

FASCICULE DE BREVET D'INVENTION

21 Numéro de dépôt : 1201300429
(PCT/EP11/073618)

22 Date de dépôt : 21.12.2011

30 Priorité(s) :
EP n° 11161703.1 du 08/04/2011

24 Délivré le : 31.08.2017

45 Publié le : 16.02.2018

73 Titulaire(s) :

Meucci Solutions NV,
Bellevue 5-601,
B-9050 GENT-LEDEBERG (BE)

72 Inventeur(s) :

VAN DER MEEREN, Guy (BE)
TUYTTE, Conrad (BE)
DE BONTRIDDER, Lieven (BE)
PHILIPS, Peter (BE)
MOUTON, Kenneth (BE)
VERLINDE, Dirk (BE)

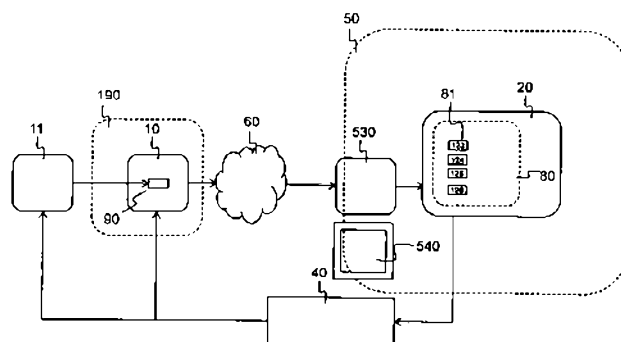
74 Mandataire : Cabinet Spoor & Fisher Inc. Ngwafor & Partners, Blvd. du 20 Mai, Immeuble Centre Commercial de l'Hôtel Hilton, 2è Etage, Porte 208A, P.O. Box 8211, YAOUNDE (CM).

54 Titre : A bypass detection system with number masking.

57 Abrégé :

According to the invention there is provided a system (1) for detection of a bypass (540) of an interconnect (30) to a communication network (50) under test, said system (1) comprising a control system (40) that is configured to use a set of virtual numbers (81) as called party of said test calls. Said set of virtual numbers (81) is configured such that said test calls are terminated on said terminating subscription (80) to avoid counter detection.

Fig. 3



A BYPASS DETECTION SYSTEM WITH NUMBER MASKINGField of the Invention

5

The present invention generally relates to a system for detection of an interconnect bypass in telecommunication networks, especially in wireless telecommunication networks such as for example of the type GSM, GPRS, UMTS or similar, but also in wired telecommunication networks.

10

Background of the Invention

15

When a telecommunication network operator provides access from his network to a network of another telecommunication network operator and vice versa, both operators, by means of agreement or sometimes subject to regulatory requirements, set up a suitable interconnection facility which is subjected to extensive testing in order to assess technical reliability and the quality of service of the interconnection facility so that the agreed upon or regulatory standards are met. Next to the technical arrangements there are in many cases also interconnection charges that the telecommunication network operator receiving a call charges for the calls passing through the interconnection facility. When a calling party calls from another telecommunication network to the network of the telecommunication network operator of the receiving party, for example because the calling party is a client of another network operator than the receiving operator or because the calling party is abroad and is making use of a partnering network operator that provides roaming services for its network operator, this call has to pass through the interconnection facility.

20

25

30

Sometimes there are attempts to bypass the interconnection facilities of the network operator in an attempt to make money by avoiding at least a part of the interconnection charges. These attempts are made by bypass operators that reroute a part of the traffic of calling parties within the network of another operator to the network of the receiving operator without going through the interconnection facility. Generally these bypass operators make use of end user facilities from the receiving operator.

This leads to a direct loss of revenue for the receiving network operators and this leads to technical problems. First of all as the bypass operator uses end user facilities to provide a network interconnection. Furthermore the use of these end user facilities and the setup of a new call creates an additional interface. Therefor there is a serious risk of quality problems such as degraded quality of audio or data transmissions, interruptions during the call, a prolonged waiting time during the call initiation, unacceptable delays in the transmissions, ... Further, because of the bypass operators reroute the call by setting up a new call making use of end user facilities of the receiving operator, the CLI of the calling party will be replaced with the CLI of the new call. This leads to inconveniences for the receiving parties which receive an erroneous CLI, but can also have more serious safety issues involved when a call to emergency services or police is involved. Furthermore this also creates serious technical difficulties for automatic telephone switchboards that operate on the basis of the CLI of the incoming call.

A system for setting up test calls in a telecommunication network is known from for example WO99/01974 and WO2008/071857. These call charge verification systems generate a series of calls between different sites on one or more networks to enable the network operator to check the billing procedure of the network. These systems however rely on collection of billing data produced by the operator in order to extract data, such as for example the CLI for analysis. Therefor these systems require access to sensitive data of the telecommunication network operator. This data is sensitive because it is related to the calling behaviour of its customers which might be subjected to privacy regulations or because it relates to billing information which is considered as commercial know how of the telecommunication network operator. These problems are especially relevant if the call charge verification system is operated by third parties that offer such system as a service to the telecommunication network operator. As then extensive access by these third parties to information of the telecommunication network operator requires specific interfaces to be developed to provide access to the billing information for each specific telecommunication network operator. This is time and resource intensive and makes it difficult to scale the verification system to multiple telecommunication network operators.

A known system that overcomes the abovementioned drawbacks is the Meucci system as described on their website: <http://www.meucci-solutions.com> . This system for detection of a bypass of an interconnect to a telecommunication network under test comprises means

adapted to originate a test call to said telecommunication network under test from outside the telecommunication network under test and at least one receiver probe with a subscription for terminating said test call. Further this system comprises a control system configured to initiate the test call; receive from the receiver probe call information comprising a received calling line identification (CLI) of the test call; and analyse the received calling line identification (CLI) such that presence of the bypass can be detected. The Meucci system does not require an interface with the billing system as it obtains the received CLI of the test call from the receiver probe. However in this case difficulties can arise for detecting and disabling a bypass when the bypass operator makes use of the CLIR function in order to mask the calling line identification of their bypass equipment as will be explained in further detail below.

One problem with these systems that make use of test calls is that they are exposed to the risk of identification of their calling behaviour. In prior art systems the test calls are normally never picked up and are performed according to a fixed pattern of start time, ringing duration, etc, which may cause a suspicious calling pattern. Another problem is that the means to originate test calls and the subscriptions that terminate test calls may originate or terminate a large number of calls, such volume being suspicious. This creates the risk that the bypass operators can detect and identify the means for originating the test calls and/or the subscriptions used by the receiver probes used for receiving the test call. The bypass operator can then subsequently blacklist these specific means and/or subscriptions in order to avoid detection. In order to be effective afterwards parts of the system for making test calls, such as for example the receiver probe or the means for originating test calls, have to be reconfigured extensively, for example by providing them with new subscriptions for receiving or generating test calls, which is a slow process, which casts money and may require physical intervention such as for example replacing a SIM card.

