

SPOT BEAM BASED AUTHENTICATION OF A SATELLITE RECEIVER

RELATED APPLICATIONS

[0001] None

5

BACKGROUND

[0002] The subject matter described herein relates to electronic communication and network security, and more particularly to authentication techniques which may be used in satellite based systems for reducing system vulnerabilities.

[0003] Electronic security and network security remain an important
10 infrastructural elements as electronic communication and data transmittal systems including networks become more engrained into society. Such systems are utilized for extensive data processing and general processes through the web and other networks whose vulnerability threatens our national infrastructure. Both foreign and domestic efforts to infiltrate, compromise, and/or disable infrastructural elements are increasing
15 and thus there is a need to bolster computing security in order to protect these systems from these growing threats. Access of these systems by an unauthorized party, may have varying degrees of societal impact and while any given attack may seem to be less significant in nature, it could be the predecessor to a more aggressive future attack. Electronic systems world-wide are seeing a dramatic increase in cyber attacks. Cyber
20 attacks often stem from network vulnerabilities and are often conducted by impersonating a legitimate end user.

[0004] Existing methods to detect unauthorized users or compromised electronic systems are lacking, in that, even if an attack is discovered the culprit's methods may hide where the unauthorized access originated from. This issue creates additional

problems in that if the attack is believed to have originated in, for instance, a foreign country, the inability to validate the general vicinity of the unauthorized user, means that officials may not be able to seek amends or more aggressively pressure foreign countries for conducting such cyber attacks on the United States.

5 [0005] Existing identity verification methods are, in general, non-dynamic, such as passwords, pins, etc. that leave systems more vulnerable to interception and other brute force hacking methods.

[0006] Accordingly, additional techniques used to restrict access to unauthorized users as well as techniques to authenticate one or more parties attempting to access
10 electronic communication or networks could strengthen these existing system's security.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The detailed description is described with reference to the accompanying figures.

[0008] Fig. 1 is a schematic illustration of a satellite-based communication
5 system, according to embodiments.

[0009] Figs. 2A, 2B and 2C are schematic illustrations of satellite-based authentication systems, according to embodiments.

[0010] Fig. 3A is a schematic illustration of a computing device which may be adapted to implement a satellite based authentication system, according to
10 embodiments.

[0011] Fig. 3B is a schematic illustration of a satellite-based communication system, according to embodiments.

[0012] Fig. 4 is a flowchart illustrating operations in a method to authenticate a claimant, according to embodiments.

15

SUMMARY

[0012a] According to a first aspect, there is provided a method to authenticate a claimant comprising: receiving, from the claimant, at least one set of data that has been captured by the claimant from at least one spot beam transmission wherein the data comprises a pseudo-random number and a time stamp associated with the data; further receiving, from the claimant, at least one location identifier; comparing the location identifier and the at least one set of data to a known valid data set, including comparing the location identifier with a known location for the spot beam at a time corresponding to the time stamp; and authenticating the claimant when a difference between the claimant data and the valid data set is less than a threshold.

[0012b] According to a second aspect, there is provided an apparatus to authenticate a claimant, comprising: a processor; and a memory module comprising logic instructions which, when executed, configure the processor to operate in accordance with the first aspect.

[0012c] According to a third aspect, there is provided a system to authenticate a claimant, comprising: at least one signal source to transmit a spot beam in accordance with a known spot-beam geometry; at least one electronic device comprising a receiver to receive at least one set of data from the spot beam transmission wherein the data comprises a pseudorandom number and a time stamp associated with the data, wherein the at least one electronic device is able to determine its location; and at least one verifier communicatively coupled to the at least one electronic device to authenticate a claimant comprising the electronic computing device, wherein the at least one verifier comprises a processor and a memory module, the memory module comprising logic instructions which, when executed, configure the processor to: receive, from the electronic device, the at least one set of data that the electronic device captured from the spot beam transmission; further receive, from the electronic device, at least one location identifier determined by the electronic device; compare the location identifier and the at least one set of data to a known valid data set, including comparing the location identifier with a known location for the spot beam at a time corresponding to the time stamp; and authenticate the claimant when a difference between the electronic device data and the valid data set is less than a threshold.

[0013] Described herein are an apparatus, systems, and methods for spot beam based authentication. In one or more embodiments, a method to authenticate a claimant involves a satellite transmitting distinctive beam data via a spot beam, a claimant
5 capturing said data from said satellite transmission, a claimant transmitting the data to a verifier which may include the use of a mediatory means of data transmission, the verifier then authenticating the claimant when the difference between the claimed data and the known valid data set is within a defined threshold. In one or more
10 embodiments, the claimant is provided access to a system or resource once they have been authenticated via this "one-way" authentication method. In one or more
embodiments, a third party verifier may complete authentication of the claimant for a host network. In one or more embodiments the claimant may have a device that is
capable of both receiving data and transmitting data, whereas in alternative
embodiments the two functionalities may be housed in separate pieces of hardware
15 coupled together.

