(12)Indian Patent Application

(21) Application Number: 202241044743

(22) Filing Date: 05/08/2022 (43) Publication Date: 09/02/2024

(71) Applicant(s): L&T TECHNOLOGY SERVICES LIMITED

(72) Inventor(s): Magge, Arunadri Jayaprakash Narayan

(51) International Classifications: H04L 12/26 G07C 5/00 H04L 29/06 G07C 5/08 H04W 88/16

(54) Title: METHOD AND SYSTEM FOR PERFORMING VEHICLE DIAGNOSTICS COMMUNICATION

(57) Abstract: A method of performing end-to-end vehicle diagnostics communication is disclosed. A Diagnostics Over Internet Protocol (DoIP) based gateway device may implement a DoIP edge node which receives and accepts a first connection request from a testing device over a first communication network. DoIP network node client which is part of the DoIP gateway device initiates and establishes second connection(s) over a second communication network with at least one target network node. The DoIP gateway device may receive a diagnostic input from the testing device, through the first connection. The DoIP gateway device may determine at least one target network node and transmits the diagnostic input to one or more network nodes over a second connection. Diagnostics may be performed with at least one target network node based on the received diagnostic input and diagnostic output from target network node will be transmitted back to the testing device via DoIP gateway.

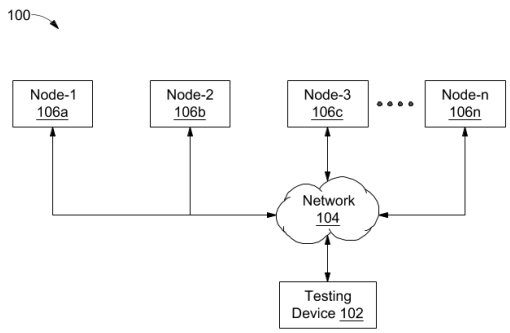

FIG. 1 (PRIOR ART)

FORM 2

THE PATENTS ACT 1970
(39 OF 1970)
&
The Patent Rules, 2003

Complete Specification
(See Section 10 and Rule 13)

1. TITLE OF THE INVENTION

METHOD AND SYSTEM FOR PERFORMING VEHICLE DIAGNOSTICS COMMUNICATION

2. APPLICANT(S)

(a) NAME : **L&T TECHNOLOGY SERVICES LIMITED**
(b) NATIONALITY : **INDIAN**
(c) ADDRESS : DLF IT SEZ Park, 2nd Floor – Block 3
1/124, Mount Poonamallee Road,
Ramapuram, Chennai – 600 089,
INDIA.

3. PREAMBLE TO THE DESCRIPTION

COMPLETE

The following specification describes the invention and the manner in which it is to be performed

DESCRIPTION

Technical Field

[001] This disclosure relates generally to vehicle diagnostics, more particularly to a system and method for performing vehicle diagnostics communication using Diagnostics Over Internet Protocol (DoIP) protocol.

BACKGROUND

[002] Presently, the modern-day vehicles are equipped with various Electronic Control Units (ECUs) which may be used to monitor and implement various functionalities of the vehicle such as security, engine health, infotainment, etc. Therefore, ECUs are connected to various systems of the vehicle through different installed sensors. Through the ECUs, vehicle diagnostics is performed by connecting a testing device to the vehicle network. Further, for an off-board diagnostic of the vehicle the vehicle may be required to brought to a service technician. To avoid this and for efficient time management, remote diagnostics would be time saving and could be performed remotely. To perform diagnostics remotely, the diagnostics node of a vehicle is to be connected to an external device via the internet, which may then receive a set of commands to perform the desired action. However, performing the vehicle diagnostics, either remotely or off-board requires the diagnostic nodes to be discovered by the external devices, which additionally may give access to other system nodes and compromise the security of the vehicle.

[003] Further, OEM provided services may not always be feasible for a user and they may wish to get the diagnostics for uncritical issues done by a third-party diagnostic tool. However, the OEMs would not recommend such unauthorized third-party diagnostic tools in order to prevent any tampering of critical features of the vehicle related to security.

[004] Therefore, there is a need to provide a secured vehicle diagnostic communication system which can perform the diagnostics, either off-board or remotely without compromising the security of the vehicle.

SUMMARY OF THE INVENTION

[005] In an embodiment, a method for performing end-to-end vehicle diagnostics communication is disclosed. The method may include, receiving, by a Diagnostics Over Internet Protocol (DoIP) by a gateway device, a connection request from a testing device over a first communication network, to establish a first connection with the testing device via a DoIP edge node. The DoIP gateway device implements a DoIP network node client. Further the DoIP gateway device receives a diagnostic input from the testing device, through the first connection over the first communication network. The DoIP gateway device then determines at least one target network node from one or more network nodes, based on the diagnostic input. The diagnostic input is transmitted by the DoIP gateway device to the at least one target node from the one or more network nodes through a second connection between the DoIP gateway device and each of the one or more network nodes (also referred to as DoIP network nodes in the present disclosure) over a second communication network. The second connection is established simultaneously between the DoIP gateway device and each of the one or more DoIP network nodes via network node client. Also, the DoIP network node client keeps the second connection active with at least one target node during the transmission of the diagnostic input. One or more diagnostics are performed at least with one target network node, based on the diagnostic input.

