(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 576 348 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
20.08.2025 Bulletin 2025/34

(21) Application number: **17894411.2**

(22) Date of filing: **08.05.2017**

(51) International Patent Classification (IPC):
H04L 43/50 *(2022.01)* ***H04W 12/12*** *(2021.01)*
G06F 21/44 *(2013.01)* ***G06F 21/57*** *(2013.01)*
H04L 9/40 *(2022.01)* *H04L 43/028* *(2022.01)*
H04L 43/18 *(2022.01)*

(52) Cooperative Patent Classification (CPC):
H04L 43/50; G06F 21/44; G06F 21/577; H04L 63/1433; H04W 12/12; H04L 41/24; H04L 43/028; H04L 43/18; H04L 67/12

(86) International application number:
PCT/KR2017/004778

(87) International publication number:
WO 2018/139708 (02.08.2018 Gazette 2018/31)

(54) APPARATUS FOR TESTING HACKING OF VEHICLE ELECTRONIC DEVICE

VORRICHTUNG ZUR PRÜFUNG DES HACKENS EINER ELEKTRONISCHEN VORRICHTUNG EINES FAHRZEUGES

APPAREIL SERVANT À TESTER LE PIRATAGE D'UN DISPOSITIF ÉLECTRONIQUE DE VÉHICULE

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **24.01.2017 KR 20170010769**

(43) Date of publication of application:
04.12.2019 Bulletin 2019/49

(73) Proprietors:
- **LG Electronics Inc.**
  Seoul 07336 (KR)
- **Korea University Research and Business Foundation**
  Seoul 02841 (KR)

(72) Inventors:
- **KIM, Cheolseung**
  Seoul 06772 (KR)
- **JO, Byeongrim**
  Seoul 06772 (KR)
- **KIM, Seongsoo**
  Seoul 06772 (KR)
- **LEE, Heejo**
  Seoul 03711 (KR)
- **LEE, Choongin**
  Euijeongbu-si
  Gyeonggi-do 11665 (KR)
- **KIM, Donghyeok**
  Youngju-si
  Gyeongsangbuk-do 36092 (KR)

(74) Representative: **Mooser, Sebastian Thomas**
Wuesthoff & Wuesthoff
Patentanwälte und Rechtsanwalt PartG mbB
Schweigerstraße 2
81541 München (DE)

(56) References cited:
KR-A- 20080 043 209
KR-A- 20150 017 255
KR-B1- 101 446 525
KR-B1- 101 525 398
US-A1- 2013 340 083
US-A1- 2016 350 211

- **HUMBERTO ABDELNUR ET AL: "KiF: A stateful SIP fuzzer", PROCEEDINGS OF THE 1ST INTERNATIONAL CONFERENCE ON PRINCIPLES, SYSTEMS AND APPLICATIONS OF IP TELECOMMUNICATIONS, 19 July 2007 (2007-07-19), pages 47 - 56, XP055717917, ISBN: 978-1-60558-006-7, DOI: 10.1145/1326304.1326313**

Processed by Luminess, 75001 PARIS (FR)

(Cont. next page)

- STEPHANIE BAYER ET AL: "Don't Fuss about Fuzzing: Fuzzing Controllers in Vehicular Networks", 1 January 2015 (2015-01-01), XP055393346, Retrieved from the Internet <URL:https://www.escar.info/images/Datastore/2015_escar_EU_Papers/3_escar_2015_Stephanie_Bayer.pdf> [retrieved on 20170724]
- NEVES N ET AL: "Using Attack Injection to Discover New Vulnerabilities", DEPENDABLE SYSTEMS AND NETWORKS, 2006. DSN 2006. INTERNATIONAL CONFERENCE ON, PHILADELPHIA, PA, USA, 25 June 2006 (2006-06-25), pages 457 - 466, XP010925332, ISBN: 978-0-7695-2607-2, DOI: 10.1109/DSN.2006.72
- GREG BANKS ET AL: "SNOOZE: Toward a Stateful NetwOrk prOtocol fuzZEr", 1 January 2006, INFORMATION SECURITY LECTURE NOTES IN COMPUTER SCIENCE;;LNCS, SPRINGER, BERLIN, DE, PAGE(S) 343 - 358, ISBN: 978-3-540-38341-3, XP019042380
- HONG, JINKEUN: "Cyber Security Issues in Connected Vehicle of Intelligent Transport System", INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY, vol. 9, no. 24, June 2016 (2016-06-01), pages 1 - 7, XP055558955

Description

TECHNICAL FIELD

[0001] The present invention relates to a vehicular electronic device hacking test apparatus.

BACKGROUND ART

[0002] A vehicle refers to a device that carries a passenger in a passenger-intended direction. A car is a major example of the vehicle.

[0003] To increase the convenience of vehicle users, a vehicle is equipped with various sensors and electronic devices. Especially, an advanced driver assistance system (ADAS) and an autonomous vehicle are under active study to increase the driving convenience of users.

[0004] Various devices are installed in such vehicles. Recently, various media have released cases of hacking a vehicle. As a method of preventing such hacking, a device that is not vulnerable to hacking is manufactured.

[0005] Further prior art can be found in Humberto Abdelnur et al, "KiF: A stateful SIP Fuzzer", 10.1145/1326304.1326313, in Stephanie Bayer et al, "Don't Fuss About Fuzzing: Fuzzing Controllers in Vehicular Networks", in US 2016/350211 A1 which generally relates to whitebox network fuzzing, in Neves N. et al, "Using Attack Injection to Discover New Vulnerabilities", 10.1109/DSN.2006.72, in Greg Banks et al, "SNOOZE: Toward a Stateful NetwOrk protocol fuzZEr", 978-3-540-38341-3 and in US 2013/340083 A1 which generally relates to methods, systems, and computer readable media for automatically generating a fuzzer that implements functional and fuzz testing and testing a network device using the fuzzer.

DISCLOSURE

TECHNICAL PROBLEM

[0006] To overcome the above problems, embodiments of the present invention provide a hacking test apparatus for checking whether a vehicular electronic device is vulnerable to hacking.

[0007] It is to be understood that both the foregoing general description and the following detailed description of the present invention are exemplary and explanatory and are intended to provide further explanation of the invention as claimed.

TECHNICAL SOLUTION

[0008] The invention is set out in the independent claim. Preferred embodiments of the invention are outlined in the dependent claims.

[0009] We describe a vehicular electronic device hacking test apparatus comprising: a transmitter; a receiver; and a processor configured to classify a communication-connection procedure into one state out of a plurality of states based on a preset communication protocol, to generate a first mutated packet appropriate for the state within which the communication-connection procedure has been classified, and to transmit the first mutated packet to a vehicular electronic device through the transmitter wherein the processor is further configured to: randomly determine a next state among the plurality of states, in case that a first reception packet corresponding to the first mutated packet is received through the receiver, generate a second mutated packet appropriate for the randomly determined next state, and transmit the second mutated packet appropriate for the randomly determined next state to the vehicular electronic device through the transmitter, wherein the first mutated packet is generated by mutating a portion of an original packet to be transmitted in the state within which the communication-connection procedure has been classified and the second mutated packet is generated by mutating a portion of an original packet to be transmitted in the randomly determined next state, wherein the processor is further configured to mutate an arbitrary portion of an information payload of the original packet to generate the first mutated packet or the second mutated packet, wherein the processor is further configured to determine whether the vehicular electronic device is vulnerable to hacking based on whether the first reception packet corresponding to the first mutated packet or a second reception packet corresponding to the second mutated packet is received through the receiver. .

[0010] Details of other embodiments are included in detailed descriptions and drawings.

ADVANTAGEOUS EFFECTS

[0011] As is apparent from the foregoing description, the embodiments of the present invention have the following one or more effects.

[0012] First, whether a vehicular electronic device is vulnerable to hacking may be determined for each of a plurality of states, and thus whether the vehicular electronic device is vulnerable to hacking may be more precisely determined.

[0013] Second, hacking of the vehicular electronic device may be prevented through a test with respect to various devices included in a vehicle.

[0014] Third, a test may be performed while a plurality of states are randomly changed, and thus whether the vehicular electronic device is vulnerable to hacking may be more accurately identified.

[0015] It will be appreciated by persons skilled in the art that that the effects that could be achieved with the present invention are not limited to what has been particularly described hereinabove and other advantages of the present invention will be more clearly understood from the following claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016]

FIG. 1 is a diagram showing a hacking device for a vehicle and a vehicle according to an embodiment of the present invention.

FIG. 2 is a block diagram for explanation of a vehicle according to an embodiment of the present invention.

FIG. 3 is a block diagram for explanation of a vehicular electronic device hacking test apparatus according to an embodiment of the present invention.

FIG. 4 is a diagram for explanation of an operation of a vehicular electronic device hacking test apparatus according to an embodiment of the present invention.

FIG. 5 is a diagram for explanation of an operation of generating a mutated packet according to an embodiment of the present invention.

FIG. 6 is a diagram for explanation of a mutated packet implemented in a hexadecimal digit according to an embodiment of the present invention.

FIGS. 7 and 8 are diagrams for explanation of a vehicular electronic device hacking test apparatus based on Wi-Fi protocol according to an embodiment of the present invention.

FIG. 9 is a diagram for explanation of a vehicular electronic device hacking test apparatus based on a Wi-Fi protocol according to an embodiment of the present invention.

FIGS. 10 and 11 are diagrams for explanation of a vehicular electronic device hacking test apparatus based on a Bluetooth protocol according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0017] Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts. As used herein, the suffixes "module" and "unit" are added or interchangeably used to facilitate preparation of this specification and are not intended to suggest unique meanings or functions. In describing embodiments disclosed in this specification, a detailed description of relevant well-known technologies may not be given in order not to obscure the subject matter of the present invention. In addition, the accompanying drawings are merely intended to facilitate understanding of the embodiments disclosed in this specification and not to restrict the present invention. In addition, the accompanying drawings should be understood as covering all substitutions within the scope of the present invention.

[0018] Terms including ordinal numbers such as first, second, etc. may be used to explain various elements. However, it will be appreciated that the elements are not limited to such terms. These terms are merely used to distinguish one element from another.

[0019] Stating that one constituent is "connected" or "linked" to another should be understood as meaning that the one constituent may be directly connected or linked to another constituent or another constituent may be interposed between the constituents. On the other hand, stating that one constituent is "directly connected" or "directly linked" to another should be understood as meaning that no other constituent is interposed between the constituents.

[0020] As used herein, the singular forms "a", "an", and "the" are intended to include the plural forms as well, unless context clearly indicates otherwise.

[0021] In this specification, terms such as "includes" or "has" are intended to indicate existence of characteristics, figures, steps, operations, constituents, components, or combinations thereof disclosed in the specification. The terms "includes" or "has" should be understood as not precluding possibility of existence or addition of one or more other characteristics, figures, steps, operations, constituents, components, or combinations thereof.

[0022] The term "vehicle" employed in this specification may include an automobile and a motorcycle. Hereinafter, description will be given mainly focusing on an automobile.

[0023] The vehicle described in this specification may include a vehicle equipped with an internal combustion engine as a power source, a hybrid vehicle equipped with both an engine and an electric motor as a power source, and an electric vehicle equipped with an electric motor as a power source.

[0024] In the description below, the left side of the vehicle means the left side with respect to the travel direction of the vehicle and the right side of the vehicle means the right side with respect to the travel direction of the vehicle.

[0025] FIG. 1 is a diagram showing a hacking device for a vehicle and a vehicle according to an embodiment of the present invention.

[0026] FIG. 2 is a block diagram for explanation of a vehicle according to an embodiment of the present invention.

[0027] Referring to FIGS. 1 to 2, a vehicle 100 may include wheels rotated by a power source, and a steering input device 510 for controlling a travel direction of the vehicle 100.

[0028] The vehicle 100 may be an autonomous vehicle.

[0029] The vehicle 100 may switch to an autonomous driving mode or a manual mode according to a user input.

[0030] For example, the vehicle 100 may switch from the manual mode to the autonomous driving mode or from the autonomous driving mode to the manual mode, based on a user input received through a user interface

(UI) device 200.

[0031] The vehicle 100 may switch to the autonomous driving mode or the manual mode based on traveling situation information.

[0032] The traveling situation information may include at least one of information about objects outside the vehicle, navigation information, or vehicle state information.

[0033] For example, the vehicle 100 may switch from the manual mode to the autonomous driving mode or from the autonomous driving mode to the manual mode, based on traveling situation information generated from an object detection device 300.

[0034] For example, the vehicle 100 may switch from the manual mode to the autonomous driving mode or from the autonomous driving mode to the manual mode, based on traveling situation information generated from a communication device 400.

[0035] The vehicle 100 may switch from the manual mode to the autonomous driving mode or from the autonomous driving mode to the manual mode, based on information, data, or a signal provided from an external device.

[0036] If the vehicle 100 travels in the autonomous driving mode, the autonomous vehicle 100 may be operated based on an operation system 700.

[0037] For example, the autonomous vehicle 100 may travel based on information, data, or signals generated from a traveling system 710, a park-out system 740, and a park-in system.

[0038] If the vehicle 100 drives in the manual mode, the autonomous vehicle 100 may receive a user input for driving through a driving manipulation device 500. The vehicle 100 may travel based on the user input received through the driving manipulation device 500.

[0039] The overall length refers to the length of the vehicle 100 from the front to back of the vehicle 100, the width refers to the width of the vehicle 100, and the height refers to the distance from the bottom of wheels to the roof of the vehicle. In the description below, the overall-length direction L may indicate a direction in which measurement of overall length of the vehicle 100 is performed, the width direction W may indicate a direction in which measurement of width of the vehicle 100 is performed, and the height direction H may indicate a direction in which measurement of height of the vehicle 100 is performed.

[0040] The vehicle 100 may include the UI device 200, the object detection device 300, the communication device 400, the driving manipulation device 500, a vehicle driving device 600, the operation system 700, a navigation system 770, a sensing unit 120, an interface unit 130, a memory 140, a controller 170, and a power supply 190.

[0041] In some embodiments, the vehicle 100 may further include a new component in addition to the components described in the present invention, or may not include a part of the described components.

[0042] The UI device 200 is used to enable the vehicle 100 to communicate with a user. The UI device 200 may receive a user input, and provide information generated from the vehicle 100 to the user. The vehicle 100 may implement UIs or User Experience (UX) through the UI device 200.

[0043] The UI device 200 may include an input unit 210, an internal camera 220, a biometric sensing unit 230, an output unit 250, and a processor 270.

[0044] In some embodiments, the UI device 200 may further include a new component in addition to components described below, or may not include a part of the described components.

[0045] The input unit 210 is provided to receive information from a user. Data collected by the input unit 210 may be analyzed by the processor 270 and processed as a control command from the user.

[0046] The input unit 210 may be disposed inside the vehicle 100. For example, the input unit 210 may be disposed in an area of a steering wheel, an area of an instrument panel, an area of a seat, an area of a pillar, an area of a door, an area of a center console, an area of a head lining, an area of a sun visor, an area of a windshield, an area of a window, or the like.

[0047] The input unit 210 may include a voice input unit 211, a gesture input unit 212, a touch input unit 213, and a mechanical input unit 214.

[0048] The voice input unit 211 may convert a voice input of the user to an electrical signal. The electrical signal may be provided to the processor 270 or the controller 170.

[0049] The voice input unit 211 may include one or more microphones.

[0050] The gesture input unit 212 may convert a gesture input of the user to an electrical signal. The electrical signal may be provided to the processor 270 or the controller 170.

[0051] The gesture input unit 212 may include at least one of an infrared (IR) sensor or an image sensor, for sensing a gesture input of the user.

[0052] In some embodiments, the gesture input unit 212 may sense a three-dimensional (3D) gesture input of the user. For this purpose, the gesture input unit 212 may include a light output unit for emitting a plurality of IR rays or a plurality of image sensors.