[0014] In one or more embodiments, the data may be invalidated and the claimant is denied access. In one or more embodiments, the data may be marked as uncertain and may require additional data to authenticate the claimant. In one or more
embodiments, the data may be marked as uncertain based on assigned tolerance levels
20 and may either be promoted to authenticated or demoted to restricted. In one or more
embodiments the claimant may transmit additional identifiers to the verifier for use in authentication which may include one of the following: satellite identifying information,
other claimant captured data or derived information including location identifiers (e.g. earth-based coordinates, etc.), time, a pseudo-random code segment (i.e. an

authentication key), and claimant distinctive data (e.g. passwords, keys, security certificates, etc.). As used herein the term "liveness" refers to these types of identifiers. In one or more embodiments, the authentication key may be transmitted through the spot beam and varied within the spot beam geometry as a function of time so that codes
5 from varying spot beams are managed such that resultant optimum correlation properties are maintained. It is well understood in the art that multi-phased antenna arrays can be used to generate dynamic spot beams and thus, in at least one embodiment, a multi-phased antenna array may be used to generate the spot beams. In one or more embodiments, the claimant may transmit at least one waypoint datum to
10 the verifier where this waypoint datum may be captured while the claimant may be mobile. In at least one embodiment, the waypoint datum may be captured while the claimant is at least at one point in time, stationary.

[0015] In at least one embodiment, beyond the one-way client authentication method, a multi-way authentication method is used for electronic computing devices to
15 authenticate themselves to one another (i.e. two-way authentication, three-way authentication, and so on). An electronic computing device(s) may include a mobile phone, a portable computing device, a computer network node, a server, or a wireless networking node, etc. This method may be used for wireless and/or wired networks. This method allows devices to authenticate themselves to other devices, and may allow
20 such devices to determine the degree or otherwise the extent of access to information and/or services that are granted after successful authentication. A service may include access to information such as secured networks (e.g. online banking, etc), secured databases, company email and other task oriented services, etc. or other secured resources included those tied into wired, wireless, and/or ad hoc networks.

Furthermore, the degree or extent of access may also be context specific to one or more of the devices in this multi-way authentication method.

[0016] In at least one embodiment an apparatus to authenticate a claimant, comprises a processor and a memory module comprising logic instructions which, when
5 executed, configure the processor to receive, from the claimant, at least one location identifier provided by the claimant and at least one set of waypoint data captured by the claimant from a satellite beam transmission, compare the at least one location identifier and the at least one set of waypoint data to a known valid data set, and authenticate the claimant when a difference between the at least one location identifier and the at least
10 one set of waypoint data and the known data set is within a defined threshold.

[0017] In at least one embodiment, a system to authenticate a claimant comprises at least one low earth orbiting satellite to transmit a satellite beam in accordance with a known spot-beam geometry, at least one electronic device comprising a receiver to receive at least one set of waypoint data from the satellite
15 beam and a location sensor to determine a location of the electronic device, and at least one verifier communicatively coupled to the at least one electronic device to authenticate a claimant using the location determined by the electronic device, the at least one set of waypoint data, and a known data set.

DETAILED DESCRIPTION

[0018] In the following description, numerous specific details are set forth to provide a thorough understanding of various embodiments. However, it will be understood by those skilled in the art that the various embodiments may be practiced without the specific details. In other instances, well-known methods, procedures, components, and elements have not been illustrated or described in detail so as not to obscure the particular embodiments.

[0019] Entity or user authentication techniques enable a third party verifier to validate the identity of a user, asset, or a device (e.g., a claimant) for a remote resource through a one-way authentication method. However, it should be noted that this one-way method may also be used directly by a host system to validate a claimant. An entity may be a device (e.g., a mobile phone, computer, server, or the like) or asset that needs to be tracked, while a user can be a person or other living/non-living entity. An entity and/or user may be authenticated for the duration of an entire connection or session. The entity and/or user may require re-authentication after the original authentication. The re-authentication requirements may be defined by the host network and may be context specific. Alternatively, this system may be used for a message-based authentication system which requires a separate authentication process for each message. Techniques described herein may be used for either session-based authentication, message-based authentication, or a combination thereof.

[0020] Additionally, this method may be applied to receiving devices themselves, such that the one-way authentication does not have to be completed by a remote third party but rather by one or more of the receiving devices. When this method is conducted by a single device it is still considered a one-way authentication method.

However; this method can also be applied in a multi-way authentication technique to allow at least two peer devices to authenticate each other. In this one-way or multi-way device to device authentication method, authentication may generally rely on a shared secret (symmetric and asymmetric) that each of the two legitimate receiving devices know and any unauthorized or rogue receiving device does not know. Each device may have a unique authentication credential such as a secret password shared between itself and the peer device or public/private key pairs in the form of security certificates. A device has authenticated itself when it proves, to the satisfaction of the other peer device, that it knows the shared secret, and is, therefore, legitimate. Once authentication is complete between the at least two devices in this multi-way authentication method, the devices have proven their identities to one another. The devices may then create their own authenticated network which they may choose to implement cyber security policies which have been agreed on so as to protect the communication and access to networked resources for a given context.

[0021] Existing authentication methods may be used or combined to generate the initial-security key(s). The initial-security key may, for example, be cooperatively generated using Diffie-Hellman techniques or may simply be generated by one peer device and sent to the other via an alternate secure channel/process.

