Title: LOCAL USAGE MONITORING AND FRAUD DETECTION FOR MOBILE COMMUNICATION NETWORKS

Abstract: Fraud detection provided on a mobile handset for a radio network, allows detection to take place immediately. User behaviour is recorded within the SIM card of the mobile handset, by building a subscriber signature. Fraud detection techniques can be applied to this usage data. The location of the usage can be determined, e.g., by determining cell identity in a cellular system, or network identity for roaming usage. If the usage is identified as potentially fraudulent, action can be taken such as locking the handset. Use can thus be restricted to particular predetermined locations. Fraud can be deterred since much fraud involves use at locations far from the user’s home cell. User behaviour can be captured by recording and maintaining call data such as call duration and destination. The dialled numbers can also be checked against a list of “hot” numbers, numbers known to the operators as suspicious.
Local Usage Monitoring and Fraud Detection for Radio Communication Networks

Related Patents
This application relates to US patent 5,966,650 entitled “Detecting mobile telephone misuse”, and US patent 6,038,555 entitled “Generic processing capability” hereby incorporated by reference in their entirety.

Field of the invention
The invention relates to handsets for radio communication networks such as cellular telephony networks, to removable cards such as SIM cards for such handsets, to methods of using such handsets, to methods of detecting fraudulent use of a handset, to methods of maintaining fraud detection, to management systems for fraud detection, to methods of charging for handset usage, to methods of maintaining a usage monitoring system for monitoring use of a handset used as part of a radio communication network, and to a management system for maintaining a usage monitoring system.

Background
Mobile telephony fraud has been widespread since the initial expansion of mobile phone usage. The telephone operators and handset manufacturers have put into place many security measures, fraud prevention measures and fraud detection measures. These include the use of identification codes such as IMSI (International Mobile Subscriber Identity) and IMEI (International Mobile Equipment Identity) (IMSI and IMEI were not designed primarily for fraud detection but more for subscriber and handset identification needs) and the deployment of fraud detection systems based on rules and thresholds and neural network technologies to monitor subscriber usage. Currently fraud detection systems typically use mediation data from the operator’s billing system to analyse user behaviour, construct subscriber signatures and apply fraud detection software techniques to identify potentially fraudulent use. They also take other streams of data from the network operator such as SS7, customer care and billing for
example – the essence is that network operators are having to feed single or multiple
data sources into a centralised system – even if this system is distributed.

One of the difficulties with usage monitoring is the time taken to positively identify
fraudulent usage and de-activate the phone. During this time a significant amount of
usage could have taken place resulting in a significant revenue loss to the operator. It is
in the operator’s interest to identify fraud at the earliest stage possible to minimise the
substantial revenue losses occurred.

A useful summary of some different types of fraudulent use, and a detection system is
shown in US patent 5 734 977. It is known to provide fraud detection systems for
detecting anomalous usage patterns from call detail records. These are processed at a
central location and suspicious activity is alerted to operators who can decide what
action to take. There is a heavy processing load for this central location, dealing with
thousands or millions of subscribers, and a delay involved in passing CDRs to this
location. Hence response times are typically hours. Also, detection event scenarios use
algorithms or rules that cannot be tailored to individual subscriber behaviour without a
huge and impractical processing load or processing delay.

It is also known from US patent 5 655 004 to attempt immediate detection and refusal
of fraudulent calls, while permitting continuing service to the legitimate user by
authenticating a request for communication service between a mobile communication
device, e.g., a cellular telephone, and a recipient. In particular a request for service
message includes an identification code specific to the mobile communication device
and a transmitted authentication code which represents a cumulative total of the prior
usage of the mobile communication device is received from the mobile communication
device at a central processing facility. The transmitted authentication code is compared
to a stored authentication code for the mobile communication device and
communication is initiated between the mobile communication device and the recipient
if the transmitted authentication code and the stored authentication code match.
Another US patent, 6,295,446 aims at defeating cloned cellular telephone operations including those using stolen PINs (Personal Identification Numbers). The mobile Station (MS) has a nonvolatile memory to store an electronic identification number and a first calling event table. The apparatus also includes a MSC (mobile service centre) or HLR (home location register) having a second calling event table that contains a mirror image of the first calling event table, as long as no fraud has occurred. The first and second calling event tables contain identifying information for MS calling activity, such as outgoing call information, which may comprise a called number, a call time, a call duration, and/or a call date. The first and second calling event tables are updated with each outgoing call, and authorization to make future calls is based on conditioned correspondence between the information contained in each calling event table.

However, such arrangements still involve the cost of a central facility, and the delay and cost of sending information to and from the central facility, to reach a decision on fraudulent activity, then de-activate the phone. During this time, a significant amount of usage could have taken place, resulting in significant revenue loss to the operator.

It is also known to provide mobile handsets capable of requiring a PIN to be entered before calls are allowed. An example is shown in US patent: 6,338,140, intended as a defence against cloning. However, this remedy is inconvenient and unpopular with users. US patent: 6,321,339 shows a system for authentication of network users and issuing a digital certificate. This requires users to ESN (Electronic Serial Number) or provide identification information. The user is presented with a hierarchy of queries to ensure identity. US patent 6,223,290 shows a method for preventing the fraudulent use of a cellular telephone. This involves programming a unique code into an auxiliary memory which is compared to at least one component code. The idea is to link the telephone memory, the telephone hardware and the micro-controller to prevent cloning by locking the hardware to a particular provider. This can prevent (successful) modification of ESN (Electronic Serial Number) or IMEI.

US patents 6,198,915 and 5,625,669 show a mobile phone with internal accounting. This allows call value to be calculated by use of an accounting program. The user is
alerted to account status. The phone can decrement a debit account or calculate an account charge on demand. It also shows activating, updating and programming a new phone remotely.

**Summary of the Invention**

It is an object of the invention to provide improved apparatus or methods addressing these issues.

According to a first aspect of the invention, there is provided a mobile handset for use as part of a radio communication network, the handset having a monitor arranged to monitor usage of the handset and a detector arranged to determine if such usage is fraudulent.

This has a number of advantages over conventional centralised systems. Fraud detection can be quicker if carried out at source, where the usage information originates, that is, the handset. The detector can look at usage such as calls still in progress or undertake immediate analysis after call completion. There is less delay and less communications overhead if there is no need to transmit usage information to a centralised fraud detection arrangement. Any remedial action following the detection, can be implemented with less delay. Such remedial action can include locking the handset, or sending an indication (e.g. by SMS) to inform the operator (via an application management component of interesting behaviour which may pertain to fraud. Notably, the detection can be tailored more easily to individual users or groups of users if the detection is carried out locally at the handset, resulting in more accurate detection.

