

FRAUD MONITORING SYSTEM

The present invention generally relates to a telecommunications network. More particularly, one aspect of the present invention relates to a method and
5 apparatus of automatically detecting fraudulent calls in a telecommunications network and another relates to a method of controlling calls over a telecommunications network.

Fraudulent use of a telephone communications network can cost the telecommunications operator a significant amount of money. Rule based fraud
10 detection systems have been developed with a view to combating fraud in a telecommunications network. In such systems if a particular usage of the network, determined from a call record, triggers one or more of the predefined rules, an alarm is generated enabling human operators to take the necessary action. While such systems have had some success in combating fraud, difficulties seem to arise due to
15 the sheer number of alarms that can be generated within a short time. Typically, fraud detection operators may have tens of thousands of live alarms to deal with during a day and it is therefore generally impractical to deal with each individual alarm as it arises. Methods have been developed for consolidating or grouping the fraud alarms based on their priority and for identifying patterns in the alarms once
20 generated. Such rule based fraud detection systems however only operate once alarms have been raised.

In accordance with one aspect the present invention provides method of automatically detecting fraudulent calls in a telecommunications network, the method comprising the steps of:

- 25 determining the origination of the calls; and
 determining whether the call is likely to be a fraudulent call using a predetermined pattern of previous or expected calls specific to the origination.

In accordance with a second aspect the present invention provides apparatus for automatically detecting fraudulent calls in a telecommunications
30 network, the apparatus comprising:

- determining means for determining the origination of the call;
 storage means for storing data for a pattern of previous or expected calls specific to originations; and

fraud detecting means for determining whether the call is likely to be a fraudulent call using the determined origination of the call and the stored pattern of calls specific to the origination.

Thus in accordance with the present invention the pattern of use of the
5 telecommunications network is used which is specific to the origination of the call. Fraudulent activity can be determined by detecting a deviation in the call from the predetermined pattern for the origination of the call. The predetermined pattern comprises information on calls over a period of time and the time of the current call can be used to determine whether the call fits the pattern.

10 Preferably the origination is determined by receiving a call record containing information on the call. Typically in a telecommunications network when a call is initiated a call record is sent to the exchange which contains information for example identifying the origination, the destination, the time of initiation of the call and the date. By determining the origination of the call from the call record at the initiation
15 of the call, the determination of whether the call is likely to be a fraudulent call can be determined as the call is made. This allows the call to be disallowed or disconnected if the call is determined to a call which lies significantly outside the predetermined pattern of calls.

In order to accommodate changes in the calling behaviour of the originator,
20 the predetermined pattern of calls can be adaptively modified. Such a modification can give a greater weighting to more recently made calls. All the calls which do not deviate significantly from the predetermined pattern of calls can be used to update the pattern. Also, calls which have been determined to be fraudulent can be used to adaptively modify the predetermined pattern of calls once they have been
25 investigated and cleared by, for example, an operator. In this way the pattern of calls can be adapted to more accurately reflect the expected call behaviour of an origination.

The term 'origination' is used in the specification to refer to any identifiable point of origin of a call in a telecommunications network. For example, an origination
30 can comprise an individual user or group user identification code. Examples of such an identification code are a personal number which can be input using a telephone key pad. Such a system is used for instance when using a charge-card. Also for a mobile telephone the SIM card can be used to provide a unique identification code. A code can be assigned to an individual user or a group of users and is independent

of the node in the telecommunications network i.e. the telephone number from which the call is made. Alternatively or in addition the identity of a node or group of nodes in the telecommunications network can comprise the origination i.e. a telephone number from a group of telephone numbers, or an area code. Further, the
5 origination can comprise the geographical location from which the call is made. For calls made from mobile telephones, the geographical location can comprise a true geographical location which can, for example, be obtained from the base stations in the cellular network. For a call originating from a conventional telephone handset, the geographical location can be obtained from the telephone number and can be
10 provided as an exact address, or an area such as a town or country.

Thus, one or a combination of these pieces of information identifying the origination of the call can be used to choose a predetermined pattern to be used for the call. For example, for a charge-card user, there may be more than one predetermined pattern termed a user profile assigned to that charge-card depending
15 upon the telecommunications node used to make the call or the geographical location from which the call was made. The user's calling behaviour may be different for different telecommunications nodes and/or different geographical locations. The same is true for mobile telephone users. The pattern of calls in different geographical locations can be quite different and therefore different user profiles can
20 be provided.

