A FRAUD MANAGEMENT SYSTEM ARCHITECTURE FOR NEXT-GENERATION NETWORKS

by

MADELEINE ADRIENNE BIHINA BELLA

submitted in partial fulfilment of the requirements for the degree

MASTER OF SCIENCE (COMPUTER SCIENCE)

in the

FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

at the

UNIVERSITY OF PRETORIA

SOUTH AFRICA

SUPERVISOR: Prof. J.H.P. Eloff
CO-SUPERVISOR: Prof. M.S. Olivier

Date of submission

30-07-2007

A FRAUD MANAGEMENT SYSTEM ARCHITECTURE FOR NEXT-GENERATION NETWORKS

Abstract

The telecommunications industry is shifting to a new type of network generally referred to as next-generation networks (NGNs). The concept of NGNs implies the convergence of voice, video and data networks onto the same infrastructure. It enables the offering of a new class of services that has the potential to increase revenue for operators and enhance customers' experience.

Unfortunately NGNs are highly likely to favour the rise of telecommunications fraud. Due to some of their key characteristics such as being based on the Internet Protocol, NGNs create new challenges for effective fraud detection. Besides, as they enable the provision of innovative services, NGNs may also give rise to new fraud scenarios that cannot be addressed by existing fraud management systems (FMSs) as these systems are application-dependent. They heavily depend on the service types and their underlying network platform**.** Consequently, FMSs need to be revised to effectively tackle these emerging issues.

This thesis presents an architecture for a next-generation network fraud management system (NGN FMS) specifically designed to satisfy the requirements of flexibility and application-independency that cannot be met by traditional FMSs. The architecture has a thorough multi-stage detection process that analyses billing records in Internet Protocol Detail Record (IPDR) format – an emerging IP-based billing standard – for signs of fraud. In addition to its high level of flexibility, the proposed architecture has the benefit of being largely scalable and is able to help uncover new fraud types. This is achieved through the added combination of intrusion detection and neural network technology in the architecture design. Neural networks are implemented in the form of Self-Organising Maps (SOMs) in one component of the FMS, appropriately named the SOM Analyser. A prototype of the SOM Analyser has been implemented and is discussed in the thesis.

Keywords: Billing system, fraud management system (FMS), Internet Protocol (IP), Internet Protocol Detail Record (IPDR), next-generation network (NGN), Self-Organising Map (SOM), telecommunications fraud.

Supervisor: Prof. J.H.P. Eloff

Co-supervisor: Prof. M.S. Olivier

Department of Computer Science

Degree: Magister Scientia

ACKNOWLEDGEMENTS

I would like to thank the following people for their contribution to the success of this work.

- Prof J.H.P Eloff and Prof M.S. Olivier for their thorough supervision
- Marc Johnson for his sponsorhip and his invaluable guidance
- Telkom fraud management team, expecially Roy Volkwyn and Andrew van der Spuy for their assistance and the test data they provided.
- The members of the ICSA research group, for their constructive critics through various meetings, conversations and reviews of my publications.
- Last but not least, I would like to express my special gratitude to my parents for their constant support and encouragement.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1: Research overview and objectives

1.1 Introduction

The term next-generation networks (NGNs) has been a buzzword in the telecommunications industry since 1998 (Huitema, 1999). Although the concept is interpreted differently by various parties, it generally refers to the future converged networks for voice, video and data traffic based on the Internet Protocol (IP) (Falshaw, 2001). Shifting to NGNs offers tremendous opportunities to network and service providers by reducing operational costs and generating more profit through the introduction of sophisticated high-value services. However, NGNs also bring huge challenges for management and security. One crucial issue to examine is fraud management.

Telecommunications fraud is a major problem continuously faced by network and service providers since its being identified as their primary cause of revenue loss (Jacobs, 2004). According to the Oxford Advanced Learner's Dictionary, fraud is defined as "an act of deceiving illegally in order to make money or obtain goods". In other words, it is a financial crime whereby one person impersonates another (the victim) in order to obtain an economic gain on his behalf (Karlsson, 2001). Telecommunications fraud specifically refers to the "theft of services or the deliberate abuse of voice and data networks" (Jacobs, 2004). It is estimated that operators lose between 3% and 8% of their annual revenues due to fraud, which amounts to USD 700 million in Africa alone (Jacobs, 2004) and more than USD 44 billion globally (Ibbett, 2007). Fraud can also have indirect negative consequences such as the business losing both customers' trust and its competitive advantage. Effective fraud management is therefore essential for operators.

Fraud management is a broad concept that combines aspects of not only security, but also of accounting (Hearne, 2004). It involves various activities such as fraud detection, prevention and avoidance, as well as risk analysis and estimation of losses (Palshikar, 2002). Fraud management can be automated through fraud management systems (FMSs), which are automated tools designed to detect, manage and assist in the investigation of fraudulent activities (IEC, 2004b). Such a system has successfully helped Telkom, South Africa's leading fixed-line telephone company, reduce its loss due to fraud from R274 million in 2001 to R174 million in 2002 (Stones, 2003). FMSs use information generated for billing purposes as their main source of input. This information is usually referred to as Call Detail Records (CDRs). An alarming fact is that many

companies that are currently launching or have already launched some form of NGN service are still relying on their existing FMS to secure their business operations. This puts them at high risk of being victims of NGN fraud, because due to their lack of flexibility (i.e. they are application specific), the FMSs currently deployed in the industry are not able to successfully serve these upcoming networks (Karlsson, 2001).

Indeed, as they are based on the Internet Protocol, NGNs belong to *datacommunications* (the interaction between computers), in contrast to traditional *telecommunications* (distance communication via telephones) (Abramowicz & Ledberg, 2002). This creates new challenges for fraud management in NGNs as currently available FMSs were specifically designed for telecommunications networks and lack the flexibility to accommodate the new service models and billing schemes of IP services. Besides, today's FMSs have a strong emphasis on rule-based fraud detection, which uses rules or signatures that define characteristics of a known fraud type. As new NGN services are introduced, new forms of fraud will emerge that cannot be addressed by rule-based FMSs.

In view of the above-mentioned issues, current FMSs need to be revised to effectively prevent and detect fraud in NGNs. Although some work, such as research from Kvarnström (2000), Abramowicz and Ledberg (2002) and Hearne (2004), has already been conducted in this regard, researchers only focus on discovering more intelligent and flexible fraud detection techniques. They tend to overlook necessary changes to the billing systems and how these modifications may impact on the FMSs. Such information is indeed of crucial importance, given that a data analysis system can only be as good as its input data. If the FMS is fed with incorrect or outdated billing records, no actual fraud cases will be detected, no matter how sophisticated the fraud detection techniques are. This research project therefore attempts to fill this gap by designing an FMS suitable for NGNs, based on a set of requirements identified for NGN billing systems.

1.2 Problem statement

The problem addressed in this research can be formulated as follows: what should the architecture for an FMS suitable for NGNs look like? In order to design such an architecture, research will be conducted to answer the following fundamental questions that arise as sub-problems:

1.2.1 What is the likely evolution of fraud in NGNs?

NGNs provide new opportunities to commit fraud due to the introduction of new technologies and services. It is therefore necessary to determine which new types of fraud are likely to prevail in NGNs and how these will affect the traditional fraud detection process. Although new forms of fraud may occur, many of the old fraud types will still be present as their associated services will still be offered. It is therefore important to also consider the detection of these existing fraud types in the design of the NGN FMS architecture.

1.2.2 What is (are) the most suitable source(s) of information for an FMS for NGNs?

Answering this question actually implies answering each of the following three subquestions:

1.2.2.1 Which information is required to detect NGN fraud?

The quality of the input data is crucial for the effectiveness of the FMS. The FMS needs timely and accurate information about both the network and the customers. It is thus necessary to critically assess, from an NGN perspective, the suitability of the content of the billing records used as input to traditional FMSs. As NGNs differ radically from traditional telecommunications networks, billing records might not provide all the information necessary for effective fraud detection. Therefore, the possibility of using other sources of information for fraud detection will be investigated.