[006] In another embodiment, a system for performing vehicle diagnostics communication is disclosed. The system may include a Diagnostics Over Internet Protocol (DoIP) gateway device which may comprise one or more processors and a memory. The memory may be communicatively connected to the one or more processors, wherein the memory stores a plurality of processor-executable instructions, which, upon execution, cause the processors to receive a connection request from a testing device over a first communication network, to establish a first connection with the testing device via a DoIP edge node. The DoIP gateway device implements a DoIP network node client. The DoIP gateway device may receive a diagnostic input from the testing device, through the first connection over the first communication network. The DoIP gateway device may then determine at least one target network node from one or more network nodes, based on the diagnostic input. The DoIP gateway device may then transmit the diagnostic input to the at least one target node from the one or more network nodes through a second connection between the DoIP gateway device and each of the one or more network nodes over a second communication network, via the

network node client. Further, the second connection may be established simultaneously between the DoIP gateway device and each of the one or more network nodes via the network node client, and the DoIP network node client may keep the second connection active with the at least one target node during the transmission of the diagnostic input. The DoIP gateway device may then perform diagnostics at least with one target network node, based on the diagnostic input.

[007] Various objects, features, aspects, and advantages of the inventive subject matter will become more apparent from the following detailed description of preferred embodiments, along with the accompanying drawing figures in which like numerals represent like components.

BRIEF DESCRIPTION OF THE DRAWINGS

[008] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, serve to explain the disclosed principles.

[009] **FIG. 1** illustrates a network diagram of a vehicle diagnostic network, in accordance with a prior art.

[010] **FIG. 2A** illustrates a network diagram of a vehicle diagnostic communication network, in accordance with an embodiment of the current disclosure.

[011] **FIG. 2B** illustrates a DoIP message format and payload encapsulation, in accordance with an embodiment of the current disclosure.

[012] **FIG. 3** illustrates functional modules of a gateway device of FIG. 2A, in accordance with an embodiment of the current disclosure.

[013] **FIG. 4** illustrates a flowchart describing the methodology of performing vehicle diagnostics communication, in accordance with an embodiment of the current disclosure.

DETAILED DESCRIPTION OF THE DRAWINGS

[014] Exemplary embodiments are described with reference to the accompanying drawings. Wherever convenient, the same reference numbers are used throughout the drawings

to refer to the same or like parts. While examples and features of disclosed principles are described herein, modifications, adaptations, and other implementations are possible without departing from the scope of the disclosed embodiments. It is intended that the following detailed description be considered as exemplary only, with the true scope being indicated by the following claims. Additional illustrative embodiments are listed.

[015] In the figures, similar components and/or features may have the same reference label. Further, various components of the same type may be distinguished by following the reference label with a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

[016] Presently, vehicle diagnostics related communication is facilitated between a testing device and the electronic control units (ECUs)–of vehicles using TCP/IP or UDP connection as defined by ISO 13400-2 standard. Recently, the number of electronic control systems mounted on a vehicle has increased which in addition has led to increase in resources required such as storage volume, or the processing capacity of the electronic control units. Furthermore, the volume of data transferred to and from an external testing device has also increased rapidly. Thus, there is requirement for more efficient and secure communications between an off-board electronic control units and an external testing device.

[017] According to the DoIP standard communications between a vehicle-mounted electronic control system and an external tool is given by ISO13400-2, in which the external tool communicates with an in-vehicle electronic control unit (ECU) on an in-vehicle LAN using Ethernet which is an IP-based network. A communication protocol such as controller area network (CAN) and local interconnect network (LIN) are used in the in-vehicle network, and the communication protocols inside and outside the vehicle are possibly different in some scenarios. There is thus a vehicle communication control device (DoIP network coupler or a so-called DoIP gateway) for distributing messages between a network inside the vehicle and a network outside the vehicle. Accordingly,-it may be possible to connect external or third-party testing-devices to the vehicle which may compromise the security of the vehicle. Therefore, a DoIP gateway may be provided which may forward appropriate messages to the required vehicle-mounted ECUs depending on classes of messages from the external or third-party testing device.

[018] Referring to **FIG. 1**, a network diagram of a vehicle diagnostic network is illustrated, in accordance with a prior art. As shown in **FIG. 1** a vehicle diagnostic network 100 including a testing device 102 connected to a plurality of network nodes 106a, 106b, … 106n (collectively referred to as 106) over a network 104.

[019] In general, the diagnostic over IP as illustrated in **FIG. 1** are implemented using the ISO 13400-2 standards. As shown in **FIG. 1**, the testing device 102 in compliance with ISO 13400-2 standards, may support all the payload types like node management, vehicle information, and diagnostic payloads, etc. In the auto industry, AUTOSAR is used as a standardized software architecture and supported diagnostics over Ethernet per this architecture is based on ISO 13400-2 standards. Accordingly, the testing device 102 may establish a TCP/IP connection with each node 106 identified. This means that with help of the vehicle diagnostics applications, based on the ISO 13400-2 standards, the testing device 102 may connect with each of the nodes 106.

[020] Further, the testing device 102 which may be an external testing device, may connect with the nodes 106. It is important to note that in such a situation all the systems of a vehicle including, but not limited to, active safety, infotainment, etc. become discoverable by the testing device 102, thus leaving the vehicle vulnerable to security threats and possibly be compromised.

[021] Further, as per the DoIP standards, all the nodes in the vehicle diagnostics system are configured to comply with the ISO 13400-2 standards, i.e., whether it may be a DoIP edge node, DoIP gateway or a network node, must support all the requirements like the DHCP, the IPv6, etc. This may unnecessarily increase the burden upon the configuration requirements such as increased requirement of RAM/ROM on the target network node.

[022] Referring now to **FIG. 2A** which illustrates a network diagram of an enhanced vehicle diagnostic system 200, in accordance with an embodiment of current disclosure. In some embodiment, the vehicle diagnostics system 200 may include a testing device 202 which may be an external testing device connected to an edge node 206 through a first network 204 which may be a LAN or an Ethernet connection. The gateway device 208 may include an edge node 206. The gateway device 208 may further include a processor 210 and a memory 212. The system 200 may further include a switch 214, which may act as a bridge between the network nodes 216a-n and the testing device 202 via gateway device 208. In an embodiment,

the network nodes 216 may include ECUs that may control, but not limited to, a powertrain system of a vehicle (such as an engine, a transmission, and an anti-lock brake system), body-related components (such as doors, seats, and mirrors), multi-media systems (such as a navigation system, and an audio system), or various sensors.