In one embodiment the user profile includes information on the call destination for the pattern of calls and thus for the call made the destination is determined in order to determine whether the call fits the normal pattern of calling behaviour for the origination. The call destination information can comprise
25 information identifying a node or group of nodes in the telecommunications network i.e. a specific telephone number, group of numbers, or an area code, and/or a geographical location.

In an embodiment of the present invention the time and/or day or date of the call is determined and the user profile includes information on the time of day of
30 the calls, the day or date of the calls, and/or the frequency of calls made. In this way the information and/or date of the call made can be used to determine whether the call fits the user profile.

Although information on the call such as the origination, the destination, the time, and date of the call can be determined as soon as the call is made from the call

record and this information can be used immediately to determine whether the call represents fraudulent activity, if no fraudulent activity is detected, at the termination of the call the duration of the call can be determined and used to carry out a further check since in a preferred embodiment the user profile includes information on the
5 duration of the calls. This specific embodiment provides a further check for fraudulent activity using the full duration parameter.

In accordance with another aspect of the present invention there is provided a method of controlling calls over a telecommunications network, the method comprising the steps of:

- 10 determining the origination of a call, and
determining whether the call is to be allowed or disallowed using a predetermined pattern of calls specific to the origination.

In accordance with a further aspect of the present invention there is provided apparatus for controlling calls over a telecommunications network, the
15 apparatus comprising:

- determining means for determining the origination of a call;
- storage means for storing data for a pattern of calls specific to originations;
- allowance determining means for determining whether the call is to be
allowed or disallowed using the determined origination of the call and the stored
20 pattern of calls specific to the origination; and
control means for controlling the call in accordance with the determination.

Thus in accordance with these aspects of the present invention if the call made does not fit the pattern for the origination of the call, the call is automatically disallowed or disconnected.

- 25 The call pattern can thus be used to control calls from the origination. It can allow for a level of usage of the telecommunications network which is not fixed but is determined as a pattern. This can also provide automatic protection against fraudulent calls since any calls which do not fit a user profile will not be allowed.

In order to allow a user to force the telecommunications network to allow a
30 call, the user can be allowed to input a code which must be validated by the telecommunications network. If the code is valid the telecommunications network will allow the input of pattern update data to update the pattern of calls for user profile. In this way if a user wishes to significantly change their calling behaviour for

example by making a series of long distance telephone calls, the user profile can be manually updated to accept this change in user behaviour.

The predetermined pattern of calls (user profile) is a pattern which is specific to the origination and can be formed during a 'learning' phase during which the calls
5 made from an origination are recorded in order to form the predetermined pattern. Alternatively, the telecommunications network could form the predetermined pattern from the call records for the origination for a previous period of time. Further, the predetermined pattern could be formed based on the expected pattern of calls for the origination.

10 Embodiments of the present invention will now be described with reference to the accompanying drawings in which:

Figure 1 is a schematic drawing of a telecommunications network including the fraud detection system in accordance with an embodiment of the present invention.

15 Figure 2 is a flow diagram illustrating the steps carried out in detecting fraudulent calls using the method of an embodiment of the present invention; and

Figure 3 is a flow diagram illustrating the steps of a preferred method of forming the user profile.

Referring now to Figure 1 there is illustrated schematically a telephone
20 communications network in which individual telephone handsets 1a, 1b, 1c and 1d are connected to respective digital local exchanges (DLEs) 2a and 2b. The digital local exchanges 2a and 2b receive telephone calls from the telephone handsets 1a, 1b, 1c and 1d and if the telephone call is a local telephone call, the call is routed to the appropriate telephone handset 1a, 1b, 1c and 1d. If however the telephone call
25 is not local, the digital local exchange 2a and 2b routes the call to respective digital main switching units 3a, 3b and 3c. The digital main switching units 3a, 3b and 3c route the calls accordingly between digital local exchanges 2a and 2b.