There is known from FR2938392 the disclosure of a system which generates test calls which makes use of a forwarding mechanism to cascade client subscriptions implemented with SIM cards. This system decreases the risk of counter detection by increasing the number of subscriptions used as called party for the test calls, however the implementation of this system suffers from important limitations. as the cascading mechanism increases cost, complexity and decreases the ease of maintenance of such a system and presents difficulties in scaling up the number of such subscriptions. Even when the large number of SIM cards or customer subscriptions, for example five hundred, is not used at once in such a system, but for example are introduced into the system in a sequential manner this still requires a thorough

documentation of the setup of the system and the available SIM cards or subscriptions for use in the system. Furthermore the proposed cascading mechanism with two or potentially even more stages presents specific problems. A subscription and its associated configuration to forward or deviate calls must be documented in a multitude of systems and database or otherwise they risk being wiped out when data quality and integrity checks are performed. The configuration of call forwards or deviations is not always stable. Setting up a call forward or deviation takes time at the setup of a call. A forward or deviation may be a pay for service which might generate costs on subscriptions used in the cascading mechanism, it might lead to transfer cost within an operator and it makes it difficult to use prepaid subscriptions. Also, when forwarding or deviating a call, in some cases the CLI is changed by the operator into the CLI of the subscription that is forwarding or deviating the call, making the whole setup useless. When a subscription used in such a system must be replaced by a new subscription, for example because it was detected by a bypass operator, this requires a multitude of operations as all documentation about the state of the system needs to be updated and also the configuration of the forwarding or deviation mechanism needs to be adapted accordingly.

As such there is a need for a system that can provide real time information about the availability of a bypass. This system should be able to be operated by third parties and should not require access to sensitive data of the telecommunication network operator. The system should also have a decreased risk of counter-detection by a bypass operator and should enable a simple configuration, allow ease of maintenance and improved scalability.

Summary of the Invention

According to the invention there is provided a system for detection of a bypass of an interconnect to a telecommunication network under test, said system comprising:

means adapted to originate a test call to said telecommunication network under test from outside the telecommunication network under test;

at least one receiver probe with a terminating subscription for terminating said test call; and

a control system configured to:

initiate the test call;

- 5 -

receive from the receiver probe call information comprising a received calling line identification of the test call; and

analyse the received calling line identification such that presence of the bypass can be detected,

5 CHARACTERIZED IN THAT

said system further comprises:

a non-cascaded set of virtual numbers being configured such that said test calls are terminated in one stage on said terminating subscription; and

means configured to manipulate calling line identifications, and in that

10 said control system is further configured:

to use a plurality of virtual numbers from said non-cascaded set of virtual numbers as called party of a plurality of test calls;

to instruct said means configured to manipulate calling line identifications to generate a plurality of manipulated calling line identifications;

15 to use said plurality of calling line identifications as calling party at initiation of said plurality of test calls; and

to set up said plurality of test calls from said plurality of manipulated calling line identifications, through said means to originate a test call towards said plurality of virtual numbers.

20

This system according to the invention is capable of decreased risk of counter-detection by a bypass operator because it can make use of a large amount of virtual numbers and manipulated CLI. Furthermore this makes it impossible for the operator of a bypass to identify the terminating subscription and/or the means for originating test calls and subsequently
25 blacklist them, as there are provided means to manipulate the calling line identification which prevent detection of the means for originating a test call and there are provided virtual numbers as called parties which prevent detection of the terminating subscription. As both the called party and calling party of the test call are available in combination to a bypass operator, this means that if the bypass operator is able to identify one of both as being used in a system for
30 detection of a bypass automatically the other one is also subject to detection. It is therefore essential that both the called party and calling party are provided with mechanisms to reduce the risk of detection, respectively the non-cascaded set of virtual numbers and the means configured to manipulate calling line identifications. As such it is also important that both the

- 6 -

called party numbers (virtual numbers) and the calling party numbers (manipulated CLI) exist in large quantities to avoid detection, because as explained above, the detection of one would inevitably and immediately lead to the detection of the other.

5 It is also essential that use is made of a non-cascaded set of virtual numbers, which means that said test calls are terminated in one stage on said terminating subscription, instead of a cascaded set of numbers associated with a cascaded set of subscriptions comprising two or more stages of cascading, because otherwise scaling up the amount of numbers to a level that is sufficient to avoid counter detection by the bypass operator would involve extensive and
10 complex operations and a large configuration overhead that result in extensive maintenance, extensive documentation requirements and difficult and error prone configuration.

This system further does not require complex computations nor extensive amounts of data to be able to detect the existence of a bypass. It only needs to analyse the received calling line
15 identification (CLI). The analysis can be implemented in a simple manner, such as for example determining whether the received CLI is from a call that originated from within the telecommunication network under test by analysing the prefix of the received CLI for the presence of a prefix belonging to the numbering plan of the telecommunication network under test.

20 According to an embodiment of the invention said means configured to manipulate calling line identifications comprise:

- end user subscriptions with the possibility to manipulate the CLI; or
- a call generator connected to a telecommunication network on a network level.

25 According to a further embodiment of the invention said means to originate a test call comprises said means configured to manipulate calling line identifications.

30 According to an alternative embodiment the means configured to manipulate calling line identifications route test calls through said means to originate a test call.

According to still a further embodiment the means for originating said test call comprise an originating subscription to an originating network outside the telecommunication network under

- 7 -

test, that is configured to be routed to said virtual numbers, and wherein test calls are set up from said means configured to manipulate calling line identifications with different calling line identifications to said originating subscription for enabling test calls routed through the originating network but not necessarily generating a calling line identification identifying the originating network.

This reduces the risk that a bypass operator blacklists all calls with a CLI identifying a specific network, or blacklists an entire originating network or an interconnect with a carrier, of which the bypass operator suspects it serves as originating network for test calls of a bypass detection system. Furthermore this advantageous embodiment implements a mechanism for indirectly manipulating the CLI even when direct manipulation of the CLI in the originating network is not technically possible or allowed.

According to an embodiment of the invention said set of non-cascaded virtual numbers is implemented as:

- multiple Subscriber Number options on single physical ISDN BRI fixed line;
- multiple PBX numbers on a single physical ISDN PRI line;
- multiple Mobile Subscriber Integrated Service Digital Network numbers on a single physical SIM card subscription; or
- multiple numbers routed to a single IMSI (International Mobile Subscriber Identity) by means of the routing table.

This allows the non-cascaded virtual numbers to be set up with technology that is readily available in most telecommunication networks and further minimizes requirements as to physical resources such as for example SIM cards and associated interfaces.

According to still a further embodiment said set of virtual numbers comprises one or more of the following:

- re-used and unused numbers;
- non-consecutive numbers; and
- numbers from multiple geographical areas in the case of a fixed line network or multiple network prefixes in the case of mobile networks.

- 8 -

According to a further embodiment the set of virtual numbers is renewed regularly.

In this way the risk that these virtual numbers are correlated with test call behaviour is reduced.

5 According to still a further embodiment said set of virtual numbers is divided in subsets of virtual numbers that are used consecutively in a rotating order. Optionally said rotating order is randomized or usage of virtual numbers within said subsets of virtual numbers is randomized.