[0022] In any case, accompanying the initial-security key may include some shared liveness information (as previously defined). In this application, the liveness information is provided through a satellite spot beam and may include such parameters for use in authentication as a timestamp and pseudo-random number (PRN).

[0023] The use of the shared liveness information may be used in the derivation allowing for different security keys to be used every time the initiating device

authenticates itself to the peer device. This prevents a potential rogue eavesdropper from initiating a statistical attack every time the initiating device is authenticated, adding newly intercepted messages to its analysis of messages intercepted during the initiating device's previous sessions. The liveness information and the initial-security key may
5 then be passed as inputs to a determinative function. As used herein the term "determinative" refers to a function for which the outputs of the function are completely determined by the inputs. This determinative function may be run separately on the initiating device and on the peer device. If these two devices were to produce different outputs when they ran the determinative function, then the security keys derived from
10 the function would not match, the device could not be authenticated, and thus could not be used for intercommunication.

[0024] In addition to being determinative, for security's sake the function should be inherently irreversible. Knowing the function's outputs, it should be very difficult or impossible to determine its inputs. Hashes form a class of functions that are both
15 determinative and inherently irreversible and, as such, are often used in encryption and authentication calculations. Pseudo-random function (PRF) used with the well known Transport Level Security (TLS) protocol are an example of the determinative function implementation which may be used.

[0025] PRF combines the results of two well known hash functions, Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm 1 (SHA-1). PRF uses two hash
20 functions in order to preserve security just in case someone determines how to reverse one of the two hash functions. These two hash functions produce outputs that may be too short to be optimum for security. SHA-1 produces 20-byte outputs, and MD5 produces 16-byte outputs. Therefore, for each of the two hash functions, a "data

expansion function" may be defined that uses the hash function to produce output of arbitrary length. For SHA-1, the data expansion function may be defined as P_SHA-1:

EQ 1: $P_SHA-1(\text{initial-security key, liveness}) = SHA-1(\text{initial-security key, } A(1) + \text{liveness}) + SHA-1(\text{initial-security key, } A(2) + \text{liveness}) + SHA-1(\text{initial-security key, } A(3) + \text{liveness}) + \dots$

where $A(0) = \text{liveness}$;
 $A(i) = SHA-1(\text{initial-security key, } A(i - 1))$;
 and the "+" sign indicates string concatenation.

[0026] The definition of the data expansion function P_MD5 is similar to the above definition with "MD5" replacing "SHA-1" wherever it appears. The data expansion functions may be iterated to as many steps as necessary to produce output of a desired length. The desired output length may be set as an implementation option.

In at least one embodiment, the desired output length for each hash function is 128 bytes. P_SHA-1 may be iterated out to A(7) for a total output length of 140 bytes (each iteration increasing the output length by 20 bytes). The output may then be truncated to 128 bytes. Each iteration of P_MD5 produces 16 bytes, so iterating it out to A(8) produces the desired 128 bytes with no truncation.

[0027] In one embodiment for spot beam based authentication, having chosen the hash functions and iterated their data expansion functions out to the desired output length, PRF takes as inputs the expanded initial-security key, a label (a pre-determined ASCII string), and the liveness information exchanged. PRF is defined to be the exclusive bit-wise OR (XOR) of the output of the two hash data expansion functions, P_MD5 and P_SHA-1:

EQ: 2 $PRF(\text{expanded initial-security key, label, liveness}) = P_MD5(S1, \text{label} + \text{liveness}) \text{ XOR } P_SHA-1(S2, \text{label} + \text{liveness})$

[0028] where S1 is the first half of the expanded initial-security key, measured in bytes, and S2 is the second half of the expanded initial-security key. (If the expanded initial-security key's length is odd, then its middle byte is both the last byte of S1 and the first byte of S2). As P_MD5 and P_SHA-1 are iterated to produce 128-byte outputs, the
5 output of PRF is also 128 bytes.

[0029] The 128-byte output of PRF is divided into four 32-byte session security keys. Then each of the session security keys and truncates it to the length required by the authentication and encryption protocols being used. The truncated result is one of the new set of transient session security keys. The derivation of the transient session
10 security keys allows for both the initiating device and peer device to not directly use either the initial-secret key or the expanded initial-security key in order to minimize, or at least to reduce, the leakage of the security key information. The derivation of the transient session security keys also allows for the initiating device and the peer device to refresh the session security keys derived from the expanded initial-security key at
15 regular intervals or when commanded to prevent statistical analysis by limiting the use of the session security keys.

[0030] Each of the authentication and encryption transient session security keys have the following specific purpose: i) encryption of data exchanges, for confidentiality, from initiating device to peer device; ii) encryption of data exchanges, for confidentiality,
20 from peer device to initiating device; iii) signing of data exchanges, for integrity, from initiating device to peer device; and iv) signing of data exchanges, for integrity, from peer device to initiating device.

[0031] Derivation of the initial-security key for the spot beam based authentication may use Diffie-Hellman techniques using agreed upon and well known

public primitive root generator "g" and prime modulus "p". The initiating device and the peer device each choose a random secret integer and exchange their respective $((g^{\text{secret integer}}) \bmod p)$. This exchange allows the initiating device and peer device to derive the shared initial-secret key using Diffie-Hellman.

