

TECHNIQUES FOR SECURING LIVE POSITIONING SIGNALS

CROSS-REFERENCE TO RELATED APPLICATIONS

5 [0001] This application is based on and derives the benefit of the filing date of United States Patent Application No. 14/260,162, filed April 23, 2014. The entire content of this application is herein incorporated by reference in its entirety.

TECHNICAL FIELD

10 [0002] This patent document relates to the fields of satellite communication, and in one aspect, to global positioning system satellite communication.

BACKGROUND

15 [0003] Global Positioning System (GPS) technology can be used for location determination, clock synchronization and navigation of an automobile, an airplane or a ship. GPS receivers can receive GPS signals from multiple GPS satellites and determine their position using information embedded in the GPS signals. Several governments and commercial organizations have deployed satellites that transmit GPS signals for military and
20 commercial use. Position and time bearing signals for commercial use are typically sent unencrypted by the GPS satellites.

SUMMARY

[0004] Techniques are disclosed for providing anti-spoofing, or validation, information to
25 a receiver of live satellite positioning signals. Using the validation information, the receiver can verify that the information received from a positioning satellite is not compromised or corrupted.

[0005] In one example aspect, a method of providing anti-spoofing positioning data is disclosed. The method includes receiving, at a device, positioning signals originating from
30 multiple broadcast sources, generating validity data for each broadcast source and corresponding positioning signals, encrypting the validity data resulting in encrypted validity data and transmitting the entitlement messages over a television distribution network.

[0006] In another example aspect, a system for securing positioning data is disclosed. The system includes a global positioning system (GPS) receiver that receives live GPS data from GPS satellites, a checksum generator that, for each GPS satellite, generates checksums over a predetermined amount of received live GPS data, an encapsulation module that
5 encapsulates the checksums for insertion into encrypted messages such as entitlement management messages (EMMs), and a network interface that provides the encapsulated checksums on an interface with a conditional access server.

[0007] In yet another example aspect, a method of operating a navigation system is disclosed. The method includes receiving positioning signals over a first network interface
10 from multiple positioning signal sources, receiving an encrypted reference signal over a second network interface that is different from the first network interface, decrypting the encrypted reference signal using a conditional access module to produce a positioning validation signal, deciding, using the positioning validation signal, whether the received positioning signals are valid, determining, when the positioning signals are decided to be
15 valid, a position of a receiving device that includes the first network interface, and navigating the receiving device based on the valid positioning signals.

[0008] These and other aspects and their implementations are described in greater detail in the drawings, the description and the claims.

20 BRIEF DESCRIPTION OF DRAWINGS

[0009] Embodiments described herein are illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like reference numbers indicate similar elements and in which:

[0010] FIG. 1 is an example of a satellite communication network.

25 [0011] FIG. 2 is a block diagram of an example of a validity-assisted global positioning system.

[0012] FIG. 3 is a flowchart representation of an example method of providing validation data for positioning signals.

30 [0013] FIG. 4 is a block diagram representation of an example system for securing positioning data.

[0014] FIG. 5 is a flowchart representation of an example method of operating a navigation system.

DETAILED DESCRIPTION

[0015] Global Positioning System (GPS) technology is incorporated in many consumer and commercial products, including, e.g., phones, navigation receivers, aviation navigation electronics, maritime navigation systems, goods tracking devices, and so on. While several
5 different techniques exist, a typical GPS receiver receives signals from multiple GPS satellites and estimates its position and/or time zone based on the received signals.

[0016] In some deployments, a GPS receiver may be incorporated in a navigation system for an auto-pilot operation of a transportation equipment. For example, using the navigation system, a ship or an airplane may be able to navigate itself, without constant human control,
10 based on a travel plan programmed into the navigation system and a periodic determination of its position using signals received by the GPS receiver.

