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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 November 2003 (20.11.2003)

PCT

(10) International Publication Number
WO 03/096129 A1

(51) International Patent Classification[7]: G05B 13/00, H04Q 7/38

(21) International Application Number: PCT/AU03/00577

(22) International Filing Date: 13 May 2003 (13.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0210938.7 13 May 2002 (13.05.2002) GB

(71) Applicant *(for AE, AG, AL, AM, AT, AU, AZ, BA, BB, BE, BG, BR, BY, CA, CH, CN, CO, CR, CU, CY, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, FR, GB, GD, GE, GH, GM, GR, HR, HU, ID, IE, IL, IN, IS, IT, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MC, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SZ, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW only)*: **NEURAL TECHNOLOGIES LTD** [GB/GB]; Ideal House, Bedford Road, Petersfield, Hampshire GU32 3QA (GB).

(71) Applicant *(for BZ only)*: **TOMS, David** [AU/AU]; c/-Straits Resources, Level 1, 35 Ventnor Avenue, Perth, Western Australia 6005 (AU).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MANSLOW, John** [GB/GB]; 10 Wide Lane, Swaythling, Southampton, Hampshire SO18 2HH (GB). **BOLT, George** [GB/GB]; 1 Half Moon Cottage, Petersfield Road, Midhurst, Hampshire GU29 9LL (GB).

(74) Agent: **WALLACE, Rohan, James**; c/-Griffith Hack, 256 Adelaide Terrace, Perth, Western Australia 6000 (AU).

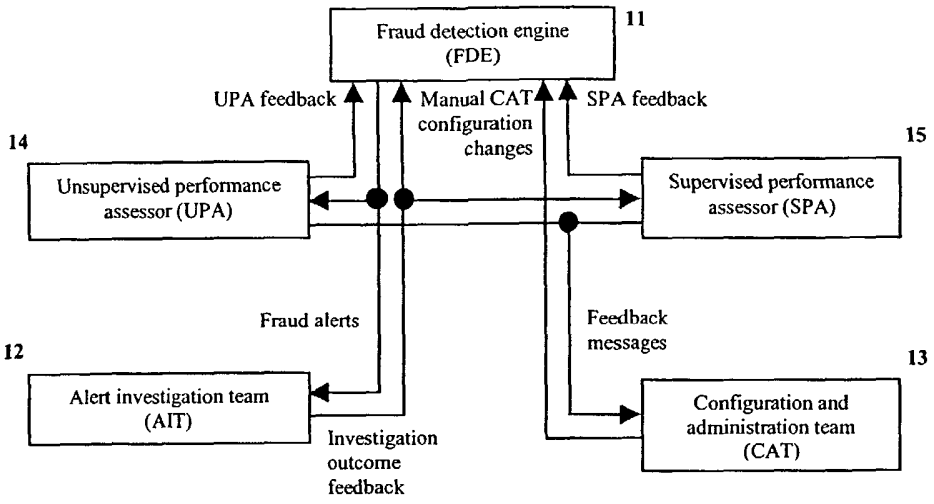
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: AN AUTOMATED PERFORMANCE MONITORING AND ADAPTATION SYSTEM



(57) Abstract: An event detection system (10) with an automatic performance monitoring and adaptation system therefore comprise an event detection engine (11) and a performance assessor (14 and 15). The event detection engine generates an alert if the specified event is suspected. An alert investigation team investigates if the alert is real of false. The performance assessor is configured to monitor the rate at which alerts and/or false alerts are generated by the event detection engine and to perform certain actions if the rate of alerts and/or false alerts falls outside a configurable range or crosses a threshold.

WO 03/096129 A1

AN AUTOMATED PERFORMANCE MONITORING AND ADAPTATION SYSTEM

FIELD OF THE INVENTION

[0001] The present invention relates to an automatic performance monitoring and adaptation system for adapting an event detection system to improve system performance.

BACKGROUND OF THE INVENTION

[0002] Fraud is a serious problem in modern telecommunications systems, and can result in revenue loss by the telecommunications service provider, reduced operational efficiency, and increased subscriber churn. In the highly competitive telecommunications sector, any provider that can reduce revenue loss resulting from fraud – either by its prevention or early detection – has a significant advantage over its competitors.

[0003] To minimise the impact of fraud, complex fraud detection systems are frequently employed, which are typically composed of large numbers of manually configured components. For example, many systems contain hundreds of hand-written rules that examine the system's input for known indicators of fraudulent activity. Terms within the antecedents of individual rules form yet more components that interact to determine the outcome of applying each rule. For example, the antecedent of the rule 'IF call duration is greater than 120 minutes AND call destination is an international number THEN call is fraudulent' consists of two components that interact to determine whether the rule fires. Most modern fraud detection systems support their rule-based components with other algorithms, such as scorecards (designed, for example, to estimate the chance that individual calls are fraudulent), and change detection algorithms (designed to highlight suspicious changes in behaviour).