[0053] The gesture input unit 212 may sense a 3D gesture input of the user by Time of Flight (ToF), structured light, or disparity.

[0054] The touch input unit 213 may convert a touch input of the user to an electrical signal. The electrical signal may be provided to the processor 270 or the controller 170.

[0055] The touch input unit 213 may include a touch sensor for sensing a touch input of the user.

[0056] In some embodiments, a touch screen may be configured by integrating the touch input unit 213 with a display unit 251. The touch screen may provide both an input interface and an output interface between the vehicle 100 and the user.

[0057] The mechanical input unit 214 may include at

least one of a button, a dome switch, a jog wheel, or a jog switch. An electrical signal generated by the mechanical input unit 214 may be provided to the processor 270 or the controller 170.

[0058] The mechanical input unit 214 may be disposed on the steering wheel, the center fascia, the center console, the cockpit module, a door, or the like.

[0059] The internal camera 220 may acquire a vehicle interior image. The processor 270 may sense a state of a user based on the vehicle interior image. The processor 270 may acquire information about the gaze of a user in the vehicle interior image. The processor 270 may sense the user's gesture in the vehicle interior image.

[0060] The biometric sensing unit 230 may acquire biometric information about a user. The biometric sensing unit 230 may include a sensor for acquiring biometric information about a user, and acquire information about a fingerprint, heart beats, and so on of a user, using the sensor. The biometric information may be used for user authentication.

[0061] The output unit 250 is provided to generate a visual output, an acoustic output, or a haptic output.

[0062] The output unit 250 may include at least one of the display unit 251, an audio output unit 252, or a haptic output unit 253.

[0063] The display unit 251 may display graphic objects corresponding to various kinds of information.

[0064] The display unit 251 may include at least one of a liquid crystal display (LCD), a thin film transistor-liquid crystal display (TFT LCD), an organic light-emitting diode (OLED) display, a flexible display, a 3D display, or an e-ink display.

[0065] The display unit 251 may form a layered structure together with the touch input unit 213 or be integrated with the touch input unit 213, thereby implementing a touchscreen.

[0066] The display unit 251 may be implemented as a head up display (HUD). In this case, the display unit 251 may be provided with a projection module, and output information by an image projected onto the windshield or a window.

[0067] The display unit 251 may include a transparent display. The transparent display may be attached to the windshield or a window.

[0068] The transparent display may display a specific screen with a specific transparency. To have a transparency, the transparent display may include at least one of a transparent Thin Film Electroluminescent (TFFL) display, a transparent OLED display, a transparent LCD, a transmissive transparent display, or a transparent LED display. The transparency of the transparent display is adjustable.

[0069] The UI device 200 may include a plurality of display units 251a to 251g.

[0070] The display unit 251 may be disposed in an area of the steering wheel, areas 251a, 251b, and 251e of the instrument panel, an area 251d of a seat, an area 251f of a pillar, an area 251g of a door, an area of the center console, an area of a head lining, or an area of a sun visor, or may be implemented in an area 251c of the windshield, and an area 251h of a window.

[0071] The audio output unit 252 converts an electrical signal received from the processor 270 or the controller 170 to an audio signal, and outputs the audio signal. To this end, the audio output unit 252 may include one or more speakers.

[0072] The haptic output unit 253 generates a haptic output. For example, the haptic output unit 253 may vibrate the steering wheel, a seat belt, a seat 110FL, 110FR, 110RL, or 110RR, so that a user may perceive the output.

[0073] The processor 270 may control an operation of each unit of the UI device 200.

[0074] In some embodiments, the UI device 200 may include a plurality of processors 270 or no processor 270.

[0075] If the UI device 200 does not include any processor 270, the UI device 200 may operate under control of a processor of another device in the vehicle 100, or under control of the controller 170.

[0076] The UI device 200 may be referred to as a vehicle display device.

[0077] The UI device 200 may operate under control of the controller 170.

[0078] The object detection device 300 is used to detect an object outside the vehicle 100. The object detection device 300 may generate object information based on sensing data.

[0079] The object information may include information indicating presence or absence of an object, information about the location of an object, information indicating the distance between the vehicle 100 and the object, and information about a relative speed of the vehicle 100 with respect to the object.

[0080] The object may be any of various objects related to driving of the vehicle 100.

[0081] The object O may include a lane OB10, another vehicle OB11, a pedestrian OB12, a two-wheeled vehicle OB13, a traffic signal OB14 and OB15, light, a road, a structure, a speed bump, a geographical feature, and an animal.

[0082] The lane OB10 may include a traveling lane, a lane next to the traveling lane, and a lane in which a vehicle is driving in the opposite direction. The lane OB10 may conceptually include left and right lines that define each of the lanes.

[0083] The other vehicle OB11 may be a vehicle traveling in the vicinity of the vehicle 100. The other vehicle OB11 may be located within a predetermined distance from the vehicle 100. For example, the other vehicle OB11 may precede or follow the vehicle 100.

[0084] The pedestrian OB12 may be a person located around the vehicle 100. The pedestrian OB12 may be a person located within a predetermined distance from the vehicle 100. For example, the pedestrian OB12 may be a person on a sidewalk or a roadway.

[0085] The two-wheel vehicle OB13 may refer to a

transportation means moving on two wheels, located around the vehicle 100. The two-wheel vehicle OB13 may be a transportation means having two wheels, located within a predetermined distance from the vehicle 100. For example, the 2-wheel vehicle OB13 may be a motorcycle or bicycle on a sidewalk or a roadway.

[0086] The traffic signals may include a traffic signal lamp OB15, a traffic sign OB14, and a symbol or text drawn or written on a road surface.

[0087] The light may be light generated from a lamp of another vehicle. The light may be generated from a street lamp. The light may be sunlight.

[0088] The road may include a road surface, a curve, and a slope such as an uphill or downhill road.

[0089] The structure may be an object fixed on the ground, near to a road. For example, the structure may be any of a street lamp, a street tree, a building, a utility pole, a signal lamp, and a bridge.

[0090] The geographical feature may include a mountain, a hill, and so on.

[0091] Objects may be classified into mobile objects and stationary objects. For example, the mobile objects may conceptually include another vehicle and a pedestrian. For example, the stationary objects may conceptually include a traffic signal, a road, and a structure.

[0092] The object detection device 300 may include a camera 310, a Radio Detection and Ranging (RADAR) 320, a Light Detection and Ranging (LiDAR) 330, an ultrasonic sensor 340, an IR sensor 350, and a processor 370.

[0093] In some embodiments, the object detection device 300 may further include a new component in addition to components described below or may not include a part of the described components.

[0094] To acquire a vehicle exterior image, the camera 310 may be disposed at an appropriate position on the exterior of the vehicle 100. The camera 310 may be a mono camera, a stereo camera 310a, around view monitoring (AVM) cameras 310b, or a 360-degree camera.

[0095] The camera 310 may acquire information about the location of an object, information about a distance to the object, or information about a relative speed with respect to the object by any of various image processing algorithms.

[0096] For example, the camera 310 may acquire information about a distance to an object and information about a relative speed with respect to the object in an acquired image, based on a variation in the size of the object over time.

[0097] For example, the camera 310 may acquire information about a distance to an object and information about a relative speed with respect to the object through a pin hole model, road surface profiling, or the like.

[0098] For example, the camera 310 may acquire information about a distance to an object and information about a relative speed with respect to the object based on disparity information in a stereo image acquired by the stereo camera 310a.

[0099] For example, to acquire an image of the front view of the vehicle 100, the camera 310 may be disposed in the vicinity of a front windshield inside the vehicle 100. Alternatively, the camera 310 may be disposed around a front bumper or a radiator grille.

[0100] For example, to acquire an image of what lies behind the vehicle 100, the camera 310 may be disposed in the vicinity of a rear glass inside the vehicle 100. Or the camera 310 may be disposed around a rear bumper, a trunk, or a tail gate.

[0101] For example, to acquire an image of what lies on a side of the vehicle 100, the camera 310 may be disposed in the vicinity of at least one of side windows inside the vehicle 100. Alternatively, the camera 310 may be disposed around a side view mirror, a fender, or a door.

[0102] The camera 310 may provide an acquired image to the processor 370.

[0103] The RADAR 320 may include an electromagnetic wave transmitter and an electromagnetic wave receiver. The RADAR 320 may be implemented by pulse RADAR or continuous wave RADAR. The RADAR 320 may be implemented by Frequency Modulated Continuous Wave (FMCW) or Frequency Shift Keying (FSK) as a pulse RADAR scheme according to a signal waveform.

[0104] The RADAR 320 may detect an object in TOF or phase shifting by electromagnetic waves, and determine the location, distance, and relative speed of the detected object.

[0105] The RADAR 320 may be disposed at an appropriate position on the exterior of the vehicle 100 in order to sense an object ahead of, behind, or on a side of the vehicle 100.

[0106] The LiDAR 330 may include a laser transmitter and a laser receiver. The LiDAR 330 may be implemented in TOF or phase shifting.

[0107] The LiDAR 330 may be implemented in a driven or non-driven manner.

[0108] If the LiDAR 330 is implemented in the driven manner, the LiDAR 330 may be rotated by a motor and detect an object around the vehicle 100.

[0109] If the LiDAR 330 is implemented in a non-driven manner, the LiDAR 330 may detect an object within a predetermined range from the vehicle 100 by optical steering. The vehicle 100 may include a plurality of non-driven LiDARs 330.

[0110] The LiDAR 330 may detect an object in TOF or phase shifting by laser light, and determine the location, distance, and relative speed of the detected object.

[0111] The LiDAR 330 may be disposed at an appropriate position on the exterior of the vehicle 100 in order to sense an object ahead of, behind, or on a side of the vehicle 100.

[0112] The ultrasonic sensor 340 may include an ultrasonic wave transmitter and an ultrasonic wave receiver. The ultrasonic sensor 340 may detect an object by ultrasonic waves, and determine the location, distance, and relative speed of the detected object.

[0113] The ultrasonic sensor 340 may be disposed at

an appropriate position on the exterior of the vehicle 100 in order to sense an object ahead of, behind, or on a side of the vehicle 100.

[0114] The IR sensor 350 may include an IR transmitter and an IR receiver. The IR sensor 350 may detect an object by IR light, and determine the location, distance, and relative speed of the detected object.

[0115] The IR sensor 350 may be disposed at an appropriate position on the exterior of the vehicle 100 in order to sense an object ahead of, behind, or on a side of the vehicle 100.

[0116] The processor 370 may control an overall operation of each unit of the object detection device 300.

[0117] The processor 370 may compare data sensed by the camera 310, the RADAR 320, the LiDAR 330, the ultrasonic sensor 340, and the IR sensor 350 with prestored data to detect or classify an object.

[0118] The processor 370 may detect and track an object based on the acquired image. The processor 370 may calculate a distance to the object, a relative speed with respect to the object, and so on by an image processing algorithm.

[0119] For example, the processor 370 may acquire information about a distance to an object and information about a relative speed with respect to the object from an acquired image, based on a variation in the size of the object over time.

[0120] For example, the processor 370 may acquire information about a distance to an object and information about a relative speed with respect to the object from an image acquired from the stereo camera 310a.

[0121] For example, the processor 370 may acquire information about a distance to an object and information about a relative speed with respect to the object from an image acquired from the stereo camera 310a, based on disparity information.

[0122] The processor 370 may detect an object and track the detected object based on electromagnetic waves which are transmitted, are reflected from an object, and then return. The processor 370 may calculate a distance to the object and a relative speed with respect to the object, based on the electromagnetic waves.

[0123] The processor 370 may detect an object and track the detected object based on laser light which is transmitted, is reflected from an object, and then returns. The sensing processor 370 may calculate a distance to the object and a relative speed with respect to the object, based on the laser light.

[0124] The processor 370 may detect an object and track the detected object based on ultrasonic waves which are transmitted, are reflected from an object, and then return. The processor 370 may calculate a distance to the object and a relative speed with respect to the object, based on the ultrasonic waves.

[0125] The processor 370 may detect an object and track the detected object based on IR light which is transmitted, is reflected from an object, and then returns. The processor 370 may calculate a distance to the object and a relative speed with respect to the object, based on the IR light.

[0126] In some embodiments, the object detection device 300 may include a plurality of processors 370 or no processor 370. For example, the camera 310, the RADAR 320, the LiDAR 330, the ultrasonic sensor 340, and the IR sensor 350 may include individual processors.

[0127] If the object detection device 300 includes no processor 370, the object detection device 300 may operate under control of a processor of a device in the vehicle 100 or under control of the controller 170.

[0128] The object detection device 300 may operate under control of the controller 170.

[0129] The communication device 400 is used to communicate with an external device. The external device may be another vehicle, a mobile terminal, or a server.

[0130] The communication device 400 may include at least one of a transmit antenna and a receive antenna, for communication, or a Radio Frequency (RF) circuit and device, for implementing various communication protocols.

[0131] The communication device 400 may include a short-range communication unit 410, a location information unit 420, a vehicle-to-everything (V2X) communication unit 430, an optical communication unit 440, a broadcasting transceiver unit 450, an intelligent transport system (ITS) communication unit 460, and a processor 470.

[0132] In some embodiments, the communication device 400 may further include a new component in addition to components described below, or may not include a part of the described components.

[0133] The short-range communication module 410 is a unit for conducting short-range communication. The short-range communication module 410 may support short-range communication, using at least one of Bluetooth™, Radio Frequency Identification (RFID), Infrared Data Association (IrDA), Ultra Wideband (UWB), ZigBee, Near Field Communication (NFC), Wireless Fidelity (Wi-Fi), Wi-Fi Direct, or Wireless Universal Serial Bus (Wireless USB).

[0134] The short-range communication unit 410 may conduct short-range communication between the vehicle 100 and at least one external device by establishing a wireless area network.

[0135] The location information unit 420 is a unit configured to acquire information about a location of the vehicle 100. The location information unit 420 may include at least one of a global positioning system (GPS) module or a Differential Global Positioning System (DGPS) module.

[0136] The V2X communication unit 430 is a unit used for wireless communication with a server (by vehicle-to-infrastructure (V2I)), another vehicle (by Vehicle to Vehicle (V2V)), or a pedestrian (by Vehicle to Pedestrian (V2P)). The V2X communication unit 430 may include an RF circuit capable of implementing a V2I protocol, a V2V protocol, and a V2P protocol.

[0137] The optical communication unit 440 is a unit

used to communicate with an external device by light. The optical communication unit 440 may include an optical transmitter for converting an electrical signal to an optical signal and emitting the optical signal to the outside, and an optical receiver for converting a received optical signal to an electrical signal.

[0138] In some embodiments, the optical transmitter may be integrated with a lamp included in the vehicle 100.

[0139] The broadcasting transceiver unit 450 is a unit used to receive a broadcast signal from an external broadcasting management server or transmit a broadcast signal to the broadcasting management server, on a broadcast channel. The broadcast channel may include a satellite channel and a terrestrial channel. The broadcast signal may include a TV broadcast signal, a radio broadcast signal, and a data broadcast signal.

[0140] The ITS communication unit 460 may exchange information, data, or signals with a traffic system. The ITS communication unit 460 may provide acquired information and data to the traffic system. The ITS communication unit 460 may receive information, data, or a signal from the traffic system. For example, the ITS communication unit 460 may receive traffic information from the traffic system and provide the received traffic information to the controller 170. For example, the ITS communication unit 460 may receive a control signal from the traffic system, and provide the received control signal to the controller 170 or a processor in the vehicle 100.

[0141] The processor 470 may control an overall operation of each unit of the communication device 400.

[0142] In some embodiments, the communication device 400 may include a plurality of processors 470 or no processor 470.

