(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 October 2017 (19.10.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/180512 A1

(51) International Patent Classification:
G06F 17/30 (2006.01) *G04R 20/14* (2013.01)
G06F 21/50 (2013.01)

(21) International Application Number:
PCT/US2017/026799

(22) International Filing Date:
10 April 2017 (10.04.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/320,627 11 April 2016 (11.04.2016) US

(71) Applicant: **TATA COMMUNICATIONS (AMERICA) INC.** [US/US]; 2355 Dulles Corner Blvd., Suite 700, Herndon, Virginia 20171 (US).

(72) Inventors: **MIRANDA, Carlos**; c/o Tata Communications (America) Inc., 2355 Dulles Corner Boulevard, 7th Floor, Herndon, Virginia 20171 (US). **ARORA, Manish**; c/o Tata Communications (America) Inc., 2355 Dulles Corner Boulevard, 7th Floor, Herndon, Virginia 20171 (US). **THIRUMALAIAPPAN, Kumar**; c/o Tata Communications (America) Inc., 2355 Dulles Corner Boulevard, 7th Floor, Herndon, Virginia 20171 (US). **DOWD, Brian**; c/o Tata Communications (America) Inc., 2355 Dulles Corner Boulevard, 7th Floor, Herndon, Virginia 20171 (US).

(74) Agent: **ENATSKY, Aaron**; Hubbs, Enatsky & Inoue PLLC, 1765 Greensboro Station Place, 9th Floor, McLean, Virginia 22102 (US).

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

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

Published:

— *with international search report (Art. 21(3))*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR REAL TIME FRAUD ANALYSIS OF COMMUNICATIONS DATA

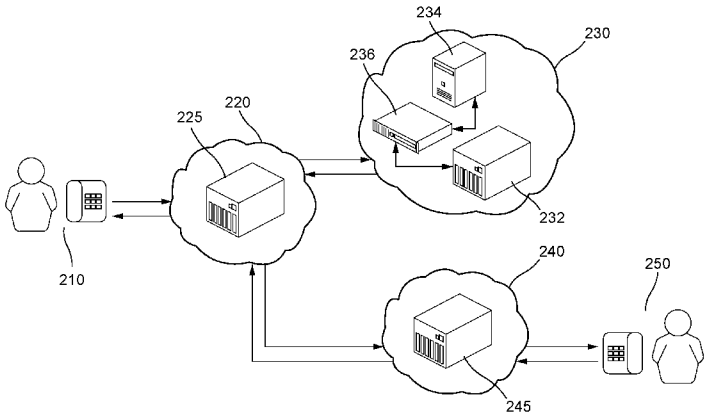


FIG. 2

(57) Abstract: A telecommunications service provider's real time analysis system analyzes communications data to detect potentially fraudulent communications data, where the analysis is performed in real time in the routing path of the communications data. The communications data may include calls (*e.g.*, SS7, VoIP, etc. based calls) and messages (*e.g.*, SMS, MMS, etc.). The real time analysis system rejects potentially fraudulent communications data and non-fraudulent communications data in order to be used in real time in the routing path of the communications data. A rejection by the real time analysis system may cause non-fraudulent communications data to still be sent to the intended destination of the communications data. The real time analysis system can be in the routing path of the communications data without further routing non-fraudulent communications data traffic to the next appropriate hop in the routing path.

WO 2017/180512 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

SYSTEM AND METHOD FOR REAL TIME FRAUD ANALYSIS OF COMMUNICATIONS DATA

FIELD OF THE INVENTION

[0001] This application claims priority to U.S. Provisional Application No. 62/320,627, filed on April 11, 2016, the contents of which are hereby incorporated by reference.

SUMMARY OF THE INVENTION

[0002] In accordance with the present disclosure, a real time analysis system analyzes communications data to detect and block fraudulent communications. The real time analysis system may automatically block fraudulent communication data and non-fraudulent communications data in real time. For example, the real time analysis system may automatically generate and transmit blocking messages for fraudulent communications and non-fraudulent communications during a communications initiation or set up process.

[0003] In accordance with one embodiment, the real time analysis system analyzes calls for fraud in real time. A telecommunications service provider's real time analysis system analyzes call termination requests and detects potentially fraudulent calls. The real time analysis system may automatically block potentially fraudulent calls and non-fraudulent calls in real time. For example, the real time analysis system may automatically block potentially fraudulent calls and non-fraudulent calls during a call initiation or set up process.

[0004] In one embodiment, the real time analysis system enables efficient correction of false positives. A false positive is a call that was incorrectly identified as potentially fraudulent and blocked, but in reality should not have been blocked. The real time analysis system enables false positives to be identified and corrected such that the real time analysis system does not continue to inappropriately block such a call in the future, as well as calls with similar attributes in the future.

[0005] In one embodiment, the telecommunications service provider's network and equipment is not within the natural call termination path for an analyzed call (*e.g.*, the telecommunications service provider's network and equipment would not normally be used to route a call to its final destination). The telecommunications service provider's network and equipment associated with the real time analysis system is configured to send a "reject call" message back to a telecommunication network that originally routed the call to the real time analysis system for analysis when the real time analysis system determines that the call should be blocked. In another such embodiment, if the real time analysis system determines that the analyzed call should not be blocked (*i.e.*, should be allowed to be terminated to the intended destination), the telecommunications service provider's network and equipment associated with the real time analysis system is configured to send a "reject call" message back to a telecommunication network that originally routed the call to the real time analysis system for analysis. In other words, in one such embodiment, the telecommunications service provider's network and equipment associated with the real time analysis system is configured to send a "reject call" message regardless of whether or not the call should be blocked.

[0006] In accordance with one embodiment, the call analysis system detects potentially fraudulent calls based upon one or more factors. Some of the factors include unallocated numbers, invalid number ranges, known fraudulent A-numbers, known fraudulent B-numbers, highly repeated A-numbers, highly repeated B-numbers, high cost destinations, European out-of-region surcharge calls, customer-specific requirements, etc.

[0007] While in one embodiment, the real time analysis system can be implemented in a telecommunications network (PSTN or VoIP), the invention is applicable to call analysis in any network over which calls are routed.

[0008] It should also be appreciated that the real time analysis system for communications data is not limited to call analysis. For example, the real time analysis system can be applied to other forms of communications, such as messaging or any other suitable form of communications. Certain messaging embodiments are described in more detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The following drawings illustrate examples of various components of the invention disclosed herein, and are for illustrative purposes only.

[0010] Fig. 1 is a diagrammatic view of one embodiment of a network system adapted to analyze communication data in real time.

[0011] Fig 2. is a diagrammatic view of one embodiment of a network system adapted to analyze communication data in real time.

[0012] Fig. 3 is a diagrammatic view of a call signaling flow of one embodiment of a network system that rejects a call while still allowing the call to be completed to its intended destination.

[0013] Fig. 4 is a diagrammatic view of a call signaling flow of one embodiment of a network system that rejects a call and blocks the call from being completed to its intended destination.

[0014] Fig. 5 is a diagrammatic view of a message signaling flow of one embodiment of a network system that rejects a message while still allowing the message to be sent to its intended destination.

[0015] Fig. 6 is a diagrammatic view of a message signaling flow of one embodiment of a network system that rejects a message and blocks the message from being sent to its intended destination.

[0016] Fig. 7 is a diagram of example components of computing devices of a network system adapted to analyze communications data in real time.

DETAILED DESCRIPTION OF THE INVENTION

[0017] The fields of Internet based communication and telephony have proven to be a viable technology and are evolving at an ever-increasing rate. It is now common to use any type of end point such as a telephone terminal, handset, cell phone, computer, smart phone, etc. to initiate or receive a voice call either over the traditional public switched telephone network (PSTN) or the Internet using Voice over Internet Protocol (VoIP). A call may be "terminated" (*i.e.*, completed to an appropriate destination, in telephony parlance) by connecting one end point to either the Internet or PSTN, which in turn accesses at least one or more gateways to ultimately terminate the call to another endpoint. The terminated call may travel through the PSTN, the Internet, and even over private networks (or any combination of the foregoing) to reach the call's ultimate destination. The end points and networks may also be frequently used for exchanging asynchronous communications, such as messaging.

[0018] The PSTN is a circuit switched network. That is, the PSTN assigns a dedicated communication line or resource to a user with which to complete the telephone call, and the user can utilize the assigned resource of the PSTN in any chosen manner. It is understood that the user is paying for the use of the dedicated resource of the PSTN. While the circuit switched

approach of the PSTN system is not necessarily the most efficient system in terms of call traffic, it is relatively easy to ensure that information destined for a particular user is delivered.

[0019] The Internet is a packet switched network in which communication is accomplished by breaking transmitted data into "packets" and interleaving the packets to best utilize the bandwidth available at any given time on the Internet. When the packets reach their intended destination, they must be reassembled into the originally transmitted data. Loss of packets, and thus data, occurs frequently in such a network, and the ability of the network to successfully transmit information from one point in the network to another determines the quality of the network.

[0020] A system of gateways located at various endpoints on the Internet can facilitate VoIP telephony by permitting the gateways to act as protocol bridges between the PSTN and the Internet. A VoIP service provider may operate a VoIP network which can route/terminate a VoIP call that traverses both PSTN networks and packet switched networks like the Internet. The originator of a call may use a standard telephone connected to a first PSTN to dial a telephone number of another person on a second PSTN. A trunk line of the first PSTN connects to an originator gateway (telephony switch or server) that connects the first PSTN to a packet switched network, such as the Internet. The initiator gateway may send its position in the network along with the telephone number of the call recipient (within the second PSTN) to a route server, which determines which of many other gateways should be used to complete the call to the telephone number in the second PSTN and transmits this information to the initiator gateway. A call connection is then established between the originator gateway and a terminator gateway serving the second PSTN, which may involve routing the call through several intermediate servers on the Internet. The terminator gateway completes the call to the called party by connecting to the second PSTN.

[0021] The connection of a call between users on PSTNs is just provided as an example. Those skilled in the art will appreciate that the users need not necessarily communicate via a PSTN. In general, a call will be considered as originating with a caller of one telephony service provider and being destined to a call recipient (regardless of the type of connection to the customer or the recipient).

[0022] The telephony service provider typically generates revenue, at least in part, by buying and reselling call completion services (also known as termination services). That is, when an originator gateway in the United States, for example, needs to complete a call to Luxembourg, for example, the originator gateway will send that call through a particular terminating gateway that can terminate the call to an end point at the final destination in Luxembourg. The telephony

service provider associated with the originating gateway will pay the terminating gateway operator a fee, for example, fifty cents per minute, for such termination services. In one embodiment, if a VoIP service provider provides call termination services to the originating gateway (*e.g.*, sits in the call path between originating service provider and the termination service provider and routes the call to the terminating gateway in Luxembourg), the VoIP service provider may charge the originating service provider (associated with the originator gateway) fifty-five cents per minute for such termination services to Luxembourg. The five-cent difference in this example is the VoIP service provider's profit.

[0023] Further details of techniques used in furtherance of the foregoing are described in commonly owned U.S. Pat. No. 6,404,864, ("the '864 patent") assigned to the same assignee as the present application. The disclosure of the '864 patent is hereby incorporated by reference in its entirety. Other suitable mechanisms may be used to route and terminate calls over the PSTN and the Internet.

[0024] The above business model is viable in large part due to the fact that the various carriers that operate around the world often do not have individual contractual relationships with each other. Without such relationships, it is difficult to terminate calls to every location in the world. A VoIP service provider may perform, in a loose sense, a matching service that matches those seeking to send calls to specific destinations, with those seeking to earn money by terminating (completing) such calls in those destinations. The contractual relationships required however, are typically between the various carriers that operate the originating and terminating gateways, and the VoIP service provider.

