Forensic Science International xxx (2009) xxx–xxx

Contents lists available at ScienceDirect

Forensic Science International

journal homepage: www.elsevier.com/locate/forsciint

A fraud management system architecture for next-generation networks

M.A. Bihina Bella *, J.H.P. Eloff, M.S. Olivier

Information and Computer Security Architectures (ICSA) Research Group, Department of Computer Science, University of Pretoria, Pretoria, South Africa

ARTICLE INFO

Article history:
Received 21 January 2008
Received in revised form 9 December 2008
Accepted 19 December 2008
Available online xxx

Keywords:
Fraud management system (FMS)
Internet protocol (IP)
Internet protocol detail record (IPDR)
Next-generation network (NGN)
Self-organising map (SOM)
Telecommunications fraud

ABSTRACT

This paper proposes an original architecture for a fraud management system (FMS) for convergent. Next-generation networks (NGNs), which are based on the Internet protocol (IP). The architecture has the potential to satisfy the requirements of flexibility and application-independency for effective fraud detection in NGNs that cannot be met by traditional FMSs. The proposed architecture has a thorough four-stage detection process that analyses billing records in IP detail record (IPDR) format – an emerging IP-based billing standard – for signs of fraud. Its key feature is its usage of neural networks in the form of self-organising maps (SOMs) to help uncover unknown NGN fraud scenarios. A prototype was implemented to test the effectiveness of using a SOM for fraud detection and is also described in the paper.

1. Introduction

Telecommunications fraud management is a broad field that generally encompasses all aspects of detecting, managing and investigating any attempt – successful or not – to steal by deception or to deliberately abuse services offered via a telecommunications system [1]. These processes can be automated through a fraud management system (FMS) that systematically analyses customers' usage records generated for billing purposes in the form of call detail records (CDRs) [2]. FMSs are invaluable tools to network operators as they can help significantly reduce revenue leakage due to fraud.

Indeed, telecommunications fraud is a widespread problem that generally costs operators between 3% and 8% of their annual revenue, in addition to severely damaging their reputation and jeopardising their customer relationships. This amounts to more than USD 44 billion globally [3]. One typical fraud scenario is that of subscription fraud associated with call selling, whereby an individual subscribes to a phone service with no intention to pay and by providing false personal details. He then resells these fraudulently obtained phone services (usually high-rate international calls) at cheap rates [4]. Fraud is ever evolving and is likely to worsen in next-generation networks (NGNs) due to the advent of new technologies and services.

NGNs refer to emerging converged networks for voice, video and data traffic based on the Internet protocol (IP) [5]. As such, NGNs belong to *data-communications* (the interaction between computers), in contrast to traditional *telecommunications* (distance communications via telephones) [6]. This creates new challenges for fraud management in NGNs as currently available FMSs were designed specifically for telecommunications networks and thus lack the flexibility to accommodate new IP-based services, their billing models and associated fraud scenarios.

Traditional FMSs are application-specific as they depend on the type of service offered and its underlying network technology. For this reason, different FMSs are deployed to uniquely address specific types of fraud [7]. With the introduction of a multitude of new services in NGNs, the application-specificity of current FMSs will become a serious obstacle to effective fraud detection. This situation is accentuated by the fact that traditional FMSs place a strong emphasis on rule-based fraud detection [8] which uses rules or signatures that define characteristics of a known fraud type. Rigid rule-based FMSs cannot detect previously unknown NGN fraud patterns.

The new fraud attacks in NGNs mostly target the *content* of the service (e.g. multimedia content) rather than the *connection* to the service, since the value of the content largely exceeds the cost of the connection [9]. One typical example of a content-based fraud type is the illegal redistribution of a service whereby a legitimate customer downloads multimedia content such as a movie and illegally redistributes it to other individuals. The redistribution can

* Corresponding author at: Information and Computer Security Architectures (ICSA) Research Group, Department of Computer Science, University of Pretoria, Pretoria, South Africa. Tel.: +27 12 482 0000/012 420 3035; fax: +27 12 482 0326.
E-mail addresses: mbihina@yahoo.fr (M.A. Bihina Bella), eloff@cs.up.ac.za (J.H.P. Eloff), martin@mo.co.za (M.S. Olivier).

0379-0738/$ – see front matter © 2008 Elsevier Ireland Ltd. All rights reserved.
doi:10.1016/j.forsciint.2008.12.013

be free of charge or at a low cost. Redistributing media involves breaking the encryption mechanism used to protect the broadcast material. It is very hard to detect occurrence of this fraud by using only network indicators, since the fraudster may be likely to reproduce and resell the content on a storage device (e.g. CD-ROM, DVD) instead of redistributing it over the network [10].

More appropriate tools are therefore needed for managing NGN fraud. The design methodology of such a tool is described in Ref. [11] and an initial fraud detection model based on that methodology was presented in Ref. [12]. The current paper presents the original NGN FMS architecture that resulted from the fraud detection model referred to above. In addition to its flexibility due to its modular design, the proposed architecture has the benefits of being largely scalable and able to discover unknown fraud patterns.

The remainder of the paper is organised as follows. Section 2 reviews previous work in the field of fraud detection for NGNs and contrasts previous solutions to the approach presented in the current paper. Section 3 presents the NGN FMS architecture proposed for NGNs. Section 4 describes the prototyping of a so-called self-organising map (SOM) analyser module of the architecture. The prototype implementation focuses on the SOM analysis as it is the key novelty of the architecture and the tool used to detect unknown NGN fraud scenarios. An evaluation of the architecture and of the test results is provided in Section 5, followed by Section 6 that concludes the paper.