[0143] If the communication device 400 does not include any processor 470, the communication device 400 may operate under control of a processor of another device in the vehicle 100 or under control of the controller 170.

[0144] The communication device 400 may be configured along with the UI device 200, as a vehicle multimedia device. In this case, the vehicle multimedia device may be referred to as a telematics device or an Audio Video Navigation (AVN) device.

[0145] The communication device 400 may operate under control of the controller 170.

[0146] The driving manipulation device 500 is used to receive a user command for driving the vehicle 100.

[0147] In the manual mode, the vehicle 100 may travel based on a signal provided by the driving manipulation device 500.

[0148] The driving manipulation device 500 may include the steering input device 510, an acceleration input device 530, and a brake input device 570.

[0149] The steering input device 510 may receive a travel direction input for the vehicle 100 from a user. The steering input device 510 may take the form of a wheel to rotate to provide a steering input. In some embodiments, the steering input device 510 may be configured as a touch screen, a touchpad, or a button.

[0150] The acceleration input device 530 may receive an input for acceleration of the vehicle 100 from the user. The brake input device 570 may receive an input for deceleration of the vehicle 100 from the user. The acceleration input device 530 and the brake input device 570 are preferably formed into pedals. In some embodiments, the acceleration input device 530 or the brake input device 570 may be configured as a touch screen, a touchpad, or a button.

[0151] The driving manipulation device 500 may operate under control of the controller 170.

[0152] The vehicle driving device 600 is used to electrically control operations of various devices of the vehicle 100.

[0153] The vehicle driving device 600 may include at least one of a power train driving unit 610, a chassis driving unit 620, a door/window driving unit 630, a safety device driving unit 640, a lamp driving unit 650, or an air conditioner driving unit 660.

[0154] In some embodiments, the vehicle driving device 600 may further include a new component in addition to components described below or may not include a part of the components.

[0155] The vehicle driving device 600 may include a processor. Each unit of the vehicle driving device 600 may include a processor.

[0156] The power train driving unit 610 may control operation of a power train device.

[0157] The power train driving unit 610 may include a power source driver 611 and a transmission driver 612.

[0158] The power source driver 611 may control a power source of the vehicle 100.

[0159] For example, if the power source is a fossil fuel-based engine, the power source driver 610 may perform electronic control on the engine. Therefore, the power source driver 611 may control an output torque of the engine, and the like. The power source driver 611 may adjust the engine output torque under control of the controller 170.

[0160] For example, if the power source is an electrical energybased motor, the power source driver 610 may control the motor. The power source driver 610 may adjust a rotation speed, torque, and so on of the motor under control of the controller 170.

[0161] The transmission driver 612 may control a transmission.

[0162] The transmission driver 612 may adjust a state of the transmission. The transmission driver 612 may adjust the state of the transmission to drive D, reverse R, neutral N, or park P.

[0163] If the power source is the engine, the transmission driver 612 may adjust the engagement state of gears in the drive mode D.

[0164] The chassis driving unit 620 may control operation of a chassis device.

[0165] The chassis driving unit 620 may include a steering driver 621, a brake driver 622, and a suspension

driver 623.

[0166] The steering driver 621 may perform electronic control on a steering device in the vehicle 100. The steering driver 621 may change a travel direction of the vehicle 100.

[0167] The brake driver 622 may perform electronic control on a brake device in the vehicle 100. For example, the brake driver 622 may decrease the speed of the vehicle 100 by controlling an operation of a brake disposed at a wheel.

[0168] The brake driver 622 may control a plurality of brakes individually. The brake driver 622 may control braking power applied to a plurality of wheels differently.

[0169] The suspension driver 623 may perform electronic control on a suspension device in the vehicle 100. For example, if the surface of a road is rugged, the suspension driver 623 may control the suspension device to reduce jerk of the vehicle 100.

[0170] The suspension driver 623 may control a plurality of suspensions individually.

[0171] The door/window driving unit 630 may perform electronic control on a door device or a window device in the vehicle 100.

[0172] The door/window driving unit 630 may include a door driver 631 and a window driver 632.

[0173] The door driver 631 may perform electronic control on a door device in the vehicle 100. For example, the door driver 631 may control opening and closing of a plurality of doors in the vehicle 100. The door driver 631 may control opening or closing of the trunk or the tail gate. The door driver 631 may control opening or closing of the sunroof.

[0174] The window driver 632 may perform electronic control on a window device in the vehicle 100. The window driver 632 may control opening or closing of a plurality of windows in the vehicle 100.

[0175] The safety device driving unit 640 may perform electronic control on various safety devices in the vehicle 100.

[0176] The safety device driving unit 640 may include an airbag driver 641, a seatbelt driver 642, and a pedestrian protection device driver 643.

[0177] The airbag driver 641 may perform electronic control on an airbag device in the vehicle 100. For example, the airbag driver 641 may control inflation of an airbag, upon sensing an emergency situation.

[0178] The seatbelt driver 642 may perform electronic control on a seatbelt device in the vehicle 100. For example, the seatbelt driver 642 may control securing of passengers on the seats 110FL, 110FR, 110RL, and 110RR by means of seatbelts, upon sensing a danger.

[0179] The pedestrian protection device driver 643 may perform electronic control on a hood lift and a pedestrian airbag. For example, the pedestrian protection device driver 643 may control the hood to be lifted up and the pedestrian airbag to be inflated, upon sensing collision with a pedestrian.

[0180] The lamp driving unit 650 may perform electronic control on various lamp devices in the vehicle 100.

[0181] The air conditioner driving unit 660 may perform electronic control on an air conditioner in the vehicle 100. For example, if a vehicle internal temperature is high, the air conditioner driver 660 may control the air conditioner to operate and supply cool air into the vehicle 100.

[0182] The vehicle driving device 600 may include a processor. Each unit of the vehicle driving device 600 may include a processor.

[0183] The vehicle driving device 600 may operate under control of the controller 170.

[0184] The operation system 700 is a system that controls various operations of the vehicle 100. The operation system 700 may operate in the autonomous driving mode.

[0185] The operation system 700 may include the traveling system 710, the park-out system 740, and the park-in system 750.

[0186] In some embodiments, the operation system 700 may further include a new component in addition to components described below or may not include a part of the described components.

[0187] The operation system 700 may include a processor. Each unit of the operation system 700 may include a processor.

[0188] In some embodiments, if the operation system 700 is implemented in software, the operation system 700 may lie under the controller 170 in concept.

[0189] In some embodiments, the operation system 700 may conceptually include at least one of the UI device 270, the object detection device 300, the communication device 400, the driving manipulation device 500, the vehicle driving device 600, the navigation system 770, the sensing unit 120, or the controller 170.

[0190] The traveling system 710 may drive the vehicle 100.

[0191] The traveling system 710 may drive the vehicle 100 by providing a control signal to the vehicle driving device 600 based on navigation information received from the navigation system 770.

[0192] The traveling system 710 may drive the vehicle 100 by providing a control signal to the vehicle driving device 600 based on object information received from the object detection device 300.

[0193] The traveling system 710 may drive the vehicle 100 by receiving a signal from an external device through the communication device 400 and providing a control signal to the vehicle driving device 600.

[0194] The traveling system 710 may include at least one of the UI device 270, the object detection device 300 and the communication device 400, the driving manipulation device 500, the vehicle driving device 600, the navigation system 770, the sensing unit 120, and the controller 170 and may be conceptually a system for performing traveling of the vehicle 100.

[0195] The traveling system 710 may be referred to as a vehicle traveling control apparatus.

[0196] The park-out system 740 may perform park-out

of the vehicle 100.

[0197] The park-out system 740 may perform park-out of the vehicle 100 by providing a control signal to the vehicle driving device 600 according to navigation information received from the navigation system 770.

[0198] The park-out system 740 may perform park-out of the vehicle 100 by providing a control signal to the vehicle driving device 600 based on object information received from the object detection device 300.

[0199] The park-out system 740 may perform park-out of the vehicle 100 by receiving a signal from an external device through the communication device 400 and providing a control signal to the vehicle driving device 600.

[0200] The park-out system 740 may include at least one of the UI device 270, the object detection device 300, the communication device 400, the driving manipulation device 500, the vehicle driving device 600, the navigation system 770, the sensing unit 120, or the controller 170 and may be conceptually a system for performing park-out of the vehicle 100.

[0201] The park-out system 740 may be referred to as a vehicle park-out control apparatus.

[0202] The park-in system 750 may perform park-in of the vehicle 100.

[0203] The park-in system 750 may perform park-in of the vehicle 100 by providing a control signal to the vehicle driving device 600 according to navigation information received from the navigation system 770.

[0204] The park-in system 750 may perform park-in of the vehicle 100 by providing a control signal to the vehicle driving device 600 based on object information received from the object detection device 300.

[0205] The park-in system 750 may perform park-in of the vehicle 100 by providing a control signal to the vehicle driving device 600 according to a signal received from an external device via the communication device 400.

[0206] The park-in system 750 may include at least one of the UI device 270, the object detection device 300, the communication device 400, the driving manipulation device 500, the vehicle driving device 600, the navigation system 770, the sensing unit 120, or the controller 170 and may be conceptually a system for performing park-in of the vehicle 100.

[0207] The park-in system 750 may be referred to as a vehicle park-in control apparatus.

[0208] The navigation system 770 may provide navigation information. The navigation information may include at least one of map information, set destination information, route information based on setting of a destination, information about various objects on a route, lane information, or information about a current location of a vehicle.

[0209] The navigation system 770 may include a memory and a processor. The memory may store navigation information. The processor may control operation of the navigation system 770.

[0210] In some embodiments, the navigation system 770 may receive information from an external device via the communication device 400 and update pre-stored information with the received information.

[0211] In some embodiments, the navigation system 770 may be classified as a lower-level component of the UI device 200.

[0212] The sensing unit 120 may sense a vehicle state. The sensing unit 120 may include an attitude sensor (e.g., a yaw sensor, a roll sensor, or a pitch sensor), a collision sensor, a wheel sensor, a speed sensor, an inclination sensor, a weight detection sensor, a heading sensor, a gyro sensor, a position module, a vehicle drive/reverse sensor, a battery sensor, a fuel sensor, a tier sensor, a steering sensor for rotation of the steering wheel, an in-vehicle temperature sensor, an in-vehicle humidity sensor, an ultrasonic sensor, an illuminance sensor, an acceleration pedal position sensor, a brake pedal position sensor, and so on.

[0213] The sensing unit 120 may acquire a sensing signal of vehicle position information, vehicle collision information, vehicle heading information, vehicle location information (GPS information), vehicle angle information, vehicle speed information, vehicle acceleration information, vehicle inclination information, vehicle drive/reverse information, battery information, fuel information, wheel information, vehicle lamp information, vehicle internal temperature information, vehicle internal humidity information, a steering wheel rotation angle, a vehicle external illuminance, a pressure applied to an accelerator pedal, a pressure applied to a brake pedal, and so on.

[0214] The sensing unit 120 may further include an accelerator pedal sensor, a pressure sensor, an engine speed sensor, an air flow sensor (AFS), an air temperature sensor (ATS), a water temperature sensor (WTS), a throttle position sensor (TPS), a top dead center (TDC) sensor, a crank angle sensor (CAS), and so on.

[0215] The sensing unit 120 may generate vehicle state information based on the sensing data. The vehicle state information may be generated based on data detected by various sensors included in the vehicle.

[0216] For example, the vehicle state information may include vehicle position information, vehicle speed information, vehicle inclination information, vehicle weight information, vehicle heading information, vehicle battery information, vehicle fuel information, vehicle wheel air pressure information, vehicle steering information, in-vehicle temperature information, in-vehicle humidity information, pedal position information, vehicle engine temperature information, and so on.

[0217] The interface unit 130 serves paths to various types of external devices connected to the vehicle 100. For example, the interface unit 130 may be provided with a port connectable to a mobile terminal, and may be connected to a mobile terminal through the port. In this case, the interface unit 130 may exchange data with the mobile terminal.

[0218] The interface unit 130 may serve as a path along which electric energy is supplied to a connected mobile terminal. When the mobile terminal is conductibly

connected to the interface unit 130, the interface unit 130 may supply electric energy received from the power supply 190 to the mobile terminal under control of the controller 170.

[0219] The memory 140 is conductibly connected to the controller 170. The memory 140 may store default data for a unit, control data for controlling the operation of the unit, and input and output data. The memory 140 may be any of various storage devices in hardware, such as read only memory (ROM), random access memory (RAM), erasable and programmable ROM (EPROM), flash drive, and hard drive. The memory 140 may store various data for an overall operation of the vehicle 100, such as programs for processing or control in the controller 170.

[0220] In some embodiments, the memory 140 may be integrated with the controller 170, or configured as a lower level component of the controller 170.

[0221] The controller 170 may control an overall operation of each unit in the vehicle 100. The controller 170 may be referred to as an electronic control unit (ECU).

[0222] The power supply 190 may supply power required for an operation of each component under control of the controller 170. In particular, the power supply 190 may receive power from a battery, etc. in the vehicle.

[0223] One or more processors and the controller 170, included in the vehicle 100, may be implemented using at least one of application specific integrated circuits (ASICs), digital signal processors (DSPs), digital signal processing devices (DSPDs), programmable logic devices (PLDs), field programmable gate arrays (FPGAs), processors, controllers, micro-controllers, microprocessors, or an electrical unit for performing other functions.

[0224] As described above, the vehicle 100 may include various electronic devices such as the UI device 200, the object detection device 300, the communication device 400, the driving manipulation device 500, the controller 170, the vehicle driving device 600, the operating system 700, the navigation system 770, the sensing unit 120, the interface unit 130, a memory 140, and the power supply 190.

[0225] A vehicular electronic device may be communication-connected to a system outside the vehicle 100. For example, the vehicular electronic device may be communication-connected to a system outside the vehicle 100 through a gateway inside the vehicle 100. Here, the gateway may be on-board diagnostics (OBD) or on-board diagnostic version 2 (OBD 2).

[0226] Wired communication or wireless communication may be performed between vehicular electronic devices. For example, communication may be performed between vehicular electronic devices through a controller area network (CAN).

[0227] The vehicular electronic device may be communication-connected to a system outside the vehicle 100 by wire or wirelessly. For example, the vehicular electronic device may be communication-connected to an external device of the vehicle 100 through a Wi-Fi protocol or a Bluetooth protocol.

[0228] The system outside the vehicle 100 may include a server, a computer, a mobile terminal, a clouding service, and a network.

[0229] The vehicular electronic device may receive a file or data from the system outside the vehicle 100. For example, the vehicular electronic device may receive a firmware upgrade file from the system outside the vehicle 100 and may update firmware.

[0230] Communication-connection between the vehicular electronic device and the system outside the vehicle 100 may be a target of hacking.

[0231] For example, a hacker may access a vehicular electronic device through a gateway or a CAN and may induce an abnormal operation of the vehicular electronic device.

[0232] For example, the hacker may mutate an access point connection protocol and may attack the UI device 200 for a vehicle when the UI device 200 for a vehicle operates as a Wi-Fi access point.

[0233] For example, the hacker may attack and take control of an access point, and then may attack the UI device 200 for a vehicle using a Wi-Fi protocol when the UI device 200 for a vehicle operates as a Wi-Fi station.

[0234] For example, the hacker may mutate and attack a Bluetooth profile/protocol packet (e.g., L2CAP, RFCOMN, OBEX, or SDP).

[0235] For example, the hacker may change and attaché firmware of the vehicular electronic device. In detail, the hacker may execute buffer overflow attack through firmware hacking.

[0236] A vehicular electronic device hacking test apparatus 800 may be communication-connected to the vehicular electronic device by wire or wirelessly. The vehicular electronic device hacking test apparatus 800 may determine whether the vehicular electronic device is vulnerable to hacking in response to a state classified according to a preset communication protocol.