10 All these measures decrease the risk that the bypass operator will be able to link the calling behaviour of the bypass detection system to a specific number and especially to the subscriptions of the receiver probes for terminating the test calls as the number of these receiver probe subscriptions is not visible at all for any carrier or bypass operator.

15 According to a preferred embodiment said terminating subscription is configured with calling line identification restriction override (CLIRO).

20 This advantageously enables a simple and robust system for detection of a bypass that is able to detect a bypass even if the bypass operator makes use of a calling line identification restriction (CLIR) function in order to hide the CLI from detection. This enables to identify and subsequently disable the subscriptions that are being used in a bypass even if the bypass operator makes use of the CLIR function. When third parties provide the system for detection of a bypass as a service to a telecommunication network operator this requires neither access to sensitive data like for example billing data nor complex technical interfaces to provide that access. The third party only requires a subscription configured with CLIRO for terminating the
25 test call.

Brief Description of the Drawings

30 Fig. 1 illustrates an embodiment according to the invention without the presence of a bypass;

Fig. 2 illustrates the embodiment according to Figure 1 with the presence of a bypass;

Fig. 3 illustrates an alternative embodiment according to the invention without the presence of a bypass; and

5 Fig. 4 illustrates the embodiment according to Figure 3 with the presence of a bypass.

Detailed Description of Embodiment(s)

10 Figure 1 shows a system 1 for detection of a bypass of an interconnect 530 to a telecommunication network 50 under test. The system 1 according to the invention comprises a means 10 to originate a test call to said telecommunication network 50 under test from outside the telecommunication network 50 under test. This means 10 can be a suitable sender probe such as for example a GSM mobile phone or any other type of device capable of initiating a call
15 on a predetermined outside telecommunication network other than the telecommunication network 50 of the network operator that is undertaking the investigation regarding the presence of a bypass of an interconnect 530, such as for example calling cards, a telephone number providing access to voip systems, call back mechanisms, any type of pc originating calls, a suitable subscription to mobile networks such as for example a SIM card, wireline networks or
20 call generators directly connected to telecommunication network equipment. The means 10 can comprise for example a fixed line subscription in the UK "+44 20 1234 5678" and the telecommunication network 50 under test can for example be a telecommunication network of a Belgian mobile operator with a numbering plan with a 474 prefix, this means "+32 474 xxx xxx". The means 10 is for this purpose connected to a suitable control system 40 which enables to
25 initiate the test call according to instructions received from this control system 40. The control system 40 is for example a suitably programmed computer that is directly connected to the means 10, but it might also be a remote computer system that is connected to the means 10 by means of a suitable network interface, such as for example a LAN or the internet, to enable exchange of instructions and/or data through this networks. It is clear that the system 1 for
30 detection of a bypass is not limited to a system with only one means 10, it can however comprise any suitable number of means 10 dispersed among any suitable number of outside telecommunication networks, such as for example eight means 10 for different telecommunication networks in France and three means 10 for roaming telecommunication network partners in Ghana.

As can be seen in Figure 1 the bypass detection system 1 also comprises a receiver probe 20. This receiver probe 20 can for example also be a GSM mobile phone or any other type of device with a subscription for terminating the test call. The receiver probe 20 can for example
5 comprise a subscription to the telecommunication network 50 under test "+32 474 123 456". The receiver probe 20 is also connected to a suitable control system 40. The control system 40 receives from the receiver probe 20 call information comprising a received calling line identification (CLI) of the test call. It is clear that the system 1 is also not limited to a system with only one receiver probe 20. It can comprise any suitable number of receiver probes 20 with a
10 subscription for terminating test calls.

The call information comprises a received CLI of the test call and optionally other data relating to the call such as for example the time and date the test call was exactly received, the time and date at which the test call started ringing, the time and date at which the test call was
15 terminated, an indicator for whether the test call was picked up, the phone number associated with the means 20, the presentation indicator, ...

As shown in Figure 1 when no bypass is present the control system 40 initiates the test call by activating the means 10 which subsequently originates the test call by calling the subscription to the telecommunication network 50 under test in the receiver probe 20. The test call is then sent
20 to the telecommunication network 50 under test, for example optionally via one or more carriers 60. Subsequently the test call passes interconnect 530 of the telecommunication network 50 under test who routes the test call to the receiver probe 20. The receiver probe 20 then receives the incoming test call. It is not required for the receiver probe 20 to actually answer the test call. The control system 40 could for example be configured in such a way that it instructs means 10
25 to initiate the test call to the receiver probe 20 and to automatically disconnect the test call after allowing three rings. The control system 40 then receives from the predetermined receiver probe 20 call information that comprises a received CLI, which is transmitted just before or after the first ring, and optionally other data concerning the test call. This could be done for example
30 by downloading the call information from the receiver probe 20 to the control system 40 or by transmitting it to the control system 40 in any suitable way, by for example a wired or wireless connection means. The control system 40 then analyses the received CLI.

- 11 -

This analysis can be executed as a simple comparison with the calling party number associated with means 10 that the control system 40 instructed to initiate the test call. In the case illustrated in Figure 1 where the test call passed through the interconnect facility 530 this received CLI, for example "+44 20 1234 5678", will match the calling party number, "+44 20 1234 5678", associated with means 10 and the control system 40 will be able to determine that for this test call no bypass was detected.

As the means 10 originates the test call from outside the telecommunication network 50 under test, the analysis can be done with even more reduced complexity and increased reliability. It can be determined whether the received CLI is a call that originated from within the telecommunication network 50 under test, this means an on net call, by for example analysing whether the prefix of the received CLI differs from the prefix associated with the numbering plan of the telecommunication network 50 under test. If this analysis of the received CLI indicates the calling party of the test call is not from within the telecommunication network under test, no bypass was detected. Thus as soon as the analysis is able to ascertain that the received CLI does not belong to the numbering plan associated with the telecommunication network 50 under test, no bypass within the network under test was detected. In order to also take into account number portability the analysis could comprise a check if the received CLI comprises a number which is comprised in the number database of the telecommunication network 50 under test. If this is not the case, no bypass within the network under test was detected. In general, because the means 10 originates the test call from outside the telecommunication network 50 under test, the presence of a bypass can be detected if the received CLI belongs to a subscription to the telecommunication network 50 under test.

Another possibility for analysis is to check if the received CLI comprises the same country code as the country code associated the telecommunication network 50 under test. As the means 10 in many cases originates a test call from a country other than the one from the telecommunication network 50 under test this provides a tool for determining whether a bypass is present.

Figure 2 shows the same system 1 according to Figure 1 in operation, but now there is a bypass 540 in place and this bypass 540 reroutes the test call. When the control system 40 now initiates a test call between means 10 and receiver probe 20 and the call is rerouted optionally

- 12 -

via one or more carriers 60 to the bypass 540 a detection of the bypass 540 is possible as explained below.