[023] In an embodiment, the testing device 202 may connected to the edge node 206 thorough a communication line for communicating with the gateway device 208. The gateway device 208 may conform to, for example, International Organization for Standardization (ISO) 13400-2 standards and AUTOSAR standards in the context of supported diagnostics over Ethernet per this architecture. For example, the testing device 202 may perform diagnostics communication for maintenance management of the network node 216. The diagnostics communication may include receiving communication by the gateway device 208 from the testing device 202 intended for network node 216. The diagnostic message information may be transmitted and received between the ECUs and the gateway device 208. Also, in response to the request, diagnostic message information from the electronic ECUs is transmitted to the gateway device 208 which then transmits the diagnostic message information to the testing device 202 through the gateway device 208. The gateway device 208 includes a DoIP edge node 206 which may be communicatively coupled with a DoIP Network node client (described later). The diagnostic message information may include, but not limited to, information related to failure diagnostics of the ECUs or the components (for example, sensors, actuators, and the like) under the control of the ECUs. In some embodiments, the diagnostics communication may also include reprogramming ECUs with new software content as an upgrade.

[024] In an embodiment, with the testing device 202 may be connected to the gateway device 208 through an activation line (not shown) for detecting a connection request from the testing device 202. In an embodiment, the activation line may conform to ISO 13400-2 standards. The activation line may transit from non-active to active when the testing device 202 is communicably connected to the gateway device 208 via a switch or a connector.

[025] In an embodiment, each network node 216 may be connected to the gateway device 208 through a communication line for transmitting and receiving communication from the gateway device 208. A DoIP network node client may be implemented as a software or an algorithm in the gateway device 208 which may implement various functionalities including, but not limited to, a security module (described in FIG. 3 in detail) that may perform a connection authentication process and determining security related property of a connection

request from the testing device 202. The gateway device 208 may be a computer system including a communication interface (for example, an Ethernet transceiver, an Ethernet controller, or the like) including an edge node 206 via a communication line over a first network. The gateway device 208 may be connected to the testing device 202 via an activation line and the communication line. The gateway device 208 may include a processor 210, and a storage device such as a memory 212. The memory 212 may store a computer program (hereinafter referred to as "connection authentication program") describing a command for executing the connection security process and other processes. In an embodiment, the processor 210 may perform the connection authentication process by interpreting and executing the security program. Further, an activation line may be provided for detecting a connection request from the testing device 202. The communication line between the testing device 202 and the gateway device 208 may be via an Ethernet LAN. The gateway device 208 may be capable of gating DoIP messages to all vehicle subnetworks and/or the DoIP network nodes 216. In an embodiment, the latency between gateway device 208 and testing device 202 for DoIP to DoIP routing may be, but not limited to, 1ms or less. In an embodiment, different Global Protocol Data Units (GPDUs) may be provided to transport the data to the next layer for all communications from the gateway device 208 to the network nodes 216. The gateway device 208 may include a router (not shown) which may create mapping tables which may be used to map the GPDU associated with source logical address to the GPDU associated with target logical address in the diagnostic message received/transmitted back and forth from the testing device 202 for the intended target network node(s). In an embodiment, the mapping table may be used in both transmission and reception of communication between the network nodes and the testing device 202.

[026] The gateway device 208 may receive from the testing device 202, a connection request. The gateway device 208 may determine a routing information in the diagnostic input. A router of the gateway device 208 may determine the target address of target network nodes for which the connection request is aimed to be transmitted. The gateway device 208 may be simultaneously connected via a second connection with each of the one or more vehicle network nodes 216. The second connection between the gateway device 208 and the network nodes 216 may be implemented through the switch 214. In an embodiment, separate switches may be provided to connect the testing device 202 with the gateway device 208 over the first network and to connect the gateway device 208 with the one or more vehicle network nodes 216 over the second network 224. After establishing the second connection with each of the

one or more vehicle network nodes 216 by the gateway device 208, one or more target network nodes 216 may be determined from the one or more network nodes 216, based on the target address information detected in the diagnostic input received from the testing device 202 in the diagnostics communication. Accordingly, the network nodes 216 may be decoupled from the testing device 202, by using the gateway device 208. The gateway device 208 may provide a gateway functionality in a DoIP network. This may allow third party testing devices 202 to connect to the electronic ECUs of the network nodes 216 indirectly through the gateway device 208 without comprising the security of the vehicle. Thus, third party testing devices 202 may be able to provide diagnostics to the network nodes 216 in a secure manner. It may be noted that the connection request or diagnostic communication is transmitted to the target network nodes 216 simultaneously via an individual second connection line to each of the target network nodes. Each of the second connection line to the network nodes 216 may conform to static IPv4 standards and support transmission of 0x8001 type payload only. In an embodiment, the DHCP functionality may not be implemented by the network nodes 216. In an embodiment, the gateway device 208 may always be connected to the network nodes 216 and may not require discovery mechanism.

[027] In an embodiment, diagnostic output in the form of system information may be transmitted from the network nodes 216 to the gateway device 208 over the second connection using second network 224. The received diagnostic output from the network nodes 216 may be transmitted to the testing device 202 by the gateway device 208 over the first connection using the first network 204. In an embodiment, the system information may be generated as a result or output of any diagnostics performed on the network node 216 or based on occurrence of one or more errors in any system associated with the network nodes 216. The information when transmitted to the gateway device 208 may be transmitted to the testing device 202 in order to provide an appropriate diagnostic to the errors occurred in the network nodes 216 or monitor the diagnostic output of target network node.