[0237] For example, the vehicular electronic device hacking test apparatus 800 may determine whether the vehicular electronic device is vulnerable to hacking in response to a state classified according to a Wi-Fi protocol.

[0238] For example, the vehicular electronic device hacking test apparatus 800 may determine whether the vehicular electronic device is vulnerable to hacking in response to a state classified according to a Bluetooth protocol.

[0239] FIG. 3 is a block diagram for explanation of a vehicular electronic device hacking test apparatus according to an embodiment of the present invention.

[0240] Referring to FIG. 3, the vehicular electronic device hacking test apparatus 800 may include a communication unit 810, a processor 870, an interface unit 880, a memory 885, and a power supply 890.

[0241] The communication unit 810 may be communication-connected to the vehicular electronic device by wire or wirelessly. The communication unit 810 may be

communication-connected to the vehicular electronic device based on a preset communication protocol.

[0242] The communication unit 810 may include a transmitter 811 and a receiver 812.

[0243] The transmitter 811 may transmit data to the vehicular electronic device by wire or wirelessly.

[0244] The transmitter 811 may transmit data to the vehicular electronic device based on a preset wireless communication protocol. In this case, the transmitter 811 may include a transmission radio frequency (RF) circuit appropriate for a wireless communication protocol.

[0245] The receiver 812 may receive data from the vehicle electronic device by wire or wirelessly.

[0246] The receiver 812 may receive data from the vehicular electronic device based on a preset wireless communication protocol. In this case, the receiver 812 may include a reception radio frequency (RF) circuit appropriate for a wireless communication protocol.

[0247] The processor 870 may control an overall operation of each unit of the vehicular electronic device hacking test apparatus 800.

[0248] The processor 870 may control the transmitter 811 to transmit data to the vehicle electronic device. For example, the processor 870 may control the transmitter 811 to transmit a mutated packet.

[0249] The processor 870 may control the transmitter 811 to transmit data to the vehicle electronic device based on a preset communication protocol.

[0250] The processor 870 may control the receiver 812 to receive data from the vehicle electronic device.

[0251] The processor 870 may control the receiver 812 to receive data from the vehicle electronic device based on a preset communication protocol.

[0252] The processor 870 may classify a communication-connection procedure into a plurality of states based on a preset communication protocol.

[0253] For example, the Wi-Fi access point may have a state such as a probe request listening state, an association listening state, and a connected state. When determining whether the vehicular electronic device that operates as a Wi-Fi access point is vulnerable to hacking, the processor 870 may classify a communication-connection procedure into states such as a probe request listening state, an association listening state, and a connected state.

[0254] The processor 870 may generate the mutated packet appropriate for a plurality of states. The processor 870 may transmit the mutated packet to the vehicular electronic device through the transmitter 811.

[0255] The processor 870 may generate the mutated packet corresponding to a plurality of states. The processor 870 may transmit the mutated packet to the vehicular electronic device through the transmitter 811.

[0256] For example, the processor 870 may generate the mutated packet appropriate for a plurality of states via a fuzzing scheme.

[0257] For example, the processor 870 may generate the mutated packet corresponding to a plurality of states via a fuzzing scheme.

[0258] For example, the processor 870 may arbitrarily mutate a portion of an original packet to be transmitted in a plurality of states to generate the mutated packet.

[0259] For example, the vehicular electronic device hacking test apparatus 800 may determine whether the vehicular electronic device that operates as a Wi-Fi access point is vulnerable to hacking. In this case, the processor 870 may arbitrarily mutate a portion of an original packet to be transmitted in each of a probe request listening state, an association listening state, and a connected state to generate the mutated packet. Then, the processor 870 may transmit the mutated packet to the vehicular electronic device in each of the probe request listening state, the association listening state, and the connected state.

[0260] The processor 870 may determine whether the vehicular electronic device is vulnerable to hacking based on whether a reception packet to the mutated packet is received through the receiver 812.

[0261] For example, when a normal reception packet is received, the processor 870 may determine whether the vehicular electronic device is not vulnerable to hacking.

[0262] For example, when the normal reception packet is not received, the processor 870 may determine whether the vehicular electronic device is vulnerable to hacking. When a reception packet is not received, the processor 870 may determine whether the vehicular electronic device is vulnerable to hacking. When an abnormal packet is received, the processor 870 may determine whether the vehicular electronic device is vulnerable to hacking.

[0263] The processor 870 may classify a communication-connection procedure with the vehicular electronic device into a first state, a second state, and a third state.

[0264] Here, classification into a plurality of states may be exemplary and may be defined according to a preset communication protocol.

[0265] According to the present embodiment, although classification into three states is exemplified, the processor 870 may also classify a communication-connection procedure into two states or four or more states.

[0266] The processor 870 may generate a first mutated packet appropriate for the first state and may transmit the first mutated packet to the vehicular electronic device through the transmitter 811.

[0267] The processor 870 may generate the first mutated packet corresponding to the first state and may transmit the first mutated packet to the vehicular electronic device through the transmitter 811.

[0268] When a first reception packet corresponding to the first mutated packet is received from the vehicular electronic device through the receiver 812 in the first state, the processor 870 may generate a second mutated packet appropriate for the second state.

[0269] When the first reception packet corresponding to the first mutated packet is received from the vehicular electronic device through the receiver 812 in the first

state, the processor 870 may generate the second mutated packet corresponding to the second state.

[0270] When the first reception packet is not received through the receiver 812 in the first state, the processor 870 may determine that the vehicular electronic device is vulnerable to hacking. For example, when the first reception packet is not received through the receiver 812 for a preset time or more, the processor 870 may determine that the vehicular electronic device is vulnerable to hacking.

[0271] When the first reception packet corresponding to the first mutated packet is not received from the vehicular electronic device through the receiver 812, the processor 870 may repeatedly generate the first mutated packet and may transmit the first mutated packet to the vehicular electronic device through the transmitter 811.

[0272] When the number of times the first mutated packet is repeatedly generated is equal to or greater than a preset number of times, the processor 870 may determine that the vehicular electronic device is vulnerable to hacking.

[0273] When the number of times the first mutated packet is repeatedly transmitted is equal to or greater than a preset number of times, the processor 870 may determine that the vehicular electronic device is vulnerable to hacking.

[0274] The processor 870 may transmit the generated second mutated packet to the vehicular electronic device through the transmitter 811.

[0275] When a second reception packet corresponding to the second mutated packet is received, the processor 870 may generate a mutated packet appropriate for another state and may transmit the mutated packet to the vehicular electronic device through the transmitter 811.

[0276] When the second reception packet corresponding to the second mutated packet is received, the processor 870 may generate a mutated packet corresponding to another state and may transmit the mutated packet to the vehicular electronic device through the transmitter 811.

[0277] The processor 870 is configured to receive the second reception packet and may randomly determine a next state. The processor 870 is configured to generate a mutated packet appropriate for the randomly determined state and may transmit the mutated packet to the vehicular electronic device through the transmitter 811.

[0278] The processor 870 is configured to receive the second reception packet and may randomly determine a next state. The processor 870 is configured to generate a mutated packet corresponding to the randomly determined state and is configured to transmit the mutated packet to the vehicular electronic device through the transmitter 811.

[0279] When the second reception packet corresponding to the second mutated packet is received, the processor 870 may generate a third mutated packet appropriate for the third state. The processor 870 may transmit the generated third mutated packet to the vehicular electronic device through the transmitter 811.

[0280] When the second reception packet corresponding to the second mutated packet is received, the processor 870 may generate the third mutated packet corresponding to the third state. The processor 870 may transmit the generated third mutated packet to the vehicular electronic device through the transmitter 811.

[0281] When the second reception packet corresponding to the second mutated packet is received, the processor 870 may generate the first mutated packet appropriate for the first state. The processor 870 may transmit the generated first mutated packet to the vehicular electronic device through the transmitter 811.

[0282] When the second reception packet corresponding to the second mutated packet is received, the processor 870 may generate the first mutated packet corresponding to the first state. The processor 870 may transmit the generated second mutated packet to the vehicular electronic device through the transmitter 811.

[0283] The interface unit 880 may exchange information, a signal, or data with other device. The interface unit 880 may receive information, a signal, or data from other device. The interface unit 880 may transmit the received information, signal, or data to the processor 870. The interface unit 880 may transmit information, a signal, or data, which is generated or processed by the processor 870, to other device.

[0284] The memory 885 may be conductibly connected to the processor 870. The memory 885 may store basic data of a unit, control data for control of an operation of the unit, and input and output data. The memory 885 may be various storage devices such as ROM, RAM, EPROM, a flash drive, or a hard drive in terms of hardware. The memory 885 may store various data for an overall operation of the vehicular electronic device hacking test apparatus 800, such as a program for processing or control of the processor 870.

[0285] In some embodiments, the memory 885 may be integrally formed with the processor 870 or may be a component that lies under the processor 870.

[0286] The power supply 890 may supply power required for an operation of each component under control of the processor 870. In particular, the power supply 890 may receive power from a battery inside a vehicle, or the like.

[0287] FIG. 4 is a diagram for explanation of an operation of a vehicular electronic device hacking test apparatus according to an embodiment of the present invention.

[0288] Referring to FIG. 4, a vehicular electronic device 10 may include at least one of the UI device 200, the object detection device 300, the communication device 400, the driving manipulation device 500, the controller 170, the vehicle driving device 600, the operating system 700, the navigation system 770, the sensing unit 120, the interface unit 130, the memory 140, or the power supply 190.

[0289] The processor 870 may be communication-connected to the vehicular electronic device 10.

[0290] The processor 870 may classify a communication-connection procedure with the vehicular electronic device 10 into a first state 821, a second state 822, and a third state 823 based on a preset communication protocol.

[0291] The processor 870 may enter the first state 821, may generate a first mutated packet 831 appropriate for (or corresponding to) the first state 821, and may transmit the same to the vehicular electronic device 10. Here, the first mutated packet 831 is configured to be a packet formed by arbitrarily mutating a portion of the original packet to be transmitted in the first state 821.

[0292] The processor 870 may determine whether a first reception packet 841 corresponding to the first mutated packet 831 is received from the vehicular electronic device 10. Here, the first reception packet 841 may be a response packet that is generated in response to the first mutated packet 831 in a first state 11 by the vehicular electronic device 10.

[0293] When the first reception packet 841 is received and is determined to be the same reception packet as a reception packet corresponding to the original packet, the processor 870 is configured to determine that the vehicular electronic device 10 is not vulnerable to hacking in the first state 821.

[0294] When the first reception packet 841 is not received or is different from a reception packet corresponding to the original packet and is determined to be an abnormal reception packet, the processor 870 is configured to determine that the vehicular electronic device 10 is vulnerable to hacking in the first state 821.

[0295] The first reception packet 831 may be received, and then the processor 870 may be converted into the second state 821.

[0296] The processor 870 may enter the second state 822, may generate a second mutated packet 832 appropriate for (or corresponding to) the second state 822, and may transmit the same to the vehicular electronic device 10. Here, the second mutated packet 832 is configured to be a packet formed by arbitrarily mutating a portion of the original packet to be transmitted in the second state 822.

[0297] The processor 870 may determine whether a second reception packet 842 corresponding to the second mutated packet 832 is received from the vehicular electronic device 10. Here, the second reception packet 842 may be a response packet that is generated in response to the second mutated packet 832 in a second state 12 by the vehicular electronic device 10.

[0298] When the second reception packet 842 is received and is determined to be the same reception packet as a reception packet corresponding to the original packet, the processor 870 is configured to determine that the vehicular electronic device 10 is not vulnerable to hacking in the second state 822.

[0299] When the second reception packet 842 is not received or is different from a reception packet corresponding to the original packet and is determined to be an abnormal reception packet, the processor 870 is configured to determine that the vehicular electronic device 10 is vulnerable to hacking in the second state 822.

[0300] The second reception packet 832 may be received, and then the processor 870 may be converted into a third state 823.

[0301] The processor 870 may enter the third state 823, may generate a third mutated packet 833 appropriate for (or corresponding to) the third state 823, and may transmit the same to the vehicular electronic device 10. Here, the third mutated packet 833 may be a packet formed by arbitrarily mutating a portion of the original packet to be transmitted in the third state 823.

[0302] The processor 870 may determine whether a third reception packet 843 corresponding to the third mutated packet 833 is received from the vehicular electronic device 10. Here, the third reception packet 843 may be a response packet that is generated in response to the third mutated packet 833 in a third state 13 by the vehicular electronic device 10.

[0303] When the third reception packet 843 is received and is determined to be the same reception packet as a reception packet corresponding to the original packet, the processor 870 may determine that t the vehicular electronic device 10 is not vulnerable to hacking in the third state 823.

[0304] When the third reception packet 843 is not received or is different from a reception packet corresponding to the original packet and is determined to be an abnormal reception packet, the processor 870 may determine that the vehicular electronic device 10 is vulnerable to hacking in the third state 823.

[0305] The second reception packet 832 may be received in the second state 822, and then the processor 870 may return back to the first state 821.

[0306] In this case, the processor 870 may re-generate the first mutated packet 831 and may transmit the same to the vehicular electronic device 10.

[0307] FIG. 5 is a diagram for explanation of an operation of generating a mutated packet according to an embodiment of the present invention.

[0308] FIG. 6 is a diagram for explanation of a mutated packet implemented in a hexadecimal digit according to an embodiment of the present invention.

[0309] Referring to FIGS. 5 and 6, the processor 870 may mutate an original packet 861 for each field to generate a mutated packet.

[0310] The original packet 861 may be defined as a data packet to be transmitted in any one of a plurality of states classified based on a preset communication protocol.

[0311] The original packet 861 may be divided into a header and an information payload.

[0312] The processor 870 may mutate a region except for the header among original packets appropriate for (or corresponding to) a plurality of states to generate a mutated packet 862.

[0313] When a region including the header is mutated to generate a mutated packet, the mutated packet is against a basic structure, and thus the vehicular electronic device 10 may not process the corresponding packet.

[0314] When the region except for the header is mutated to generate the mutated packet 862, an arbitrary field may be modulated to an arbitrary value while a field structure defined depending on each state of a communication protocol is maintained, and thus the vehicular electronic device 10 may process a corresponding packet. In this case, whether the vehicular electronic device 10 is vulnerable to hacking may be more effectively tested.

[0315] When a protocol is processed, there is a routine for processing each field. Hacking vulnerability occurs because exceptional processing is not performed in the routine for processing each field. For example, when a length field of a protocol is not examined, there is possibility that buffer overflow vulnerability occurs.

[0316] The processor 870 may mutate an arbitrary portion of an information payload of the original packet to generate the mutated packet 862.

[0317] The processor 870 may contain a larger amount of data than the original packet 861 appropriate for (or corresponding to) a plurality of states and may generate the mutated packet 862.

[0318] For example, the processor 870 may contain a larger amount of data than original data in an information payload region of the original packet 861 and may generate the mutated packet 862.

[0319] Upon receiving a larger amount of data than the original packet 861, memory capacity of the vehicular electronic device 10, which is allocated according to a protocol, may be exceeded, and thus the vehicular electronic device 10 may malfunction. Such hack attack may be referred to as buffer overflow.

[0320] Through such a test procedure, the vehicular electronic device hacking test apparatus 800 may check whether it is possible to attack the vehicular electronic device via buffer overflow.

[0321] FIGS. 7 and 8 are diagrams for explanation of a vehicular electronic device hacking test apparatus based on Wi-Fi protocol according to an embodiment of the present invention.

[0322] FIGS. 7 and 8 are diagrams for explanation of an operation of the vehicular electronic device hacking test apparatus 800 when the vehicular electronic device 10 operates as a Wi-Fi access point.

