



- (51) **International Patent Classification:**
B60R 25/10 (2006.01) **G08B 25/10** (2006.01)
H04K 3/00 (2006.01)

(21) **International Application Number:**
PCT/US2012/029730

(22) **International Filing Date:**
20 March 2012 (20.03.2012)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
13/094,099 26 April 2011 (26.04.2011) US

(71) **Applicant** (for all designated States except US): **CONTINENTAL AUTOMOTIVE SYSTEMS, INC.** [US/US]; 1 Continental Drive, Auburn Hills, Michigan 48326-1581 (US).

(72) **Inventors; and**

(75) **Inventors/Applicants** (for US only): **SEYMOUR, Shafer** [US/US]; 840 Honey Locust Court, Bartlett, Illinois 60103 (US). **SALADIN, Peter** [US/US]; 758 South Benton, Palatine, Illinois 60067 (US).

(74) **Agents:** **KLEIN, William** et al.; Continental Automotive Systems, Inc, Patents & Licenses, 21440 W. Lake Cook Road Floor 7, Deer Park, Illinois 60010 (US).

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report (Art. 21(3))

(54) Title: A SYSTEM AND METHOD FOR SELF-DETECTING VEHICLE THEFT

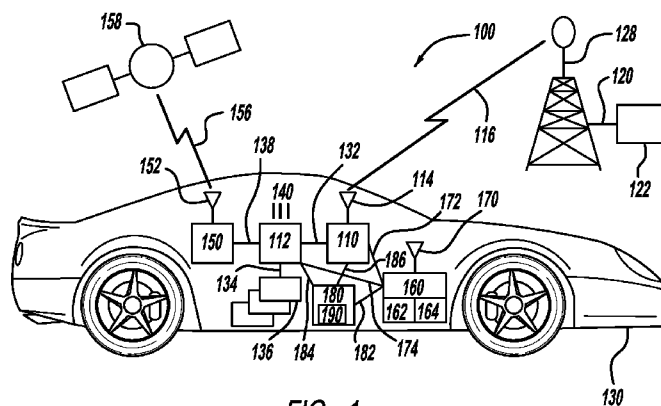


FIG - 1

(57) Abstract: A system and method for self-detecting vehicle theft is provided that includes a first antenna (114) and a second antenna (170), both located on a vehicle (130). The first antenna transmits the signal (116) and the second antenna receives the signal. A monitoring module (160) in communication with the second antenna is configured to determine whether the signal has changed. A vehicle security system (190) is configured to activate based on a change in the signal.

A SYSTEM AND METHOD FOR SELF-DETECTING VEHICLE THEFT

FIELD

[0001] The present disclosure generally relates to vehicle security systems, and more particularly to automatically detecting vehicle theft.

BACKGROUND

[0002] Vehicles implement various security measures to combat vehicle theft. For example, upon theft, an antenna within the vehicle can transmit a signal to and thus notify a service provider, who may then remotely disable the vehicle.

[0003] However, a thief may thwart such a security measure by covering the antenna with a radio frequency (RF) absorbing device, for example a Faraday blanket, which prevents the service provider from receiving the signal. The vehicle can thus no longer be tracked, and the thief may successfully steal the vehicle.

SUMMARY

[0004] In overcoming the drawbacks and other limitations of the related art, the present disclosure provides a system and method for self-detecting vehicle theft by monitoring signal transmissions in the vehicle.

[0005] In some implementations, the present disclosure relates to a method for self-detecting vehicle theft in a vehicle, comprising the following steps. A signal is transmitted from a first location on the vehicle. The signal is received at a second location on the vehicle. Whether the signal was changed is determined. A vehicle security system may be activated based on the change in the signal.

[0006] In some implementations, the present disclosure relates to an apparatus for self-detecting theft in a vehicle. A first antenna is configured to transmit a signal

and attached to a network access device that is located on the vehicle. A second antenna is configured to receive the signal and located on the vehicle. A monitoring module is in communication with the second antenna and configured to determine whether the signal has changed. A vehicle security system is configured to activate based on a change in the signal.

[0007] In some implementations, the present disclosure relates to a computer readable storage medium having stored therein instructions executable by a programmed processor for determining if a vehicle is stolen, the storage medium comprising instructions for the following steps. Determinations are made as to whether a received signal was changed at the transmission source and whether the received signal was changed after transmission. A vehicle security device is activated if the received signal was changed.

[0008] In some implementations, the present disclosure relates to an apparatus for self-detecting theft in a vehicle. A first antenna is configured to transmit a signal and attached to a network access device that is located on the vehicle. A second antenna is configured to receive the signal and located on the vehicle. A receiver is in communication with the second antenna and configured to analyze the signal, the analysis of the signal comprising determining whether the signal is interrupted, determining whether the signal magnitude varies from a predetermined baseline magnitude, detecting patterns in the signal, and analyzing data in the signal. A processor is configured to detect a functional status of a transmitter. A vehicle security device is configured to disable the vehicle based upon the analysis of the signal and if the functional status of a transmitter is operative.

[0009] Further areas of applicability will become apparent from the description provided herein. It should be understood that the description and specific examples

are intended for purposes of illustration only and are not intended to limit the scope of the present disclosure.

DRAWINGS

[0010] In order that the disclosure may be well understood, there will now be described various implementations thereof, given by way of example, reference being made to the accompanying drawings, in which:

[0011] FIG. 1 is a schematic view of a system for self-detecting vehicle theft with a telematics controller and network access device implemented within a motor vehicle;

[0012] FIG. 2 is a schematic view of a network access device connected a transmit and receive antenna pair;

[0013] FIG. 3 is a schematic view of a network access device connected to a transmit/receive antenna and a receive antenna;

[0014] FIG. 4 is a schematic view of a third antenna connected to a transmitter;

[0015] FIG. 5 is a flow chart illustrating a method for self-detecting vehicle theft in a vehicle;

[0016] FIG. 6 is a schematic view of a telematics system including a telematics controller and a network access device; and

[0017] FIG. 7 is a schematic view of a computer system that may be used for implementing the methods provided herein.

[0018] The drawings described herein are for illustration purposes only and are not intended to limit the scope of the present disclosure in any way.