[028] **FIG. 2B** illustrates a DoIP message format and payload encapsulation, in accordance with an embodiment of the current disclosure. The gateway device 208 may identify the target network node based on the data payload which may include a source address and a target address. A diagnostic message request, packed in the form of the DoIP message format as shown in **FIG. 2B**, includes TCP/IP payload from the testing device 202 may be received by the gateway device 208. A router of the gateway device 208 may then unpack the

received communication message to determine the payload data and separate the required diagnostic information which may include a payload, a payload length, a protocol version, an inverse protocol version, a payload type which in the current embodiment may be 0x8001 type, a source address, and a target address. For the current embodiment, the gateway device 208, may conform to DoIP standards. The gateway device 208 may identify, from the diagnostics communication, a payload to be transmitted to the target nodes from the one or more network nodes 216. The edge node 206 may be DoIP compliant and may transmit the payload based on the target logical address via the switch 214. Further, if the payload carries a functionally addressed request to be broadcasted then the gateway device 208 may transmit the same diagnostics information to all the nodes 216.

[029] In an embodiment, the second connection line may be implemented using TCP/IP connection and over a LAN network. In an embodiment, the network nodes 216 other than the target network nodes may be deactivated or become dormant at the time of transmitting and receiving the diagnostic communication over the second connection to one or more target network nodes. After identifying the target node, the network node client (described later) of the gateway device 208 may keep the second connection alive or activated with the target nodes during the transmission or reception of the diagnostic input or communication. In an embodiment, the DoIP network node client may transmit TCP keep alive messages after a pre-defined timeout period has passed. In an embodiment, the pre-defined timeout period is 10 seconds.

[030] Referring now to **FIG. 3**, a block diagram 300 of a gateway device 208 of **FIG. 2A**, in accordance with an embodiment of the current disclosure. As shown in FIG. 3, the block diagram 300 of a gateway device 208 may include a routing module 302, a security module 304, a DoIP network node client 306, other module(s) 308. The DoIP gateway device 208 may include a DoIP Edge node 206. Further, the gateway device 208 may be communicably coupled to the DoIP edge node 206.

[031] In an embodiment, the routing module 302 may determine routing information from the communication request or diagnostic input received from the testing device 202. **FIG. 2B**, shows an exemplary DoIP message format and payload encapsulation, in accordance with an embodiment of the present disclosure. The routing module 302 of the gateway device 208 may identify the target network node based on the data payload which may include a source address and a target address. A diagnostic message request, packed in the form of TCP/IP

payload from the testing device 202 may be received by the gateway device 208. The routing module 302 of the gateway device 208 may then unpack the received communication message to determine the payload data and separate the required diagnostic information which may include a payload, a payload length, a protocol version, an inverse protocol version, a payload type which in the current embodiment may be 0x8001 type, a source address, and a target address. For the current embodiment, the gateway device 208, may conform to DoIP standards. The routing module 302 may identify, from the diagnostics communication, a payload to be transmitted to the one or more network nodes 216.

[032] The security module 304 may enable SSL (Secure Socket Layer), TLS (Transport Layer Security) for secure communication between the gateway device 208 and the network nodes 216. The security module 304 may perform a connection authentication process and determine security related property of a connection request from the testing device 202. Further, the security module 304 may determine authentication of the testing device 202 based on pre-defined registration of the testing device 202. In an embodiment, the security module 304 may determine a possibility of a security breach based on an unauthorized/unsecure connection request made by an external or third-party testing device 202.

[033] In another embodiment, the security module 304 may allow or reject gating of the diagnostic input from the testing device 202. This is done by analyzing the payload data and current vehicle operating conditions as a countermeasure to potential security threats & vulnerabilities. In an embodiment, the security condition may relate to the vehicle's operational condition associated to the node 216. In an embodiment, the security module 304 may restrict transmission of a specific diagnostic communication from the gateway device 208 to the network nodes 216 in case a vehicle speed determined is greater than the pre-defined value. In an embodiment, in case the connection request has a diagnostics request related to operation control of the vehicle network node 216 as per the OEM specific security policy engine, the security module 304 may restrict such communication between the testing device 202 and the electronic control unit of the network node 216.

[034] In an embodiment, the security module 304 may restrict the communication with the network nodes 216 when a vehicle is moving at a speed above a threshold value. Accordingly, safety, security and performance may be enhanced. In an embodiment, the gateway device 208 may reject the connection request altogether when it is determined that the security condition is not satisfied. In an embodiment, the gateway device 208 may periodically

check if the security condition is satisfied in order to allow the communication from the testing device 202. In an embodiment, the testing device 202 may determine the rejection of the diagnostic request based on timeout mechanism.

[035] The network node client 306 may be connected with the network node server to establish the second connections with the network nodes 216 over a secured VLAN and may conform to DoIP standards partially. In an embodiment, the network node client 306 shall only support 100 Mb OPEN SIG Ethernet. The network node client 306 shall disable the Auto-Negotiation function. The network node client 306 shall support the ICMP protocol specified by IETF RFC 792. The network node client 306 shall establish all DoIP related TCP socket connections simultaneously with each of the network nodes 216. The network node client 306 shall have direct TCP socket connections to all network nodes 216 in the vehicle. Hence, the network node client 306 may support communication to multiple network nodes 216 from the DoIP gateway device 208. The network nodes 216 shall support the Keep Alive Mechanism as specified in RFC 1122 (Requirements for Internet Hosts – Communication Layers). In an embodiment, the DoIP Network Node Client 306 may support transmission of TCP Keep Alive Messages to keep established sockets open in idle condition. In an embodiment, the TCP Keep Alive Messages would be sent after a predefined timeout period tracked over a TCP Keep Alive timer. In an embodiment, the predefined timeout period may be, but not limited to, 10 seconds.