Costs of implementing and running the fraud detection can be reduced since the detection processing no longer needs a large central processing facility with expensive communications links and interfaces to complex billing systems. This also means the solution is inherently more scalable as numbers of subscribers increase and as types of activity increase with the increase in use of revenue based services such as WAP, permanently-on services using GPRS and future 3G network services like EMS and MMS. Fraudulent usage is intended to encompass any usage for which the
corresponding revenue is not collected for any reason. This can include calls not properly billed, as well as calls billed but not paid.

As a dependent claim feature, the handset is arranged as part of a distributed processing network fraud management system. This can enable improved detection compared to a completely centralised or a completely autonomous arrangement. The advantages of both can be combined. Average patterns of many users usage over the network can be built up, yet still be personalised to each user, on a time of day and day of week basis, for example.

Another dependent claim feature is a lock for preventing further usage in the event of the detector determining fraudulent (including inappropriate) usage. This can also act as a trigger mechanism which may lock the phone when interesting events have been recognised. This can enable quicker reaction to fraud detection, than a network based lock. Also, it enables the logistical difficulty and delay of preventing use on other operators’ networks to be avoided.

Another dependent claim feature is sending an indication to a network operator in the event of the detector detecting unusual usage such as fraudulent or inappropriate usage. This can enable an operator to take appropriate action, such as closer monitoring, or prompting the user for authentication, or warning the user that a lock will be activated. The indication can be carried by a message service, including SMS, EMS, MMS, email or others. An advantage of a message service over network signalling type solutions is that it can be easier to implement, requiring no interface into complex network management or billing systems. Also it can be faster and more efficient, especially across many networks. This addresses the common problem of roaming fraud where mobile phone usage on other operators’ networks may not be identified for some time due to common time lag of days or weeks in call records reaching the home operators (Home Public Land Mobile Network) (HPLMN) mediation system.

Another dependent claim feature is the monitor or the detector being adaptable by means of a message sent from a network operator -. Amongst other advantages, this
can enable the handset to be upgraded remotely. Also thresholds or other parameters
can be adjusted if fraud is not being detected accurately, to reduce inconvenience to
users, or to reduce inconvenience to operators.

5 Another dependent claim feature is the monitor having an aggregator for aggregating
current usage information into a current signature. This can enable easier processing of
the usage information, if it is summarised or standardised. The limited processing and
storage resources of the handset can thus be used more efficiently.

10 Another dependent claim feature is the detector being arranged to detect anomalous
usage by comparing the current signature with a typical signature representing usage
over a long period. This can enable various types of fraud to be detected quickly and
accurately.

15 Another dependent claim feature is the monitor being arranged to adapt the typical
behavioural signature with the current usage information. This can enable the detection
accuracy to increase with time and each SIM card having an accurate view of the
individual behavioural characteristics of usage of Network services.

20 Another dependent claim feature is the detector being arranged to compare the current
usage to thresholds of levels of activity. This is a particularly useful indicator of fraud.
It can be one of several detection methods. A particularly useful method involves a
combination of behavioural detection over a period of time and detection of current
activity, also termed event based detection. The usage usefully includes both incoming
calls and messages, and outgoing activity. Even if such incoming activity is not itself
fraudulent, it can be an indication or predictor of fraudulent outgoing activity.

Another dependent claim feature is the detector being arranged to compare the current
usage to predetermined activities categorised as fraudulent. These activities can include
calling predetermined numbers or countries or premium rate numbers for example. This
can be used in addition to other detection methods.
Another dependent claim feature is the detector being arranged to be adjustable remotely by a network operator. This can enable detection sensitivity to be adjusted, or thresholds or hot list numbers or categories to be updated for example.

The monitor and detector can be in the form of software. The monitor and the detector can be implemented on a removable card. This could be for example a SIM card, or a Java card for the 2.5G or 3G environment where usage includes data service usage and transactions.

Another aspect of the invention provides a removable card for a handset for use as part of a radio communication network, the removable card having a monitor arranged to monitor usage of the handset and a detector arranged to determine if such usage is fraudulent.

This reflects that cards such as SIM cards can be the most valuable part of a handset, and may be a separately tradeable commodity, suitable for use with handsets from many manufacturers. The term monitor is intended to encompass monitors arranged as part of a hybrid solution with some of the processing being based in the handset and some in the network.

Another aspect of the invention provides a method of using a mobile handset suitable for use with a radio communications network, the handset having a fraud detector, the method having the step of:

- using the handset to communicate over the radio communications network, following activation of the fraud detector, such usage being monitored by the fraud detector.

This aspect, concentrating on the actions of the subscriber, could be particularly useful if the subscriber is the only party within the jurisdiction of the patent, for example.

Another aspect of the invention provides a method of detecting fraudulent use of a handset used as part of a radio communication network, the handset having a fraud detector, the method having the steps of:
monitoring usage of the handset, in the handset, and
determining in the handset if such usage is fraudulent.

This corresponds to the apparatus aspects, and may be particularly useful if there is
more value in the use of the apparatus, in service, than in the selling value of the
apparatus.

Another aspect of the invention provides a method of offering a fraud detection service
for detecting fraudulent use of a handset used as part of a radio communication
network, the handset having a fraud detector, the method having the steps of:
receiving from a subscriber, a request for service activation, and
sending a message to the handset to cause the detector to detect fraudulent use.

This aspect, concentrating on the actions of the operator, could be particularly valuable
if the benefits to the operator are large compared to the value of the individual handsets.
An advantage of handset based fraud detection is the ease with which it can be activated
or de-activated for each subscriber, either by activating software installed at
manufacturing time on the handset card, or conceivably by downloading the appropriate
software to the handset card when the handset card is already in the field or in service.

Another aspect of the invention provides a method of maintaining a fraud detection
service for detecting fraudulent use of a handset used as part of a radio communication
network, the handset having a fraud detector, the method having the steps of:
maintaining a record of which handsets have fraud detectors, and
remotely updating the fraud detectors in one or more of these handsets.

