SECURE ROUTING BASED ON THE PHYSICAL LOCATIONS OF ROUTERS

~~CROSS-REFERENCE TO RELATED APPLICATIONS~~

~~This application is a *Continuation-In-Part* application of, and claims priority to and the benefit of U.S. patent application Ser. No. 12/949,404, filed November 18, 2010, entitled "Spot Beam Based Authentication". This application is a *Continuation-In-Part* application of, and claims priority to and the benefit of U.S. patent application Ser. No. 13/283,491, filed October 27, 2011, entitled "Geothentication Based on Network Ranging". The contents of both of these applications are hereby incorporated by reference in their entirety.~~

FIELD

The present disclosure relates to secure routing. In particular, it relates to secure routing based on the physical locations of routers.

BACKGROUND

Position-based routing is a general term describing the method of using the position of routers (e.g., network nodes) for making data packet routing and/or forwarding decisions. Previous implementations of position-based routing have aimed to optimize the network route for efficiency, not for security. Cyber attacks are becoming more advanced and having more catastrophic impacts on the networks in question and their associated users. One such attack, the man-in-the-middle (MITM) attack, has been used to reroute data for ill-intentioned purposes. The present disclosure provides an enhanced data routing security system and associated methods to mitigate data being routed outside of defined constraints.

SUMMARY

The present disclosure relates to a method, system, and apparatus for secure routing based on the physical locations of routers (e.g., network nodes). In particular, the present disclosure teaches the use of position-based routing techniques to ensure that information is securely transferred from a source to a destination. A method is defined to send a data packet through a network path that requires that security constraints are met. The security constraints are based on the physical location of one or more network routers.

In an example, there is provided a method for secure data transmission of at least one data packet through a plurality of network nodes. The method includes defining, by at least one user, a source network node and a destination network node. The source network node and the destination network node are in the plurality of network nodes. The method also includes defining, by the at least one user, at least one security constraint, wherein at least one of the at least one security constraint is based on a physical geographical location of at least one of the network nodes. The at least one security constraint is at least one of: the at least one data packet is routed through network nodes that are physically located within at least one specified geographic region, or through network nodes that are not physically located within the at least one specified geographic region, the at least one data packet is routed through network nodes that can have their physical locations authenticated by using at least one of: satellite geolocation techniques, network ping ranging measurements, or triangulation methods, if any network nodes are unable to have their physical locations authenticated, the at least one data packet can be routed through such network nodes if the at least one data packet is encrypted while the at least one data packet passes through such network nodes, and the at least one data packet travels from the source network node to the destination network node on a route that has a length less than a threshold distance. The method also includes comparing, by at least one processor, available network nodes in a map of the network nodes with the at least one security constraint to determine which of the available network nodes are qualified network nodes, wherein the qualified network nodes are the available network nodes that meet the at least one security constraint. The map of the network nodes includes at least one of: information regarding whether any of the network nodes are physically located within the at least one specified geographic region, or are not physically located within the at least one specified geographic region, information regarding whether the physical location of any of the network nodes can be authenticated by using at least one of: satellite geolocation techniques, network ping ranging measurements, or triangulation methods, information regarding whether any of the network nodes can encrypt or decrypt data packets, and information regarding whether any of the network nodes have been determined to be qualified network nodes. The method further includes determining, by the at least one processor, a route including at least one of the qualified network nodes to route the at least one data packet through from the

source network node to the destination network node. Any of the network nodes that does not meet the at least one security constraint is removed from consideration, and the route includes a network path that is optimized both for efficiency and security based on a requirement that the at least one security constraint is met by the at least one qualified network node. The method further includes transmitting the at least one data packet from the source network node to the destination network node through the optimal route including the at least one qualified network node.
In another example, there is provided a method for secure data transmission of at least one data packet through a plurality of network nodes. The method includes defining, by at least one user, a source network node and a destination network node. The source network node and the destination network node are in the plurality of network nodes. The method also includes defining, by the at least one user, at least one security constraint, wherein at least one of the at least one security constraint is based on physical geographical location of at least one of the network nodes. The at least one security constraint is at least one of: the at least one data packet is routed through network nodes that are physically located within at least one specified geographic region, or through network nodes that are not physically located within the at least one specified geographic region, the at least one data packet is routed through network nodes that can have their physical locations authenticated by using at least one of: satellite geolocation techniques, network ping ranging measurements, or triangulation methods, if any network nodes are unable to have their physical locations authenticated, the at least one data packet can be routed through such network nodes if the at least one data packet is encrypted while the at least one data packet passes through such network nodes, and the at least one data packet travels from the source network node to the destination network node on a route that has a length less than a threshold distance. The method also includes encoding, by at least one processor, the at least one security constraint into the at least one data packet and comparing, by the source network node, available network nodes in a map of the network nodes with the at least one security constraint to determine which of the available network nodes connected to the source network node are qualified network nodes. The qualified network nodes are the available network nodes that meet the at least one security constraint. The map of the network nodes includes at least one of: information regarding whether any of the network nodes are physically located within the at least one specified geographic region, or