[0004] Patterns in the behaviour of users of a telecommunications network change gradually as their fashions, habits, and socio-economic environment change. The introduction of new products also changes behaviour by encouraging and facilitating

new ways of using the network. For example, the growth of the Internet has led to a gradual increase in the number of long calls made by domestic subscribers to telecommunications services. These changes cause the performance of automated fraud detection systems to degrade with time, with increasingly large number of false alarms being generated, and increasingly large numbers of frauds being missed. This degradation is frequently ignored, or, according to present best practice, avoided by regular modifications to the fraud detection engine's configuration. Such reconfiguration is time consuming and expensive, however, and increases the risk of introducing errors.

[0005] Most fraud detection systems consist of at least two subsystems – a fraud detection engine (FDE), which analyses incoming data for evidence of fraudulent behaviour (in response to which it generates alerts), and an alert investigation team (AIT), which investigates the causes of the alerts to determine whether they were caused by an actual fraud. The data that the fraud detection engine monitors would typically be a call data record (CDR) stream within which descriptions of the characteristics of calls made on a telecommunications network appear shortly after their termination. A section of a real call data record is given in Table 1.

Table 1

CDR Field	Value
A_NO	11484XXXX
B_NO	11789XXXX
B_TY	2
CCU	1
CD	92
Sdate	05/05/98
Stime	11:13:28

[0006] The fields contained in the call data record are (from top to bottom) A-number (the number of the phone from which the call was made), B-number (the number to which the call was made), B-number type (whether the call was local, national,

international, etc. encoded as a number), the call's cost, its duration, and the date and time at which it started. Note that the four rightmost digits of the A- and B-numbers have been masked with 'X's to conceal the identities of the calling and called parties. The stream may also contain additional information, such as customer data (which can provide a customer's address, payment history, etc.). The fraud detection engine usually contains many components, including change detection algorithms (which search for the changes in behaviour that occur during periods of fraudulent activity), rules (which look for known characteristics of fraudulent behaviour), and data-driven classifiers such as neural networks (which can be trained using examples of real frauds to provide an indication of the likelihood that a fraud is in progress).

[0007] In addition to the fraud detection engine and alert investigation team, many systems add a configuration and administration team which is responsible for the initial configuration of the system (defining its rules, setting its sensitivity, deciding what data it will analyse, etc and it's maintenance through continual modification of the configuration to prevent to a slow deterioration of it's fault detection performance etc.).

SUMMARY OF THE PRESENT INVENTION

[0008] In accordance with a first aspect of the present invention there is provided a performance monitoring and adaptation system comprising at least:

a performance assessor configured to monitor the rate at which alerts are generated by an event detection system and to perform a first set of actions if the rate crosses a threshold.

[0009] In accordance with a second aspect of the present invention there is provided an event detection system comprising at least:

an event detection engine that generates an alert if the event is suspected; and

a performance assessor configured to monitor the rate at which alerts are generated by the event detection engine and to perform a first set of actions if the rate crosses a threshold.

[0010] Preferably the threshold is an end of a configurable range, wherein the first set

of actions is triggered if the rate falls outside of the range.

[0011] Preferably a configurable number of thresholds may be provided, each of which trigger a respective set of actions if the rate of alerts crosses the respective threshold.

[0012] Preferably the set of actions includes one or more actions.

[0013] Preferably the action of the first set of actions performed is determined by the direction in which the rate of alerts crosses the threshold.

[0014] Preferably the system further comprises a second performance assessor configured to monitor the rate at which false alerts are generated by the event detection system to perform a second set of actions if the rate of false alerts crosses a second threshold. False alerts are false positives, false negatives or both.

[0015] Preferably the second threshold is an end of a second configurable range, wherein the second set of actions is triggered if the rate of false alerts falls outside the second configurable range.

[0016] Preferably a configurable number of thresholds may be provided, each of which trigger a respective set of actions if the rate of false alerts crosses the respective threshold.

[0017] Preferably the action of the second set of actions performed is determined by the direction in which the rate of false alerts crosses the second threshold.

[0018] Preferably the first set of actions includes a first alert flood action conducted when the rate of alerts crosses above a configurable first upper trigger rate. Preferably the first set of actions includes a first alert drought action which occurs when the rate of alerts crosses below a first configurable lower trigger rate.