[0017] When relying on GPS signals for determining location of the receiving device, reception and/or calculation of incorrect or erroneous positioning data may result in undesirable effects. Without human supervision, these errors may go un-noticed for long time
15 periods. For example, in one undesirable scenario, a ship may receive corrupted or spoofed satellite positioning data and may travel an incorrect route. This may result in expenses such as increased fuel consumption or travel delays. Another undesirable scenario may involve malicious interference with a navigation system's received satellite signals in which fake data is transmitted to the satellite receiver to take control of a ship or an airplane from a remote
20 location.

[0018] Data encryption is used in satellite television delivery networks to encrypt high value content such as premium channels or program guide information. When television signals are encrypted for conditional access, only receivers that are authorized to receive a particular program channel can successfully decrypt the encrypted content for presentation to
25 a user. Conditional access technology used for encrypting satellite signals has been known to be robust to accidental or intentional breaches. Further, in some embodiments, the conditional access algorithms (e.g., the encryption scheme used or the key management techniques) can themselves be modified from time to time via renewable security such as removable smartcards. Such renewability may offer additional resistance against ever-improving
30 malicious attacks.

[0019] Using the techniques provided in the present document, positioning signal transmissions can be secured by providing information via satellite television broadcast signals that can be used to cross-check or validate veracity of the received positioning data.

In some disclosed embodiments, validation information about live ephemeris data and/or other GPS satellite data, possibly including the encrypted military data, is provided through a second, independent communication channel that is different from the communication channel over which the positioning signals are received. For example, secure hashes of live positioning data from available GPS satellites around the Earth may be provided from a digital television broadcast satellite by embedding these hashes within the digital television signals, thereby allowing a receiver to validate the positioning data and ascertain that the received positioning data is indeed coming from the real positioning satellite and not from a rogue device. In some embodiments, the validation data is encoded using an error correction coding, e.g., Reed-Solomon or Low Density Parity Coding, to provide additional robustness against communication errors. In some embodiments, the existing infrastructure of pay-television satellites, which provides an almost identical coverage around the Earth as the positioning satellites, may be used for secure delivery of the anti-spoofing information. These, and other, aspects are described in the present document.

[0020] Fig. 1 depicts an example communication network 100 in which a positioning device 102 receives positioning data from positioning signal sources such as GPS satellites 110. The device 102 may be able to determine its position using the received signals and/or perform navigation using the determined position at the current time. The device 102 may also receive a validation signal, e.g., message hash for the received positioning signal from a module 106 that en-encrypts validation data or hash of the live GPS signals via a television distribution network from a digital television broadcast satellite 104.

[0021] The validation data may be generated and provided to the digital television broadcast satellite 104 as follows. A satellite antenna (network interface) 112 may receive live GPS data from the GPS satellites 110. The live GPS data may be encapsulated be recovered by a GPS receiver 114 and transferred to a conditional access server (CAS) 116. The CAS 116 may perform authorization/deauthorization of subscribers of the television distribution network. The CAS 116 may control subscriber entitlements using encrypted messages such as entitlement management messages (EMMs) and entitlement control messages (ECMs). Both EMMs and ECMs are associated with managing and providing user entitlement or rights on whether a receiver or customer is authorized for accessing a program or service. The CAS 116 may further include the hashes of the live GPS data in the encrypted entitlement messages, e.g., EMMs, with encryption being performed by the encrypter 118. The encrypted messages may be uplinked to the digital television broadcast satellite 104 by an uplink antenna 120.

[0022] Fig. 2 is a block diagram depiction of an example of a combined GPS and validation data reception system 200. The system 200 includes a positioning subsystem 202, a television subsystem 204 and a validation subsystem 206. The system 200 may be deployed in a transportation equipment such as a ship, an airplane, a truck or a car. The positioning subsystem 202 receives live GPS signals over a first network interface (e.g., GPS satellites, digital terrestrial transmissions, etc.). The television subsystem 204 receives television programming over a second network interface (e.g., from a digital television broadcast satellite or digital terrestrial television signals). The received television signals include entitlement messages that are encrypted using the conditional access encryption scheme used in the digital television network for securing television programming and other content.

