

CUSTOMIZATION OF DATA SESSION RETRY MECHANISM
IN A WIRELESS PACKET DATA SERVICE NETWORK

FIELD OF THE APPLICATION

[0001] The present patent application generally relates to wireless packet data service networks. More particularly, and not by way of any limitation, the present patent application is directed to a scheme for customization of a mobile device's data session retry mechanism in a wireless packet data service network.

BACKGROUND

[0002] Radio resources in a wireless packet data service network are scarce. When a data-centric mobile device continues to negotiate with the network infrastructure for establishing a data session even after it receives certain reject codes, such repeated attempts can contribute to an increase in the signaling load in the network whereby the overall performance of the network may be negatively impacted.

SUMMARY

[0003] In one embodiment, a scheme is provided for customization of a mobile communications device's data session retry mechanism in a wireless packet data service network. Upon detecting that a cause code has been returned by a node disposed in a wireless packet data service network, a structure is interrogated to determine if the cause code is mapped to a flag relating to the device's data session retry mechanism. Responsive to determining that the received cause code is mapped as a critical cause code, the

data session retry mechanism of the mobile communications device is disabled so that further signaling messages towards the network are prevented.

[0004] In another embodiment, a mobile communications device is disclosed which comprises: means for detecting that a cause code has been returned by a node disposed in a wireless packet data service network operable with the mobile communications device; means for interrogating a structure to determine if the cause code is mapped to a flag relating to the mobile communications device's data session retry mechanism; and means for disabling the mobile communications device's data session retry mechanism responsive to determining that the cause code is mapped as a critical cause code in the structure.

[0005] In yet another embodiment, a wireless packet data service network is disclosed which comprises: a serving node operable to serve a mobile communications device for establishing a data session with a public packet-switched network; a gateway node disposed between the serving node and the public packet-switched network; and a structure having a database for mapping a cause code generated by a node in the wireless packet data service network to a flag relating to the mobile communications device's data session retry functionality, wherein the flag is operable for identifying the cause code as a critical cause code that triggers disabling of the mobile communications device's data session retry functionality.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] A more complete understanding of the embodiments of the present patent application may be had by reference to the following Detailed Description when taken in conjunction with the accompanying drawings wherein:

[0007] FIG. 1 depicts an exemplary network environment including a wireless packet data service network wherein an embodiment of the present patent application may be practiced;

[0008] FIG. 2A depicts additional details of an exemplary wireless packet data service network operable with a mobile communications device in accordance with an embodiment;

[0009] FIGS. 2B-2D depict message flow diagrams with respect to various signaling procedures utilized in accordance with an embodiment;

[0010] FIG. 3 depicts an exemplary list of cause codes operable with the wireless packet data service network shown in FIG. 2A in servicing a mobile communications device according to one embodiment;

[0011] FIG. 4 depicts an exemplary structure for mapping cause codes of a wireless packet data service network to a flag relating to a mobile communications device's data session retry mechanism;

[0012] FIG. 5 depicts a software architectural view of a mobile communications device operable to customize its data session retry mechanism according to one embodiment;

[0013] FIG. 6 depicts a flowchart of an embodiment for customizing data session retry operations in a mobile communications device; and

[0014] FIG. 7 depicts a block diagram of a mobile communications device operable to customize its data session retry mechanism according to one embodiment.

DETAILED DESCRIPTION OF THE DRAWINGS

[0015] A system and method of the present patent application will now be described with reference to various examples of how the embodiments can best be made and used. Like reference numerals are used throughout the description and several views of the drawings to indicate like or corresponding parts, wherein the various elements are not necessarily drawn to scale. Referring now to the drawings, and more particularly to FIG. 1, depicted therein is an exemplary network environment 100 including a wireless packet data service network 112 wherein an embodiment of the present patent application may be practiced. An enterprise network 102, which may be a packet-switched network, can include one or more geographic sites and be organized as a local area network (LAN), wide area network (WAN) or metropolitan area network (MAN), et cetera, for serving a plurality of corporate users. A number of application servers 104-1 through 104-N disposed as part of the enterprise network 102 are operable to provide or effectuate a host of internal and external services such as email, video mail, Internet access, corporate data access, messaging, calendaring and scheduling, information management, and the like. Accordingly, a diverse array of personal information appliances such as desktop computers, laptop computers, palmtop computers, et cetera, although not specifically shown in FIG. 1, may be operably networked to

one or more of the application servers 104-i, $i = 1, 2, \dots, N$, with respect to the services supported in the enterprise network 102.