[0019] Preferably a lower reset threshold is built into the first lower trigger rate, such that the rate of alerts must rise above the first lower trigger rate added to a first lower threshold amount before the lower trigger will re-activate the first alert drought action after a previous activation. Preferably an upper reset threshold is built into the first upper trigger rate, such that the rate of alerts must fall below the first upper trigger rate less a first upper reset threshold amount before the upper trigger will re-activate the first alert flood action after a previous activation.

[0020] Preferably the second set of actions includes a second alert flood action which is triggered when a function of the false alert rate rises above a configurable second upper trigger rate. Preferably the second set of actions includes a second alert drought action which is triggered when a function of the rate of false alerts are under a second configurable lower trigger rate. Preferably the function is a moving average function.

[0021] Preferably a lower reset threshold is built into the range of rate of false alerts, such that the moving average of the rate of false alerts must rise above the second lower trigger rate added to a second lower reset threshold amount before the lower trigger will re-activate the second drought alert action.

[0022] Preferably an upper reset threshold is built into the range or rates of false alerts, such that the moving average of the rate of false alerts must fall below the second upper trigger rate less a second upper reset threshold amount before the second upper trigger will re-activate the second alert flood action.

[0023] Preferably the actions modify the event detection engine. Preferably the actions modify a respective parameter of the event detection engine.

[0024] Preferably the event detection engine is comprised of a plurality of components, wherein each component uses a different method to detect possible occurrences of the specified event. Preferably the performance assessor maintains a configurable number of configurable alert thresholds for each component.

[0025] Preferably the actions are conducted by execution of a respective script. Preferably each script can send signals to the event detection engine to modify the configuration of the event detection engine so as to produce a change in the rate of generation of alerts or false alerts.

[0026] Preferably each action includes sending a message to a configuration/administration team.

[0027] Preferably a positive transition script is associated with the first upper trigger rate and a negative transaction script is associated with the lower trigger rate. Preferably the positive transition script disables the associated event detection engine component and sends a message to the configuration/administration team. Preferably the negative transition script sends a message to the configuration/administration team.

[0028] Preferably the second performance assessor obtains false alert information from an alert investigation team that investigates whether each alert is real or false. Preferably the false alert information includes or is used to derive false art rates. Preferably the moving average is calculated by taking the average of the false negative or false positive rates over a configurable number of configurable periods. Preferably the second performance assessor identifies components within the event detection engine that are generating too many false alerts in response to normal activity or generating too few alerts in response to actual instances of the event.

[0029] Preferably the event detection engine detects events by inference. Typically, the event detective engine is a fraud detection engine.

[0030] In accordance with a third aspect of the present invention there is provided a performance monitoring and adaptation system for an event detection system comprising at least:

a performance assessor configured to monitor a function of the rate at which false alerts are generated by an event detection system and to perform a second set of actions if the function of the rate crosses a threshold.

[0031] In accordance with a fourth aspect of the present invention there is provided an event detection system comprising at least:

an event detection engine that generates an alert if the event is suspected; and

a performance assessor configured to monitor a function of the rate at which false alerts are generated by the specified event detection engine and to perform a second set of actions if the function of the rate crosses a threshold.

[0032] In accordance with a fifth aspect of the present invention there is provided a method of detecting an event from data comprising the steps of:

providing an event detection engine for analysing data for an indication of the event;

generating an alert if the event is suspected;

monitoring the rate at which alerts are generated by the event detection engine;

determining whether the rates crosses a threshold; and

if the rates crosses the threshold performing a first set of actions.

[0033] In accordance with a sixth aspect of the present invention there is provided a method of detecting an event from data comprising the steps of:

providing an event detection engine for analysing data for an indication of the event;

generating an alert if the event is suspected;

investigating whether the alert is real or false;

monitoring the rate at which false alerts are generated by the event detection engine;

determining whether the rate of false alerts crosses a threshold; and

if the rate of false alerts crosses the threshold performing a second set of actions.

BRIEF DESCRIPTION OF THE DRAWINGS

[0034] In order to provide a better understanding, preferred embodiments of the present invention will now be described with reference to the accompanying drawings, by way of example only, in which:

Figure 1 is a schematic representation of an indirect event detection system having an automatic performance monitoring and adaptation system according to the present invention; and

Figure 2 is an example showing hysteresis based threshold triggering based on rates of alert generated by the system of Figure 1.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0035] Referring to Figure 1, there is shown an automatic performance monitoring and adaptation system incorporated into an event detection system 10 which includes an event detection engine 11, an alert investigation team 12, a configuration and administration team 13, an unsupervised performance assessor 14 and a supervised performance assessor 15. The event detection engine 11 is a fraud detection engine used, for example, to indirectly detect fraud, (such as by inference), in a telecommunication network. It provides fraud alert messages to the alert investigation team 12. The alerts are also provided to the unsupervised performance assessor 14 to determine over time the rate of generation of alerts.