Such a bypass 540, also known as for example a GSM gateway or SIM box when it concerns a wireless telecommunication network or a leaky PBX when it concerns a wired telecommunication network, is operated by interconnection bypass operators that route part of the traffic to the telecommunication network 50 under test from outside telecommunication network 50 via for example a suitable internet interface with one of the carriers 60 towards a bypass 540 which normally makes use of a plurality of subscriptions, for example "+32 474 111 222", that operate within the telecommunication network 50 under test and which convert the incoming test call into a new call originating from a subscription to the telecommunication network 50, "+32 474 111 222", and to the same destination and as such bypass the interconnect 530. However when the control system 40 now receives the receiver call information from the receiver probe 20 that received the test call initiated from means 10, the received CLI, "+32 474 111 222" will not match the calling party number, "+44 20 1234 5678", associated with means 10. This is because instead of the calling party number of means 10, the calling party number of one of the subscriptions in the bypass 540, "+32 474 111 222", will be in the CLI received by receiver probe 20. The control system 40 is then able to assess that a bypass 530 is present.

As explained above because the means 10 originates the test call from outside the telecommunication network 50 under test, the presence of a bypass 540 can be detected if the received CLI belongs to a subscription to the telecommunication network 50 under test. This can be implemented by checking whether the received CLI comprises a prefix which belongs to the numbering plan of the telecommunication network 50 under test "+32 474 xxx xxx" or when to also take into account number portability by checking whether the received CLI comprises a number which is comprised in the number database of the telecommunication network 50 under test.

When in use the system 1 initiates multiple test calls that are routed to a terminating subscription 80 in receiver probe 20 as shown in Figures 1 and 2. According to an alternative embodiment (not shown) the receiver probe could comprise a plurality of subscriptions 80 for terminating test calls. However there are practical limits as to how many subscriptions 80 a receiver probe 20 can hold as each subscription has its associated physical components. If the

- 13 -

receiver probe 20 comprises subscriptions in the form of SIM cards in the case of a wireless telecommunication network 50 under test sufficient physical connectors for introducing a SIM card and associated electronics must be present. Also in the case of a wired telecommunication network 50 under test, where the subscriptions might be implemented as suitable electronic circuits also this implementation requires sufficient physical electronics hardware to be present.

Even when the system 1 according to the invention makes use of a plurality of receiver probes 20 each comprising a plurality of physical subscriptions 80 for terminating the test calls, the volume of test calls and the long term use of the system 1 according to the invention increase the risk of detection by the operator of the bypass 540. As explained above the test calls are not required to be picked up for the system 1 to function and thus in order to diminish the cost of operating the system 1 and in order to shorten test call duration for increasing efficiency of the system 1 test calls are normally not picked up. This however would result in a specific long term calling behaviour towards these receiver probes 20 because the resulting answer/seizure ratio for a subscription used in this receiver probes 20 would clearly diverge from that of normal human calling behaviour. Furthermore, the total volume of calls to said subscription 80 would also be suspicious, as would be the range of different CLI calling that subscription.

According to an embodiment of the system 1 according to the invention as shown in Figures 1 and 2 the virtual numbers 81 are prevented from detection (explained in further detail below), and also the means 10 for originating test calls are prevented from detection because means 10 comprise end user subscriptions that allow to manipulate CLI or call generators or alternative means 11 to perform direct CLI manipulation. In this way the risk is reduced that the bypass operator can detect the called party and calling party from the test calls. When the bypass operator would detect a test call and blacklist one of the virtual numbers 81 or one of the CLIs generated by means 10 they can be very easily replaced. As the risk of being detected by a bypass operator can never be totally eliminated and as time goes by the chance of such a detection rises it is important to have an increased flexibility to swap phone numbers used in a system 1 according to the invention. Replacing a non-cascaded virtual number 81 can be performed efficiently as only the virtual number itself must be replaced and furthermore its configuration is very simple as there is only a single stage involved.

An alternative embodiment of the system 1 according to the invention as shown in Figures 3 and 4 advantageously decreases the risk for counter-detection and black listing as the

- 14 -

terminating subscription 80 is prevented from detection by means of the virtual numbers 81 (explained in further detail below), and also the means 10 for originating test calls are prevented from detection. In order to accomplish this, the means 10 comprise an originating subscription 90 to an originating network 190 outside the telecommunication network 50 under test. This
5 originating subscription 90 is configured to route the test call to the virtual numbers 81. The test calls are then setup from means 11 with different calling line identifications to said originating subscription 90 for enabling test calls routed through the originating network 190 but not necessarily generating a calling line identification identifying the originating network 190. This
10 avoids that an operator of a bypass 540 will be able to detect what network 190 the originating subscription 90 is part of, which could lead to the operator of a bypass 540 blacklisting the entire originating network 190 or subscription 90 as in this embodiment the test calls would appear to be originated from outside the originating network 190, while still being routed through the originating network 190 in order to detect a bypass in the route of this originating network 190 to the telecommunication network 50 under test. Said means 11 configured to
15 manipulate calling line identifications are for example a VoIP subscription or a call generator connected to telecommunication network on a network level configured to manipulate calling line identifications. As shown in Figures 3 and 4 these means 11 configured to manipulate calling line identifications are outside the originating network 190 because in most fixed and mobile networks direct manipulation of the CLI is not possible. This advantageous embodiment
20 in this way implements a mechanism for indirectly manipulating the CLI even when direct manipulation of the CLI in the originating network 190 is not technically possible or allowed.

In order to decrease this risk the system 1 according to the invention, as shown in Figures 1 and 2 also makes use of a set of virtual phone numbers 81 as called party of these test calls.
25 This set of virtual numbers 81 terminates the incoming test calls directly on the terminating subscription 80. In this way the terminating subscription 80 is prevented from detection by the bypass 540 network as the phone number of this virtual number will be presented as called party instead of the number associated with the terminating subscription 80. It is important that this is a non-cascaded set of virtual numbers 81 instead of a cascaded set of numbers
30 associated with a cascaded set of subscriptions, because otherwise scaling up the amount of numbers to a level that is sufficient to avoid counter detection by the bypass 540 operator would involve extensive and complex operations and a large configuration overhead that result in extensive maintenance, extensive documentation requirements and difficult and error prone configuration.

35

- 15 -

According to the embodiments of the invention as shown in Figures 1 to 4, the set of virtual numbers 81 is implemented as a set of numbers available on the terminating subscription 80. This can for example be implemented by making use of Multiple Subscriber Number options on single physical ISDN BRI fixed line, by making use of multiple PBX numbers on a single physical ISDN PRI line, or by populating by means of the databases or the IN Platform multiple Mobile Subscriber Integrated Service Digital Network numbers on a single physical SIM card subscription identified by its International Mobile Subscriber Identity (IMSI). As, for example in a mobile telecommunication context, the MSISDN numbers defined on an IMSI are an attribute defined on this IMSI in the HLR such an operation does not require any physical intervention and a swap can thus be executed without unnecessary delays.

It is clear that these multiple virtual numbers 81 are associated with a single physical entity, such as a physical line in a fixed line telecommunication context or a SIM in a mobile telecommunication context, in a non-cascaded configuration. This means that no additional means or configurations, such as for example forwarding mechanisms, need to be implemented to terminate test calls to these virtual numbers 81 in one stage on subscription 80. In this way, when number swapping would be required, for example because one or more of the virtual numbers is detected by a bypass operator, the only operation that needs to be performed is a swap of the respective virtual number. This also allows for a simple setup of the system 1 that doesn't require extensive documentation and configuration as there are no multiple levels of cascading and associated cascading mechanisms and corresponding configuration thereof is involved. The non-cascaded setup as described above even prohibits the setup of multiple levels of cascading on a technical level.