DETAILED DESCRIPTION

[0019] The following description is merely exemplary in nature and is not intended to limit the present disclosure, application, or uses.

[0020] Now referring to FIG. 1, an implementation of a system 100 for self-detecting vehicle theft is provided within a vehicle 130. The network access device 110 may be provided in the same or a separate package from the telematics controller 112. The network access device 110 may be located on the vehicle 130, for example in the dashboard. As defined herein, "located on" means located anywhere on the interior or exterior of the vehicle 130, or anywhere on within, inside, outside, attached to, or integral with of any particular part of the vehicle 130 such as the dashboard, roof, trunk, hood, or any other part of the vehicle 130. The network access device 110 may be connected to an antenna 114. The antenna 114 may be representative of a plurality of antennas or a matrix of antennas depending upon the particular communication mode selected, and may have transmit/receive functionality. The antenna 114 may be located on a vehicle's dashboard, roof, trunk, hood, or any other part of the vehicle 130. Communication of the network access device 110 is facilitated with a remote station 128, as denoted by a signal 116. As described previously, the remote station 128 may be in communication with a service provider 122 including a network server through a network 120.

[0021] The telematics controller 112 may be in communication with a global positioning device 150 over the vehicle bus 140 or a custom connection as denoted by line 138. The global positioning device 150, such as a satellite global positioning system (GPS), may be in communication with an antenna 152. The antenna 152 may be one of a plurality of antennas or a matrix of antennas. Further, the antenna or plurality of antennas represented by reference number 152 may be the same

antennas, as denoted by reference number 114. The GPS unit may be in communication with a satellite 158, as denoted by line 156. As such, the GPS unit 150 may retrieve positional data for the vehicle or in other implementations 150 may also represent a general satellite receiver and, therefore, may receive other general broadcast information or communication from the satellite 158.

[0022] The telematics controller 112 may also be in communication with various other vehicle devices and systems through the vehicle bus, wire harnesses, or other wireless connections, as denoted by line 134. The various other devices 136 may include but are not limited to the engine control system, the vehicle locks, the vehicle safety systems (e.g. seatbelt retractors, airbags, etc.), vehicle entertainment system, or a suspension control system.

[0023] The system 100 may also provide a monitoring module 160. The monitoring module 160 may include a transmitter, receiver, processor, and memory (not pictured). The monitoring module 160 may be connected to an antenna 170. The antenna 170 may be representative of a plurality of antennas or a matrix of antennas depending upon the particular communication mode selected. The monitoring module 160 and/or the antenna 170 may be located on the vehicle 130. In some implementations, the monitoring module 160 and/or the antenna 170 are located remotely from the antenna 114. In some implementation, the antenna 114 may be in the dash and the antenna 170 may be on the hood, for example at a distance of 5 feet. As a result, a thief who attempts to place a Faraday blanket over the antenna 114 would not be able to cover both antennas 114 and 170 simultaneously. Particularly, the antennas 114 and 170 may be placed in locations such that a Faraday blanket placed over the antenna 114 would disrupt the transmission of the signal between the antennas 114 and 170. In various

implementations, the monitoring module 160 may communicate with the network access device 110. In some implementations, the monitoring module 160 may be in communication with the telematics controller 112 over the vehicle bus 140, and the telematics controller 112 may then communicate to the network access device 110. The monitoring module 160 may also be in communication with the network access device 110 through a custom connection 172. Further, the monitoring module 160 may also be in communication with the telematics controller 112 through custom connection 174, and the telematics controller 112 may then communicate to the network access device 110.

[0024] The system 100 may also provide a stolen vehicle tracking (SVT) module 180. In various implementations, the SVT module 180 may communicate with the monitoring module 160. For example, the SVT module 180 may be in communication with the monitoring module 160 over the vehicle bus 140 or over a custom connection, as denoted by line 182. The SVT module 180 may, further, be in communication with the telematics controller 112 over the vehicle bus 140 or over a custom connection, as denoted by line 184. The SVT module may also be in communication with the network access device 110 over custom connection 186.

[0025] The antenna 114 connected to the network access device 110 may transmit the signal 116, with the intended recipient being, for example, a remote station 128. In various implementations, the network access device 110 may insert one or more patterns or one or more data markers into the signal 116, for purposes of signal authentication. The pattern in the signal can be a cyclic pattern of transmitting the signal and not transmitting the signal. This pattern can be implemented by turning the network access device 110 on and off, or by turning the antenna 114 on and off. In another example, the signal magnitude may be varied

according to a specific pattern, for example, cycling the signal between one or more magnitudes, including full, 90%, 80%, 70%, 60%, 50%, and all other magnitudes. The patterns may also be sinusoidal, or be any other patterns well known to those skilled in the art. The data marker may, for example, be metadata or a watermark. The signal may also contain data content. The term “data” is defined herein to include both data markers and data content in the signal 116.

[0026] The antenna 170 connected to the monitoring module 160 may receive the signal 116 transmitted by the antenna 114 connected to the network access device 110. Components of the monitoring module 160, for example the receiver 162 and processor 164, may be configured to continuously monitor and analyze the signal 116 received by the antenna 170.

[0027] The monitoring module 160 may detect, monitor, and analyze properties of the signal 116, for example its magnitude, patterns, and data, particularly by determining whether any measured properties of the signal 116 have changed relative to expected properties of the signal 116. The receiver 162 or the processor 164 of the monitoring module 160 may compare the measured properties of the signal 116 with the expected properties of the signal 116. The expected properties of the signal 116 may be based on predetermined expected properties stored in, for example, the memory of the monitoring module 160. The expected properties of the signal 116 may also be based on dynamic updates from the network access device 110 over the custom connection 172, or from the telematics controller 112 over the custom connection 174 or the vehicle bus 140. The monitoring module 160 may also employ artificial intelligence techniques, for example symbolic rules or neural networks, to dynamically vary the expected properties of the signal 116 in accordance with changing external and environmental conditions.

