoT node, second trusted IoT node, and third trusted IoT node. Figure 9 illustrates a timing diagram of the flow of data of a sequence based on the alternative set of instructions as illustrated in
5 step 720 of process 700.

Timing diagram 900 begins with sequence 905 where master node transmits the instructions to respective first, second and third IoT nodes. Upon receipt of the instructions from the master node, the first, second and third IoT nodes proceed as
10 follows:

- the first IoT node generates C1 and C3 based on the instructions received,
- the second IoT node monitors for C1 and C3,
- the third IoT node monitors for C1-C4.

15 In sequence 910, the first IoT node transmits C1 and C3 to the second IoT node. In response to receiving C1 and C3, the second IoT node generates C2 and C4.

In sequence 915, the second IoT node transmits C1-C4 to the third IoT node. In response to receiving C1-C4, the third IoT node generates a stream.

20 In sequence 920, the third IoT node transmits the stream to the master node. Upon receipt of the stream from the third IoT node, the master node generates a master key with an expiry time and broadcasts the master key with the expiry time and the time stamp to all the trusted IoT nodes. Timing diagram ends after sequence 920.

25 Figure 10 illustrates an example of a security planning template 1000. The security planning template 1000 includes 1) Master Key; 2) Parameter for trusted IoT

nodes; 3) Attribute for master node; 4) Master key information; and 5) Trusted IoT nodes list.

The Master Key contains the master key, valid period and time stamp. The validity
5 of the master key is determined based on the valid period calculated from the time stamp.

The Parameter for trusted IoT nodes contains the parameter for determining IoT
nodes that are considered trusted. In this example, a primary parameter (i.e. Application
layer) and a secondary parameter (i.e. transport layer) are provided. The trusted IoT
10 nodes determined are updated to the Trusted IoT nodes list.

The Attribute for master node contains attribute for determining the master node.
In this example, a primary attribute (i.e. processor power) and a secondary attribute (i.e.
battery power) are provided. The secondary attribute may be used if more than one IoT
15 node are determined based on the primary attribute. The attribute may also be used by
the master node to determine the first, second and third IoT nodes for generating the
master key.

The Master Key information contains the master key, K, information and the
20 sequence of actions. In this example, the master key comprises 4 cycles with A|P
sequence and a length of 1 minute for a duration of 60 minutes. The instructions to be
generated are:

To first trusted IoT node: Generate C2, A|P; Transmit to third trusted IoT node
25 To second trusted IoT node: Generate C1, C3 and C4, A|P; Transmit to third
trusted IoT node

To third trusted IoT node: Receive C1-C4; Generate C1-C4, L; Transmit to master node

One skilled in the art will recognise that security planning template as shown in figure 10 is for illustrative purposes only and other details may be provided in the security planning template without departing from the invention.

The above is a description of exemplary embodiments of a system and method for generating a security key for an ad-hoc network for IoT devices in accordance with this invention. It is foreseeable that those skilled in the art can and will design alternative systems and methods based on this disclosure that infringe upon this invention as set forth in the following claims.

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.

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

- 20 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.

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

- 25 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.

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.

5

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.

10

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

15 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:

20 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.

25 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.

5

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

10 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:

15 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.

20 11. The method according to claim 1 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

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

12. The method according to claim 11 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

5 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.

10 13. 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,

15 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,

20 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

25 distributing the master key and the expiry time to each of the at least four trusted IoT nodes.

14. The system according to claim 13 wherein the instruction to determining the at 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.

5

15. The system according to claim 13 wherein the instruction to determining the at 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.

10

16. The system according to claim 13 wherein the instruction to determining the at 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.

15

17. The system according to claim 13 wherein the instruction to determining the at 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.

20

18. The system according to any one of claims 14-17 wherein the instruction to 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

25

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.

19. The system according to claim 1 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

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

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

10 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.

15 21. The system according to claim 19 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

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

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

25 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.

23. The system according to claim 13 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:

- 5 retrieving a master key information from the security planning template; and
- generating instructions based on the information provided in the master key information.

24. The system according to claim 23 wherein the instructions based on the
10 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
- 15 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.