In this embodiment of the present invention a fraud management system (FMS) 4 monitors the calls being switched by the digital main switching units 3a, 3b
30 and 3c. In order to monitor the calls, the call record for each call is sent to the fraud management system 4 by the appropriate digital main switching unit 3a, 3b and 3c which is handling the call. Since the call record containing information identifying the origination of the call, the destination of the call, and the time and date of the call is available as soon as the call is placed, the fraud management system 4 is able

to detect whether the call is a fraudulent call immediately the call is placed. If it is detected that the call is fraudulent and does not fit the profile of use expected for the point of origin of the call, the fraud management system 4 can instruct the digital main switching units 3a, 3b and 3c to disallow or disconnect the call. Alternatively, 5 an alarm can be raised to bring the call to the attention of an operator to analyze whether action should be taken. Thus, the call can either be automatically barred if the call does not fit the expected profile for the origination, or operator intervention can be instigated.

If a call is allowed to proceed since from the information available at the 10 onset of the call does not indicate that the call represents a significant deviation from the expected calling behaviour for the origination, at the termination of the call the call duration is added to the call record and this further piece of information can be used to carry out a further fraud detection step. If it is determined that this call duration does not fit the expected calling behaviour and the call lies significantly 15 outside the expected call pattern, although it is not possible to bar the call, an alarm can be raised to bring the call to the attention of an operator who can then look into the circumstances surrounding the call.

Figure 2 is a flow diagram illustrating the steps of a call detection method in accordance with an embodiment of the present invention. In step S1 a user makes a 20 call and the call is connected to the digital local exchange in step S2. In step S3 the digital local exchange determines whether the call is local and if so in step S9 the call is proceeded with and the digital local exchange connects the local telephone handsets. If the call is not local the digital local exchange passes the call to a digital main switching unit in step S4. The digital main switching unit then passes on the 25 call information to the fraud management system in step S5. The fraud management system selects a profile in accordance with the caller's ID i.e. the origination of the call in step S6 and in step S7 it is determined whether the call is in keeping with the profile. If a call is in keeping with the profile in step S8 the profile can be updated to take into consideration this call and in step S9 the call is proceeded with i.e. the 30 digital main switching units routes the call. If in step S7 it is determined that the call is not in keeping with the profile, in step S10 an alarm is raised allowing an operator to intervene in step S11. In step S12 the operator can determine whether the call or calls should be barred from the caller's ID. The call is not to be barred the profile

can be updated in step S8 and the call can proceed. Otherwise in step S13 the call or calls from the caller's ID are barred.

Thus in the embodiment of Figure 2 an alarm is raised allowing an operator to intervene to determine whether to bar the call or not. However, in an alternative
5 embodiment if the call is not in keeping with the profile, the call can be automatically barred.

Figure 3 is a flow diagram illustrating one method of forming a user profile. This method represents a method of learning a user's profile during a learning phase. In step S30 a user makes a call and in step S31 the call is connected to the local
10 exchange. In step S32 it is determined whether the call is local and if the call is local the process proceeds to step S37 where the call proceeds. If the call is not local the call is passed by the digital local exchange to the digital main switching unit in step S33. The digital main switching unit then passes the call information to the fraud management system in step S34 and in step S35 the fraud management system
15 selects the profile in accordance with the caller's ID. The selected profile can then be updated in step S36 using the information about the call and in step S37 the call can proceed.

In an alternative method of forming the user profile, instead of carrying this out on line as illustrated in Figure 3, a telecommunications operator can utilize stored
20 call records for a period of time in order to form a user profile 'off line'.

Alternatively, unexpected user profiles can be generated based on the expected calling behaviour of the user. This technique may be used for instance where there is a new user with no historical call information.

It can be seen from Figure 2 that the profile can be constantly updated in
25 order to track changes in calling behaviour for a user or origination.

The user profile represents a pattern of calling behaviour for a point of origin of a call in a telecommunications network. The point of origin can be specific to a personal number such as a charge-card or mobile telephone SIM, a node or group of nodes of the telecommunications network i.e. a telephone number or group of
30 telephone numbers, or a geographical location i.e. a specific location which for a mobile telephone can, for example, be provided by the cellular base stations and for a conventional fixed telephone handset can be provided by a database identifying the telephone number and location, or a generalised locations such as a building, area, city, or country. A combination of this origination information can be used to

provide more than one profile for a user. For example, if a charge-card user uses telephones in two different regions of the country regularly, two different profiles can be provided for the charge-card depending upon the geographical location from which the call was made. Similarly, for mobile telephone users more than one user
5 profile can be provided.