2. A review of previous work in NGN fraud detection

The EURESCOM (European Institute for Research and Strategic Studies in Telecommunications) project P1007, which was carried out between 2000 and 2002, is the most significant recent contribution to the area of NGN fraud detection [13]. The project looked at how intelligent techniques from the domains of learning, personalisation and data-mining could improve fraud detection in future high-value IP services. A technique that was proposed is the emerging pattern detection (EPD) [14]. The EPD attempts to detect new forms of fraud by comparing two data sets – one with "clean" usage records and another one supposedly containing fraudulent records – to identify patterns recurring in the second data set but not present in the first data set. One drawback of this solution is that, prior to the investigation, the user must know or at least assume that fraud exists in one data set. This implies that some knowledge about the new fraud scenarios should already exist.

Students from the Chalmers University of Technology in Sweden participated actively in the EURESCOM Project P1007. Master's students from this university published several theses on the subject of IP fraud detection. For example [10] studied fraud detection in IP multicast services and determined likely fraud scenarios and their fraud indicators for such services. [15] investigated fraud in IP multimedia services and proposed the integration of the functionality of an IDS (intrusion detection system) into the FMS. [8] suggested the combination of fraud and intrusion detection techniques for future fraud scenarios.

Apart from EURESCOM, a few other institutions also conducted research projects on IP fraud detection. The first of these was the Master's thesis jointly written by [6] from the Swedish Royal Institute of Technology, who tested the efficiency of a commercial FMS called Visual CDR in detecting some likely IP fraud scenarios. Their research concluded that Visual CDR and similar products will need improvement in the area of input data collection to cater for future fraud types.

In 2004, Hearne, a student at the Waterford Institute of Technology in Ireland, published his Master's thesis [16] on the problem of fraud management for NGNs. [16] proposed a high-level architecture for a rule-based FMS capable of analysing data in flexible formats. The main novelty of this architecture was that it had rules specific to each service offered. The obvious disadvantage was that knowledge was needed about the particular fraud type in order to define appropriate rules. No allowance was therefore made for the detection of unknown NGN fraud types.

Except for Ref. [16], the earlier researchers do not propose a new FMS architecture to address the lack of flexibility that characterises existing FMSs. No novel technique is suggested for the effective detection of unknown NGN fraud scenarios either. The current paper attempts to fill this gap by presenting an FMS architecture specifically designed to meet the requirement of flexibility for effective fraud detection in NGNs. A powerful data analysis method is also proposed to help discover unknown fraud patterns. Some suggestions made by the researchers referred to above are used in the architecture design, such as:

- Incorporating intrusion detection technology into the FMS, more specifically using IDS logs in the fraud detection process.
- Using service-specific fraud detection modules as suggested by [16].

3. The NGN FMS architecture

This section presents the FMS architecture proposed for effective fraud detection in NGNs. It starts with a discussion of some main challenges to fraud detection, followed by a list of requirements for NGN FMSs. Finally the NGN FMS architecture is described in detail.

3.1. Challenges to fraud detection

Effective fraud detection presents many challenges, among which are the high number of detection errors that can be generated by an FMS and the potential breach of user privacy. These are directly related to the fraud detection approach used.

There are two approaches to fraud detection: absolute analysis and differential analysis. Absolute analysis seeks calling patterns of previous fraud attacks to detect occurrences of these attacks. Differential analysis looks for deviations from users' past calling patterns that were considered normal [17]. Both fraud detection approaches try to minimise the number of errors that may occur during the detection process.

Fraud detection errors can be of two kinds: false positives and false negatives. A false positive occurs when an alarm is generated although there is no attack. In contrast, a false negative happens when no alarm is generated despite an attack [18]. Typically, false negatives result in revenue loss while false positives generate more workload for the fraud analysts [6]. Indeed, once a fraud has been detected, the alarm as well as the related fraudulent records is logged by the FMS. The fraud analyst can use that information to either immediately suspend the customer account or to collect more evidence such as verifying the customer's identity. As a source of revenue loss, false negatives are therefore usually far more threatening for the operator.

Differential analysis generally produces fewer false negatives than absolute analysis. However, it requires the creation of user profiles providing a detailed overview of a customer's usage patterns, which can greatly compromise a user privacy. In case an event is deemed suspicious, the fraud analyst may need to confirm the user's identity (e.g. by calling him) which may endanger the user's privacy even more. On the contrary, absolute analysis is less of a threat to privacy since no customer profile is created and the identity of the user is not needed to identify a fraudulent event. However, it generates a lot of false negatives when new fraud attacks are committed, since it looks only for known fraud

Please cite this article in press as: M.A. Bihina Bella, et al., A fraud management system architecture for next-generation networks, Forensic Sci. Int. (2009), doi:10.1016/j.forsciint.2008.12.013

patterns. It therefore allows many fraudulent transactions to go undetected.

In order to achieve a fair balance between user privacy and the success rate of the FMS, both fraud detection approaches need to be implemented.

3.2. Requirements for NGN FMSs

In light of the above dicussion and the challenges to fraud detection in NGNs mentioned earlier, the authors have identified the following requirements for an effective NGN FMS.

- *Flexibility*: The FMS must be application independent to detect any type of fraud for any type of service, regardless of its underlying technology. The FMS architecture must also be flexible to enable the easy addition, removal and update of fraud detection algorithms to accommodate changing fraud scenarios.
- *Complete network coverage*: The FMS needs to analyse all the data flowing through all the different access points in NGNs. Indeed, due to the availability of several access mechanisms in NGNs (e.g. wired, wireless, cable, modem), fraud attacks can be launched from various access points simultaneously.
- *Scalability*: New fraud scenarios will appear, which implies that more fraud rules will have to be added to the FMS detection engine. The number of billing records to inspect will also increase with the new services offered. Old fraud attacks, on the other hand, may disappear over time when their associated services are no longer offered. The FMS architecture must be able to easily scale up or down to accommodate the dynamic NGN environment.

The FMS architecture that was designed to satisfy these requirements is described in the next section.

3.3. Description of the NGN FMS architecture

The proposed NGN FMS architecture is shown as a UML (Unified Modelling Language) component diagram in Fig. 1. The UML notation is used because it is a standard system modelling language used worldwide [19].