[0036] The unsupervised performance assessor 14 provides feedback to the fraud detection engine 11 based on the rates of alerts; and provides feedback messages to the configuration and administration team 13, alerting the team 13 of the feedback provided to the engine 11. The alert investigation team 12 investigates fraud alerts and provides feedback based on the outcome of that investigation to the fraud detection engine 11 and the supervised performance assessor 15. The supervised performance assessor 15 uses the investigation outcome feedback to determine rates of generation of false alerts. Based on the assessment of the rates of generation of false alert further feedback is provided by the supervised performance assessor 15 to the fraud detection engine 11. Feedback messages are also provided to the configuration and investigation team 13. Based on the alerts from the unsupervised performance assessor 14 and supervised performance assessor 15, the configuration and administration team 13 provides further manual configuration to the fraud detection engine 11 and components thereof.

[0037] The unsupervised performance assessor 14 and the supervised performance assessor 15 may be in the form of a programmed computer or a network of computers that may be independent from or form part of the overall fraud detection system. The unsupervised performance assessor 14 and supervised performance assessor 15 both automatically monitor the performance of individual components within the fraud detection engine 11 and according to the method described above provide so that the feedback is used to modify the behaviour of components of the fraud detection engine 11 to maximise fraud detection performance.

[0038] The unsupervised performance assessor 14 monitors the rates at which individual fraud detection engine components generate alerts, and execute scripts to provide the feedback to the fraud detection engine 11 should the rates fall below or rise above acceptable levels set by the configuration and administration team 13. The unsupervised performance assessor 14 estimates the alert rate for each component within the fraud detection engine 11 by counting the number of alerts generated by each component over a configurable period of time. The period should be as long as possible to minimise the random variation in the measured alert rate (which results from the finite size of the sample of alert instances), but as short as possible to minimise the response time of the unsupervised performance assessor 14. In practice a time period of one hour has been found to provide a good trade off between these requirements in systems that monitor call data records in telecommunications networks.

[0039] For each fraud detection engine 11 component, the unsupervised performance assessor (UPA) maintains a configurable number of configurable alert rate thresholds. Associated with each threshold is a hysteresis, and a pair of scripts, which control the action taken by the UPA 14 when each threshold is passed as a component's alerts rate either increases or decreases. The script executes when a component's alert rate passes the threshold as it decreases is referred to as the negative transition script. The script executed when the components alert rate passes the other threshold as it increases is referred to as the positive transition script. The hysteresis is provided to reset the triggering of the respective script to stop the positive and negative transition scripts

being executed in rapid succession as a result of random variation in a component's alert rate when it lies close to one of the thresholds.

[0040] For example, a threshold of 0.001 percent could be defined with a hysteresis of 0.001 percent. A component of the fraud detection engine 11 that starts off with an alert rate of 0.1 percent would not cause either of the scripts associated with the threshold to be executed. If its alert rate fell below the 0.001 percent, however, the negative transition script associated with the threshold would be executed. If the alert rate repeatedly crossed the threshold, the negative transition script would not be re-executed unless the alert rate first rose above the threshold plus the hysteresis (i.e. rose above 0.002 percent), causing the positive transition script to be executed. Thereafter, if the alert rate repeatedly crossed the threshold plus the hysteresis, the positive transition script would not be re-executed unless the alert rate first fell below the threshold. The hysteresis-based operation of the thresholds, and the points of execution of the positive and negative transition scripts is illustrated in Figure 2.

[0041] The scripts can send signals to the fraud detection engine 11 components, and the signals may be used to modify the configurations of these components. Different fraud detection engine 11 components can accept different signals from the scripts, depending on their design and implementation. For example, a change detection algorithm within the fraud detection engine 11 may be able to accept signals instructing it to reduce its sensitivity by a specific amount (for example, by increasing an internal threshold), whereas a neural network may only be able to accept a signal instructing it to disable itself. Alternatively, rather than the change detection algorithm adjusting its sensitivity in response to a signal generated by a script, its sensitivity could be specified explicitly in the algorithm's configuration, and modified directly by the script without any signal being sent to the algorithm itself.