5 **[0032]** Having derived the initial-secret key that is shared between both the initiating device and the peer device they may use the data expansion to derive the expanded initial-secret using, for example, the P_SHA-1. The liveness information for the data expansion process may be a known random value or timestamp that is agreed upon by the initiating device and the peer device. In some embodiments, the peer
10 device may select a random value and transmit it to the initiating device via the satellite or the terrestrial network. Alternatively, both the initiating device and the peer device may agree upon a timestamp, since they are tightly time synchronized, and thereby avoid data exchanges while being able to select liveness from the shared/common timestamp value.

15 **[0033]** Following this the initiating device and the peer device have a shared expanded initial-secret key that may be used to derive the new set of transient session security keys. Again for liveness the initiating device and the peer device may use either a shared random value that is transmitted by the peer device or a shared/common timestamp value. The transient session security keys may be used by
20 initiating device and the peer device for further encryption and signing of geolocation and other context information exchanges between initiating device and peer device. Geolocation and other context information is considered confidential and hence it is required that such information be encrypted to ensure that only the authenticated initiating device and peer device can extract the exchanged geolocation and context

information. Note that the geolocation is authenticated by the procedure described in this patent application using pseudorandom (PRN) code segments and distinctive beam parameter. The context information shared may include other state or control information for targeted cyber defense application execution or decision support systems. In addition to encryption the integrity of the exchanged geolocation and context information is ensured by the use of the transient session security keys for signing purposes as discussed earlier.

[0034] In brief overview, in some embodiments the authentication systems and methods described herein may leverage geolocation techniques for determining the position of the claimant as part of the authentication process. One such geolocation technique is defined in commonly assigned and copending U.S. Patent Application Serial No. 12/756961, entitled Geolocation Leveraging Spot Beam Overlap, the disclosure of which is incorporated herein by reference in its entirety. When authentication is required, the claimant device may capture and transmit the distinctive signature parameters to a verifying device. In addition, the claimant device may transmit its claimed travel path (i.e., waypoint(s) and time at each). Waypoints may be transmitted whether the device is stationary or mobile. A verification device may use the claimant's claimed beam signature parameters, at least one location waypoint, and at least one time associated with this waypoint and beam parameter capture to authenticate the claimant. For example, a claimant may be considered authenticated by the verifier if the beam parameters captured from the at least one spot beam and the at least one claimed waypoint are affirmed against a known valid data set. In this manner, the claimant can be authenticated as being within a region at a particular time. The composite code based on these parameters provide a signal that is extremely difficult to emulate, hack, or spoof. Furthermore, the signal structure and satellite's

received signal power allows for the authentication to be used indoors or other attenuated environment. This improves the overall utility of this system approach.

[0035] The subject matter of this application is described primarily in the context of low-earth orbiting (LEO) satellites such as those implemented by Iridium satellites.

5 However, one skilled in the art will recognize that the techniques described here are readily applicable to other satellite systems, e.g., medium-earth orbit (MEO) satellite systems or geosynchronous orbit (GEO) satellite systems. Such satellite based communication systems may include or utilize other mobile communication systems, e.g., airborne communication systems or the like, as well as, stationary communication
10 platforms including but not limited to a ship or a cell phone tower.

[0036] Fig. 1 is a schematic illustration of a satellite-based communication system 100, according to embodiments. In practice, a satellite based communication system 100 may comprise of at least one satellite 110 in orbit. In the interest of brevity, a single satellite is illustrated in Fig. 1. Referring to Fig. 1, in some embodiments a
15 system 100 comprises one or more satellites 110 in communication with one or more receiving devices 120. In some embodiments the satellites 110 may be embodied as LEO satellites such as those within the Iridium satellite constellation. Satellite(s) 110 orbit the earth in a known orbit and may transmit one or more spot beams 130 onto the surface of the earth in a known pattern. Each spot beam 130 may include information
20 such as pseudorandom (PRN) data and one or more distinctive beam parameters (e.g. time, satellite ID, time bias, satellite orbit data, etc.).

[0037] Receiving device(s) 120 may be implemented as communication devices such as satellite or cellular phones or as components of a communication or computing device, e.g., a personal computer, laptop computer, personal digital assistant or the like.

In some embodiments, a receiving device (120) may comprise one or more locating or navigation devices or modules analogous to devices used in connection with the global positioning system (GPS).

[0038] Figs. 2A, 2B, and 2C are schematic illustrations of satellite-based authentication systems 200, according to embodiments. Referring first to Fig. 2A, in some embodiments a satellite 110 in orbit transmits one or more spot beams 130 onto the earth's surface. A receiving device 120 may be configured to receive a signal from the spot beam. In the embodiment depicted in Fig. 2A the receiving device is ground-based and may be operating in attenuated environment. By way of example, an object 210 such as a roof, building, or the like may obstruct a portion of the communication path between satellite 110 and the receiving device.