Only the unshaded blocks in Fig. 1 represent the components of the FMS. The shaded blocks (the billing system and the IDS) are entities that do not belong to the FMS although they are used during the fraud detection process. As shown in Fig. 1, the FMS consists of seven main components that are listed below in their logical sequence:

- The Intrusion-based Fraud Detector.
- The General Fraud Detector.
- The IPDR Dispatcher.
- A Service-specific Fraud Detector.
- The SOM Analyser.
- The Alarm Manager.
- The Case Manager.

Each of these components processes the usage records from the billing system. The billing records are in the IPDR format [20] and are therefore referred to as IPDRs in the remainder of the paper. IPDR is an emerging and flexible billing standard for IP-based services. A detailed discussion of the IPDR and its advantages over traditional billing standards is documented in Ref. [21].

The seven main components of the NGN FMS are used to perform a thorough multi-stage fraud detection process, which goes from a very general to a very service-specific analysis in the terms as explained below.

The IPDRs are first compared to known general intrusions in the Intrusion-Based Fraud Detector, and to general fraud scenarios in the General Fraud detector. Next, they are analysed with fraud rules (Service-specific Fraud Detectors) that are specific to each service type. When at any of the above stages any of the IPDRs are identified as suspicious, they are not sent to the next module but to the Alarm Manager which promptly raises an alarm. The IPDRs are also processed by the SOM Analyser to identify anomalies suggestive of unknown fraud scenarios. Finally the Case Manager is used to conduct further investigation into a likely fraud attack, either due to the alarms generated by the

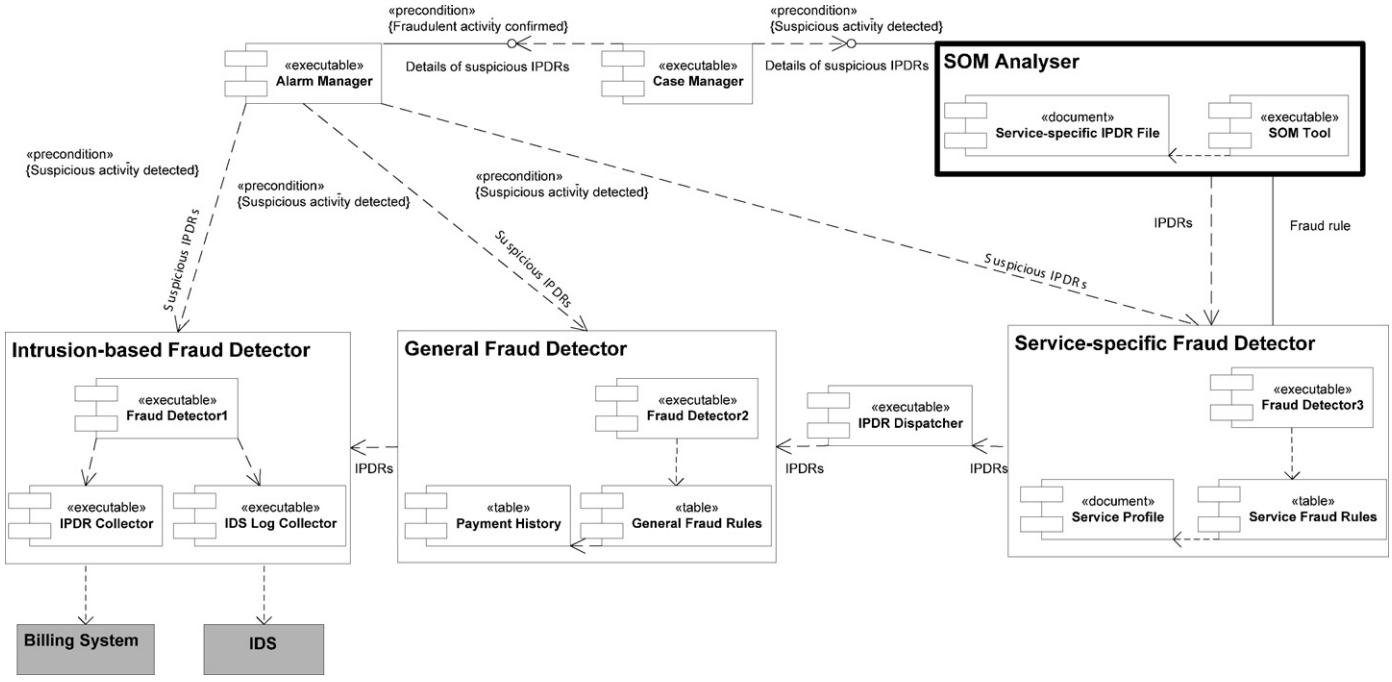

Fig. 1. UML component diagram of the NGN FMS architecture.

Please cite this article in press as: M.A. Bihina Bella, et al., A fraud management system architecture for next-generation networks, Forensic Sci. Int. (2009), doi:10.1016/j.forsciint.2008.12.013

Alarm Manager or based on the suspicious patterns revealed by the SOM Analyser.

Although the FMS architecture shown in Fig. 1 is designed to accommodate any type of service, this paper focuses on two types of service only: phone calls and media-on-demand services. Phone calls are traditional voice services, while media-on-demand refer to an IP-based service combining multimedia and data content. Both these services are highly vulnerable to fraud attacks and combining them gives a good indication of a simple but typical NGN service. For illustration, the FMS described presently is used by an operator that offers two services: mobile phone calls and video-on-demand (VoD). The videos are accessible from the operator's website and can be downloaded to the user's mobile phone.

A more detailed description of the main components of the architecture follows.

3.3.1. The Intrusion-based Fraud Detector

Application of the Intrusion-based Fraud Detector constitutes the first phase of analysing the IPDRs. It compares the IDS log files to the billing records to provide full coverage of the network traffic. The IDS analyses network traffic for signs of intrusions, which include any attempt to compromise the confidentiality, integrity and availability of the operator's data [18]. The Intrusion-based Fraud Detector has three sub-components: the IPDR Collector, the IDS Log Collector and the Fraud Detector.

