

GEOAUTHENTICATION BASED ON NEW NETWORK PACKET STRUCTURE**CROSS-REFERENCE TO RELATED APPLICATIONS**

This application is a *Continuation-In-Part* application of, and claims the benefit of, U.S. patent application Ser. No. 13/114,013, filed May 23, 2011, which is a *Continuation-In-Part* application of, and claims the benefit of, U.S. patent application Ser. No. 12/130,880, filed May 30, 2008, both of which are hereby incorporated by reference in their entirety. This application is related to U.S. patent application Ser. No. 13/073,830, filed March 28, 2011, and U.S. patent application Ser. No. 12/949,404, filed November 18, 2010, both of which are hereby incorporated by reference in their entirety.

BACKGROUND

The present disclosure relates to geolocation. In particular, it relates to geolocation based on new network packet structure.

To date, many large scale cyber attacks have not only left the recipients of the attacks still recovering from the damage left behind, but the recipients are also unable to deter any further damage through retaliation, or otherwise, as without having a clear traceability to the attack's originator and, thus, often lack the authority to respond. If attack motives are unclear, it is further unlikely that the recipient could tell if the attack was a mere act of vandalism, a purposeful theft, or a more sinister approach to threaten national security. As such, any system that would aid in denying network access to rogue users and/or provide traceable data to aid in identifying the originator would have great utility to reduce and mitigate denial of service (DoS) and network data interception attacks.

SUMMARY

The present disclosure relates to a method, system, and apparatus for verifying and/or geolocating network nodes in a network in attenuated environments for cyber and network security applications. In particular, the present disclosure teaches a system involving an origination network node and a destination network node. The system further involves at least one router network node. In one or more embodiments, the origination network node, the destination network node, and/or at least one router network node is/are an enabled network node. Further, the system involves the origination network node and the destination network

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

a verified location, and by a signal received by at least one network node the data has traveled through from the network node at the verified location.

In one or more embodiments, when at least one enabled network node verifies any of the network nodes, the enabled network node(s) removes at least a portion of data contained in the header portion of the data packet. In some embodiments, when at least one enabled network node verifies (or authenticates) any of the network nodes, the enabled network node(s) removes at least a portion of data contained in the header portion of the data packet and/or the payload data portion of the data packet. In one or more embodiments, when at least one enabled network node verifies any of the network nodes, the enabled network node(s) removes at least a portion of the data from the IPv6 data packet header. In at least one embodiment, the routing data portion of the data packet contains data relating to all of the network nodes that the data packet has traveled through. In at least one embodiment, the routing data portion of the data packet contains data relating to at least one of the network nodes that the data packet has traveled through.

In at least one embodiment, when at least one enabled network node verifies at least one of the network nodes, the enabled network node(s) adds data to the header portion of the data packet regarding the network node(s) that was/were verified. In one or more embodiments, the added data to the security signature portion includes geolocation information (e.g., a geotag) related to the network node(s) that was verified. In at least one embodiment, the data that an upstream network node adds to the data packet may be different than the data that a downstream network node may add to the data packet after the downstream network node verifies the upstream network node and removes at least a portion of the data from the data packet. For example, the upstream network node may add a large amount of sampled signal data to the data packet, and the enabled downstream network node may subsequently replace this large amount of data with a smaller amount of data, such as data relating to the geolocation information of the upstream network node, after the enabled downstream network node verifies the upstream network node. Since the smaller amount of data is related to the geolocation information of the upstream network node, this data may be considered to be more secure than the large amount of data relating to the sampled signal data. In some embodiments, at least one of the enabled network nodes is configured to only transmit data packets that the enabled network node(s) receives directly from any of the verified network nodes. In one or more embodiments, at least one of the enabled network node(s) is configured to only transmit data packets that have traveled through

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
5 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
10 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 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
15 packet contains a payload data portion and a header portion, wherein the header portion comprises 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 by analyzing at least a portion of
20 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
25 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
30 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
35 other network nodes or its own geolocation information), an enabled network node encrypts the

data packet on one end of the non-enabled network path. In at least one embodiment, the data packet(s) traveling through the non-enabled network node(s) is decrypted on the other end of the non-enabled network path by another enabled network node. In at least one embodiment, at least one data packet traveling through at least one non-enabled network node is not decrypted until it
5 arrives to its destination network node (i.e. the network node that the data is being routed to).

In some embodiments, information contained in the header portion (e.g., the security signature portion) of the data packets may continue to grow in size as the data packet travels through the network nodes until the data packet reaches its destination network node, where it may be verified (or authenticated) if the destination network node is an enabled network node. In some
10 embodiments, a downstream enabled network node may be utilized to verify (or authenticate) an upstream network node, and then the downstream enabled network node may remove the verified (or authenticated) information from the data packet header. In at least one embodiment, the upstream network node may be verified (or authenticated) by an enabled downstream network node by reviewing the security signature of the upstream network node that is contained
15 in the data packet. In at least one embodiment, the enabled network node that verifies the upstream network node may add information to the data packet header indicating that the enabled network node is verified (or authenticated) the upstream network node.

In at least one embodiment, the enabled network node that verifies the upstream network node may add information to the data packet header indicating that the enabled network node has
20 validated the upstream path (i.e. the path located upstream of the enabled network node that runs between at least two network nodes). In at least one embodiment, a security signature of at least one upstream network node at least partly comprises at least one geotag that represents the geolocation of the upstream network node(s). In some embodiments, when a data packet travels through a network path containing at least two network nodes, at least one enabled network node
25 adds new information to the data packet header without removing the potentially authenticable information in the data packet, which was appended by at least one upstream enabled network node. In addition, at least one enabled network node removes information in the data packet header relating to at least one upstream network node the data packet has traveled through and, adds new information to the data packet header.

30 In some embodiments, only enabled network nodes are capable of at least one of the following: authenticating (or verifying) at least one upstream network node the data packet has traveled through; authenticating (or verifying) an upstream network path that the data packet has traveled

through; only routing data packets that have traveled through enabled network nodes and have been authenticated by the enabled network nodes that they have traveled through; appending information to the data packet header confirming authentication (or verification) of at least one network node; appending geo-tag information to the data packet header; appending trusted router (i.e. enabled network node) information to the data packet header; appending pathway information to the data packet header; removing information from the data packet header from a previous verification (or authentication) of at least one network node; removing geotag information from the data packet header of at least one network node which has been previously verified (or authenticated); removing trusted information from the data packet header of at least one network node which has been previously verified (or authenticated); and removing pathway information from the data packet header of at least one network node which has been previously verified (or authenticated).

In some embodiments, geotagging data packets, by geotag-capable nodes, may be utilized to increase the level of trust of at least one network node. In at least one embodiment, geotagging data packets may be utilized to increase the degree of trust of a path between at least two network nodes where at least one of the nodes is a geotag-capable node.

In other embodiments, the present disclosure teaches a system involving an origination network node and a destination network node. The system further involves at least one router network node. Further, the system involves the origination network node and the destination network 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 to the destination network node through at least one router network node. In addition, the system involves the data packet containing a security signature portion, a routing data portion, and a payload data portion.

In one embodiment, this method can be adopted for existing infrastructure; however, it requires additional effort given the internet engineering task force (IETF) internet protocol (IP) Networking protocols and their implementations in routers. For the existing deployed infrastructure, an inter-related router network using enabled hardware is used for a management control plane signaling that may effectively allow tracking and tracing methods to be performed for specific classes of traffic, while allowing normal data plane traffic to take the standard existing fast path forwarding. For example, a specific control plane network management packet that has a known route can be inserted that has the same route as a particular class of data plane

IP network traffic between the same peer routers. This allows a solution to be developed using elements such as appropriate analytics, such as an event correlation engine for network attribution and a decision support engine, which may be deployed on existing and future deployed infrastructures on the control plane while being fully compliant with IETF RFCs. The elements that are listed, which the data packets would contain, would now be conveyed via the control plane data and data plane flows and can be assumed to be following the current processing and forwarding mechanisms.

In one or more embodiments, the security signature portion comprises a digital signature. In some embodiments, the security signature portion comprises a listing of at least one network node that the data packet travelled through from the origination network node to the destination network node. In at least one embodiment, the security signature portion comprises timing information for at least one network node in the listing indicating when the data packet was received and/or transmitted by the network node(s). In some embodiments, the security signature portion comprises identifier information for at least one network node in the listing. In one or more embodiments, the identifier information is biometric information and/or a bit sequence identification code.