This aspect, also concentrating on the actions of the operator, could be particularly
valuable if the benefits to the operator are large compared to the value of the individual
handsets. Notably, the updating can be more easily tailored to individual usage patterns
without an impractical amount of processing or storage capacity being required, since
the detectors are handset based, rather than being centralised.
Another aspect of the invention provides a method of maintaining a fraud detection service for detecting fraudulent use of a handset used as part of a radio communication network, the handset having a fraud detector, the method having the steps of: receiving an indication that a handset has been locked by the fraud detector, and remotely unlocking the handset if the use is not fraudulent.

This aspect, also concentrating on the actions of the operator, could be particularly valuable if the benefits to the operator are large compared to the value of the individual handsets. Notably this helps to overcome the possible risk of inconvenience to subscribers from false fraud detections. Remote unlocking is intended to encompass sending an unlock code for the subscriber to enter into the handset to unlock it.

Another aspect of the invention provides a management system for offering a fraud detection service for detecting fraudulent use of a handset used as part of a radio communication network, the handset having a fraud detector, the system having: an interface arranged to receive from a subscriber, a request for service activation, and a processor arranged to send an indication to the handset to cause the detector to detect fraudulent use.

This aspect is a system corresponding to one of the above methods.

Another aspect of the invention provides a management system for maintaining a fraud detection service for detecting fraudulent use of a handset used as part of a radio communication network, the handset having a fraud detector, the system having: a record of which handsets have fraud detectors, and a processor arranged to remotely update the fraud detectors in one or more of these handsets.

This aspect is a system corresponding to one of the above methods.
Another aspect of the invention provides a management system for maintaining a fraud detection service for detecting fraudulent use of a handset used as part of a radio communication network, the handset having a fraud detector, the system having: an interface for receiving an indication that a handset has been locked by the fraud detector, and a processor arranged to send a command to remotely unlock the handset if the use is not fraudulent.

This encompasses sending an unlock code to the user. This aspect is also a system corresponding to one of the above methods.

Another aspect of the invention provides a mobile handset having a lock for preventing use, and a lock controller for activating the lock based on monitored usage.

An advantage of the lock being in the handset rather than in the network, is that it can prevent the handset card being used with other networks. Also, it can enable the use to be prevented more quickly than conventional centralised network based usage prevention. The monitoring and detection in this case can be local or centralised or a hybrid of the two.

A dependent claim feature is the activation being dependent on the location of the handset. An advantage of location dependence is that it can help deter theft, or limit the revenue loss. This is particularly the case for mobile handsets or SIMs that are fraudulently recycled for use on other networks perhaps in different countries. A handset based solution is much more cost effective than maintaining network based lock out since there are so many networks around the world.

Another dependent claim feature is the handset being for use with a cellular network, being arranged to determine location by identifying which cell the mobile is in. This can enable more efficient fraud prevention by locking out or limiting calls made from particular cells, or only allowing calls in specified cells where the user is likely to be.
Another dependent claim feature is the handset being adjustable remotely by a network operator. This enables updating to alter the locations, or the sensitivity of any monitoring or fraud detection for example. This can make the arrangement much more user friendly.

Another aspect of the invention provides a mobile handset for use as part of a radio communication network, the handset having a monitor arranged to monitor and record usage of the handset.

There are many advantages of monitoring in the handset rather than the conventional arrangement of monitoring in the network. Cost can be greatly reduced if the monitoring in the handset enables the monitoring to be carried out without major modification to the complex, expensive network signalling, management, or billing systems. The usage information can be used for a variety of purposes, including fraud detection, other revenue assurance activity such as for marketing purposes and other customer relationship management (CRM) activities.

Another dependent claim feature is sending information relating to the monitored usage to a network operator using a message service. This can enable the network operator to have near real time information about usage more directly, without having to rely on conventional signalling networks or billing systems. Particularly for roaming, meaning usage on other networks than the user’s home network, there could be a considerable delay of hours, or days before the home network is made aware of such usage. For applications such as fraud prevention, or location based services, it can be valuable to have more up to date usage information. A high risk or identified group or individuals that are roaming across networks, can be monitored more closely. Using a hybrid of centralised and distributed technologies, their handsets can monitor and inform a centralised network fraud detection manager in real time when the roamers are behaving suspiciously.

Another dependent claim feature is an aggregator for aggregating and storing in the handset an aggregated profile of the usage. There are a number of advantages of doing
this in the handset rather than elsewhere in the network. The information can be condensed to reduce communication costs. There is less need for a large central processing facility with expensive communications links and interfaces to complex billing systems. This also means the solution is inherently more scalable as numbers of subscribers increase.

Another aspect of the invention provides a method of charging for handset usage, the charging being dependent on whether the handset has active fraud detection.

An advantage of this is that if the fraud detection is local, in the handset, it can be made more visible to subscribers, and can be selectively activated more easily than a centralised system. Thus it is easier for the operator to convince subscribers that it brings added value and so is worth an extra fee. Thus revenue can be increased. Alternatively, if revenue increases sufficiently by the reduction in fraud, or other revenue loss, the operator can opt to offer a discount to subscribers to activate the fraud detector, to encourage more to do so. The better scalability of the local handset based detection makes this more feasible.

Another aspect of the invention provides a method of charging for handset usage, the charging being dependent on whether the handset has active usage monitoring.

Similar advantages apply to such usage monitoring as to fraud detection. Potentially, if such usage information can be valuable for marketing purposes, it could be sold on, with the user’s permission, and the users could be offered a discounted charging scheme. This has benefits for the user and the operator.

Another aspect of the invention provides a method of maintaining a usage monitoring system for monitoring use of a handset used as part of a radio communication network, the handset having a usage monitor, the method having the steps of: maintaining a record of which handsets have usage monitors, and receiving usage information from these handsets.
An advantage of this is that the local aggregation of such information can reduce the amount of processing and communication overhead compared to a centralised solution. Also, it can reduce the need for expensive interfaces to complex installed systems, such as billing systems, yet can produce extremely valuable information about subscriber behaviour. As above, it is more scalable than a conventional centralised system.

Another aspect of the invention provides a management system for maintaining a usage monitoring system for monitoring use of a handset used as part of a radio communication network, the handset having a usage monitor, the system having:

a record of which handsets have usage monitors, and

a processor arranged to receive usage information from these handsets. This corresponds to the above method.

Another aspect of the invention provides a removable card as set out above and having an aggregator for aggregating current usage information into a signature.

Another aspect of the invention provides a removable card for a handset for use as part of a radio communication network, the removable card having software arranged to monitor usage of the handset and for storing in the handset a signature summarising the usage.