[0023] The television subsystem 204 may extract validation data related to the live GPS data from the received entitlement messages by decrypting and parsing the entitlement messages. The validation data may be passed to the validation subsystem 206. The positioning subsystem 202 may provide live positioning data (or a portion thereof) received via the first network interface to the validation subsystem 206. The validation subsystem 206 may perform a cross-check that the live positioning data, as received by the positioning subsystem 202, is identical to the positioning data that originated from the GPS satellites, as indicated by the hash values received via the television subsystem 204.

[0024] The validation subsystem 206 may provide results of its validation of live positioning data. The results may be displayed to a user, e.g., via an operator's user interface. Alternatively or additionally, the validation subsystem 206 may raise an alert when there is a mismatch between the live positioning data and the corresponding checksums or hash values received from the digital television network.

[0025] In some embodiments, positioning signal sources may include GPS satellites. Each GPS satellite may continuously broadcasts a navigation message. A typical information transmission rate may be about 50 bits per second. The positioning message may be organized as 37,500 bit messages, that are divided into 25 equal sized frames (1500 bits each), which are further divided into 5 subframes per frame (300 bit each). Each subframe may thus take 6 seconds transmission time. In some embodiments, the transmitted signal may be error protected using, e.g., code division multiple access (CDMA) technology.

[0026] In some embodiments, positioning messages may include information as follows. The first subframe of each frame may carry the week number and the time within the week. The second and the third subframes contain information about the precise orbit for the

satellite (called ephemeris information). The fourth and fifth subframes may include coarse orbit and status information as well as data related to error correction of the message.

[0027] Taking some current GPS satellite deployments as an example, a network of about 12 GPS satellites can provide GPS signals to all areas around the Earth. With each satellite transmitting its GPS signals at around 50 bits / second rate, this means that the validation signals should provide hashing information for about 600 bits of information per second. In some embodiments, this information rate may not pose a significant bandwidth overhead to the downlink capacity of a digital satellite broadcasting network and the positioning information from all satellites may be repeated in the downlink signals of television satellite transmissions. The GPS signals may be secured by encrypting using, e.g., encryption techniques that are used for encrypting entitlement messages transmitted in the downlink. The use of same encryption advantageously allows the inclusion of positioning validation signal without having to provide additional decryption functionality at a receiver of the satellite signals. In some embodiments, a hash function that provides data compression (e. g., by a factor of 2) may be used to reduce the data bandwidth used by the positioning validation signals. For example, a one-way hash function may be used to reduce the data bandwidth from 600 bits/s to 300 bits/seconds. In some embodiments, different amount of hashing/compression may be used to different parts of GPS message fields, e.g., timing information, satellite identity, coarse position data, and so on.

[0028] Fig. 3 is a flowchart representation of an example method 300 for providing anti-spoofing positioning data in a television distribution network. The method 300 may be implemented using hardware/software controlled by, e.g., a service provider who provided the anti-spoofing service or by a broadcast satellite television network operator.

[0029] At 302, a device, e.g., a GPS receiver module in a server, receives positioning signals from multiple broadcast resources. In some embodiments, the multiple broadcast sources may be global positioning system (GPS) satellites. In some embodiments, the multiple broadcast sources may include digital terrestrial television broadcasting transmitters.

[0030] At 304, the method 300 generates validity data for each broadcast source and the corresponding positioning signal. The validity data may include data validating each broadcast source's identity (e.g., a unique global identifier, a medium access control address, etc.) and data for authenticating each of the positioning signals. In some embodiments, the validity data may be generated by computing a hash of at least a portion of a positioning message included in the positioning signal. The hash may be based on a hashing function

that provides a substantially unique mapping between the portion of the positioning message and the computed hash.