In at least one embodiment, the security signature portion comprises geolocation information for at least one network node in the listing. In one or more embodiments, the geolocation information is obtained by the network node receiving a resultant signal that is transmitted from at least one transmission source. The resultant signal contains at least one authentication signal. The network node location is verified by comparing properties of the resultant signal the network node receives to expected properties of the resultant signal that the network node should receive due to its location. In some embodiments, at least one transmission source is a satellite, a pseudo-satellite, and/or a terrestrial transmission source. In at least one embodiment, the satellite is a low Earth orbiting (LEO) satellite, a medium Earth orbiting (MEO) satellite, or a geosynchronous Earth orbiting (GEO) satellite.

In at least one embodiment, in lieu of geolocation data being appended to every data packet, a secure network server could be used to periodically validate the location of the capable participating routers. End users with capable devices could verify the routing path by periodically checking with the secure network server to confirm the location of the routers in the path. As each router may have its own key, as long as the keys have not been compromised, this could be used in lieu or in combination of adding geolocation data to every packet.

In one or more embodiments, the disclosed system employs an Iridium LEO satellite constellation, where each of the satellites in the constellation has an antenna geometry that transmits forty-eight (48) spot beams with a distinctive spot beam pattern. In at least one embodiment, at least one authentication signal may be transmitted from at least one of the Iridium satellites in the constellation. The forty-eight (48) spot beams of an Iridium satellite may be used to transmit localized authentication signals to network nodes located on or near the Earth's surface. The broadcasted message burst content associated with these authentication signals includes pseudorandom noise (PRN) data. Since a given message burst may occur within a specific satellite spot beam at a specific time, the message burst content including PRN and unique beam parameters (e.g., time, satellite identification (ID), time bias, orbit data, etc.) may be used to authenticate the location of the network nodes. It should be noted that when employing one of the above-described Iridium LEO satellites, the transmission signal power is sufficiently strong enough to allow for the signal to penetrate into an indoor environment. This allows for the disclosed system to be used for many indoor applications for authentication technologies.

In one or more embodiments, the geolocation information is determined from ranging information obtained by a signal transmitted by the network node to another network node at a verified location and a signal received by the network node from the network node at the verified location. In at least one embodiment, the disclosed system utilizes the principles of network level ranging for Internet IP traffic on a per Quality of Service (QoS) flow basis. In at least one embodiment, the routing data portion contains routing information for the data packet, where the routing information includes information regarding the destination network node that the data packet is to be sent. In one or more embodiments, the payload data portion includes the data that is to be transmitted from the origination network node to the destination network node.

In at least one embodiment, a method for verifying and/or geolocating network nodes in attenuated environments for cyber and network security applications involves transmitting, with an origination network node, a data packet to a destination network node through at least one router network node. The origination network node and the destination network node are connected to each other via at least one router network node. The data packet contains a security signature portion, a routing data portion, and a payload data portion.

In one or more embodiments, a network node device for cyber and network security applications involves a receiver and a processor. The receiver is capable of receiving a signal from a signal

source. The processor is able to append information related to the signal as a security signature onto data packets that are routed through the network node device.

In at least one embodiment, an authentication system for cyber and network security applications involves a *network node device* and a *processing device*. The *network node device* comprises a receiver that is capable of receiving a signal from a signal source, and a processor that is able to append information related to the signal as a security signature onto data packets that are routed through the network node device. The processing device is able to compare the security signature of the data packets being routed through the network node device to known information related to the signal that the network node device received to authenticate the network node device.

In one or more embodiments, authentication of the network node device is at least partly comprised of determining if the network node device is physically located in its anticipated geographic location. In at least one embodiment, the network node device is authenticated before data is authorized to be passed. In some embodiments, the processing device is a cell phone, a personal digital assistant (PDA), a personal computer, a computer node, an internet protocol (IP) node, a server, a Wi-Fi node, and/or a tethered or untethered node.

Additionally, the present disclosure relates to a method, system, and apparatus for using guard spot beams for authenticating the location of a network node. In particular, the present disclosure teaches a method for a transmission-based authentication system to verify geolocation information for a network node. In one or more embodiments, the disclosed method involves transmitting, from at least one transmission source, an authentication signal and at least one guard signal. The method further involves receiving, from at least one receiving source, at least one resultant signal. At least one resultant signal includes the authentication signal and/or at least one guard signal. In addition, the method further involves authenticating, with at least one authenticator device, at least one network node by evaluating at least one resultant signal that the network node(s) receives from at least one receiving source. In at least one embodiment, at least one network node is utilized by an entity and/or a user.

In one or more embodiments, the authentication signal and at least one guard signal are transmitted from the same transmission source. In at least one embodiment, the authentication signal and at least one guard signal are transmitted from different transmission sources. In some embodiments, the authentication signal and at least one guard signal are transmitted on the same

frequency. In alternative embodiments, the authentication signal and at least one guard signal are transmitted on different frequencies.

In at least one embodiment, data transmitted by at least one guard signal is used for a legitimate purpose. In one or more embodiments, at least one guard signal at least partially includes an authentication signal. In various embodiments, the guard signal may include an authentication signal and/or data, which may be legitimate or false. In some embodiments, data transmitted by at least one guard signal includes localized information and/or regional information.

In one or more embodiments, data transmitted by the guard signal can be received by a network node that is located within an overlap area of the signals. In some embodiments, the data is transmitted via at least two out-of-phase binary phase shift keying (BPSK) signals, where the out-of-phase BPSK signals appear to be at least one quadrature phase shift keying (QPSK) signal. In at least one embodiment, a changing of the modulation of the bit stream of at least one guard signal modifies the broadcast power of the bits in the bit stream on a bit by bit basis. In some embodiments, when at least two guard signals are transmitted, a relative power of the guard signals is varied such that the guard signals located closer to the authentication signal have a higher power than the guard signals located further from the authentication signal.

Additionally, the present disclosure teaches a transmission-based authentication system to verify geolocation information for a network node. In one or more embodiments, the disclosed system involves at least one transmitter, at least one receiver, and at least one authenticator device. In one or more embodiments, at least one transmitter transmits an authentication signal and at least one guard signal; and at least one receiver receives at least one resultant signal. At least one resultant signal includes the authentication signal and/or at least one guard signal. In at least one embodiment, at least one authenticator device authenticates at least one network node by evaluating at least one resultant signal that at least one network node receives from at least one receiver. It should be noted that, in one or more embodiments, the system also includes a cyber locate portal. The cyber locate portal is a secure interface between the network and the authenticator device that adds an additional level of security to the system. In these embodiments, the resultant signal is sent to the authenticator device for authentication via the cyber locate portal.

In one or more embodiments, the authentication data is encrypted to avoid being intercepted and re-used. Additionally, the data may be signed with a signature, which can be used to confirm the data originated from a specific portal device by comparing the signature of the data to the

signature for that specific portal device. Each cyber locate portal device may have a unique key for encrypting, and may have an additional key for signing the sample data. These keys would optimally only be known by the authentication server and the portal device.

In at least one embodiment, at least one receiver and at least one transmitter are incorporated together in at least one transceiver. In some embodiments, the authentication signal and at least one guard signal are transmitted from the same transmitter. In at least one embodiment, the authentication signal and at least one guard signal are transmitted from different transmitters. In one or more embodiments, at least one authenticator device includes a server and/or a processor. In some embodiments, the authentication signal and at least one guard signal are transmitted on the same frequency.

In at least one embodiment, at least one authenticator device operates at least part of a host network. In one or more embodiments, the disclosed system further comprises a host network that operates as an intermediary between at least one network node and at least one authenticator device. In some embodiments, at least one receiver is employed in a cell phone, a personal digital assistant (PDA), a personal computer, a computer node, an internet protocol (IP) node, a server, a wi-fi node and/or a tethered or untethered node.

In some embodiments, the receiver may also encompass the functionality of a cyber locate portal device. In some embodiments, the receiver and the cyber locate portal device are combined in a cell phone or PDA. Note that if a cell phone or PDA includes the cyber locate portal device, the signal processing, encryption, and signature functions may ideally be performed in hardware and/or firmware that are not part of the operating system of the cell phone or PDA. For example, optionally, the encryption and signature keys as well as the unencrypted sample data are not accessible by the cell phone or PDA operating system.