According to an alternative embodiment, these non-cascaded virtual numbers 81 could also be created in the HLR of a telecommunication network, for example the telecommunication network 50 under test. A preferred way of terminating test calls directly, this means in one stage, on the terminating subscription 80 is by making use of the routing tables to terminate these virtual numbers 81 to the terminating subscription 80. In this way call forwarding or deviation is avoided and not cascading subscriptions are needed. Although in most telecommunication networks such forward function is readily available, call forwarding configuration is not always stable, costs a lot of time to set up and could incur costs. So setting up and configuration of these virtual numbers 81 does not require extensive resources neither does scaling up to a scale that decreases the risk of counter detection does not involve the cost and resources that would be associated with a physical implementation. Also reconfiguring the

- 16 -

system, for example in the event that one of the virtual subscriptions was blacklisted by a bypass operator does not involve physical interference with the system 1 and because of the non-cascaded setup does not require any additional operations but the swap of the virtual numbers. As explained above this allows for a system 1 that does not require extensive documentation and configuration.

In order to further decrease the risk of counter detection by for example operators of the bypass 540 the set of virtual numbers or manipulated CLI could optionally be a mix of re-used and unused numbers, non-consecutive numbers, and numbers from multiple geographical areas in the case of a fixed line network or multiple network prefixes in the case of mobile networks. Another mechanism is regular renewal of the set of virtual numbers 81 or manipulated CLI in use or dividing the set of virtual numbers 81 or manipulated CLI in subsets of virtual numbers that are used consecutively in a rotating order, preferably a randomized rotating order. Still a further mechanism is the randomisation of the usage of virtual numbers or manipulated CLI within a specific set of virtual numbers 81 or manipulated CLI. All these measures make it difficult for an operator to allocate test calling behaviour to specific called parties, calling parties or originating networks as the number of numbers used is sufficiently elevated in order to spread the risk of detection and the systematic calling behaviour of the system 1 according to the invention when making multiple test calls is randomized which makes it more difficult to counter-detect the patterns of the test calling behaviour.

When using a system 1 according to the invention there exists a risk that the bypass 540 operator makes use of the CLIR function such that the system 1 would not be able to guarantee the detection of the presence and/or subsequent disabling of a bypass 540. The signals exchanged between telecommunication networks namely comprise two fields, a CLI field which contains the calling party telephone number and a presentation indicator (PI) which indicates whether the CLI can be shown or not. The PI has three states: "available" means that there is a CLI and it can be shown, "unavailable" means that there is no CLI present and "restricted" means that there is a CLI present, but it cannot be shown. When the bypass 540 operator enables the CLIR function for the subscriptions the bypass 540 makes use of, the last switch in the path will not pass on the CLI to the terminating subscription used in the receiver probe 20. A more detailed description of the CLIR function can for example be found in the ITU CCITT I.251.4 specification or the 3GPP TS 24.081 specification.

Therefore the system according to the invention makes use of a receiver probe 20 that comprises a terminating subscription 80 configured with a calling line identification restriction override (CLIRO) function. This is a feature implemented in the equipment of the telecommunication network 50. The feature will instruct the final switch in the path of the test call to ignore the PI if it is set to "restricted" and still pas on the CLI to the terminating subscription of the receiver probe 20. Then, even if the bypass 540 makes use of a CLIR function the receiver probe 20 will always be able to detect the CLI of the incoming test call. This will enable the system 1 to detect and/or subsequently disable the specific subscriptions that are in use in the bypass 540.

Once a virtual number 81 or a manipulated CLI is blacklisted by a bypass operator it is advantageous to replace it with a new virtual number 81 or a new manipulated CLI. However before this can be accomplished one must first be able to detect that the virtual number 81 or the manipulated CLI was blacklisted by a bypass operator. Therefore, according to an advantageous embodiment of the invention there is provided a method for detecting that a virtual number of a system was blacklisted by a bypass operator. In a first step of this method there is set a predetermined time period for monitoring certain events as will be explained below in further detail. This predetermined time period could for example be one or more days. Further there is also set a predetermined blacklist threshold rate, which will also be explained further below. Subsequently a specific virtual number is selected from the non-cascaded set of virtual numbers 81 that is in use by the system 1 according to the invention. For this selected virtual number there is now determined the cumulated amount of bypasses as detected by system 1 during the predetermined time period, for example during one day. Further there is also determined for this selected virtual number the cumulated amount of test calls analysed by the system 1 during this same time period, as in the example during that same day. Based on the form determinations subsequently there is calculated a bypass detection rate. This bypass detection is calculated as the ratio between the cumulated amount of bypasses that were detected during that day, for example forty and the cumulated amount of test calls analysed during that day, for example one thousand, both of course for the selected virtual number, which in the example would lead to a bypass detection rate of $40/1000=0.04=4\%$. Finally it is determined that this selected virtual number was blacklisted by a bypass operator when the bypass detection rate is lower than the predetermined blacklist threshold rate. So if in the example the predetermined blacklist threshold rate was set to 5% then according to this method this would signal the selected virtual was blacklisted by a bypass operator as the bypass detection rate of 4% is lower than the blacklist threshold rate of 5%. This predetermined

blacklist threshold rate can be set based on experience of the operator of the system 1 according to the invention and can be chosen for example in function of the specific routes along the telecommunication networks being used during the test calls, the time during the day, the day during the week, specific holiday periods and so on. However according to an advantageous method the predetermined blacklist threshold rate is calculated in function of the average bypass detection rate as determined for the other virtual numbers comprised within the non-cascaded set of virtual numbers in use by the system 1 according to the invention. For example, if the bypass detection rate for all these virtual numbers would average to 8%. The predetermined blacklist threshold could be calculated in function of this average, for example as 125% or 150% of this average, which would then for example be 10% or 12% respectively.

It is clear that the aforementioned method can also be applied to any plurality of selected virtual numbers from the set of virtual numbers 81 as in use by the system 1 according to the invention.

According to a further embodiment an equivalent method can be applied to one or more manipulated CLI's as in use by the system 1 according to the invention, or any suitable combination of a selection of one or more manipulated CLI's or one or more selected virtual numbers.

Finally according to a further embodiment of the invention there is also provided a method for replacing the virtual number or manipulated CLI of a system according to the invention after detection that this virtual number 81 or manipulated CLI was blacklisted by a bypass operator as explained above. This method comprises the subsequent step of replacing the blacklisted virtual number 81 or manipulated CLI by means of a virtual number 81 that is not yet comprised within the non-cascaded set of virtual numbers 81 or set of manipulated CLI's as in use by the system 1 according to the invention.