[0031] In some embodiments, the validity data is generated by generating a first portion of the validity data to validate an identity of a broadcast source and a second portion of the validity data to validate the corresponding positioning signal of the broadcast source. In some embodiments, the first portion of the validity data and the second portion of the validity data are transmitted at different rates. For example, some live data (e.g., precise satellite orbit data or ephemeris data) may be transmitted more frequently compared to some other live data (e.g., coarse satellite orbit data). As another example, the timing information embedded in the positioning signals, which in turn is included in validity data, may be transmitted more frequently, compared to the satellite orbit position information (coarse or fine positioning information) that is typically transmitted by GPS satellites. In some embodiments, the timing signal is used to generate a third portion of validity data.

[0032] At 306, the method 300 encapsulates the validity data into a television system message. In a typical television system, several messages are sent in the downlink direction. Examples of these messages include program table information, e.g., as specified by the Moving Pictures Expert Group (MPEG) standard or the Digital Video Broadcasting (DVB) standard. In some embodiments, the encapsulated validity signals may be sent using table header and structure of an entitlement message in the television system. In some embodiments, a user defined table format may be used for downlink transmission of the validity signals. The entitlement messages may be, e.g., entitlement management messages (EMMs) transmitted in a satellite television distribution network and may include information pertaining to authorization/deauthorization of individual subscribing receivers to be able to decrypt certain transmitted content for viewing. The encapsulation of the validity data within EMMs may be based on run-time factors such as the bandwidth availability.

[0033] At 308, the method 300 transmits the entitlement messages over a television distribution network. In some embodiments, the television distribution network may be, e.g., a satellite television distribution network. The entitlement messages may be sent over the satellite downlink, e.g., targeted at receivers of the television programming. In some embodiments, the EMMs may be first generated at equipment in an uplink facility for the television distribution network and uplinked (uploaded) to the satellite via a transmission to the satellite.

[0034] In some embodiments, a system 400 for securing positioning data includes a global positioning system (GPS) receiver (402) a checksum generator (404), an encapsulation module (406) and a network interface 408.

[0035] The GPS receiver 402 receives live GPS data from GPS satellites. In some
5 embodiments, the GPS receiver 402 may receive data from three GPS satellites and use triangulation to figure out its own position.

[0036] The checksum generator 404, for each GPS satellite, generates checksums over a predetermined amount of received live GPS data. For example, in various embodiments, checksum may be generated over a GPS message frame, a GPS message subframe, or
10 different checksums may be generated for header/payload fields of GPS messages.

[0037] The encapsulation module 406 encapsulates the checksums for insertion into encryption packets such as EMMs. In one advantageous aspect, EMMs can be targeted at individual receivers (e.g., by encrypting using a key that only a given receiver is able to decrypt with). Thus, carriage of checksum in EMMs can thus “automatically” benefit from
15 the security provided by a conditional access system to entitlement messages carried in a digital satellite television broadcast network. Further, by encapsulating the checksum into EMMs, legacy satellite television receivers (e.g., set-top boxes) can be updated by simply downloading new code for parsing the EMMs. Alternatively, legacy satellite set-top boxes can be updated to include GPS validation technology by providing new smartcards that
20 include a processor/ software that performs EMM parsing and validation as described in the present document.

[0038] The network interface 408 provides the encapsulated checksums on an interface with a conditional access server. The network interface 408 may be, e.g., an Internet connection (e.g., wired or wireless Ethernet). Messages transmitted over the network
25 interface 408 may be encrypted for security reasons.

[0039] In some embodiments, the system 400 further includes an uplink module that receives encapsulated checksums from the conditional access server and uplinks the encapsulated checksums to a satellite for transmissions as EMMs. In some embodiments, the satellite transmits the EMMs on a satellite-to-receivers-on-earth downlink channel (“on
30 earth” means on ground, or in a ship or airplane during transit).