In one or more embodiments, at least one transmitter is employed in at least one satellite and/or at least one pseudo-satellite. In some embodiments, at least one satellite is a Lower Earth Orbiting (LEO) satellite, a Medium Earth Orbiting (MEO) satellite, and/or a Geosynchronous Earth Orbiting (GEO) satellite. In one or more embodiments, at least one network node is stationary and/or mobile. In at least one embodiment, at least one authenticator device is a peer device.

In one or more embodiments, a method for a transmission-based authentication system involves transmitting, from at least one transmission source, a plurality of authentication signals. The method further involves receiving, from at least one receiving source, a resultant signal that

includes at least two of the authentication signals. Further, the method involves authenticating, with at least one authenticator device, at least one network node by comparing properties of the resultant signal the network node(s) receives from the receiving source location(s) to expected properties of the resultant signal that the network node(s) should receive from the receiving source location(s).

In one or more embodiments, a system and method for a transmission based authentication system involve transmitting, from at least one transmission source, a plurality of authentication signals in spot beams, where each spot beam contains one authentication signal. In at least one embodiment, the transmission source(s) is employed in at least one LEO satellite from an Iridium satellite constellation. In some embodiments, the authentication signals are transmitted on the same frequency. The method further involves receiving, from at least one receiving source, a resultant signal that includes at least two of the authentication signals. Further, the method involves authenticating at least one network node by comparing properties of the resultant signal the network node(s) receives from the receiving source location(s) to expected properties of the resultant signal that the network node(s) should receive from the receiving source location(s).

In at least one embodiment, the authentication signals are transmitted from the same transmission source. In alternative embodiments, the authentication signals are transmitted from the different transmission sources. In some embodiments, the transmission source(s) is employed by at least one satellite and/or at least one pseudo-satellite. In one or more embodiments, the authentication signals are transmitted on the same frequency and at the same time, and each authentication signal has a different modulation than the other authentication signals. In at least one embodiment, the different modulations are different pseudorandom digital modulation sequences. In some embodiments, the different pseudorandom digital modulation sequences are different BPSK code sequences.

In one or more embodiments, the properties that are compared are signal power, doppler shift, time of arrival, and/or signal modulation. In particular, the received signal modulation is the combination of a plurality of authentication signals, and this resultant combined modulation has characteristics that will change with the receiving source's location. In some embodiments, the disclosed system and method relate to network security for networks including, but not limited to, self-forming, peer-to-peer, and/or ad hoc networks.

The features, functions, and advantages can be achieved independently in various embodiments of the present inventions or may be combined in yet other embodiments.

DRAWINGS

These and other features, aspects, and advantages of the present disclosure will become better understood with regard to the following description, appended claims, and accompanying drawings where:

FIG. 1A illustrates an embodiment of the disclosed system for geolocating network nodes in attenuated environments for cyber and network security applications.

FIG. 1B illustrates an embodiment of the disclosed system for geolocating network nodes in attenuated environments for cyber and network security applications, where an enabled network node verifies at least one upstream network node and then removes appended data relating to the upstream network node(s) from the data packet.

FIG. 1C illustrates an embodiment of the disclosed system for geolocating network nodes in attenuated environments for cyber and network security applications, where an upstream network node verification method is used for a data packet traveling downstream from an origination network node to a destination network node through multiple router network nodes.

FIG. 1D illustrates an embodiment of the disclosed system for geolocating network nodes in attenuated environments for cyber and network security applications that utilizes geo-tagging and data encryption techniques.

FIG. 1E illustrates an embodiment of the disclosed system for geolocating network nodes in attenuated environments for cyber and network security applications that utilizes geo-tagging and makes use of the IPv6 packet header's 8-bit Next Header field.

FIG. 1F illustrates an embodiment of the disclosed system for geolocating network nodes in attenuated environments for cyber and network security applications, where the data packet is to be routed only through network nodes that are located within a defined geographical region.

FIG. 1G illustrates an embodiment of the disclosed system for geolocating network nodes in attenuated environments for cyber and network security applications, where two network nodes are able to receive transmission signals from at least one LEO satellite.

FIG. 2 illustrates the locations of three network nodes being verified by a transmission based authentication system and by the use of ranging information.

FIG. 3 illustrates an embodiment of the transmission-based authentication system employing a satellite to transmit an authentication beam along with multiple guard beams.

FIG. 4A illustrates an embodiment of a transmission-based authentication system having four network nodes located at various positions within and near three overlapping spot beams.

5 FIG. 4B illustrates an embodiment of a graph of signals transmitted by the three spot beams of FIG. 4A.

FIG. 4C illustrates an embodiment of an array of signal strengths of the three spot beams at the locations of the four network nodes of FIG. 4A.

FIG. 4D illustrates an embodiment of an array of bits for the three spot beams of FIG. 4A.

10 FIG. 4E illustrates an embodiment of an array of resultant signal sequences received by the four network nodes of FIG. 4A.

FIG. 4F illustrates an embodiment of a graph depicting resultant signals received by the four network nodes of FIG. 4A

FIG. 5 illustrates an embodiment of a transmission-based authentication system using guard
15 beam transmission as part of a secondary mission.

FIG. 6 illustrates an embodiment of a transmission-based authentication system employing out-of-phase binary phase shift keying (BPSK) guard beam transmission.

FIG. 7 illustrates an embodiment of the disclosed system having a network node that is able to perform in an occluded or jammed environment.

20 DESCRIPTION

The methods and apparatus disclosed herein provide an operative system for geothentication used for data routing security based on applications based on a new network packet structure. More specifically, the present disclosure teaches using enabled network nodes to geotag data packets to improve data packet traceability, and to verify or authenticate the geolocation
25 information relating to other network nodes (i.e. to geothenticate other network nodes). Once a network node is verified or authenticated by an enabled network node, the network node is then referred to as a trusted network node. In addition, it should be noted that the present disclosure also teaches using geotag-capable network nodes that are capable of geotagging data packets with geolocation information, but are not capable of verifying or authenticating network nodes.
30 In at least one embodiment, at least one enabled network node in a system may not be capable of

geotagging, but is still capable of verifying (or authenticating) the geolocation information relating to other network nodes (i.e. to geothenticate other network nodes).

A geotag references the geolocation information related to the location of at least one network node. The geolocation information may include, but is not limited to, a snippet of raw satellite data, at least part of a known or unknown code specific to a particular satellite beam, geolocation coordinates (e.g., latitude and longitude coordinates), time the geolocation information was derived, at least a portion of the sampled radio frequency (RF) signal data (e.g., satellite RF data), and/or coding information (e.g., unique identifier codes) derived from at least a portion of some of the sampled RF signal data. This geolocation information may be incorporated into the existing structure of the IPv6 data packet header, and specifically may be incorporated into the data packet header's 8-bit Next Header field (i.e. as an extension header). This particular field specifies the type of the Next Header, and usually specifies the higher-level transport layer protocol used by a data packet's payload. When extension headers are present, this field indicates which extension header follows. In some embodiments, the geotag extension headers reside between the fixed header and the upper-layer protocol header. In at least one embodiment, the extension headers form a chain, all using the Next Header field, where: the Next Header field in the fixed header indicates the first geotag header; the Next header field in a geotag header indicates the subsequent geotag header; and the Next Header field of the last geotag header indicates the type of the upper-layer protocol header in the payload of the data packet.

Currently, IPv6 data packets support Internet Protocol Security (IPsec) via extension headers, specifically using an Authentication Header (AH) and Encapsulating Security Payload (ESP). AH guarantees connectionless integrity and data origin authentication of IP packets, while ESP provides origin authenticity, integrity, and confidentiality protection of the data packets. In some embodiments, a new extension header set may be created. In other embodiments, geotag headers may be incorporated into these existing extensions. While in yet other embodiments, an entirely new paradigm may be defined.

In at least one embodiment, network nodes in a network path append geolocation information to all of the data packets that pass through the network nodes, thereby creating a verifiable history of the network path that the data packet has traversed. Appending information to the data packet header at each network node may be impractical since the data packet size could become very large with much appended information. In some embodiments, information containing the full network path may be too large to be stored within the header of the data packet. In at least one

embodiment, enabled routers (i.e. enabled network nodes) assess each data packet for authenticity as it travels through the network and, are able to confirm the route the data packet has traveled through as being secure.