[0025] Take for example, a VoIP service provider contracts for termination services with a particular terminating gateway operator. An operator of an originating gateway also contracts with the VoIP service provider to send/terminate call traffic to appropriate destinations for the operator of the originating gateway. If the originating gateway sends the VoIP service provider a call to terminate with the terminating gateway, but the operator of the originating gateway does not pay the VoIP service provider for such call termination services, the VoIP service provider will still be contractually bound to pay the terminating gateway operator for terminating the call. This potentially results in a loss of revenue for the VoIP service provider. This often happens in the case of fraud or hacking. For example, if someone hacks into the local network connected to an originating gateway, the hacker can cause the originating gateway to send fraudulent calls to the VoIP service provider. The VoIP service provider may send the fraudulent calls to a terminating gateway operator to terminate (*e.g.*, complete) the fraudulent calls. The operator of the originating gateway may not pay for those calls, while the

VoIP service provider may have contracted with the terminating gateway operator to pay for calls that the terminating gateway operator terminates to a destination (including fraudulent calls). Hence, a loss of revenue to the VoIP service provider may result.

[0026] Further, an originating gateway operator may be a small carrier without a sophisticated security system. It is thus often possible for a malicious source to breach a system and relay malicious traffic to the VoIP service provider, which appears to be legitimate customer traffic, without the customer (*i.e.*, the originating gateway operator) even being aware. The VoIP service provider is ultimately responsible to remunerate the downstream service providers, and often the defrauded customer is too small to assume the financial losses, or is not contractually or legally responsible. It should be appreciated that the VoIP service provider could be any suitable telecommunication service provider that routes or terminates calls.

[0027] One more serious problem is that the fraudulent traffic may not be discovered until days or weeks later, when call detail records ("CDR") show an unusually high amount of traffic and unusually high charges to a specific destination, for example. Another problem is that the fraud that results in loss to the VoIP service provider is often fraud committed against one of the carriers' networks, not directly against the VoIP service provider. Hence, it is difficult for the VoIP service provider to manage the fraud, even though the resulting loss may largely be borne by the VoIP service provider.

[0028] The VoIP service provider must play a delicate balancing act between catching enough fraudulent call traffic and allowing legitimate call traffic to be terminated. For example, allowing legitimate traffic from to flow between customers and destinations even when the call volume increases. And even being exposed to significant financial losses if the VoIP service provider does not properly and quickly react to situations that do, in fact, involve fraudulent traffic from trusted customers.

[0029] The VoIP service provider may also desire to sell real time fraud monitoring service to other telecom carriers without terminating a call for such other carriers. The VoIP service provider may also desire to sell a real time fraud monitoring services to other telecom carriers by utilizing existing telecommunications infrastructure equipment.

[0030] Fig. 1 is a diagrammatic view of one embodiment of a network system adapted to perform real time analysis of voice calls and to minimize fraudulent calls.

[0031] End point 10 is a device that enables a user to transmit and receive data, such as making and receiving telephone calls. End point 10 may include a telephone terminal, handset, cell phone, computer, smart phone, etc. Other suitable devices are described below. End point 10 is in communication with at least carrier network 15. Carrier network 15 may be a PSTN or an

IP network that enables end point 10 to make and receive calls. Carrier network 15 includes at least one network element 20 that can transmit and receive telephone calls from devices such as end point 10 and other network elements (from within the carrier network 15 or outside of carrier network 15). In some embodiments, carrier network 15 may include any number of network elements necessary to operate a carrier network. Network element 20 may be a telephony switch or telephony gateway or other suitable network device or server (as is further described below). Network element 20 may be configured to transmit and receive telephone calls over either the PSTN or an IP network (*e.g.,* for VoIP calls), or both. As shown in Fig. 1, carrier network 15 may be in communication with many other networks such as carrier network 25, carrier network 65, network 45, and carrier network 50. It should be appreciated that carrier network 15 may communicate with any suitable number of other networks and devices.

[0032] In one embodiment, carrier network 25 includes several network elements. Carrier network 25 includes at least one network element 30 that can transmit and receive telephone calls. In some embodiments, carrier network 25 may include any number of network elements necessary to operate a carrier network. Network element 30 may be a telephony switch or telephony gateway or other suitable network device or server (as is further described below). Network element 30 may be configured to transmit and receive telephone calls over either the PSTN (*e.g.,* for TDM calls) or an IP network (*e.g.,* for VoIP calls), or both. Network element 30 may include an SMS or MMS server or other messaging service that permits end points (*e.g.,* 10, 60, 62, 75) to communicate with asynchronous communications. Network element 30 may be a stand alone messaging server. Where multiple network elements 30 are present in carrier network 15, network elements 30 may be any suitable combinations of telephony or messaging switches, gateways, servers, etc. As shown in Fig. 1, carrier network 25 may be in communication with many other networks such as carrier network 15, carrier network 50, and network 45. It should be appreciated that carrier network 25 may communicate with any suitable number of other networks and devices. While not shown, carrier network 25 may be configured to communicate with any number of end points (*e.g.,* to receive or terminal calls to these end points).

[0033] In one embodiment carrier network 25 further includes a routing system. The routing system may include specially programmed servers or network elements such as network element 35 and network element 40. The specially programmed network elements 35 and 40 may perform operations such as network policy and routing management. Network elements 35 and 40 may perform decision analysis for network policy and route management such as toll-free routing, least-cost routing, number portability, voice VPN, SIP trunking, centralized

dial plans, emergency services, etc. In some embodiments (not shown), the routing system may divide the work of network policy and route management over more than two network elements. Alternatively, in some embodiments (not shown), the routing system may rely on one network element to perform such operations.

[0034] In one embodiment, network 45 may be a PSTN network. In an alternative embodiment, network 45 may be an IP network such as the Internet. As shown in Fig. 1, network 45 is in communication with carrier network 15, carrier network 25, carrier network 50. However, it should be appreciated that network 45 may be in communication with any suitable number of networks.

[0035] Carrier network 50 may be a PSTN or an IP network that enables end points to make and receive calls. Carrier network 50 includes at least one network element 55 that can transmit and receive telephone calls from end points and other network elements (from within the carrier network 50 or outside of carrier network 50). In some embodiments, carrier network 50 may include any number of network elements necessary to operate a carrier network. Network element 55 may be a telephony switch or telephony gateway or other suitable network device or server (as is further described below). Network element 55 may be configured to transmit and receive telephone calls over either the PSTN (*e.g.,* for TDM calls) or an IP network (*e.g.,* for VoIP calls), or both. As shown in Fig. 1, carrier network 50 may be in communication with many other networks such as carrier network 25, and network 45. It should be appreciated that carrier network 50 may communicate with any suitable number of other networks and devices. As shown in Fig. 1, carrier network 50 is in communication with at least end point 60 and end point 62. End points 60 and 62 are devices that enables a user to transmit and receive data, such as making and receiving telephone calls. End points 60 and 62 may include a telephone terminal, handset, cell phone, computer, smart phone, etc. Other suitable devices are described below for end points 60 and 62.

[0036] Carrier network 65 may be a PSTN or an IP network that enables end points to make and receive calls. Carrier network 65 includes at least one network element 70 that can transmit and receive telephone calls from end points and other network elements (from within the carrier network 65 or outside of carrier network 65). In some embodiments, carrier network 65 may include any number of network elements necessary to operate a carrier network. Network element 70 may be a telephony switch or telephony gateway or other suitable network device or server (as is further described below). Network element 70 may be configured to transmit and receive telephone calls over either the PSTN (*e.g.,* for TDM calls) or an IP network (*e.g.,* for VoIP calls), or both. As shown in Fig. 1, carrier network 65 may be in communication with

many other networks such as carrier network 15. It should be appreciated that carrier network 65 may communicate with any suitable number of other networks and devices. As shown in Fig. 1, carrier network 65 is in communication with at least end point 75. End point 75 is a device that enables a user to transmit and receive data, such as making and receiving telephone calls. End point 75 may include a telephone terminal, handset, cell phone, computer, smart phone, etc. Other suitable devices are described below for end point 75.

[0037] One embodiment of an operation of the real time analysis system is disclosed below. End point 60 makes a call to end point 10. In this embodiment, end point 60 is in communication with carrier network 50. Thus, carrier network 50 handles the call from end point 60. The call may be handled by network element 55. As part of the call setup request, network element 55 receives at least end point 60's information (*e.g.,* an A-number) as well as the end point 10 or the called party's number (*e.g.,* a B-number). In one embodiment, network element 55 is a telephony switch that determines that end point 60 is attempting to place a call to end point 10. In an alternative embodiment, network element 55 works with other network elements in carrier network 50 to determine how and where to route the call to end point 10. Based on the B-number associated with end point 10, network element 55 determines that the best path for the call is through network 45 to carrier network 15 (where end point 10 is located). Network element 55 routes the call through network 45 and terminates the call with carrier network 15. Network element 20 may handle incoming calls from network 45. Network element 20 may determine where to next route the call to reach end point 10. In one such embodiment using the real time analysis system, network element 20 determines that carrier network 25 should receive the call.

[0038] In one embodiment network element 20 does not realize that carrier network 25 is not in the typical call termination path and may only be in the call termination path for fraud analysis. That is, in one such embodiment, carrier network 25 is not used to actually route the call to a different carrier network for termination. In one embodiment, carrier network 25 will always send the call back to carrier network 15 for termination whether to an end point on the network of carrier network 15 or to another carrier network. In one embodiment, network element 30 receives the call for carrier network 25. In one embodiment, where network element 30 relies on a routing system (*e.g.,* network elements 35 and 40) to make determinations about how to route a call, network element 30 may route the call to network element 35 for processing. Network element 35 may analyze the call and determine that the call was routed from carrier network 15. Network element 35 may be configured to further route the call to network element 40 for further analysis.

[0039] In one embodiment, network element 40 may be specially programmed or configured to store and maintain a blacklist of known problematic attributes associated with a phone call. For example, the blacklist may cause network element to analyze the call to determine if the phone number (*e.g.,* the A-number) associated with end point 60 is an unallocated number, from invalid number ranges, known fraudulent A-numbers, highly repeated A-numbers, high cost destinations, European out-of-region surcharge area, customer-specific requirements, etc. Any single one of these factors may be used alone in any suitable combination to determine potential fraud.

[0040] Similarly, network element 40 may be specially programed or configured to use its blacklist to analyze the phone number (*e.g.,* the B-number) associated with the destination of end point 10 for similar problems. For example, the blacklist may cause network element 40 to analyze the call to determine if the phone number (*e.g.,* the B-number) associated with end point 10 is an unallocated number, an invalid number range, known fraudulent B-numbers, highly repeated B-numbers, high cost destinations, European out-of-region surcharge, customer-specific requirements, etc. Any single one of these factors may be used alone in any suitable combination to determine potential fraud.