[0040] In some embodiments, the checksum generator computes the checksum using a hashing function. As previously discussed, in some embodiments, the hashing function may be selected that the resulting checksum reduces the number of bits compared to the predetermined amount of received live GPS data. For example, in some embodiments, a GPS

signal may comprise 1500 bit frames and a hash function that maps the 1500 bits to 128 or 256 bit hash may be used. In some embodiments, an entire positioning message may include 25 frames, and a hash may be calculated on the entire message (i.e., on 37,500 bits). A hash result of 1,024 or 4,096 bits may be used, resulting in a factor of 10 to 30 reduction in the amount of data to be carried as validity data.

[0041] Fig. 500 is a flowchart depiction of an example method 500 of operating a navigation system. In some embodiments, the method 500 may be implemented at a navigation system that is “on earth.” In some embodiments, the method 500 may be implemented at a digital television receiver (e.g., a satellite or digital terrestrial set-top box). In some embodiments, the digital television receiver may be modified to interface with a navigation system.

[0042] At 502, the method 500 receives positioning signals over a first network interface from multiple positioning signal sources. In some embodiments, the positioning signals include a timing signal. Using the timing signals, the method 500 may also determine a wall clock time (time of day) at the geographic location of the receiving device at which the method 500 is being executed.

[0043] As previously described, in some embodiments, the multiple positioning signal sources may include the global satellite network, e.g., of GPS satellites, that provides coverage at all places on Earth where satellite signals can be received.

[0044] At 504, the method 500 receives an encrypted reference signal over a second network interface that is different from the first network interface. In some embodiments, the encrypted reference signal may be encapsulated within an EMM carried over the digital television distribution network, and thus may benefit from encryption of the EMM using conditional access technology used in the digital television distribution network.

[0045] At 506, the method 500 decrypts the encrypted reference signal using a conditional access module to produce a positioning validation signal. In some embodiments, the conditional access module may include a removable smart card. In some embodiments, the conditional access module may be a hardware/software module that may be attached (e.g., soldered on a printed circuit board or included in a silicon die that performs other functions) of the received device.

[0046] At 508, the method 500 determines, using the positioning validation signal, whether the received positioning signals are valid. In some embodiments the validity is determined by computing a first checksum from the received positioning signals, and

comparing the first checksum with the positioning validation signal for a match between them.

[0047] At 510, the method 500 utilizes, when the positioning signals are determined to be valid, the positioning signals to determine a position of a receiving device.

5 [0048] At 512, the method 500 facilitates navigation of the receiving device based on the valid positioning signals. In some embodiments, the method 500 may provide the validation signal over a secure interface between the pay television and the positioning subsystems. For example, in some embodiments, a human “transcriber” may be used to enter current GPS coordinates received from the positioning subsystem into a validation interface (e.g., a user
10 interface displayed by a set-top box). In return, the method 500 may compare the GPS coordinates with the validation signal to check whether the hash of the entered GPS coordinates matches the hash values received in the position validation signal. When the hashes match, an indication may be provided to the user that there is a match and the received GPS coordinates can be trusted. Alternatively or additionally, when the hashes do not match,
15 an alert may be raised for the user to take an action.

[0049] In some embodiments, the validation may be performed automatically, i.e., without user intervention. For example, in some embodiments, both the positioning subsystem and the pay television subsystem may provide their respective positioning signals to a validation module. The validation module may verify, based on the hash function,
20 whether the two inputs match. The validation may be performed continuously or upon a pre-determined schedule or upon user command to validate GPS signals.

[0050] In some embodiments, an apparatus for performing secure navigation includes a module that receives positioning signals over a first network interface from multiple positioning signal sources; a module that receives an encrypted reference signal over a
25 second network interface that is different from the first network interface, a module that decrypts the encrypted reference signal using a conditional access module to produce a positioning validation signal, a module that decides, using the positioning validation signal, whether the received positioning signals are valid, a module that determines, when the positioning signals are decided to be valid, a position of a receiving device that includes the first network interface; and a module that facilitates navigation of the receiving device based
30 on the valid positioning signals.