5 In some embodiments, at least one enabled network node is authorized to confirm the validity of the information in the header of the data packet that relates to all of the network nodes that the data packet has traveled through (i.e. auditing the pathway). After the enabled network node(s) has verified the information, the enabled network node(s) then removes that information from the header of the data packet, thereby reducing the size of the data packet header and not requiring the security signature portion of the data packet to increase in size after the data packet has
10 traveled through each network node. In at least one embodiment, the enabled network node(s) may add information to the data packet header indicating that the upstream path that the data packet traveled through was authenticated. While in other embodiments, the enabled network node(s) may be designed to only pass data packets that have information in their header that they traveled through an authenticated upstream network path. In these cases, the enabled network
15 node(s) would not need to append information to the data packet header regarding the upstream path being authenticated. In either case, the enabled network node(s) may add its own security signature to the data packet, which may include a geotag, before the enabled network node(s) passes the data packet to the next network node, and/or it may add information to the data packet header indicating to a data packet recipient downstream that the data packet passed through a
20 trusted router (i.e. enabled network node).

In some embodiments, at least one network node may be authenticated by using signals that are transmitted from at least one transmission source located in space, thereby increasing the difficulty in spoofing. In some embodiments, in order to prevent a malicious network node from inappropriately stripping or modifying geolocation information (e.g., a geotag) from the data
25 packet header, at least one enabled network node is able to perform a method to determine which network nodes are its neighboring network nodes, and to determine which of those neighboring network nodes are geotag-capable network nodes and/or enabled network nodes. Any path that traverses only enabled network nodes can be inferred to be a trusted path (i.e. a verified or authenticated path).

30 In other embodiments of the present disclosure, the methods and apparatus disclosed herein provide an operative system for geolocating network nodes. Specifically, this system relates to geolocating network nodes in attenuated environments for cyber and network security

applications, such as for authentication and/or for authorization of network nodes. In particular, the present disclosure teaches participating network nodes, or other junctions in the network chain, that tag transmitted data packets with appending authentication data. This authentication data has a specific data packet structure, which includes unique data such as security signature data, routing data, and/or payload data. The security signature data includes information regarding the location of the participating network nodes in the network chain and may also include information regarding whether their location has been verified.

Currently, cyber-security is becoming increasingly important as electronic systems become more engrained into everyday business and social tasks. Many previously managed business processes have expanded into electronic data processing online, which has made on-going information and computing security advancement techniques a necessary requirement in order to protect these everyday-used systems. Critical documents and other data using information from social security numbers to national infrastructure related information are stored in networked systems that if accessed by an unauthorized party would have varying degrees of societal impact from nuisances to significant societal infrastructure breakdown. In parallel with increased reliance on electronic systems, the nation has also seen a dramatic increase in terrorism and computer hacking; thus requiring society to work towards improving methods to protect our networked computer systems.

Cyber attacks and network penetrations are becoming all too common. These frequent occurrences have brought discussions of dangers of network penetrations by external threats in both commercial and military environments to the forefront. Current access control approaches are principally based on either static passwords, or are authentication based using passwords and smart badge credentials based on Public Key Infrastructure (PKI). As system attacks are often conducted by impersonating the end user, there has been a tendency for organizations to focus on user authentication methods to curtail network data interception network vulnerabilities. These approaches continue to be vulnerable to sophisticated attacks and, thus, a need has developed for a new paradigm of access control leveraging additional dimension/information beyond the normal three dimensions (what you know, what you have, and who you are) of authentication by adding the geospatial location/context, such as user location, to provide an additional and orthogonal layer of protection, which provides an enhanced correlation between location and context awareness from integrated physical geolocation mapping to logical network and information management views.

Furthermore, the fact that existing cyber attacks are often shrouded in anonymity has created additional concerning problems. Larger attacks are often precluded by attempts of the originator to make small intrusions/attacks to better understand the system's vulnerabilities for future exploitation and laying the groundwork for a later, more destructive attack.

5 The present disclosure relates generally to networked systems that benefit from cyber security. More specifically, the system of the present disclosure leverages at least one self-geolocating network node to employ a signature packet structure that may allow for the data packet to be traceable back to a specific network node at a defined point in time. This signature packet structure can be used to improve cyber security in participating networks. As an example, a
10 signature packet structure may include elements such as payload data, routing data, and/or security data. The security data may be defined as geolocation data, biometrics data, and/or timing data. In at least one embodiment, this signature packet structure collectively may be referred to as the cyber security signature when being used for cyber security applications. For example, a file may be transmitted from one user to another user through a connection such an
15 email transmitted through the internet. Participating network nodes, or other sort of junctions, in the network chain may tag the data with appending authentication data, which may include elements of the signature packet structure (e.g., payload data, routing data, and/or security data). As the data packet moves to the next junction in the network chain, the network junction may authenticate it. Authentication may occur when the physical location as represented through the
20 geolocation data is validated against the known network node location.

The present disclosure may be used to provide access to a networked system as well as to restrict access to such a system. In at least one embodiment, it is envisioned that networks leveraging this form of cyber security may require such cyber security signature data in order to accept data packets. It is through this means that rogue users may be identified prior to entering the system
25 as the signature is virtually unspoofable, or that man-in-the-middle or other similar attacks are recognized as discrepancies in the signature data. In at least one embodiment, the system may incorporate existing trace back methods, such as constraining the number of node hops (i.e., numerical counter Time to Live (TTL)). This invention may introduce a paradigm shift (i.e., Internet 3.0) in terms of cyber security, which could lead to its adoption by the masses for
30 hardware and/or software that is able to support a signature packet data structure.

The system of the present disclosure may be adapted for networked systems that include wired and/or wireless network nodes. In at least one embodiment, at least one network node uses at

least one satellite to geolocate. In one example, a self-geolocating network node may use a low Earth orbiting (LEO) constellation that is enabled to provide a signal that can be received indoors. This system may or may not be used in combination with global positioning system (GPS) or any other system used for positioning, navigation, and/or timing. In addition, the system of the present disclosure may employ biometrics in order to validate a user/node by something inherent to the user/node, as well as employ any other authentication method that when used in combination with the described methods will improve the overall security of the system.

The system of the present disclosure has four main features. The first main feature of the system is that teaches a self-geolocating networking device (e.g., a self geolocating server, router, personal computing device, cell phone, and/or television) that has many applications, including general cyber security and authentication; but may also be used in other applications such as gaming.

The second main feature of the disclosed system is that it teaches a data packet structure that enables authentication and cyber security. The data packet structure enables a means to trace the data packet back to network nodes that were part of the series of junctions used for the packet to get to its destination location. This signature packet structure can be used to improve cyber security in participating networks. As an example, a signature packet structure may include elements such as payload data, routing data, and/or security data. The security data may be defined as geolocation data, biometrics data, and/or timing data. In at least one embodiment, this signature packet structure collectively may be referred to as the cyber security signature if used for cyber security applications.

The third main feature of the disclosed system is that it teaches elements of the signature packet structure that are unique. Participating network nodes, or other sort of junctions, in the network chain may tag the data with appending authentication data, which may include elements of the signature packet structure (i.e., payload data, routing data, and/or security data). The participating network nodes act similar to touch DNA from a fingerprint in terms of traceability as each router that the data packet utilizes provides some traceable data to the signature. As the data packet moves to the next junction in the network chain, it will accumulate, for example, small bit sequences and each subsequent junction may authenticate it. This accumulation of small bit sequences can lead to a statistically compelling fingerprint of the network path. Authentication may occur by comparing the network latencies for the anticipated network path

(along with their corresponding unique appended data) to the signature data packet and anticipated network latency acceptable ranges. Additionally, other network parameters may be monitored to validate that a man-in-the-middle (MITM) attack is not underway. In one embodiment, if a MITM attack is suspected, the network may be configured to respond based on the network's policy.

The fourth main feature of the disclosed system is that the system employs the use of at least one LEO satellite to transmit a signal to the network nodes. The LEO satellite signal is able to penetrate into an indoor environment due to its higher received power at the receiver. As such, this feature allows for the disclosed system to be used for many indoor applications for authentication technologies.