- The IPDR Collector retrieves IPDRs from the billing system.
- The IDS Log Collector extracts IDS logs from the IDS.
- The Fraud Detector compares entries from both collectors to determine if a network intrusion detected by the IDS corresponds to an IP address in the IPDRs. Indeed, for every intrusion detected by the IDS, an alarm is generated in the FMS.

For example, if the IDS detects a hacking attack, the source IP address of the hacking is compared to the source IP address of the VoD IPDRs in the IPDR Collector. If a match is found, this could suggest a fraudster's attempt to get unauthorised access to the video database. This allows the fraud attack to be detected before the videos are illegally accessed.

3.3.2. The General Fraud Detector

The General Fraud Detector is a rule-based fraud detection module that inspects the IPDRs with general fraud rules and thresholds applicable to all the service types offered by the operator. Rule-based analysis is an absolute analysis technique. The General Fraud Detector consists of three sub-components:

- The General Fraud Rules table stores the fraud rules.
- The Payment History table stores details about every user's account status and past usage behaviour. This information is used to define general thresholds included in the rules.
- The Fraud Detector applies the fraud rules to the IPDRs.

The fraud rules in the General Fraud Detector are very basic and used to for the quick identification of obvious cases of fraud. Examples of fraud cases stored in the General Fraud Rules table and applicable to both the mobile calls service and the VoD service are listed below.

- *Unknown customer*: An IPDR is received from a subscriber not present in the Payment History table.
- *Blacklisted customer*: The calling number or source IP address matches an entry in a blacklist of the operator.
- *Collision*: Simultaneous calls or logins are received from the same number or user account.

```
If service-type = "MobileCall" then send IPDR to MobileCalls-specific Fraud Detector
Else if service-type = "VoD" then send IPDR to VoD-specific Fraud Detector
```

Fig. 2. Illustration of the entries in the IPDR Dispatcher.

3.3.3. The IPDR Dispatcher

The IPDR Dispatcher identifies the type of service recorded in the IPDRs and sends the billing records to the relevant Service-specific Fraud Detector. The IPDR Dispatcher stores a list of all the active service types. If the operator adds or removes a service type, its corresponding entry needs to be added or removed from the service list. The IPDR Dispatcher is built as a set of "if statements" as illustrated in Fig. 2, which shows the entries in that component.

3.3.4. The Service-specific Fraud Detector

There is one Service-specific Fraud Detector for each of the different services offered by the operator. Each of these detectors (in this case, the MobileCalls-specific Fraud Detector and the VoD-specific Fraud Detector) has three sub-components:

- The Service Fraud Rules table contains rules for known fraud scenarios specific to the service.
- The Service Profile is a document file that contains values for various parameters describing how the service is normally used by the average user. The profile is used to define thresholds included in the fraud rules.
- The Fraud Detector applies the fraud rules to the IPDRs to detect any fraudulent activity.

For instance, the MobileCalls-specific Fraud Detector has fraud rules for call selling and subscription fraud. It also has a service profile specifying values for the average and standard deviations with regard to the duration, number, frequency, cost and time of the calls. The VoD-specific Fraud Detector has a table of rules for detecting unauthorised access to and illegal redistribution of the videos. The service profile of the VoD-specific Fraud Detector also contains statistics for the average number of downloaded videos in a session, the file size of the requested videos, the requested quality of service, and the bandwidth used.

3.3.5. The SOM Analyser

The SOM Analyser processes the IPDRs with the SOM algorithm. The SOM is a model of unsupervised neural networks used for the analysis and visualisation of multi-dimensional data [22]. Neural network analysis is a differential analysis technique. It classifies input data based on the similarity of the input vectors (fields in the input data). Similar vectors are grouped in the same cluster. Usually, a SOM can be graphically visualised by displaying a coloured map that shows the different clusters identified in the input data. A detailed description of the SOM algorithm can be found in Ref. [22].

The SOM Analyser is used to detect unknown fraud patterns once the IPDRs have been analysed with known intrusion and fraud rules. It has two main components: a Service-specific IPDR File for each service type (the MobileCalls-specific IPDR File and the VoD-specific IPDR File) and a SOM Tool.

- Service-specific IPDR Files are created at regular time intervals (e.g. every 2 h). Each file contains IPDRs produced over the last specified time interval and not identified as suspicious by both the Intrusion-based Fraud Detector and the relevant Service-specific Fraud Detector. If no suspicious activity is found, the files are deleted after the SOM analysis.
- The SOM Tool implements the SOM algorithm. It uses Service-specific IPDR Files as input to generate service-specific maps. The maps show clusters of the usage records based on the similarity

Please cite this article in press as: M.A. Bihina Bella, et al., A fraud management system architecture for next-generation networks, Forensic Sci. Int. (2009), doi:10.1016/j.forsciint.2008.12.013

of their parameter values. The fraud analyst analyses the maps to identify outliers or unusual patterns that may indicate suspicious activity. A more detailed description of the SOM Analyser, as well as of its prototype implementation, is provided in Section 4.

3.3.6. The Alarm Manager

The Alarm Manager is responsible for generating alarms when suspicious IPDRs are detected. It enables the configuration of various alarm notification settings (e.g. email, short message service, pop-up screen) and stores both the suspicious IPDRs and the following information about an alarm:

- The source component of the alarm.
- The alarm number for the source component and for the FMS (e.g. alarm number 10 for VoD-specific Fraud Detector and number 120 for the FMS).
- The fraud or intrusion rule that triggered the alarm.
- The suspected fraud or intrusion attack.
- The time of the alarm generation.

The fraud analyst uses this information to open a case in the Case Manager.