[0039] A transmitter 220 transmits data received by the receiving device 120 and/or data generated by the receiving device 120 to a verifier 230. The transmitter 220 depicted in Fig. 2 is a wireless transmitter that relays the data from the receiving device to the verifier. However, one skilled in the art will recognize that data from receiving device 120 may be transmitted via a wired communication system, wireless communication system, or a combination of wired and wireless systems. The verifier 230 uses data captured via a spot beam by the receiving device 120 to prove to the verifier 230 that it is an authorized user via a one-way authentication approach which is also the case in Fig. 2B.

[0040] Furthermore, Fig. 2B depicts an arrangement in which the receiving device 120 may be airborne, e.g., in an aircraft 125. In the embodiment depicted in Fig. 2B the aircraft 125 may maintain an uplink with the satellite 110, e.g., an L-Band Uplink, and data captured by the receiving device 120 in the aircraft may be transmitted back to

the satellite 110 via the uplink. The satellite 110 may transmit the data to a second cross-linked satellite 110, which in turn may transmit the data to a verifier 230.

[0041] The system depicted in Fig 2C illustrates an embodiment in which two (or more) peer devices 120 may implement a two-way authentication technique to authentication each other. Referring briefly to Fig. 2C as described above a satellite 110 in orbit transmits one or more spot beams 130 onto the earth's surface. A first receiving device 120A may be configured to receive a signal from the spot beam. The first receiving device 120A may be configured to derive a security key, e.g., using a Diffie-Helman approach as described above, which incorporates PRN data from the spot beam.

[0042] The PRN data is also transmitted to a second device 120B. In some embodiments the second device 120B may be outside the spot beam 130, in which case the PRN data may be transmitted by a computing device 240 coupled to the second device 120B via a communication network. The computing device 240 may be communicatively coupled to the satellite 110. By way of example, and not limitation, the computing device 240 may be a server that is separately coupled to the satellite 110 via a communication link. The computer 240 may be associated with a control network for satellite 110 and may thereby possess PRN data associated with the spot beam 130.

[0043] In operation, the first receiving device 120A initiates a request for authentication data, which is transmitted to the second receiving device 120B. The communication link between the first receiving device 120B may be direct or may be implemented through a transmit network 220. The second receiving device 120B responds to the request and issues a near-simultaneous request for authentication data from the first receiving device 120A. The first receiving device 120A authenticates the

second receiving device 120B and issues a near-simultaneous response to for authentication data to the second receiving device 120B, which may then authenticate the first receiving device 120A.

[0044] As described above, the authentication process implemented between the first receiving device 120A and the second receiving device 120B may be a Diffie-Hellman exchange in which the shared secret comprises at least a portion of the PRN data transmitted by the spot beam 130. Thus, the system depicted in Fig. 2C enables peer-to-peer authentication of receiving device 120A, 120B. One skilled in the art will recognize that this two-way authentication approach could be extended to a receiving device and a server as well as other hardware architectures, or to more than two devices.

[0045] Fig. 3 is a schematic illustration of a computing system which may be adapted to implement a satellite based authentication system, according to embodiments. For example, in the embodiments depicted in Figs. 2A and 2B the verifier 230 may be implemented by a computing system as depicted in Fig. 3. Referring to Fig. 3, in one embodiment, system 300 may include a computing device 308 and one or more accompanying input/output devices including a display 302 having a screen 304, one or more speakers 306, a keyboard 310, one or more other I/O device(s) 312, and a mouse 314. The other I/O device(s) 312 may include a touch screen, a voice-activated input device, a track ball, and any other device that allows the system 300 to receive input from a user.

[0046] The computing device 308 includes system hardware 320 and memory 330, which may be implemented as random access memory and/or read-only memory. A file store 380 may be communicatively coupled to computing device 308. File store

380 may be internal to computing device 308 such as, *e.g.*, one or more hard drives, CD-ROM drives, DVD-ROM drives, or other types of storage devices. File store 380 may also be external to computer 308 such as, *e.g.*, one or more external hard drives, network attached storage, or a separate storage network.

5 **[0047]** System hardware 320 may include one or more processors 322, at least two graphics processors 324, network interfaces 326, and bus structures 328. In one embodiment, processor 322 may be embodied as an Intel ® Core2 Duo® processor available from Intel Corporation, Santa Clara, California, USA. As used herein, the term "processor" means any type of computational element, such as but not limited to, a
10 microprocessor, a microcontroller, a complex instruction set computing (CISC) microprocessor, a reduced instruction set (RISC) microprocessor, a very long instruction word (VLIW) microprocessor, or any other type of processor or processing circuit.

[0048] Graphics processors 324 may function as adjunct processors that manage
15 graphics and/or video operations. Graphics processors 324 may be integrated onto the motherboard of computing system 300 or may be coupled via an expansion slot on the motherboard.

[0049] In one embodiment, network interface 326 could be a wired interface such as an Ethernet interface (see, *e.g.*, Institute of Electrical and Electronics
20 Engineers/IEEE 802.3-2002) or a wireless interface such as an IEEE 802.11a, b or g-compliant interface (see, *e.g.*, IEEE Standard for IT-Telecommunications and information exchange between systems LAN/MAN--Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, 802.11G-2003). Another example of

a wireless interface would be a general packet radio service (GPRS) interface (see, e.g., Guidelines on GPRS Handset Requirements, Global System for Mobile Communications/GSM Association, Ver. 3.0.1, December 2002).