Another dependent claim feature is software arranged to detect anomalous usage by comparing a short term usage with the signature representing usage over a longer period. Another dependent claim feature is software arranged to update the signature with current usage information. Another dependent claim feature is software arranged to use the signature for revenue assurance purposes. Another dependent claim feature is software arranged to use the stored signature to send usage information from the handset to an operator of the network to enable services to the user to be tailored according to the usage information. Another dependent claim feature is the removable card being arranged to receive software updates when installed in the handset, sent by an operator of the network over the network. Another aspect is software for storing on a removable card for implementing the above features. Another aspect is a mobile handset having the removable card having any of the above features.
Advantages of the various aspects of the invention and optional features set out above include the following considerations:

a). Scalability: Unlike Moore's Law referring to CPU power (doubling every 2 years), online storage is not increasing in the same proportions, therefore centralised fraud management approach will eventually become too cost restrictive for all but the top few operators due to the increasing online storage requirements per subscriber as more and more revenue delivering services are provided.

b). Monitor at Source: Fraudulent calls are made by the mobile handset therefore the best place to detect and prevent these calls is on the handset in real-time not later after the call records (CDR's) have been collected, converted and distributed to up-stream back office systems run by the operator.

c). Exploit existing unused processing resource: Today's generation of mobile phones possess enough computing power to provide a whole host of services and features (calender, address books, email, SMS, EMS/MMS). Tapping into a small percentage of this computing power can enable monitoring of the usage patterns of the legitimate owner and prediction of future calling habits, with little or no effect on other applications.

d) Tailored Service: rather than centrally trying to monitor and predict every single subscriber's usage patterns and future calling habits, the empowered handset is devoting its entire resources to one single subscriber. With the aid of the operator tagging the subscriber with a single class of subscription (pre-paid, post-paid consumer, post-paid business etc) the solution is tailored and targeted to one market arena with its own unique thresholds and particular rules (e.g. pre-paid customers do not frequently roam, but may have higher rate of SMS usage than post-paid business). This can reduce any potential false positives that could be generated by a centralised approach and can increase the success rate of fraud prevention.
e) Global Solution: - By utilising the GSM based SIM Card and the industry standard SIM Toolkit for developing the software, embodiments of the invention can work in all of today's handsets without the need for unique distributions being required for each mobile handset manufacturer.

f) Ease of deployment – Embodiments of the invention can be included into every SIM Card during the operators' point-of-sale (manufacturing) process. Later using Over-The-Air Activation, the service can be remotely enabled either at the subscriber's wish or the operators' demands.

g) New Service Support - When operators launch new services, the signatures and class of subscription can be updated and remotely sent over the air to enabled handsets, thus allowing new services protected or new hot spots guarded.

h) Customer Loyalty Protection - Rather than annoy high revenue subscribers, new services can be tagged with warning status rather than lock status to allow the operator to centrally decide whether this subscriber is actually performing fraud or just making unforeseen calling patterns and exceeding thresholds as the new service increases its associated market penetration.

i) Brand Recognition: Subscribers will be more inclined to select handsets from operators which boast this mobile fraud detection/prevention solution, knowing full well that if their handset is lost or stolen at the first attempt of fraud the handset will be locked and they will not be liable to any call charges that the operator may wish to apply to fraudulent usage.

j) Portability: For embodiments using software located on the SIM Card, when a subscriber updates the handset they automatically take the software with them. As no handset can be used without a SIM Card, any fraud protected handset will require an alternative SIM card (and alternative operator/billing contract) if the original SIM Card is removed.
k) CRM (customer relationship management)- optionally calling patterns can be sent from the handset to the operator, allowing current usage trends to be monitored, and future service trends to be forecast, which can lead to better tailoring of services to suit users and increase revenues.

l) Location Based Services - Usage of the handset in particular geographic locations can be blocked or recorded while at the same time reversing this concept and prevent the subscriber from calling particular locations.

m) Future Proof - The basis for 3G and the forthcoming 4G generation of mobile services is all based upon the highly successful GSM 2G standard. By supporting the core features of the GSM 2G standard and later 2.5G/3G standards, compatibility can be maintained with future standards.

Any of the dependent claim features can be combined with each other and with any of the aspects of the invention, as would be apparent to those skilled in the art. Aspects may be combined together. Advantages other than those set out above will be apparent to those skilled in the art.

Brief Description of the Drawings

Embodiments of the invention will now be described to show by way of example how the invention can be implemented, with reference to the figures, in which:

Fig 1 shows a schematic view of a first embodiment of the invention, with a handset having a monitor and a fraud detector,

Fig 2 shows a schematic view of another embodiment, having a network fraud management system,

Fig 3 shows a schematic view of another embodiment, having a handset arranged to monitor usage,

Fig 4 shows a schematic view of another embodiment, having a handset with a lock,

Fig 5 shows a schematic view of another embodiment, having a handset arranged to send usage information using a message service
Fig 6 shows a schematic view of another embodiment, showing a removable card for a handset.

Fig 7 shows a schematic view of another embodiment, showing steps in activating monitoring,

Fig 8 shows a schematic view of another embodiment, showing steps in detecting fraudulent usage, and

Fig 9 shows a schematic view of another embodiment, showing steps in reactivating a locked handset.

**Detailed Description**

Figure 1 shows a schematic view of a first embodiment of the invention, with a handset having a monitor and a fraud detector, in the context of a typical radio communications network. The network, shown as item 10, can be a GSM or other cellular network, or an IP network running over radio links or cellular telephone links or radio data links such as GPRS (General Packet Radio Service) or 3G networks. A first handset 20 is shown for users to communicate over the network. Other handsets 50 can be conventional handsets or handsets similar to the first handset. The handsets can be PDAs (Personal Digital Assistants) or portable or handheld computers with radio communication capability. The network is shown coupled to other networks 70, which may be radio or terrestrial or any kind. Network management and billing systems 60 are also shown. Conventionally, there are signalling channels to enable the network management system to communicate with base stations around the network, for conventional network management purposes. Such network management systems could have some level of traffic monitoring, at least of levels of traffic at different parts of the network, to identify any congestion problems.

The first handset has a usage monitor 30, and a fraud detection function 40, which uses the output of the usage monitor. The output of the fraud detection function can be used for any purpose, so for clarity, none is illustrated in this figure. The usage monitor can be completely stand alone, or coupled to the network. This can be achieved using the conventional signalling channels, or other methods such as SMS (short message
service) messages. Usage information from many such handsets can be collated in the network, its output can be in any form, but can usefully include a summary of usage over a period of time. An example of this is the behaviour signatures described in more detail below. The output can be used for other purposes as well as for fraud detection.