3.3.7. The Case Manager

The Case Manager is a graphical user interface used to conduct further investigation into a likely fraud attack. It presents to the fraud analyst all the gathered information about a suspected fraud attack, including:

- The suspicious IPDRs obtained either from the Alarm Manager or the SOM Analyser.
- The likely fraud type and the fraud rule that triggered the alarm, as specified in the Alarm Manager.
- The priority level of the suspected fraud attack, to ensure that the fraud analyst investigates the most risky fraud cases first. The priority level is assigned by the Case Manager based on various criteria specified by the fraud analyst, such as the service feature and cost (e.g. international calls are considered riskier than local calls), the time (peak or non-peak time), and the service location (e.g. the calling or called area is a high-risk zone for fraud).
- The payment history of the suspicious user account obtained from the billing system.
- Previous fraud cases from the suspicious user account, if applicable.

The fraud analyst uses this aggregated information to confirm or refute the fraud attack and take the appropriate action: ignore the case; put the user account on a high-risk account list and monitor the recurrence of a similar fraud scenario; warn the suspicious user, or immediately suspend the user. If the investigation from the Case Manager proves that no fraud attack occurred, the suspicious IPDRs are deleted.

The architecture described above presents several novel features compared to traditional FMSs: the integration of the functionality of the IDS into the FMS; the implementation of different Service-specific Fraud Detectors, and the application of the SOM algorithm. The first two features suggested are from previous researchers, while performing a SOM analysis is the author's suggested method for identifying new fraud scenarios that are likely to occur in NGNs. The prototype implementation of the SOM Analyser is documented in the next section.

4. Prototyping the SOM Analyser of the NGN FMS

This section describes the experiment that was conducted to prototype the SOM Analyser module of the NGN FMS architecture proposed earlier. The SOM Analyser is represented as a block with thick lines (see Fig. 1). The goal of the prototype implementation was to assess the viability of using a SOM for detecting suspicious usage patterns.

The prototype implementation of the SOM Analyser followed the main processes mentioned in Section 3.3.5. Some files of service-specific usage records were created; they were processed with a SOM implementation tool and some service-specific maps were generated. The prototype implementation required some test data and a SOM implementation tool, which are described in Sections 4.1 and 4.2, respectively. The output of the prototype implementation is presented in Section 4.3.

4.1. The test data set

The authors obtained an Excel file containing 2 595 real CDRs of past customer usage from a major fixed-line operator. The CDRs were sanitised and confidential information identifying the users was removed by the operator prior to the tests. The CDRs represented different call types (e.g. international calls and free calls) made on a weekday over a brief period of 242 s or 4 min (between 12:34:40 p.m. and 12:38:42 p.m.) from various cities throughout South Africa. Fig. 3 shows a few CDRs from the CDR file, with the nine parameters used in the prototype implementation.

As a computational method, the SOM can only process numerical data. The only numeric values in the CDR file were the duration (in seconds) and the rating (estimation of the cost, no unit specified) of the calls and thus, they were the only numeric input fields to the SOM. Other parameters were used as labels.

4.2. The SOM implementation software

MATLAB [23] was used as the software application to apply the SOM algorithm to the data set provided. It is a commercial product used for technical computation and has a built-in functionality for the SOM algorithm. MATLAB was chosen because it is a well-known and recognised application and the authors had some prior experience of using that tool. A MATLAB add-on, the SOM Toolbox [24], was also used because of the limited visualisation features of MATLAB's built-in SOM module. The SOM Toolbox package, which is freely available online [24], has very powerful and flexible functions to visualise the output of the SOM.

The SOM Toolbox reads the file, initialises and trains the SOM and then displays the trained neural network in the form of a coloured map. The map shows on a colour bar the scale of the values in the input field (the CDR parameter) and also represents clusters in that field. The values on the colour bar are not always accurate and representative of the values in the input file, as the colour bar merely represents the distribution of the values in the input file and not the actual values.

1	STARTTIME	DURATION	DESTINATION	REFERENCE	B_CURR_TYPE	B_CURR_N2	RATING	A_NP_CURR	B_CURR_N1
2	2005/06/03 12:34:40 PM	63	0926612345678	0211234567	16	266	310	021	09
3	2005/06/03 12:34:40 PM	103	0861123456	0111234567	10		186	011	861
4	2005/06/03 12:34:40 PM	99	0860123456	0511234567	9		124	051	0860
5	2005/06/03 12:34:40 PM	36	092641234567	0212345678	16	264	186	021	09

Fig. 3. Sample CDRs from the test data set.

Please cite this article in press as: M.A. Bihina Bella, et al., A fraud management system architecture for next-generation networks, Forensic Sci. Int. (2009), doi:10.1016/j.forsciint.2008.12.013

4.3. The SOM output

In order to prototype the SOM Analyser, some service-specific text files of the CDRs in the provided data set were created and used as input to the SOM Toolbox. Since the test data set contained CDRs for one service type (phone calls from a fixed line) only, the different call types in the data set were considered different services. Each input file contained CDRs of only one call type. Fig. 4 shows the maps that were generated for international calls.

Fig. 4 shows the component maps for the duration and the rating of international calls:

- The Duration map shows the scale (on the colour bar) of the values for the duration of the calls (roughly between 8 s and 176 s). As is clear from the map, most of the calls are short (in blue). However, a small number are relatively long (in red). The map clearly shows the existence of three clusters: short calls in blue, medium duration calls in green and long calls in red.
- The Rating map shows the scale of the rating of the calls. Only a very small percentage of the calls are expensive. The map also presents three clusters: cheap calls in blue, moderately priced calls in green and expensive calls in red.