[036] In an embodiment, the DoIP Network Node Client 306 may establish the TCP DATA Socket connections with all the DoIP Network Nodes 216 whenever the Network Nodes 216 are awake or after reset. In an embodiment, the reset time for the network nodes 216 may be, but not limited to, 500ms or less. In an embodiment, the DoIP Network Node Client 306 may connect to TCP port 13400 of the Network Nodes 216. Further, the Network Node Client 306 may have one static IPv4 IP-address. In an embodiment, the Routing activation mechanism may not be required between the DoIP Network Node Client 306 and Network Nodes 216. The communication between the gateway device 208 may be done through a Diagnostic Message payload type (0x8001) may be transmitted and received between the testing device 202 and the DoIP Network Node Client 306. In an embodiment, the socket connections between the network nodes 216 and the gateway device 208 may be established and closed by standard TCP handshake specified in RFC 793. In case the sockets connection gets disconnected, the connection shall be re-established again.

[037] Referring now to **FIG. 4**, a method of performing vehicle diagnostics communication is disclosed via a flowchart 400 in accordance with an embodiment. FIG. 4 is explained in conjunction with FIGs. 1-3. Each step of the flowchart 400 may be executed by various modules (same as the modules of the system 200).

[038] At step 402, a Diagnostics Over Internet Protocol (DoIP) gateway device 208 implementing a DoIP network node client 306 may receive a connection request from a testing device 202 over a first communication network 204, to establish a first connection with the testing device 202 via a DoIP edge node 206.

[039] At step 404, the DoIP gateway device 208 may receive a diagnostic input from the testing device 202, through the first connection over the first communication network 204.

[040] At step 406, the gateway device 208 may determine at least one target network node from one or more network nodes 216 based on the diagnostic input.

[041] At step 408, the gateway device 208 may transmit the diagnostic input to the at least one target node from the one or more network nodes 216 through a second connection between the gateway device 208 and each of the one or more network nodes over a second communication network 224. In an embodiment, the second connection is established simultaneously between the DoIP gateway device 208 and each of the one or more network nodes 216 via the DoIP network node client 306. Further, the DoIP network node client 306 keeps the second connection active with at least one target node during the transmission or reception of the diagnostic input.

[042] At step 410, diagnostics may be performed at the at least one target network node, based on the diagnostic input. In an embodiment, diagnostic results in the form of system information may be transmitted from the network nodes 216 to the gateway device 208 over the second connection using second network 224. The received diagnostic results from the network nodes 216 may be transmitted to the testing device 202 by the gateway device 208 over the first connection using the first network 204.

[043] It is intended that the disclosure and examples be considered as exemplary only, with a true scope of disclosed embodiments being indicated by the following claims.

WE CLAIM:

1. A method of performing vehicle diagnostics communication, the method comprising:

receiving, by a Diagnostics Over Internet Protocol (DoIP) gateway device, a DoIP connection request from a testing device over a first communication network, to establish a first connection with the testing device, wherein the DoIP gateway device implements a DoIP network node client;

receiving, by the DoIP gateway device, a diagnostic input from the testing device, through the first connection over the first communication network;

determining, by the DoIP gateway device, at least one target network node from one or more network nodes, based on the diagnostic input;

transmitting, by the DoIP gateway device, the diagnostic input to the at least one target network node from the one or more network nodes through a second connection between the DoIP gateway device and each of the one or more network nodes over a second communication network,

wherein the second connection is established simultaneously between the DoIP gateway device and each of the one or more network nodes via the DoIP network node client, and

wherein the DoIP network node client keeps the second connection active with the at least one target network node during the transmission of the diagnostic input; and

performing diagnostics at the at least one target network node, based on the diagnostic input.

2. The method as claimed in claim 1, wherein the first connection is compliant to ISO 13400-2 specification.

3. The method as claimed in claim 1, wherein the diagnostic input is transmitted to the target network node over the second connection based on routing data, wherein the routing data is determined by a router associated with the DoIP gateway device.

4. The method as claimed in claim 3, wherein the routing data comprises DoIP source logical address and a target logical address associated with the target network node.

5. The method as claimed in claim 1, wherein the first connection between the test tool and the gateway device over the first communication network is an Ethernet-based connection.

6. The method as claimed in claim 1, wherein the DoIP network node client is communicatively coupled to the one or more network nodes via a switch.

7. The method as claimed in claim 1, wherein the second network connection is IPv4 complaint.

8. The method as claimed in claim 1, wherein the DoIP network node client keeps the second connection active with each of the target node by transmitting TCP Keep Alive messages to each of the target node.

9. The method as claimed in claim 1, wherein the one or more network nodes are configured to transmits and receive 0x8001 DoIP payload type.

10. A system for performing vehicle diagnostics communication comprising:

a Diagnostics Over Internet Protocol (DoIP) gateway device comprising:

one or more processors; and

a memory communicatively connected to the one or more processors, wherein the memory stores a plurality of processor-executable instructions, which, upon execution, cause the processor to:

receive, a connection request from a testing device over a first communication network, to establish a first connection with the testing device,

wherein the DoIP gateway device implements a DoIP network node client;

receive a diagnostic input from the testing device, through the first connection over the first communication network;

determine at least one target network node from one or more network nodes, based on the diagnostic input;

transmit the diagnostic input to the at least one target network node from the one or more network nodes through a second connection between the DoIP gateway device and each of the one or more network nodes over a second communication network,

wherein the second connection is established simultaneously between the DoIP gateway device and each of the one or more network nodes via the DoIP network node client, and

wherein the DoIP network node client keeps the second connection active with the at least one target network node during the transmission of the diagnostic input; and

perform diagnostics at the at least one target network node, based on the diagnostic input.