The fraud detection element can be implemented to use any of various conventional methods. Depending on the processing and memory capabilities of the handset and the desired level of detection, it may be appropriate to use a simpler algorithm or one requiring less processing or memory resource than those typically used for network based fraud detection. An example will be described in more detail below.

Figure 2 shows a schematic view of another embodiment, having a network fraud management system as well as a handset 210 with local detection of fraud (also called "Terminator"™). - The handset can be similar to the first handset of figure 1, or have some other arrangement. It can be used by users to communicate over the network 220, (which can be a similar network to that of figure 1). A control centre 230 is coupled to the network and provides an interface to the network fraud management centre. This has a network fraud detection system 250, fraud analyst workstations 260, and a handset detection management centre 240, to which help desk terminals 270 for the terminator application, are coupled.

This is a hybrid system with the network fraud management system implemented following conventional principles, but adapted to cooperate with the terminator applications, to provide the advantages of fraud detection at local and network levels. The network fraud management system can identify fraudulent behaviour across groups of users, and produce statistics representing "normal" behaviour over large numbers of subscribers, categorised into different types (also called classes) of subscribers. This information can be downloaded in summarised form to the terminator applications on users handsets, to improve accuracy of the local detection. In the other direction, usage information, or potential fraud detections can be fed in real time from the terminator applications to the network fraud system, to improve its accuracy.
Figure 3 shows a schematic view of another embodiment, having a handset arranged to monitor usage. Corresponding reference numerals are used to those in figure 1. In this case, instead of a local fraud detection application in the first handset, a usage store 300 is provided. This enables a summary of the usage to be stored in the handset. This usage can include calls, messages, email usage, data communications, and non-communications usage, e.g. games, calendars, and other applications. This would often be impractical to store in the handset, or transmit from the handset without some type of compression or summarising. An example is the behaviour signature described below, which can be updated continuously.

The usage information can be used for marketing purposes either external, by selling on to others, or internal for use by the operator. It might also be used for network management purposes, or revenue assurance purposes. For example, the usage stored in the handset could be compared to the bill prepared for that user, to identify any anomalies.

Figure 4 shows a schematic view of another embodiment, having a handset arranged to lock the handset to prevent usage. Corresponding reference numerals are used to those in figure 1. Having a local lock 410 rather than merely barring use in the network enables quicker action to prevent fraudulent calls, and prevents use on other networks more easily and effectively. The lock can be implemented by software on a SIM card for the handset. The software would interact with a processor on the handset to bar the use. The details of implementation would vary with different types of handset, but could follow established practice.

A lock controller 400 is shown, again implementable in software on a SIM card for example, for ensuring the lock is activated for the correct criteria, and can be unlocked remotely by the network operator. The controller is also optionally arranged to alert the network operator when the lock is activated. The lock can be activated based on usage, which in this case can be monitored locally or in the network, for example at a base station, an MLC (mobile location controller) or MSC (mobile services switch centre) or
equivalents, or a network management or billing centre. The lock controller is arranged
to communicate with such network elements or external elements by means of a
message service, such as SMS.

Fig 5 shows a schematic view of another embodiment, having a handset arranged to
send usage information using a message service. Corresponding reference numerals are
used to those in figure 1. The handset does not necessarily have a terminator fraud
detector. The usage is monitored by the usage monitor 30. The usage info is sent
onwards by element 500 over the network by a message service, such as SMS. These
elements can be implemented in the form of software on a removable card such as a
SIM card. As with other embodiments, the software can be downloaded or updated
remotely, again using the message service. The usage monitoring can include
monitoring individual calls, or messages, or monitoring trends or patterns of usage over
a period of time, or a combination. It can involve monitoring for unusual usage, and
sending a message in the event of unusual usage, and/or sending a summary of all the
usage. In particular, unusual activity can be deduced from a hybrid of behaviour over a
period of time, and current events. It can involve monitoring both incoming and
outgoing activity.

Fig 6 shows a schematic view of another embodiment, showing a removable card 600,
such as a SIM or Java card for a mobile handset. A memory map 690 shows memory
areas in 5 segments at different memory addresses. At addresses 0 to 16k is free
memory available for software applications. In this case, usage monitoring and fraud
detection applications 680 are located here. These include modules titled “Call Learn”
 ™ 630, “Call-Predict” ™ 640, “Call-Guard”, ™ 650, and “Call Control” ™ 660.

Call learn is an example of a monitor for monitoring usage. It creates and maintains by
updates, one or more behaviour signatures (also called profiles) representing an
aggregate of various parameters of usage over a period of time. These can be
implemented in various ways. An example is shown in US patent 5,966,650 entitled
“Detecting mobile telephone misuse” and hereby incorporated by reference. This shows
the core of user profiling technology and describes the creation of a user signature from
event stream data. The main adaptation required would be a reduction in the number of fields specified to accommodate the limited memory available. A long term signature is formed of an aggregation of 20 to 30 fields, each having a value representing a different parameter of the usage, selected according to the application of the signature and/or the class of subscriber. For example, the fields may have values representing a number or proportion of international calls, or emails, or premium rate calls, or local calls, over the period in question, e.g. several months. A short term signature can also be built up to represent current usage over a number of hours or days. The long term signature can be updated by using the current signature, and producing a type of weighted average of the field values, weighted according to the periods represented, or in the case of fields being time sequences of values, the oldest values can be dropped and new current values added at the other end of the sequence. To meet constrained memory resources of a SIM card for example, the number of fields and/or the precision of the values, can be reduced.

Call Predict is used to detect anomalies by comparing the current signature with the typical or long term signature. The amount of change from the typical can be represented by a behaviour change index. The level of this index which triggers action, can be adjusted according to the class of subscriber, and on an individual basis, to prevent unwanted false detections. Again implementation can follow established principles as shown in US patent 6,038,555 entitled “Generic processing capability” and hereby incorporated by reference. This shows anomaly detection for event streams, and provides a method for measuring change for event streams. The method depends upon the construction of a behaviour profile and provides a proprietary method for the efficient comparison of current activity against some benchmark activity. Once again the main adaptation envisaged would be a simplification of the method to accommodate limited processing capacity.