1.2.2.2 In which format should fraud-detection information be provided?

Currently, billing records are provided in many technology-dependent formats for voice and data services. As these technologies converge in NGNs, the adoption of a unified format would be beneficial. Selecting the best possible format for this purpose is an important matter that will be solved in this thesis.

1.2.2.3 How should fraud-detection information be collected by the FMS?

It is also important to determine how the billing records should be exported from their generating system to the FMS to maximise the quick detection of fraud. This necessitates the identification of requirements for NGN billing systems and of viable solutions to these requirements.

1.2.3 Which data analysis technique(s) is (are) required for detecting NGN fraud?

Current FMSs heavily rely on rule-based analysis. However, as mentioned previously, rule-based fraud detection might not be an effective solution for NGNs. Furthermore, some operators still perform a degree of manual analysis of CDRs. Given the high volume of billing records generated in distributed IP-based networks, this is no longer a viable option in NGNs. This research project will therefore attempt to identify more suitable techniques that are capable of handling the expected volume increase of CDRs and flexible enough to detect previously unknown fraud scenarios in an NGN environment.

1.3 Methodology

The following five steps are taken in order to solve the problem stated above.

The first step in developing an FMS suitable for NGNs is to understand the security issues related to this new form of network. One of these is that an NGN enables fraud to be committed simultaneously from various points in the network (Lamparter & Westhoff, 2002). Thus NGNs and their security vulnerabilities are carefully analysed from a fraud perspective.

The second step is to identify which types of fraud might be prevalent in NGNs. This speculation on the future fraud types is based on current fraud methods and how they might evolve in NGNs. A couple of highly potential NGN fraud types are subsequently studied in more detail and their fraud indicators are provided.

The third step is to look at NGN billing systems requirements. This entails answering the following three questions: Which qualities does a billing system need to assist fraud detection in NGNs? How can these requirements be satisfied? And how does this influence the fraud detection process? The answer is obtained by examining a typical billing system for voice networks since, unlike the data network (Internet), voice networks already have well-established billing procedures and standards. The billing process and the billing records' format are scrutinised to determine their limitations in relation to NGN fraud detection. A solution to these limitations is then suggested.

The fourth step involves critically assessing the techniques used to detect fraud in current FMSs. Appropriate techniques to spot the NGN fraud types identified in Phase 2 are selected next.

The fifth and final step is to gather all the relevant information from the previous phases to design an NGN FMS architecture and test its efficiency through the implementation of a prototype.

1.4 Dissertation layout

This study is conducted over twelve chapters related to one another as shown in Figure 1.1 below.

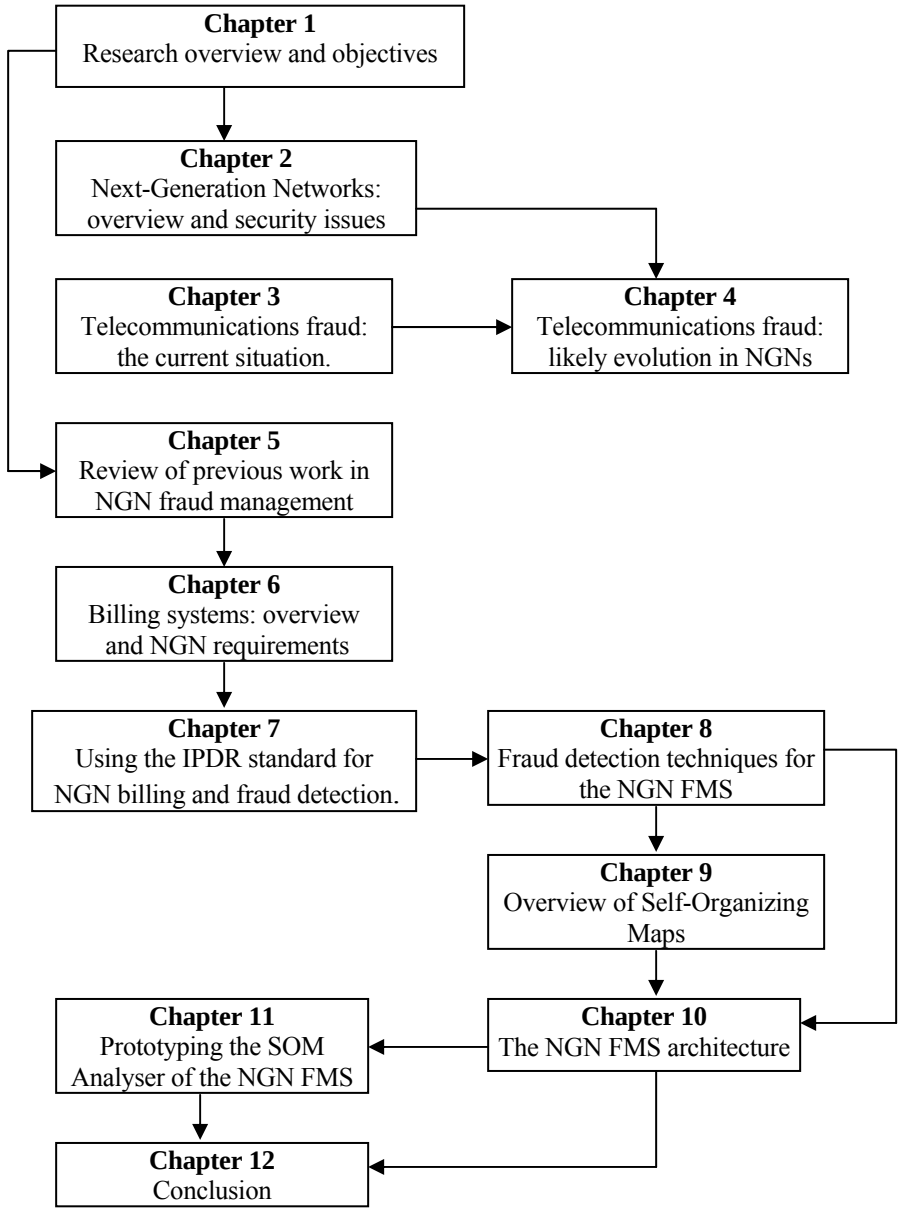

Figure 1.1: Dissertation layout

Chapter 1: Research overview and objectives

This chapter provides an introduction to the dissertation and indicates how the research is structured.

Chapter 2: Next-generation networks: overview and security issues

Background information on NGNs is given. An analysis is made of the challenges that have to be met for the deployment of the new networks to be successful. Focus is directed on security issues and fraud problems.

Chapter 3: Telecommunications fraud: the current situation

A detailed review of fraud as currently perpetrated is provided. Questions such as who commits fraud, why, and how to commit fraud, are answered.

Chapter 4: Telecommunications fraud: likely evolution in NGNs

This chapter analyses the likely evolution of fraud in NGNs, based on current fraud issues as discussed in Chapter 3.

Chapter 5: Review of previous work in NGN fraud management

This chapter provides a critical analysis of previous research projects conducted to address the problem of fraud detection in NGNs. It uses these previous results as a starting point for the features of the proposed FMS architecture. The chapter also contrasts previous work to the approach used in this dissertation.

Chapter 6: Billing systems: overview and NGN requirements

An analysis is conducted of a typical billing process, and its impact on the fraud detection process is also discussed. Requirements for NGN billing systems are determined. The chapter furthermore examines billing record formats and standards and shows how these prevent traditional billing systems from satisfying NGN requirements.

Chapter 7: Using the IPDR standard for NGN billing and fraud detection.

In this chapter, the IPDR standard is proposed as a solution for NGN billing requirements. The chapter also explains how using the IPDR standard for NGN billing systems can help improve the efficiency of FMSs in converged networks.

Chapter 8: Fraud detection techniques for the NGN FMS

A critical assessment is conducted of techniques used by current FMSs to detect fraud. Suitable techniques to detect NGN fraud types are then selected from this review.