are not physically located within the at least one specified geographic region, information regarding whether the physical location of any of the network nodes can be authenticated by using at least one of: satellite geolocation techniques, network ping ranging measurements, or triangulation methods, information regarding whether any of the network nodes can encrypt or decrypt data packets, and information regarding whether any of the network nodes have been determined to be qualified network nodes. The method also includes transmitting, by the source network node, the at least one data packet to one of the qualified network nodes. Any connected network node that does not meet the at least one security constraint is removed from consideration. The method further includes determining, by any network node that receives the at least one data packet, which available network nodes connected to the network node that receives the at least one data packet are qualified network nodes based on the map of network nodes. The method further includes transmitting, by any network node that receives the at least one data packet, the at least one data packet to one of the qualified network nodes. Any connected network node that does not meet the at least one security constraint is removed from consideration. The at least one data packet is transmitted in an optimal route from the source network node to the destination network node through the qualified network nodes. The route includes a network path that is optimized for both efficiency and security based on a requirement that the at least one security constraint is met by the qualified network nodes.

In one or more embodiments, a method for secure data transmission of at least one data packet through a plurality of network nodes is disclosed. The disclosed method

WE CLAIM:

1. A method for secure data transmission of at least one data packet through a plurality of network nodes, the method comprising:

defining, by at least one user, a source network node and a destination network node, wherein the source network node and the destination network node are in the plurality of network nodes;

defining, by the at least one user, at least one security constraint, wherein the at least one security constraint is based on a physical location of at least one of the network nodes;

comparing, by at least one processor, available network nodes in a map of the network nodes with the at least one security constraint to determine which of the available network nodes are qualified network nodes,

wherein the qualified network nodes are the available network nodes that meet the at least one security constraint;

determining, by the at least one processor, a route comprising at least one of the qualified network nodes to route the at least one data packet through from the source network node to the destination network node; and

transmitting the at least one data packet from the source network node to the destination network node through the route comprising the at least one qualified network node.

2. The method of claim 1, wherein the at least one security constraint is one of that the at least one data packet must be routed through the network nodes that are physically located within at least one specified geographic region, and that the at least one data packet must be routed through the network nodes that are not physically located within the at least one specified geographic region.

3. The method of claim 3, wherein at least one of the at least one geographic region is defined by a polygon, which is defined by points.

4. The method of claim 5, wherein the points are defined by the at least one user

specifying a longitude and a latitude of each of the points.

5. The method of claim 1, wherein the map of the network nodes comprises at least one of information regarding the physical location of at least one of the network nodes, information regarding whether the physical location of any of the network nodes can be authenticated by using satellite geolocation techniques, information regarding whether the physical location of any of the network nodes can be authenticated by using network ping ranging measurements, information regarding whether any of the network nodes can encrypt data packets, and information regarding whether any of the network nodes can decrypt data packets.

6. The method of claim 1, wherein at least one of the at least one security constraint is that the at least one data packet must be routed through the network nodes that can have their physical locations authenticated by using satellite geolocation techniques.

7. The method of claim 1, wherein at least one of the at least one security constraint is that the at least one data packet must be routed through the network nodes that can have their physical locations authenticated by using network ping ranging measurements.

8. The method of claim 1, wherein at least one of the at least one security constraint is that if the network nodes are unable to have their physical locations authenticated, the at least one data packet can be routed through the network nodes only if the at least one data packet is encrypted.

9. The method of claim 1, wherein at least one of the at least one security constraint is that the at least one data packet must travel from the source network node to the destination network node on a route that has a length less than a threshold distance.