[0050] Bus structures 328 connect various components of system hardware 128.

5 In one embodiment, bus structures 328 may be one or more of several types of bus structure(s) including a memory bus, a peripheral bus or external bus, and/or a local bus using any variety of available bus architectures including, but not limited to, 11-bit bus, Industrial Standard Architecture (ISA), Micro-Channel Architecture (MSA), Extended ISA (EISA), Intelligent Drive Electronics (IDE), VESA Local Bus (VLB), Peripheral
10 Component Interconnect (PCI), Universal Serial Bus (USB), Advanced Graphics Port (AGP), Personal Computer Memory Card International Association bus (PCMCIA), and Small Computer Systems Interface (SCSI).

[0051] Memory 330 may include an operating system 340 for managing operations of computing device 308. In one embodiment, operating system 340
15 includes a hardware interface module 354 that provides an interface to system hardware 320. In addition, operating system 340 may include a file system 350 that manages files used in the operation of computing device 308 and a process control subsystem 352 that manages processes executing on computing device 308.

[0052] Operating system 340 may include (or manage) one or more
20 communication interfaces that may operate in conjunction with system hardware 120 to transceive data packets and/or data streams from a remote source. Operating system 340 may further include a system call interface module 342 that provides an interface between the operating system 340 and one or more application modules resident in memory 330. Operating system 340 may be embodied as a UNIX operating system or

any derivative thereof (e.g., Linux, Solaris, etc.) or as a Windows® brand operating system, or other operating systems.

[0053] In various embodiments, the computing device 308 may be embodied as a personal computer, a laptop computer, a personal digital assistant, a mobile telephone,
5 an entertainment device, or another computing device.

[0054] In one embodiment, memory 330 includes an authentication module 362 to authenticate a claimant based on data received from the claimant. In one embodiment, an authentication module 362 may include logic instructions encoded in a non-transitory computer-readable medium which, when executed by processor 322,
10 cause the processor 322 to authenticate a claimant based on data received from the claimant. In addition, memory 330 may comprise a satellite orbit database 364 which includes orbit information for satellites 110 in a predetermined orbit around the earth. Additional details about the authentication process and operations implemented by authentication module 362 are described below.

[0055] In some embodiments the receiving device 120 may be implemented as a satellite communication module adapted to couple with a conventional computing device 122 (e.g., a laptop, a PDA, or a smartphone device). The receiving device 120 may be coupled to the computing device 122 by a suitable communication connection, e.g., by a Universal Serial Bus (USB) interface, an RS-232 interface, an optical
20 interface, or the like. In the embodiment depicted in Fig. 3B the receiving device 120 may be a “thin” device in the sense that it may include a receiver and limited processing capability, e.g., an application specific integrated circuit (ASIC) or a field programmable gate array (FPGA) configured to implement an authentication routine.

[0056] In operation, a user of the computing device 122 may utilize the receiving device 120 to authenticate the computing device 122 with a host network 390. As described above, the receiving device 120 depicted in Fig. 3 may receive a spot beam transmission 130 from the satellite 110 which includes a distinctive beam signature and a pseudo-random number (PRN). The computing device 122 may initiate an access request to the host network 390. The access request may include user specific information, e.g., a user ID, one or more coordinates from an earth-based coordinate system (e.g., a zip code, an area code, a latitude/longitude, a Universal Transverse Mercator (UTM); an Earth-Centered Earth-Fixed (ECEF), a World Geographic Reference System (GEOREF), or other miscellaneous system, for example, a zip code) and at least a portion of the PRN data received from the satellite 110.

[0057] The host network 390 may transmit a user access request to the verifier 230 as an authentication request. In some embodiments the host network may add additional information to the request to enable the verifier 230 to authenticate the computer 122. By way of example, the host network 390 may provide limitations regarding where (i.e., from what geographic locations) the claimant may be authenticated). The verifier 230 may verify the claimant and provide an authentication response to the host network 390. The host network 390, in turn, may forward an access response to the computing device 122.

[0058] Fig. 4 is a flowchart illustrating operations in a method to authenticate a claimant, according to embodiments. Referring to Fig. 4, at operation 410 a claimant device determines a physical location of the claimant device. In some embodiments a claimant device 120 may comprise one or more location modules to determine a location of the claimant device 120. By way of example and not limitation, claimant

device 120 may include, or be communicatively coupled to, a global positioning system (GPS) module to determine a location based on signals from the global positioning system. Alternatively, or in addition, claimant device 120 may include logic to determine a location based on signals from one or more LEO or MEO satellites 110 as described
5 in one or more of U.S. Patent Nos. 7,489,926, 7,372,400, 7,579,987, and 7,468,696, the disclosures of which are incorporated herein by reference in their respective entireties. In some embodiments the location of the claimant device 120 may be expressed in latitude/longitude coordinates or another earth-based coordinate system.