Chapter 9: Overview of Self-Organising Maps

The chapter presents the Self-Organising Map (SOM) algorithm, identified in Chapter 8 as the data analysis technique most suitable for identifying unusual service usage patterns indicative of unknown NGN fraud types.

Chapter 10: The NGN FMS architecture

The chapter provides a description of the proposed architecture of NGN FMSs. The architecture design combines information acquired from the previous chapters, more specifically Chapters 5, 7, Chapter 8 and 9.

Chapter 11: Prototyping the SOM Analyser of the NGN FMS

This chapter serves as a partial proof-of-concept for the architecture proposed in the preceding chapter. The chapter describes the prototype implementation of the SOM Analyser, which is the component of the FMS that applies the SOM algorithm for fraud detection. Both the viability and the effectiveness of the SOM Analyser are tested. The SOM Analyser is the only component which is prototyped as it is the only module of the architecture that enables the identification of unknown NGN fraud scenarios.

Chapter 12: Conclusion.

This chapter concludes the thesis.

Chapter 2: Next-generation networks: overview and security issues

2.1 Introduction

NGNs are generally considered to be the future revolution in the telecommunications industry (Intel, 2001). Shifting to NGNs has the potential to be highly beneficial for both operators and their customers. The potential deployment of NGNs has consequently received a lot of attention from the telecommunication industry. However, operators usually focus on aspects of service delivery and on network implementation technologies, and thus far NGN security threats and especially fraud issues have not been the subject of much literature. It is obviously essential that these challenges need to be addressed before NGNs can yield the expected benefits.

This chapter provides an overview of NGNs and analyses their security issues. An examination of the security vulnerabilities of NGNs is required to understand why technical fraud is likely to increase in NGNs and why the effective detection of the new fraud scenarios is so challenging in view of the limited capabilities of current FMSs. The chapter is structured as follows. Section 2.2 gives a description of NGNs, followed by a review of NGN business and technology drivers in Section 2.3. The presentation of NGN drivers explains why fully convergent networks are needed in the telecommunications industry. It also shows that the upcoming deployment of NGNs is not just a new marketing campaign. Finally, NGN security challenges are analysed in Section 2.4, and reasons are given for the potential rise of fraud in NGNs.

2.2 Description of NGNs

This section comprises two subsections. The first (2.2.1) defines the term next-generation networks, while the second (2.2.2) provides key characteristics of NGNs based on this definition.

2.2.1 Definition

NGN has been a buzzword in the telecommunications industry since 1998 (Huitema, 1999) but currently no commonly agreed upon definition for next-generation network exists. This is due to the fact that the term NGN merely refers to the way telecommunications networks will perform in the future, after a series of modifications over current networks have taken place (Research and Markets, 2002). A vision of exactly how NGNs will operate and what they will look like varies from one person to the next.

ITU, the International Telecommunication Union (ITU, 2004), proposes the following definition of NGNs: "A Next-Generation Network is a packet-based network able to provide services including telecommunication services and able to make use of multiple broadband, quality of service-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalised mobility which will allow consistent and ubiquitous provision of services to users". Note that this high-level definition describes the desired functionality and features of NGNs, but does not specify their underlying network technology.

A simpler definition from Ovum, a European research and consulting company for the telecommunications market, is as follows: "Next-Generation Networks are single, multiservice networks that carry voice, data and video bitstreams using the Internet Protocol (IP) over common transmission links and routers" (Falshaw, 2001).

According to the above definitions, an NGN is the combination of the following four network types (Intel, 2002):

1. Circuit-switched telephony networks or PSTN (public switched telephone network) – for voice communication and dial-up data access services.
2. Cable-telephony networks – for one-way multimedia, voice communication and broadband data access services.
3. Mobile networks – for mobile voice communication services.
4. Internet – for "best effort" content and transaction services.

In this regard, the term NGN is often used as a synonym of convergence: convergence between the previously distinct industries of broadcasting, telecommunications and information technology but also convergence within industries themselves, such as the integration of mobile and fixed telecommunication services (Gillwald, 2003).

The author's own definition of NGNs, which is proposed as a summary of the previous descriptions, is the following: *A next-generation network is a single IP-based infrastructure used to carry all voice, data and multimedia traffic and associated telecommunications services using a packet-based transport.* This definition will be adopted throughout the remainder of this document.

2.2.2 Key characteristics of NGNs

Key aspects of NGNs can be inferred from the definition proposed above (Gentry, 2001; Hanrahan, 2002; ITU, 2004):

- IP-centric. NGNs are based on the Internet Protocol.
- Packet-based. A high-speed packet network is used for transporting and routing services.
- Many access mechanisms: e.g. wired, wireless, cable, modem.
- Interoperability between legacy and future networks via open interfaces.
- Built on open modular elements and standard protocols.
- Broadband capability (i.e. able to quickly carry a considerable amount of information) with end-to-end quality of service.
- Services are logically developed on platforms separate from the transport and access layers of the network.

These characteristics are clearly visible in Figure 2.1, which shows a basic NGN architecture.

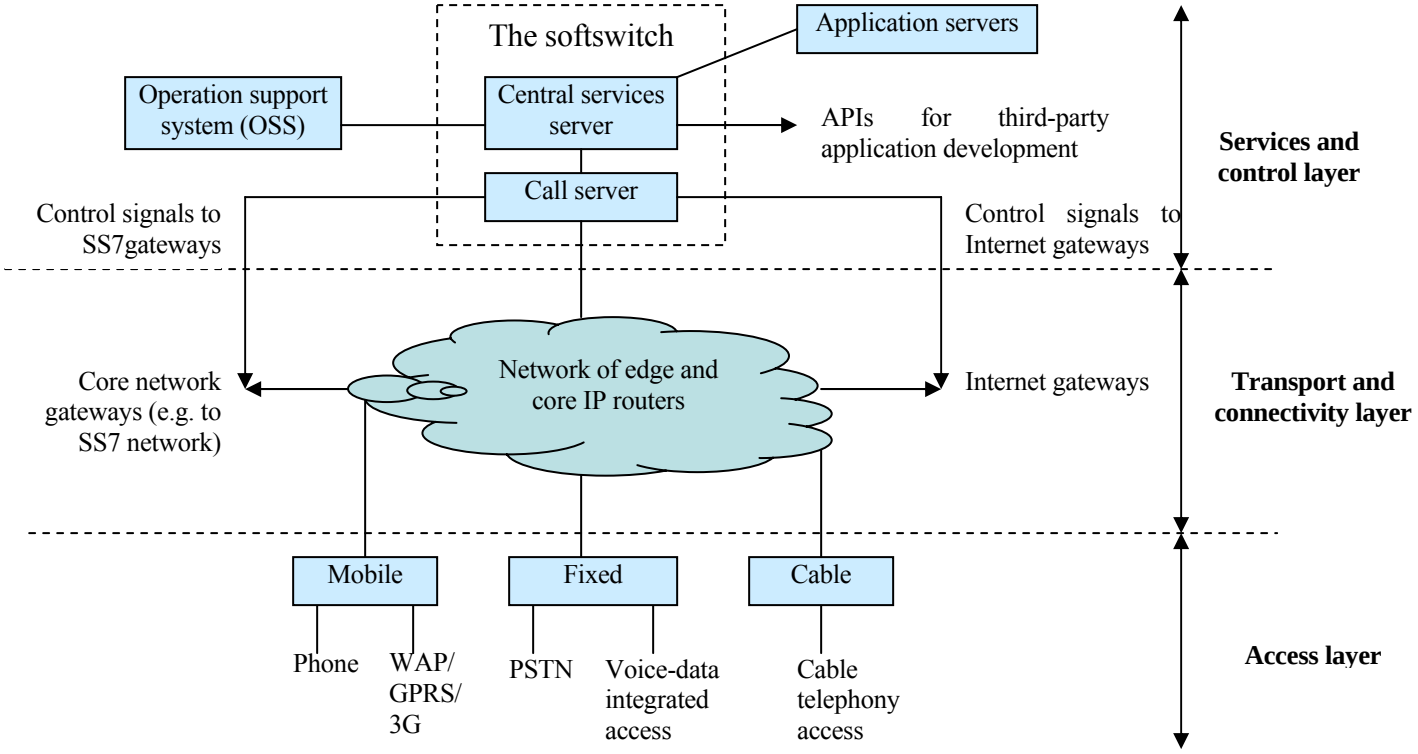

Figure 2.1: Basic NGN architecture, adapted from Stevenson *et al* (2001)

The architecture in Figure 2.1 is composed of three independent and interacting layers:

- The access layer – It enables access to the network from many types of terminals and converts incoming traffic to IP data streams via the access gateways.