[0042] Scripts can also send messages to the configuration and administration team 13 to inform them that alert thresholds have been passed. This provides the team 13 with important information about the performance of individual fraud detection engine 11 components that is useful for maintaining the system's configuration. For example,

when the configuration is reviewed by the configuration and administration team 13, the messages sent by the scripts tell the team 13 which components in the original configuration generated too many or too few alerts, and hence need to be modified. A typical application of the unsupervised performance assessor 14 is to define two thresholds: 1) the 'flood' threshold, which identifies fraud detection engine 11 components that generate too many alerts, and 2) the 'drought' threshold, which identifies fraud detection engine 11 components that generate too few. The flood threshold would be defined to be around 5 percent or so (depending on the rate at which the alert investigation team 12 can process alerts), and the drought threshold to be around 0.001 percent. Hystereses associated with each of 4 and 0.001 percent have been found to work well in practice.

[0043] The positive transition script associated with the flood threshold is set to disable the associated fraud detection engine 11 component and send a message to the configuration and administration team 13, as shown below.

```
OnPositiveTransitionOfFloodThreshold( FDEComponentID )
{
      SendMessage ( 'Warning: FDE component ' FDEComponentID' is in
flood and has been disabled' )
      Disable ( FDEComponentID )
}
```

The negative transition script associated with the drought threshold is set to send a message to the configuration and administration team 13 but to leave the fraud detection engine 11 component enabled below.

```
OnNegativeTransitionOfDroughtThreshold( FDEComponentID )
{
SendMessage ( 'Warning: FDE component' FDEComponentID 'is in drought' )
}
```

In the pseudo-code, the functions 'OnPositiveTransitionOfFloodThreshold' and 'OnNegativeTransitionOfDroughtThreshold' are passed to identifiers of the fraud

detection engine 11 components responsible for the scripts being invoked. The identifiers are numeric, alphanumeric, or alphabetic strings that are associated with, and unique to, each fraud detection engine 11 component. For example, a change detection component within the fraud detection engine 11 that monitors the cost of calls may be given the identifier 'ChangeDetector_UniversalCallCost'. The argument of the 'SendMessage' function is the string that is to be sent to the configuration and administration team 13. Note that the identifier responsible for the script's execution is inserted into that string in the pseudo-code so that, for example, if the aforementioned change detection algorithm caused the positive flood transition script to be executed, the message 'Warning: FDE component ChangeDetector_CallCost is in flood and has been disabled' would be sent to the configuration and administration team.

[0044] The negative and positive transition scripts associated with the flood and drought thresholds respectively may be empty (i.e. they do nothing). Alternatively, if the unsupervised performance assessor 14 be configured to disable fraud detection engine 11 components that generate unexpectedly large numbers of alerts, which would swamp the alert investigation team 12 if they were allowed to continue, but only warns the configuration and administration team 13 if a component generates too few alerts so that its configuration can be modified at the next configuration review.

[0045] An alternative arrangement could add an additional 'flood warning' threshold at around 3 percent, with a hysteresis of 2 percent. By setting its positive transition script to send a warning message to the configuration and administration team 13, the team 13 can be issued with a warning that a fraud detection engine 11 component is at risk of being disabled by the positive transition flood threshold script, allowing time for the team 13 to modify the component's configuration to reduce its alert rate before this occurs.

[0046] Monitoring the alert rate of fraud detection engine 11 components with the unsupervised performance assessor 14 is of great practical importance because it allows components that are generating too few or too many alerts to be identified. For example, if a component generates too many alerts, the throughput of the system is reduced by the

overhead of processing the alerts and transferring them to the alert investigation team 12. This can cause the fraud detection system to lag behind its input, producing a backlog and robbing the system of its ability to search for fraud in real time. This increases the amount of time that frauds can persist before they are detected and stopped, increasing the revenue lost by the network operator. Any component that generates a large number of alerts is also likely to be generating many more alerts in response to events that are not frauds than those that are, and is thus a poor fraud detector. The overall fraud detection performance of the system could therefore be improved by modifying the configuration of the component or removing it altogether.

[0047] A fraud detection engine 11 component that generates too few alerts is also problematic, because the resources it uses within the system may not be justified by its fraud detection abilities. (For example, this is certainly the case for a component that never generates alerts.) Such components can usually operate at higher sensitivities without generating an excessive number of alerts, while also offering increased speed and strength of response to actual fraud events. Alternatively, the performance of the system can sometimes be improved if these components are removed completely because the increase in throughput that results can increase the speed at which frauds are detected, thus reducing the revenue lost by the network operator before the fraud is stopped. By allowing the unsupervised performance assessor 14 to execute configurable scripts when the alert rates of individual fraud detection engine 11 components rise above, or fall below, configurable thresholds, the assessor 14 can respond to changes in the alert rates of individual fraud detection engine 11 components far faster than can the configuration and administration team 13. A fraud detection system with a UPA-type mechanism is thus able to respond to changes in its environment, far more quickly than one without.