Additionally, it should be noted that the disclosed system can be used for a variety of applications where it is desirable to confirm, trace, monitor, and/or track the location of a "node". In addition, the system may provide additional utility to existing tracking methods for credit cards, especially since payment options are currently being more integrated into personal portable devices, such as cellular telephones. Not only could the location of a user of a credit card be monitored, but the user could potentially be tracked to be re-located for the case of trying to retrieve a stolen item from the user. Also, it should be noted that this feature may be used in combination with personal computing devices for gaming, such as for geo-caching.

In the following description, numerous details are set forth in order to provide a more thorough description of the system. It will be apparent, however, to one skilled in the art, that the disclosed system may be practiced without these specific details. In the other instances, well known features have not been described in detail so as not to unnecessarily obscure the system.

FIG. 1A illustrates an embodiment of the disclosed system 100 for geolocating network nodes in attenuated environments for cyber and network security applications. In this figure, a user located at origination network node (Node A) 110 wishes to transmit a data packet 130 to a user located at destination network node (Node D) 120. The origination network node (Node A) 110 and the destination network node (Node D) 120 are connected to each other via a plurality of router network nodes 140, which include Node B 140 and Node C 140. The origination network node (Node A) 110 is shown to transmit the data packet 130 to the destination network node (Node D) 120 through router network nodes Node B 140 and Node C 140.

The data packet 130 contains a header portion and a payload data portion 160. The header portion includes a security signature portion 170 and a routing data portion 150. The routing

data portion 150 of the data packet 130 contains routing information for the data packet 130. The routing information includes information regarding the destination network node (e.g., the address for the destination network node (Node D) 120) that the data packet 130 is to be sent. The payload data portion 160 of the data packet 130 contains the data and/or information that the user at the origination network node (Node A) 110 wants to send to the user at the destination network node (Node D) 120. The security signature portion should be unable to be copied from one packet and pasted into another packet, otherwise the essence of the invention would be compromised as it would be possible to make another packet appear as though it has followed the same route as the first. This may be applied differently in various embodiments. In one embodiment, the security signature may be a function of the payload data. For example, the security signature could include a component that is a digital signature, which may be a function of the payload data. These digital signatures could be accumulated along the route or could be validated as having come from the last participating router and replaced with a new digital signature at each hop. In one or more embodiments, the security signature portion of the data packet is not necessarily a true digital signature, but may comprise various types of data including, but not limited to, sample signal data, geolocation data, timing information, and/or routing information relating to where the data packet has traveled.

The security signature portion 170 of the data packet 130 includes a listing of all of the network nodes that the data packet 130 travelled through from the origination network node (Node A) 110 to the destination network node (Node D) 120. As shown in this example, the listing of network nodes in the security signature portion 170 includes Node A 110, Node B 140, Node C 140, and Node D 120. As the data packet 130 travels through the network of nodes, every time the data packet 130 travels through a network node, that particular network node is added to the listing of network nodes. As such, the security signature 170 develops into unique key identifier for the data packet 130, much like a specific DNA sequence for a particular organism.

In one or more embodiments, the security signature portion 170 also contains timing information for at least one of the network nodes in the listing. The timing information indicates when the data packet 130 was received and/or transmitted by the network node(s). In addition, in at least one embodiment, the security signature portion 170 of the data packet 130 contains identifier information for at least one of the network nodes in the listing. Types of identifier information that may be used for the disclosed system include, but are not limited to, various types of biometric information and/or unique bit sequence identification codes for each of the network nodes.

Additionally, the security signature portion 170 of the data packet 130 includes geolocation information for at least one of the network nodes in the listing. The geolocation information includes the specific physical location of the network node and may also include indication as to whether the location of the network node is verified. In at least one embodiment, the geolocation information of a network node is verified by the network node receiving at least one authentication signal that is transmitted from at least one transmission source. A detailed description of how the location of a network node is verified by the use of an authentication signal(s) is discussed in the descriptions of FIGS. 3, 4, 5, and 6. In some embodiments, the geolocation information of a network node is verified by using ranging information that is obtained from signals that are transmitted to and from network nodes that are at verified locations. A detailed description of how the ranging information is obtained is described in the description of FIG. 2.

FIG. 1B illustrates an embodiment of the disclosed system for geolocating network nodes in attenuated environments for cyber and network security applications, where an enabled network node verifies (or authenticates) at least one upstream network node and then removes appended data relating to the upstream network node(s) from the data packet. In this figure, a user located at origination network node (Node D) 102 wishes to transmit a data packet downstream to a user located at destination network node (Node A) 112. The origination network node (Node D) 102 and the destination network node (Node A) 112 are connected to each other via a plurality of router network nodes 122, 162, which include Node B 162 and Node C 122. The origination network node (Node D) 102 transmits the data packet downstream to the destination network node (Node A) 112 through router network nodes Node B 162 and Node C 122. For this example, Node C 122 is an enabled network node, which means that it has the ability to verify (or authenticate) any of the network nodes that lie upstream from itself. The other network nodes (Node D 102, Node B 162, and Node A 112) are not enabled network nodes.

The data packet contains a header portion and a payload data portion 152. The header portion comprises a security signature portion 132 and a routing data portion 142. The routing data portion 142 of contains routing information for the data packet. The payload data portion 152 contains the data and/or information that the user at the origination network node (Node D) 102 wants to send to the user at the destination network node (Node A) 112. The security signature portion 132 includes a listing of and/or geolocation information for all of the network nodes that the data packet has travelled through from the origination network node (Node D) 102 to the destination network node (Node A) 112. In this example, when the data packet is located at the

origination network node (Node D) 102, Node D 102 adds information (e.g., geolocation information) in the header portion (i.e. routing data portion 142 and/or security signature portion 132) of the data packet relating to Node D 102, thereby indicating that the data packet has traveled through Node D 102.

- 5 The data packet then travels from Node D 102 to Node C 122, which is an enabled network node. An enabled network node has the ability to verify any of the network nodes that are located upstream from itself by analyzing the header portion (i.e. the security signature portion 132 and/or the routing data portion 142) and/or the payload data portion 152 of the data packet. It should be noted that in some embodiments, the enabled network node additionally analyzes
- 10 geolocation information (e.g., a geotag) related to an upstream network node(s) that is contained in the header portion (i.e. the security signature portion 132 and/or the routing data portion 142) of the data packet header. In addition, enabled network nodes have the ability to geotag data packets with geolocation information.

- It should be noted that in one or more embodiments, the geolocation information related to a
- 15 network node is obtained by the network node receiving a resultant signal that is transmitted from at least one transmission source, where the resultant signal contains at least one authentication signal. A location of the network node is verified by comparing the properties of the resultant signal the network node receives to expected properties of the resultant signal that the network node should receive due to its location. In some embodiments, the header portion of
- 20 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 LEO satellite, a MEO satellite, or a GEO satellite. In other embodiments, the geolocation information related to a
- 25 network node is determined from ranging information obtained by a signal transmitted, either wirelessly or by wire, by the network node to another network node at a verified location, and a signal received, either wirelessly or by wire, by the network node from the network node at the verified location.

- In this example, once the data packet reaches enabled network Node C 122, Node C 122
- 30 analyzes the data packet, and determines that Node D 102 is a trusted network node (i.e. a legitimate network node, not a spoofed network node). Node C 122 essentially determines that Node D 102 is a trusted network node because Node C 122 has verified (or authenticated) Node

D 102 after analyzing the data packet. After Node C 122 verifies (or authenticates) Node D 102, Node C removes the information in the header portion (i.e. the routing data portion 142 and/or security signature portion 132) of the data packet that is related to Node D 102. In one or more embodiments, Node C 122 additionally adds information in the header portion (i.e. the routing data portion 142 and/or security signature portion 132) of the data packet regarding Node D 102 being verified (or authenticated). In at least one embodiment, the added information includes geolocation information (e.g., a geotag) related to the verified network node (i.e. Node D 102). Then, Node C 122 adds information in the header portion (i.e. the routing data portion 142 and/or security signature portion 132) of the data packet that is related to itself (i.e. information related to Node C 122).