[0323] In FIGS. 7 and 8, the vehicular electronic device hacking test apparatus 800 may operate as a Wi-Fi client (or a station).

[0324] The processor 870 may classify a communication-connection procedure into a plurality of states based on a Wi-Fi protocol.

[0325] The processor 870 may generate a mutated packet in terms of a Wi-Fi station.

[0326] FIG. 7 illustrates an example of a communication-connection state of the vehicular electronic device 10 when the vehicular electronic device 10 operates as a Wi-Fi access point.

[0327] When the vehicular electronic device 10 operates as a Wi-Fi access point, the vehicular electronic device 10 may be classified into a probe request listening state 911, an association listening state 912, and a connected state 913 and may perform communication-connection.

[0328] The processor 870 may retrieve the vehicular electronic device 10 that operates as a Wi-Fi access point. For example, the processor 870 may receive a beacon signal transmitted from the vehicular electronic device 10 and may retrieve the vehicular electronic device 10.

[0329] The processor 870 may select the vehicular electronic device 10 among a plurality of Wi-Fi access points. For example, the processor 870 may select the vehicular electronic device 10 based on a basic service set identification (BSSID) included in a beacon signal.

[0330] The processor 870 may arbitrarily change a state to the probe request listening state 911, the association listening state 912, and the connected state 913.

[0331] For example, the processor 870 may change the probe request listening state 911 to the association listening state 912.

[0332] For example, the processor 870 may change the association listening state 912 to the connected state 913 or the probe request listening state 911.

[0333] For example, the processor 870 may change the connected state 913 to the probe request listening state 911 or the association listening state 912.

[0334] The processor 870 may generate a mutated packet in any one state of the probe request listening state 911, the association listening state 912, and the connected state 913 and may transmit the generated mutated packet to the vehicular electronic device 10. The processor 870 may mutate any one of a probe packet, an authentication packet, and an association packet to generate a mutated packet and may transmit the mutated packet.

[0335] When a generated reception packet is not received or a generated abnormal reception packet is received in any one state of the probe request listening state 911, the association listening state 912, and the connected state 913 of the vehicular electronic device 10, the processor 870 may determine that the vehicular electronic device 10 is vulnerable to hacking.

[0336] When a reception packet corresponding to a mutated packet is not received or an abnormal reception packet is received in any one state of an initial state, a probe response/beacon listening state, an authentication listening state, an association response listening state, and a connected state of the vehicular electronic device hacking test apparatus 800, the processor 870 may determine that the vehicular electronic device 10 is vulnerable to hacking.

[0337] As exemplified in FIG. 8, the processor 870 may transmit an original authentication packet to convert the vehicular electronic device 10 into the association listen-

ing state 912.

[0338] The vehicular electronic device 10 may generate and transmit an association packet corresponding to an original authentication packet in the association listening state 912.

[0339] The processor 870 may generate and transmit a mutated association request packet.

[0340] When a response signal corresponding to a mutated association request packet is not received, the processor 870 may determine that the vehicular electronic device 10 is vulnerable to hacking.

[0341] FIG. 9 is a diagram for explanation of a vehicular electronic device hacking test apparatus based on a Wi-Fi protocol according to an embodiment of the present invention.

[0342] FIG. 9 is a diagram for explanation of an operation of the vehicular electronic device hacking test apparatus 800 when the vehicular electronic device 10 operates as a client (or a station).

[0343] In FIG. 9, the vehicular electronic device hacking test apparatus 800 may operate as a Wi-Fi access point.

[0344] The processor 870 may classify a communication-connection procedure into a plurality of states based on a Wi-Fi protocol.

[0345] The processor 870 may generate a mutated packet in terms of a Wi-Fi access point.

[0346] FIG. 9 is a diagram showing an example of a communication-connection state of the vehicular electronic device 10 when the vehicular electronic device 10 operates as a client (or a station).

[0347] When the vehicular electronic device 10 operates as a Wi-Fi client (or a station), the vehicular electronic device 10 may be classified into an initial state 920, a proberesp/beacon listening state 921, an authentication listening state 922, an association response listening state 923, and a connected state 924 and may perform communication-connection.

[0348] The processor 870 may generate and transmit a beacon signal. The processor 870 may receive a response signal corresponding to the beacon signal, and then may generate a mutated packet.

[0349] The processor 870 may receive any one of a probe packet, an authentication packet, and an association packet from the vehicular electronic device 10 that operates as a Wi-Fi client (or a station).

[0350] The processor 870 may generate and transmit a mutated response packet in response to the received packet. The processor 870 may mutate any one of a probe response packet, an authentication response packet, and an association response packet to generate a mutated packet and may transmit the mutated packet.

[0351] When a generated reception packet is not received or a generated abnormal reception packet is received in any one state of the initial state 920, the probe-resp/beacon listening state 921, the authentication listening state 922, the association response listening state 923, and the connected state 924 of the vehicular electronic device 10, the processor 870 may determine that the vehicular electronic device 10 is vulnerable to hacking.

[0352] When a reception packet corresponding to a mutated packet is not received or an abnormal reception packet is received in any one state of a probe request listening state, an association listening state, and a connected state of the vehicular electronic device hacking test apparatus 800, the processor 870 may determine that the vehicular electronic device 10 is vulnerable to hacking.

[0353] As shown in FIG. 9, the processor 870 may transmit the original packet up to the initial state 920, the proberesp/beacon listening state 921, and the authentication listening state 922 of the vehicular electronic device 10.

[0354] The vehicular electronic device 10 may enter the association response listening state 923, and then the processor 870 may transmit a mutated association response packet.

[0355] The processor 870 may monitor whether a disassociation packet is received. When the disassociation packet is not received, the processor 870 may determine that the vehicular electronic device 10 is vulnerable to hacking.

[0356] FIGS. 10 and 11 are diagrams for explanation of a vehicular electronic device hacking test apparatus based on a Bluetooth protocol according to an embodiment of the present invention.

[0357] Referring to the drawings, the processor 870 may classify a communication-connection procedure into a plurality of states based on a Bluetooth protocol.

[0358] The Bluetooth protocol may include L2CAP, SDP, RFCOMN, and OBEX.

[0359] The processor 870 may classify a communication-connection procedure into a plurality of states based on at least one of L2CAP, SDP, RFCOMN, or OBEX.

[0360] FIGS. 10 and 11 are diagrams showing an example of the vehicular electronic device hacking test apparatus 800 based on L2CAP of a Bluetooth protocol.

[0361] The vehicular electronic device 10 may classify communication-connection into four states and may perform communication-connection.

[0362] In each state, the vehicular electronic device hacking test apparatus 800 and the vehicular electronic device 10 may transmit and receive a packet.

[0363] As shown in FIG. 11, until the vehicular electronic device 10 is changed to a 0^{th} state 1010, a first state 1011, and a second state 1012, the processor 870 may transmit the original packet to the vehicular electronic device 10.

[0364] In a state in which the vehicular electronic device 10 is converted into the second state 1012, the processor 870 may mutate a configuration request packet and may transmit a mutated packet.

[0365] Then, when a configuration response packet is not received within a preset time, the processor 870 may determine that the vehicular electronic device 10 is vul-

nerable to hacking.

[0366] The aforementioned present invention can also be embodied as computer readable code stored on a computer readable recording medium. The computer readable recording medium is any data storage device that can store data which can thereafter be read by a computer. Examples of the computer readable recording medium include a hard disk drive (HDD), a solid state drive (SSD), a silicon disk drive (SDD), read-only memory (ROM), random-access memory (RAM), CD-ROM, magnetic tapes, floppy disks, optical data storage devices, carrier waves (e.g., transmission via the Internet), etc. In addition, the computer may include a processor and a controller. Accordingly, it is intended that the present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims.

Claims

1. A vehicular electronic device hacking test apparatus (800) comprising:

a transmitter (811);
a receiver (812); and
a processor (870) configured to classify a communication-connection procedure into one state out of a plurality of states (821, 822, 823) based on a preset communication protocol, to generate a first mutated packet (831, 832, 833) appropriate for the state within which the communication-connection procedure has been classified, and to transmit the first mutated packet to a vehicular electronic device through the transmitter (811),
wherein the processor (870) is further configured to:

randomly determine a next state among the plurality of states (821, 822, 823), in case that a first reception packet corresponding to the first mutated packet (831, 832, 833) is received through the receiver (812),
generate a second mutated packet (831, 832, 833) appropriate for the randomly determined next state, and
transmit the second mutated packet (831, 832, 833) appropriate for the randomly determined next state to the vehicular electronic device through the transmitter (811),

wherein the first mutated packet (831, 832, 833) is generated by mutating a portion of an original packet to be transmitted in the state within which the communication-connection procedure has been classified and the second mutated packet (831, 832, 833) is generated by mutating a portion of an original packet to be transmitted in the randomly determined next state,
wherein the processor (870) is further configured to mutate an arbitrary portion of an information payload of the original packet to generate the first mutated packet (831, 832, 833) or the second mutated packet (831, 832, 833),
wherein the processor (870) is further configured to determine whether the vehicular electronic device is vulnerable to hacking based on whether the first reception packet corresponding to the first mutated packet (831, 832, 833) or a second reception packet corresponding to the second mutated packet is received through the receiver (812).

2. The vehicular electronic device hacking test apparatus (800) of claim 1,
wherein the processor (870) is configured to classify the communication-connection procedure into a first state (821), a second state (822), or a third state (823).

3. The vehicular electronic device hacking test apparatus (800) of claim 2,
wherein the processor (870) is configured to generate and transmit the first mutated packet (831) appropriate for the first state (821).

4. The vehicular electronic device hacking test apparatus (800) of claim 3, wherein, when the first reception packet is not received, the processor (870) is configured to determine that the vehicular electronic device is vulnerable to hacking.

5. The vehicular electronic device hacking test apparatus (800) of claim 3, wherein, when the first reception packet is not received, the processor (870) is configured to repeatedly generate and transmit the first mutated packet (831).

6. The vehicular electronic device hacking test apparatus (800) of claim 5, wherein, when the number of times the first mutated packet (831) is repeatedly transmitted is equal to or greater than a preset number of times and no first reception packet is received after each of the transmitted first mutated packets (831), the processor (870) is configured to determine that the vehicular electronic device is vulnerable to hacking.

7. The vehicular electronic device hacking test apparatus (800) of claim 3,

wherein the processor (870) is configured to randomly determine the next state among the second state (822) and the third state (823), and generate and transmit the second mutated

packet (831, 832, 833) appropriate for the second state (822) based on the randomly determined next state being the second state (822) upon receiving the first reception packet corresponding to the first mutated packet (822) or generate and transmit the second mutated packet (831, 832, 833) appropriate for the third state (823) based on the randomly determined next state being the third state (823) upon receiving the first reception packet corresponding to the first mutated packet (831, 832, 833).

8. The vehicular electronic device hacking test apparatus (800) of claim 1,

wherein the preset communication protocol is a Wi-Fi protocol, and
wherein the processor (870) is further configured to:

classify the communication-connection procedure into the one state out of the plurality of states (821, 822, 823) based on the Wi-Fi protocol,
generate the first mutated packet (831, 832, 833), based on an original packet to be transmitted by a Wi-Fi station according to the Wi-Fi protocol or
generate and transmit a beacon signal, and receive a response signal corresponding to the beacon signal, and generate the first mutated packet (831, 832, 833), based on an original packet to be transmitted by a Wi-Fi access point according to the Wi-Fi protocol.

9. The vehicular electronic device hacking test apparatus (800) of claim 1,

wherein the preset communication protocol is a Bluetooth protocol, and
wherein the processor is configured to classify the communication-connection procedure into one state out of the plurality of states (821, 822, 823) based on the Bluetooth protocol.

10. The vehicular electronic device hacking test apparatus (800) of claim 1, wherein the first mutated packet (831, 832, 833) or the second mutated packet (831, 832, 833) contains a larger amount of data than the original packet.

Patentansprüche

1. Vorrichtung (800) zur Prüfung des Hackens einer elektronischen Vorrichtung eines Fahrzeugs, umfassend:

einen Sender (811);
einen Empfänger (812) und
einen Prozessor (870), der dazu eingerichtet ist, einen Kommunikationsverbindungsvorgang basierend auf einem voreingestellten Kommunikationsprotokoll in einen Zustand aus einer Mehrzahl von Zuständen (821, 822, 823) einzuordnen, ein erstes mutiertes Paket (831, 832, 833) zu erzeugen, das für den Zustand geeignet ist, in den der Kommunikationsverbindungsvorgang eingeordnet wurde, und das erste mutierte Paket über den Sender (811) an eine elektronische Fahrzeugvorrichtung zu senden,
wobei der Prozessor (870) weiterhin eingerichtet ist zum:

zufälligen Bestimmen eines nächsten Zustands unter der Mehrzahl von Zuständen (821, 822, 823), falls ein erstes Empfangspaket, das dem ersten mutierten Paket (831, 832, 833) entspricht, über den Empfänger (812) empfangen wird,
Erzeugen eines zweiten mutierten Pakets (831, 832, 833), das für den zufällig bestimmten nächsten Zustand geeignet ist, und
Senden des zweiten mutierten Pakets (831, 832, 833), das für den zufällig bestimmten nächsten Zustand geeignet ist, über den Sender (811) an die elektronische Fahrzeugvorrichtung,
wobei das erste mutierte Paket (831, 832, 833) durch Mutation eines Teils eines ursprünglichen Pakets erzeugt wird, das in dem Zustand gesendet werden soll, in den der Kommunikationsverbindungsvorgang eingeordnet wurde, und das zweite mutierte Paket (831, 832, 833) durch Mutation eines Teils eines ursprünglichen Pakets erzeugt wird, das in dem zufällig bestimmten nächsten Zustand gesendet werden soll,
wobei der Prozessor (870) weiterhin dazu eingerichtet ist, einen beliebigen Teil einer Informationsnutzlast des ursprünglichen Pakets zu mutieren, um das erste mutierte Paket (831, 832, 833) oder das zweite mutierte Paket (831, 832, 833) zu erzeugen,
wobei der Prozessor (870) weiterhin dazu eingerichtet ist, basierend darauf, ob das erste Empfangspaket, das dem ersten mutierten Paket (831, 832, 833) entspricht, oder ein zweites Empfangspaket, das dem zweiten mutierten Paket entspricht, über den Empfänger (812) empfangen wird, zu bestimmen, ob die elektronische Fahrzeugvorrichtung anfällig für Hacken ist.

2. Vorrichtung (800) zur Prüfung des Hackens einer elektronischen Vorrichtung eines Fahrzeugs nach Anspruch 1, wobei der Prozessor (870) dazu eingerichtet ist, den Kommunikationsverbindungsvorgang in einen ersten Zustand (821), einen zweiten Zustand (822) oder einen dritten Zustand (823) einzuordnen.

3. Vorrichtung (800) zur Prüfung des Hackens einer elektronischen Vorrichtung eines Fahrzeugs nach Anspruch 2, wobei der Prozessor (870) dazu eingerichtet ist, das erste mutierte Paket (831), das für den ersten Zustand (821) geeignet ist, zu erzeugen und zu senden.

4. Vorrichtung (800) zur Prüfung des Hackens einer elektronischen Vorrichtung eines Fahrzeugs nach Anspruch 3, wobei der Prozessor (870) dazu eingerichtet ist, zu bestimmen, dass die elektronische Fahrzeugvorrichtung anfällig für Hacken ist, wenn das erste Empfangspaket nicht empfangen wird.

5. Vorrichtung (800) zur Prüfung des Hackens einer elektronischen Vorrichtung eines Fahrzeugs nach Anspruch 3, wobei der Prozessor (870) dazu eingerichtet ist, das erste veränderte Paket (831) wiederholt zu erzeugen und zu senden, wenn das erste Empfangspaket nicht empfangen wird.