In embodiments of the present invention the user profile contains information not just on the point of origin of the calls but also the destinations. The destinations can be identified as nodes or groups of nodes in the telecommunications network i.e. telephone numbers, groups of telephone numbers, or area codes, and/or
10 geographical locations i.e. specific locations or areas. Thus, the user profile can identify calls made from an origination to a destination over a period of time. The profile can also include summary information such as the frequency of calls to be made by the origination during a period of time. Also subsets of this information can be provided e.g. the frequency of calls made to a specific telephone number, area
15 code or geographical location during a period of time. As calls are made during a period of time the pattern of calls being made during the current time period can be compared with the pattern of calls made during a previous time period to detect fraudulent activities e.g. if frequency of calls increases significantly outside the
behaviour range there is potential fraud. The calling patterns of each origination can
20 extend over any period of time e.g. a number of hours, a day, a week, a month, or any desired period.

For a mobile user e.g. using a charge-card or a mobile telephone, when a call is made from a new location i.e. a new node in the telecommunications network or a new geographical location, a new user profile can be generated for that location
25 adaptively.

User profiles can be stored for preceding periods of time e.g. an hour, a day, or a week. A user profile which is an average for previous periods of time can be stored and the averaging can be carried out by performing a weighted average to give favour to the most recently recorded profiles. In order to update the user profile
30 the current profile recorded during the most recent period of time is averaged in their weighted manner with the average user profile automatically. This average user profile is the user profile which is used for fraud detection. If a fraudulent call was detected during the recording of the current or most recent profile, this profile can be ignored in the updating of the average user profile at the end of the period. If this

'fraudulent' call recurs, this call could be allowed to be included in the profile once an investigation has been undertaken to ensure that the call is not fraudulent.

If a call is outside a usual pattern of calling, an embodiment of the present invention provides for a user to enter a validation code to force the acceptance of
5 the call and to update the current user profile.

Although in the foregoing embodiments an origination comprising a personal identification number has been described only with reference to charge-cards and mobile telephone SIMs, the present invention is applicable to a system wherein users are provided with codes which must be entered to allow a user to make a telephone
10 call. The code is a unique identifier to identify the user which causes the selection of the appropriate user profile to provide calls allowed for by the user profile. Thus in this embodiment calls over the communications network from a user can be controlled in accordance with the user's profile which can be preset in advance to restrict the user's access to telephone numbers over the network. Similarly, the
15 access to telephone numbers over the network at any point of origination e.g. charge-card, mobile telephone, or telephone number can be controlled by a predetermined user's profile. In this way the telephone numbers available at periods of time i.e. the pattern of calls for a user can be controlled. Thus the user profile represents a pattern of allowed calls specific to the origination rather than a pattern
20 of previous or expected calls as described hereinabove with reference to the previous embodiments. Embodiments of the present invention can thus provide for the control of calls over a telecommunications network not just the detection of potentially fraudulent calls.



CLAIMS

1. A method of automatically detecting fraudulent calls in a telecommunications network, the method comprising the steps of:
5 determining the origination of the calls;
determining whether the call is likely to be a fraudulent call using a predetermined pattern of previous or expected calls specific to the origination.
2. A method according to claim 1 including the step of receiving a call record
10 containing information on the call, wherein the step of determining the origination of the call uses the call record.
3. A method according to claim 1 or claim 2 wherein the call is determined to be a fraudulent call if it lies significantly outside the predetermined pattern of calls.
15
4. A method according to any preceding claim including the step of adaptively modifying the predetermined pattern of calls to update the pattern to accommodate changes in calling behaviour of the origination.
- 20 5. A method according to claim 4 wherein the adaptive modification of the predetermined pattern of calls is a weighted averaging operation which is weighted to favour the most recent calls.
6. A method according to claim 4 or claim 5 wherein calls determined to be
25 fraudulent are used for adaptively modifying the predetermined pattern of calls once they have been investigated and cleared.
7. A method according to any preceding claim wherein the origination is determined as at least one of the set comprising a user or group identification code,
30 a node or group of nodes in the telecommunications network, and a geographical location.



