

**METHOD AND SYSTEM FOR SECURED SERVICE-ORIENTED NODES
DISCOVERY AND ROUTE DETERMINATION IN MOBILE AD-HOC
NETWORK**

5

FIELD OF INVENTION

The present invention relates to a mobile network. More particularly, the present invention relates to a system and method of securing a mobile ad-hoc network.

BACKGROUND

10

Mobile Ad-hoc Network (MANET) is an autonomous network system of mobile routers and associated mobile hosts connected via wireless links - the union of which forms an arbitrary graph. The routers and hosts are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology changes rapidly and unpredictably.

15

Current technology and implementation focusing more on IP based MANET system only and use a complex and bulky routing protocol in route determination. There is no commercial MANET product known to-date and if have they will not have an integrated set of the security and application parameters being used in route determination.

20

In a wireless network, ad-hoc network particularly, data security is always a concern to eliminate unauthorized access and usage of the data transmits among the network.

FIG. 1 illustrates a simplified MANET that consists three mobile nodes (MN1, MN2, and MN3). As shown, MN1 is able to communicate with MN3 through MN2 when MN1 cannot reach MN3 via a direct communication.

SUMMARY

5 In accordance with one aspect, the present invention provides a mobile node for generating and transmitting a data packet to a designation mobile node through a mobile Ad-hoc network (MANET). The mobile node comprises a service or application module defining a code for each service or application executable on the mobile node, a security code generator operable to generate a security code, a
10 connection history recorded Identities (IDs) of the other mobile node connected to the mobile node, a routing table defining possible routes for routing the data packet within the MANET, a packet generator operable to generate a data packet having parameters that include the service or application code, the security code, the IDs and a counter defining a number of hops required for transmission and a communication
15 module for broadcasting the data packet. When the another mobile nodes receives the data packet, the another mobile nodes verifies all the parameters of the data packet to authenticate the transmission.

In one embodiment, the data packet is transmitted to the designation mobile node through at least one gateway node. It is possible that the gateway node is one of
20 the mobile nodes among the MANET.

In another embodiment, the routing table is updated regularly for increasing the number of possible routes for routing the data packet.

In a further embodiment, the number of hops is decreasing by 1 each time the data packet is transmitted to a designation mobile node. The ID may include a MAC address or other possible physical unique identification. Possibly, the service or application is embedded as part of the security code.

5 In yet a further embodiment, the security code includes a login ID, a group ID and an encryption or license key.

Yet, the data packet may further includes dummy characters for filling up a prescribe length of the data packet.

10

BRIEF DESCRIPTION OF DRAWINGS

This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

FIG. 1 illustrates a simplified known MANET;

FIG. 2 illustrates a block diagram of a mobile node in accordance with one
15 embodiment of the present invention;

FIG. 3 illustrates a flow diagram showing communications between three network nodes in accordance with one embodiment of the present invention;

FIG. 4 exemplify a format of a data packet in accordance with one embodiment of the present invention;

20 FIG. 5 exemplifies a format of a data packet in accordance with another embodiment of the present invention;

FIG. 6 exemplifies a format of a data packet in accordance with a further embodiment of the present invention; and

FIG. 7 exemplifies a format of a data packet in accordance with yet another embodiment of the present invention.

5

DETAILED DESCRIPTIONS

In line with the above summary, the following description of a number of specific and alternative embodiments is provided to understand the inventive features of the present invention. It shall be apparent to one skilled in the art, however that this invention may be practiced without such specific details. Some of the details may not
10 be described at length so as not to obscure the invention. For ease of reference, common reference numerals will be used throughout the figures when referring to the same or similar features common to the figures.

The present invention provides a system and method for nodes discovery and route determination with service aware and sufficient security features built-in to
15 support portable wireless devices with limited resources within a Mobile Ad-hoc Network (MANET). To achieve the objectives, the present invention make use of the increasing deployment of innovative solutions and the popularity wireless handheld devices, coupling with the demands in supporting business and lifestyle of mobile users. Wireless network supporting MANET can either be a single or combinations
20 of wireless Personal Area Network (WPAN), wireless LAN (WLAN) or wireless Metropolitan Area Network (WMAN).