[0059] At operation 415 the claimant device 120 receives a spot beam
10 transmission from a satellite 110. In some embodiments the claimant device 120 extracts one or more distinctive beam parameters (e.g. time, satellite ID, beam ID, time bias, satellite orbit data, etc.) including a pseudo random code segment from the satellite spot beam. In some embodiments the claimant device 120 may store the beam parameters in a memory module in, or communicatively coupled to, the claimant device
15 120. In one or more embodiments operation 415 may occur near simultaneously to its preceding operation 410.

[0060] At operation 420 the claimant device 120 may continue to generate one or more waypoint data snapshots which may include the location information for the claimant device 120 from operation 410, and one or more of the distinctive beam
20 parameters transmitted via the satellite spot beam as noted in operation 420. In some embodiments the waypoint data snapshots may be stored in a memory module in, or communicatively coupled to, the claimant device 120.

[0061] In some embodiments the claimant device 120 may collect an array of waypoint data snapshots over time. For example an array of waypoint data snapshots

may be constructed by receiving spot beams from a plurality of satellites 110 passing over the claimant device 120 over time. Alternatively, or in addition, an array of waypoint data snapshots may be constructed by moving the claimant device 120 in relation to the satellites 110, for example by placing the claimant device 120 in an aircraft 125 as depicted in Fig. 2B. An additional example would include a claimant device which acts as a tracker to validate the traveled route of an entity or asset which may include dangerous materials. The claimant device may be polled to provide waypoint data to verify the expected path matches that of the actual. The claimant device may be polled randomly.

10 [0062] At operation 420 the waypoint data snapshot(s) are transferred from the claimant device 120 to a verifier device 230. By way of example, in the embodiment depicted in Fig. 2A the waypoint data snapshot(s) may be transmitted via a transmitter 220 or by another communication network. In the embodiment depicted in Fig. 2B the waypoint data snapshot(s) may be transmitted from the aircraft 125 to a satellite 110, 15 then may be transmitted via a satellite network to a verifier device 230.

[0063] At operation 425 the verifier device 230 receives location data and waypoint data from the claimant device 120. At operation 430 the verifier device 230 compares the location information and the waypoint data to corresponding data in a known valid data set in order to authenticate the claimant. By way of example, a LEO 20 satellite such as the Iridium satellite constellation circumnavigates the earth in a known orbit, the approximate parameters of which are available well in advance. A verifier device 230 may include a satellite orbit database 364, or be communicatively coupled to a satellite orbit database 364, which includes orbit information about satellites 110 in a known orbit about the earth.

[0064] In some embodiments the location data and waypoint data received from the claimant device is compared (operation 430) with location and waypoint data from the known data set to determine whether the claimant device 120 is, in fact, within a reasonable threshold distance of an expected geographic location at an expected time.

5 By way of example and not limitation, the satellite orbit database 364 may be searched for a data record corresponding to the distinctive beam parameters transmitted from the claimant device 120. When a matching record is located, the orbit data from the record retrieved from the orbit database 364 may be compared to the data received from the claimant device 120. For example, the known data may comprise a coordinate for the
10 center of the spot beam 130 and an indication of the radius of the spot beam 130 on the surface of the earth. The coordinates received from the claimant device 120 may be compared to the location of the spot beam to determine whether the received data indicates that the claimant device 120 is within the region circumscribed by the spot beam at the time indicated in the data received from the claimant device. In at least one
15 embodiment, the spot beam may be irregular shaped. In at least one embodiment the claimant device may be at an altitude above the surface of the earth.

[0065] If, at operation 435, the data received from the claimant device 120 indicates that the claimant device 120 is within a geographic region encompassed by the spot beam from the satellite 110 at the time associated with the data from the
20 claimant device, then the claimant device 120 may be considered authenticated. In an authentication system, control then passes to operation 440 and the claimant is allowed to access a resource. By way of example and not limitation, the verifier device 230 may grant a token to an authenticated claimant device 120. The token may be used by a remote system to grant access to a resource.

[0066] By contrast, if the data received from the claimant device 120 indicates that the claimant device 120 is not within a geographic region encompassed by the spot beam from the satellite 110 at the time associated with the data from the claimant device 120, then the claimant device 120 may not be considered authenticated. In an authentication system, control then passes to operation 445 and the claimant is denied access to a resource. By way of example and not limitation, the verifier device 230 may deny a token to an authenticated claimant device 120. In the absence of a token the claimant device may be denied access to a resource managed by a remote system.

[0067] Thus, the system architecture depicted in Figs. 1-3 and the method depicted in Fig. 4 enable satellite-based authentication of one or more claimant device(s) 120. The authentication system may be used to allow or deny access to one or more resources managed by a remote computing system. In some embodiments the claimant device(s) may be stationary, while in other embodiments the claimant device(s) may be mobile, and the authentication process may be either time-based, location-based, or a combination of both.

[0068] In some embodiments the system may be used to implement session-based authentication in which the claimant device(s) 120 are authenticated to use a resource for an entire session. In other embodiments the system may implement message-based authentication in which the claimant device(s) 120 must be authenticated separately for each message transmitted from the claimant device(s) 120 to a remote resource.