Call Guard is used in parallel with Call predict as another way of detecting anomalies in usage and thus detecting fraud. In this case, actual call or message attributes are compared to rules, thresholds and hot lists. For example, there could be a threshold of the number of international calls made in a period of minutes or hours. There could be a
threshold of the number of short calls made in a similar period, or the number and duration of calls made to premium rate numbers could be thresholded. Rules can be set for exceeding combinations of lower thresholds, or for calls at unusual times of day for example. Again more details are set out in the above referenced US patent. Comparison with hot lists involves comparing destination addresses for the usage, e.g. phone numbers, email addresses, web site addresses and so on, with addresses known to be related to fraudulent activity. The hot list can also include cell or network identities which are compared to the current cell or network of the handset, to detect if it is outside a prearranged limited area of bona fide usage.

Call control is arranged as a receiver for over-the-air activities (OTA) including processing of Terminator SIM-Updates of hot lists. Call control also maintains and undertakes Network Operator requested adjustments to:

- Hot-List entries
- Rules & Thresholds values including call types
- CRM analysis of Signatures
- Loading new Live and Decayed Signatures

Another task is Alarm (detection) queue management, which includes determining what action to take. Options can include override of the consumer's handset control with a (potentially branded) user interface indicating:

- Terminator Logo/3rd Party Branding
- Message to Consumer indicating fraud detected
- Fraud Code

Another option is to dial automatically, or send an SMS message to a Network Operator Help Desk, to enable the user to verify their identity, or face locking of the handset after a predetermined time. Another option is to alert the operator without alerting the user. Another option is immediate locking of the handset. Once locked, the call control is arranged to enable unlocking through an entry code provided remotely or - through remote unlocking. Call control validates the unlock code received from the operator before unlocking the handset. Partial locking can be arranged, e.g. to limit use to a
subset of types of communication, or a subset of addresses, or locations (e.g. cells) of usage.

Also shown in figure 6 are other areas of the memory map of the SIM. Addresses 16k to 32k can be used as workspace for persistent storage of data 670 for the applications. For example, as shown, the rules and thresholds can be stored here, also hotlists, the current or live signature, the long term or decayed signature, and temporary storage of messages or programmes received OTA.

The software can be implemented in any appropriate language according to the application, such as the well known C, or Java languages. Particularly for handsets other than mobile phones, it may be stored in on board memory rather than on a removable card. The software can be executed by conventional hardware in the handset, such as standard general purpose microprocessors or digital signal processors, or processor modules on ASICs (application specific integrated circuits).

Fig 7 shows a schematic view of another embodiment, showing steps in activating monitoring. At step 710, the user (subscriber) requests Terminator subscription via the Network Operator. Optionally, the operator can activate without user initiative. At step 720, the Network Operator starts the activation process and sets or adjusts the subscriber class for that subscriber, either depending on user input, or by reference to other sources. At step 730, the Terminator Mobile Application is activated via a SIM-Update SMS message. At step 740, the Call-Predict & Call-Guard modules are initialised with default values. At a later date, optionally as shown at step 750, Call-Predict & Call-Guard are remotely adjusted via Call-Control to reflect a revised subscriber class (e.g. Pay as you go, Business, international etc) via SIM-Update.

Fig 8 shows a schematic view of another embodiment, showing steps in detecting fraudulent usage. At step 800, the subscriber initiates outgoing call or message, or receives an incoming call or message. At step 810, during the outgoing call, Call-Learn and Call-Predict are monitoring call details (duration, dialed number, destination). Similarly, for incoming calls, the same details can be recorded. At step 820, Call-
Control will lock-down the handset and/or send a message to the operator if Call Predict generates an Alert. At step 830, Call-Control will lock-down the handset and/or send a message to the operator if Call Guard generates an Alert. At step 840, Call control will lock down the handset and/or send a message to the operator, if it detects usage in a non permitted location, e.g. another network, or particular cells of the home network. Hybrid combinations of these types of monitoring are particularly useful for deducing unusual activity. For example if behaviour patterns are unusual, then lower event thresholds can be used, to trigger action. Similarly, the location information can be used in combination with behaviour and or events, to provide more accurate detection. At 850, the display 855 of the handset shows an indication that the handset has been locked, and offers the opportunity to call the operator with a code for the type of fraud detected, to request remote unlocking, as will now be explained in more detail.

Fig 9 shows a schematic view of another embodiment, showing steps in reactivating a locked handset. At step 900 Call-Guard has locked the phone, the consumer must contact the Network Operator to obtain unlock code. Only the Network Operator HelpDesk number can be dialed. At step 910, the Network Operator undertakes verification procedures and ascertains the fraud code nature from the subscriber’s handset. At step 920, the handset remains locked and withdrawn from the network, or, at step 930, the Network Operator provides an unlock code to the subscriber and makes any necessary adjustments to consumer subscription class or to thresholds, to prevent more unwanted false detections. At step 940, Call-Predict & Call-Learn are remotely adjusted via Call-Control to reflect consumer subscription class via SIM-Update.

Concluding remarks
As has been discussed above, installing fraud detection on the handset allows detection to take place at the earliest opportunity. A means of capturing user behaviour within the SIM card of the mobile handset, by building a subscriber signature is provided. One option is to apply fraud detection techniques to this user data. Another is to determine the location of the usage, e.g. by determining cell identity in a cellular system, or network identity for roaming usage. If the usage is identified as potentially fraudulent, action can be taken. One option is to lock the handset and allow it to be unlocked only
by the network operator. Use can thus be restricted to particular predetermined locations. Fraud can be deterred since much fraud involves use at locations far from the user’s home cell. In 2.5G/3G networks, data network usage monitoring can take place by maintaining a list of ‘hot’ URLs or other indicator.

User behaviour can be captured by recording and maintaining call data for that user. This information can include dialled number and behavioural data such as call duration and call destination. The behavioural data will be maintained and aggregated into a subscriber usage profile. These two elements are then analysed by the fraud detection software for potential fraud. The dialled numbers can be checked against a list of ‘hot’ numbers, numbers known to the operators as suspicious. If there is a match the phone is immediately locked. The hot number list can be downloaded from a central Fraud Management System by means of a mobile control unit and can be updated whenever the hot number list changes.

The behavioural data, aggregated into a user profile, is compared to the user’s typical profile. If there is a major discrepancy, showing a dramatic change in behaviour the phone can be locked. The method of comparison used may include standard statistical analysis techniques, proprietary techniques such as Dynamic Deviation, neural networks or other advanced techniques. The result of the comparison will provide an indication of the likelihood of fraud. The behavioural data is also compared against thresholds of activity for the category of user and any threshold exceeded will provide evidence of fraud.