6. Vorrichtung (800) zur Prüfung des Hackens einer elektronischen Vorrichtung eines Fahrzeugs nach Anspruch 5, wobei der Prozessor (870) dazu eingerichtet ist, zu bestimmen, dass die elektronische Fahrzeugvorrichtung anfällig für Hacken ist, wenn die Anzahl der wiederholten Übertragungen des ersten mutierten Pakets (831) gleich oder größer als eine voreingestellte Anzahl ist und nach jedem der gesendeten ersten mutierten Pakete (831) kein erstes Empfangspaket empfangen wird.

7. Vorrichtung (800) zur Prüfung des Hackens einer elektronischen Vorrichtung eines Fahrzeugs nach Anspruch 3,

wobei der Prozessor (870) dazu eingerichtet ist, den nächsten Zustand unter dem zweiten Zustand (822) und dem dritten Zustand (823) zufällig zu bestimmen, und
das zweite mutierte Paket (831, 832, 833), das für den zweiten Zustand (822) geeignet ist, basierend darauf, dass der zufällig bestimmte nächste Zustand der zweite Zustand (822) ist, nach Empfang des ersten Empfangspakets, das dem ersten mutierten Paket (822) entspricht, zu erzeugen und zu senden, oder
das zweite mutierte Paket (831, 832, 833), das für den dritten Zustand (823) geeignet ist, basierend darauf, dass der zufällig bestimmte nächste Zustand der dritte Zustand (823) ist, nach Empfang des ersten Empfangspakets, das dem ersten mutierten Paket (831, 832, 833) entspricht, zu erzeugen und zu senden.

8. Vorrichtung (800) zur Prüfung des Hackens einer elektronischen Vorrichtung eines Fahrzeugs nach Anspruch 1,

wobei das voreingestellte Kommunikationsprotokoll ein Wi-Fi-Protokoll ist und
wobei der Prozessor (870) weiterhin eingerichtet ist zum:

Einordnen des Kommunikationsverbindungsvorgangs in den einen Zustand aus der Mehrzahl von Zuständen (821, 822, 823) basierend auf dem Wi-Fi-Protokoll,
Erzeugen des ersten mutierten Pakets (831, 832, 833) basierend auf einem ursprünglichen Paket, das von einer Wi-Fi-Station gemäß dem Wi-Fi-Protokoll gesendet werden soll, oder
Erzeugen und Senden eines Bakensignals, Empfangen eines dem Bakensignal entsprechenden Antwortsignals und Erzeugen des ersten mutierten Pakets (831, 832, 833) basierend auf einem ursprünglichen Paket, das von einem Wi-Fi-Zugangspunkt gemäß dem Wi-Fi-Protokoll gesendet werden soll.

9. Vorrichtung (800) zur Prüfung des Hackens einer elektronischen Vorrichtung eines Fahrzeugs nach Anspruch 1,

wobei das voreingestellte Kommunikationsprotokoll ein Bluetooth-Protokoll ist und
wobei der Prozessor dazu eingerichtet ist, den Kommunikationsverbindungsvorgang basierend auf dem Bluetooth-Protokoll in einen Zustand aus der Mehrzahl von Zuständen (821, 822, 823) einzuordnen.

10. Vorrichtung (800) zur Prüfung des Hackens einer elektronischen Vorrichtung eines Fahrzeugs nach Anspruch 1, wobei das erste mutierte Paket (831, 832, 833) oder das zweite mutierte Paket (831, 832, 833) eine größere Datenmenge enthält als das ursprüngliche Paket.

Revendications

1. Appareil de test de piratage de dispositif électrique de véhicule (800) comprenant:

un émetteur (811);
un récepteur (812); et

un processeur (870) configuré pour classer une procédure de communication-connexion dans un état parmi plusieurs états (821, 822, 823) sur la base d'un protocole de communication prédéfini, pour générer un premier paquet muté (831, 832, 833) approprié à l'état dans lequel la procédure de communication-connexion a été classée, et pour transmettre le premier paquet muté à un dispositif électronique de véhicule par l'intermédiaire de l'émetteur (811),
dans lequel le processeur (870) est en outre configuré pour:

déterminer aléatoirement un état suivant parmi la pluralité d'états (821, 822, 823), au cas où un premier paquet de réception correspondant au premier paquet muté (831, 832, 833) serait reçu par le récepteur (812),
générer un deuxième paquet muté (831, 832, 833) approprié à l'état suivant déterminé de manière aléatoire, et
transmettre le deuxième paquet muté (831, 832, 833) approprié à l'état suivant déterminé de manière aléatoire au dispositif électronique de véhicule par l'intermédiaire de l'émetteur (811),

dans lequel le premier paquet muté (831, 832, 833) est généré par la mutation d'une partie d'un paquet d'origine à transmettre dans l'état dans lequel la procédure de connexion de communication a été classée et le second paquet muté (831, 832, 833) est généré par la mutation d'une partie d'un paquet d'origine à transmettre dans l'état suivant déterminé de manière aléatoire,
dans lequel le processeur (870) est en outre configuré pour modifier une partie arbitraire d'une charge utile d'information du paquet d'origine afin de générer le premier paquet muté (831, 832, 833) ou le second paquet muté (831, 832, 833),
dans lequel le processeur (870) est en outre configuré pour déterminer si le dispositif électronique de véhicule est vulnérable au piratage en fonction de la réception par le récepteur (812) du premier paquet de réception correspondant au premier paquet muté (831, 832, 833) ou du deuxième paquet de réception correspondant au deuxième paquet muté.

2. Appareil de test de piratage de dispositif électrique de véhicule (800) selon la revendication 1, dans lequel le processeur (870) est configuré pour classer la procédure de connexion=communication dans un premier état (821), un deuxième état (822) ou un troisième état (823).

3. Appareil de test de piratage de dispositif électrique de véhicule (800) selon la revendication 2, dans lequel le processeur (870) est configuré pour générer et transmettre le premier paquet muté (831) approprié au premier état (821).

4. Appareil de test de piratage de dispositif électrique de véhicule (800) selon la revendication 3, dans lequel, lorsque le premier paquet de réception n'est pas reçu, le processeur (870) est configuré pour déterminer que le dispositif électronique de véhicule est vulnérable au piratage.

5. Appareil de test de piratage de dispositif électrique de véhicule (800) selon la revendication 3, dans lequel, lorsque le premier paquet de réception n'est pas reçu, le processeur (870) est configuré pour générer et transmettre de manière répétée le premier paquet muté (831).

6. Appareil de test de piratage de dispositif électrique de véhicule (800) selon la revendication 5, dans lequel, lorsque le nombre de fois où le premier paquet muté (831) est transmis de manière répétée est égal ou supérieur à un nombre de fois prédéfini et qu'aucun premier paquet de réception n'est reçu après chacun des premiers paquets mutés (831) transmis, le processeur (870) est configuré pour déterminer que le dispositif électronique de véhicule est vulnérable au piratage.

7. Appareil de test de piratage de dispositif électrique de véhicule (800) selon la revendication 3,

dans lequel le processeur (870) est configuré pour déterminer aléatoirement l'état suivant parmi le deuxième état (822) et le troisième état (823), et
générer et transmettre le second paquet muté (831, 832, 833) approprié pour le second état (822) sur la base de l'état suivant déterminé de manière aléatoire qui est le deuxième état (822) à la réception du premier paquet de réception correspondant au premier paquet muté (822) ou
générer et transmettre le deuxième paquet muté (831, 832, 833) approprié pour le troisième état (823) sur la base de l'état suivant déterminé de manière aléatoire qui est le troisième état (823) à la réception du premier paquet de réception correspondant au premier paquet muté (831, 832, 833).

8. Appareil de test de piratage de dispositif électrique de véhicule (800) selon la revendication 1,

dans lequel le protocole de communication prédéfini est un protocole Wi-Fi, et
dans lequel le processeur (870) est en outre

configuré pour:

classer la procédure de communication-connexion dans un état parmi la pluralité d'états (821, 822, 823) sur la base du protocole Wi-Fi,
générer le premier paquet muté (831, 832, 833), sur la base d'un paquet d'origine à transmettre par une station Wi-Fi conformément au protocole Wi-Fi ou
générer et transmettre un signal de balise, et recevoir un signal de réponse correspondant au signal de balise et générer le premier paquet muté (831, 832, 833), sur la base d'un paquet d'origine à transmettre par un point d'accès Wi-Fi conformément au protocole Wi-Fi.

9. Appareil de test de piratage de dispositif électrique de véhicule (800) selon la revendication 1,

dans lequel le protocole de communication prédéfini est un protocole Bluetooth, et
dans lequel le processeur est configuré pour classer la procédure de communication-connexion dans un état parmi la pluralité d'états (821, 822, 823) sur la base du protocole Bluetooth.

10. Appareil de test de piratage de dispositif électrique de véhicule (800) selon la revendication 1, dans lequel le premier paquet muté (831, 832, 833) ou le second paquet muté (831, 832, 833) contient une plus grande quantité de données que le paquet d'origine.