[0016] Additionally, a remote services server 106 may be interfaced with the enterprise network 102 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable mobile communications device (MCD) 116. A secure communication link with end-to-end encryption may be established that is mediated through an external IP network, i.e., a public packet-switched network such as the Internet 108, as well as the wireless packet data service network 112 operable with MCD 116 via suitable wireless network infrastructure that includes a base station (BS) 114. In one embodiment, a trusted relay network 110 may be disposed between the Internet 108 and the infrastructure of wireless packet data service network 112. By way of example, MCD 116 may be a data-enabled handheld device capable of receiving and sending messages, web browsing, interfacing with corporate application servers, et cetera.

[0017] For purposes of the present patent application, the wireless packet data service network 112 may be implemented in any known or heretofore unknown mobile communications technologies and network protocols, as long as a packet-switched data service is available therein for transmitting packetized information. For instance, the wireless packet data service network 112 may be comprised of a General Packet Radio Service (GPRS) network that provides a packet radio access for mobile devices using the cellular infrastructure of a Global System for Mobile Communications

(GSM)-based carrier network. In other implementations, the wireless packet data service network 112 may comprise an Enhanced Data Rates for GSM Evolution (EDGE) network, an Integrated Digital Enhanced Network (IDEN), a Code Division Multiple Access (CDMA) network, or any 3rd Generation (3G) network. By way of providing an exemplary embodiment, the teachings of the present patent application will be illustrated with a GPRS-based carrier network, although those skilled in the art should readily recognize that the scope of the present patent application is not limited thereby.

[0018] FIG. 2A depicts additional details of an exemplary wireless packet data service network operable with a mobile communications device in accordance with an embodiment. As illustrated, reference numeral 202 refers to a GPRS network operable as the wireless packet data service network with respect to MCD 116 that is provided with a number of data-centric user applications 210 such as, e.g., web browsing, email, multimedia, File Transfer Protocol or FTP, telnet, etc. Base station 114 serves MCD 116 via the air interface using applicable radio layer protocols.

[0019] GPRS uses a packet-switching technique to transfer both high-speed and low-speed data and signaling in an efficient manner over GSM radio networks. Packet switching means that GPRS radio resources are used only when users are actually sending or receiving data. Rather than dedicating a radio channel to a mobile data user, e.g., MCD 116, for a fixed period of time, the available radio channels can be concurrently shared between several users. Therefore, GPRS is designed to support from intermittent and bursty data

transfers (e.g., web browsing) to occasional transmission of large volumes of data (e.g., FTP). Allocation of GPRS radio channels can be flexible: from 1 to 8 radio interface timeslots can be allocated per one Time Division Multiple Access (TDMA) frame. Typically, timeslots are shared by the active users, and uplinks and downlinks are allocated separately. Various radio channel coding schemes are available to allow a range of data bit transfer rates.

[0020] Two additional network nodes are provided within a GSM network in order to implement a packet-switched data transfer service. A Serving GPRS Support Node (SGSN) 206, which is coupled to a Home Location Register (HLR) 204 and disposed at the same hierarchical level as a Mobile Switching Center (MSC) of the circuit-switched cellular network, is operably coupled to BS 114 and keeps track of the location of a GPRS user such as the user of MCD 116. Further, SGSN 206 is responsible for performing security functions and handling access control with respect to MCD 116. A Gateway GPRS Support Node (GGSN) 208 provides interworking with the external packet-switched IP network 108, and is operably coupled to one or more SGSNs, e.g., SGSN 206, via an IP-based GPRS backbone network.

[0021] In order to access the packet data service, MCD 116 makes its presence known to the network by performing what is known as a GPRS Attach. Thereafter, to send and receive packet data, MCD 116 activates the packet data address that it wants to use. This operation renders MCD 116 "visible" in the corresponding GGSN, and interworking with external data networks can then begin. User data is transferred transparently between MCD 116 and the external

data networks with a method known as encapsulation and tunneling wherein data packets are equipped with GPRS-specific protocol information and transferred transparently between MCD 116 and GGSN 208.