The present invention provides a system and method to enhance security and mobility of mobile nodes of a Mobile Ad-hoc Network (MANET). Generally, it

enables mobile nodes to have a fast nodes discovery and establish secured communications with each other with the use of a unifying security and application codes.

In one embodiment of the present invention, the MANET comprises an automated system that includes security and service aware codes together with the knowledge of previous authorised mobile nodes to speed up the nodes discovery and route determination processes in a MANET. The MANET may comprise mobile nodes (MN) that are Internet Protocol (IP) based devices and the non-IP based devices. Each mobile node can be defined with its own definition of logical address, security and application codes to be used in the determination of route for mobile nodes to enhance security level for MANET devices. The system is able to link the process of nodes discovery and route determination closely to the service that a user using for the benefit of performance. It further links applications, network and systems level parameters in one single logical unit for the purpose of speedy response time. It is a scalable system and method that are able to support small handheld mobile nodes or devices in MANET.

FIG. 2 illustrates a block diagram of a mobile node 200 in accordance with one embodiment of the present invention. The mobile node 200 comprises a service or application a selection module 210, a security code generator 220, and a packet generator 230, a routing table 240, an access history 250, a communication role 260 and a communications module 290, and applications or services module 280. Briefly, the selection module 210 operationally initiates a communication with other mobile node through the MANET. Once the communication is initiated, the security code generator 220 appends a security code that is required for transmissions between the

mobile nodes. The packet generator 230 extracts relevant information, which includes the security code, and forms a data packet based on a predefined format and extracted relevant information for transmission through the MANET. The routing table 240 provides routes for transmitting the data packet within the MANET. The communications among various mobile nodes are carried out by referring to the routing table 240. The access history 250 provides archives or history on neighbouring MNs that communicated with the mobile node 200. The communication module 290 is provided to perform wireless communication with other mobile nodes that includes a corresponding communication module 290. The communication module 290 may include one or more transceiver of different protocols, such as Wi-Fi, GSM, etc. The applications or services module 280 handles the applications or services run on the mobile node 200. During the communications, the MANET requires to execute the same applications or services to provide appropriate communications between the mobile nodes.

FIG. 3 illustrates a flow diagram showing communications between three network nodes (MN1, MN2, MN3) in accordance with one embodiment of the present invention. The network nodes MN1, MN2 and MN3 communicate with each other as shown in FIG. 1. The communication flow is herewith illustrated in conjunction with FIG. 2. In the nutshell, the network node MN1 communicates with the network node MN3 via the network node MN2 as a MANET gateway. It is understood to a skilled person that the MANET may consist more than one gateway nodes for communications between two mobile nodes. The present embodiment provides only one gateway node MN2 for simplicity reason, not limitations. The relevant steps in FIG. 3 illustrate how a mobile node performs discovery and routing processes to establish communications between MN1 and MN3 through MN2. The

mobile nodes include Access Points (AP), wireless base stations, laptop computers, PCs, personal digital assistants, and any other mobile or stationary wireless devices. The method further provides security features on the services supported within the MANET with security parameter(s) and service pre-selected by the users, together
 5 with information of previous or recent neighbouring nodes will be grouped together to speed up the nodes discovery and routing process.

The mobile node MN1 initiates a communication with the mobile node MN3 at step 302 by invoking a suitable service or application on the mobile node MN1 through the service selection module 210. Each of the services or applications is
 10 assigned with a relevant service or application code. For examples, an instant messaging application corresponds to the service or application code of APP₁; a VoIP (voice over Internet Protocol) related applications corresponds to the service or application code of APP₂; and a file transfer related applications corresponds to the service or application code APP₃.