[0028] The change of the measured properties of the signal 116 relative to the expected properties of the signal 116 may take many forms. The change may constitute a disruption or interruption in signal reception caused, for example, by a Faraday blanket. In another example, the change may constitute a measured magnitude of the signal 116 being lower than a predetermined expected baseline magnitude. In a further example, the change may constitute the measured magnitude of the signal 116 being higher than a predetermined expected baseline magnitude, caused for example by a decoy transmitter employed by a thief. In another example, the change may constitute one or more expected patterns in the signal 116, which are inserted by the network access device 110, not matching one or more measured patterns in the signal 116. In a further example, the change may constitute one or more expected data markers in the signal 116, inserted by the network access device 110, not matching one or more measured data markers in the signal 116. In another example, the change may constitute expected data content in the signal 116 not matching measured data content in the signal 116. Moreover, any of the foregoing examples may be implemented together and/or with other parameters indicative of theft, for example with an RF key fob.

[0029] If the monitoring module 160 and its associated components determine that one or more of the changes in the signal properties has occurred, the monitoring module 160 may report the changes to the SVT module 180, or in some implementations, the SVT module 180 may query the monitoring module 160 regarding whether one or more of the changes in the signal properties has occurred. In some implementations, any change must exceed a certain change threshold for a report to be sent to the SVT module 180. For example, the magnitude of the signal

may have to vary more than 50% from the predetermined expected baseline magnitude for a report to be sent to the SVT module 180.

[0030] Once the SVT module 180 receives a report from the monitoring module 160, the SVT module 180 may then communicate with the network access device 110 over the custom connection 186, or with the telematics controller 112 over the custom connection 184 or the vehicle bus 140. The telematics controller 112 or the network access device 110 may send a report to or receive a query from the SVT module 180 regarding the functional status of the antenna 114 and/or network access device 110. The functional status of the antenna 114 and/or the network access device 110 may each be operative or inoperative. Determining the functional status of the antenna 114 and/or the network access device 110 may comprise verifying whether the signal 116 is being transmitted from the transmission source, for example the antenna 114.

[0031] If the SVT module 180 determines that the functional status of the antenna 114 and/or the network access device 110 is inoperative, or if it detects that the signal 116 is no longer being transmitted from the antenna 114, the SVT module 180 may then activate a vehicle security system 190. In some implementations, the vehicle security system 190 may be a component of the SVT module 180. In other implementations, the vehicle security system 190 may be a separate component in communication with the SVT module 180 over the vehicle bus 140 or a custom connection (not pictured). In some implementations, the SVT module 180 may activate the vehicle security system 190 without a determination of the functional status of the antenna 114 and/or the network access device 110, and base the activation of the vehicle security system 190 solely on the changes in signal properties as determined by the monitoring module 160.

[0032] The activation of the vehicle security system 190 may constitute disabling the vehicle 130. For example, the vehicle security system 190 may automatically shut down the vehicle 130, for example by disabling the powertrain or applying the brakes. The vehicle security system 190 may also prevent the vehicle 130 from exceeding a predetermined speed (for example, 5, 10, 15 or 20 miles per hour), flashing a vehicle light, or honking a vehicle horn. The vehicle security system 190 may also utilize the global positioning device 150 and the antenna 152 to determine a location where the vehicle 130 is to be disabled, automatically shut down, have its brakes applied, speed limited, lights flashed, or horn honked. The vehicle security system 190 may determine the most advantageous location based on a current and anticipated route. For example, a busy street in town would be preferred to a deserted country road, as there is a higher likelihood of discovery by the police. The vehicle security system 190 may also utilize the antenna 170 connected to the monitoring module 160, or a backup antenna (not pictured) in communication with vehicle security system 190 to report the theft to a service provider.

[0033] Now referring to FIG. 2 and FIG. 3, implementations of the network access device and connected antennas are provided. Now referring to FIG. 2, a network access device 210 connected to a receive antenna 216 and a transmit antenna 218 pair is provided. The receive antenna 216 and the transmit antenna 218 may be located remotely from one another on the vehicle 130. For example, the receive antenna 216 may be located on one of the vehicle's dashboard, roof, trunk, hood, or any other part of the vehicle 130, and the transmit antenna 218 may be located on another of the vehicle's dashboard, roof, trunk, hood, or any other part of the vehicle 130. The network access device 210, the receive antenna 216, and the transmit antenna 218 may be used in place of the network access device 110, the antenna

170, and the antenna 114, respectively. In this implementation, the monitoring module 160 may be in communication with or connected to the receive antenna 216. In some implementations, the monitoring module 160 may be a component of the network access device 210. In some implementations, the monitoring module 160 may be an integral part of the network access device 210 and the network device 210 may perform all the functions of the monitoring module 160.

[0034] Now referring to FIG. 3, a network access device 310 is provided that has a first input and a second input, the first input being connected to a transmit/receive antenna 314 and the second input being connected to a receive antenna 316. The transmit/receive antenna 314 and the receive antenna 316 may be located remotely from one another in the vehicle 130. For example, the transmit/receive antenna 314 may be located on one of the vehicle's dashboard, roof, trunk, hood, or any other part of the vehicle 130, and the receive antenna 316 may be located on another of the vehicle's dashboard, roof, trunk, hood, or any other part of the vehicle 130. The network access device 310, the transmit/receive antenna 314, and the receive antenna 316 may be used in place of the network device 110, the antenna 114, and the antenna 170, respectively. In this implementation, the monitoring module 160 may be in communication with or connected to the receive antenna 316. In some implementations, the monitoring module 160 may be a component of the network access device 310. In some implementations, the monitoring module 160 may be an integral part of the network access device 310 and the network device 310 may perform all the functions of the monitoring module 160.