[0022] To get access to the GPRS network 202 and to start data transmission, various signaling procedures are therefore effectuated before activating a Packet Data Protocol (PDP) context between MCD 116 and the network. FIGS. 2B-2D depict a plurality of message flow diagrams with respect to various signaling procedures utilized in the GPRS network 202 in accordance with an embodiment. Referring in particular to FIG. 2B, an Attach signaling procedure is described therein. In an Attach procedure, MCD 116 provides its identity, e.g., International Mobile Station Identity (IMSI), and the type of attach (i.e., GPRS Attach) via an Attach Request message 220 to SGSN 206. Once SGSN 206 obtains the identity of MCD 116, it retrieves the subscriber information from HLR 204. If the subscriber information cannot be found, SGSN 206 will return an Attach Reject reply message to MCD 116. If the requisite subscriber information is found in HLR 204, SGSN 206 accepts the Attach Request message 220 and allocates a new identifier, e.g., Packet-Temporary Mobile Station Identity or P-TMSI, to MCD 116. A Temporary Logical Link Identifier (TLLI) is then derived from the P-TMSI received from SGSN 206. The derived TLLI will be used by MCD 116 to identify itself for subsequent signaling or data procedures with the GPRS network.

[0023] Accordingly, responsive to the Attach Request message 220, SGSN 206 updates HLR 204 with the current location of MCD 116 by sending an Update GPRS Location

Request message 222. In response, HLR 204 sends the subscriber information relating to MCD 116 to SGSN 206 through an Insert Subscriber Data Request message 224, which is acknowledged by SGSN 206 via an Acknowledge message 226. Thereafter, HLR 204 acknowledges completion of update location to SGSN 206 via an Update GPRS Location Acknowledge message 228. Since appropriate subscriber information has been found in HLR 204, SGSN 206 sends an Attach Accept message 230 with a P-TMSI to MCD 116. In response, MCD 116 returns an Attach Complete message 232 with a TLLI derived from the P-TMSI to acknowledge the receipt of the P-TMSI.

[0024] After the Attach procedure is successfully executed, MCD 116 enters a Ready state whereupon a Mobility Management (MM) context, which is a record that contains subscriber information and MCD identity, is established in both MCD 116 and SGSN 206. Thereafter, MCD 116 may activate a PDP context via an Activation signaling procedure for communicating with an external data network. FIG. 2C depicts a message flow diagram with respect to an Activation signaling procedure. MCD 116 is operable to specify a Transaction Identifier (TI) and a Network Service Access Point Identifier (NSAPI) which are used by the GPRS infrastructure to uniquely identify a data session. In a further implementation, MCD 116 can include an Access Point Name (APN) in the message, which directs SGSN 206 to select a particular GGSN for use. By way of example, MCD 116 may send an Activate PDP Context Request message 250 with such parameters as TI, NSAPI, APN, Requested Quality of Service (QoS), etc., to SGSN 206. Upon validating the message, SGSN 206 sends a Create PDP Context Request message 252 to the

appropriate GGSN 208 with a Tunnel Identifier (TID) constructed by appending the identity of MCD 116 and the NSAPI. GGSN 208 validates the parameters in the Create PDP Context Request message 252 and returns a Create PDP Context Response message 254 with no error code if the Request is accepted. Thereafter, SGSN 206 sends an Activate PDP Context Accept message 256 to MCD 116 to indicate that the requested data session has been activated.

[0025] User data coming from the application layer may be encapsulated before reaching the external packet data network. As shown in FIG. 2D, user data 260 is first tunneled between MCD 116 and SGSN 206 in a SubNetwork(SN)-UNITDATA message 262. The user data is then tunneled between SGSN 206 and GGSN 208 in a GPRS Tunneling Protocol (GTP) Tunneling-Packet Data Unit (T-PDU) message 264. Thereafter, GGSN 208 extracts the user data 266 and sends it to the external packet data network.