[0051] In some embodiments, a method of operating a navigation system includes receiving a global positioning system (GPS) signal and detecting whether the GPS signal is trustable. The method may be implemented at a computer or a device that navigates a

transportation equipment such as a ship, an airplane or a land-based vehicle. Upon determination of the trustability of the GPS signal, navigation may be performed using the GPS signal. In some embodiments, one or more of previously described techniques of checksum verification and/or the use of error correction codes may be used for the determination of trustability of the GPS signal. When the GPS signal is detected to be untrustable, navigation may be performed using an alternate method of navigation. The received GPS signal may be deemed trustable when a hash of the received GPS signal matches a hash value received from another, independent source.

[0052] In some embodiments, alternate navigation systems may include using positioning signals such as from a different positioning signal source (e.g., signals from the European Galileo system instead of the U.S. GPS signals). In some embodiments, the alternate navigation system may include human intervention and navigation using other positioning methods such as magnetic field orientation or other radio frequency transmissions to assist the location of a receiver (e.g., cellular or terrestrial digital broadcasting).

[0053] In some embodiments, the detecting includes receiving an encrypted reference signal, e.g., described in this document with respect to the use of EMMs in a television distribution system. The encrypted reference signal may be received over the television distribution network and may include a validation signal or information that can be used to cross-check trustability of the GPS signal. For example, the validation signal may include a checksum, as previously described, or may use error correction coding, e.g., Reed Solomon error correction coding or Low Density Parity Codes or another error correction code. In some embodiments, the second network connection may consist of a broadcast satellite television delivery network. As described in the present document, in such a network, a secure downlink mechanism, e.g., an entitlement message, may be used for carrying the encrypted reference signals to the receivers.

[0054] In some embodiments, the television distribution network may be used as follows. A secure communication channel may be allocated by the television distribution network (e.g., a satellite channel) to deliver full data from all satellites that comprise a GPS system. Satellite television transmission is often performed using satellites comprising 24 to 56 transponders, with each transponder comprising around 27 MHz bandwidth that typically carries around 40 Mbps of television signal data. The totality of GPS signal transmissions may be in the range of 1 to 12 Mbps and thus a small fraction of the entire bandwidth available to a satellite. A satellite television broadcast system may thus be modified to include, on one or more transponders, GPS validation data (which could be a duplication of

live GPS data carried by the GPS satellites). In one beneficial aspect, this would allow a strong anti-spoofing cross-check and also could be used to improve the time to lock and the accuracy of a GPS signal. In some embodiments, the secure channel could also contain differential GPS reference points to recover the full accuracy of GPS anywhere in the world.

5 [0055] It will be appreciated that a server communicating with all live GPS satellites around the world can be used to hash the live data that can then be delivered to GPS devices using a secure channel. For example the secure channel could be a conditional access channel encrypted using a pay-television encryption technology and the GPS device could be running a conditional access technique, such as Nagra's conditional access solution, with the
10 hash delivered inside an EMM.

[0056] The disclosed and other embodiments, modules and the functional operations described in this document (e.g., a content network interface, a look-up table, a fingerprint processor, a bundle manager, a profile manager, a content recognition module, a display controller, a user interaction module, a feedback module, a playback indication module, a
15 program guide module, etc.) can be implemented in digital electronic circuitry, or in computer software, firmware, or hardware, including the structures disclosed in this document and their structural equivalents, or in combinations of one or more of them. The disclosed and other embodiments can be implemented as one or more computer program products, i.e., one or more modules of computer program instructions encoded on a computer
20 readable medium for execution by, or to control the operation of, data processing apparatus. The computer readable medium can be a machine-readable storage device, a machine-readable storage substrate, a memory device, a composition of matter effecting a machine-readable propagated signal, or a combination of one or more them. The term "data processing apparatus" encompasses all apparatus, devices, and machines for processing data, including
25 by way of example a programmable processor, a computer, or multiple processors or computers. The apparatus can include, in addition to hardware, code that creates an execution environment for the computer program in question, e.g., code that constitutes processor firmware, a protocol stack, a database management system, an operating system, or a combination of one or more of them. A propagated signal is an artificially generated signal, e.g., a machine-generated electrical, optical, or electromagnetic signal, which is generated to
30 encode information for transmission to suitable receiver apparatus.