[0048] The supervised performance assessor (SPA) 15 is similar to the unsupervised performance assessor 14, except that the supervised performance assessor 15 uses feedback provided by the alert investigation team 12 to maintain statistics on, and apply thresholds to, a function of the false positive and false negative rates of fraud detection engine 11 components. A false positive occurs when a fraud detection engine 11

component generates an alert that, upon investigation by the alert investigation team 12 turns out not to be associated with a real fraud. Conversely, a false negative occurs when a fraud detection engine 11 component fails to generate an alert for an event that was part of a fraud. Thresholds within the supervised performance assessor 15 are defined on the function of the false negative and false positive rates of fraud detection engine 11 components, and trigger the execution of scripts in the same way as scripts are triggered within the unsupervised performance assessor 14. The function of the false negative and false positive rates of fraud detection engine 11 components are moving averages of their false negative and false positive rates over a configurable number of configurable periods. For example, a period of one day is often chosen as the configurable period, and the moving average is taken over a fourteen day window of such periods.

[0049] Like the unsupervised performance assessor 14, the supervised performance assessor 15 has an important role to play in maintaining good fraud detection performance within the system by identifying components within the fraud detection engine 11 that are generating too many fraud alerts in response to normal activity, or generating too few alerts in response to fraud. The former are problematic because they use system resources – particularly those of the alert investigation team 13 – to search for fraudulent activity that does not exist. This increases the amount of time that the team 12 takes to identify the real frauds, and hence increases the revenue lost by the network operator to the fraudsters before the fraud is stopped. If a fraud detection engine 11 component generates too few alerts in response to real frauds, it is likely that its sensitivity could be increased, with the result that it responds more rapidly to real fraud events. The SPA's ability to automatically execute scripts in response to false positive and false negative alert rate moving averages crossing thresholds means that it can adapt the fraud detection engine 11 components far more rapidly to changing conditions than can a fraud detection system that relies on human intervention.

[0050] The skilled addressee will realise that the present invention provides advantages over existing fraud detection systems that do not have a performance assessor automatically monitoring the performance of the fraud detection engine. The

overall systems performance in terms of fraud detection sensitivity, and throughput, may be maximised as well as minimising the number of false alerts sent to the alert investigation team.

[0051] Modifications and variations may be made to the present invention without departing from the basic inventive concept. Such modifications may include adapting the system to other specified event detection circumstances. The alert investigation team and configuration and administration team may overlap or be the same unit. The alert investigation team and/or configuration/administration team may be partly or wholly automated or include expert systems. Such modifications and variations and intended to fall within the scope of the present invention, the nature of which is to be determined by the foregoing description.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A performance monitoring and adaptation system for an event detection system comprising at least:

a performance assessor configured to monitor the rate at which alerts are generated by an event detection system and to perform a first set of actions if the rate crosses a threshold.

2. In accordance with the present invention there is provided an event detection system comprising at least:

an event detection engine that generates an alert if the event is suspected; and

a performance assessor configured to monitor the rate at which alerts are generated by the event detection engine and to perform a first set of actions if the rate crosses a threshold.

3. A system according to either claim 1 or 2, wherein the threshold is an end of a configurable range, wherein the first set of actions is triggered if the rate falls outside of the range.

4. A system according to either claim 1 or 2, wherein a configurable number of thresholds may be provided, each of which trigger a respective set of actions if the rate of alerts crosses the respective threshold.

5. A system according to either claim 1 or 2, wherein the first set of actions includes one or more actions.

6. A system according to either claim 1 or 2, wherein the first set of actions includes more than one action, one or more actions of the first set of actions is performed, said one or more actions being determined by the direction in which the rate of alerts crosses the threshold.

7. A system according to either claim 1 or 2, wherein the system further comprises

a second performance assessor configured to monitor the rate at which false alerts are generated by the event detection system to perform a second set of actions if the rate of false alerts crosses a second threshold.

8. A system according to claim 7 wherein the second threshold is an end of a second configurable range, wherein the second set of actions is triggered if the rate of false alerts falls outside the second configurable range.

9. A system according to claim 7, wherein a configurable number of thresholds may be provided, each of which trigger a respective set of actions if the rate of false alerts crosses the respective threshold.