[0026] From the foregoing Description, it can be appreciated that various signaling procedures are executed pursuant to activating PDP contexts in a wireless packet data service network such as the GPRS-based network 202. Further, the manner and mode of the signaling behavior in the network can be dependent on the state and condition of the network, e.g., availability of resources, signaling load, congestion, integrity of the physical plant, et cetera. Accordingly, the network management infrastructure is operable to issue a number of cause codes, which signify different network responses based on network conditions as well as MCD-related information (e.g., the network is busy, invalid APN entry, GGSN is out of order, subscriber in

default or unauthenticated, et cetera) that can impact a PDP activation procedure initiated by a mobile device.

[0027] FIG. 3 depicts an exemplary list of cause codes operable with the wireless packet data service network shown in FIG. 2 in servicing a mobile communications device according to one embodiment. As set forth in table 300, a cause code (CC) column 302 shows a plurality of cause codes, each with a corresponding entry in a related column 304 that provides an explanation of the CC. For example, upon receipt of an Activate PDP Context Request message the network may reject the MCD-initiated context activation by sending an Activate PDP Context Reject message to the MCD that includes a CC #26 (which may be embodied as an n-bit integer) to indicate insufficient resources. Similarly, a CC #29 may be issued if user authentication has failed. Other CC entries of the table 300 are likewise operable to indicate corresponding network responses.

[0028] As alluded to in the Background section of the present patent application, when a data-centric mobile device continues to retry establishing a data session with the network upon receiving certain cause codes, e.g., indicating failure of a PDP context, its retransmission logic keeps sending signaling messages towards the network, thereby increasing the signaling load therein. In accordance with the teachings of the present patent application, a scheme is provided wherein the data session retry mechanism of the mobile device is customized based on the cause code functionality so as to reduce such signaling load in the network.

[0029] FIG. 4 depicts an exemplary structure 400 for mapping cause codes of a wireless packet data service network to a flag or indicium relating to a mobile communications device's data session retry mechanism. In essence, a subset of the cause codes associated with a carrier network may be identified as "critical" cause codes that are mapped to a "NO RETRY" indicium to signify that the retransmission logic of the data session retry mechanism be disabled when such a cause code is received from the network. In one embodiment, the structure 400 may be provided as a configurable resource file associated with a library that is integrated within the mobile device such as MCD 116. In another embodiment, the configurable library/structure 400 may be provisioned as part of a carrier network's infrastructure, e.g., associated with a GGSN.

[0030] As illustrated in FIG. 4, a CC column 404 is provided on a carrier-by-carrier basis identifying various critical codes for the carriers in a carrier column 402. In a retry mechanism flag column 406, each CC is marked with a suitable indicium that indicates whether or not the data session retry mechanism is to be disabled. It should be appreciated that such data may also be configured on a mobile communications device by mobile communications device basis. As will be described in detail hereinbelow, an MCD's communications transport protocol stack is operable to query the structure 400 in order to customize its retransmission logic, depending on the status of a new PDP context activation or an existing PDP context.

[0031] FIG. 5 depicts a software architectural view of a mobile communications device operable to customize its data session retry mechanism according to one embodiment. A multi-layer transport stack (TS) 506 is operable to provide a generic data transport protocol for any type of corporate data, including email, via a reliable, secure and seamless continuous connection to a wireless packet data service network. As illustrated in the embodiment of FIG. 5, an integration layer 504A is operable as an interface between the MCD's radio layer 502 and the transport stack 506. Likewise, another integration layer 504B is provided for interfacing between the transport stack 506 and the user applications 507 supported on the MCD, e.g., email 508, calendar/scheduler 510, contact management 512 and browser 514. Although not specifically shown, the transport stack 506 may also be interfaced with the MCD's operating system. In another implementation, the transport stack 506 may be provided as part of a data communications client module operable as a host-independent virtual machine on a mobile device.

[0032] The bottom layer (Layer 1) of the transport stack 506 is operable as an interface to the wireless network's packet layer. Layer 1 handles basic service coordination within the exemplary network environment 100 shown in FIG. 1. For example, when an MCD roams from one carrier network to another, Layer 1 verifies that the packets are relayed to the appropriate wireless network and that any packets that are pending from the previous network are rerouted to the current network. The top layer (Layer 4) exposes various application interfaces to the services supported on the MCD.