FIG. 1

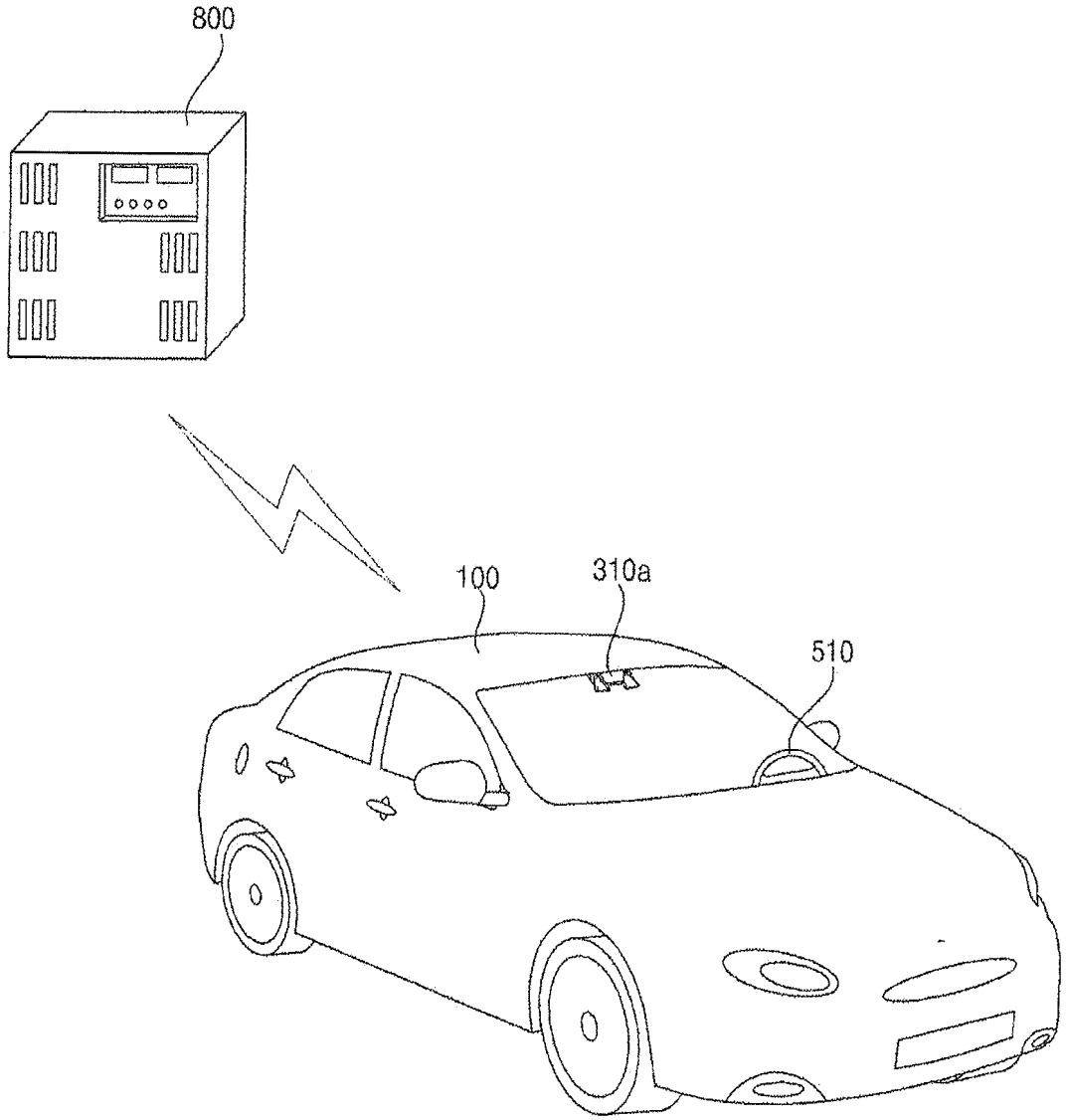


FIG. 2

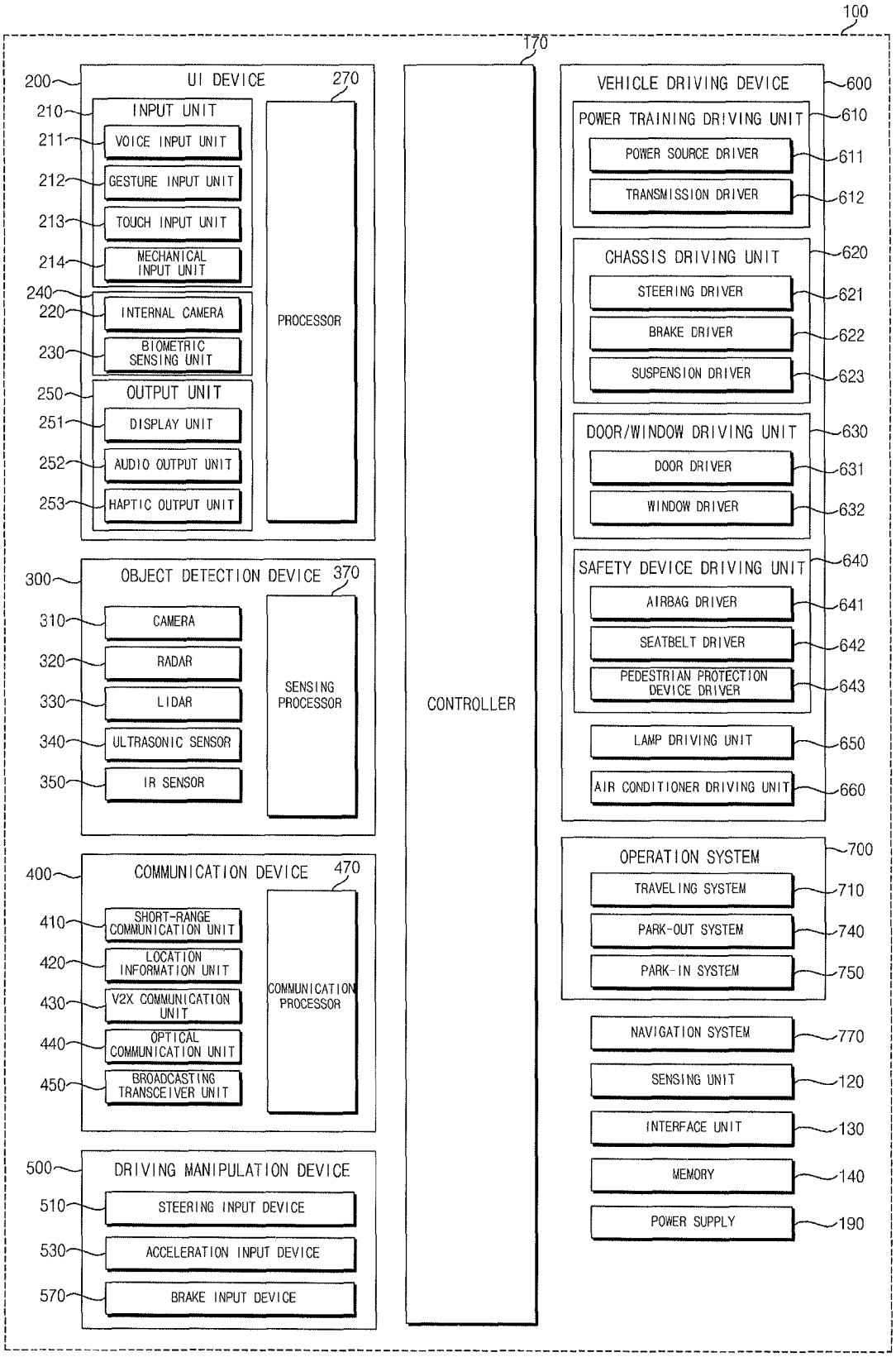

100
170
200
UI DEVICE
270
210
INPUT UNIT
211
VOICE INPUT UNIT
212
GESTURE INPUT UNIT
213
TOUCH INPUT UNIT
214
MECHANICAL INPUT UNIT
240
220
INTERNAL CAMERA
230
BIOMETRIC SENSING UNIT
250
OUTPUT UNIT
251
DISPLAY UNIT
252
AUDIO OUTPUT UNIT
253
HAPTIC OUTPUT UNIT
PROCESSOR
300
OBJECT DETECTION DEVICE
370
310
CAMERA
320
RADAR
330
LIDAR
340
ULTRASONIC SENSOR
350
IR SENSOR
SENSING PROCESSOR
400
COMMUNICATION DEVICE
470
410
SHORT-RANGE COMMUNICATION UNIT
420
LOCATION INFORMATION UNIT
430
V2X COMMUNICATION UNIT
440
OPTICAL COMMUNICATION UNIT
450
BROADCASTING TRANSCEIVER UNIT
COMMUNICATION PROCESSOR
500
DRIVING MANIPULATION DEVICE
510
STEERING INPUT DEVICE
530
ACCELERATION INPUT DEVICE
570
BRAKE INPUT DEVICE
CONTROLLER
VEHICLE DRIVING DEVICE
600
POWER TRAINING DRIVING UNIT
610
POWER SOURCE DRIVER
611
TRANSMISSION DRIVER
612
CHASSIS DRIVING UNIT
620
STEERING DRIVER
621
BRAKE DRIVER
622
SUSPENSION DRIVER
623
DOOR/WINDOW DRIVING UNIT
630
DOOR DRIVER
631
WINDOW DRIVER
632
SAFETY DEVICE DRIVING UNIT
640
AIRBAG DRIVER
641
SEATBELT DRIVER
642
PEDESTRIAN PROTECTION DEVICE DRIVER
643
LAMP DRIVING UNIT
650
AIR CONDITIONER DRIVING UNIT
660
OPERATION SYSTEM
700
TRAVELING SYSTEM
710
PARK-OUT SYSTEM
740
PARK-IN SYSTEM
750
NAVIGATION SYSTEM
770
SENSING UNIT
120
INTERFACE UNIT
130
MEMORY
140
POWER SUPPLY
190

FIG. 3

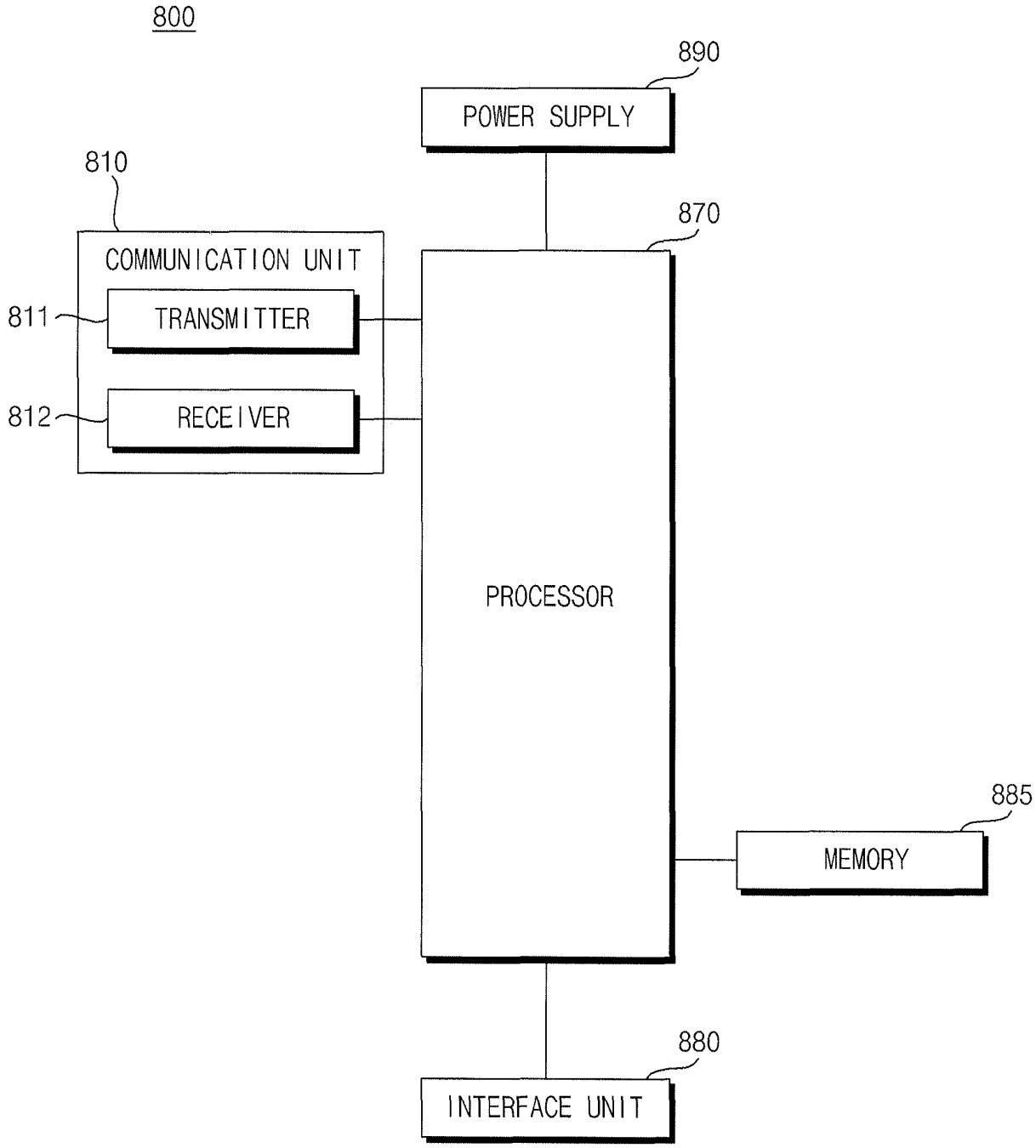

800
890
POWER SUPPLY
810
870
COMMUNICATION UNIT
811
TRANSMITTER
812
RECEIVER
PROCESSOR
885
MEMORY
880
INTERFACE UNIT

FIG. 4

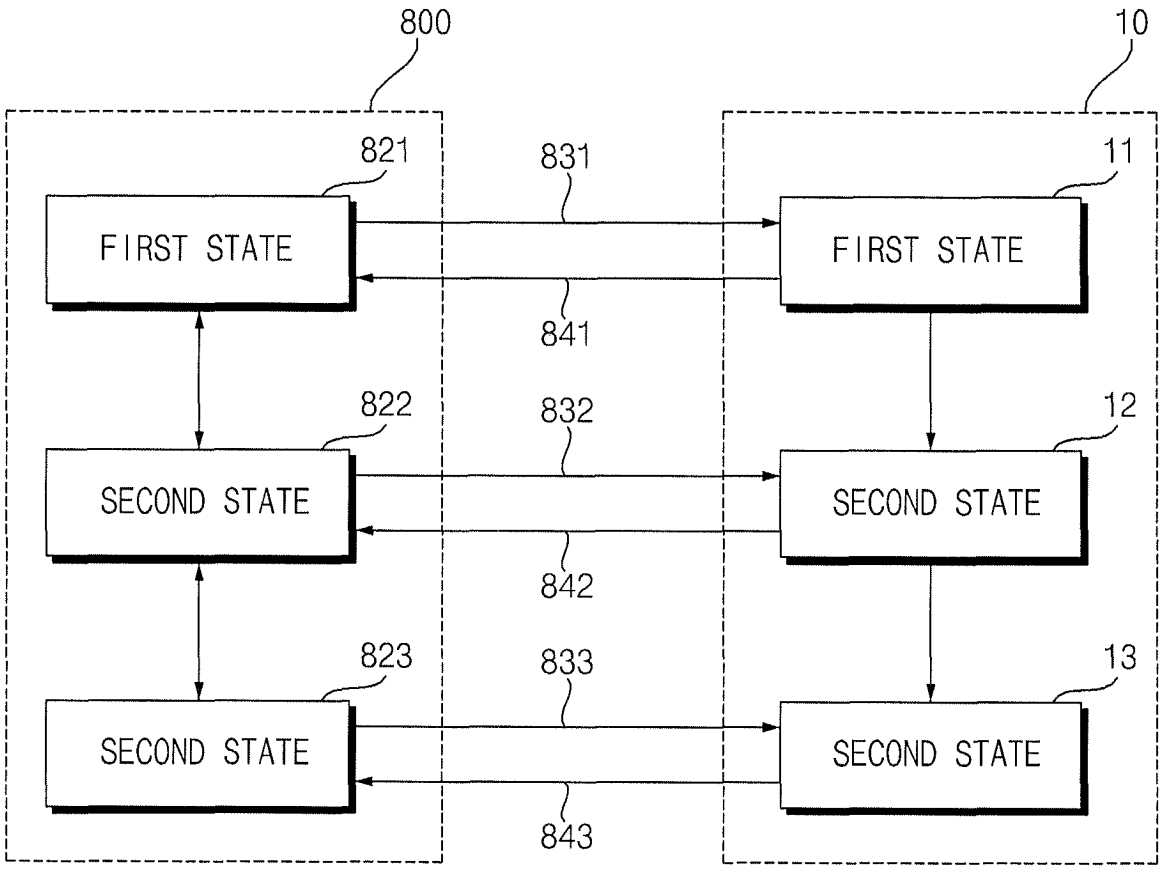

800
10
821
831
11
FIRST STATE
FIRST STATE
841
822
832
12
SECOND STATE
SECOND STATE
842
823
833
13
SECOND STATE
SECOND STATE
843

FIG. 5

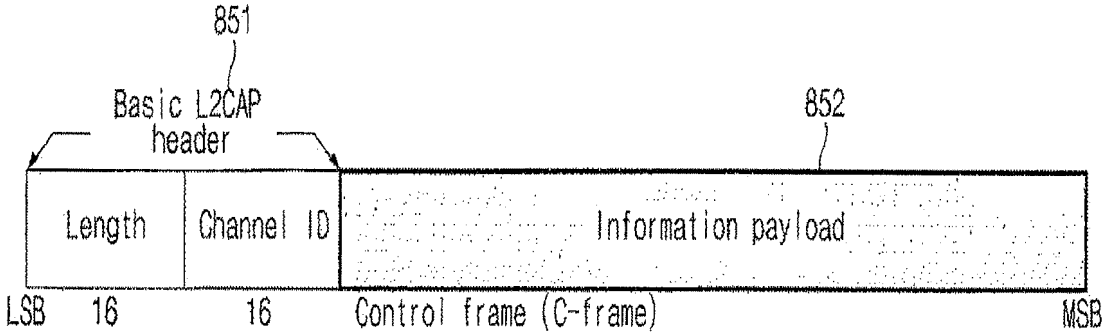

851
Basic L2CAP header
852
Length
Channel ID
Information payload
LSB
16
16
Control frame (C-frame)
MSB

FIG. 6

861

[Original Packet]

00 00 3a 01 00 21 29 e8 93 1d 3c d0 f8 5f bd e5 00 21 29 e8 93 1d 50 17 21 04 0f 00 00 09 6c 69 6e 6b 73 79 73
2d 6e 01 08 82 84 8b 96 24 30 48 6c 32 04 0c 12 18 60 2d 1a 00 01 19 ff 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 dd 09 00 10 18 02 01 00 04 00 00 dd 1e 00 90 4c 33 00 01 19 ff 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 dd 07 00 50 f2 02 00 01 00

862

[Mutated Packet]

00 00 3a 01 00 21 29 e8 93 1d 90 9f 33 ed e9 f6 00 21 29 e8 93 1d 50 17 21 04 0f 00 00 09 6c 69 6e 6b 73 79 73 2d
6e d6 04 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 01 08 82 84 8b 96 24 30 48 6c
8f 00 dd 1e 00 90 4c 33 00 01 19 ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 dd 09 00
10 18 02 01 00 04 00 00 dd 07 00 50 f2 02 00 01 00

FIG. 7

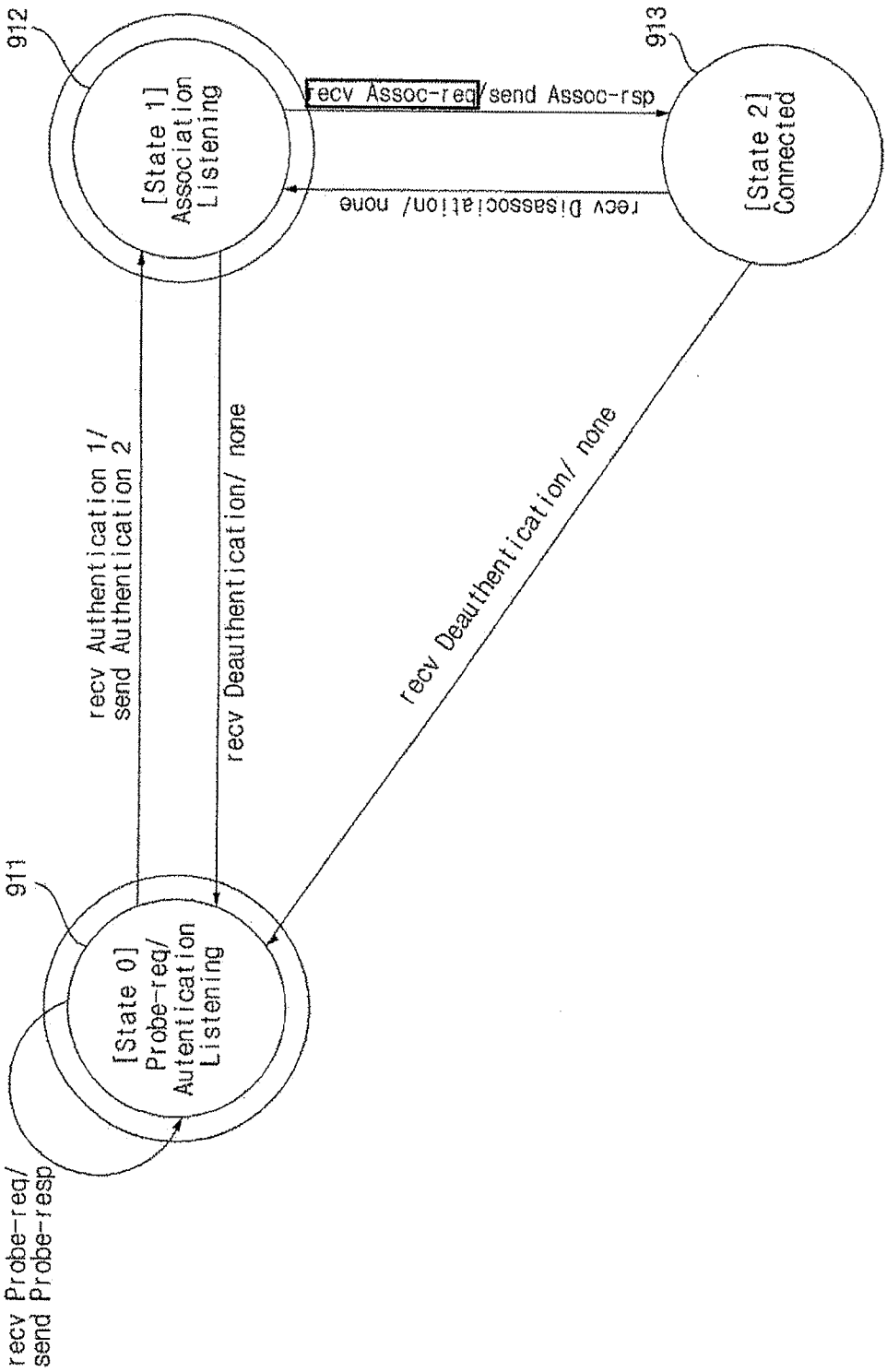

912
913
911
[State 1]
Association
Listening
[State 2]
Connected
[State 0]
Probe-req/
Autentication
Listening
recv Assoc-req/send Assoc-rsp
recv Disassociation/ none
recv Authentication 1/
send Authentication 2
recv Deauthentication/ none
recv Deauthentication/ none
recv Probe-req/
send Probe-resp