[0035] Referring now to FIG. 4, the system 100 may provide a third antenna 416 connected to a transmitter 412, wherein the third antenna 416 is co-located with a transmit/receive antenna 414 (a first antenna) and located remotely from the antenna

170 (a second antenna). The transmitter 412 may be a component of a network access device 410. The third antenna 416 may be connected to the network access device 410. In some implementations, the transmitter 412 may be in communication with the network access device 410 over a custom connection. In some implementations, the transmitter 412 may be in communication with the telematics controller 112 over the vehicle bus 140, and the telematics controller 112 may then communicate with the network access device 410. The transmit/receive antenna 414 and the network access device 410 may be used in place of the antenna 114 and the network access device 110. The third antenna 416 may operate at a different frequency, lower power, and/or use a different protocol than the antenna 414. The third antenna 416 and the transmit/receive antenna 414 may operate together, such that if one is transmitting, the other will also be transmitting. The third antenna 416 may then transmit a signal intended for the antenna 170 of the monitoring module 160. Because the signal transmitted by the third antenna 416 may only be intended to be received by the antenna 170, the transmitted data need not comply with network standards, and on/off pattern modulation may be easier to implement. In some implementations, the components of FIG. 4 may be implemented together with the components of FIG. 2 and/or FIG. 3.

[0036] Now referring to FIG. 5, a method 500 for self-detecting vehicle theft in a vehicle is provided. The ordering of the steps presented herein is merely one implementation of the method 500. Those skilled in the art will recognize that the ordering may be varied, that some steps may occur simultaneously, that some steps may be omitted, and that further steps may be added. In block 510, a first antenna attached to a network access device that is located at a first location on the vehicle transmits a signal, if the network access device and the first antenna are functional.

In block 520, a second antenna located at a second location on the vehicle attempts to receive the signal. In decision block 530, a monitoring module analyzes the signal to determine whether the signal was changed after transmission. If the signal was not changed after transmission, then the method 500 returns to block 510. If the signal was changed after transmission, then the method 500 proceeds to block 540. In decision block 540, a stolen vehicle tracking device verifies whether the first antenna is transmitting the signal according to established specifications, for example at a correct power level or if the signal is being transmitted at all. If the verification of whether the first antenna is transmitting the signal according to established specifications fails, for example because one of the first antenna or the network access device is not functioning, or because the first antenna is transmitting the signal at the wrong power level, then the method 500 returns to block 510. If the first antenna is transmitting the signal according to established specifications, then the method 500 proceeds to block 550. In block 550, a vehicle security system is activated.

[0037] Now referring to FIG. 6, a telematics system 600 is provided. All components found in the telematics system 600 but not pictured in system 100 may be included in the system 100. The system includes a network access device 610 and a telematics controller 612. The network access device 610 may include a processor 614 and storage 616. The processor 614 may be a programmable microprocessor or alternatively may be an application specific integrated circuit (ASIC), or other known processor. The storage 616 may be a memory, for example, random access memory, static memory, or other data storage device. The network access device 610 may also include a transceiver 618 which includes a transmitter 622 and a receiver 620. Alternatively, the network access device 610 may include

an independent transmitter and receiver. The transceiver 618 may be in communication with an antenna 624. The transceiver 618 may communicate with a radio tower 628 as denoted by line 626. The communication 626 between the network access device 610 and the radio tower 628 may comprise one of a plurality of communication modes.

[0038] The transceiver 618 in the network access device 610 may be used for transmitting uplink communications and receiving downlink communication to and from the network 630 and service center 632 over the wireless communication link 626. The wireless communication link 626 may use a wireless protocol such as a standard cellular network protocol such as Advanced Mobile Phone Service (AMPS), Global System for Mobile Communications (GSM), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), and the like. To transmit data in the cellular environment, different types of standard bearer services exist including, but not limited to, general packet radio service (GPRS), short message service (SMS), circuit switched data service (CSD), and high-speed circuit switched data service (HSCSD). Further, standard transmission control protocol/internet protocol (TCP/IP) may also be used as well as satellite communications. In a further example, the transceiver 618 may be enabled using other wireless technologies such as Bluetooth technology. Bluetooth technology allows for the replacement of a wired connection by enabling devices to communicate with each other through a universal short-range radio link.

[0039] The radio tower 628 may be in communication with a service provider 632 including for example, a network server through a network 630. Network 630 may be an analog network such as a plain old telephone service (POTS) or a digital network for example, Ethernet over transmission control protocol / internet protocol

(TCP/IP). In other examples, the network 630 could be one of several standard cellular communication networks, a satellite-based network, a public switched telecommunication network (PSTN), the Internet, an integrated services digital network (ISDN), and/or other communication networks. The service provider may include a service center to provide telematics applications and services to the vehicle. For instance, the service center may contain operators, content servers and content databases. The content servers for telematics applications and services may include traffic servers, map servers, user profile servers, location information servers, and the like. The content databases for telematics applications and services may include location information, user profiles, traffic content, map content, point-of-interest content, usage history, and the like.

[0040] The network access device 610 may be in communication with the telematics controller 612 through a communication interface 634. In some implementations the network access device 610 may be in the same package as the telematics controller 612. However, other implementations the network access device 610 may be provided in a separate package from the package of the telematics controller 612 and, therefore, may be located in a different area of the vehicle. Various information may be communicated between the telematics controller 612 and the network access device 610.

[0041] The telematics controller 612 may include a processor 636 and storage 638. The processor 636 may be a microprocessor, an application specific integrated circuit, a programmable gate array, or other processor. Further, the storage 638 may be a memory device for example, random access memory, read only memory, static memory, or may even be a hard drive or optical drive, or other means of data storage. The telematics controller 612 may be in communication with a plurality of

other vehicle sensors and devices through a wire harness or over the vehicle bus as denoted by lines 640. In addition, the telematics controller 612 may be in communication with a user interface 644 as denoted by line 642. The user interface 644 may include a display 646 and controls 648 for providing user input such as vehicle parameters into the telematics controller 612. Also, the user interface 644 may include elements such as a keyboard or keypad, one or more control buttons, indicator lights, one or more speakers, a microphone, and any other user interface type elements for telematics applications and services. Optionally, the telematics controller 612 may also be connected to a positioning unit. The positioning unit could be a system that determines the geographic location of the vehicle such as a global positioning system (GPS), a dead-reckoning system, and the like.

[0042] Further, the telematics controller 612 may be in communication with other vehicle systems, such as the engine control system, the vehicle lock controls, the vehicle safety systems (e.g. seatbelt retractors, airbags, etc.), vehicle entertainment system, or a suspension control system to implement the described functions of the telematics controller 612 or network access device 610 based on parameters of such systems.