8. A method according to any preceding claim including the step of determining the destination of the call, wherein said predetermined pattern of calls includes information on the call destination.
- 5 9. A method according to claim 8 wherein the call destination information in said predetermined pattern of calls comprises information identifying a node or group of nodes in the telecommunications network and/or a geographical location.
- 10 10. A method according to any preceding claim including the step of determining the time and/or day or date of the call, wherein the predetermined pattern of calls includes information on at least one of the set of the time of day of the calls, the day or date of the calls, and the frequency of calls made.
- 15 11. A method according to any preceding claim including the step of determining the duration of the call, wherein said predetermined pattern of calls includes information on the duration of calls.
- 20 12. A method according to claim 2 wherein the call record is received and used in the determination as the call is made.
- 25 13. A method according to any preceding claim including the steps of receiving an input code from the origination, validating the input code, and receiving pattern update data from the origination and updating said predetermined pattern of calls if the input code is valid.
- 30 14. A method according to any preceding claim wherein a pattern of calls from the origination for a current time period is compared with a pattern of calls for a previous time period in order to determine whether there is likely to be fraudulent activity.
15. Apparatus for automatically detecting fraudulent calls in a telecommunications network, the apparatus comprising:
determining means for determining the origination of the call;



storage means for storing data for a pattern of previous or expected calls specific to origination; and

fraud detecting means for determining whether the call is likely to be a fraudulent call using the determined origination of the call and the stored pattern of
5 calls specific to the origination.

16. Apparatus according to claim 15 wherein said determining means includes means for receiving a call record containing information on the call, and the fraud detecting means is adapted to use the call record information in the determination.

10

17. Apparatus according to claim 15 or claim 16 wherein said fraud detecting means is operative to determine that a call is fraudulent if it lies significantly outside the predetermined pattern of calls.

15 18. Apparatus according to any one of claims 15 to 17 including adaptive means for adaptively modifying the predetermined pattern of calls to update the pattern to accommodate changes in calling behaviour of the origination.

19. Apparatus according to claim 18 wherein said adaptive means is operative
20 to carry out a weighted averaging operation wherein the most recent calls are given the highest weighting in the adaption process.

20. Apparatus according to claim 18 or claim 19 wherein said adaptive means is
25 operative to use calls determined to be fraudulent in the adaptive process once the calls have been investigated and cleared.

21. Apparatus according to any one of claims 15 to 20 wherein said determining means is operative to determine the origination as at least one of the set comprising a user or group identification code, a node or group of nodes in the
30 telecommunications network, and a geographical location.

22. Apparatus according to any one of claims 15 to 21 including means for determining the destination of the call, wherein said storage means is adapted to



store said predetermined pattern of calls which includes information on the call destination.

23. Apparatus according to claim 22 wherein said storage means is adapted to
5 store the information on the call destination which comprises information identifying
a node or group of nodes in the telecommunications network and/or a geographical
location.
24. Apparatus according to any one of claims 15 to 23 including means for
10 determining the time and/or day or date of the call, wherein said storage means is
adapted to store said predetermined pattern of calls which includes information on at
least one of the set of the time of day of the calls, the day or date of the calls, and
the frequency of the calls.
- 15 25. Apparatus according to any one of claims 15 to 24 including means for
determining the duration of the call, wherein said storage means is adapted to store
said information on said predetermined pattern of calls which includes information
on the duration of calls.
- 20 26. Apparatus according to claim 16 wherein said means for receiving the call
record is operative to receive the call record as the call is made and said fraud
detecting means is operative to determine whether the call is likely to be a fraudulent
call as the call is made.
- 25 27. Apparatus according to any one of claims 15 to 26 including means for
receiving an input code from the origination, means for validating the input code, and
means for receiving pattern update data from the origination and for updating said
predetermined pattern of calls if the input code is valid.
- 30 28. A method according to any one of claims 15 to 27 including current storage
means for storing a pattern of calls from the origination for a current time period,
wherein said storage means stores a pattern of calls for a previous time period, and
said fraud detection means is adapted to compare the pattern for the current time



period with the pattern for the previous time period in order to determine whether there is likely to be fraudulent activity.

29. A method of controlling calls over a telecommunications network, the
5 method comprising the steps of:

determining the origination of a call, and

determining whether the call is to be allowed or disallowed using a
predetermined pattern of calls specific to the origination.

10 30. A method according to claim 29 including the step of receiving a call record
containing information on the call, wherein the step of determining whether the call
is to be allowed or disallowed uses the call record in the determination.