Each user is initially provided with a default profile that constitutes the typical use for this type of user. The default profiles are based on information provided by the central fraud management system that processes all user activity. The aggregated behavioural profiles are decayed into the user profile to maintain an adaptive record of user behaviour as described in above mentioned US patent 5,966,650.

Embellishments include a software application capable of running on the SIM card of a mobile phone and a fraud management system that can communicate with mobile
handsets and download information such as hot list updates to handsets running the fraud detection application.

Benefits include fraud detected and prevented at source, potentially thousands of Fraud Management System’s (FMS) deployed in the field for a specific network operator, each FMS uniquely tuned to one consumer. Also, the solution is portable between various mobile handsets due to industry support for SIM cards and a SIM Toolkit allowing the network operator to add the application to every new SIM card as a standard component at the time of manufacture. The subscriber could enable the Terminator Agent, just as easily as enabling Conference Calling, Data Services and 2nd Line Services. The Network Operator could charge for Terminator Agent activation, either via monthly subscription to Retail consumers or as standard service offering to Business consumers. Branding incorporated in alerts to subscribers could increase market awareness for the selected Network Operator and for a fraud detection service operator or supplier.

Other variations
Callguard can be used to monitor other scenarios e.g. children not being allowed to call certain numbers, by adding to the hot lists. User adjustable hot-lists could be used.

Different levels of monitoring or revenue assurance could be provided. The fraud alert or the “out of authorised location” alert could be sent to other people or agencies, e.g. alerts of children’s inappropriate usage could be sent to parents. Alerts on company handsets could be alerted to the company as well as the user. Credit card companies could be alerted to increase monitoring of the users credit card. Insurance excess discounts could be offered if activation of monitoring is accepted by the user. The remote locking function could be used by emergency services to prevent usage in the vicinity of an emergency, to prevent congestion and ensure availability to higher priority users such as emergency services.

Other variations and additions can be conceived by those skilled in the art and are intended to be encompassed within the scope of the claims.
Claims:

1. A mobile handset for use as part of a radio communication network, the handset having a monitor arranged to monitor usage of the handset and a detector arranged to determine if such usage is fraudulent.

2. The handset of claim 1, arranged as part of a distributed processing network fraud management system.

3. The handset of claim 1, having a lock for preventing further fraudulent usage in the event of the detector determining fraudulent usage.

4. The handset of claim 1, arranged to send an indication to a network operator in the event of the detector detecting fraudulent usage.

5. The handset of claim 4, the indication being carried by a message service.

6. The handset of claim 1, the monitor or the detector being adaptable by means of a message sent from a network operator using a message service.

7. The handset of claim 1, the monitor having an aggregator for aggregating current usage information into a current signature.

8. The handset of claim 7, the detector being arranged to detect anomalous usage by comparing the current signature with a typical signature representing usage over a long period.

9. The handset of claim 8, the monitor being arranged to adapt the typical behavioural signature with the current usage information.

10. The handset of claim 7, the detector being arranged to compare the current usage to thresholds of levels of activity.
11. The handset of claim 1, the detector being arranged to compare the current usage to predetermined activities categorised as fraudulent.

12. The handset of claim 1, the detector being arranged to be adjustable remotely by a network operator.

13. The handset of claim 1, the monitor and detector being in the form of software.

14. The handset of claim 1, the monitor and the detector being implemented on a removable card.

15. A removable card for a handset for use as part of a radio communication network, the removable card having a monitor arranged to monitor usage of the handset and a detector arranged to determine if such usage is fraudulent.

16. A method of using a mobile handset suitable for use with a radio communications network, the handset having a fraud detector, the method having the step of: using the handset to communicate over the radio communications network, following activation of the fraud detector, such usage being monitored by the fraud detector.

17. A method of detecting fraudulent use of a handset used as part of a radio communication network, the handset having a fraud detector, the method having the steps of: monitoring usage of the handset, in the handset, and determining in the handset if such usage is fraudulent.

18. A method of offering a fraud detection service for detecting fraudulent use of a handset used as part of a radio communication network, the handset having a fraud detector, the method having the steps of: receiving from a subscriber, a request for service activation, and sending a message to the handset to cause the detector to detect fraudulent use.
19. A method of maintaining a fraud detection service for detecting fraudulent use of a 
handset used as part of a radio communication network, the handset having a fraud 
detector, the method having the steps of: 
maintaining a record of which handsets have fraud detectors, and 
remotely updating the fraud detectors in one or more of these handsets.

20. A method of maintaining a fraud detection service for detecting fraudulent use of a 
handset used as part of a radio communication network, the handset having a fraud 
detector, the method having the steps of: 
receiving an indication that a handset has been locked by the fraud detector, and 
remotely unlocking the handset if the use is not fraudulent.

21. A management system for offering a fraud detection service for detecting fraudulent 
use of a handset used as part of a radio communication network, the handset having a 
fraud detector, the system having: 
an interface arranged to receive from a subscriber, a request for service activation, and 
a processor arranged to send an indication to the handset to cause the detector to detect 
fraudulent use.

22. A management system for maintaining a fraud detection service for detecting 
fraudulent use of a handset used as part of a radio communication network, the handset 
having a fraud detector, the system having: 
a record of which handsets have fraud detectors, and 
a processor arranged to remotely update the fraud detectors in one or more of these 
handsets.

23. A management system for maintaining a fraud detection service for detecting 
fraudulent use of a handset used as part of a radio communication network, the handset 
having a fraud detector, the system having: 
an interface for receiving an indication that a handset has been locked by the fraud 
detector, and
a processor arranged to send a command to remotely unlock the handset if the use is not fraudulent.

24. A mobile handset having a lock for preventing use, and a lock controller for activating the lock based on monitored usage.

25. The mobile of claim 24, the activation being dependent on the location of the handset.

26. The mobile of claim 25, being for use with a cellular network, being arranged to determine location by identifying which cell the mobile is in.

27. The mobile of claim 24, the lock controller being adjustable remotely by a network operator.

28. A mobile handset for use as part of a radio communication network, the handset having a monitor arranged to monitor and record usage of the handset.

29. The mobile handset of claim 28, being arranged to send information relating to the monitored usage to a network operator using a message service.

30. The mobile handset of claim 28 having an aggregator for aggregating and storing in the handset an aggregated profile of the usage.