[0043] The telematics controller 612 may be powered by the vehicle battery 650 as denoted by lines 652 and 654. Alternatively, a voltage converter may be provided to convert from the vehicle battery voltage to a different voltage that may be appropriate for running the telematics controller 612. The voltage converter may be included in the package for the telematics controller 612 or alternatively may be in a separate package between the vehicle battery 650 and the telematics controller 612. The vehicle battery 650 may also provide power to the network access device 610.

[0044] A circuit 658 may be included between the vehicle battery 650 and the network access device 610. The circuit 658 may include a voltage converter to change the voltage provided to the network access device 610 in lines 660 and 662. In addition, the circuit 658 may be connected to a network access device battery 656. The network access device battery 656 may be charged while the vehicle is running and may for example, be switched to provide power to the network access device 610 when power from the vehicle power system (e.g., the battery or alternator) is not available. Further, the circuit 658 may control the monitoring and periodic powering of the network access device if the vehicle is turned off for a long period of time. Further, the circuit 658 may control the charging of the network access device battery 656 at appropriate times according to the environmental variables or the expected use cycle of the vehicle.

[0045] Any of the modules, servers, or engines described may be implemented in one or more computer systems. One exemplary system is provided in FIG. 7. The computer system 700 includes a processor 710 for executing instructions such as those described in the methods discussed above. The instructions may be stored in a computer readable medium such as memory 712 or storage devices 714, for example a disk drive, CD, or DVD. The computer may include a display controller 716 responsive to instructions to generate a textual or graphical display on a display device 718, for example a computer monitor. In addition, the processor 710 may communicate with a network controller 720 to communicate data or instructions to other systems, for example other general computer systems. The network controller 720 may communicate over Ethernet or other known protocols to distribute processing or provide remote access to information over a variety of network

topologies, including local area networks, wide area networks, the Internet, or other commonly used network topologies.

[0046] In other embodiments, dedicated hardware implementations, such as application specific integrated circuits, programmable logic arrays and other hardware devices, can be constructed to implement one or more of the methods described herein. Applications that may include the apparatus and systems of various embodiments can broadly include a variety of electronic and computer systems. One or more embodiments described herein may implement functions using two or more specific interconnected hardware modules or devices with related control and data signals that can be communicated between and through the modules, or as portions of an application-specific integrated circuit. Accordingly, the present system encompasses software, firmware, and hardware implementations.

[0047] In accordance with various embodiments of the present disclosure, the methods described herein may be implemented by software programs executable by a computer system. Further, in an exemplary, non-limited embodiment, implementations can include distributed processing, component/object distributed processing, and parallel processing. Alternatively, virtual computer system processing can be constructed to implement one or more of the methods or functionality as described herein.

[0048] Further, the methods described herein may be embodied in a computer-readable medium. The term "computer-readable medium" includes a single medium or multiple media, such as a centralized or distributed database, and/or associated caches and servers that store one or more sets of instructions. The term "computer-readable medium" shall also include any medium that is capable of storing, encoding or carrying a set of instructions for execution by a processor or that cause a

computer system to perform any one or more of the methods or operations disclosed herein.

[0049] Further, the methods described herein may be embodied in a computer-readable medium. The term "computer-readable medium" includes a single medium or multiple media, such as a centralized or distributed database, and/or associated caches and servers that store one or more sets of instructions. The term "computer-readable medium" shall also include any medium that is capable of storing, encoding or carrying a set of instructions for execution by a processor or that cause a computer system to perform any one or more of the methods or operations disclosed herein.

[0050] As a person skilled in the art will readily appreciate, the above description is meant as an illustration of the principles of the invention. This description is not intended to limit the scope or application of the invention in that the invention is susceptible to modification, variation and change, without departing from the spirit of the invention, as defined in the following claims.

CLAIMS

What is claimed is:

1. A method for self-detecting vehicle theft in a vehicle, comprising the following steps:
 - transmitting a signal from a first location on the vehicle;
 - attempting to receive the signal at a second location on the vehicle;
 - determining whether the signal was changed; and
 - activating a vehicle security system based on the change in the signal.
2. The method of claim 1, further comprising:
 - verifying whether the signal is being transmitted from a transmission source;
 - wherein activating the vehicle security system is based on both the change in the signal and the verification of whether the signal is being transmitted from the transmission source.
3. The method of claim 1, wherein determining whether the signal has changed comprises detecting whether the signal reception is interrupted, and wherein activating the vehicle security system is further based on whether the signal reception is interrupted.
4. The method of claim 1, wherein determining whether the signal has changed comprises determining whether a measured magnitude of the signal is lower than a predetermined baseline magnitude, wherein activating the vehicle

security system is further based on whether the measured magnitude of the signal is lower than the predetermined baseline magnitude.

5. The method of claim 1, wherein determining whether the signal has changed comprises determining whether a measured magnitude of the signal is higher than a predetermined baseline magnitude, wherein activating the vehicle security system is further based on whether the measured magnitude of the signal is higher than the predetermined baseline magnitude.

6. The method of claim 1, further comprising:
inserting a pattern into the signal at the transmission source; and
detecting the pattern in the signal, wherein activating the vehicle security system is further based on the detection of the pattern in the signal.

7. The method of claim 6, wherein the pattern comprises a cyclic pattern of transmitting the signal and not transmitting the signal.

8. The method of claim 1, further comprising:
monitoring data in the signal;
determining authenticity of the signal based on the data, wherein activating the vehicle security system is further based on the authenticity of the signal.

9. An apparatus for self-detecting theft in a vehicle, the apparatus comprising:

a first antenna configured to transmit a first signal and attached to a network access device that is located on the vehicle;

a second antenna configured to receive the first signal and located on the vehicle;

a monitoring module in communication with the second antenna and configured to determine whether the first signal has changed; and

a vehicle security system configured to activate based on a change in the first signal.

10. The apparatus of claim 9, further comprising a stolen vehicle tracking module configured to detect a functional status of one or both of the first antenna and a transmitter coupled to the first antenna, wherein the activation of the vehicle security system is further based on the functional status.