- The transport and connectivity layer – It consists of routers, transmission links and gateways for interconnection with other networks.
- The services and control layer – It performs various functions through its main components, which are the operation support system (OSS), the call servers, the central services server and the application servers. The call servers and the central services servers make use of some software, the so-called softswitch, to function.
  - The OSS gathers information about performance and usage from the network elements and uses it for billing and network management.
  - The call servers (also called call agents) control sessions between terminals, gateways and SS7 (the signalling system used in the PSTN) networks.
  - The central services server, in association with the application servers, provides APIs (application programming interfaces) used by the operator and third parties to develop services. It also controls the relevant subscriber management and usage data (Stevenson *et al*, 2001).

NGNs are not just a new hype in the telecommunications industry. Although the term sounds futuristic, migration from traditional telephone networks to NGNs is already under way in developed telecommunications markets (Falshaw, 2001). Such migration is motivated by various market and technology drivers and by the need to overcome limitations of existing networks – as is further explained in the next section.

2.3 Motivations for shifting to NGNs

The reason for migrating to NGNs is twofold. Firstly, NGNs can help solve some of the limitations of currently separate networks, and secondly, NGNs provide a solution to new economic constraints facing telecommunications operators. A discussion of these motivations follows in Section 2.3.1 and Section 2.3.2 respectively.

2.3.1 Shortcomings of existing networks

Various problems with conventional separate networks are driving operators towards network convergence. Limitations exist within the network infrastructure itself and problems are experienced with the management of separate networks.

2.3.1.1 Limitations of existing network infrastructure

Today's public network infrastructure is divided into two main components: the public switched telephone network (PSTN) and the Internet (IEC, 2004b).

The PSTN, essentially designed for voice traffic, uses a circuit-switched infrastructure, in other words a fixed amount of two-way bandwidth is allocated for the entire duration of a phone call. This provides reliable and consistent quality of service. However, circuit-switching technology is very costly to deploy and maintain. Existing circuit-switched platforms are vendor-specific, which implies that operators fully depend on their vendors for upgrading their software applications and introducing new services. Due to the high cost of these operations, the range of services offered to customers is very limited (IEC, 2004b).

On the other hand, the Internet, with its low-cost packet-switched infrastructure is very flexible and enables the rapid creation of new services. Developed for data traffic, it can also carry multimedia and more recently voice, with the development of VoIP (voice over IP) technology. However, primarily designed as a "best effort" network, it lacks reliability and does not offer a high level of quality of service (Hanrahan, 2002).

Table 2.1 recaps the mentioned differences between the PSTN and the Internet.

	Circuit-switched PSTN	**Packet-switched Internet**
Advantages	Optimised for voice	Highly efficient
	Low delay	Flexible and standard-based
	Consistent availability	Both narrowband and broadband
	High and reliable quality of service	Cheap to build and operate
Limitations	Narrowband	Best-effort services
	Inflexible and proprietary	Inconsistent availability
	Expensive to build and operate	Inconsistent performance

Table 2.1. Advantages and disadvantages of the PSTN over the Internet, adapted from Stevenson *et al* (2001)

2.3.1.2 Shortcomings of maintaining separate networks

Currently voice, data and multimedia are carried over specialised networks. Maintaining separate networks is cumbersome and expensive. Integrating various operations such as customer management and billing over these specialised networks can become very tedious and costly (Gulyani & Gauthier, 2003).

Besides, operators are searching for means to increase the efficiency of their networks, as the volume of traffic they carry is ever increasing. This is a real nightmare when equipment needs to be supplied for every type of traffic (Baumgartner, 2002).

Some convergence between the PSTN and the Internet seems the ideal solution to these problems, which explains why operators are turning towards NGNs. NGNs are expected to combine "the scalability and reliability of the public telephone network with the reach and flexibility of the Internet" (Sweeney, 2001). It is also estimated (Tekelec, 2001) that up to 50% of savings on operational costs can be made when voice and data networks are combined.

In addition to the above, various technical and economic forces are leading the way towards the deployment of next-generation networks.

2.3.2 Market and technology drivers for NGNs

Several combined market and technology factors are now pushing network operators towards introducing NGNs.

2.3.2.1 NGN market drivers

NGN market drivers are, in order of importance, the growth of data traffic, the need for service providers to satisfy new customer requirements, and increased competition.

2.3.2.1.1 Growth of data traffic

The main driving force behind the shift towards NGNs is the growth of data services directly caused by the growth of the Internet. According to many estimates (Krogfoss & Pirot, 2001) the volume of data traffic already exceeds that of voice traffic and keeps on growing at a rate of at least 100% a year, while voice traffic is only growing at about 10% a year. This may result in voice traffic only representing a small portion of the network traffic in the coming years. It is therefore sensible to carry voice as an application over the data network instead of maintaining a separate voice infrastructure. This convergence is unavoidable, given that revenue from data services is gradually exceeding revenue from voice services and that the data infrastructure is actually cheaper to implement than the traditional voice platform (Huitema, 1999).

2.3.2.1.2 New customer requirements

The second market driver for NGNs is the increasing demand among customers for new services and applications offering more sophisticated features that cannot be provided by today's networks. Users are demanding more bandwidth for their services at a lower price. They want more flexible and innovative services that can be tailored to their individual social and professional needs (Tekelec, 2001). For example, customers want mobility in various forms (access device or application), easy-to-use communication over different media and content of higher quality for entertainment or education (Modaressi & Mohan, 2000).

NGN services can be classified in three categories: access, interconnectivity and application (Falshaw, 2001). Examples of such services (so-called *triple-play* services, since they combine voice, video and data) are the following:

- Access services

They enable access to voice, video and data services through a single network connection. Users can enjoy a direct control over service configuration through web-based interfaces. They can also get cost and time reduction for service usage by using only one interface for different types of services (Falshaw, 2001).

- Interconnectivity services

This type of service enables a company's resources to be shared more effectively between its employees, partners and customers. The main types of interconnectivity services are IP VPN (Virtual Private Networks) and IP Centrex (Falshaw, 2001). A Centrex (a contraction of Central Exchange) is an advanced telephone switching service offered by a telephone company (Melamed, 2005). An IP Centrex enables enterprises to unify voice telephony and Internet technology on a single network managed by a service provider. It provides the functionality of a Centrex with the added advantages of VoIP (Melamed, 2005).

- Application services

Application services provide a set of features to address the specific needs of an organisation. Common examples of application services are the following:

  – Voice portals or speech-enabled Internet portals: They offer callers any kind of information such as news, weather, stock quotes and account balances through a webpage via simple voice commands and any telephone (Intel, 2001).

- Unified messaging: It enables the integration of various message types (such as SMS, e-mail, voice-mail) into a single multimedia mailbox and permits translations between the different media (e.g. voice to text, text to voice) (Tekelec, 2001).
- Multimedia conferencing: It allows remotely located users to converse, see each other and share or modify electronic documents at the same time from an electronic device such as their mobile phone or their PC (Falshaw, 2001).

2.3.2.1.3 Growing competition

The third market force that drives operators towards the wide deployment of NGNs is increased competition accentuated by deregulation in the telecommunications market. Governments worldwide are forcing carriers to operate in a competitive industry in an open market (Modaressi & Mohan, 2000). Although revenues from voice services are still the main source of income for operators, the high competition continuously lowers their profits. Thus they are seeking new ways to distinguish themselves in the future by offering advanced services as mentioned in the previous section. In a competitive market, operators need to reduce costs, operate efficiently and respond more flexibly to market demands (Falshaw, 2001). NGNs have the potential to help achieve these objectives.