10. A system according to claim 7, wherein the second set of actions includes more than one action, one or more actions of the second set of actions is performed, said one or more actions being determined by the direction in which the rate of false alerts crosses the second threshold.

11. A system according to claim 3, wherein the first set of actions includes a first alert flood action conducted when the rate of alerts crosses above a configurable first upper trigger rate.

12. A system according to claim 3, wherein the first set of actions includes a first drought action which occurs when the rate of alerts crosses below a first configurable lower trigger rate.

13. A system according to claim 12, wherein a lower reset threshold is built into the first lower trigger rate, such that the rate of alerts must rise above the first lower trigger rate added to a first lower reset threshold amount before the lower trigger will re-activate the first alert drought action after a previous activation.

14. A system according to claim 11, wherein an upper reset threshold is built into the first upper trigger rate, such that the rate of alerts must fall below the first upper

trigger rate less a first upper reset threshold amount before the upper trigger will re-activate the first alert flood action after a previous activation.

15. A system according to claim 7, wherein the second set of actions includes a second alert flood action which is triggered when a function of the false alert rate rises above a configurable second upper trigger rate.

16. A system according to claim 7, wherein the second set of actions includes a second alert drought action which is triggered when a function of the rate of false alerts falls under a configurable second lower trigger rate.

17. A system according to either claim 1 or 2, wherein the first set of actions modify the event detection engine.

18. A system according to either claim 1 or 2, wherein the first set of actions modify a respective parameter of the event detection engine.

19. A system according to either claim 1 or 2, wherein the first set of actions include sending a message to a configuration and/or administration team.

20. A system according to claim 7, wherein the second performance assessor obtains false alert statistics from an alert investigation team that investigates whether an alert is real or false.

21. A system according to claim 1, wherein the event detection system is a fraud detection system.

22. A system according to claim 2, wherein the event detection engine is a fraud detection engine.

23. A performance monitoring and adaptation system for an event detection system comprising at least:

a performance assessor configured to monitor a function of the rate at which false alerts are generated by an event detection system and to perform a first set of actions if the function of the rate crosses a threshold.

24. In accordance with the present invention there is provided an event detection system comprising at least:

an event detection engine that generates an alert if the event is suspected; and

a performance assessor configured to monitor a function of the rate at which false alerts are generated by the specified event detection engine and to perform a first set of actions if the function of the rate crosses a threshold.

25. A system according to either claim 23 or 24, wherein the system further comprises a second performance assessor configured to monitor the rate at which alerts are generated by the event detection system to perform a second set of actions if the rate crosses a threshold.

26. A method of detecting an event from data comprising the steps of:

providing an event detection engine for analysing data for an indication of the event;

generating an alert if the event is suspected;

monitoring the rate at which alerts are generated by the event detection engine;

determining whether the rates crosses a threshold; and

if the rates cross the threshold performing a set of actions.

27. A method of detecting an event from data comprising the steps of:

providing an event detection engine for analysing data for an indication of the event;

generating an alert if the event is suspected;

investigating whether the alert is real or false;

monitoring the rate at which false alerts are generated by the event detection engine;

determining whether the rate of false alerts crosses a threshold; and

if the rate of false alerts crosses the threshold performing a set of actions.

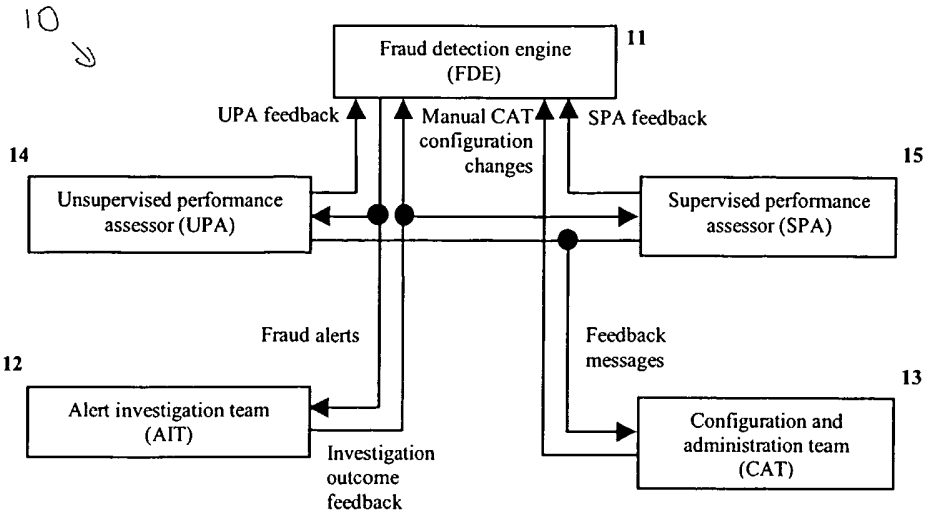

10
Fraud detection engine (FDE)
11
UPA feedback
Manual CAT configuration changes
SPA feedback
14
15
Unsupervised performance assessor (UPA)
Supervised performance assessor (SPA)
Fraud alerts
Feedback messages
12
13
Alert investigation team (AIT)
Configuration and administration team (CAT)
Investigation outcome feedback

