CLAIMS

1. A method to authenticate a claimant, comprising:

receiving, from the claimant, at least one set of data that has been captured by the claimant from at least one spot beam transmission wherein the data comprises a pseudo-random number;

comparing the at least one set of data to a known valid data set; and

authenticating the claimant when a difference between the claimed data and the valid data set is less than a threshold.

2. The method of claim 1, wherein the at least one spot beam transmission is emitted from at least one of a low earth orbit satellite, a medium earth orbit satellite, a geosynchronous earth orbit satellite, or a pseudo-satellite.

3. The method of claim 1, wherein the method is used for at least one of a one-way authentication, a multi-way authentication, a multi-way peer to peer device authentication.

4. The method of claim 1, wherein the claimant also provides at least one of the following to the verifier: at least one location identifier and time.

5. The method of claim 4, wherein the at least one location identifier is based on an earth-based coordinate system, comprising at least one of a latitude, longitude, altitude or a geographic locator.

6. The method of claim 1, wherein the at least one set of data further comprises at least one of the following: a time stamp, a timing code segment, a spot beam transmitting vehicle identifier, a beam identifier, a time bias parameter, or spot beam transmitting vehicle trajectory data.

7. The method of claim 4, wherein comparing the location identifier and the at least one set of data to a known valid data set includes comparing the location identifier with a known location for the spot beam at a time corresponding to the

time stamp.

8. The method of claim 1, wherein:

the claimant comprises an electronic computing device; and

the claimant is authenticated independently for each message transmitted by the electronic computing device.

9. The method of claim 1, wherein:

the claimant establishes a communication session with a remote device; and

the claimant is authenticated at least once for the communication session.

10. The method of claim 1, wherein:

the claimant collects at least two locations over time (e.g., polling), and wherein the at least two locations are compared against a known valid data set to authenticate the claimant using knowledge of the claimant's planned traveled path.

11. An apparatus to authenticate a claimant, comprising:

a processor; and

a memory module comprising logic instructions which, when executed, configure the processor to:

operate as in any of claims 1 through 10.

12. The apparatus of claim 11, further comprising logic instructions which, when executed, configure the processor to:

allow the claimant to access a service provided by a remote host when the claimant has been authenticated.

13. A system to authenticate a claimant, comprising:

at least one signal source to transmit a spot beam in accordance with a known spot-beam geometry;

at least one electronic device comprising a receiver to receive at least one set of data from the spot beam transmission wherein the data comprises a pseudo-

random number; and

at least one verifier communicatively coupled to the at least one electronic device to authenticate a claimant using the at least one set of data and a known valid data set.

14. The system of claim 13, wherein the at least one electronic device is able to determine its location.

15. The system of claim 14, wherein the at least one electronic device's determined location is further used to authenticate the electronic device.

16. The system of claim 13, wherein the at least one electronic device comprises at least one of the following: a mobile phone, a portable computing device, a computer network node, a server, a wireless networking node or a biometric verification system.

17. The system of claim 13, wherein the at least one verifier comprises:

a processor; and

a memory module comprising logic instructions which, when executed, configure the processor to:

receive, from the electronic device, the at least one set of data that the electronic device captured from the spot beam transmission; and

compare the at least one set of data to a known valid data set; and

authenticate the claimant when a difference between the at least one set of data and the known valid data set is less than a threshold.

18. The system of claim 13, wherein the claimant is authenticated when the difference between the at least one location identifier and the known valid data set is less than a threshold.

19. The system of claim 17, wherein the at least one verifier comprises logic instructions which, when executed, configure the processor to compare the location identifier with a known location for the spot beam at a time corresponding to the time stamp.

20. A system to authenticate a claimant device with a host network, comprising:

a receiving device communicatively coupled to the claimant device and the host network, wherein the receiving device receives at least one pseudo-random code that has been captured by the claimant device from a spot beam transmitted from a satellite; and

an authentication server coupled to the host network, and

wherein the receiving device transmits an authentication request from the claimant to the host network.