In addition to market drivers that justify the trend towards converged networks, a number of technology drivers encourage the development of NGNs.

2.3.2.2 NGN technology drivers

Various technology developments enable the deployment of NGNs. Two such key technologies are voice over IP (VoIP) and IP routers.

2.3.2.2.1 VoIP

VoIP refers to the technology used to transmit voice traffic as packets over a data network using the Internet Protocol. Since these packets are made of compressed digital bits, less bandwidth is needed to carry the same amount of voice traffic in IP-based networks than in the PSTN. It also allows saving money since smaller bits are transmitted with digital compression (Gillwald, 2003). As VoIP services are increasingly closer to PSTN quality and are much cheaper, they represent a valid alternative for public network voice services and are a fundamental enabling technology for converged voice and data networks (Falshaw, 2001).

2.3.2.2.2 IP routers

IP routers, as computing hardware, generally follow Moore's law for their price/performance, as this doubles every 18 months. As the performance of IP routers increases, it becomes easier to manage and support real-time traffic such as voice. As their price decreases, it becomes much cheaper to build a packet-switched network instead of a circuit-switched network (Hall *et al*, 2000).

NGNs can offer numerous advantages over current networks, but these expected benefits can be jeopardised by various security issues that are likely to be a threat to this new type of networks.

2.4 NGN security threats

NGNs face security vulnerabilities that may lead to many fraudulent activities. These vulnerabilities stem from key characteristics of NGNs, such as the fact that they are IP-centric and can be accessed from many different mechanisms. A review of the potential security threats follows below.

2.4.1 NGNs are IP-centric

As mentioned in Chapter 1, NGNs belong to *data communications* in contrast to traditional *telecommunications,* because they are based on IP (Abramowicz & Ledberg, 2002). This exposes NGNs to all IP inherent security threats, such as malware and denial-of-service attacks.

The term malware is a contraction of 'malicious software' and refers to any software designed with the purpose of causing damage to a computer system. Examples include a virus and a Trojan horse (Dwan, 2004). A computer virus is a piece of code that can modify executable files so that they include a copy of the virus and corrupt any infected programs (Dwan, 2000). A Trojan horse is a destructive program that is disguised as a legitimate and harmless application (Qian *et al*, 2006).

A denial-of-service attack is a severe assault against a computer host or a network aimed at limiting or preventing legitimate users' access to the network. It either concentrates on overloading the network with many simultaneous requests or on making the server (s) crash. This could render the communications networks momentarily unusable (Karlsson, 2001).

Besides, IP networks have open, multilayered architectures with no embedded security mechanisms (IEC, 2004b). Thus, they can be easily exploited for fraudulent actions such as IP spoofing (the use of a forged IP address for impersonation), making it easier to conceal fraud (Modaressi & Mohan, 2000).

In an IP network platform, some of the infrastructure's components such as the domain servers and a default router need to be visible to end-systems for communication. However, these components can be vulnerable to attacks and exploited to gain access to other components in the infrastructure (Rolfe, 2003). Being able to access NGN network elements such as gateways and call agents through the Internet puts these components and the whole network at risk. Hackers can exploit design and programming errors to gain control of the network infrastructure through these elements. For instance, malicious users could use the call agents to modify the control signals in order to make free calls. They could also send messages through the SS7 gateways that would damage the infrastructure (Huitema, 1999).

Proprietary interfaces and protocols used by telecommunications equipment in traditional voice networks have the advantage of being protected from public knowledge and external access. Committing fraud on these closed networks is therefore somewhat limited and usually necessitates the assistance of an insider (Hearne, 2004). This security feature is lost in IP networks as their open interfaces are well documented and understood by a far wider number of people. For instance, protocols such as routing, VoIP signalling, DNS (domain name service) and SMTP (simple mail transfer protocol**)** for e-mail are publicly known, which makes it fairly easy for hackers to misuse them by altering their transmission. Attacking and compromising the security of previously highly protected systems is therefore much easier (Dunham, 2004).

The PSTN follows a centralised architecture where the intelligence is located in the switch and the phones are just dumb terminals. This is different from IP networks that have a decentralised architecture where the endpoints hold the intelligence of the network. As these endpoints interact with other IP-based network elements, there is a greater risk of misuse for an IP-based network than for traditional voice networks (Hearne, 2004).

2.4.2 NGNs are accessed by many mechanisms

The possibility to use various mechanisms to access the network makes it possible for fraud to be committed from different access points simultaneously. Detecting fraud therefore necessitates the continuous exchange of information between all service elements and network devices, followed by the comparison of all network traffic. Unfortunately, current network elements cannot effectively exchange relevant information between them, because they use vendor-specific data formats. They need the assistance of a mediator to aggregate the necessary information (Modaressi & Mohan, 2000), which causes delays in data analysis and makes timely fraud detection more problematic in NGNs.

Shared media of communication also allow many indiscretions such as eavesdropping (intercepting the line between the sender and the receiver) and password sniffing (the illegal analysis of network traffic to intercept user passwords) (Modaressi & Mohan, 2000).

As mentioned previously, many of the security loopholes of NGNs result directly from their key characteristics. Since these characteristics are specific to this new type of networks, the associated vulnerabilities are also new in the network security and fraud management communities. This explains why no adequate FMS to prevent and detect the abuse of these vulnerabilities exists at present. It is therefore reasonable to assume that any NGN will be a target of choice for hackers. Fraudsters will feel free to devise new techniques to exploit NGN vulnerabilities without even having to run the risk of being caught, unless a suitable FMS is put in place. This argument motivates the goal of this thesis, which is to design such a system to be implemented and deployed before the general lauching of NGN services.

2.5 Conclusion

An NGN is a big opportunity to enhance the range and quality of telecommunications services. It enables not only a reduction in operational costs, but also increased profits for operators and enhanced customer experience. Unfortunately, it also poses many security risks. Releasing new products without adequate security controls and secure technologies in place is a huge risk for network operators and customers, as it opens the door to a plethora of fraudsters. They will be very quick to exploit the numerous security holes present in NGNs, and this will severely undermine the efficiency of the networks and compromise customers' acceptance of the new services.

Although the primary reason for investing in NGNs is to maximise profits, operators have no option but to also invest heavily in minimising revenue loss resulting from fraud. Effective fraud management therefore becomes vital. However, finding a suitable solution to the fraud problem in an NGN environment first of all necessitates a deep understanding of fraud techniques, motivations and types of perpetrators. These are dealt with in the next chapter, which gives detailed information on the current situation of telecommunications fraud. The discussion in Chapter 3 goes on to provide the basis for the analysis of the evolution of fraud in NGNs, which appears in Chapter 4.

Chapter 3: Telecommunications fraud: the current situation

3.1 Introduction

Telecommunications fraud is a major threat to the well-being of the telecommunications industry and has the potential to increase in NGNs as shown in the preceding chapter. Fraud has even been identified as the main source of revenue leakage for operators (Jacobs, 2004). This chapter reviews the problem of telecommunications fraud as faced by operators on current network types with the aim of understanding how and why fraud is traditionally committed. This knowledge will enable us to determine how fraud techniques may change in NGNs. The chapter is composed of two main sections. Section 3.2 provides some background information on fraud and explains its main causes and consequences. Section 3.3 reviews common types of telecommunications fraud.

3.2 Background on telecommunications fraud

This section gives in-depth background information on the current problem of telecommunications fraud. The section begins with a definition of telecommunications fraud and an explanation of the different motivations of fraudsters. This is followed by an analysis of the severity of the issue based on its consequences and the numerous challenges of fighting this crime.

3.2.1 Definition of telecommunications fraud

For clarity, the author first defines fraud and then distinguishes it from bad debt. This differentiation is necessary since people often confuse these two concepts.