11. The apparatus of claim 9, wherein the first antenna and the second antenna are not co-located.

12. The apparatus of claim 9, wherein the first antenna and the second antenna comprise a transmit and receive pair.

13. The apparatus of claim 9, further comprising a first receive input in communication with the first antenna, and a second receive input in communication with a receive antenna, the first and second receive inputs being located on the network access device.

14. The apparatus of claim 9, further comprising a third antenna co-located with the first antenna and configured to transmit a second signal using a different protocol or at a different frequency than the first signal.

15. The apparatus of claim 14, wherein the second signal has a lower power than the first signal.

16. The apparatus of claim 9, wherein the activation of the vehicle security system comprises sending from a backup antenna a report to a service provider that the first signal has changed.

17. The apparatus of claim 9, wherein the activation of the vehicle security system comprises automatically shutting down the vehicle.

18. The apparatus of claim 17, wherein the activation of the vehicle security system further comprises utilizing a global positioning device to determine a location where the vehicle is to be automatically shut down.

19. The system of claim 9, wherein the activation of the vehicle security system comprises one or more of flashing a vehicle light, honking a vehicle horn, or preventing the vehicle from exceeding a predetermined speed.

20. In a computer readable storage medium having stored therein instructions executable by a programmed processor for determining if a vehicle is stolen, the storage medium comprising instructions for:

determining whether a received signal was changed at the transmission source and whether the received signal was changed after transmission; and

activating a vehicle security device if the received signal was changed.

21. An apparatus for self-detecting theft in a vehicle, comprising:

a first antenna configured to transmit a signal and attached to a network access device that is located on the vehicle;

a second antenna configured to receive the signal and located on the vehicle;

a monitoring module in communication with the second antenna and configured to analyze the signal, the analysis of the signal comprising determining whether the signal is interrupted, determining whether the signal magnitude varies from a predetermined baseline magnitude, detecting patterns in the signal, and analyzing data in the signal;

a stolen vehicle tracking device configured to detect a functional status of a transmitter; and

a vehicle security device configured to disable the vehicle based upon the analysis of the signal and if the functional status of a transmitter is operative.