Although the present invention has been illustrated by reference to specific embodiments, it will be apparent to those skilled in the art that the invention is not limited to the details of the foregoing illustrative embodiments, and that the present invention may be embodied with various changes and modifications without departing from the scope thereof. The present embodiments are therefore to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the appended claims rather than by the foregoing

- 19 -

description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein. In other words, it is contemplated to cover any and all modifications, variations or equivalents that fall within the scope of the basic underlying principles and whose essential attributes are claimed in this patent application. It will
5 furthermore be understood by the reader of this patent application that the words "comprising" or "comprise" do not exclude other elements or steps, that the words "a" or "an" do not exclude a plurality, and that a single element, such as a computer system, a processor, or another integrated unit may fulfil the functions of several means recited in the claims. Any reference signs in the claims shall not be construed as limiting the respective claims concerned. The
10 terms "first", "second", third", "a", "b", "c", and the like, when used in the description or in the claims are introduced to distinguish between similar elements or steps and are not necessarily describing a sequential or chronological order. Similarly, the terms "top", "bottom", "over", "under", and the like are introduced for descriptive purposes and not necessarily to denote relative positions. It is to be understood that the terms so used are interchangeable under
15 appropriate circumstances and embodiments of the invention are capable of operating according to the present invention in other sequences, or in orientations different from the one(s) described or illustrated above.

20

25

30

CLAIMS

1. A system (1) for detection of a bypass (540) of an interconnect (30) to a
5 telecommunication network (50) under test, said system (1) comprising:

- means (10) adapted to originate a test call to said telecommunication network (50) under test from outside the telecommunication network (50) under test;

- at least one receiver probe (20) with a terminating subscription (80) for terminating said test call; and

10 - a control system (40) configured to:

- initiate the test call;
- receive from the receiver probe (20) call information comprising a received calling line identification (CLI) of the test call; and
- analyse the received calling line identification (CLI) such that presence of the bypass
15 (540) can be detected,

CHARACTERIZED IN THAT

- said system (1) further comprises:

- a non-cascaded set of virtual numbers (81) being configured such that said test calls are terminated in one stage on said terminating subscription (80); and

- 20 • means (11) configured to manipulate calling line identifications (CLI), and in that

- said control system (40) is further configured:

- to use said non-cascaded set of virtual numbers (81) as called party of said test calls; and
- to set up test calls towards said set of virtual numbers (81) from said means (11)
25 configured to manipulate calling line identifications (CLI) through said means (10) to originate a test call.

2. A system according to claim 1, wherein said means (11) configured to manipulate calling line identifications (CLI) comprise:

30 - end user subscriptions with the possibility to manipulate CLI; or

- a call generator connected to a telecommunication network on a network level.

- 21 -

3. A system according to claim 1 or 2, wherein said means (10) to originate a test call comprises said means (11) configured to manipulate calling line identifications (CLI).

5 4. A system according to claim 1 or 2, wherein said means (11) configured to manipulate calling line identifications (CLI) route test calls through said means (10) to originate a test call.

10 5. A system according to claim 4, wherein the means (10) for originating said test call comprise an originating subscription (90) to an originating network (190) outside the telecommunication network (50) under test, that is configured to be routed to said virtual numbers (81), and wherein test calls are set up from said means (11) configured to manipulate calling line identifications (CLI) with different calling line identifications (CLIs) to said originating subscription (90) for enabling test calls routed through the originating network (190) but not necessarily generating a calling line identification (CLI) identifying the originating network (190).

15 6. A system according to any of the preceding claims, wherein said non-cascaded set of virtual numbers (81) is implemented as:

- multiple Subscriber Number options on single physical ISDN BRI fixed line;
- multiple PBX numbers on a single physical ISDN PRI line;
- multiple Mobile Subscriber Integrated Service Digital Network numbers on a single physical SIM card subscription; or

multiple numbers routed to a single IMSI (International Mobile Subscriber Identity) by means of the routing table.

25 7. A system according to any of the preceding claims, wherein said set of virtual numbers (81) comprises one or more of the following:

- re-used and unused numbers;
- non-consecutive numbers; and
- numbers from multiple geographical areas in the case of a fixed line network or multiple network prefixes in the case of mobile networks.

30

8. A system according to any one of the preceding claims, wherein said set of virtual numbers (81) or manipulated CLI is renewed regularly.

9. A system according to any of the preceding claims, wherein said set of virtual numbers (81) or manipulated CLI is divided in subsets that are used consecutively in a rotating order.

5 10. A system according to claim 9, wherein said rotating order is randomized.

11. A system according to claim 9 or 10, wherein usage of virtual numbers (81) within said subsets of virtual numbers (81) is randomized.

10 12 A system according to any one of the preceding claims, wherein said terminating subscription (80) is configured with calling line identification restriction override (CLIRO).

13. A method for detecting that a virtual number of a system according to any of the preceding claims was blacklisted by a bypass operator, comprising the steps of:

- 15 • setting a predetermined time period;
- setting a predetermined blacklist threshold rate;
- selecting a specific virtual number from said non-cascaded set of virtual numbers (81)
- determining the cumulated amount of bypasses detected by said system during said predetermined time period for said selected virtual number;
- 20 • determining the cumulated amount of test calls analysed by said system during said predetermined time period for said selected virtual number;
- calculating a bypass detection rate as the ratio between said cumulated amount of bypasses detected and said cumulated amount of test calls analysed for said selected virtual number; and
- 25 • determining that said selected virtual number was blacklisted by a bypass operator when said bypass detection rate is lower than said predetermined blacklist threshold rate.

14. A method according to claim 13, characterised in that said predetermined blacklist threshold rate is calculated in function of the average bypass detection rate as determined for the
30 other virtual numbers comprised within said non-cascaded set of virtual numbers.

- 23 -

15. A method for replacing a virtual number (81) of a system according to any of the preceding claims after detection that said virtual number (81) or said manipulated CLI was blacklisted by a bypass operator according to claim 13 or 14, comprising the subsequent step of replacing said blacklisted virtual number (81) by means of a virtual number (81) that is not yet
5 comprised within said non-cascaded set of virtual numbers (81).