3.2.1.1 What is telecommunications fraud?

No standard definition for "telecommunications fraud" currently exists. However, from an industry point of view, fraud managers commonly use this term to refer to "the theft of services or deliberate abuse of voice and data networks" (Jacobs, 2004). From a legal perspective, APRI (American Prosecutors Research Institute) defines this type of offence as "the use of telecommunications devices to intentionally deceive or criminally manipulate a person for financial gain" (Johnson *et al*, 2004). Given that fraud always involves some form of deception as will be shown in the fraud types described in Section 3.3, the author slightly modifies the industrial definition of Jacobs (2004) given previously to provide her own meaning of telecommunications fraud as follows:

Telecommunications fraud is the theft by deception or the deliberate misuse of services offered via a telecommunications system.

3.2.1.2 What is the difference between fraud and bad debt?

Fraud is often treated as bad debt, although the two concepts are actually quite different. This misconception is due to the fact that both result in revenue loss due to customers' failure to pay for their service usage. The fundamental difference between fraud and bad debt is the *intention to pay or not to pay* (Meyer, 1997).

Fraud occurs when someone contracts a service with *no intention* to pay. This can be achieved by either using another person's legitimate service without his prior agreement or by using false personal details, thereby making it hard or impossible to identify the subscriber. Fraud is intentionally harmful and therefore causes far more damage than bad debt.

Bad debt occurs when someone contracts a service and cannot pay for it due to a change in his financial situation, such as bankruptcy. Bad debt can also be the result of technical errors, such as some errors in the billing systems. Sometimes, bad debt is merely due to poor account administration by the service provider or the customer himself (TUFF, 2004). For instance, the customer moves out and forgets to inform the operator of his new address, or changes in the customer's bank details are not updated in the billing database.

In many cases, fraud and bad debt are indistinguishable, until a thorough investigation is conducted. For this reason, fraud losses are sometimes concealed in bad debt figures and are treated as such. This means that the same techniques used for counteracting bad debt are also applied to fraud. They generally involve sending several bills followed by warning letters and restrictions on the service, until complete disconnection. This results in totally ineffective fraud management measures and actually allows a much greater window of opportunity for the fraudster (Meyer, 1997). It has been assessed that fraud accounts for 50% to 70% of total bad debt (Beck Computer Systems, 2004).

This thesis will focus only on fraud, because fraud will definitely be affected by NGNs, while bad debt may not. Telecommunications fraud is highly dependent on network technology and service types, while bad debt is not. For this reason, fraud is likely to increase and new forms of fraud may emerge due to new NGN services and technologies. Whereas fraud can be prevented and

considerably reduced with effective measures in place, bad debt is unintentional and unpredictable and thus cannot be prevented. It is generally accepted as a cost of doing business.

Given that telecommunications fraud is a punishable crime in many countries, what motivates people to engage in this illegal activity? The next section attempts to provide an answer to this question.

3.2.2 Motivations for telecommunications fraud

The section starts with an identification of the main types of fraudsters and then gives the main reasons why these individuals commit fraud. This information is used in the next chapter to determine the likely effect of NGN services on fraudsters' profiles and motivations and how this will affect the types of fraud committed in NGNs.

3.2.2.1 Who commits telecommunications fraud?

On an industrial scale, fraud is mainly perpetrated by organised criminal gangs, professional hackers and operators' own employees (Beck Computer Systems, 2004). In fact, it is estimated that almost 73% of all telecommunications fraud is initiated from inside the victim telecommunications company (Beck Computer Systems, 2004). However, due to the availability of numerous hacking and phreaking tools on the Internet, fraud has become a widespread crime that can be committed by anybody depending on one's individual goal (Jacobs, 2004). The term phreaking is used in the hacker community to refer to the act of using a computer or other device to trick a telephone system. Typically, phreaking is used to make free calls or to have calls charged to a different account (Grossman, 1998, p. 127).

Although fraud is generally perpetrated by a criminal at the expense of the operator, the operator and the scammer are not the only actors that can be involved in fraud. Other possible actors include the customer, a third party operator, and as mentioned earlier, the employee (Wikipedia, 2007). The researcher's diagram in Figure 3.1 illustrates the potential involvement of different possible fraud actors.

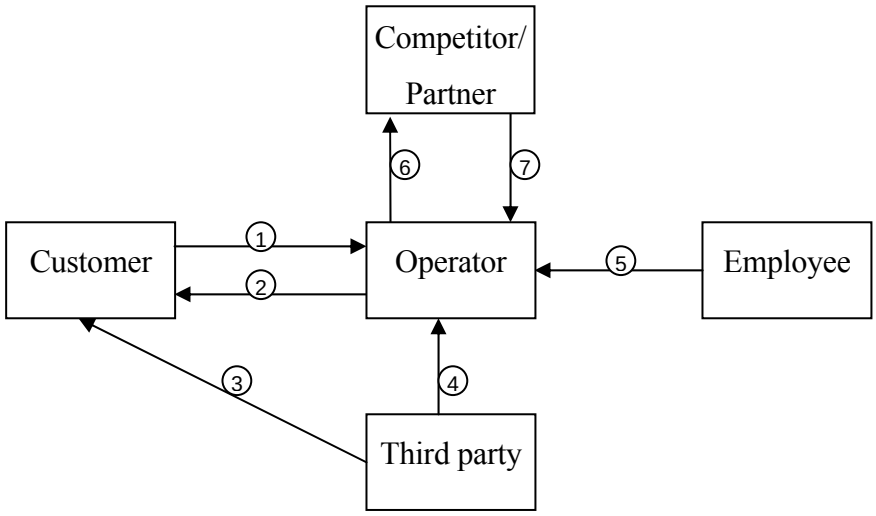

Figure 3.1: Relations between fraud actors in traditional telecommunications networks

In Figure 3.1, the so-called third party refers to an individual who is not related to the operator. That is, a third party is neither a customer, an employee, a partner nor a competitor. Typically, a third party is either an isolated hacker or a member of a criminal gang.

The arrows in the diagram indicate the flow of fraudulent activities from the perpetrator to his target. For instance, arrow 1 indicates that fraud can be committed by a customer against his operator, while arrow 2 shows that the operator can also commit fraud at the expense of his customer. Actors in the diagram and their associated arrows are representative of the fraud types publicly reported in the telecommunications industry. The absence of arrows between two actors (e.g. between a third party and an employee) indicates that no such fraud scenario has been reported so far and it can therefore be considered very unlikely.

Available literature on telecommunications fraud only contains details on fraud types related to arrows 1, 3 and 4. It is not quite surprising that hardly any papers (GAO, 1999; Smith, 1998) mention fraud associated with arrows 2 and 6, as such scams are initiated by the operator. Staff fraud, represented by arrow 5, is often treated as a taboo subject (Meyer, 1997). This research project focusses on frauds that target the operator (arrows 1, 4, 5 and 7) as the latter is the only sponsor and main beneficiary of effective fraud management solutions. For obvious reasons, no operator wants its FMS to detect frauds that it initiated. Examples of such fraud types are however given in this chapter for illustration purposes.

3.2.2.2 Why do people commit telecommunications fraud?

The main reason for committing fraud is to make money. Fraud perpetrated for this purpose is often referred to as *revenue fraud*, which can be achieved by selling fraudulently obtained services at cheap rates or by selling critical company information to other criminals (Cerebrus Solutions, 2002c). Revenue fraudsters often exploit socio-economic conditions such as poverty, migration and demographics (Johnson, 2002a). For instance, an organised call-selling operation – explained in Section 3.4 – is more likely to be profitable in a small urban area with many poor immigrants. These immigrants probably want to contact family members in their home country but cannot afford the high rates of international phone calls (Johnson, 2002a).