15 Once the required application or service is invoked, at step 304, the security code generator 220 appends a security code, herein denoted as "SEC". The security code can be a pre-defined security code, or a user-defined key code. Typically, the security code is agreed upon at least at the sender side and the recipient side in order to establish an authenticated communication. Depending on the security requirement,
 20 it is possible that, the security code is required to be agreed among other mobile nodes that routing the data packet as a gateway in order to establish an authenticated communication. A response to the security code (SEC_R) is generated by the receiver to serve as authentications for the sender. The security code is a combination of one or more parameters that includes login ID, password, encryption or license key, etc.

For example, Group ID + password forms a SEC_1 ; and login ID + Application_Key forms a SEC_2 .

During any communications, the mobile node MN1 records a connection history of recent neighbouring mobile nodes that connected thereto at step 306. The connection history details is utilised by the packet generator 230 for generating data packets. At step 308, the packet generator 230, searches the connection history record for all mobile nodes that communicated with the mobile node MN1 under the requested service or application based on the service or application requested. At the same time, a routing table stored on the mobile node MN1 is updated at step 309. The packet generator 230 extracts the mobile node addresses, OldStn, which include any one of user-defined logical address, Medium Address Control (MAC) address, (MAC + IP) address, and (MAC + logical) address. With the mobile node address (from the step 306), the service or application code (from the step 302) and the security code (from the step 304), the packet generator 230 forms the data packet, P_1 , with the structure as show in FIG. 4.

In FIG. 4, OldStn_{n-1} represents recent or previous mobile nodes MN_(n-1) addresses that accessed to the mobile node MN1, APP₁ represents the requested service or application code, which is generally pre-defined based on the service or application; SEC₁ represents the encrypted security code; S_{n-1}Add represents source MN_(n-1) address (i.e. mobile node MN1's address), which can by any of the addresses that include MAC address, (MAC + IP) address, (MAC + logical) address and the like; T_{L1} represents a time or time period that the data packet remains valid for transmission; and Dummy represents dummy characters that make up to a standard packet length, L.

In an alternative embodiment, T_{Li} represents a maximum number of hop allowed for transmitting the data packet. Further, APP_1 , SEC_1 can also be used defined code.

Referring back to FIG. 3, once the packet is formed in accordance with the
5 above data packet format, the packet generator 230 sends the data packet to the communications module 290 at step 310 for broadcasting. A Sent_Timer is also activated to track the time required for the data packet P_1 to be transmitted to mobile node MN3. Any neighbouring mobile nodes with their address matches one of the OldStn addresses shall serve the MN1 as a gateway to transmit the data packet, which
10 in the case of FIG. 3, the mobile node MN2. The relevant addresses of the neighbouring mobile nodes are stored in the routing table stored in the respective nodes, which is updated regularly. The routing table may include unique identification number of the transmitting nodes, applications served thereon, mode of access, time accessed previously and gateway node identification number and etc.

15 Still referring to FIG. 3, at step 311, the mobile node MN2 receives the data packet via its communication module 290. At step 312, the mobile node MN2 checks if its own address matches any of the $OldStn_{n-1}$ provided in the data packet. Once a match is found, at step 313, the mobile node MN2 decreases the value of T_{Li} by 1 where the T_{Li} represents the maximum number of hop allowable. At step 314, the
20 packet generator 230 subsequently generates a response packet, P_2 , as shown in FIG. 5 for acknowledging receipt to the mobile node MN1. Once acknowledged, the mobile node MN2 establishes a communication link with mobile node MN1 at step 315. Further, when the T_{Li} is greater than 0, the mobile node MN2 broadcasts a new

data package P_3 , which is generated based the P_1 . At step 318, the routing table is updated at step 318.