The remaining two layers, Layer 2 and Layer 3, are responsible for datagram segmentation/reassembly and security, compression and routing, respectively.

[0033] A configurable CC resource file 516 provided as part of the software environment, is disposed in operable communication with the transport stack 506 as well as the MCD's radio layer 502. In one embodiment, the CC resource file 516 may comprise a query-able library structure such as the embodiment described above in reference to FIG. 4, which includes appropriate mapping between critical cause codes and the MCD's data session retry mechanism. The contents of the library structure may be dynamically configured upon instantiation of the CC resource file 516. The transport stack 506 is operable to access and interrogate the CC resource library under suitable conditions when the retransmission logic of the MCD's data session retry mechanism is invoked. Also, the flag descriptor (i.e., "Retry"/"No Retry") may be passed to the integration layer between the user interface and the radio, where the integration layer manages the retry mechanism.

[0034] FIG. 6 depicts a flowchart of an embodiment for customizing data session retry operations in a mobile communications device. Upon detecting by the transport stack of the MCD that a PDP context has failed to be established or is lost (e.g., because the device is out of coverage area, the PDP context is torn down because of a timeout, et cetera) (block 602), a CC resource file structure/library is queried by the transport stack (block 604). In one implementation, the transport stack may query the structure/library prior to invoking the MCD's

retransmission logic or may wait until after a few retransmission attempts have been made. A determination is made if the CC issued by the network is a critical cause code mapped to a "NO RETRY" indicium relating to the MCD's data session retry mechanism (block 606). If not, the retransmission logic of the MCD's data session retry mechanism continues to attempt establishing a PDP context (block 608). Otherwise, the data session retry mechanism is disabled or deactivated (block 610). By way of an exemplary implementation, the data session retry mechanism may be deactivated until the CC structure/library (which has access to the radio layer as an observer) resolves that the retry mechanism may be re-activated.

[0035] FIG. 7 depicts a block diagram of a mobile communications device operable to customize its data session retry mechanism according to one embodiment. It will be recognized by those skilled in the art upon reference hereto that although an embodiment of MCD 116 may comprise an arrangement similar to one shown in FIG. 7, there can be a number of variations and modifications, in hardware, software or firmware, with respect to the various modules depicted. Accordingly, the arrangement of FIG. 7 should be taken as illustrative rather than limiting with respect to the embodiments of the present patent application. A microprocessor 702 providing for the overall control of an embodiment of MCD 116 is operably coupled to a communication subsystem 704 which includes a receiver 708 and transmitter 714 as well as associated components such as one or more local oscillator (LO) modules 710 and a processing module such as a digital signal processor (DSP) 712. As will be

apparent to those skilled in the field of communications, the particular design of the communication module 704 may be dependent upon the communications network with which the mobile device is intended to operate. In one embodiment, the communication module 704 is operable with both voice and data communications. Regardless of the particular design, however, signals received by antenna 706 through BS 114 are provided to receiver 708, which may perform such common receiver functions as signal amplification, frequency down conversion, filtering, channel selection, analog-to-digital (A/D) conversion, and the like. Similarly, signals to be transmitted are processed, including modulation and encoding, for example, by DSP 712, and provided to transmitter 714 for digital-to-analog (D/A) conversion, frequency up conversion, filtering, amplification and transmission over the air-radio interface via antenna 716.

[0036] Microprocessor 702 also interfaces with further device subsystems such as auxiliary input/output (I/O) 718, serial port 720, display 722, keyboard 724, speaker 726, microphone 728, random access memory (RAM) 730, a short-range communications subsystem 732, and any other device subsystems generally labeled as reference numeral 733. To control access, a Subscriber Identity Module (SIM) or Removable user Identity Module (RUIM) interface 734 is also provided in communication with the microprocessor 702. In one implementation, SIM/RUIM interface 734 is operable with a SIM/RUIM card having a number of key configurations 744 and other information 746 such as identification and subscriber-related data.