[0041] In one embodiment, if network element 40 analyzes the call and at least one call attribute can be matched against the blacklist, the network element 40 flags the call as a potentially fraudulent call. For example, if the calling party (end point 60) is calling from a high cost destination, network element 40 flags the call as a potentially fraudulent call. In one embodiment, after network element 40 flags the call as potentially fraudulent, network element 40 further analyzes the call and the call attributes against a stored and maintained whitelist. If network element 40 determines that nothing stored in the whitelist provides a reason to remove the flag on the call from end point 60, network element 40 determines that the call from end point 60 should be blocked. Network element 40 may transmit a rejection message to network element 35. Network element 35 may transmit the rejection message to network element 30. Network element 30 may generate and transmit a rejection message to network element 20 of carrier network 15. The rejection message may be in the form of a standard Session Initiation Protocol (SIP) rejection message used between telephony switches. The SIP message may be in a predefined format that carrier network 15 and carrier network 25 agreed upon to indicate that a fraudulent call was suspected. It should be appreciated that the SIP rejection message may be in a form that would not normally convey to the recipient telephony switch that the call was rejected for suspected fraud. It should also be appreciated that the rejection message may be in the form of rejection “cause codes” for ITU or SS7 compliant systems. In either case, if

network element 20 received a rejection message from network element 30 where the rejection message typically indicated that the B-number associated with the call could not be found, carrier network 15 may determine that such a rejection message from network element 30 means that carrier network 25 rejected the call due to suspected fraud. Upon receiving such a rejection from carrier network 25, carrier network 15 may block the call and send a message back to carrier network 50 indicating that the call could not be completed.

[0042] In one embodiment, carrier network 15 may determine that calls from end point 60 destined for end point 10 are not fraudulent. For example, end point 60 may be associated with a satellite office of a company associated with end point 10. Thus, despite the concern about the call from end point 60 originating from a high cost destination, the call should be completed. Carrier network 15 may transmit a message to network element 40 (or the network element performing the real time analysis in carrier network 25) to indicate that the whitelist should include an entry for calls originating from end point 60 and destined for end point 10 and should not be flagged as fraudulent. In one embodiment, if carrier network 15 provided a reason why network element 40 should include end point 60 on the whitelist, network element 40 may modify the whitelist to add additional entries based on applying a similar rational to other similar calls. For example, network element 40 may identify that the phone number associated with end point 60 is associated with a block of phone numbers assigned to the same company. Thus, network element 40 may update its whitelist automatically such that calls from the identified block of phone numbers destined for end point 10 should not be blocked in the future. It should be appreciated if network element 40 is provided reasons for modifying the whitelist, network element 40 may be configured to apply these reasons to other calls to prevent other future calls from being improperly blocked. These improperly blocked calls are considered false positives.

[0043] In another embodiment, network element 40 may not receive any reason why end point 60 should be included on the whitelist. Carrier network 15 may transmit a message to network element 40 (or the network element performing the real time analysis in carrier network 25) to indicate that the call originating from end point 60 and destined for end point 10 should not have been flagged as fraudulent. In one embodiment, network element 40 may store the message from carrier network 15, but not take further action. If another end point 62 on carrier network 50 attempts to call end point 10, network element 40 may again determine that such a call should be flagged as fraudulent and blocked for the same or similar reasons as the call from end point 60 to end point 10 was blocked. Carrier network 15 may transmit a message to network element 40 to indicate that that the call originating from end point 62 and destined for

end point 10 should not have been flagged as fraudulent. In one embodiment, network element 40 may store the message from carrier network 15, but not take further action.

[0044] In one embodiment, based on receiving messages indicating that calls from end points 60 and 62 to end point 10 were not fraudulent, network element 40 may compare attributes between the calls from end point 60 and 62 to determine if there is a common attribute that is a subset of the blacklist attribute associated with the first call (the call from end point 60) and the second call (the call from end point 62). For example, if the blacklist attribute associated with the calls from end points 60 and 62 is that both calls originate from a high cost destination (determined by examining, for instance, the country code associated with phone numbers of both end points), network element 40 may examine other common subset attributes associated with both phone numbers.

[0045] In one embodiment, network element 40 may determine that both phone numbers associated with end points 60 and 62 are from the same area code (*e.g.,* where phone numbers include a country code + an area code + a line number). As the area code is a subset of the county code in an example phone number, network element 40 may determine that the shared subset attribute of the area code combined with the message indicating that such calls should not be flagged means that calls from end points 60 and 62 to end point 10 should not be blocked. In one embodiment, network element 40 may update the whitelist to permit calls from end points 60 and 62 to end point 10 to be completed.

[0046] In another embodiment, network element 40 may determine that calls from the same area code shared by end points 60 and 62 should be added to the whitelist as a result of receiving a message that both calls should not be flagged as fraudulent (*e.g.,* calls from the same country code and area code). In some embodiments, a network element 40 must receive a certain threshold quantity of messages indicating that calls should not be flagged where such calls also have at least one common attribute or subset attribute before network element 40 updates the whitelist to permit such calls.

[0047] It should be appreciated that any attribute commonality may be used to determine what additional whitelist changes to make to avoid improperly flagging calls in the future. For example, in another embodiment, network element 40 may determine that both phone numbers associated with end points 60 and 62 are assigned to a company that is named the same or similar to the company assigned the phone number associated with end point 10. In another embodiment, network element 40 may determine that both phone numbers associated with end points 60 and 62 are from the same block of numbers (*e.g.,* the last 4 digits or some other

suitable number of n digits of both phone numbers are from the block of phone numbers assigned to a single company).

[0048] Continuing the above example, where network element 40 has modified its whitelist to remove the flag on calls from end point 60 to end point 10. In one such embodiment, end point 60 attempts to call end point 10 again. The call is routed in the same manner as described above. However, once network element 40 determines that an entry in the whitelist provides a reason to remove the flag on the call from end point 60, network element 40 determines that the call from end point 60 should be allowed. As with the scenario where the call was flagged as potentially fraudulent, network element 40 may again transmit a rejection message to network element 35. Network element 35 may transmit the rejection message to network element 30. Network element 30 may generate and transmit a rejection message to network element 20 of carrier network 15. The rejection message may be in the form of a standard Session Initiation Protocol (SIP) rejection message used between telephony switches. However, in this embodiment, the SIP rejection message may be in a predefined format that carrier network 15 and carrier network 25 agreed upon to indicate that the call is a normal call and should not be blocked. It should be appreciated that the SIP rejection message may be in a form that would not normally convey to the recipient telephony switch that the call is normal and should be allowed. It should also be appreciated that the rejection message may be in the form of rejection "cause codes" for ITU or SS7 compliant systems. In either case, in one embodiment, if network element 20 received a rejection message from network element 30 where the rejection message indicated that the call was rejected because no circuits were available or the service was unavailable, carrier network 15 may determine that such a rejection message from network element 30 actually means that carrier network 25 determined that the call should be allowed to proceed/terminated to the intended destination. Upon receiving such a rejection from carrier network 25, carrier network 20 may terminate/route the call to the intended destination of end point 10. Thus, end point 60 and end point 10 would be allowed to hold a voice call.

[0049] It should be appreciated that when calls are routed to the real time analysis system for analysis, in one embodiment, all such calls result in a rejection of the call by the carrier network associated with the real time analysis system regardless of whether the call should be completed or the call is flagged as potentially fraudulent. Whereas, in a typical call routing scenario, if a carrier network is in a call path, the carrier network would normally attempt to route/terminate a call. By utilizing the rejection messages (rejection "cause codes" for ITU or SS7 compliant system or SIP rejections for IP based networks) for both normal and suspected fraudulent calls, the real time analysis system is specially programmed or configured to interact with standard

telephony equipment and can be inserted into any call path for analysis without requiring the real time analysis system to actually route the call to completion (and incur call termination/completion costs). This is advantageous for a telephony carrier network (*e.g.*, carrier network 15, 50, 65, etc.) that wishes to use the real time analysis of another party, but does not wish to use the other carrier network associated with the real time analysis system (*e.g.*, carrier network 25) to terminate/complete calls. This is also advantageous to the carrier network associated with the real time analysis system because the such a carrier network can provide a new service without requiring customers to incur extra expenses to interoperate with a previously unavailable real time analysis system.

[0050] Similar to the embodiments described above, in another example embodiment, carrier network 15 may utilize the real time analysis system of carrier network 25 to analyze whether to complete calls coming from carrier network 65 (such as from end point 75) to end point 60 (or some other destination on carrier network 50). The same blacklist and whitelist analysis could be performed for the call. Carrier network 25 may issue the same call rejection messages to carrier network 15 (which may indicate either that carrier network 15 should terminate the call or block the call) regardless of whether carrier network 25 will route or terminate the call to carrier network 50 for carrier network 15 (which carrier network 25 could if requested, as shown in Fig. 1). It should be appreciated that carrier network 50, 65, and any other communications provider (not shown) may use the real time analysis system.

[0051] It should be appreciated that a carrier network providing the real time analysis system may also route/terminate calls that have been analyzed by the real time analysis system. In one such embodiment, the system to reject all calls transmitted to carrier network 25 for real time fraud is still employed. Once carrier network 25 provides the appropriate rejection notice as discussed above, then the carrier network receiving the rejection may decide to send the analyzed call back to carrier network 25 for termination. It should also be appreciated that the above analysis can be applied to other forms of electronic communication, such as, but not limited to the messaging scenarios discussed herein.

[0052] Fig 2. is a diagrammatic view of one embodiment of a network system adapted to analyze communication data in real time.

[0053] End point 210 is a device that enables a user to transmit and receive communications data, such as making and receiving telephone calls, sending and receiving messages, holding interactive multimedia conference calls, or some combination of the forgoing. End point 210 may include a telephone terminal, handset, cell phone, computer, smart phone, etc. Other suitable devices are described below. End point 210 is in communication with at least carrier

network 220. Carrier network 220 may be a PSTN or an IP network that enables end point 210 to make and receive calls, send and receive messages, or other forms of communication. Carrier network 220 includes at least one network element 225 that can transmit and receive communications from devices such as end point 210 and other network elements (from within the carrier network 220 or outside of carrier network 220). In some embodiments, carrier network 220 may include any number of network elements necessary to operate a carrier network. Network element 225 may be a telephony switch or telephony gateway or other suitable network device or server (as is further described below). Network element 225 may be configured to transmit and receive telephone calls or messages (*e.g.,* short message service (SMS), multimedia messaging service (MMS) messages) over either the PSTN or an IP network, or both. As shown in Fig. 2, carrier network 220 may be in communication with many other networks such as network 230 and network 240. It should be appreciated that carrier network 220 may communicate with any suitable number of other networks and devices.

[0054] In one embodiment, network 230 includes several network elements. Network 230 includes at least one network element 232 that can transmit and receive telephone calls. In some embodiments, network 230 may include any number of network elements 232 and other network elements necessary to operate a carrier network. Network element 232 may be a telephony switch or telephony gateway or other suitable network device or server (as is further described below). Network element 232 may be configured to transmit and receive telephone calls over either the PSTN (*e.g.,* for TDM calls) or an IP network (*e.g.,* for VoIP calls), or both. Network element 232 may include an SMS or MMS server or other messaging service that permits end points (*e.g.,* 210, 250, etc.) to communicate with synchronous or asynchronous communications. Network element 232 may be a stand-alone messaging server. Where multiple network elements 232 are present in network 230, network elements 232 may be any suitable combinations of telephony or messaging switches, gateways, servers, etc. As shown in Fig. 2, network 230 may be in communication with another network such as carrier network 220. It should be appreciated that network 230 may communicate with any suitable number of other networks and devices (not shown). While also not shown, network 230 may also be configured to communication with any number of end points (*e.g.,* to receive or terminate calls or send and receive messages to and from these end points).

[0055] In one embodiment carrier network 230 further includes a routing system. The routing system may include specially programmed servers or network elements such as network element 236 and network element 234. The specially programmed network elements 236 and 234 may perform operations such as network policy and routing management. Network

elements 236 and 234 may perform decision analysis for network policy and route management such as fraud monitoring/detection, voice call routing, toll-free routing, least-cost routing, number portability, voice VPN, SIP trunking, centralized dial plans, emergency services, SMS routing, MMS routing, etc. In some embodiments (not shown), the routing system may divide the work of network policy and route management over more than two network elements and operate in parallel or using parallel processing. Alternatively, in some embodiments (not shown), the routing system may rely on one network element to perform all such operations, depending on the scale required to handle incoming analysis requests.