FIG. 8

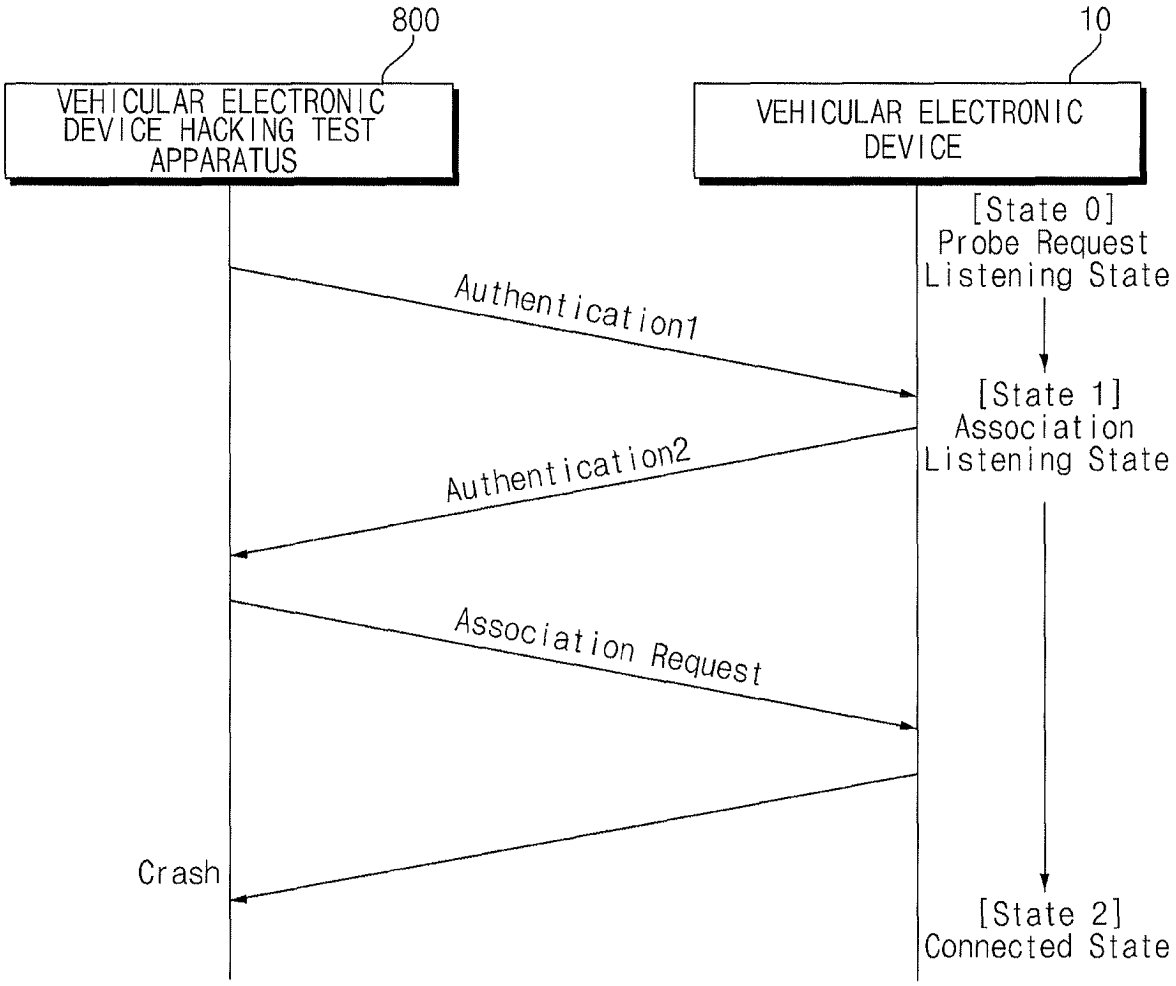

800
VEHICULAR ELECTRONIC DEVICE HACKING TEST APPARATUS
10
VEHICULAR ELECTRONIC DEVICE
[State 0] Probe Request Listening State
Authentication1
[State 1] Association Listening State
Authentication2
Association Request
Crash
[State 2] Connected State

FIG. 9

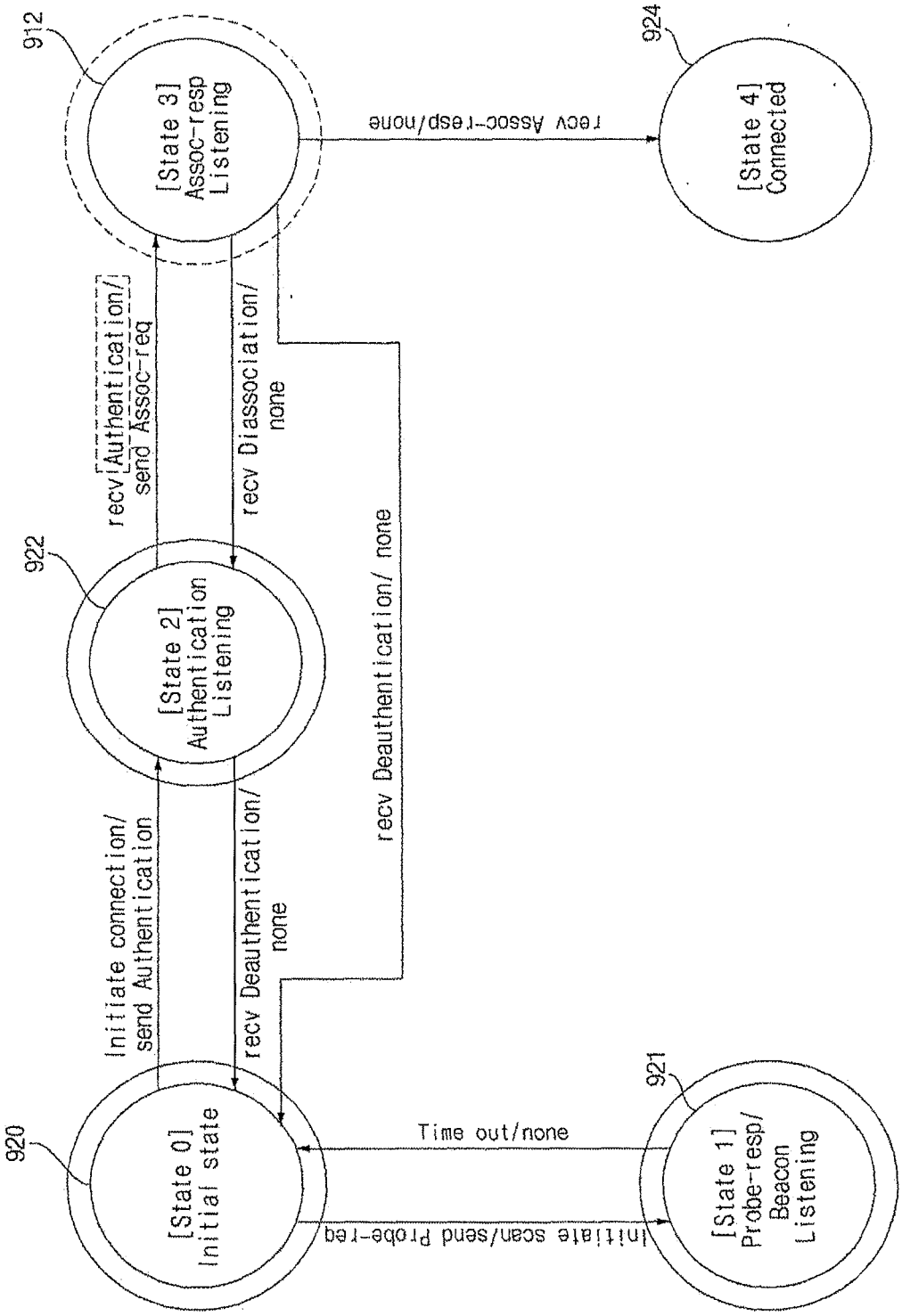

912
[State 3]
Assoc-resp
Listening
924
[State 4]
Connected
recv Assoc-resp/none
recv [Authentication/]
send Assoc-req
recv Diassociation/
none
922
[State 2]
Authentication
Listening
recv Deauthentication/ none
Initiate connection/
send Authentication
recv Deauthentication/
none
920
[State 0]
Initial state
921
[State 1]
Probe-resp/
Beacon
Listening
Time out/none
Initiate scan/send Probe-req

FIG. 10

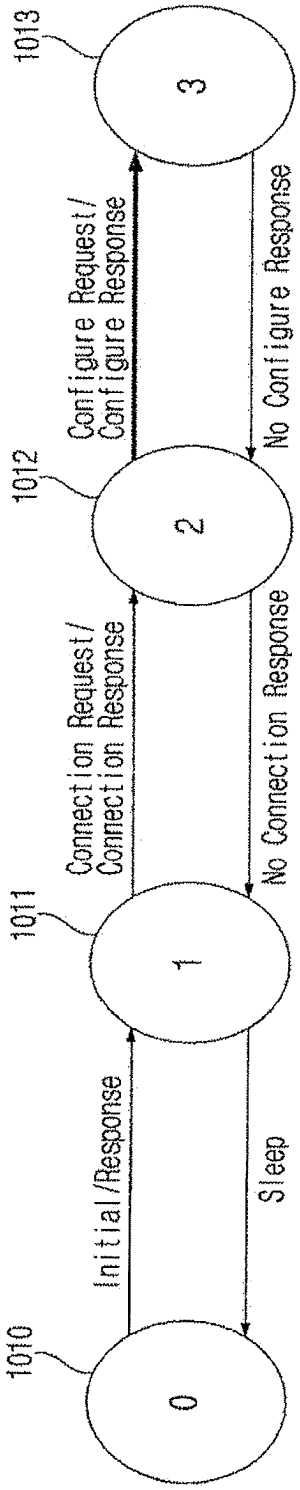
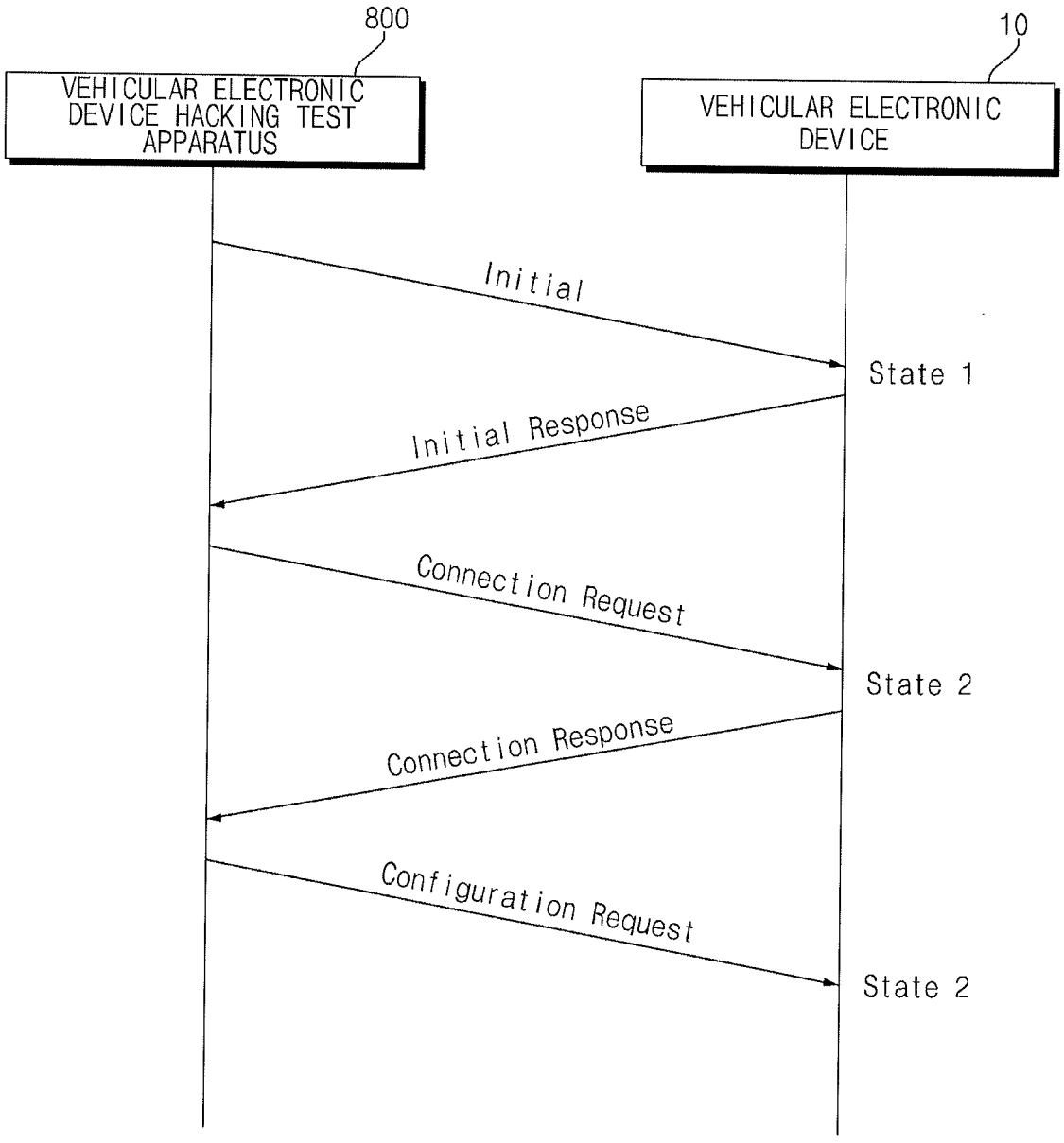

1013
3
Configure Request/
Configure Response
No Configure Response
1012
2
Connection Request/
Connection Response
No Connection Response
1011
1
Initial/Response
Sleep
1010
0

FIG. 11


800
VEHICULAR ELECTRONIC DEVICE HACKING TEST APPARATUS
10
VEHICULAR ELECTRONIC DEVICE
Initial
State 1
Initial Response
Connection Request
State 2
Connection Response
Configuration Request
State 2

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 2016350211 A1, Stephanie Bayer **[0005]**
- US 2013340083 A1, Greg Banks **[0005]**

Non-patent literature cited in the description

- **HUMBERTO ABDELNUR et al.** *KiF: A stateful SIP Fuzzer* **[0005]**
- **NEVES N. et al.** *Using Attack Injection to Discover New Vulnerabilities* **[0005]**