After Node C 122 adds the information to the data packet, the data packet is transmitted downstream to Node B 162. Once the data packet reaches Node B 162, Node B 162 adds information in the header portion (i.e. the routing data portion 142 and/or security signature portion 132) of the data packet that is related to itself (i.e. information related to Node B 162). It should be noted that since Node B 162 is not an enabled network node, Node B 162 does not verify (or authenticate) Node C 122, and Node B 162 does not remove any information in the header portion (i.e. the routing data portion 142 and/or the security signature portion 132) of the data packet that is related to Node C 122. Then, the data packet is passed to the destination network node (Node A) 112. Once the data packet reaches Node A 112, Node A 112 adds information in the header portion (i.e. the routing data portion 142 and/or security signature portion 132) of the data packet that is related to itself (i.e. information related to Node A 112). As such, the resultant data packet will contain information in the header portion (i.e. the routing data portion 142 and/or security signature portion 132) of the data packet that is related to Node C 122, Node B 162, and Node A 112. It should be noted that in some embodiments, the resultant data packet will also contain information in the header portion (i.e. the routing data portion 142 and/or security signature portion 132) of the data packet regarding Node D 102 being verified (or authenticated).

It should be noted that in one or more embodiments of the disclosed system, an enabled network node is configured to only transmit data packets that the enabled network node receives directly from a verified network node (i.e. a trusted network node). In some embodiments, an enabled network node is configured to only transmit (or pass) data packets that have previously traveled only through verified network nodes (i.e. trusted network nodes). In at least one embodiment, an enabled network node is configured to determine which of the network nodes are geotag-capable

network nodes. In one or more embodiments, an enabled network node is configured to determine which of the network nodes in the network are enabled network nodes.

FIG. 1C illustrates an embodiment of the disclosed system for geolocating network nodes in attenuated environments for cyber and network security applications, where an upstream network node verification method is used for a data packet traveling downstream from an origination network node to a destination network node through multiple router network nodes. For this example, a data packet is routed from an origination network node (Node G) to a destination network node (Node A) through a plurality of network nodes (Node F, Node E, Node D, Node C, and Node B). Node E and Node B are enabled network nodes, and the remaining nodes (Node G, Node F, Node D, Node C, and Node A) are not enabled network nodes.

The data packet contains a header portion and a payload data portion 123. The header portion comprises a security signature portion 103 and a routing data portion 113. The routing data portion 113 of contains routing information for the data packet, and the payload data portion 123 contains the data and/or information that the user at the origination network node (Node G) wants to send to the user at the destination network node (Node A). The security signature portion 132 includes a listing of all of the network nodes that the data packet has travelled through from the origination network node (Node G) to the destination network node (Node A).

In this example, when the data packet is at the origination network node (Node G), Node G adds information 133 in the header portion (i.e. the routing data portion 113 and/or security signature portion 103) of the data packet relating to Node G, thus indicating that the data packet has traveled through Node G. Then, the data packet is transmitted from Node G to Node F. Node F adds information 143 in the header portion (i.e. the routing data portion 103 and/or security signature portion 113) of the data packet that is related to itself (i.e. information related to Node F). The data packet is then transmitted from Node F to Node E, which is an enabled network node. An enabled network node has the ability to verify any of the network nodes that are located upstream from itself by analyzing the header portion (i.e. the security signature portion 103 and/or the routing data portion 113) and/or the payload data portion 123 of the data packet. Optionally, the enabled network node additionally analyzes geolocation information (e.g., a geotag) related to an upstream network node(s) that is contained in the header portion (i.e. the security signature portion 103 and/or the routing data portion 113) of the data packet header.

Then, Node E analyzes the data packet, and determines that Node F and Node G are trusted network nodes (i.e. legitimate network nodes, not spoofed network nodes). Node E determines

that Node F and Node G are trusted network nodes because Node E has verified (or authenticated) Node F and Node G by analyzing the information in the data packet. After Node E verifies Node F and Node G, Node E removes the information 133, 143 in the header portion (i.e. the routing data portion 113 and/or security signature portion 103) of the data packet that is related to Node F and Node G. In some embodiments, Node E additionally adds information (not shown) in the header portion (i.e. the routing data portion 113 and/or security signature portion 103) of the data packet regarding Node F and Node G being verified (or authenticated). In at least one embodiment, the added information includes geolocation information (e.g., a geotag) related to the verified network nodes (i.e. Node F and Node G). Then, Node E adds information 153 in the header portion (i.e. the routing data portion 113 and/or security signature portion 103) of the data packet that is related to itself (i.e. information 153 related to Node E).

After Node E adds the information 153 to the data packet, the data packet is transmitted downstream to Node D. Once the data packet reaches Node D, Node D adds information 163 in the header portion (i.e. the routing data portion 113 and/or security signature portion 103) of the data packet that is related to itself (i.e. information 163 related to Node D). Then, the data packet is passed downstream to Node C. After the data packet reaches Node C, Node C adds information 173 in the header portion (i.e. the routing data portion 113 and/or security signature portion 103) of the data packet that is related to itself (i.e. information 173 related to Node C).

Then, the data packet is transmitted downstream from Node C to Node B, which is an enabled network node. Node B analyzes the data packet, and determines that Node C, Node D, and Node E are trusted network nodes (i.e. legitimate network nodes, not spoofed network nodes). Node B determines that Node C, Node D, and Node E are trusted network nodes because Node B has verified (or authenticated) Node C, Node D, and Node E by analyzing information in the data packet. After Node B verifies Node C, Node D, and Node E, Node C removes the information 153, 163, 173 in the header portion (i.e. the routing data portion 113 and/or security signature portion 103) of the data packet that is related to Node C, Node D, and Node E. In one or more embodiments, Node B additionally adds information (not shown) in the header portion (i.e. the routing data portion 113 and/or security signature portion 103) of the data packet regarding Node C, Node D, and Node E being verified (or authenticated). In some embodiments, the added information includes geolocation information (e.g., a geotag) related to the verified network nodes (i.e. Node C, Node D, and Node E). Then, Node E adds information 183 in the header portion (i.e. the routing data portion 113 and/or security signature portion 103) of the data packet that is related to itself (i.e. information 183 related to Node B).

Then, the data packet is passed from Node B to the destination network node (Node A). Once the data packet reaches Node A, Node A adds information 193 in the header portion (i.e. the routing data portion 113 and/or security signature portion 103) of the data packet that is related to itself (i.e. information 193 related to Node A). Thus, the resultant data packet will contain
5 information 183, 193 in the header portion (i.e. the routing data portion 113 and/or security signature portion 103) of the data packet that is related to Node B and Node A. In some embodiments, the resultant data packet will also contain information in the header portion (i.e. the routing data portion 113 and/or security signature portion 103) of the data packet regarding Node G, Node F, Node E, Node D, and Node C being verified (or authenticated). In one or more
10 embodiments, the resultant data packet will also contain information in the header portion (i.e. the routing data portion 113 and/or security signature portion 103) of the data packet regarding Node E and Node B being enabled network nodes.

FIG. 1D illustrates an embodiment of the disclosed system for geolocating network nodes in attenuated environments for cyber and network security applications that utilizes geo-tagging
15 and data encryption techniques. In this figure, Nodes A, B, and C are enabled network nodes, and Nodes D, E, F, G, H, and I are non-enabled network nodes. Where Node A is the origination network node and Node C is the destination network node.

In this example, a data packet is routed only through enabled network nodes (i.e. through Node A, Node B, and Node C). Since Nodes A, B, and C are enabled network nodes, they have the
20 ability to be geothenticated (i.e. have their geolocation verified or authenticated). When they are geothenticated, they are considered to be trusted network nodes. In one or more embodiments, Nodes A, B, and C are able to geothenticate themselves by each receiving at least one signal transmitted from at least one transmission source. In some embodiments, at least one transmission source is a LEO satellite (e.g., an Iridium satellite).

25 In at least one embodiment, the data packet is routed through the network nodes by using a tunneling method. A tunneling method allows for a secure means to transmit a data packet through network nodes that have not been confirmed to be trusted network nodes and/or enabled network nodes. For example, if enabled network node B is malfunctioning, it may be necessary to send the data packet from the origination network node (Node A) to the destination network
30 node (Node C) through Node B, Node F, and Node H (i.e. via the A-B-F-H-C path). When doing so, when the data packet reaches Node B, Node B will encrypt the data packet. This allows for the data in the data packet to be secure when the data packet is traveling through

Nodes F and H, which have not been confirmed to be trusted network nodes and/or enabled network nodes. Once the data packet arrives at Node C, which is an enabled network node, Node C decrypts the data in the data packet. In at least one embodiment, a tunneling indicator is added to the header portion (i.e. the routing data portion and/or the security signature portion) of the data packet to indicate that the data packet was routed using the tunneling method in order to securely route the data packet to the destination network node.