[0056] Carrier network 240 may be a PSTN or an IP network that enables end points to make and receive calls, send and receive messages, or other forms of communication. Carrier network 240 includes at least one network element 245 that can transmit and receive telephone calls from end points and other network elements (from within the carrier network 50 or outside of carrier network 50). In some embodiments, carrier network 240 may include any number of network elements necessary to operate a carrier network. Network element 245 may be a telephony switch or telephony gateway or other suitable network device or server (as is further described below). Network element 245 may be configured to transmit and receive telephone calls or messages (*e.g.,* short message service (SMS), multimedia messaging service (MMS) messages) over either the PSTN or an IP network (*e.g.,* for VoIP calls), or both. As shown in Fig. 2, carrier network 240 may be in communication with other networks such as network 220. As shown in Fig. 2, carrier network 240 may be in communication with end points such as end point 250. End point 250 may be an end point such as described above in connection with end point 210. It should be appreciated that carrier network 240 may communicate with any suitable number of other networks and devices.

[0057] While not shown, networks 220, 230, 240 may be in communication via any suitable type of network such as a PSTN network or an IP network such as the Internet. It should also be appreciated that the limited number of networks and end points shown in Fig. 2 are merely to simplify illustration of how the real time analysis system works and in no way limit the quantity of networks and end points that can work with the real time analysis system. The number of networks and end points that can take advantage of the real time analysis system is limited only to the computing resources available relative to the quantity of specifically configured servers and connections devoted to the real time analysis.

[0058] Figs. 3-6 below are diagrammatic views of communication signaling flows of various embodiments of the network system for real time analysis of fraudulent communications based on the system illustrated in Fig. 2. It should be appreciated that the signaling flows of Fig. 3-6

may be applied to systems that differ from that illustrated in Fig. 2. It should also be appreciated that that although the call and message routing illustrated throughout this disclosure show only a limited number of hops and networks used to complete calls and other communications data transmissions between end points, it should be appreciated that additional hops, networks, etc. may be used between communicating end points, whether for calls or message transmissions.

[0059] Fig. 3 is a diagrammatic view of a call signaling flow of one embodiment of a network system that rejects a call while still allowing the call to be completed to its intended destination. A legitimate caller associated with end point 210 attempts to make a call to a callee associated with end point 250. To initiate the call, the end point 210 sends an IAM or an Invite message 310 to carrier network 220. The type of message depends on the type of network and equipment used by the callee at end point 210 and carrier network 220. The message 310 may be received at a network element 225 of carrier network 220. Upon receiving the message 310, carrier network 220 may be configured to send a message 320 (routing the call setup signaling) to network 230 (hereinafter referred to as the real time analysis system 230 or RTAS 230) for fraud detection processing by the RTAS 230. The RTAS 230 may send a message 330 to carrier network 220. The message 330 may include a trying message that indicates an acknowledgment of receipt of message 320.

[0060] Upon receipt of the message 320, the RTAS 230 may also perform real time analysis on the message 320, as discussed above, to determine whether or not fraud is detected in connection with the call from end point 210. In this embodiment, RTAS 230 determined that the call from end point 210 was not fraudulent (using the methods described above). Even though the RTAS 230 determined that the call from end point 210 was not fraudulent or associated with fraud, RTAS 230 sends a call rejection message 340 back to carrier network 220. The call rejection message 340 may be in the form of a 503 service unavailable message (for SIP based calls), a REL (34) message (for an SS7 based call), or some other suitable rejection message. Upon receiving the rejection message 340 from RTAS 230, carrier network 220 determines that the rejection message is associated with a determination that the call from end point 210 is not fraudulent and should be terminated (*e.g.,* completed) to the intended destination. Carrier network 220 determines the next appropriate hop or route to send the call from end point 210. In the embodiment illustrated in Fig. 3, carrier network 220 determines carrier network 240 is the destination network where end point 250 is located. Thus, carrier network 220 sends a call setup signaling message 350 to carrier network 240. The message 350 may include an IAM or Invite message. When carrier network 240 receives the message 350,

carrier network 240 may send message 360 to end point 250. The message 360 may include an IAM or Invite message.

[0061] The flow diagram of Fig. 3 does not show the remainder of the call setup signaling, media transmission between end point 210 and end point 250, and the call teardown. However, these aspects follow the standards used for SS7 and VoIP systems and should be apparent to one of ordinary skill in the art.

[0062] It should also be appreciated that the rejection message 340 from the RTAS 230 may prevent the call from being routed back to the RTAS 230 once the carrier network 220 determines that the rejection message 340 means the call should be completed. However, it should also be appreciated that in some alternative embodiments, the RTAS 230 may be used to route the call from end point 210 to the next appropriate hop in a call route to the end point 250. That is, after sending the rejection message 340, in some embodiments, carrier network 220 may route the call setup signaling back to RTAS 230 for termination/completion.

[0063] Fig. 4 is a diagrammatic view of a call signaling flow of one embodiment of a network system that rejects a call and blocks the call from being completed to its intended destination. An illegitimate caller associated with end point 210 attempts to make a call to a callee associated with end point 250. To initiate the call, the end point 210 sends an IAM or an Invite message 410 to carrier network 220. The type of message depends on the type of network and equipment used by the callee at end point 210 and carrier network 220. The message 410 may be received at a network element 225 of carrier network 220.

[0064] Upon receiving the message 410, carrier network 220 may be configured to send a message 420 (routing the call setup signaling) to RTAS 230 for fraud detection processing. The RTAS 230 may send a message 430 to carrier network 220. The message 430 may include a trying message that indicates an acknowledgment of receipt of message 420. Upon receipt of the message 420, the RTAS 230 may also perform real time analysis on the message 420, as discussed above, to determine whether or not fraud is detected in connection with the call from end point 210. In this embodiment, RTAS 230 determined that the call from end point 210 is fraudulent or potentially fraudulent (using the methods described above). Because the RTAS 230 determined that the call from end point 210 is fraudulent or associated with fraud, RTAS 230 sends a call rejection message 440 back to carrier network 220. The call rejection message 440 may be in the form of a 403 service unavailable message (for SIP based calls), a REL (21) message (for an SS7 based call), or some other suitable rejection message. Upon receiving the rejection message 440 from RTAS 230, carrier network 220 determines that the rejection message is actually associated with a determination that the call from end point 210 is

fraudulent and should be blocked. Carrier network 220 sends a message 450 back to end point 210 to end the call. The message 450 may be in the form of a 403 service unavailable message (for SIP based calls), a REL (21) message (for an SS7 based call), or some other suitable rejection message.

[0065] The flow diagram of Fig. 4 does not show all of the call setup and tear down signaling between end point 210 and end point 250. However, these aspects follow the standards used for SS7 and VoIP systems and should be apparent to one of ordinary skill in the art.

[0066] Fig. 5 is a diagrammatic view of a message signaling flow of one embodiment of a network system that rejects a message while still allowing the message to be sent to its intended destination. A legitimate message sender associated with end point 210 attempts to send a message to a recipient associated with end point 250. To initiate the message transmission, the end point 210 send a message 510 to carrier network 220. The type of message depends on the type of message, network, and equipment used by the callee at end point 210 and carrier network 220. The message 510 may be in the form of an SMS, MMS, or other suitable message. The message 510 may be received at a network element 225 of carrier network 220. Upon receiving the message 510, carrier network 220 may be configured to send a message 520 to RTAS 230 for fraud detection processing by the real time analysis system. The message 520 may include a Submit or Deliver SM message.

[0067] Upon receipt of the message 520, the RTAS 230 may perform real time analysis on the message 520, as discussed above (*e.g.*, apply an analysis of attributes associated with the message similar analyzing the attributes associated with a call), to determine whether or not fraud is detected in connection with the message from end point 210. In this embodiment, RTAS 230 determined that the message from end point 210 was not fraudulent (using the methods described above). Even though the RTAS 230 determined that the message from end point 210 was not fraudulent or associated with fraud, RTAS 230 send a rejection message 530 back to carrier network 220. The rejection message 530 may be in the form of a Resp Status: P_APPN (0x65) or some other suitable rejection message. Upon receiving the rejection message 530 from RTAS 230, carrier network 220 determines that the rejection message is actually associated with a determination that the message from end point 210 is not fraudulent and should be sent to the intended destination. Carrier network 220 determines the next appropriate hop or route to send the message from end point 210. In the embodiment illustrated in Fig. 5, carrier network 220 determines carrier network 240 is the destination network where end point 250 is located. Thus, carrier network 220 sends a message 540 to carrier network 240. The message 540 may include a Submit or Deliver SM message. When carrier network

240 receives the message 540, carrier network 240 may send message 550 to end point 250. The message 540 may include a Submit or Deliver SM message.

[0068] The flow diagram of Fig. 5 does not show all of the message transmissions between end point 210 and end point 250. However, these aspects follow the standards used for message transmission based on the type of messaging system used and should be apparent to one of ordinary skill in the art.

[0069] It should also be appreciated that the rejection message 530 from the RTAS 230 may prevent the message from being routed back to the RTAS 230 once the carrier network 220 determines that the rejection message 530 means the message should be completed. However, it should also be appreciated that in some alternative embodiments, the RTAS 230 may be used to route the message from end point 210 to the next appropriate hop in a message route to the end point 250. That is, after sending the rejection message 530, in some embodiments, carrier network 220 may route the message transmission back to RTAS 230 for further routing/completion.

[0070] Fig. 6 is a diagrammatic view of a message signaling flow of one embodiment of a network system that rejects a message and blocks the message from being sent to its intended destination. An illegitimate message sender associated with end point 210 attempts to send a message to a recipient associated with end point 250. To initiate the message transmission, the end point 210 sends a message 610 to carrier network 220. The type of message depends on the type of message, network, and equipment used by the callee at end point 210 and carrier network 220. The message 610 may be in the form of an SMS, MMS, or other suitable message. The message 610 may be received at a network element 225 of carrier network 220. Upon receiving the message 610, carrier network 220 may be configured to send a message 620 to RTAS 230 for fraud detection processing by the real time analysis system. The message 620 may include a Submit or Deliver SM message.

[0071] Upon receipt of the message 620, the RTAS 230 may perform real time analysis on the message 620, as discussed above, to determine whether or not fraud is detected in connection with the message from end point 210. In this embodiment, RTAS 230 determined that the message 620 from end point 210 is fraudulent (using the methods described above). Because the RTAS 230 determined that the message from end point 210 is fraudulent or associated with fraud, RTAS 230 sends a rejection message 630 back to carrier network 220. The rejection message 630 may be in the form of a Resp Status: P_APPN (0x66) or some other suitable rejection message. Upon receiving the rejection message 630 from RTAS 230, carrier network 220 determines that the rejection message is actually associated with a determination that the

message from end point 210 is fraudulent and should be blocked from being sent to the intended destination. Thus, carrier network 220 sends a rejection message 640 to end point 210. The rejection message 640 may be in the form of a Resp Status: P_APPN (0x66) or some other suitable rejection message.

[0072] The flow diagram of Fig. 6 does not show all of the message transmissions between end point 210 and the other network elements. However, these aspects follow the standards used for message transmission based on the type of messaging system used and should be apparent to one of ordinary skill in the art.

[0073] Using the architecture described herein to perform real time analysis on communication data transmissions results in technological improvements over existing systems for a cheaper, more efficient, and more secure system.