Fig. 1

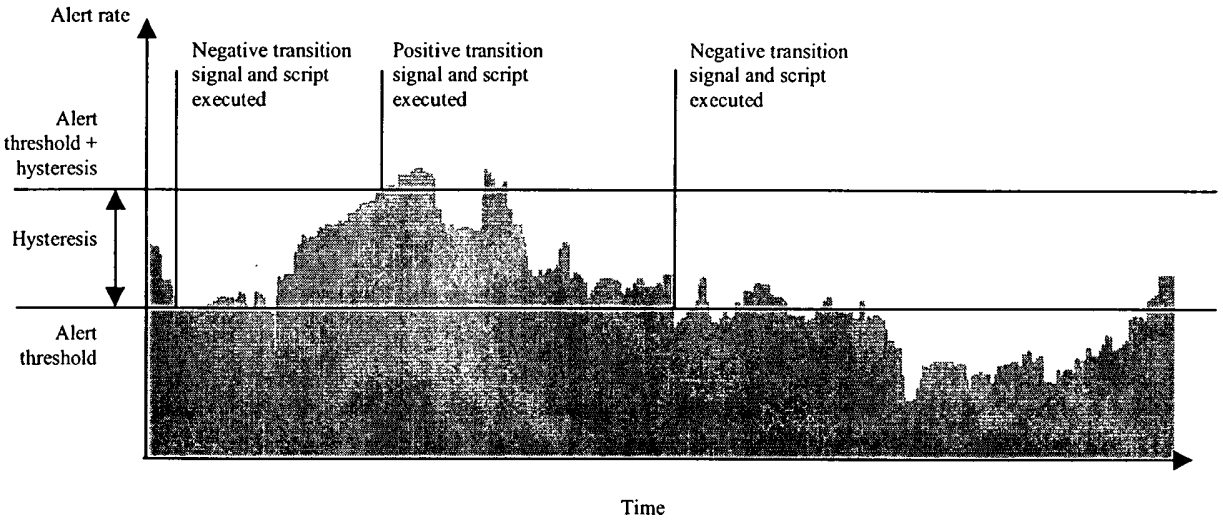

Alert rate
Negative transition signal and script executed
Positive transition signal and script executed
Negative transition signal and script executed
Alert threshold + hysteresis
Hysteresis
Alert threshold
Time

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/00577

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G05B 13/00, H04Q 7/38

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)

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 practicable, search terms used)
WPAT, USPTO, INSPEC, ESPACE. KEYWORDS: ADAPTIVE, HISTORY, THRESHOLD, EVENT, FAULT, ALERT, RATE, TELEPHONE AND SIMILAR.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00/47006 A1 (NOKIA NETWORKS OY et al) 10 August 2000 Whole document including figure 1 and page 7 line20 to page 10 line 30	1 - 27
X	US 5819226 A (GOPINATHAN et al) 6 October 1998 Whole document including abstract, column 2 lines 39 to 43, and column 31 line 49 to column 32 line 31.	1 - 27
X	US 4213127 A (COLE) 15 July 1980 Whole document.	1 - 27

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 June 2003	06 JUN 2003
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **RICHARD REED** Telephone No : (02) 6283 7927

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/00577

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6327352 B1 (BETTS et al) 4 December 2001. Whole document.	
A	Wo 00/64193 A2 (AMDOCS (ISRAEL) LTD) 26 October 2000. Whole document.	
A	US 5966650 A (HOBSON et al) 12 October 1999. Whole document.	
A	US 5627886 A (BOWMAN) 6 May 1997. Whole document.	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU03/00577

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	200047006	AU	25204/99				
US	5819226	AU	48500/93	EP	669032	WO	9406103
		US	6330546				
US	4213127	NONE					
US	6327352	AU	66642/98	US	2002071538	WO	9839899
WO	200064193	AU	200039862	BR	200011200	CA	2371132
		US	6526389	US	2002184080		
US	5966650	CA	2223521	EP	838123	GB	2303275
		WO	9703533				
US	5627886	NONE					

END OF ANNEX