[0057] A computer program (also known as a program, software, software application, script, or code) can be written in any form of programming language, including compiled or interpreted languages, and it can be deployed in any form, including as a stand alone program

or as a module, component, subroutine, or other unit suitable for use in a computing environment. A computer program does not necessarily correspond to a file in a file system. A program can be stored in a portion of a file that holds other programs or data (e.g., one or more scripts stored in a markup language document), in a single file dedicated to the program
5 in question, or in multiple coordinated files (e.g., files that store one or more modules, sub programs, or portions of code). A computer program can be deployed to be executed on one computer or on multiple computers that are located at one site or distributed across multiple sites and interconnected by a communication network.

[0058] The processes and logic flows described in this document can be performed by
10 one or more programmable processors executing one or more computer programs to perform functions by operating on input data and generating output. The processes and logic flows can also be performed by, and apparatus can also be implemented as, special purpose logic circuitry, e.g., an FPGA (field programmable gate array) or an ASIC (application specific integrated circuit).

[0059] Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any kind of digital computer. Generally, a processor will receive instructions and data from a read only memory or a random access memory or both. The essential elements of a
15 computer are a processor for performing instructions and one or more memory devices for storing instructions and data. Generally, a computer will also include, or be operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data, e.g., magnetic, magneto optical disks, or optical disks. However, a computer need not have such devices. Computer readable media suitable for storing computer program instructions and data include all forms of non volatile memory, media and memory devices,
20 including by way of example semiconductor memory devices, e.g., EPROM, EEPROM, and flash memory devices; magnetic disks, e.g., internal hard disks or removable disks; magneto optical disks; and CD ROM and DVD-ROM disks. The processor and the memory can be supplemented by, or incorporated in, special purpose logic circuitry.

[0060] While this patent document contains many specifics, these should not be construed
30 as limitations on the scope of an invention that is claimed or of what may be claimed, but rather as descriptions of features specific to particular embodiments. Certain features that are described in this document in the context of separate embodiments can also be implemented in combination in a single embodiment. Conversely, various features that are described in the context of a single embodiment can also be implemented in multiple embodiments separately

or in any suitable sub-combination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a sub-combination or a variation of a sub-combination.

5 Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results.

[0061] Only a few examples and implementations are disclosed. Variations, modifications, and enhancements to the described examples and implementations and other

10 implementations can be made based on what is disclosed.

CLAIMS

What is claimed is what is disclosed and illustrated, including:

- 5 1. A method of providing anti-spoofing positioning data in a television distribution network, comprising:
- receiving, at a device, positioning signals originating from multiple broadcast sources;
- generating validity data for validating an identity of each broadcast source and
- 10 for authenticating each of the corresponding positioning signals;
- encapsulating the validity data into a television system message; and
- transmitting the television system message over the television distribution network.
- 15 2. The method of claim 1, wherein the multiple broadcast sources comprise global positioning system (GPS) satellites.
3. The method of claim 1, wherein the television system message comprises an entitlement message.
- 20 4. The method of claim 3, wherein the television distribution network comprises a satellite downlink and the transmitting comprises transmitting the entitlement messages over the satellite downlink.
5. The method of claim 1, wherein the television distribution network comprises
- 25 a satellite uplink and the transmitting comprises transmitting the entitlement messages over the satellite uplink.
6. The method of claim 1, wherein the television system message include a television subscription authorization message.
- 30 7. The method of claim 1, wherein the generating includes:
- computing, using a hashing function, a hash of at least a portion of a positioning message included in the positioning signal, wherein the hashing function provides a

substantially unique mapping between the portion of the positioning message and the computed hash.