[0074] The above described real time analysis system (RTAS) architecture is cheaper than preexisting systems for several reasons. One reason is that the RTAS architecture saves network operators from high costs associated with paying for transmitting fraudulent communications data traffic. As noted above, network operators generally must pay other network operators to send communications traffic to networks and end points run by the other network operators. If fraudulent communications data traffic is sent to another network to reach the intended destination of the communications traffic, the sending network may be required to pay for the communications data traffic whether it was legitimate or not. Under preexisting systems, communications traffic was reviewed after the communications were already completed. Data identifying that particular communications traffic was fraudulent was not detected until weeks or months after the fraudulent communications traffic was sent to another network and the costs for the fraudulent traffic were already incurred. This is because it was not previously possible to analyze communications data traffic in real time before the communications traffic was provided to the intended destination. Preexisting systems to detect fraud in communications data traffic analyzed records created after communications data reached their intended destination. For example, when a call is made and completed, a call data record (CDR) is generated. Network operators would use the millions of CDR records to prepare invoices and audit billing/invoicing records. Analysis of the CDR records were also used to detect and determine whether call traffic was fraudulent. On the other hand, using the RTAS architecture enables the communications data traffic to be analyzed for fraud in real time before the communications data traffic is sent to its intended destination. The RTAS architecture prevents network operators from incurring costs associated with fraudulent communications data traffic by blocking the traffic before the communications data traffic is

sent to the intended destination. Blocking fraudulent communications traffic in real time also creates a more secure communications system.

[0075] Another reason that the RTAS architecture is cheaper and more efficient than preexisting systems is that network operators create less records of communications traffic. When communications data traffic is sent (and completed) to the intended destination, records of the communication are generated and stored. These records may be used, as noted above, for billing/invoicing and auditing purposes. When fraudulent traffic is blocked, less records of the communication data traffic are generated because there is less communications data traffic. Communications data results in extremely large quantities of records. By reducing the amount of records generated, less system server resources are used to create the records and less server and memory resources are used to store the records. Moreover, when the quantity of records are reduced, this also reduces the amount of analysis that must be performed on the generated records. A reduction in the amount of analysis required results in less processor and memory intensive operations. A reduction in the amount of analysis required also results fewer disputes with other network operators over fees owed for communications data traffic passed to the other network operators to handle.

[0076] Another reason that the RTAS architecture is cheaper and more efficient than preexisting systems is that less network resources are used when fraudulent communications data traffic is blocked in real time. For example, if a fraudulent communications data is sent to an intended destination, many different system resources are used on one or more networks to deliver the communication data. Many communication devices will be used to transmit the communications data, which requires unnecessary use of processors, memory, and power. Physical ports of the telecommunication devices and network bandwidth are also used to unnecessarily deliver the communications data. All of the above are generally limited resources. When these limited resources are heavily used, network operators are forced to add additional capacity in terms of additional communications devices and bandwidth. If the network operators do not add additional resources in a timely manner, the existing communication devices may drop portions of the communications data or cause the communication devices to even fail. The RTAS architecture prevents unnecessary use of limited resources and prevents the need to purchase additional resources to meet a false demand generated by fraudulent communications data traffic.

[0077] Yet another reason that the RTAS architecture is cheaper and more efficient than preexisting systems is that network operators using the RTAS system (or communications networks such as telephony carriers) do not need to purchase new hardware to use the RTAS

for fraud detection. The RTAS architecture discussed herein works with existing communications and telephony systems to leverage/recycle certain communications or telecom principals and processes for new purposes. The RTAS architecture allows the fraud detection to be placed in the path of a communications transmission and analyze the communications transmission for fraud before the communications transmission incurs substantial costs. Specifically, the RTAS architecture uses and repurposes rejection messages to communicate a determination of fraud or no fraud, whether or not a communications transmission is determined to be fraudulent.

[0078] Accordingly, using the RTAS architecture described herein to perform real time analysis on communication data transmissions results in technological improvements over existing systems for a cheaper, more efficient, and more secure system.

[0079] Fig. 7 is a diagram of example components of computing devices 700 which may be used to implement various computer devices of the network system adapted to analyze communications data in real time described herein. For example, computer devices 700 may be used to describe devices such as network elements 30, 35, 40 in carrier network 25 and network elements 232, 234, and 236 of RTAS 230 as well as other devices described herein.

[0080] Various computing devices may be used to implement the systems and methods described in this document, as either a client or as a server or plurality of servers. Computing devices are intended to represent various forms of digital computers, such as laptops, desktops, workstations, personal digital assistants, servers, blade servers, mainframes, and other appropriate computers. Other computing devices may include various forms of mobile devices, such as personal digital assistants, cellular telephones, smartphones, and other similar computing devices. The components shown here, their connections and relationships, and their functions, are meant to be examples only, and are not meant to limit embodiments of the inventions described and/or claimed in this document.

[0081] In one embodiment, a computing device used herein may include a specially configured processor 710, memory 720, a storage device 730, a high and low speed interfaces and buses 740 connecting to the memory. Each of the components of the computing devices are interconnected using various busses, and may be mounted on a common board or in other manners as appropriate. The processor can process instructions for execution within the computing device, including instructions stored in the memory or on the storage device to display graphical information for a graphic user interface on an external input/output device 850 such as a display. In other embodiments, multiple processors and/or multiple buses may be used, as appropriate, along with multiple memories and types of memory. Also, multiple

computing devices may be interconnected, with each device providing portions of the necessary operations (*e.g.*, as a server bank, a group of blade servers, or a multi-processor system).

[0082] The processor may be implemented as a chipset of chips that include separate and multiple analog and digital processors. Additionally, the processor may be implemented using any of several architectures. For example, the processor may be an x86 processor, RISC (Reduced Instruction Set Computers) processor. The processor may coordinate with the other components of the device, such as control of user interfaces, applications run by the device, and wireless communication. Multiple processors or processors with multiple cores may also be used.

[0083] The processor may communicate with a user through a control interface and display interface coupled to a display. The display may be, for example, an LED (Liquid Crystal Display) display, or other appropriate display technology. The display interface may comprise suitable circuitry for driving the display to present graphical and other information to a user. The control interface may receive commands from a user and convert them for submission to the processor. In addition, an external interface may be provided in communication with processor to enable near field communication with other devices. An external interface may provide, for example, for wireless and/or wired communication. Multiple interfaces may also be used.

[0084] The memory 720 may store information within the computing device. In one embodiment, the memory is a volatile memory unit or units. In another embodiment, the memory is a non-volatile memory unit or units. The memory may also be another form of computer-readable medium, such as a magnetic or optical disk.

[0085] The storage device 730 is capable of providing mass storage for the computing device. In one embodiment, the storage device may contain a computer-readable medium, such as a hard disk device, an optical disk device, or a tape device, a flash memory or other solid state memory device, or an array of devices, including devices in a storage area network or other configurations. The storage device may be anyone of the foregoing and be located remotely, such as in a cloud infrastructure. A computer program product can be tangibly embodied in an information carrier. The computer program product may also contain instructions that, when executed, perform one or more methods, such as those described above. The information carrier is a computer or machine readable medium, such as the memory 720, the storage device 730, or memory on processor 710.

[0086] The computing device may be implemented in several different forms. For example, it may be implemented as a standard server, or multiple times in a group of such servers. It may also be implemented as part of a rack server system. In addition, it may be implemented in a desktop computer or a laptop computer. Alternatively, components from the computing device may be combined with other components in a mobile device. Each of such devices may contain one or more computing devices. An entire system may be made up of multiple computing devices that communicate with each other and also may execute functions in a parallel processing environment.

[0087] The computing devices may communicate wirelessly through communication interfaces 760, which may include digital signal processing circuitry. Communication interfaces may provide for communications under various modes or protocols, such as GSM, SMS, MMS, CDMA, among others. Such communication may occur, for example, through a radio-frequency transceiver. In addition, short-range communication may occur, such as using a Bluetooth, Wi-Fi, or other such transceiver. A GPS (Global Positioning System) receiver module may provide additional navigation and location related wireless data to the computing devices.

[0088] The computing devices may communicate audibly using an audio codec, which may receive spoken information from a user and convert it to usable digital information. The audio codec may likewise generate audible sound for a user, such as through a speaker. Such sound may include sound from voice telephone calls and may include recorded sound.

[0089] Various embodiments of the systems and techniques described here can be realized in digital electronic circuitry, integrated circuitry, specially designed ASICs (application specific integrated circuits), computer hardware, firmware, and combinations thereof. These various embodiments can include embodiments that are executable and interpretable on a programmable system including at least one programmable processor, which are special purpose computers for performing the functions of the RTAS 230, coupled to receive data and instructions from, and to transmit data and instructions to, a storage system, at least one input device, and at least one output device.

[0090] To provide for interaction with a user, the systems and techniques described here can be implemented on a computer having any suitable display device for displaying information to the user and an input device 770 (*e.g.,* a keyboard, a touchpad, touchscreen, a mouse, or a trackball) by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well. Feedback provided to the user can be any

form of sensory feedback (*e.g.*, visual feedback, auditory feedback, or tactile feedback). Input from the user can be received in any form, including acoustic, speech, or tactile input.

[0091] The computing system can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises through computer programs running on the respective computers and having a client-server relationship to each other.

[0092] The illustrative block diagrams and flowcharts depict process steps or blocks that may represent modules, segments, or portions of code that include one or more executable instructions for implementing specific logical functions or steps in the process. Although the particular examples illustrate specific process steps or procedures, many alternative implementations are possible. Some process steps may be executed in different order from the specific description herein based on, for example, considerations of function, purpose, conformance to standard, legacy structure, user interface design, and the like.

[0093] A number of embodiments of the invention have been described. It should be understood that various modifications may be made without departing from the spirit and scope of the invention. For example, various forms of the flows shown above may be used, with steps re-ordered, added, or removed. Also, although several embodiments of authorizing a remote terminal or mobile device have been described, it should be recognized that numerous other applications are contemplated. Accordingly, other embodiments are within the scope of the following claims.

CLAIMS

1. A telecommunications system comprising:

a processor; and

a memory device that stores a plurality of instructions, which when executed by the processor, causes the processor to:

receive a request from a telephony switch to terminate a call, the call including a plurality of call attributes;

analyze, the call to determine if one of the plurality of attributes associated with the call is on a blacklist;

if at least one attribute associated with the call is on a blacklist, flag the call as fraudulent;

analyze the flagged call to determine if the at least one attribute associated with the call is on a whitelist;

if the at least one attribute associated with the call is not on the whitelist, generate a rejection message;

receive a message indicating that the at least one attribute associated with the call should be added to the whitelist;

add the at least one attribute associated with the call to the whitelist to update the whitelist;

generate new entries on the whitelist based on the received message to further update the whitelist; and

apply the updated whitelist to future calls.

2. The telecommunications system of claim 1, wherein the plurality of call attributes further includes at least a calling party number and a called party number.

3. A telecommunications system of claim 1, wherein if the at least one attribute associated with the call is on the whitelist, generate a second rejection message.