1/4

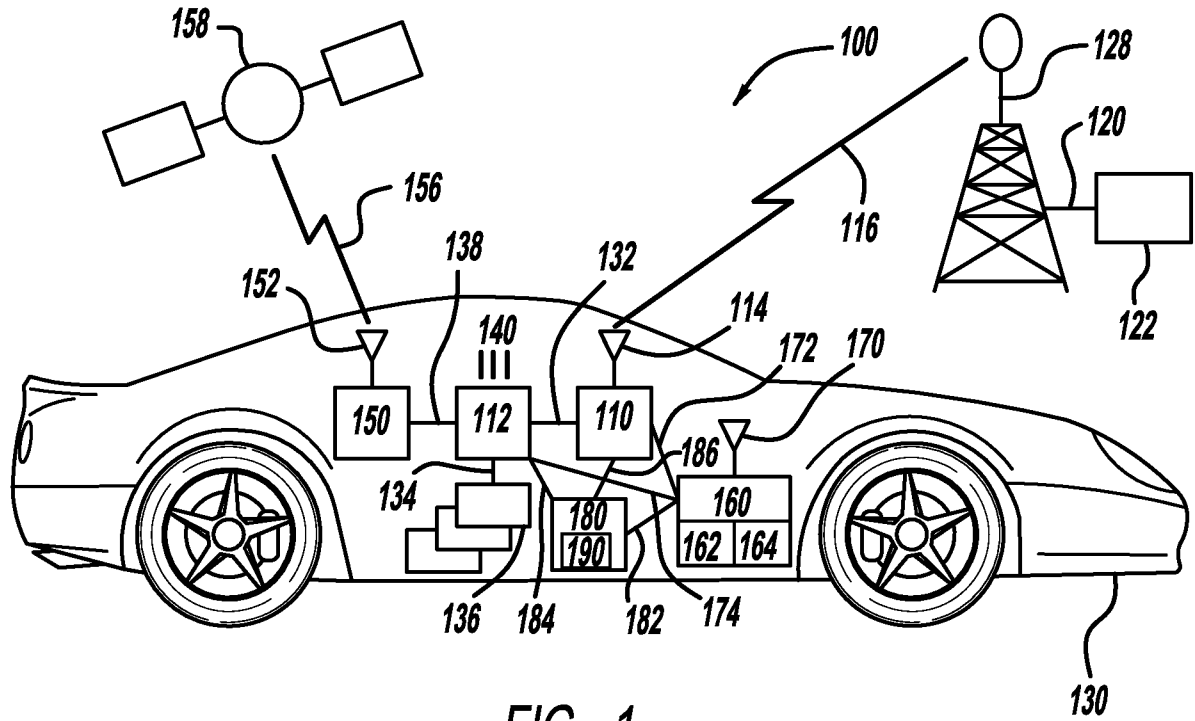


FIG - 1

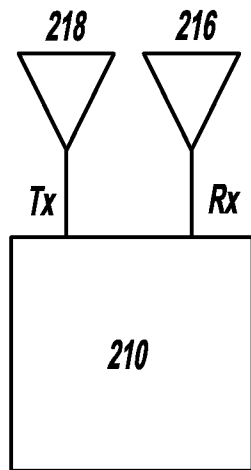


FIG - 2

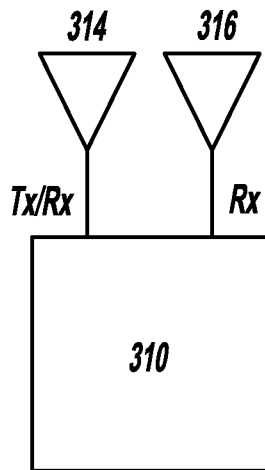


FIG - 3

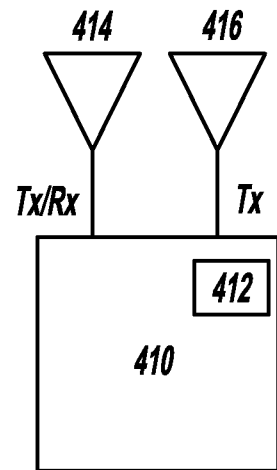
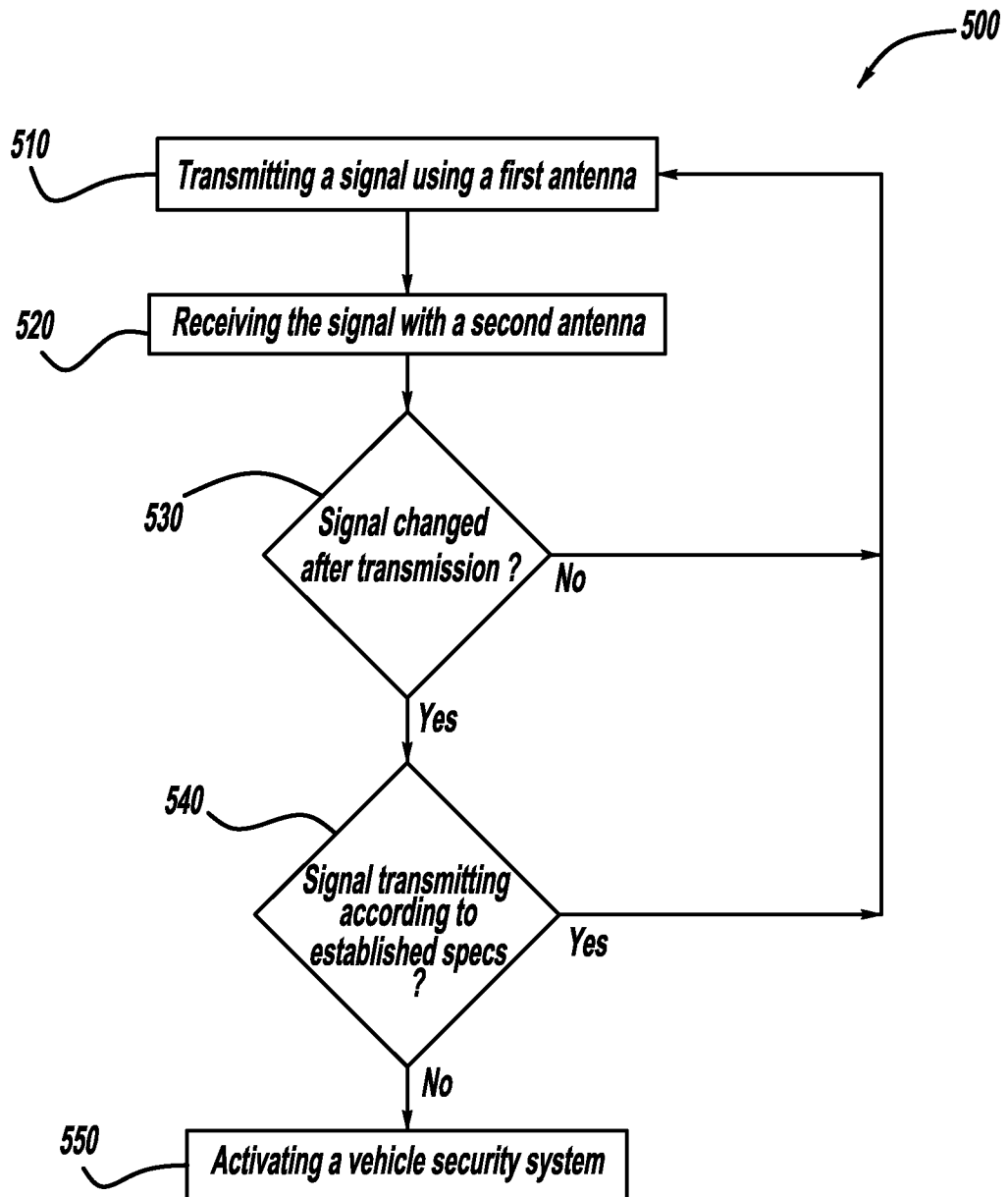
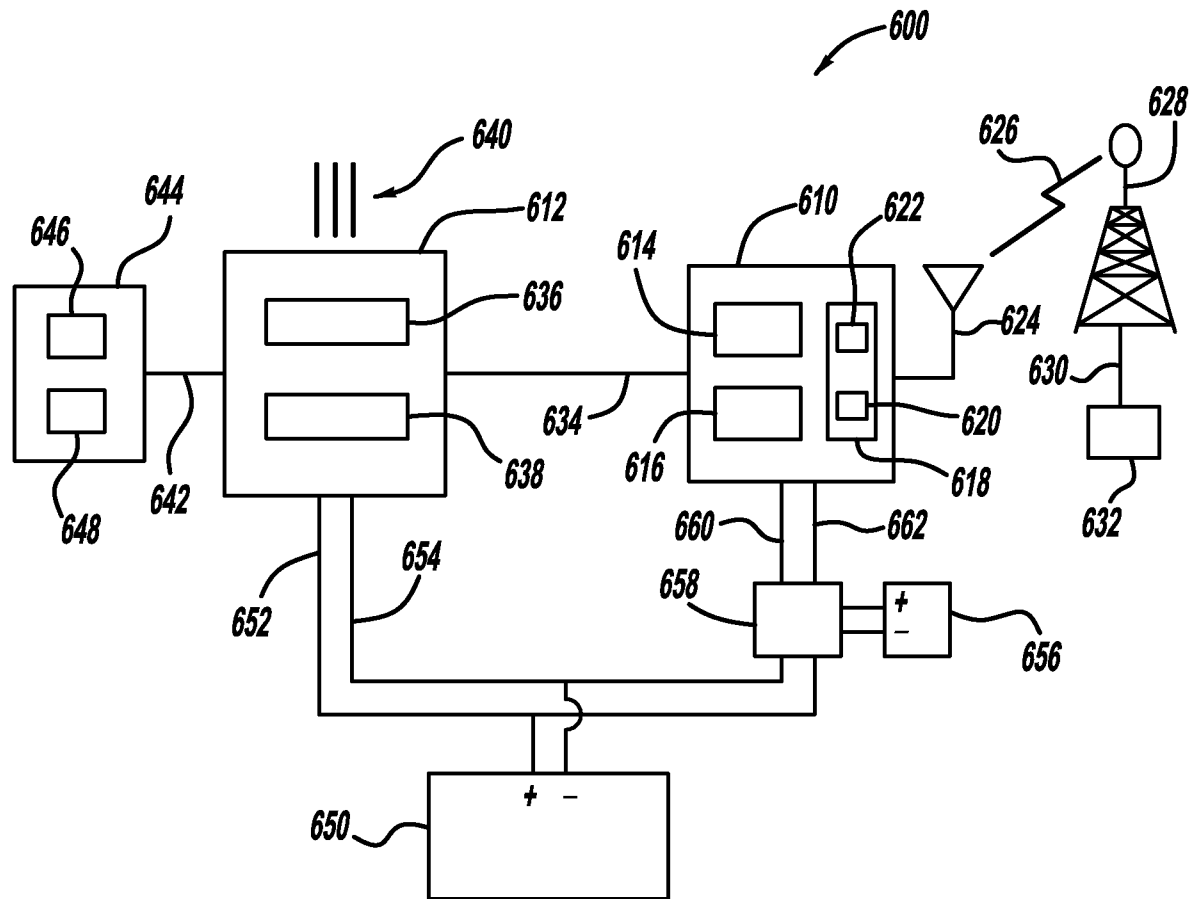


