4. The system of claim 3, 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.

5. The system of claim 4, wherein the at least one transmission source is at least one of a satellite, a pseudo-satellite, and a terrestrial transmission source.

6. The system of claim 5, wherein the satellite is one of a low Earth orbiting (LEO) satellite, a medium Earth orbiting (MEO) satellite, and a geosynchronous Earth orbiting (GEO) satellite.

7. The system of claim 3, 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.

8. The system of claim 1, wherein the header portion of the data packet employs an Internet Protocol version 6 (IPv6) data packet header.

9. The system of claim 8, wherein geolocation information is stored within the IPv6 data packet header.

10. The system of claim 1, 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.

11. The system of claim 1, wherein the header portion of the data packet contains data relating to all of the network nodes that the data packet has traveled through.

12. The system of claim 1, 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.

13. The system of claim 12, wherein the added data to the header portion is regarding geolocation information related to the at least one of the network nodes that was verified.

14. 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.

15. 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.

16. 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.

17. 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.

18. The system of claim 1, 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.

19. The system of claim 1, wherein the data packet is transmitted from the origination network node downstream to the destination network node only through enabled network nodes.

20. 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 header portion 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.

21. The method of claim 20, wherein the header portion comprises at least one of a security signature portion and a routing data portion.

22. The method of claim 21, wherein the security signature portion comprises geolocation information relating to at least one of the network nodes the data packet has traveled through.

23. The method of claim 22, 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.

24. The method of claim 23, wherein the at least one transmission source is at least one of a satellite, a pseudo-satellite, and a terrestrial transmission source.

25. The method of claim 24, wherein the satellite is one of a low Earth orbiting (LEO) satellite, a medium Earth orbiting (MEO) satellite, and a geosynchronous Earth orbiting (GEO) satellite.

25. The method of claim 22, 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.

26. The method of claim 20, wherein the header portion of the data packet employs an Internet Protocol version 6 (IPv6) data packet header.

27. The method of claim 26, wherein geolocation information is stored within the IPv6 data packet header.

28. The method of claim 20, 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.

29. The method of claim 20, wherein the header portion of the data packet contains data relating to all of the network nodes that the data packet has traveled through.

30. The method of claim 20, 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.

31. The method of claim 30, wherein the added data to the header portion is regarding geolocation information related to the at least one of the network nodes that was verified.

32. The method of claim 20, 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.

33. The method of claim 20, 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.

34. 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.

35. 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 enabled network nodes.

36. The method of claim 20, 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.

37. The method of claim 20, wherein the data packet is transmitted from the origination network node downstream to the destination network node only through enabled network nodes.

4. The system of claim 3, 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.

5. The system of claim 3, 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.

6. The system of claim 1, 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.

7. The system of claim 1, 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.

8. The system of claim 7, wherein the added data to the header portion is regarding geolocation information related to the at least one of the network nodes that was verified.

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

15. 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 header portion, at least one of a security signature portion which includes geolacation 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.

16. The method of claim 15, 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. The method of claim 15, 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. The method of claim 15, 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. The method of claim 15, 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. The method of of any of claims 15-19, 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. The method of claim 20, 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. The method of claim 20, 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. 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 enabled network nodes.

25. The method of claim 20, 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. The method of any of claims 15-25, wherein the data packet is transmitted from the origination network node downstream to the destination network node only through enabled network nodes.