4. A telecommunications system comprising:

a processor; and

a memory device that stores:

a plurality of blacklist attributes;

a plurality of whitelist attributes, each of the plurality of whitelist attributes is a subset of one of the plurality of blacklist attributes;

a plurality of instructions, which when executed by the processor, causes the processor to:

receive a first request from a telephony switch to terminate a first call, the first call includes a plurality of call attributes;

if one of the plurality of call attributes associated with the first call matches one of the plurality of blacklist attributes and the one of the plurality of call attributes does not match one of the plurality of whitelist attributes, generate a first rejection message;

receive a first message indicating that generation of the first rejection message was incorrect;

receive a second request from a telephony switch to terminate a second call, the second call includes a second plurality of call attributes;

if one of the second plurality of call attributes associated with the second call matches one of the plurality of blacklist attributes and the one of the second

plurality of call attributes does not match one of the plurality of whitelist attributes, generate a second rejection message;

receive a message indicating that generation of the second rejection message was incorrect;

if the matching blacklist attribute associated with the first call is the same as the matching blacklist attribute associated with the second call, analyze the first call and the second call to determine if there is a common attribute that is a subset of the blacklist attributes associated with the first call and the second call;

add the subset of the matching blacklist attribute associated with the first call and second call to the plurality of whitelist attributes.

5. The telecommunications system of claim 4, wherein the matching blacklist attribute associated with the first call and the second call is a high cost country code and the subset of the blacklist attribute is a local area code.

6. The telecommunications system of claim 4, wherein the matching blacklist attribute associated with the first call and the second call is a country code associated with a high level of fraudulent telephone call activity and the subset of the blacklist attribute is a block of telephone numbers.

7. A telecommunications system comprising:

a processor; and

a memory device that stores a plurality of instructions, which when executed by the processor, causes the processor to:

receive a request from a server to route communications data, the communications data including a plurality of communications attributes;

analyze, the communications data to determine if at least one of the plurality of communications attributes associated with the communications data is on a blacklist;

if at least one of the plurality of communications attributes associated with the communications data is on the blacklist, generate a first rejection message, where the first rejection message would cause the communications data to be blocked from further routing;

if none of the plurality of communications attributes associated with the communications data are on the blacklist, generate a second rejection message, where the second rejection message would cause the communications data to be blocked from further routing; and

transmit the first rejection message or the second rejection message to the server;

wherein if the second rejection message is sent, then the second rejection message causes the server to route the communications data to another server to deliver the communications data.

8. The telecommunications system of claim 7, wherein if at least one of the plurality of communications attributes associated with the communications data is on the blacklist, flag the communications data as fraudulent.

9. The telecommunications system of claim 8, wherein the processor further analyzes the flagged communications data to determine if the at least one of the plurality of communications attributes associated with the communications data is on a whitelist.

10. The telecommunications system of claim 9, wherein if the at least one of the plurality of communications attributes associated with the communications data is on the whitelist, generate the second rejection message.

11. The telecommunications system of claim 7, wherein the communications data is call signaling associated with a voice call.

12. The telecommunications system of claim 11, wherein the second rejection message is a session initiation protocol 503 service unavailable message.

13. The telecommunications system of claim 11, wherein the second rejection message is an SS7 release 34 message.

14. The telecommunications system of claim 11, wherein the first rejection message is a session initiation protocol 403 forbidden message SS7 release 34 message.

15. The telecommunications system of claim 11, wherein the first rejection message is an SS7 release 21 message.

16. The telecommunications system of claim 7, wherein the communications data is message signaling associated with a communications message.

17. The telecommunications system of claim 16, wherein the communications message is an SMS message.

18. The telecommunications system of claim 17, wherein the second rejection message is a response status: P_APPN(0x65) message.

19. The telecommunications system of claim 17, wherein the first rejection message is a response status: P_APPN(0x66) message.

20. The telecommunications system of claim 7, wherein the communications data is call signaling associated with a voice call and the at least one of the plurality of communications attributes is a country code.

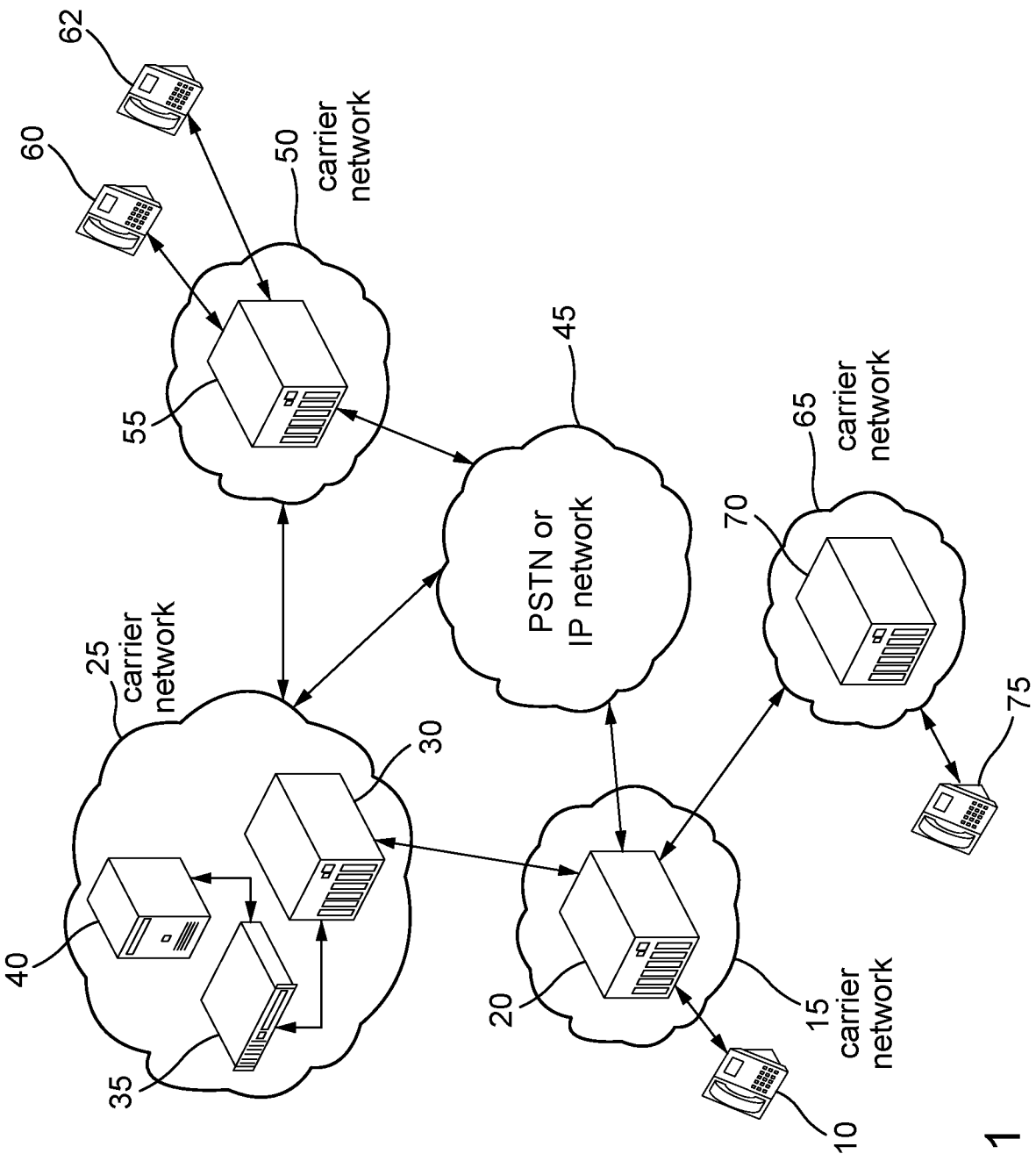

62
60
50
carrier
network
55
45
PSTN or
IP network
65
carrier
network
70
25
carrier
network
30
75
40
20
15
carrier
network
35
10

