node being connected to each other via at least one router network node. Also, the system involves the origination network node being configured for transmitting a data packet downstream to the destination network node through at least one router network node. In addition, the system involves the data packet containing a header portion and a payload data portion. Additionally, the system involves at least one enabled network node configured to verify at least one of the network nodes that are located upstream from the enabled network node(s) (i.e. from itself) by analyzing the header portion and/or the payload data portion of the data packet. The at least one enabled network mode is configured to determine which of the network nodes are geotag-capable network nodes.

In one or more embodiments, the header portion comprises a security signature portion and/or a routing data portion. In at least one embodiment, the security signature portion of the data packet includes geolocation information (e.g., a geotag) relating to at least one of the network nodes the data packet has traveled through. The geolocation information may be in various forms including, but not limited to, a standard "geotag" format as is well known in the art. For example, the geolocation information (e.g., geotag) may include, but is not limited to, any of the following: geolocation coordinates (i.e. longitude and latitude coordinates), the time the geolocation information is derived, at least a portion of the sampled radio frequency (RF) signal data, and code information (e.g., unique identifier codes) derived from at least a portion of at least some the sampled RF signals. In some embodiments, the geolocation information relating to at least one network node that the data packet has traveled through is obtained by receiving a resultant signal that is transmitted from at least one transmission source, where the resultant signal contains at least one authentication signal. In at least one embodiment, the location of the network node(s) the data packet has traveled through is verified by comparing properties of the resultant signal the network node(s) the data packet has traveled through receives to expected properties of the resultant signal that the network node(s) the data packet has traveled through should receive due to its location. In some embodiments, the header portion of the data packet employs an Internet Protocol version 6 (IPv6) data packet header. In at least one embodiment, geolocation information is stored within the IPv6 data packet header. In one or more embodiments, at least one transmission source is a satellite, a pseudo-satellite, and/or a terrestrial transmission source. In some embodiments, the satellite is a low Earth orbiting (LEO) satellite, a medium Earth orbiting (MEO) satellite, and/or a geosynchronous Earth orbiting (GEO) satellite.

In at least one embodiment, the geolocation information relating to at least one network node that the data packet has traveled through is determined from ranging information obtained by a signal transmitted by at least one network node the data has traveled through to another network node at

only the verified network nodes (i.e. where the entire node chain must consist of verified network nodes).

In one or more embodiments, at least one of the enabled network nodes is configured to determine which of the network nodes are geotag-capable network nodes. In some embodiments, at least one of the enabled network nodes is configured to determine which of the network nodes are enabled network nodes. In at least one embodiment, at least one of the enabled network nodes additionally utilizes received signals that are transmitted from at least one transmission source to verify at least one of the network nodes that are located upstream from the enabled network node(s) (i.e. from itself). In one or more embodiments, the data packet is transmitted from the origination network node downstream to the destination network node only through enabled network nodes.

In at least one embodiment, a method for ~~verifying (or authenticating) network nodes in a network~~data routing security is disclosed. The method involves transmitting a data packet from an origination network node downstream to a destination network node through at least one router network node. In one or more embodiments, the data packet contains a payload data portion and a header portion, wherein the header portion comprises ~~and a payload data portion~~a security signature portion which includes geolocation information relating to at least one of the network nodes the data packet has travelled through. The method further involves verifying, by at least one enabled network node, at least one of the network nodes that are located upstream from the at least one enabled network node~~(s) (i.e. from itself)~~ by analyzing at least a portion of the header portion and/or the payload data portion of the data packet. In at least one embodiment, at least one enabled network node is the origination network node, the destination network node, and/or the at least one router network node~~.~~, and the at least one enabled network node is configured to determine which of the network nodes are geotag-capable network nodes.

In at least one embodiment, the header portion comprises geolocation information for at least one network node in the form of at least one geotag (or geocertificate) that is appended to at least one data packet. In some embodiments, a data packet may be routed only through nodes that are geotag-capable nodes (i.e. network nodes that are capable to tag data packets with geolocation information). In some embodiments, at least one data packet is routed only through geotag-capable nodes (i.e. network nodes that are capable to tag data packets with geolocation information), which do not constitute the most direct path.

In one or more embodiments, the data packet is routed through the network nodes by using a tunneling method. In at least one embodiment, for the tunneling method, when at least one data packet is traveling through at least one non-enabled network node (i.e. a network node that is not capable of geotagging data packets with geolocation information and not capable of verifying other network nodes or its own geolocation information), an enabled network node encrypts the

WE CLAIM:

1. A system for data routing security, the system comprising:

an origination network node;

a destination network node; and

at least one router network node,

wherein at least one of the origination network node, the destination network node, and the at least one router network node is an enabled network node;

wherein the origination network node and the destination network node are connected to each other via the at least one router network node,

wherein the origination network node is configured for transmitting a data packet downstream to the destination network node through the at least one router network node,

wherein the data packet contains a header portion and a payload data portion, ~~and~~

wherein the at least one enabled network node is configured to verify at least one of the network nodes that are located upstream from the at least one enabled network node by analyzing at least one of the header portion and the payload data portion of the data packet, and

wherein the at least one enabled network node is configured to determine which of the network nodes are geotag-capable network nodes.