10. A method for secure data transmission of at least one data packet through a plurality of network nodes, the method comprising:

defining, by at least one user, a source network node and a destination network

node, wherein the source network node and the destination network node are in the plurality of network nodes;

defining, by the at least one user, at least one security constraint, wherein the at least one security constraint is based on a physical location of at least one of the network nodes;

encoding, by at least one processor, the at least one security constraint into the at least one data packet;

determining, by the source network node, which available network nodes connected to the source network node are qualified network nodes,

wherein the qualified network nodes are the available network nodes that meet the at least one security constraint;

transmitting, by the source network node, the at least one data packet to one of the qualified network nodes;

determining, by any network node that receives the at least one data packet, which available network nodes connected to the network node that receives the at least one data packet are qualified network nodes; and

transmitting, by any network node that receives the at least one data packet, the at least one data packet to one of the qualified network nodes, wherein the at least one data packet is transmitted in a route from the source network node to the destination network node through the qualified network nodes.

11. The method of claim 12, wherein the at least one user is at least one of a person, an entity, an application, a program, a node, a router, a mobile device, a processor, and a computer.

12. The method of claim 12, wherein the at least one security constraint is one of that the at least one data packet must be routed through the network nodes that are physically located within at least one specified geographic region, and that the at least one data packet must be routed through the network nodes that are not physically located within the at least one specified geographic region.

13. The method of claim 14, wherein the at least one geographic region is at least one of a nation, a state, a province, a county, a government facility, and a city.

14. The method of claim 14, wherein at least one of the at least one geographic region is defined by a polygon, which is defined by points.

15. The method of claim 16, wherein the points are defined by the at least one user specifying a longitude and a latitude of each of the points.

16. The method of claim 12, wherein at least one of the at least one security constraint is that the at least one data packet must be routed through the network nodes that can have their physical locations authenticated by using satellite geolocation techniques.

17. The method of claim 12, wherein at least one of the at least one security constraint is that the at least one data packet must be routed through the network nodes that can have their physical locations authenticated by using network ping ranging measurements.

18. The method of claim 12, wherein at least one of the at least one security constraint is that if the network nodes are unable to have their physical locations authenticated, the at least one data packet can be routed through the network nodes only if the at least one data packet is encrypted.

19. The method of claim 12, wherein at least one of the at least one security constraint is that the at least one data packet must travel from the source network node to the destination network node on a route that has a length less than a threshold distance.

CLAIMS

1. A method for secure data transmission of at least one data packet through a plurality of network nodes, the method comprising:

defining, by at least one user, a source network node and a destination network node, wherein the source network node and the destination network node are in the plurality of network nodes;

defining, by the at least one user, at least one security constraint, wherein at least one of the at least one security constraint is based on a physical geographical location of at least one of the network nodes, wherein the at least one security constraint is at least one of:

the at least one data packet is routed through network nodes that are physically located within at least one specified geographic region, or through network nodes that are not physically located within the at least one specified geographic region,

the at least one data packet is routed through network nodes that can have their physical locations authenticated by using at least one of: satellite geolocation techniques, network ping ranging measurements, or triangulation methods,

if any network nodes are unable to have their physical locations authenticated, the at least one data packet can be routed through such network nodes if the at least one data packet is encrypted while the at least one data packet passes through such network nodes, and

the at least one data packet travels from the source network node to the destination network node on a route that has a length less than a threshold distance;

comparing, by at least one processor, available network nodes in a map of the network nodes with the at least one security constraint to determine which of the available network nodes are qualified network nodes, wherein the qualified network nodes are the available network nodes that meet the at least one security constraint, wherein the map of the network nodes comprises at least one of:

information regarding whether any of the network nodes are physically located within the at least one specified geographic region, or are not physically located within the at least one specified geographic region,

information regarding whether the physical location of any of the network nodes can be authenticated by using at least one of: satellite geolocation techniques, network ping ranging measurements, or triangulation methods,

information regarding whether any of the network nodes can encrypt or decrypt data packets, and

information regarding whether any of the network nodes have been determined to be qualified network nodes;

determining, by the at least one processor, a route comprising at least one of the qualified network nodes to route the at least one data packet through from the source network node to the destination network node, wherein any of the network nodes that does not meet the at least one security constraint is removed from consideration, and wherein the route comprises a network path that is optimized both for efficiency and security based on a requirement that the at least one security constraint is met by the at least one qualified network node; and

transmitting the at least one data packet from the source network node to the destination network node through the optimal route comprising the at least one qualified network node.