[0037] Operating system software and transport stack software may be embodied in a persistent storage module (i.e., non-volatile storage) such as Flash memory 735. In one implementation, Flash memory 735 may be segregated into different areas, e.g., storage area for computer programs 736 as well as data storage regions such as device state 737, address book 739, other personal information manager (PIM) data 741, and other data storage areas generally labeled as reference numeral 743. Additionally, a CC resource file structure 748 (e.g., along with a library) may be provided as part of the persistent storage for storing a carrier-specific CC map in accordance with the teachings of the present patent application for customization of the MCD's data session retry mechanism.

[0038] It is believed that the operation and construction of the embodiments of the present patent application will be apparent from the Detailed Description set forth above. While the exemplary embodiments shown and described may have been characterized as being preferred, it should be readily understood that various changes and modifications could be made therein without departing from the scope of the present invention as set forth in the following claims.

WHAT IS CLAIMED IS:

1. A method for customizing data session retry functionality associated with a mobile communications device (116), comprising:

detecting that a cause code (404) has been returned by a node (206, 208) disposed in a wireless packet data service network (112) operable with said mobile communications device (116);

interrogating a structure (400) to determine if said cause code (404) is mapped to a flag (406) relating to said mobile communications device's data session retry functionality; and

disabling said mobile communications device's data session retry functionality responsive to determining that said cause code (404) is mapped as a critical cause code in said structure (400).

2. The method for customizing data session retry functionality associated with a mobile communications device (116) as recited in claim 1, wherein said wireless packet data service network (112) comprises one of a General Packet Radio Service (GPRS) network, an Enhanced Data Rates for Global System for Mobile Communications (GSM) Evolution (EDGE) network, a 3rd Generation (3G) network, an Integrated Digital Enhanced Network (IDEN), and a Code Division Multiple Access (CDMA) network.

3. The method for customizing data session retry functionality associated with a mobile communications device (116) as recited in claim 1 or claim 2, wherein said cause code (404) is indicative of a condition selected from the group consisting of: a signaling load condition in said wireless packet data service network (112), an invalid Access Point Name (APN) with respect to said mobile communications device (116), an invalid Packet Data Protocol (PDP) address with respect to said mobile communications device (116), a user authentication failure with respect to said mobile communications device, and a rejection of activation by said wireless packet data service network (112).

4. The method for customizing data session retry functionality associated with a mobile communications device (116) as recited in claim 1, claim 2 or claim 3, wherein said structure (400) is provided as a firmware block having a configurable mapping database for a plurality of cause codes.

5. The method for customizing data session retry functionality associated with a mobile communications device (116) as recited in claim 4, wherein said configurable mapping database is configured on a carrier-by-carrier basis.

6. The method for customizing data session retry functionality associated with a mobile communications device (116) as recited in claim 4, wherein said configurable mapping database is configured on a mobile communications device-by-mobile communications device basis.

7. A wireless packet data service network (112), comprising:

- a serving node (206) operable to serve a mobile communications device (116) for establishing a data session with a public packet-switched network (108);

- a gateway node (208) disposed between said serving node (206) and said public packet-switched network (108);
- and

- a structure (400) having a database for mapping a cause code (404) generated by a node (206, 208) in said wireless packet data service network (112) to a flag (406) relating to said mobile communications device's data session retry functionality, said flag (406) for identifying said cause code (404) as a critical cause code operable to trigger disabling of said mobile communications device's data session retry functionality.

8. The wireless packet data service network (112) as recited in claim 7, wherein said cause code (404) is indicative of a condition selected from the group

consisting of: a signaling load condition in said wireless packet data service network (112), an invalid Access Point Name (APN) with respect to said mobile communications device (116), an invalid Packet Data Protocol (PDP) address with respect to said mobile communications device (116), a user authentication failure with respect to said mobile communications device, and a rejection of activation by said wireless packet data service network (112) a signaling load condition in said wireless packet data service network.

9. The wireless packet data service network (112) as recited in claim 7 or claim 8, wherein said structure (400) is provided as a firmware block having a configurable mapping database for a plurality of cause codes.

10. The wireless packet data service network (112) as recited in claim 9, wherein said configurable mapping database is configured on a carrier-by-carrier basis.

11. The wireless packet data service network (112) as recited in claim 9, wherein said configurable mapping database is configured on a mobile communications device-by-mobile communications device basis.