21. A system for multi-way authentication, comprising:

a first receiving device to receive at least one pseudo-random code associated with a spot beam transmitted from a satellite; and

a second device communicatively coupled to the first electronic device via a communication network;

wherein the first receiving device and the second device implement a peer-to-peer authentication process using at least a portion of the pseudo-random code as a shared secret.

22. The system of claim 21, wherein at least one of the first receiving device or the second device determines an extent of access to a resource after successful authentication.

23. The system of claim 21, wherein at least one of the first receiving device or the second device creates an authenticated network which implements one or more cyber security policies to protect the communication and access to one or more networked resources for a given context.

24. The system of claim 21, wherein the authentication server uses information provided by the claimant to geolocate the claimant's position.

25. The system of claim 13, wherein the signal source comprises a multi-phased antenna array to generate at least one spot beam.

CLAIMS

1. A method to authenticate a claimant, comprising:

receiving, from the claimant, at least one set of data that has been captured by the claimant from at least one spot beam transmission wherein the data comprises a pseudo-random number and a time stamp associated with the data;

further receiving, from the claimant, at least one location identifier;

comparing the location identifier and the at least one set of data to a known valid data set, including comparing the location identifier with a known location for the spot beam at a time corresponding to the time stamp; and

authenticating the claimant when a difference between the claimant data and the valid data set is less than a threshold.

2. The method of claim 1, wherein the at least one spot beam transmission is emitted from at least one of a low earth orbit satellite, a medium earth orbit satellite, a geosynchronous earth orbit satellite, or a pseudo-satellite.

3. The method of claim 1, wherein the method is used for at least one of a one-way authentication, a multi-way authentication, a multi-way peer to peer device authentication.

4. The method of claim 1, wherein the at least one location identifier is based on an earth-based coordinate system, comprising at least one of a latitude, longitude, altitude or a geographic locator.

5. The method of claim 1, wherein the at least one set of data further comprises at least one of the following: a timing code segment, a spot beam transmitting vehicle identifier, a beam identifier, a time bias parameter, or spot beam transmitting vehicle trajectory data.

6. The method of claim 1, wherein the claimant comprises an electronic computing device, and wherein the claimant is authenticated independently for each message transmitted by the electronic computing device.

7. The method of claim 1, wherein the claimant establishes a communication session with a remote device, and wherein the claimant is authenticated at least once for the communication session.

8. The method of claim 1, wherein the claimant collects at least two locations over time (e.g., polling), and wherein the at least two locations are compared against a known valid data set to authenticate the claimant using knowledge of the claimant's planned traveled path.

9. An apparatus to authenticate a claimant, comprising:

a processor; and

a memory module comprising logic instructions which, when executed, configure the processor to operate as in any of claims 1 through 10.

10. The apparatus of claim 9, further comprising logic instructions which, when executed, configure the processor to allow the claimant to access a service provided by a remote host when the claimant has been authenticated.

11. A system to authenticate a claimant, comprising:

at least one signal source to transmit a spot beam in accordance with a known spot-beam geometry;

at least one electronic device comprising a receiver to receive at least one set of data from the spot beam transmission wherein the data comprises a pseudo-random number and a time stamp associated with the data, wherein the at least one electronic device is able to determine its location; and

at least one verifier communicatively coupled to the at least one electronic device to authenticate a claimant comprising the electronic computing device, wherein the at least one verifier comprises a processor and a memory module, the memory module comprising logic instructions which, when executed, configure the processor to:

receive, from the electronic device, the at least one set of data that the electronic device captured from the spot beam transmission;

further receive, from the electronic device, at least one location identifier determined by the electronic device;

compare the location identifier and the at least one set of data to a known valid data set, including comparing the location identifier with a known location for the spot beam at a time corresponding to the time stamp; and

authenticate the claimant when a difference between the electronic device data and the valid data set is less than a threshold.

12. The system of claim 11, wherein the at least one electronic device comprises at least one of the following: a mobile phone, a portable computing device, a computer network node, a server, a wireless networking node or a biometric verification system.