Dated this 4th day of August 2022

-- Digitally Signed--

Bhanu Prasad (INPA No: **3253**)
Manager, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

ABSTRACT

METHOD AND SYSTEM FOR PERFORMING VEHICLE DIAGNOSTICS COMMUNICATION

A method of performing end-to-end vehicle diagnostics communication is disclosed. A Diagnostics Over Internet Protocol (DoIP) based gateway device may implement a DoIP edge node which receives and accepts a first connection request from a testing device over a first communication network. DoIP network node client which is part of the DoIP gateway device initiates and establishes second connection(s) over a second communication network with at least one target network node. The DoIP gateway device may receive a diagnostic input from the testing device, through the first connection. The DoIP gateway device may determine at least one target network node and transmits the diagnostic input to one or more network nodes over a second connection. Diagnostics may be performed with at least one target network node based on the received diagnostic input and diagnostic output from target network node will be transmitted back to the testing device via DoIP gateway.

[To be published with FIG. 2]

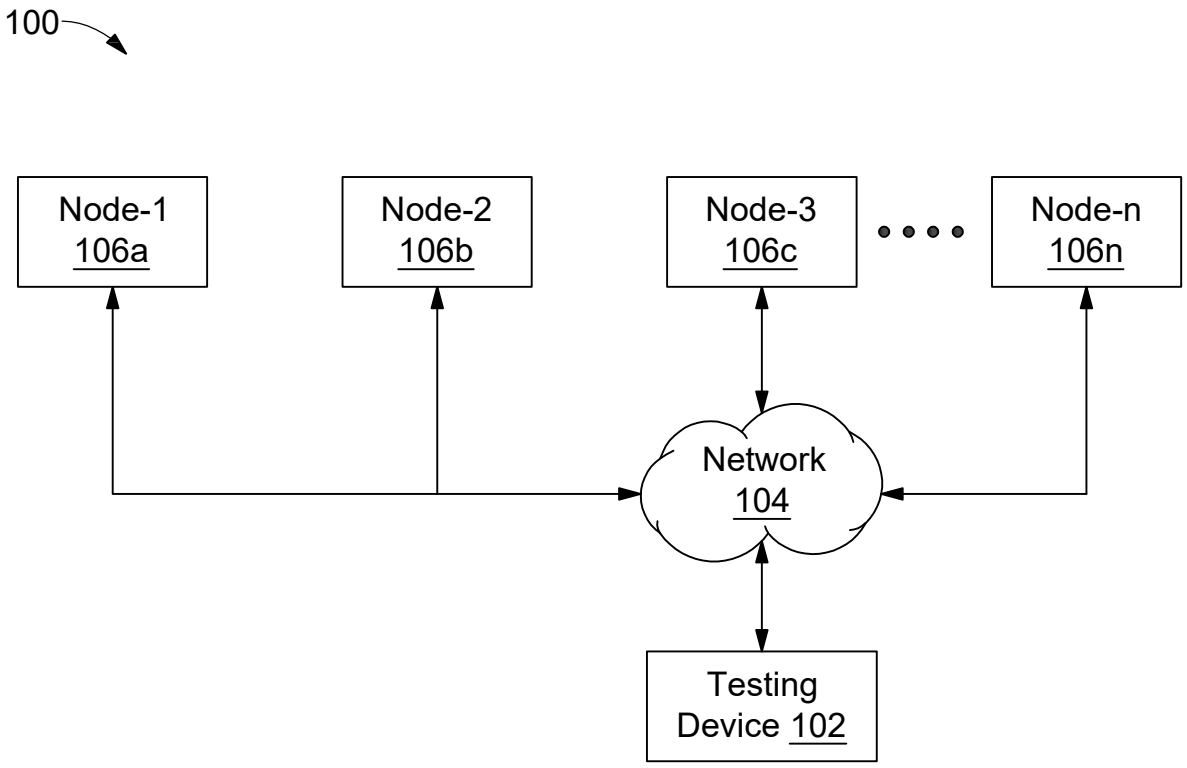

FIG. 1 (PRIOR ART)

-- Digitally Signed--

Bhanu Prasad (INPA No: 3253)
Manager, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