FIG. 1

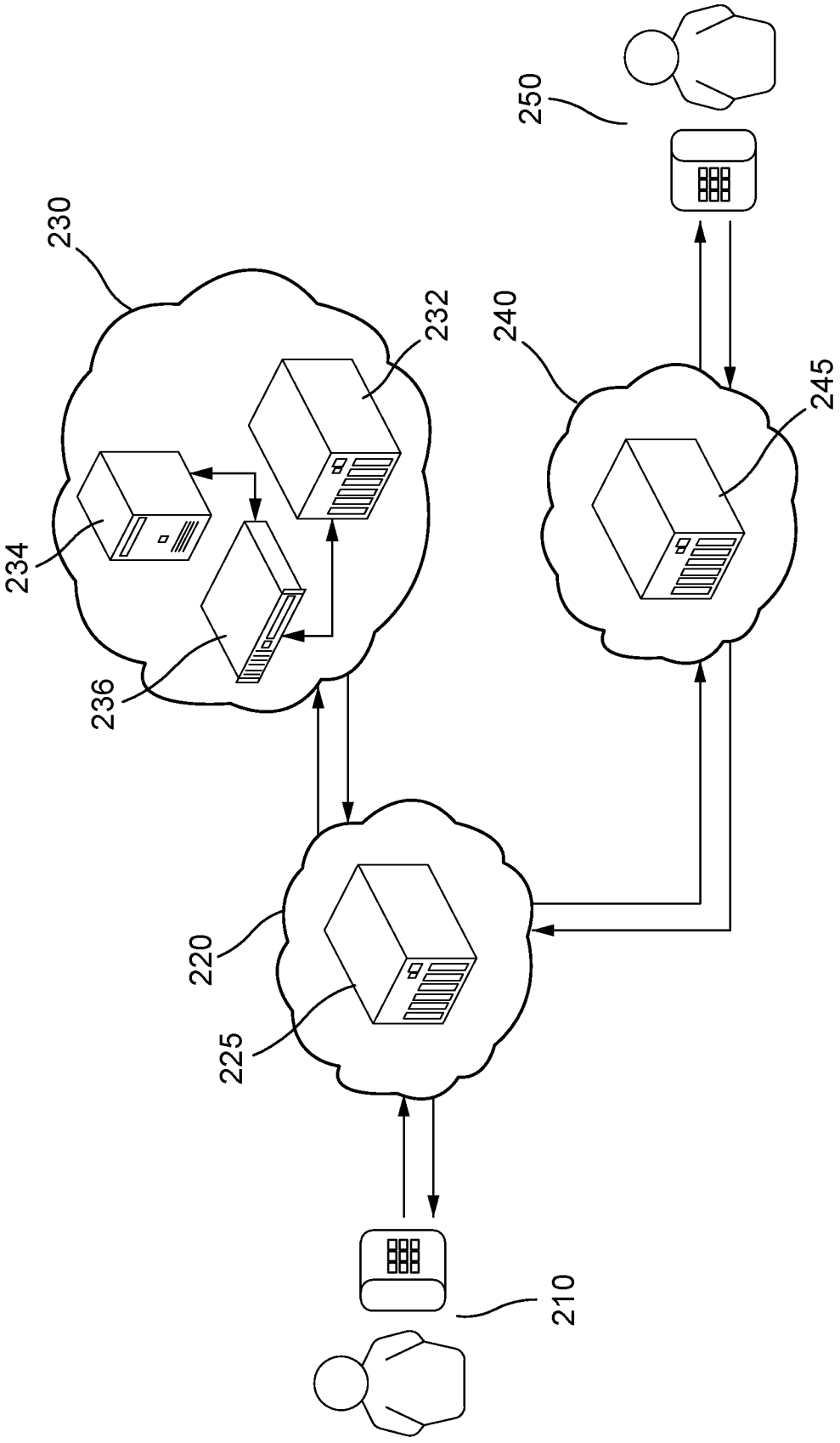


FIG. 2

FIG. 3

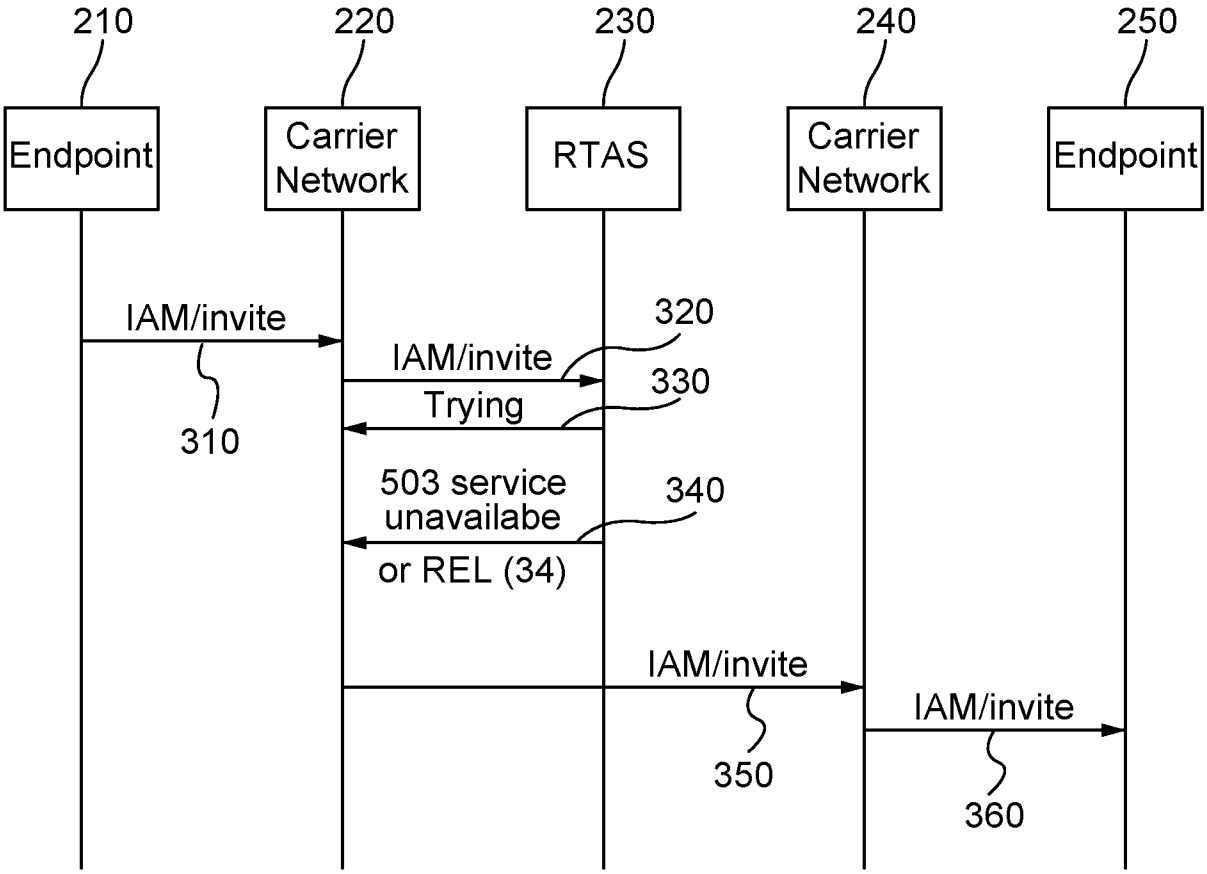

210
220
230
240
250
Endpoint
Carrier Network
RTAS
Carrier Network
Endpoint
IAM/invite
310
IAM/invite
320
Trying
330
503 service unavailabe
or REL (34)
340
IAM/invite
350
IAM/invite
360

FIG. 4

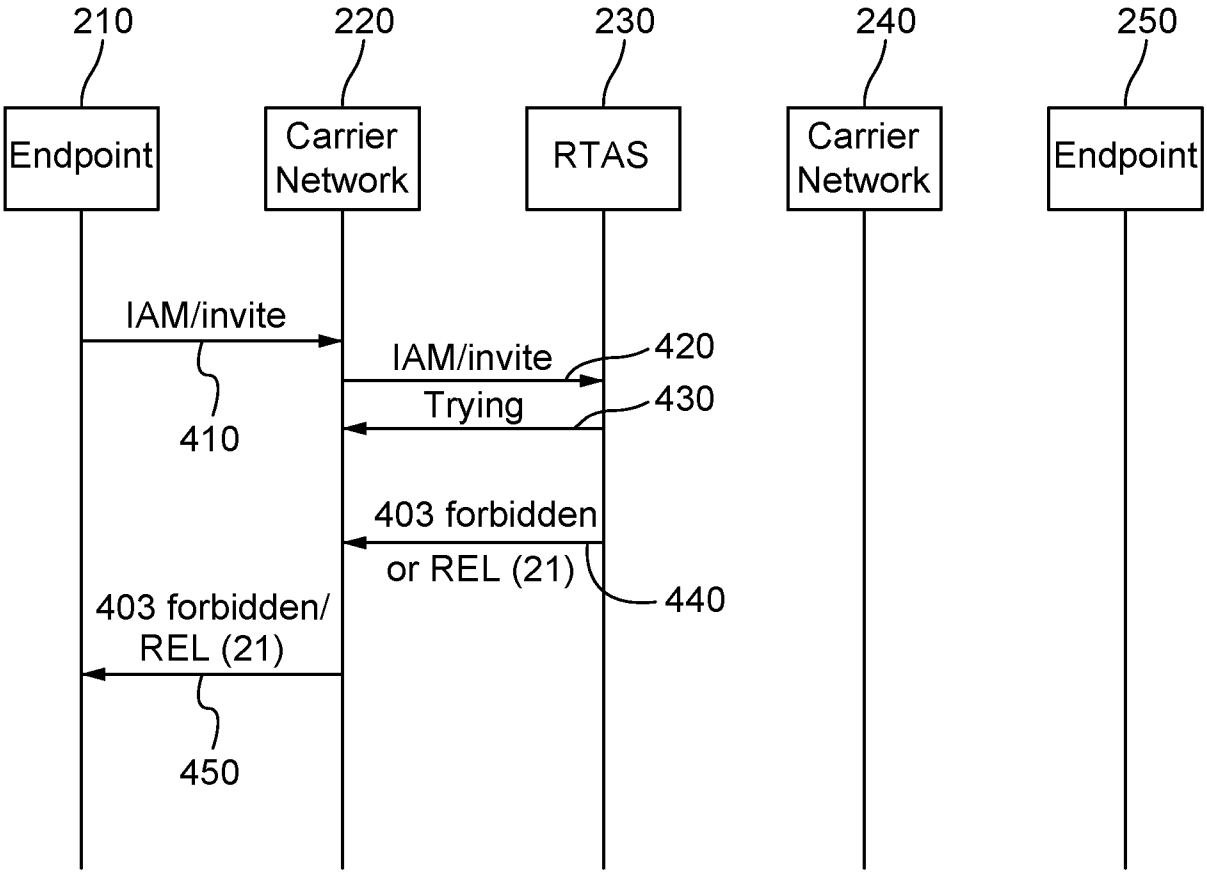

210
220
230
240
250
Endpoint
Carrier Network
RTAS
Carrier Network
Endpoint
IAM/invite
410
IAM/invite
420
Trying
430
403 forbidden or REL (21)
440
403 forbidden/ REL (21)
450

FIG. 5

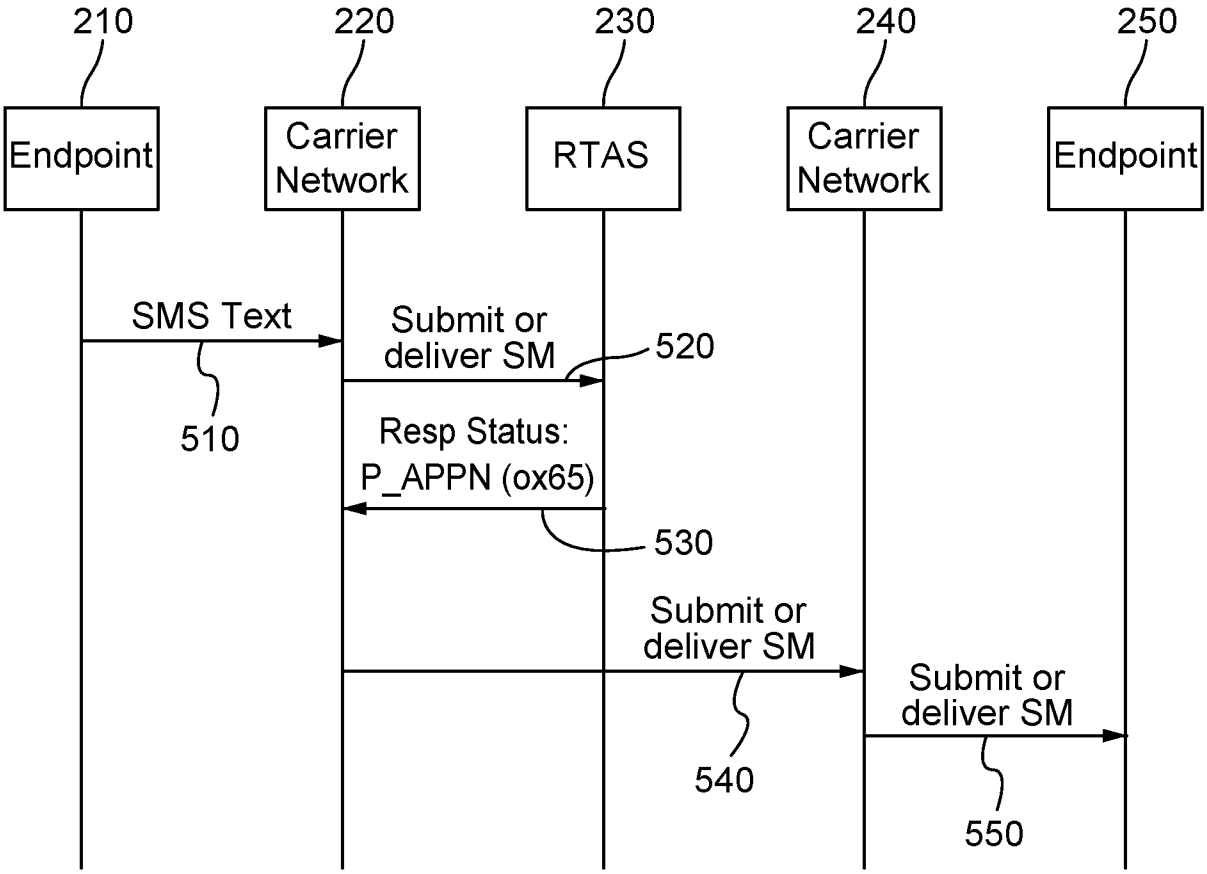

210
220
230
240
250
Endpoint
Carrier Network
RTAS
Carrier Network
Endpoint
SMS Text
510
Submit or deliver SM
520
Resp Status: P_APPN (ox65)
530
Submit or deliver SM
540
Submit or deliver SM
550