31. A method of charging for handset usage, the charging being dependent on whether the handset has active fraud detection.

32. A method of charging for handset usage, the charging being dependent on whether the handset has active usage monitoring.
33. A method of maintaining a usage monitoring system for monitoring use of a handset used as part of a radio communication network, the handset having a usage monitor, the method having the steps of:
maintaining a record of which handsets have usage monitors, and
receiving usage information from these handsets.

34. A management system for maintaining a usage monitoring system for monitoring use of a handset used as part of a radio communication network, the handset having a usage monitor, the system having:
a record of which handsets have usage monitors, and
a processor arranged to receive usage information from these handsets.

35. The removable card of claim 15, having an aggregator for aggregating current usage information into a signature.

36. A removable card for a handset for use as part of a radio communication network, the removable card having software arranged to monitor usage of the handset and for storing in the handset a signature summarising the usage.

37. The removable card of claim 35 or 36, having software arranged to detect anomalous usage by comparing a short term usage with the signature representing usage over a longer period.

38. The removable card of any of claims 35 to 37, having software arranged to update the signature with current usage information.

39. The removable card of any of claims 35 to 38 having software arranged to use the signature for revenue assurance purposes.

40. The removable card of any of claims 35 to 39 having software arranged to use the stored signature to send usage information from the handset to an operator of the network to enable services to the user to be tailored according to the usage information.
41. The removable card of any of claims 35 to 40 arranged to receive software updates when installed in the handset, sent by an operator of the network over the network.

42. Software for storing on a removable card for implementing any of claims 15 or 35 to 41.

43. The mobile handset of any of claims 28 to 30, having the removable card of any of claims 15 or 35 to 41.
Fraud detection Applications:
- Call-Learn
- Call-Predict
- Call-Guard
- Call-Control

For updating signatures representing Current and Normal usage.

For comparing the Current and Normal signatures to detect anomalous usage.

For detecting anomalies by comparison of call or message attributes to rules, thresholds and hot lists.

For application management, and for locking handset or alerting operator or user, when anomalies detected.

Application Workspace:
- Rules & Thresholds
- Hot-Lists
- Live Signature
- Decayed Signature
- OTA Receipt Area

Sim or Java card 600

Memory Map 690
- 0K Free Memory
- 16K Persistent Storage Free Memory
- 32K Free Memory
- 56K Free Memory
- ROM Encryption Services, DES/3DES/RSA/GSM
Subscriber receives incoming or initiates outgoing call or message. Network 10

During call, or message Call-Learn and Call-Predict are monitoring call or message details (duration, dialed number, destination).

Call control will lock down handset and/or send message to operator, if it detects usage in a non-permitted location, e.g., another network, or particular cells of the home network.

Call-Control will lock down handset and/or send message to operator, if Predict Alert generated.

Call-Control will lock down handset and/or send message to operator, if Guard Alert triggered.

Cerebrus Terminator

This unit has been locked due to potential fraud, please call handset provider to obtain unlock code.

Fraud Code: CG-9765-A
Unlock Code:

OK CALL
Handset can now remain locked and withdrawn from the network, or...

Network Operator provides unlock code to consumer and makes any necessary adjustments to consumer subscription class.

Terminator Mgt Centre 240

Network Operator undertakes verification procedures and ascertains the fraud code nature on the consumers handset. 910

Call-Guard has locked the phone, the consumer must contact the Network Operator to obtain unlock code. Only the Network Operator HelpDesk number can be dialed. 900

Call-Predict & Call-Learn remotely adjusted via Call-Control to reflect consumer subscription class via SIM-Update. 940
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7   H04Q/7/38   H04Q/7/22

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)

IPC 7   H04Q

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 6 295 446 B1 (ROCHA ROBERTO) 25 September 2001 (2001-09-25) column 2, line 7 - line 60 abstract; figures 1-5</td>
<td>1-43</td>
</tr>
<tr>
<td>X</td>
<td>US 6 226 530 B1 (CAVAIILES CHARLES ET AL) 1 May 2001 (2001-05-01) column 2, line 5 - line 53 abstract; figure 3</td>
<td>1-43</td>
</tr>
<tr>
<td>X</td>
<td>US 6 014 557 A (MORTON JOHN W ET AL) 11 January 2000 (2000-01-11) column 4, line 45 - column 8, line 25 abstract; figures 1-12</td>
<td>1-43</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of box C.

Designated Office:

Further 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.

"Z" document member of the same patent family.

Date of the actual completion of the international search:

24 June 2003

Date of mailing of the international search report:

09. 07. 2003

Name and mailing address of the ISA:

European Patent Office, P.B. 5816 Patentlaan 2
NL-2280 HV Rijswijk
Tel: (+31-70) 948-2040, Tx: 31 651 epo nl
Fax: (+31-70) 545-3016

Authorized officer:

BEHROZ MORADI/JA A
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>US 5 345 595 A (JENSEN FLEMMING B ET AL) 6 September 1994 (1994-09-06) column 3, line 3 -column 4, line 30 abstract; figures 1-11</td>
<td>1-43</td>
</tr>
<tr>
<td>Y</td>
<td>WO 98 19489 A (ERICSSON TELEFON AB L M) 7 May 1998 (1998-05-07) page 2, line 29 -page 4, line 16 abstract; figures 1-3</td>
<td>1-43</td>
</tr>
<tr>
<td>Y</td>
<td>WO 00 30398 A (LIGHTBRIDGE INC) 25 May 2000 (2000-05-25) page 3, line 1 -page 8, line 1 abstract; figures 1-9</td>
<td>1-43</td>
</tr>
<tr>
<td>Y</td>
<td>WO 01 45444 A (NOKIA NETWORKS OY ;PALDAN ESKO (FI); LOHTAJA JARKKO (SG)) 21 June 2001 (2001-06-21) page 1, line 1 -page 3, line 15 abstract; figures 1-3</td>
<td>1-43</td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BR 9914630 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2344596 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1232501 T</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GB 2358113 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0024219 A1</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 69810937 D1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9909521 A1</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 5596294 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2149135 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 0669061 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 8503346 T</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 5615408 A</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 4798397 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BR 9713276 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9819489 A2</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2351478 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6535728 B1</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 2375501 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2369189 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1238559 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0145444 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2003517801 T</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2351478 A1</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 1699402 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 9394901 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2363667 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1357986 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0243424 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2002247654 A</td>
</tr>
</tbody>
</table>