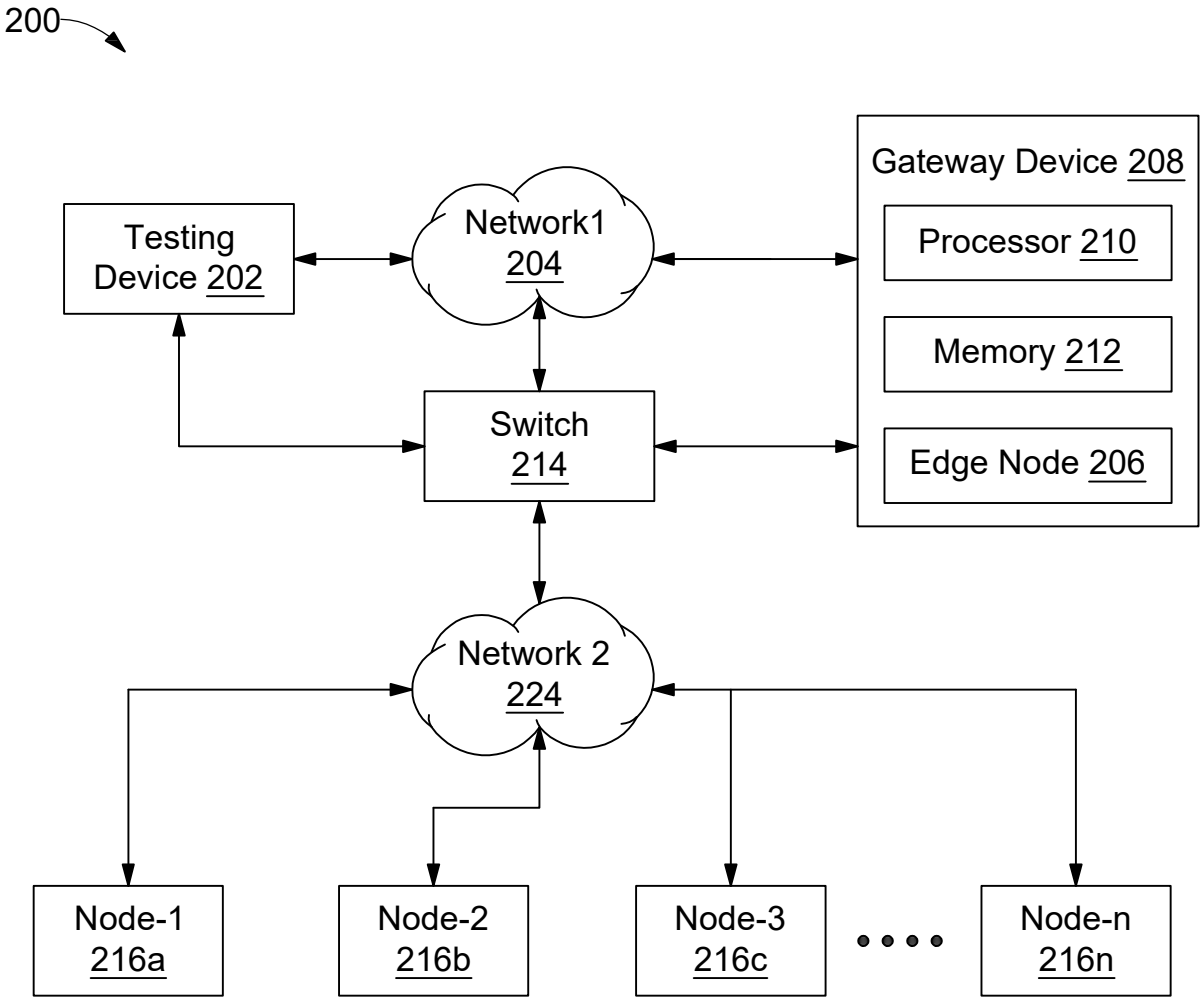

FIG. 2A

-- Digitally Signed--

Bhanu Prasad (INPA No: 3253)
Manager, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

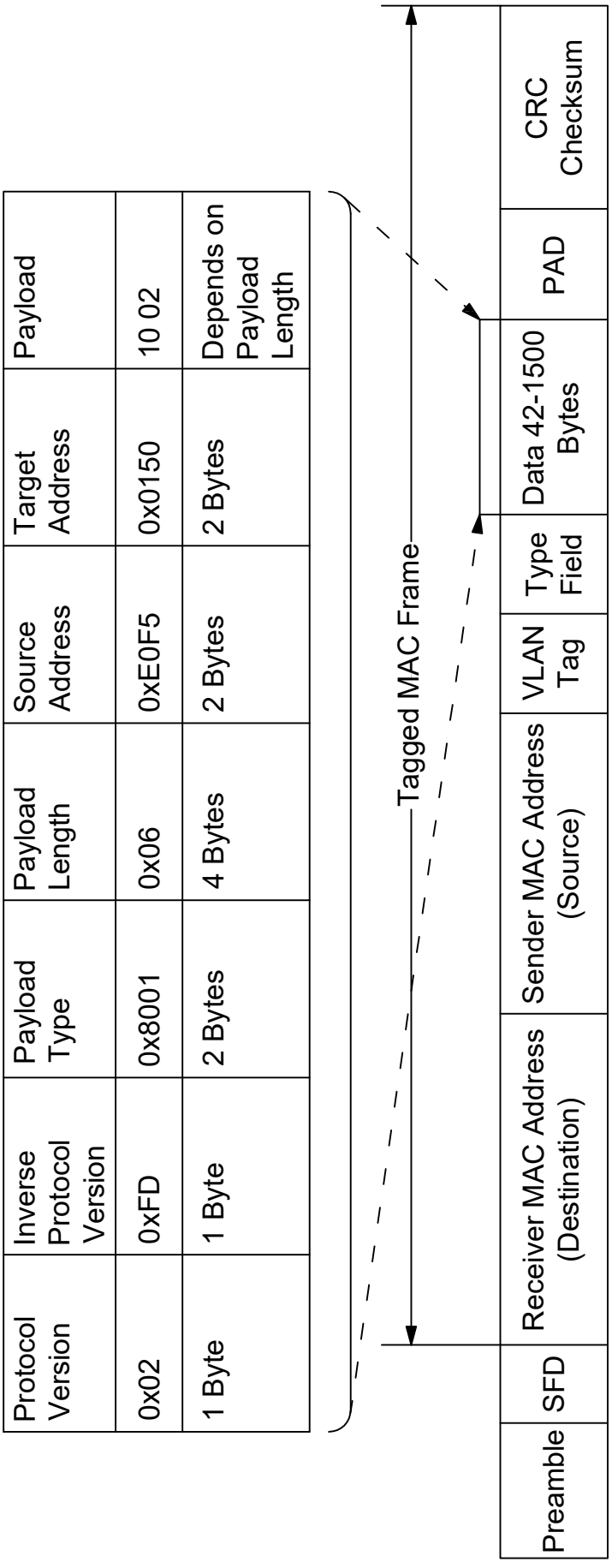

FIG. 2B

-- Digitally Signed--

Bhanu Prasad (INPA No: 3253)
Manager, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