31. A method according to claim 29 or claim 30 wherein the call is determined
15 to be disallowed if it lies significantly outside the predetermined pattern of calls.

32. A method according to any one of claims 29 to 31 including the step of
adaptively modifying the predetermined pattern of calls to update the pattern to
accommodate changes in calling behaviour of the origination.

20

33. A method according to claim 32 wherein the adaptive modification of the
predetermined pattern of calls is a weighted averaging operation which is weighted
to favour the most recent calls.

25 34. A method according to any one of claims 29 to 33 wherein the origination is
determined as at least one of the set comprising a user or group identification code,
a node or group of nodes in the telecommunications network, and a geographical
location.

30 35. A method according to any one of claims 29 to 34 including the step of
determining the destination of the call, wherein said predetermined pattern of calls
includes information on the call destination.



36. A method according to claim 35 wherein the call destination information in said predetermined pattern of calls comprises information identifying a node or group of nodes in the telecommunications network and/or a geographical location.
- 5 37. A method according to any one of claims 29 to 36 including the step of determining the time and/or day or date of the call, wherein the predetermined pattern of calls includes information on at least one of the set of the time of day of the calls, the day or date of the calls, and the frequency of calls made.
- 10 38. A method according to any one of claims 29 to 37 including the steps of receiving an input code from the origination, validating the input code, and receiving pattern update data from the origination and updating said predetermined pattern of calls if the input code is valid.
- 15 39. Apparatus for controlling calls over a telecommunications network, the apparatus comprising:
determining means for determining the origination of a call;
storage means for storing data for a pattern of calls specific to origination;
allowance determining means for determining whether the call is to be
20 allowed or disallowed using the determined origination of the call and the stored pattern of calls specific to the origination; and
control means for controlling the call in accordance with the determination.
40. Apparatus according to claim 39 wherein said determining means includes
25 means for receiving a call record containing information on the call, and the allowance determining means is adapted to use the call record information in the determination.
41. Apparatus according to claim 39 or claim 40 wherein said allowance
30 determining means is adapted to determine that a call is to be disallowed if it lies significantly outside the stored pattern of calls specific to the origination.
42. Apparatus according to any one of claims 39 to 41 including adaptive means for adaptively modifying the stored pattern of calls specific to the origination.



to update the pattern to accommodate changes in calling behaviour of the origination.

43. Apparatus according to claim 42 wherein said adaptive means is operative
5 to carry out a weighted averaging operation wherein the most recent calls are given the highest weighting in the adaption process.

44. Apparatus according to any one of claims 39 to 43 wherein said determining
means is operative to determine the origination as at least one of the set comprising
10 a user or group identification code, a node or group of nodes in the telecommunications network, and a geographical location.

45. Apparatus according to any one of claims 39 to 44 including means for
determining the destination of the call, wherein said storage means is adapted to
15 store said pattern of calls which includes information on the call destination.

46. Apparatus according to claim 45 wherein said storage means is adapted to
store the information on the call destination which comprises information identifying
a node or group of nodes in the telecommunications network and/or a geographical
20 location.

47. Apparatus according to any one of claims 39 to 46 including means for
determining the time and/or day or date of the call, wherein said storage means is
adapted to store said pattern of calls which includes information on at least one of
25 the set of the time of day of the calls, the day or date of the calls, and the frequency of the calls.

48. Apparatus according to any one of claims 39 to 47 including means for
receiving an input code from the origination, means for validating the input code, and
30 means for receiving pattern update data from the origination and for updating said pattern of calls if the input code is valid.

49. A method of controlling access to a telecommunications network, the method comprising the steps of:



determining the origination of calls over the telecommunications network over a current period of time;

comparing a pattern of calls from an origination for the current period of time with an allowed pattern of calls; and

5 controlling access to the telecommunications network for originations based on the result of the comparison.

50. Apparatus for controlling access to a telecommunications network, the apparatus comprising:

10 first storage means for storing patterns of allowed calls for originations;
determining means for determining the origination of calls over the telecommunications network over a current period of time;

second storage means for storing patterns of calls from originations over the current period of time;

15 comparing means for comparing the stored patterns of calls from originations over the current period of time with the stored patterns of allowed calls;
and

control means for controlling access to the telecommunications network for the originations based on the result of the comparison.