Note that the topology of all the component maps is the same. So, the cell in the top left corner of the Rating map (in dark red) corresponds to the cell in the same position on the Duration map. A suspicious pattern that emerges shows that some of the longest calls (in red on the Duration map) are also cheap (in light blue and green in the top right corner of the Rating map). *This visualisation shows how quickly one can identify anomalies in the data.*

In order to obtain more correlation patterns between the two maps, labels for the calling areas were added to the Duration map and labels for the destinations were added to the Rating map. The added labels showed that, for the test data set, calling code 011 by far dominated the calling area from which international calls were made, followed by code 021. Furthermore, most of the calls were to the UK (44), coming mainly from 011. Most of the long and cheap calls were (understandably) to neighbouring countries, for instance to Zimbabwe (263), Namibia (264), Malawi (265) or Swaziland (268). However, two of these calls were quite suspicious as they were made to remote destinations – India (91) and The Netherlands (31), respectively. *This explanation demonstrates how easy it is to identify suspicious activity with a SOM, even without any prior knowledge of the usage patterns in the data set.*

A few other maps were generated from aggregate values obtained from a manual calculation in Excel. This was done to obtain different input fields in the hope of finding other suspicious patterns. Some interesting results were obtained based on calculating the count of calls made from each calling number in the data set, as well as the average duration and rating of those calls. The relevant maps are displayed in Fig. 5.

The maps show the count, average duration and average rating of calls made based on the calling number. Calling numbers were added to the second map and calling areas to the third map. For the sake of visibility and confidentiality, the calling numbers in the data set were changed to shorter arbitrary numbers based on their appearance in the data set. This means that the first calling number was changed to 1, the second to 2 and so forth. Unfortunately, the called number could not be displayed using the same input file, as various called numbers could exist for the same calling number.

The first map is quite uniform except for one outlier, the red cell, that really stands out. The outlier corresponds to calling number 1 (on the second map) and comes from calling area 011 (on the third map). The map shows a count of 1.5 for most of the calls but 63.7 for the outlier. However, further manual analysis reveals that, whereas most of the calling numbers were used only once or twice (as shown on the map), calling number 1 was used 229 times in just 4 min! All the calls from that number were furthermore made to the UK. Such a finding does not necessarily imply fraud, as all depends on the payment history of the corresponding subscriber and its usage profile. Some of the operator's analysts suggested that a telemarketing activity might be indicated, since almost all

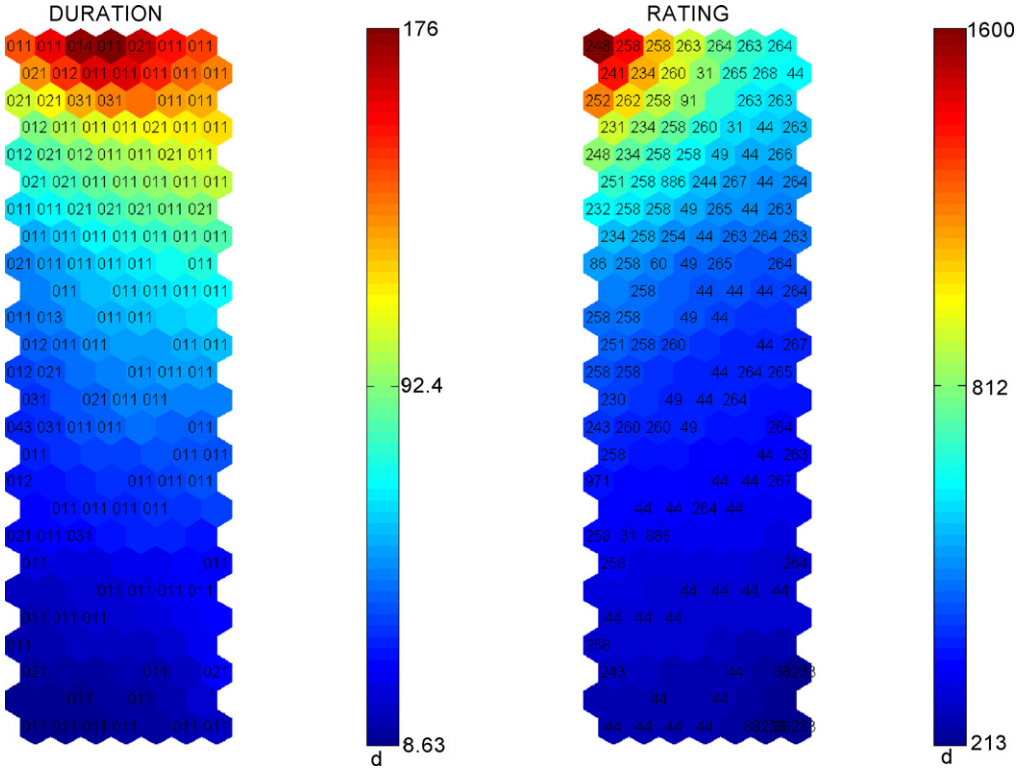

Fig. 4. Duration and rating of international calls.

Please cite this article in press as: M.A. Bihina Bella, et al., A fraud management system architecture for next-generation networks, Forensic Sci. Int. (2009), doi:10.1016/j.forsciint.2008.12.013

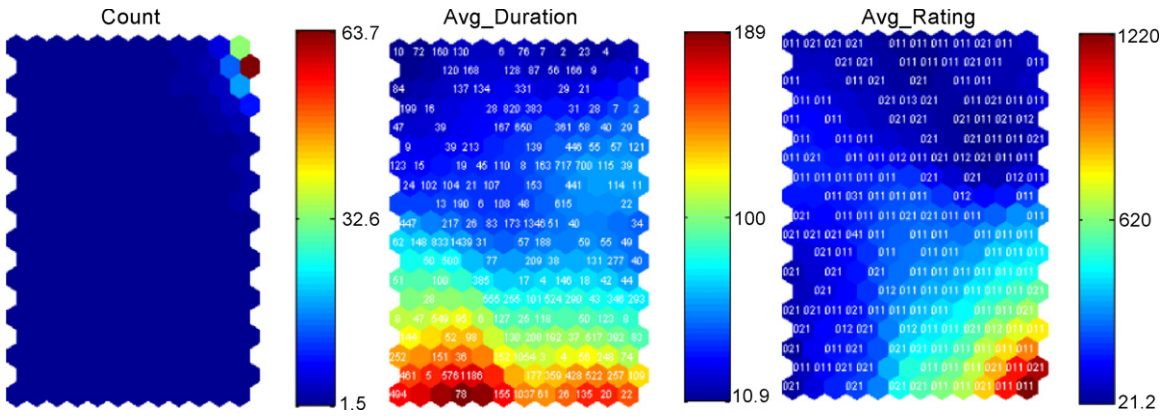

Fig. 5. Count, average duration and average rating of calls from each calling number.

the calls were very short (less than 20 s) and to different numbers (more than 100). Although, these finer details were discovered from further analysis, *it just shows how quickly one can identify outliers*.