8. The method of claim 1, wherein the generating includes:

5 generating a first portion of the validity data to validate an identity of a broadcast source and a second portion of the validity data to validate the corresponding positioning signal of the broadcast source.

9. The method of claim 8, further comprising:

10 transmitting the first portion of the validity data and the second portion of the validity data at different rates.

10. The method of claim 8, wherein the positioning signal includes a timing signal and the generating further includes:

15 a third portion of the validity data to validate the timing signal.

11. The method of claim 1, wherein the receiving at the device occurs in absence of a communication path from the receiver to the multiple broadcast sources.

20 12. The method of claim 1, wherein the encapsulating further includes: performing error correction encoding on the validity data.

13. A system for securing positioning data, comprising:

25 a global positioning system (GPS) receiver that receives live GPS data from GPS satellites;

a checksum generator that, for each GPS satellite, generates checksums over a predetermined amount of received live GPS data;

an encapsulation module that encapsulates the checksums for insertion into entitlement management messages (EMMs); and

30 a network interface that provides the encapsulated checksums on an interface with a conditional access server.

14. The system of claim 13, further including:

an uplink module that receives encapsulated checksums from the conditional access server and uplinks the encapsulated checksums to a satellite for transmissions as EMMs.

15 15. The system of claim 13, wherein the satellite transmits the EMMs on a
5 downlink channel.

16. The system of claim 13, wherein the entitlement messages include television subscription authorization messages.

10 17. The system of claim 13, wherein the checksum generator computes the
checksum using a hashing function, the checksum resulting in a number of bits less than that
of the predetermined amount of received live GPS data.

15 18. A method of operating a navigation system, comprising
receiving positioning signals over a first network interface from multiple
positioning signal sources;
receiving an encrypted reference signal over a second network interface that is
different from the first network interface;
decrypting the encrypted reference signal using a conditional access module to
20 produce a positioning validation signal;
deciding, using the positioning validation signal, whether the received
positioning signals are valid;
determining, when the positioning signals are decided to be valid, a position of
a receiving device that includes the first network interface; and
25 navigating the receiving device based on the valid positioning signals.

19. The method of claim 18, wherein the positioning signals include a timing
signal, the method further including:
determining a time of day at the receiving device.

30 20. The method of claim 18, wherein the determining includes:
computing a first checksum from the received positioning signals; and
comparing the first checksum with the positioning validation signal for a match
between them.

21. The method of claim 18, wherein the encrypted reference signal is included in an entitlement management message (EMM).

5 22. The method of claim 18, wherein the multiple positioning resources provide a full positioning signals coverage around the Earth.

23. The method of claim 18, wherein the conditional access module comprises a removable smartcard.

10 24. The method of claim 19, further comprising:
providing the validation signal over a secure interface between the pay television and the positioning subsystems.

15 25. A method of operating a navigation system, comprising:
receiving a global positioning system (GPS) signal;
detecting whether the GPS signal is trustable;
performing navigation using the GPS signal when the GPS signal is trustable; and
performing navigation using an alternate method by refraining from using the GPS
20 signal, when the GPS signal is detected to be not trustable.

25 26. The method of of claim 25, wherein the detecting includes:
receiving an encrypted reference signal over a first network connection different from a second network connection over which the GPS signal is received; and
extracting a validation signal from the received encrypted reference signal to determine trustability of the GPS signal.

30 27. The method of claim 26, wherein the second network connection comprises a broadcast satellite television network and wherein the receiving the encrypted reference signal comprises receiving the encrypted reference signal encapsulated within entitlement messages of the broadcast satellite television network.