Other reasons for committing telecommunications fraud, also known as *non revenue fraud,* include the following (Johnson, 2002a):

- To avoid or reduce payment of services. This can be related to the example described above where poor foreigners are tempted to look for illegal ways to make calls to overseas destinations at reduced costs.
- To provide free or cheap services to friends and relatives. This is often the primary reason for staff fraud.
- To maintain anonymity while committing other crimes. For instance, criminals can circumvent phone-tapping by illegitimately accessing and using the telephone network (Cerebrus Solutions, 2002c).
- To demonstrate ability to outmanoeuvre the operator's system security, in other words, to rise to the bait of the 'challenge factor'.
- To achieve political or ideological motives (e.g. cyber terrorism). Ideological beliefs can also be an incentive for revenue fraud. According to a survey conducted in 2003 by the Communications Fraud Control Association (CFCA, 2003), some operators reported that the increase in worldwide terrorism was one of the reasons for the rise of global fraud losses. Indeed, terrorist organisations often commit revenue fraud to raise money for financing their activities.

Although people usually commit fraud to make money, in practice, it has been demonstrated that an operator's fraud cases can be expected to be evenly split between revenue fraud and non revenue fraud (Cerebrus Solutions, 2002c).

Countless people in the world commit fraud for the reasons mentioned above. To find out exactly how serious this problem is, it is therefore important to analyse its real impact on the victims. This analysis constitutes the subject of the following section. Knowledge about the impact of fraud is an important aspect of fraud management as it is used as a prioritisation criterion to identify fraud types that need immediate further investigation.

3.2.3 Impact of fraud

Both the service provider and the service consumer suffer as a result of fraud. The service provider suffers from substantial loss of revenue and a damaged reputation (Brad, 2001), which can in turn result in increased customer churn. As mentioned in Chapter 1, estimates show that operators globally lose between 3% and 8% of their annual revenues to fraud (Jacobs, 2004). This amounts to more than USD 44 billion globally (Ibbett, 2007). In South Africa, Telkom reported annual fraud losses of ZAR 95.4 million, which include costs to restore stolen cables and sabotaged equipment (Mogaki, 2005). Note that these figures do not take into consideration the high cost of fraud investigation or of litigation of disputes. This requires sophisticated software with huge data storage capabilities, and highly skilled personnel available 24 hours a day and 7 days a week (Meyer, 1997).

The service consumer can also suffer from loss of privacy and negative credit rating due to identity theft. He can experience overcharged bills due to the unauthorised use of his account by criminals or as the result of his service provider's dishonesty. Furthermore, fraud can consume a significant amount of network capacity, resulting in poor quality of service and temporary loss of business continuity (Brad, 2001). The latter obviously puts the operator at risk of losing even more revenue because legitimate customers cannot access the network to use the services. To crown it all, operators often have to raise service rates to mitigate fraud losses (Hearne, 2004).

According to Hynninen (2001) fraud losses can be divided into two categories, namely soft currency and hard currency:

- Soft currency provides a theoretical figure amounting to how much the customer would have normally paid for the service if he hadn't used it illegally (Hynninen, 2001). This figure is not always realistic, for very often the fraudster would never have used the service – or at least not that extensively – if he had had to pay for it. This is because fraud usually targets very costly services such as international phone calls (Meyer, 1997). Fraud resulting

in soft currency loss has a high financial impact only when it is performed on a large scale. In such a situation, the main damage is usually a lot of bandwidth consumption, which can result in network downtime and denial of service.

- Hard currency corresponds to the money that the operator has to pay to a third party service provider for the service used by the fraudster, based on prior settlement agreements (Hynninen, 2001). For instance, this can be money that the operator has to pay to a roaming partner, irrespective of whether he receives money from the service consumer. Fraud attacks that result in hard currency loss have a high financial impact on the operator, no matter the scale on which they are perpetrated. Such fraud types therefore require a high level of priority during the fraud detection process.

In Figure 3.2 the author roughly illustrates the correlation between fraud impact and scale for hard currency and soft currency losses. The scale refers to any parameter used to evaluate the magnitude of the fraud. For instance, it can be the number of calls made fraudulently, the duration of these calls, or both. The threshold defining the largeness of the scale depends on the type of fraud committed.

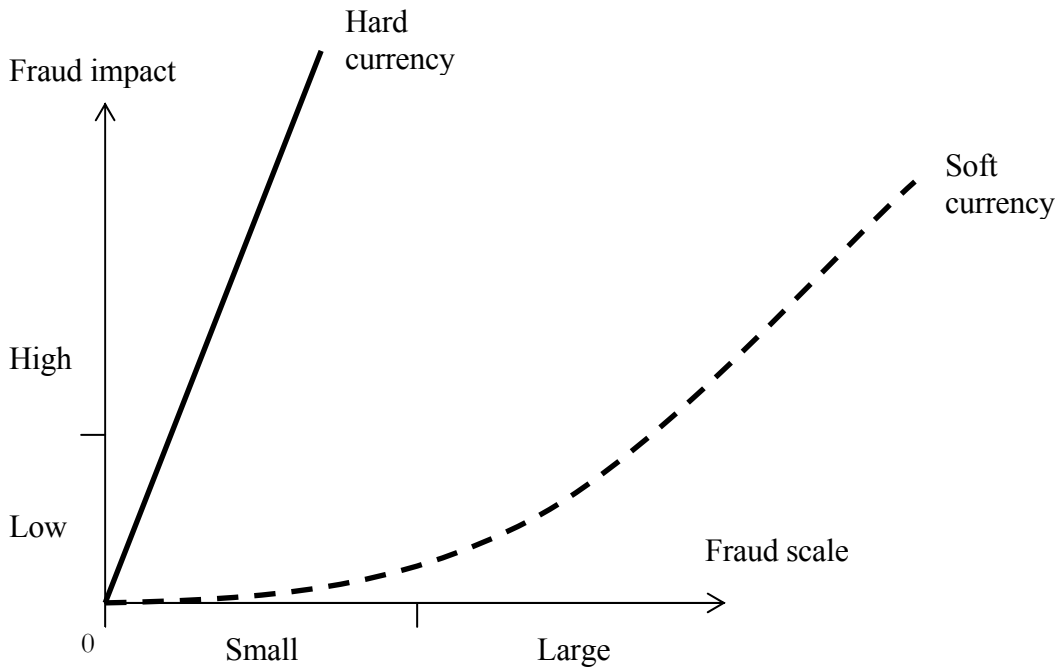

Figure 3.2: Impact of hard and soft currency losses based on fraud scale

Figure 3.2 shows that fraud resulting in soft currency has a very low impact when the scale is small, but its impact increases significantly as soon as the scale becomes large. This is because the fraud only affects the operator's own network and services, which the operator does not have to

pay for except maybe for a minimal maintenance cost. On a large scale, however, this fraud can result in network downtime and customer churn.

Fraud that creates hard currency loss, on the other hand, always necessitates the operator to pay a third party service provider and therefore always has a fairly high impact, which increases with the scale of the fraud. This thesis focusses on hard currency fraud.

3.2.4 Challenges to fighting fraud

Fraud is an ever-increasing threat that is difficult to combat. Below follows a summary of the reasons why this is the case.

- As mentioned earlier, a plethora of phreaking and hacking tools are easily accessible from the web at little or no cost. Some examples of such tools are as follows.
  - Phone Phreakers Bible (USD 8) and Cellular Hacker's Bible (USD 35) used for telephone phreaking and cellular cloning (HackersCatalog.com, 2005).
  - CIDMage (USD 59.95) used to generate fake caller IDs for the purpose of making calls on behalf of selected victims (CodeGods.net, 2005).
  - THC-PBXHacker (freeware) used for hacking any PBX (PacketStorm.com, 2005). A definition of a PBX is provided in Section 3.3.1.
- Companies keep quiet about their fraud problems for fear of losing customers' trust and attracting even more fraud attacks. In fact, as many as 70% of fraud occurrences are not reported (Hodgson, 2003). Operators do not cooperate on fraud issues as they consider this a competitive advantage (Marshall, 2002) that enables the recurrence of attacks on other operators' networks. In addition, victims very often do not report their fraud cases to telephone companies or the police.
- Current legislations provide very limited protection against this offence, as legislators perceive it as a minor issue compared to violent or physical crimes. Besides, law enforcement agencies often do not have adequate training and equipment to investigate this type of crime (Hodgson, 2003).
- Criminals have more and more technology savvy and their fraud scenarios are increasingly sophisticated and ever-changing (Johnson *et al*, 2004). Therefore, due to their 'outdated' technical knowledge, fraud managers are often left one step behind.