5. Evaluation of the NGN FMS architecture and the SOM Analyser prototype

5.1. Evaluation of the NGN FMS architecture

As is explained below, the proposed FMS architecture has the potential to satisfy the requirements for NGN FMSs identified earlier.

- *Application independency and flexibility*: The IPDRs are analysed by different Service-specific Fraud Detectors, which can be created for every type of service offered by the operator. This ensures that the FMS is not tied to a specific application and can be customised to suit every operator's need. Besides, using the SOM algorithm can also help identify previously unknown fraud scenarios not stored in the fraud rule database, thus adding flexibility to the FMS.
- *Complete network traffic coverage*: Combining intrusion and fraud detection can give a good overview of all the network traffic. It can also help prevent future fraud attacks by detecting any abuse of the network vulnerabilities that could be used for fraud (compare with the earlier example of a hacking attack).
- *Scalability*: The modular architecture enables the FMS to easily scale down or up. Service-specific Fraud Detectors can easily be added or removed to accommodate a dynamic service offering in NGNs. Scalability is also enforced in the SOM Analyser, which needs to analyse only a limited number of IPDRs for every type of service. Using service profiles instead of the individual customer profiles used in commercial products also contributes to the increased scalability of the FMS.

From the above it is clear that the proposed architecture can be an effective solution for fraud detection in NGNs. However, since a prototype of the complete architecture has not yet been implemented, it is not possible to confirm its effectiveness. Only the SOM Analyser was prototyped, and this implementation succeeded in demonstrating its viability for detecting suspicious patterns (as will be discussed in the next section).

5.2. Evaluation of the SOM Analyser prototype

The SOM analysis that was performed did not actually detect any definite fraud attack. However, it demonstrated the following advantages of using a SOM for fraud detection.

- The SOM is a visualisation technique. It enables one to visualise on a single map the correlation between many dimensions or parameters – e.g. the duration, rating, calling area and called number for a high number of CDRs. For instance, the SOM has no trouble showing that most of the international calls are made from calling area 011 to the UK and that they are usually short and inexpensive. Such a correlation is impossible to define as a set of rules.
- Since the SOM enables the quick identification of suspicious or complex usage patterns that may point to unknown fraud scenarios, it can be used to define new fraud rules. For example, if the identified outlier in Fig. 5 indeed indicates a fraud attack, a new rule to detect the recurrence of such a fraud scenario can be defined as shown in Fig. 6. The fraud rule will be applied to a set of CDRs generated over a predefined time interval (e.g. 30 min) and rule parameters will be adjusted according to that interval.

If call type = international
And count of dialled numbers from same reference X > 50
And call frequency from X > 50/min
And average call duration from X < 20 s
Then alert on likely telemarketing activity

Legend
Call frequency: 229 calls were made in 4 minutes; frequency is 57/min, 50/min is used as threshold.
Count of dialled numbers: 100 different numbers were dialled from the same number, 50 is used as threshold.

Fig. 6. Fraud rule to detect new telemarketing scam.

Please cite this article in press as: M.A. Bihina Bella, et al., A fraud management system architecture for next-generation networks, Forensic Sci. Int. (2009), doi:10.1016/j.forsciint.2008.12.013

In Fig. 6, fraud parameters are defined based on the 4-min period in the test data.

The main limitations of the SOM analysis as revealed from the prototype implementation are the following:

- The values displayed by the SOM are not very accurate, which can be conducive to many interpretation errors when the maps are to be analysed.
- The SOM Toolbox is not interactive and it cannot be queried. For instance, it is not possible to click on a map cell to get all its associated labels. The knowledge discovery of the FMS could be improved by using a commercial interactive data visualisation tool such as Viscovery SOMine from Eudaptics Software Company [25].

Please note that quality of the test data set largely impacts the validity of the test results. Indeed, although real CDRs generated from real customer calls were used, they are too biased to accurately represent a real-life scenario. The CDRs span a very short period of time and the data set is small compared to a real-life environment. Therefore, as expected, the percentage of suspicious activity is very small compared to the normal usage patterns. Besides, the detected patterns are easily identifiable. Suspicious activity detected by the SOM is not sufficient to ascertain that fraud occurred. Like in real-life, further analysis is required.

6. Conclusion

This article presented an original NGN FMS architecture proposed to overcome the limitations of existing commercial FMSs. The proposed architecture has the potential to satisfy the requirements of flexibility, coverage and scalability for effective fraud detection in NGNs. Original features of the architecture include the addition of an IDS functionality within the FMS, the creation of Service-specific Fraud Detectors for every service type and, most importantly, the use of a SOM to help uncover new NGN fraud scenarios.

The article also described the prototype that was implemented to test the viability of the SOM Analyser component of the architecture. The prototype implementation demonstrated that a SOM is an efficient tool for analysing service usage data for signs of fraud. It can help identify suspicious usage patterns and outliers and assist in the definition of fraud rules for previously unknown fraud scenarios. This provides a high level of confidence in the viability of the proposed FMS architecture. Some future work is required to implement a complete prototype so as to test the viability of the entire FMS architecture.