FIG. 1E illustrates an embodiment of the disclosed system for geolocating network nodes in attenuated environments for cyber and network security applications that utilizes geotagging and makes use of the IPv6 packet header's 8-bit Next Header field. As previously mentioned above, geolocation information for a network node(s) may be incorporated into the existing structure of the IPv6 data packet header, and specifically may be incorporated into the data packet header's 8-bit Next Header field. The Next Header field specifies the type of the Next Header, and typically specifies the higher-level transport layer protocol used by a data packet's payload. It should be noted that in some embodiments, geotags may be incorporated in other fields of the existing structure of the IPv6 data packet header than the Next Header field. In addition, it should be noted that in one or more embodiments, the disclosed system and method may employ various different types and/or structures of data packet headers than the IPv6 data packet header for the data packet.

FIG. 1F illustrates an embodiment of the disclosed system for geolocating network nodes in attenuated environments for cyber and network security applications, where the data packet is to be routed only through network nodes that are located within a defined geographical region. In one or more embodiments of the disclosed system, an enabled network node is configured to only transmit data packets that the enabled network node receives directly from a verified (or authenticated) network node. In some embodiments, an enabled network node is configured to only transmit (or pass) data packets that have previously traveled only through verified network nodes. In at least one embodiment, an enabled network node is configured to determine which of the network nodes are neighboring network nodes to itself. In one or more embodiments, an enabled network node is configured to determine which of the network nodes in the network are enabled network nodes.

In one example, as illustrated in FIG. 1F, enabled network nodes (i.e. routers) are being used to send a data packet from one user of the disclosed system to a second user. In this example, the user associated with the origination node (Node A) is a primary care physician in the state of

Oklahoma that has been asked by their patient to send test results to a specialist that is associated with the destination node (Node E) to assist in obtaining a proper diagnosis for the patient. For purposes to relay this scenario more completely, it is being assumed that the patient data cannot be sent out of the state of Oklahoma in order to comply with the state's medical records laws.

FIG. 1F shows several different potential pathways between the network nodes (i.e. Node A, Node B, Node C, Node D, and Node E) that provide for multiple routing scenarios of the data packet. As while Node A (i.e. the origination network node) and Node E (i.e. the destination network node) are both located within the state of Oklahoma, when the data packet is routed via any network node (i.e. router) that is located outside of the state of Oklahoma, the medical records laws are violated. In at least one embodiment, the data packet containing the patient test results sent from the primary care physician to their specialist is rejected because on receipt of the data packet at Node E, local enabled hardware at Node E audited the data packet's routed path and identified that the data packet was routed through a network node (Node C) that was located outside of the state of Oklahoma's bounds (i.e. the data packet was routed via Node C). In at least one embodiment, when the local enabled hardware determined that the data packet was routed through a network node located outside of the state's bounds, the data packet was returned to the sender. In another related embodiment, when the local enabled hardware determined that the data packet was routed through a network node located outside of the state's bounds, the data packet was deleted and the originating party at Node A received a notification of the deletion of the data packet and rationale for the deletion. In another embodiment, when the results of the audit by the local enabled hardware showed that the data packet was routed only via network nodes (i.e. routers) that were located inside of the state's bounds, that data packet was accepted.

FIG. 1G illustrates an embodiment of the disclosed system for geolocating network nodes in attenuated environments for cyber and network security applications, where two network nodes (Node A and Node B) are able to receive transmission signals from at least one LEO satellite 198, 199. In this figure, three network nodes (Node A, Node B, and Node C) are shown. Node A and Node B are geotag-capable network nodes (i.e. they are capable of geotagging the data packet with geolocation information related to themselves, but are not capable of verifying (or authenticating) any upstream network nodes and, as such, in this example, have no major processing capability). In one embodiment, Node A and Node B are able to receive transmission signals from LEO satellites 198, 199 that contain information that can be used for their own geolocation.

As a data packet moves through Node A, it is geotagged with at least a portion of the sampled satellite data that Node A receives from satellite 198. And, as the data packet proceeds to move through Node B, it is also geotagged with at least a portion of the sampled satellite data that Node B receives from satellite 199. Then, the data packet continues to proceed on its path to the destination node (Node C). Node C is an enabled node and, thus, has additional processing capabilities such that it is able to process the sampled satellite data obtained by Node A and Node B. Upon analyzing the sampled satellite data, enabled network Node C validates that the data packet indeed traveled through Node A and Node B and verifies (or authenticates) Node A and Node B. In one embodiment, Node C, after validating Node A and Node B in the upstream path, removes the raw appended data in the data packet and attaches a modified or advanced geotag to the data packet, which has the effect of reducing the size of the data packet and/or causing the data packet to be considered to be more secure.

FIG. 2 illustrates the locations of three network nodes 210, 220, 230 being verified by a transmission based authentication system 200 and by the use of ranging information. In this figure, network nodes 210, 220 are router network nodes that are at verified locations. The locations of these network nodes 210, 220 are verified by the use of a transmission based authentication system 200 that employs satellites 240 to transmit at least one authentication signal. Refer to the discussions of FIGS. 3, 4, 5, and 6 for a detailed description of how the transmission based authentication system 200 operates. In this figure, the location of network node 230 is not verified by the transmission based authentication system 200 because network node 230 does not have satellite 240 access. However, the location of network node 230 can be verified by using ranging information through the use of round-trip time delays (i.e., ping delays) that are obtained by transmitting signals to and from network nodes 210, 220 that are at verified locations.

The process for obtaining ranging information for this example is as follows. First, network node 230 transmits a signal (R31) to network node 210 at time t_{1a} . Network node 210 receives the signal (R31) at time t_{3a} , and transmits a return signal (R13) to network node 230 at time t_{3b} . Network node 230 receives the return signal (R13) at time t_{1b} . The delay between network node 210 receiving the signal (R31) and replying with a signal (R13) (i.e. $t_{3b} - t_{3a}$) is known. As such, the round-trip delay (times the speed of light and divided by 2) gives the range between network node 210 and network node 230. This range information can then be used to verify the location of network node 230. Similar computation is used to calculate the range between network node 230 and network node 220. The related network range equations are:

$$R13 = c [(t3a - t1a) + (t1b - t3b)] / 2$$

$$R23 = c [(t3a - t2a) + (t2b - t3b)] / 2,$$

where t is equal to time, and c is equal to the speed of light.

FIG. 3 illustrates an embodiment of a transmission-based authentication system 300 employing a satellite 310 that transmits overlapping spot beams 340 comprising an authentication beam 320, which may also be referred to as “beam zero,” along with one or more guard beams 330. A legitimate network node 360 is shown to be located within the authentication beam 320. A deceptive network node 350 attempts to simulate the location of the legitimate network node 360.

Each location within the guard beams 330 and beam zero 320 receives unique authentication signals from each beam 340 over time. The locations within the regions where the beams 340 overlap receive composite authentication signals. The deceptive network node 350 is not located at the legitimate network node's 360 location and, thus, the deceptive network node 350 will not receive the particular authentication signal 320 that the legitimate network node 360 should receive due to its location. Unless a network node is at its legitimate location, the network node will not receive the correct authentication signal and, as such, an authenticator device cannot verify the location of the network node.

In one or more embodiments, the data transmitted in the spot beams 340 may include an authentication key and/or other pseudo-random code segment that may be used to distinguish data in one of the beams from data in the other beams. The disclosed systems and methods may use other distinguishing beam characteristics and/or data characteristics to distinguish the data between the beams 340. In at least one embodiment, the guard beams 330 may be transmitted at a higher power than beam zero 320 is transmitted. This will cause the signals from the guard beams 330 to shield the beam zero 320 authentication signal.