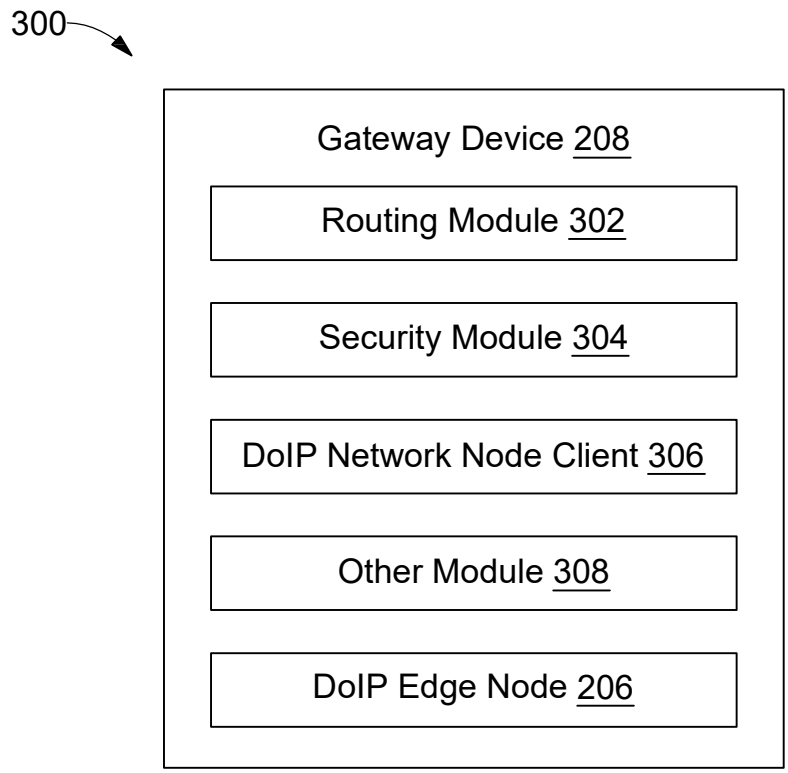

FIG. 3

-- Digitally Signed--

Bhanu Prasad (INPA No: 3253)
Manager, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

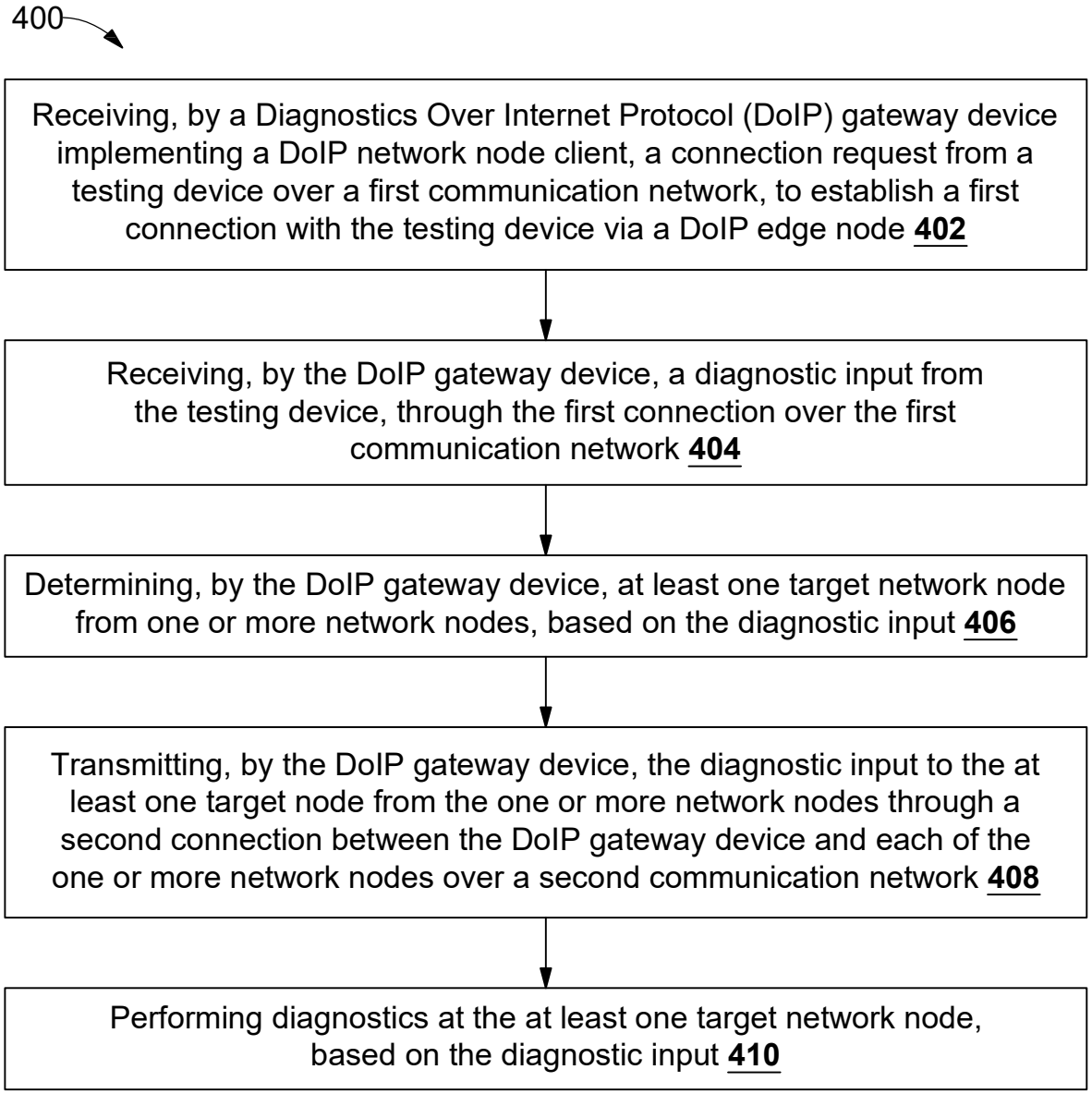

FIG. 4

-- Digitally Signed--

Bhanu Prasad (INPA No: 3253)
Manager, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.