[0069] In one example implementation, an authentication system as described herein may be used to provide authentication for access to a secure computing resource such as a corporate email system, a corporate network, a military or civil

infrastructure network, or an electronic banking facility. In other example implementations, an authentication system may be used to confirm the itinerary of a vehicle in a logistics system. By way of example, a mobile entity such as a truck, train, watercraft or aircraft may comprise one or more claimant device(s) 120. During the course of a scheduled mission a logistics system may periodically poll the claimant device(s) 120, which may respond with authentication data obtained from the satellite 110. The authentication data may be collected in the logistics system and used to confirm that the claimant device(s) are in specific locations at predetermined times in accordance with a logistics plan.

10 **[0070]** In yet another example, implementation of an authentication system as described herein may be used to verify the location of a claimant device(s) associated with a monitoring system, e.g., a house arrest surveillance system. In such embodiments the claimant device(s) may incorporate one or more biometric sensors such as a fingerprint biometric sensor to authenticate the user of the system, while the authentication system may be used to confirm that the claimant device is in a predetermined location at a predetermined time (i.e. The claimant is in the right place, at the right time, and is the right person). The authentication device may also review the claimant device location against a defined list of approved locations which may also further be refined by the authentication system by reviewing the claimant device's location and time against an approved set of location(s) at an approved time period(s). Furthermore, this system may be used to track registered sex offenders.

15 **[0071]** In some embodiments the satellite 110 may be part of a LEO satellite system such as the Iridium constellation which orbits the earth in a known orbit and which transmits spot beams having a known geometry, such that a claimant device(s)

may be authenticated by confirming that the claimant device is within a designated spot beam at a designated time. Thus, a claimant may be authenticated using a single signal source (e.g., a single satellite 110). Also because LEO satellites such as the Iridium constellation and MEO satellites transmit a relatively high power signal levels the system may be used to authenticate one or more claimant device(s) which are located in an obstructed environment, e.g., indoors or in urban locations. Also, the relatively high signal strength of LEO satellites and MEO satellites leaves these signals less susceptible to jamming efforts.

[0072] Reference in the specification to “one embodiment” or “some embodiments” means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least an implementation. The appearances of the phrase “in one embodiment” in various places in the specification may or may not be all referring to the same embodiment.

[0073] Although embodiments have been described in language specific to structural features and/or methodological acts, it is to be understood that claimed subject matter may not be limited to the specific features or acts described. Rather, the specific features and acts are disclosed as sample forms of implementing the claimed subject matter.

CLAIMS

1. A method to authenticate a claimant, comprising:
 - receiving, from the claimant, at least one set of data that has been captured by the claimant from at least one spot beam transmission wherein the data comprises a pseudo-random number and a time stamp associated with the data;
 - further receiving, from the claimant, at least one location identifier;
 - comparing the location identifier and the at least one set of data to a known valid data set, including comparing the location identifier with a known location for the spot beam at a time corresponding to the time stamp; and
 - authenticating the claimant when a difference between the claimant data and the valid data set is less than a threshold.
2. The method of claim 1, wherein the at least one spot beam transmission is emitted from at least one of a low earth orbit satellite, a medium earth orbit satellite, a geosynchronous earth orbit satellite, or a pseudo-satellite.
3. The method of claim 1, wherein the method is used for at least one of a one-way authentication, a multi-way authentication, a multi-way peer to peer device authentication.
4. The method of claim 1, wherein the at least one location identifier is based on an earth-based coordinate system, comprising at least one of a latitude, longitude, altitude or a geographic locator.
5. The method of claim 1, wherein the at least one set of data further comprises at least one of the following: a timing code segment, a spot beam transmitting vehicle identifier, a beam identifier, a time bias parameter, or spot beam transmitting vehicle trajectory data.
6. The method of claim 1, wherein the claimant comprises an electronic computing device, and wherein the claimant is authenticated independently for each message transmitted by the electronic computing device.

7. The method of claim 1, wherein the claimant establishes a communication session with a remote device, and wherein the claimant is authenticated at least once for the communication session.
8. The method of claim 1, wherein the claimant collects at least two locations over time (e.g., polling), and wherein the at least two locations are compared against a known valid data set to authenticate the claimant using knowledge of the claimant's planned traveled path.
9. An apparatus to authenticate a claimant, comprising:
 - a processor; and
 - a memory module comprising logic instructions which, when executed, configure the processor to operate as in any of claims 1 through 10.
10. The apparatus of claim 9, further comprising logic instructions which, when executed, configure the processor to allow the claimant to access a service provided by a remote host when the claimant has been authenticated.
11. A system to authenticate a claimant, comprising:
 - at least one signal source to transmit a spot beam in accordance with a known spot-beam geometry;
 - at least one electronic device comprising a receiver to receive at least one set of data from the spot beam transmission wherein the data comprises a pseudo-random number and a time stamp associated with the data, wherein the at least one electronic device is able to determine its location; and
 - at least one verifier communicatively coupled to the at least one electronic device to authenticate a claimant comprising the electronic computing device, wherein the at least one verifier comprises a processor and a memory module, the memory module comprising logic instructions which, when executed, configure the processor to:
 - receive, from the electronic device, the at least one set of data that the electronic device captured from the spot beam transmission;

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

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

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

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