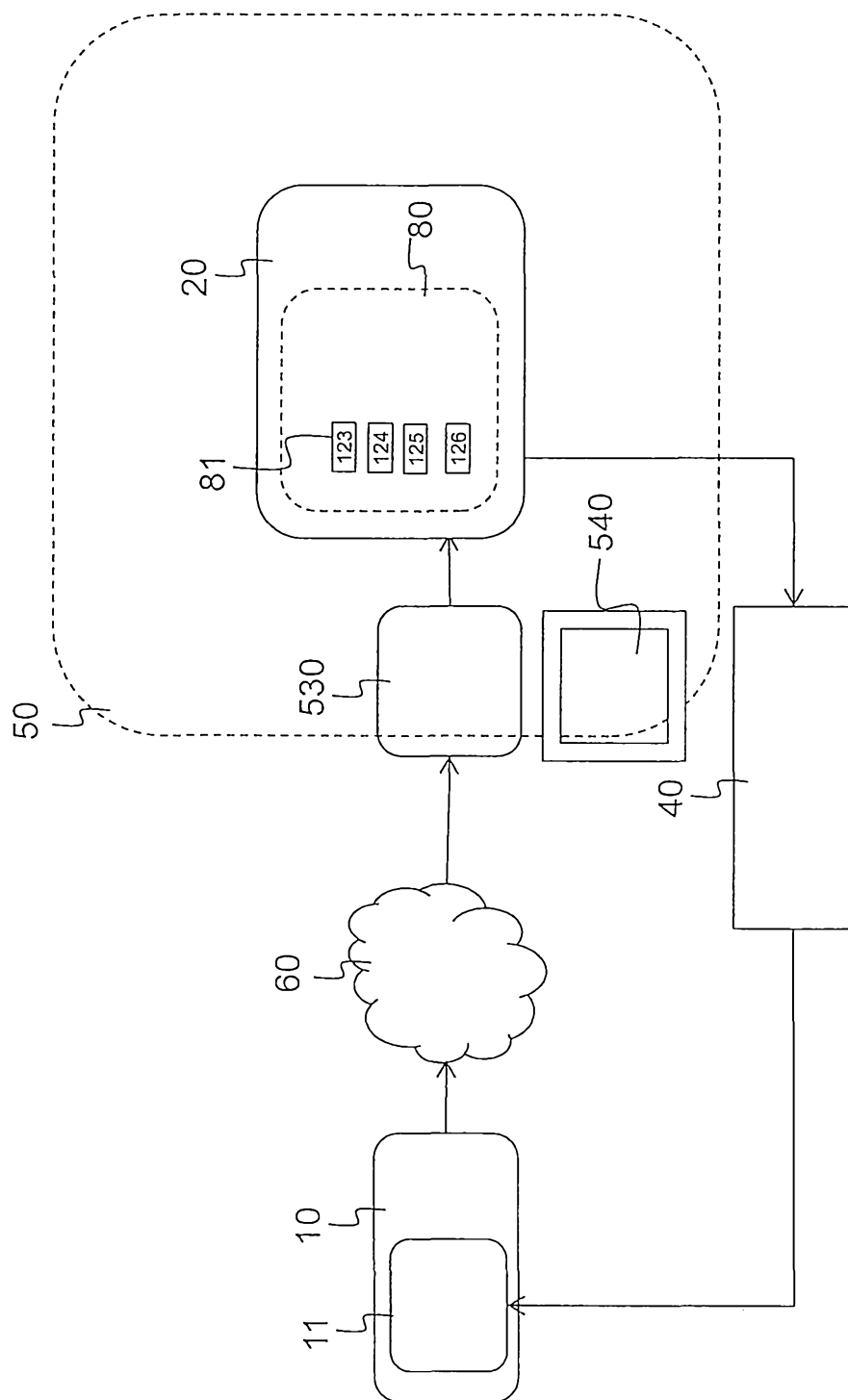


Fig. 1

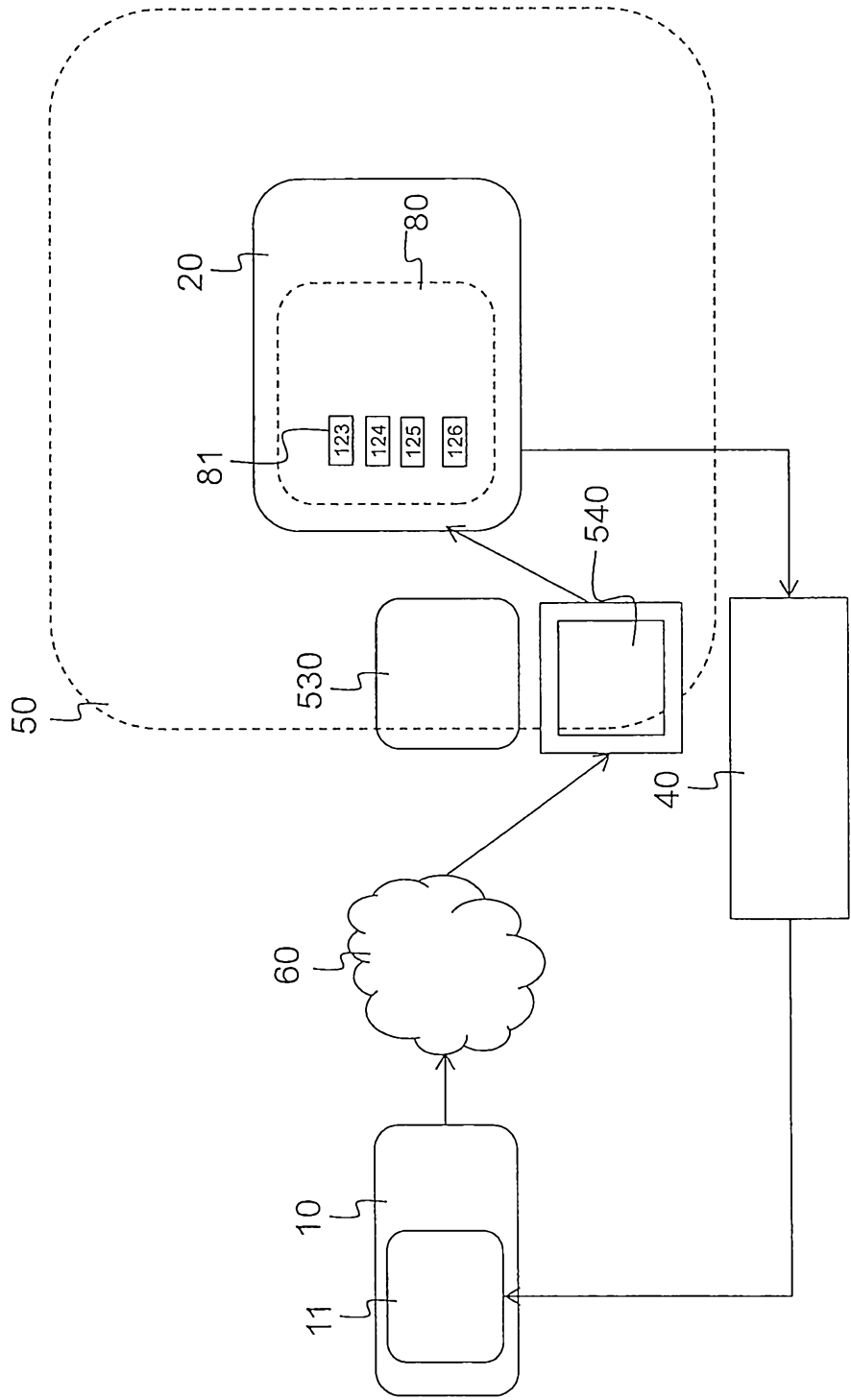


Fig. 2