2. The method of claim 1, wherein the at least one user is at least one of a person, an entity, an application, a program, a node, a router, a mobile device, a processor, and a computer.

3. The method of claim 1, wherein the at least one specified geographic region is at least one of a nation, a state, a province, a county, a government facility, and a city.

4. The method of claim 1, wherein at least one of the at least one specified geographic region is defined by a polygon, which is defined by points, wherein the polygon is one of a regular shape or an irregular shape.

5. The method of claim 4, wherein the points are defined by the at least one user specifying a longitude and a latitude of each of the points.

6. A method for secure data transmission of at least one data packet through a plurality of network nodes, the method comprising:

defining, by at least one user, a source network node and a destination network node, wherein the source network node and the destination network node are in the plurality of network nodes;

defining, by the at least one user, at least one security constraint, wherein at least one of the at least one security constraint is based on physical geographical location of at least one of the network nodes, wherein the at least one security constraint is at least one of:

the at least one data packet is routed through network nodes that are physically located within at least one specified geographic region, or through network nodes that are not physically located within the at least one specified geographic region,

the at least one data packet is routed through network nodes that can have their physical locations authenticated by using at least one of: satellite geolocation techniques, network ping ranging measurements, or triangulation methods,

if any network nodes are unable to have their physical locations authenticated, the at least one data packet can be routed through such network nodes if the at least one data packet is encrypted while the at least one data packet passes through such network nodes, and

the at least one data packet travels from the source network node to the destination network node on a route that has a length less than a threshold distance;

encoding, by at least one processor, the at least one security constraint into the at least one data packet;

comparing, by the source network node, available network nodes in a map of the network nodes with the at least one security constraint to determine which of the available network nodes connected to the source network node are qualified network nodes, wherein the qualified network nodes are the available network nodes that meet the at least one security constraint, wherein the map of the network nodes comprises at least one of:

information regarding whether any of the network nodes are physically located within the at least one specified geographic region, or are not physically located within the at least one specified geographic region,

information regarding whether the physical location of any of the network nodes can be authenticated by using at least one of: satellite geolocation techniques, network ping ranging measurements, or triangulation methods,

information regarding whether any of the network nodes can encrypt or decrypt data packets, and

information regarding whether any of the network nodes have been determined to be qualified network nodes;

transmitting, by the source network node, the at least one data packet to one of the qualified network nodes, wherein any connected network node that does not meet the at least one security constraint is removed from consideration;

determining, by any network node that receives the at least one data packet, which available network nodes connected to the network node that receives the at least one data packet are qualified network nodes based on the map of network nodes; and

transmitting, by any network node that receives the at least one data packet, the at least one data packet to one of the qualified network nodes, wherein any connected network node that does not meet the at least one security constraint is removed from consideration, wherein the at least one data packet is transmitted in an optimal route from the source network node to the destination network node through the qualified network nodes, wherein the route comprises a network path that is optimized for both efficiency and security based on a requirement that the at least one security constraint is met by the qualified network nodes.

7. The method of claim 6, wherein the at least one user is at least one of a person, an entity, an application, a program, a node, a router, a mobile device, a processor, and a computer.

8. The method of claim 6, wherein the at least one specified geographic region is at least one of a nation, a state, a province, a county, a government facility, and a city.

9. The method of claim 6, wherein at least one of the at least one specified geographic region is defined by a polygon, which is defined by points, wherein the polygon is one of a regular shape or an irregular shape.

10. The method of claim 9, wherein the points are defined by the at least one user specifying a longitude and a latitude of each of the points.

11. The method of claim 6, wherein when the source network node determines that there are not any available network nodes connected to the source network node that are qualified network nodes, a negative acknowledgment message is sent to the user indicating that the at least one data packet will not be able to reach the destination network node.

12. The method of claim 6, wherein when any network node that receives the at least one

data packet determines that there are not any available network nodes connected to the network node that received the at least one data packet that are qualified network nodes and determines that the at least one data packet did not reach the destination network node, a negative acknowledgment message is sent to the user.

13. The method of claim 11 or 12, wherein in response to receiving the negative acknowledgment message, the at least one user may define at least one different security constraint to be used for the retransmission of the at least one data packet, and attempt to resend the at least one data packet.