FIG - 4

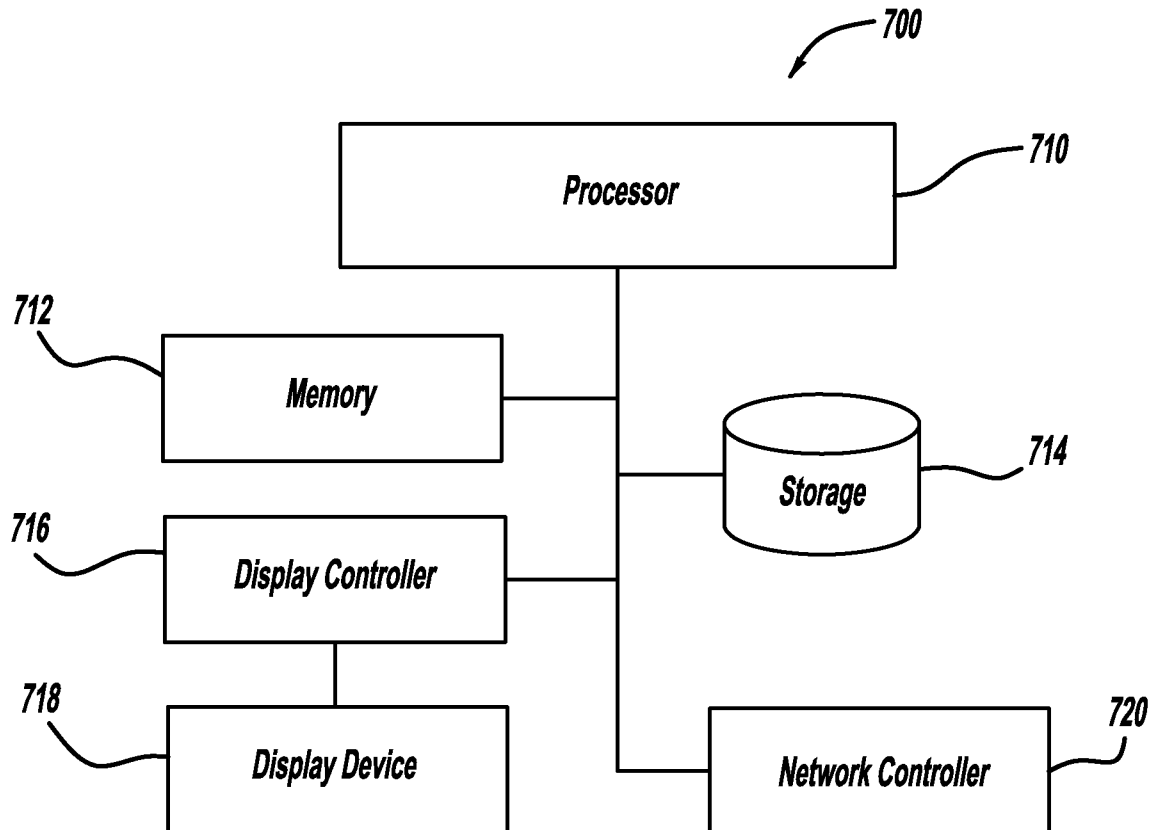
2/4

FIG - 5

3/4

FIG - 6

4/4

FIG - 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/029730

A. CLASSIFICATION OF SUBJECT MATTER
INV. B60R25/10 H04K3/00 G08B25/10
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
B60R H04K G08B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/090952 A1 (BOULAY ANDRE E [CA] ET AL) 28 April 2005 (2005-04-28) abstract; figures 1,2 paragraphs [0018] - [0022] -----	1,2, 5-12, 17-21
X	DE 10 2004 048668 A1 (STEINBRUCKER HARALD [DE]) 13 April 2006 (2006-04-13) abstract; figure paragraphs [0003], [0018], [0020], [0023] - [0024] -----	1,2,5-21
A	US 2005/085951 A1 (WALKER GLENN A [US] ET AL) 21 April 2005 (2005-04-21) abstract; figure 2 ----- -/-	2-4



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

8 June 2012

Date of mailing of the international search report

15/06/2012

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Sleightholme-Albanis

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/029730

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 93/05490 A1 (MATOUSCHEK ERICH [DE]; MATOUSCHEK THOMAS [DE]; WALLISER BRIGITTE [DE]) 18 March 1993 (1993-03-18) page 6, paragraph 3; figure 1 -----	14

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2012/029730

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005090952	A1	28-04-2005	NONE
DE 102004048668	A1	13-04-2006	NONE
US 2005085951	A1	21-04-2005	NONE
WO 9305490	A1	18-03-1993	EP 0555437 A1 18-08-1993
			ES 2093841 T3 01-01-1997
			WO 9305490 A1 18-03-1993