FIG. 6

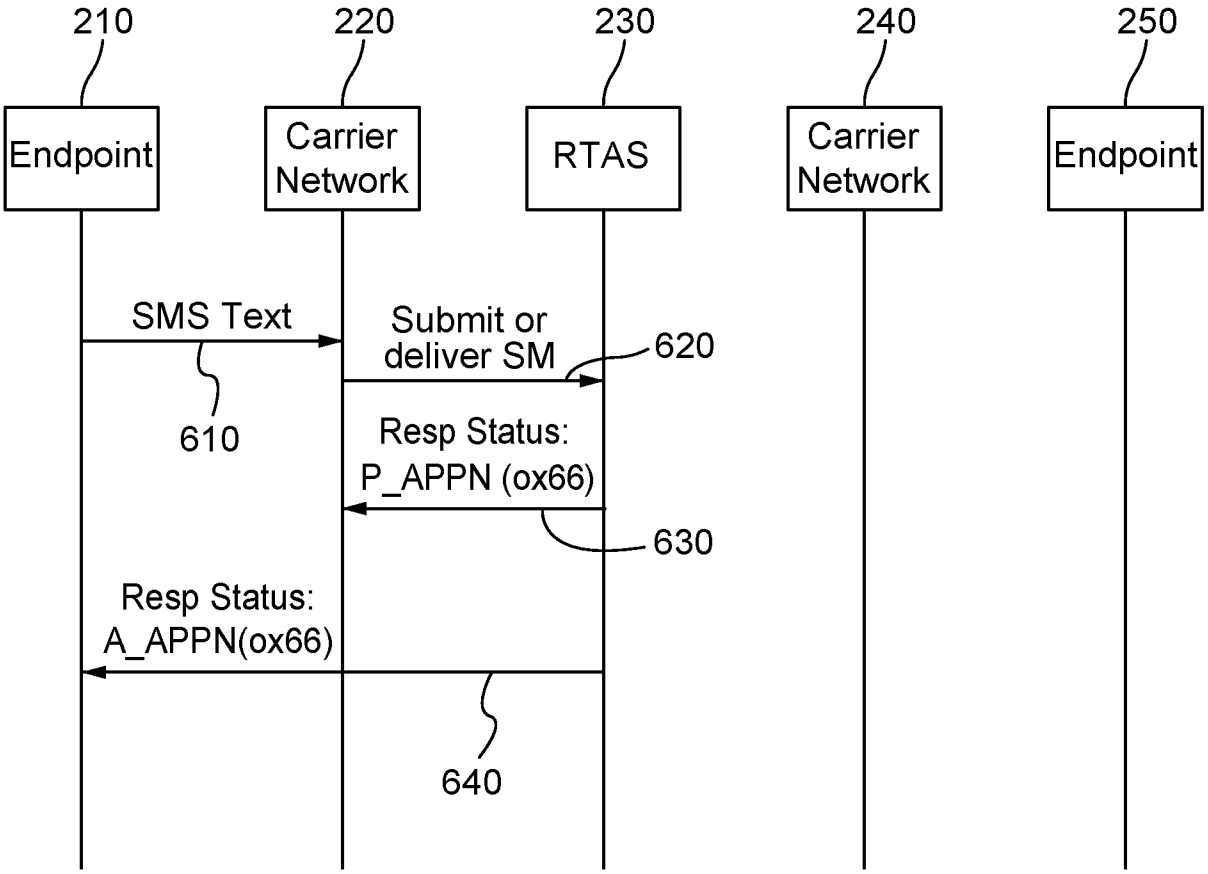
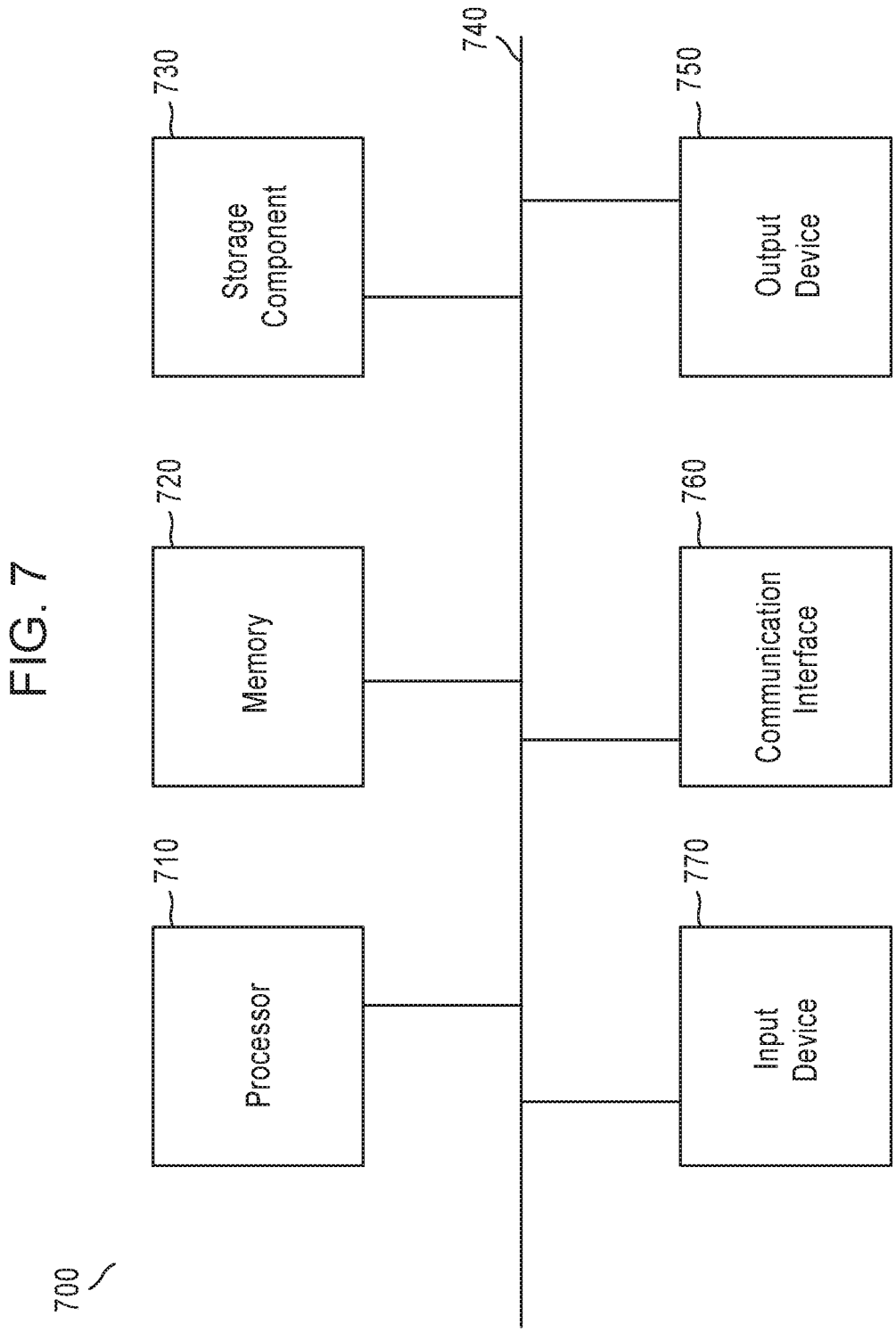

210
220
230
240
250
Endpoint
Carrier Network
RTAS
Carrier Network
Endpoint
SMS Text
610
Submit or deliver SM
620
Resp Status: P_APPN (ox66)
630
Resp Status: A_APPN(ox66)
640

FIG. 7


700
710
Processor
720
Memory
730
Storage Component
740
750
Output Device
760
Communication Interface
770
Input Device

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US17/26799

A. CLASSIFICATION OF SUBJECT MATTER

IPC - G06F 17/30; G06F 21/50; G04R 20/14 (2017.01)

CPC - G06F 21/121; G06F 21/313; H04L 51/30; H04W 12/12; H04W 12/02; H04W 4/06

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

See Search History document

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

See Search History document

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

See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/0143422 A1 (CAI, Y) 21 June 2007; paragraphs [0015], [0018], [0019].	1-3
A	US 2014/0031009 A1 (RINGCENTRAL, INC.) 30 January 2014; entire document.	1-3
A	US 8194581 B1 (SCHROEDER, D et al.) 5 June 2012; entire document.	1-3

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 July 2017 (31.07.2017)	23 AUG 2017
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US17/26799

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fee must be paid.

Group I: Claims 1-3 are directed towards a telecommunications system comprising updating a whitelist.
Group II: Claims 4-6 are directed towards a telecommunications system comprising messages indicating that generation of rejection messages were incorrect.
Group III: Claims 7-20 are directed towards a telecommunications system comprising routing communication data to another server.

*** See extra sheet ***

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-3

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US17/26799

-***-Continued from Box III -***-

The inventions listed as Groups I-III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

The special technical features of Group I include at least instructions to: if at least one attribute associated with the call is on a blacklist, flag the call as fraudulent; receive a message indicating that the at least one attribute associated with the call should be added to the whitelist; add the at least one attribute associated with the call to the whitelist to update the whitelist; generate new entries on the whitelist based on the received message to further update the whitelist; and apply the updated whitelist to future calls, which are not present in Groups II-III.

The special technical features of Group II include at least instructions to: receive a first message indicating that generation of the first rejection message was incorrect; receive a second request from a telephony switch to terminate a second call, the second call includes a second plurality of call attributes; if one of the second plurality of call attributes associated with the second call matches one of the plurality of blacklist attributes and the one of the second plurality of call attributes does not match one of the plurality of whitelist attributes, generate a second rejection message; receive a message indicating that generation of the second rejection message was incorrect; if the matching blacklist attribute associated with the first call is the same as the matching blacklist attribute associated with the second call, analyze the first call and the second call to determine if there is a common attribute that is a subset of the blacklist attributes associated with the first call and the second call, which are not present in Groups I and III.

The special technical features of Group III include at least instructions to: receive a request from a server to route communications data, the communications data including a plurality of communications attributes; generate a first rejection message, where the first rejection message would cause the communications data to be blocked from further routing; if none of the plurality of communications attributes associated with the communications data are on the blacklist, generate a second rejection message, where the second rejection message would cause the communications data to be blocked from further routing; and transmit the first rejection message or the second rejection message to the server; wherein if the second rejection message IS sent, then the second rejection message causes the server to route the communications data to another server to deliver the communications data, which are not present in Groups I-II.

The common technical features shared by Groups I-III are a telecommunications system comprising: a processor; and a memory device that stores a plurality of instructions, which when executed by the processor, causes the processor to: receive a request from a telephony switch to terminate a call, the call including a plurality of call attributes; analyze, the call to determine if one of the plurality of attributes associated with the call is on a blacklist; analyze the flagged call to determine if the at least one attribute associated with the call is on a whitelist; if one of the plurality of call attributes associated with the first call matches one of the plurality of blacklist attributes and the one of the plurality of call attributes does not match one of the plurality of whitelist attributes, generate a first rejection message; and generate a second rejection message.

However, these common features are previously disclosed by US 2007/0143422 A1 (CAI). Cai discloses a telecommunications system (a telecommunications network; para [0013]) comprising: a processor and a memory device that stores a plurality of instructions, which when executed by the processor, causes the processor (a network administration terminal 40, inherently requiring a processor and memory to store instructions, the instructions for building a black list and a white list over time; para [0015]) to: receive a request from a telephony switch to terminate a call, the call including a plurality of call attributes (before a call received in a mobile switching center is sent on to a station identified as the destination of the call, the mobile switching center will check whether the destination station is willing to accept calls from the source; para [0018]); analyze, the call to determine if one of the plurality of attributes associated with the call is on a blacklist and analyze the flagged call to determine if the at least one attribute associated with the call is on a whitelist (the anti-spam application 30 or the short message service center 20 checks the active phonebook 50 to see if the source is on a white list or black list for the destination station; para [0015]); if one of the plurality of call attributes associated with the first call matches one of the plurality of blacklist attributes and the one of the plurality of call attributes does not match one of the plurality of whitelist attributes; and generate a first rejection message (if the call or message has been rejected, then an announcement or message is sent to the caller; para [0023]); and generate a second rejection message (if the call is blocked, then another announcement message is sent to the caller; para [0024]).

Since the common technical features are previously disclosed by the Cai reference, these common features are not special and so Groups I-III lack unity.