In FIG. 5, S_{1_Add} represents the original source MN address, i.e. the mobile node MN1 address; APP_1 represents the service or application code; SEC_{1_R} represents an encrypted security response code generated in response to the data packet, and the encrypted security response code is different from the SEC_1 ; OldStn represents the address of the mobile node MN2 sending out the response packet; T_{LR} represents the number of hop count left after the deduction which should be $T_{LR}-1$; and Dummy represents characters that make up for a standard packet length,

10 D.

Referring back to FIG. 3, once the communication link is established, the required application or service is executed accordingly at step 316. Once the communication ends, the mobile node MN2 disconnects from the mobile node MN1 at step 319. Referring back to step 312, the mobile node MN2 could not find any matching address among the OldStn addresses from the data packet P_1 , the mobile node MN2 further checks whether both the application or service code and the security codes contained in the data packet match a predefined code that include combinations of application keys, security codes and addresses as it deems fit. When the match is found, the mobile node MN2 proceeds with the step 313 and thereafter the subsequent steps provided above, which include establishes (the step 315) the communication link between the mobile node MN1 and mobile node MN2 and activates the application or services (the step 316). When neither the address nor the relevant code is matched, the communication link shall cease to establish and the

15

20

communication module 290 of the MN3 listen to the next broadcast messages of step 321.

Referring back to the step 315 of FIG. 3, the mobile node MN2 further broadcasts the data packet P_3 if T_{Li} is greater than zero value. The data packet P_3 is formatted as shown in FIG. 6, where its packet format is similar to that of P_1 except that the address of the mobile node MN2 that generated P_3 is added, and preferably the address code S_2_Add representing the MN2 address is placed before the S_1_Add field in the data packet P_3 .

Once the data packet P_3 is broadcasted, the neighbouring nodes, such as the mobile node MN3, upon receiving the data packet P_3 process the data packet P_3 accordingly. When the mobile node MN3 receives the data packet P_3 via its communication module 290 at step 321, the mobile node MN3 checks if its own address matches any of the $OldStn_{n-1}$ provided in the data packet P_3 at step 322. If a match is found, at step 323, the mobile node MN3 further decreases the value of T_{Li} by 1. Otherwise, the mobile node MN3 further checks whether both the application or service code and the security codes match the data packet P_3 at step 327. If neither of the matches is found, the data packet P_3 is disregarded or discarded. When a match is found, the mobile node MN3 proceeds to the step 323 to further decreases the value of T_{Li} by 1. At step 324, its packet generator 230 subsequently generates a response packet, P_4 , in a format as shown in FIG. 7 for acknowledging receipt to the mobile node MN2. Once acknowledged, the mobile node MN2 establishes a communication link with mobile node MN3 at step 325. During the communication, mobile node MN1 communicates with the mobile node MN3 via the established connections between MN1 and MN2 and MN3. In step 326, the required application or service is

executed accordingly at step 326. Once the communication ends, the mobile node MN3 disconnects from the mobile mode MN2.

The format of the data packet P_4 is similar to that of the data packet P_2 , except that address of the mobile node MN2, S_2_Add is also included therein.

5 In one embodiment, when any of the mobile nodes receives a data packet with T_L equal to zero, the data packet shall be ignored or deleted accordingly.

Still referring to FIG. 3, the routing table 290 of mobile nodes MN1, MN2 and MN3 are provided as a reference to each mobile node to communicate within the MANET. It recorded the possible routing paths available to communicate from a
10 source mobile node to a designation mobile node. The routing table 290 is also updated once a new data packet or response packet is generated at steps 309, 319, 329.

In another embodiment, the source mobile node, i.e. the mobile node that sends out a data packet, consolidates all response packets that received from other
15 mobile nodes. The response packets are decoded and form the routing table 240. An example of the routing table is provided in TABLE A.

TABLE A : Routing Table of the Mobile Node MN1

Destination MN	Mode	Intermediate MN	No of hops	Response Time	Last Update Time
MN2	Direct (1 hop)	-	1	10ms	20081208:1403
MN3	Indirect	MN2	1	33ms	20081208:1132
MN6	Indirect	MN2, MN8	2	52ms	20081208:1134

Each mobile node keeps a routing table 290 of its own defining possible routes for communication in the MANET. The routing table 290 is built up by recording all address information of destination mobile nodes that are able to respond directly will be saved or updated in the routing table 290. Address information of destination mobile node that received through another or intermediate mobile node, will be compared with those information in the routing table 290. When duplicate record is found, it will be ignored. If not, for a particular destination mobile node, the time that the packet received by the source mobile node from an intermediate mobile node will be used to compare with the receive time of other packet(s) received through another intermediate mobile node(s) if any. Typically, the fastest end-to-end response time of a packet will be used to determine which mobile node will be the intermediate mobile node for the destination mobile node.