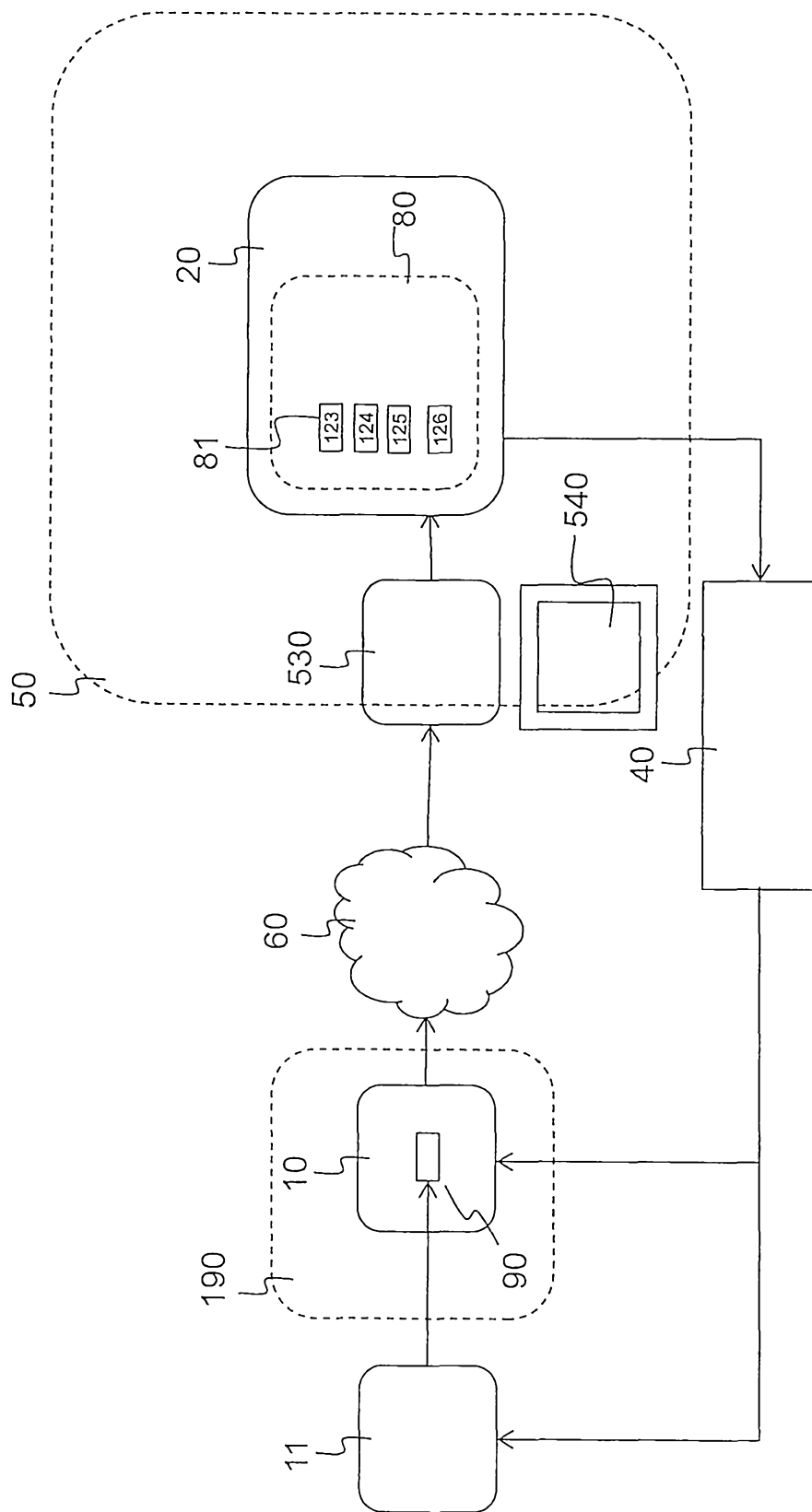


Fig. 3

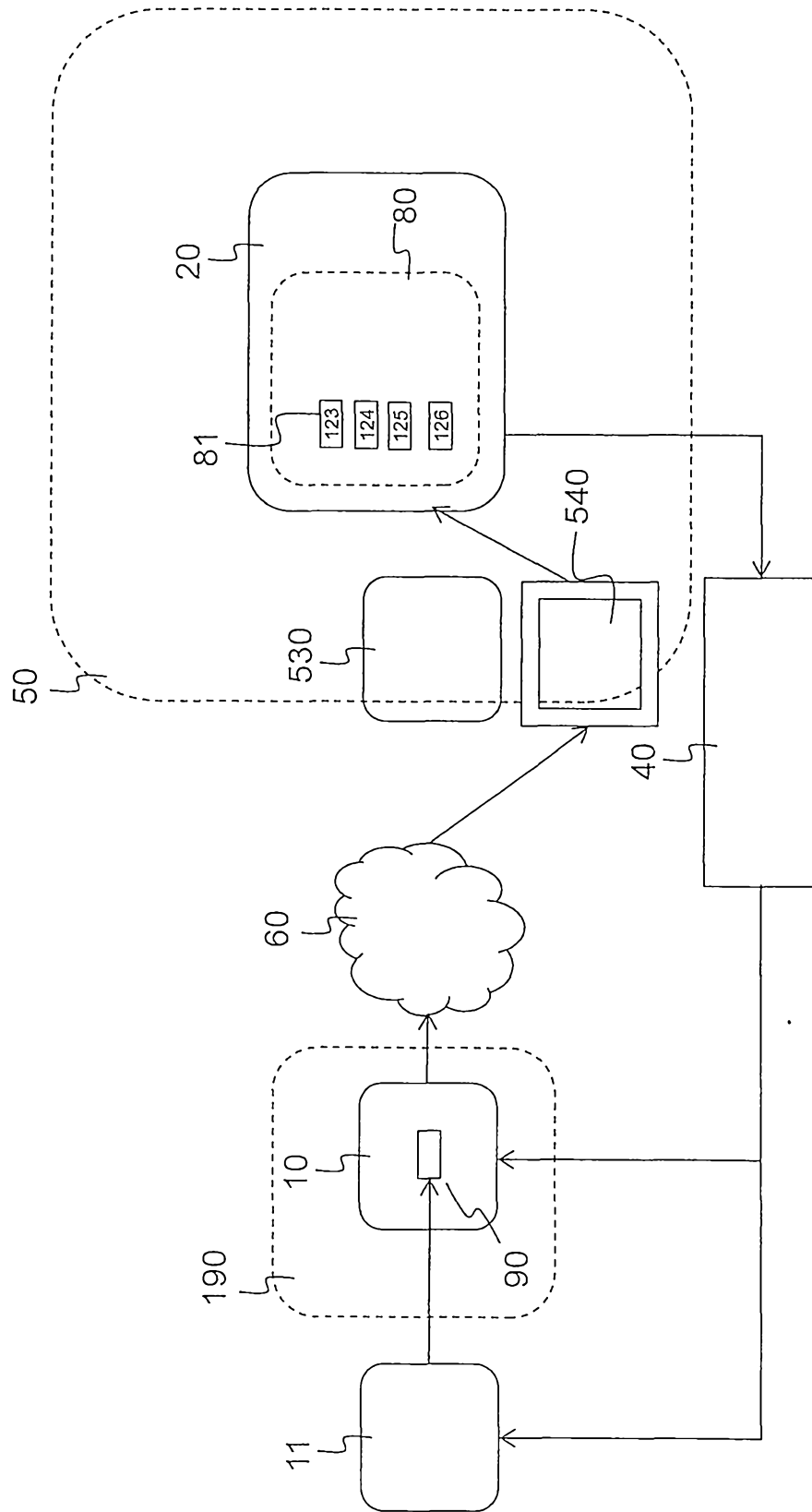


Fig. 4