2. The system of claim 1, wherein the header portion comprises at least one of a security signature portion and a routing data portion.

3. The system of claim 2, wherein the security signature portion comprises geolocation information relating to at least one of the network nodes the data packet has traveled through.

9. The system of claim 1, wherein at least one of the at least one enabled network node is configured to only transmit data packets that the at least one enabled network node receives directly from any of the verified network nodes.

10. The system of claim 1, wherein at least one of the at least one enabled network node is configured to only transmit data packets that have traveled through only the verified network nodes.

~~11. The system of claim 1, wherein at least one of the at least one enabled network node is configured to determine which of the network nodes are geotag-capable network nodes.~~

~~12.~~11. The system of claim 1, wherein ~~at least one of~~ the at least one enabled network node is configured to determine which of the network nodes are enabled network nodes.

~~13.~~12. The system of any one of claims 1-~~12~~11, wherein at least one of the at least one enabled network node additionally utilizes received signals that are transmitted from at least one transmission source to verify at least one of the network nodes that are located upstream from the at least one enabled network node.

~~14.~~13. The system of any one of claims 1-~~13~~12, wherein the data packet is transmitted from the origination network node downstream to the destination network node only through enabled network nodes.

~~15~~14. A method for data routing security, the method comprising:

transmitting a data packet from an origination network node downstream to a destination network node through at least one router network node,

wherein the data packet contains a payload data portion and a header portion, wherein the header portion comprises ~~at least one of~~ a security signature portion which includes ~~geolacation~~ geolocation information relating to at least one of the network nodes the data packet has traveled through ~~and a payload data portion~~; and

verifying, by at least one enabled network node, at least one of the network nodes that are located upstream from the at least one enabled network node by analyzing at least one of the header portion and the payload data portion of the data packet,

wherein the at least one enabled network node is at least one of the origination network node, the destination network node, and the at least one router network node, and

wherein the at least one enabled network node is configured to determine which of the network nodes are geotag-capable network nodes.

~~16~~15. The method of claim ~~15~~14, wherein the geolocation information relating to the at least one network node that the data packet has traveled through is obtained by receiving a resultant signal that is transmitted from at least one transmission source,

wherein the resultant signal contains at least one authentication signal, and

wherein a location of the at least one network node the data packet has traveled through is verified by comparing properties of the resultant signal the at least one network node the data packet has traveled through receives to expected properties of the resultant signal that the at least one network node the data packet has traveled through should receive due to its location.

~~17~~16. The method of claim ~~15~~14, wherein the geolocation information relating to the at least one network node that the data packet has traveled through is determined from ranging information obtained by a signal transmitted by the at least one network node the data has traveled through to another network node at a verified location, and by a signal received by the at least one network node the data has traveled through from the network node at the verified location.

~~18~~17. The method of claim ~~15~~14, wherein when the at least one enabled network node verifies any of the network nodes, the at least one enabled network node removes at least a portion of data contained in the header portion of the data packet.

~~19~~18. The method of claim ~~15~~14, wherein the header portion of the data packet contains data relating to all of the network nodes that the data packet has traveled through.

~~20~~19. The method of ~~of~~ any of claims 15-~~19~~18, wherein when the at least one enabled network node verifies at least one of the network nodes, the at least one enabled network node adds data to the header portion of the data packet regarding the at least one of the network nodes that was verified.

~~21~~20. The method of claim ~~20~~19, wherein at least one of the at least one enabled network node is configured to only transmit data packets that the at least one enabled network node receives directly from any of the verified network nodes.

~~22~~21. The method of claim ~~20~~19, wherein at least one of the at least one enabled network node is configured to only transmit data packets that have traveled through only the verified network nodes.

~~23. The method of claim 20, wherein at least one of the at least one enabled network node is configured to determine which of the network nodes are geotag-capable network nodes.~~

~~24~~22. The method of claim ~~20~~19, wherein ~~at least one of~~ the at least one enabled network node is configured to determine which of the network nodes are enabled network nodes.

~~25~~23. The method of claim ~~20~~19, wherein at least one of the at least one enabled network node additionally utilizes received signals that are transmitted from at least one transmission source to verify at least one of the network nodes that are located upstream from the at least one enabled network node.

~~26~~24. The method of any of claims 15-~~25~~23, wherein the data packet is transmitted from the origination network node downstream to the destination network node only through enabled network nodes.