FIGS. 4A through 4F depict an embodiment where the signal received by one or more network nodes from multiple overlapping spot beams is used to authenticate the location and identity of one or more network nodes. The basic concept is that depending upon where the network nodes are located within the overlapping spot beam pattern, each network node will receive a different composite signal from the combination of signals transmitted from the multiple spot beams. In particular, FIG. 4A shows the disclosed transmission-based authentication system having, for example, four network nodes (i.e., A, B, C, and D) being located at various positions within and near three overlapping spot beams (i.e., Beam 1, Beam 2, and Beam 3). As such, this figure

illustrates the overlapping spot beams illuminating the locations of network nodes A, B, and C. The location of network node D is shown to be just outside the beam pattern.

FIG. 4B illustrates a graph 400 showing exemplary signals (1, 2, and 3) that are transmitted by the three spot beams of FIG. 3A. In particular, this figure shows an exemplary set of signals that are transmitted by each spot beam (Beam 1, Beam 2, and Beam 3), and are used to verify the location of the network nodes. The three curves (indicated by 1, 2, and 3 on graph 400) show the bit sequence over time for the transmitted signals from each spot beam. These three bit sequences are only used to demonstrate the concept. As such, many other types of signals and forms of modulation may also be employed. The signal pattern may also be changed periodically to provide additional protection from deceptive network nodes and/or users and to provide a unique time for when a mobile network node is at a particular location. In addition, these signals that are used to authenticate a network node may be sent separate from a normal signal for brief periods during normal transmission or, alternatively, may be embedded within the normal signal.

FIG. 4C shows an array 410 of the signal strengths of the three spot beams (Beam 1, Beam 2, and Beam 3) at the locations of the four network nodes (A, B, C, and D) of FIG. 4A. In particular, the signal beam received (sbr) array 410 shows the signal strength received by each network node (A, B, C, and D) in the array 410 columns from the signal beam received (Beam 1, Beam 2, and Beam 3) in the rows of the array 410. For example, a network node at location B receives most of the signal from Beam 2, which has a signal strength of 11, compared to signal strengths 2 and 1.5 from Beams 1 and 3, respectively. The characteristics and/or properties of a network node's received signal may be the signature that is used to validate the network node's location.

FIG. 4D depicts an array 420 of bits for the three spot beams (Beam 1, Beam 2, and Beam 3) of FIG. 4A. In this figure, the bits array 420 shows the signal sequence transmitted by each beam (Beam 1, Beam 2, and Beam 3) in the three array rows, as a function of time, which is represented by the sixteen (16) columns of the array 420. Here, to illustrate the concept, the transmitted signals are binary. However, in alternate embodiments, other signal patterns may be employed.

FIG. 4E illustrates an array 430 of the resultant signal sequences that are received by the four network nodes (A, B, C, and D) of FIG. 4A. This figure shows the resultant sequence of composite signals received by the network nodes at locations A, B, C, and D from the multiple overlapping beams. The resultant signal $(rx) = g \times (sbr^T) \times (bits)$, where g equals the gain of each

network node receiver. In this example, gain (g) is chosen to be equal to 0.7 (i.e., $g = 0.7$). The sixteen (16) rows of the received array (rx^T) 430 represent time steps, and the four (4) columns correspond to the different locations (A, B, C and D) of the network nodes. It should be noted that, in this example, the network node at location D receives no signal since this location is outside of the beam pattern.

FIG. 4F shows a graph 440 depicting the resultant signals that are received by the four network nodes (A, B, C, and D) of FIG. 4A. The four curves (indicated by A, B, C, and D) show the time sequence of the resultant signals that are received by network nodes at locations A, B, C, and D. The four resultant composite signals provide unique network node location identification for the four network nodes (A, B, C, and D), respectively.

FIG. 5 illustrates an embodiment of the transmission-based authentication system 500 using guard beam transmission as part of a secondary mission. In this embodiment, at least one guard beam is used to transmit legitimate data as part of a secondary mission for the satellite 510. For example, a guard beam could be used to broadcast regional information, such as differential GPS network corrections that are valid in the guard beam footprint. However, it should be noted that for higher security this is not the preferred embodiment because the regional information is more likely to be able to be determined by a spoofer than a more random signal. As another example, the guard beam could be used to transmit data that is relevant to the primary mission (i.e., the authentication signal) and/or relevant to a secondary mission.

As shown in FIG. 5, the authentication signals may be transmitted in bursts. The authentication signals may be randomly sent in bursts, in beam zero or in alternating beams (including beam zero and guard beams), so that the timing of the authentication signals indicates the location of the network node. As such, if a network node receives multiple bursts, then the network node is located within beam zero or within a beam overlapping region.

In alternative embodiments, the authentication signals may be embedded in the normal data transmission in order to minimize their impact on satellite transmission power and/or bandwidth. The authentication signals may be embedded in the data transmission by various ways (e.g., time, frequency, polarization shifts, etc.) that do not impact normal reception, but are detectable by special processing.

In one or more embodiments, the authentication signals may be embedded in normal data transmission by varying broadcast power on a bit-by-bit basis. For these embodiments, the guard beam bit modulation changes the broadcast power of the transmitted bits on a bit-by-bit basis.

This prevents a spoofer from attempting to observe the bits in their local guard beam, and processing the data to remove them.

For example, a spoofer makes a series of measurements (m):

95 105 105 -105 105 -105 95 -105 -95 -95

5 The spoofer might guess that the guard signal (g) was sign(m):

1 1 1 -1 1 -1 1 -1 -1 -1

And, the signal the spoofer is trying to access is $\text{sign}(m - \text{sign}(m) * 100)$:

-1 1 1 -1 1 -1 -1 -1 1 1

10 If instead of a fixed power signal, the guard beam broadcast power was modulated such that its component of the received signal was:

107 97 91 -93 99 -91 93 -107 -107 -101

Then, the signal the spoofer would receive would be:

102 102 96 -98 104 -96 88 -112 -102 -96

15 It would be much more difficult for the spoofer to try to figure out the authentication signal from that set of measurements.

In addition, it should be noted that an extension of that same idea would be to add a small random quadrature phase shift keying (QPSK) signal onto the guard band signal. For this case, the guard signal could still be used to transmit useful information.

20 FIG. 6 shows the transmission-based authentication system 600 employing out-of-phase binary phase shift keying (BPSK) guard beam transmission. Specifically, in this figure, the guard beams transmit the authentication signal using out-of-phase BPSK signals between adjacent overlapping beams. The signal in the overlap region will then be a QPSK signal. The unique location of a network node within a beam can then be determined by analyzing the signal phasing and signal type that the network node receives.

25 In alternative embodiments, a secondary signal source may be used to provide additional shielding transmissions. For example, a second satellite could broadcast guard beams for the outside beams of a first satellite.

FIG. 7 illustrates an embodiment of the disclosed system 700 having a network node 710 that is able to perform in an occluded or jammed environment. In particular, FIG. 7 shows a network

node 710 receiving RF signals 709, 705, 707 from two satellites 706, 704 and a cellular tower 708. In one example, the RF signals 709, 705, 707 are down-converted, sampled, optionally encrypted, and appended to security-enhanced data packets that are routed through the network node 710. In another example, data is extracted from the RF signals 709, 705, 707. The
5 extracted data is optionally encrypted and appended to security-enhanced data packets that are routed through the network node 710. Examples of various types of RF signal sources that may be employed by the disclosed system include, but are not limited to, LEO satellites (e.g., Iridium satellites), GPS satellites (e.g., transmitting GNSS signals), and cellular towers.

Although certain illustrative embodiments and methods have been disclosed herein, it can be
10 apparent from the foregoing disclosure to those skilled in the art that variations and modifications of such embodiments and methods can be made without departing from the true spirit and scope of the art disclosed. Many other examples of the art disclosed exist, each differing from others in matters of detail only. Accordingly, it is intended that the art disclosed shall be limited only to the extent required by the appended claims and the rules and principles of
15 applicable law.

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,
 - 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.

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

5 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.

10 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
15 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.

20 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.

25 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 the at least one enabled network node is configured to determine which of the network nodes are enabled network nodes.

12. The system of any one of claims 1-11, 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.

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

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 a security signature portion which includes geolocation information relating to at least one of the network nodes the data packet has traveled through ; 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.
15. The method of claim 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.
16. The method of claim 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.

17. The method of claim 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.

18. The method of claim 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.

19. The method of any of claims 15-18, 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.

20. The method of claim 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.

21. The method of claim 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.

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

23. The method of claim 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.

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