In another embodiment, the routing table is updated frequent enough to handle the mobility and changes of topology in any MANET environment. When the time is up, section 3.5 onwards will be repeated. The frequency of updates can be adjusted in relationship with the users' mobility conditions and applications supported.

The link has to be disconnected properly by a simple detection of application already closed by any mobile node once the application no longer required and the routing table will be updated.

Based on above, the present invention is adapted to provide MANET or Ad-hoc network communication between devices in both Internet protocol (IP) and non-IP based devices. It is particularly suitable for portably MANET devices as it has a relatively thin nodes discovery and routing process. With application or service key embedded in the security codes, which is detectable at early stage of establishing a

communication link, the system enables the mobile nodes or devices to be service-aware.

While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof
5 could be made to the present invention without departing from the scope of the invention.

CLAIMS:

1. A mobile node for generating and transmitting a data packet to a designation mobile node through a mobile Ad-hoc network (MANET) having a nature of one or more mobile nodes, the mobile node comprising:
 - 5 a service or application module defining a code for each service or application executable on the mobile node;
 - a security code generator operable to generate a security code;
 - a connection history recorder operationally recording Identities (IDs) of the other mobile nodes previously connected to the mobile node;
 - 10 a routing table defining all possible routes for routing the data packet within the MANET and a number of hops required to transmit from the mobile node to the designation mobile node for each possible route,
 - wherein each mobile node within the MANET maintains their own routing table and each routing table is updated independently as the number of intermediate
 - 15 mobile nodes changes;
 - a packet generator operable to generate a data packet having security parameters that include the service or application code, the security code, the IDs and the number of hops required for transmission through the route,
 - wherein the number of hops of the data packet decreases as the data packet is
 - 20 transmitted to the next mobile node along the route; and
 - a communication module for broadcasting the data packet,
 - wherein when the another mobile nodes receives the data packet, the another mobile nodes verifies all the parameters of the data packet to authenticate the transmission.
 - 25
2. The mobile node according to claim 1, wherein the data packet is transmitted to the designation mobile node through at least one gateway node.
3. The mobile node according to claim 2, wherein the gateway node are one of
- 30 the mobile nodes among the MANET.
4. The mobile node according to claim 1, wherein the routing table is updated regularly for increasing the number of possible routes for routing the data packet.

5. The mobile node according to claim 1, wherein the number of hops in the data packet decreases by 1, each time the data-packet is transmitted to a designation mobile node.
- 5 6. The mobile node according to claim 1, wherein the ID includes a MAC address.
- 10 7. The mobile node according to claim 1, wherein the ID includes a physical unique identification.
8. The mobile node according to claim 1, wherein the service or application is embedded as part of the security code.
- 15 9. The mobile node according to claim 1, wherein the security code includes a login ID.
10. The mobile node according to claim 1, wherein the security code includes a group ID.
- 20 11. The mobile node according to claim 1, wherein the security code includes an encryption or license key.
- 25 12. The mobile node according to claim 1, wherein the data packet further includes dummy characters for filling up a length of the data packet.
13. The mobile node according to claim 1, wherein the security code is required to be agreed among other mobile node or nodes that route or routes the data packet as a gateway in order to establish an authenticated communication.
- 30

14. The mobile node according to claim 1, wherein the security code and application code is unified in the route determination process through the integration of the security parameters into a single logical unit.
- 5 15. The mobile according to claim 14, wherein the security parameters and service can be pre-selected by users, that will be grouped together with information of previous or recent neighbouring nodes to speed up the nodes discovery and routing process.
- 10 16. The mobile according to claim 1, wherein the mobile nodes in the MANET comprises Internet Protocol (IP) and non-IP based devices.