Another potential area for future research is the investigation of other visual data analysis techniques to increase their usage in commercial FMSs. Visual analysis with a SOM is a promising solution but other data mining methods to display service usage patterns can also be beneficial to detect unknown fraud scenarios and complement other techniques used for absolute analysis. Visual analysis is particularly advantageous in NGNs to get a clear picture of the high number of usage records. One possibility is the integration of a GIS (Geographic Information System) into the FMS to display interactive maps of all the usage records for a specific entity.

References

[1] R. Jacobs, Telecommunications Fraud, Dimension Data White Paper, 2002, available online at http://www.didata.com/services/white_papers/Fraud_White_Paper.pdf, Accessed: 07 May 2004.
[2] IEC – International Engineering Consortium, Fraud analysis in IP and Next-Generation Networks, IEC Web ProForum White Paper Tutorial, 2004, available online at: http://www.iec.org/tutorials/fraud_analysis/. Accessed: 07 May 2004.
[3] G. Ibbett, Top Telco Frauds and How to Stop them, Billing World and OSS Today Magazine, January 2007, 2007 edition, issue 1, electronic version, available online at: http://www.billingworld.com/secondary.cfm?page=detail&archiveId=7824. Accessed: 05 March 2007.
[4] Cerebrus Solutions, Fraud Primer, Cerebrus Solutions (2.2), September 2001, available online at http://cp.literature.agilent.com/litweb/pdf/5988-7753EN.pdf. Accessed: 21 February 2007.
[5] P. Falshaw, Next generation networks and services, in: Proceedings of PTC2001, the Pacific Telecommunications Council, Honolulu, Hawaii, January 15–17, 2001.
[6] D. Abramowicz, P. Ledberg, IP fraud – methods and algorithms for detecting IP-based fraud, MSc Thesis, Swedish Royal Institute of Technology, Göteborg, Sweden, 2002.
[7] M.H. Cahill, D. Lambert, J.C. Pinheiro, D.X. Sun, Detecting Fraud in The Real World, 2002, available online at: http://stat.bell-labs.com/cm/ms/departments/sia/doc/HMDS.pdf, accessed: 21/05/2004.
[8] E. Lundin, Aspects of employing fraud and intrusion detection systems, Licentiate Thesis, Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden, 2002.
[9] M. Johnson, Future Frauds: Telecom Fraud in Next Generation Services, Commonwealth Telecommunications Organisation article, 2002, available online at http://www.cto-ict.org/index.php?dir=04&sd=30&aid=1012, accessed: 12 April 2005.
[10] M. Horal, Fraud detection in IP multicast applications, MSc Thesis, Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden, 2000.
[11] M. Bihina, J. Eloff, M. Olivier, Requirements for Next-Generation Networks billing systems, in: Proceedings of the 4th Southern African Telecommunications Networks and Applications Conference (SATNAC 2004), Stellenbosch, South Africa, September 6–8, 2004.
[12] M.A. Bihina Bella, M.S. Olivier, J.H.P. Eloff, A fraud detection model for Next-Generation Networks, in: Proceedings of the 8th Southern African Telecommunications Networks and Applications Conference (SATNAC 2005), Central Drakensberg, KwaZulu-Natal, South Africa, September 11–14, 2005.
[13] EURESCOM, P1007: Application of Intelligent Techniques to Telecommunications Fraud Detection, Project Information, 2002, available online at http://www.eurescom.de/public/projects/P1000-series/P1007/, accessed: 16 February 2006.
[14] H. Biscaia, S. Alexiou, F. Pavon, R. Hulthen, Do intelligent techniques aid fraud detection? EURESCOM Mess@ge 1 (2002), 17–19.
[15] C. Karlsson, Methods for intrusion and fraud detection in IP-based multimedia services, MSc Thesis, Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden, 2001.
[16] S. Hearne, A fraud detection framework for next-generation telecommunications networks, MSc Thesis, Department of Physical and Quantitative sciences, Telecommunications Software and Systems Group, Waterford Institute of Technology, Ireland, 2004.
[17] Y. Moreau, B. Preneel, P. Burge, J. Shawe-Taylor, C. Stoermann, C. Cooke, Novel techniques for fraud detection in mobile telecommunication networks, in: Proceedings: ACTS (Advanced Communications Technologies and Services) Mobile Summit, Granada, Spain, November 27–29, 1996.
[18] M. Arvidson, M. Carlbark, Intrusion detection systems – technologies, weaknesses and trends, Licentiate Thesis, Department of Electrical Engineering, Linköping University, Stockholm, Sweden, 2003.
[19] M. Fowler, K. Scott, UML Distilled: A Brief Guide to the Standard Object Modeling Language, 2nd ed., Addison-Wesley, Reading, Massachusetts, 2000.
[20] Ipdr.org, Document Map and Overview, Version 3.5.0.1, Technical specification document, November 2004, available online at http://www.ipdr.org/public/DocumentMap/DMO3.5.0.1.pdf, accessed: 06 June 2004.
[21] M.A. Bihina Bella, M.S. Olivier, J.H.P. Eloff, Using the Internet Protocol Detail Record standard for NGN billing and fraud detection, in: Proceedings of the 5th Information Security South Africa (ISSA) Conference 2005, Sandton, South Africa, 29 June–1 July, 2005.
[22] A.P. Engelbrecht, Computational Intelligence: An Introduction, Hoboken, N.J. Wiley, Chichester, England, 2002.
[23] Mathworks.com, MATLAB, Product information, 2006, available online at http://www.mathworks.com/products/matlab/, accessed: 31 July 2006.
[24] CIS, SOM Toolbox 2.0, Product information, 2006, available online at http://www.cis.hut.fi/projects/somtoolbox, accessed: 31 July 2006.
[25] Eudaptics.com, Viscovery® SOMine® - Self-Organizing Maps, Product Information, 2006, available online at http://www.somine.info/, accessed: 02 August 2006.

Please cite this article in press as: M.A. Bihina Bella, et al., A fraud management system architecture for next-generation networks, Forensic Sci. Int. (2009), doi:10.1016/j.forsciint.2008.12.013