- The anonymous nature of fraud, and the usual remoteness of the fraudsters from the crime scene make it particularly hard to apprehend the culprits. This is further complicated when fraud schemes are spread over many countries or different jurisdictions (Hodgson, 2003).

Section 3.2 served as an introduction to telecommunications fraud. It answered some non-technical questions about this threat, namely what is fraud, who commits fraud, why do people do it, how much does it cost and why is it hard to fight? This general background information allows to specify the scope of this dissertation from a fraud perspective as follows: *The thesis focuses on fraud as a deliberate crime (and therefore excludes bad debt) committed at the expense of the operator, and priority is given to fraud cases resulting in hard currency loss.* The next section provides more technical details and shows examples of how fraud is perpetrated. This technical knowledge forms the basis of the analysis of the likely evolution of technical fraud in NGNs which is dealt with in the next chapter.

3.3 Common types of telecommunications fraud

The International Data Corporation has identified more than 200 forms of telecommunications fraud. These can be classified in many ways depending on the selected parameter (Jacobs, 2004). Section 3.3.1 reviews usual classification parameters and categorises common fraud types according to the network type on which they are perpetrated, while Sections 3.3.2 to 3.3.5 describe the different fraud types.

3.3.1 Fraud type classification

Most of the existing forms of fraud are perpetrated using the following two basic strategies: the fraudster either impersonates someone or technically deceives the network systems. These strategies or schemes are respectively known as *social fraud* and *technical fraud* (Beck Computer Systems, 2004). Other commonly used classification parameters are the following:

- The goal – revenue and non revenue fraud.
- The fraud perpetrator/fraud target pair (examples of such actors were shown in Figure 3.1).
- The method – the following five generic fraud methods have been identified (Cerebrus Solutions, 2002c):
  - Subscription: An individual subscribes to a service with the intention to commit fraud.
  - Surfing: Obtaining someone's account access details either electronically or through social engineering.

- Ghosting: Mechanically deceiving the network to get free or discounted rate services.
- Accounting: The abuse of billing processes to diminish charges.
- Information abuse: To obtain critical information and resell it.

In this research project, the network type is used as the primary parameter to categorise fraud techniques because this parameter provides a key indication in respect of the potential development of fraud in NGNs. The researcher's classification is shown in Table 3.1. Fraud types are sorted in alphabetical order. Note that network types used in the table are traditional telecommunications networks as known in the fraud management industry, as they do not offer any form of network technology convergence.

All voice networks	**Fixed voice networks**	**Mobile voice networks**	**Data network (Internet)**
▪ Call-forwarding fraud ▪ Call selling ▪ Calling-card fraud ▪ Cramming ▪ Interconnect fraud ▪ Internal fraud ▪ PBX (private branch exchange) fraud ▪ PRS (premium rate service) fraud ▪ Subscription fraud ▪ Telemarketing fraud	▪ Clip-on fraud ▪ Hacking	▪ Cloning and tumbling ▪ Handset theft ▪ Roaming fraud	▪ Credit card fraud ▪ E-commerce fraud ▪ Investment fraud ▪ IP spoofing ▪ Nigerian money offer ▪ Pharming ▪ Phishing ▪ Work-at-home scheme

Table 3.1. Common fraud types on traditional telecommunications networks

Globally, the top five fraud types in terms of economic losses are subscription fraud, PRS fraud, roaming fraud, internal fraud and cloning (Ibbett, 2007).

In the next four sections, an explanation of each of the fraud types indicated in Table 3.1 is provided according to the corresponding network type.

3.3.2 Fraud types that affect all voice networks

- **Call forwarding fraud**: *The set-up of a local number to fraudulently forward calls to an international number* (Jacobs, 2004). Various scenarios exist for this scheme. Typically, a con artist calls a victim pretending that he inadvertently dialled a wrong number and that he urgently needs to contact someone else but cannot make another call. Usually, the scammer

claims that he has been arrested for driving with an expired licence and that he needs to call a relative to fetch his children at school. He then begs the victim to help him reach his relative by forwarding his call to the correct number. He gives the victim some instructions, followed by a number, which actually enables the criminal to forward all incoming calls to international numbers. In the USA, where this fraud has been reported countless times, the call forwarding activation code is *72. In so doing, the victim unwittingly allows his phone number to become a relay for international calls, which are charged to his account (Snopes.com, 2004). In some other cases, the con artist poses as a telecommunications technician and instructs the victim to dial a specific number preceded by *72, purportedly for maintenance purposes (Snopes.com, 2004). The victim can even receive a message on his phone that informs him that he has won a prize and that he needs to dial a given number to claim his prize.

- **Call selling**: *The resale at discounted rates of fraudulently obtained telephone services* (Cerebrus Solutions, 2002c), *with no intention of paying the account*. This fraud type is generally well organised and carried out on an international scale (TUFF, 2004).
- **Calling-card fraud**: *Getting access to telephone services through fraudulently obtained calling-card details*. Such details can be obtained through the theft of the card, hacking or shoulder surfing (Cerebrus Solutions, 2002c).
- **Cramming**: *Cramming is the addition of charges on a customer's bill for services that were not ordered or used.* This is an example of a fraud perpetrated by an operator at the expense of his customer. The additional charges are often positioned in such a way that they are barely distinguishable from the normal charges. A consumer can be crammed by simply responding to a voice prompt in the course of a telephone conversation, by accepting a collect call (i.e. paid by the receiver) or by filling out a sweepstake form (Smith, 1998).
- **Interconnect fraud**: *The falsification of customers' usage records in order to miscalculate the money owned by one operator to another.* This affects calls that change networks between the caller and the receiver, such as international calls or calls from fixed to mobile networks. A common technique of interconnect fraud is **refilling**, which consists of changing the originating number before transmitting the call to the competitor. As call charges between operators often depend on the "percentage of the total distance over which each operator carries the call", refilling attempts to decrease this percentage to reduce the charges (Wikipedia, 2007).
- **Internal fraud**: *The use of an employee's position within a telecommunications company to commit fraud*. The employee can either perpetrate fraud himself or provide confidential

information that enables other criminals to commit fraud. Examples of internal include: removing records from billing systems, creating fictitious customer accounts, reactivating used prepaid voucher numbers or manipulating the accounting and credit processes (Ibbett, 2007). Internal fraud can be perpetrated at any job level within a company. It can also be committed by disgruntled ex-employees.

- **PBX fraud**: A PBX (Private Branch Exchange) is a privately-owned telephone switching system serving one company. Similar to a Centrex, it provides access to a given number of inside and outside lines, with the difference that the switching occurs on the customer's premises instead of at the operator's local office (Melamed, 2005). *A popular way to misuse a PBX is through DISA (Direct Inward System Access), which is a PBX feature that permits incoming employees' calls to be routed to outside lines at the expense of the company.* This feature is very handy for travelling employees who avoid high rates when making business calls overseas. Since this feature is activated via an access code, PBXs are often compromised to obtain DISA access codes and make international calls to the detriment of a private company (Hoath, 1998).
- **PRS (Premium rate service) fraud**: *A PRS offers an information or entertainment service such as weather forecasts or prize-winning competitions, at higher than normal call rates.* In such a service set-up, the network operator and the premium rate service provider share income from calls received. This is the case whether or not the operator succeeds in receiving money from the callers. PRS numbers are exploited for fraud in two ways. Firstly, they can be dialled fraudulently by people who want to use the service without paying. Secondly, the service provider itself sometimes illegally dials its own PRS numbers in order to increase the number of incoming calls. This can be don manually or with some auto-dialer software. This is performed to raise the service provider's revenue from the operator (Ibbett, 2007).
- **Subscription fraud**: *The subscription to a service with no intention of paying for the bill.* The scammer usually presents a false or stolen identity to register and makes extensive use of the service for a short period of time before disappearing. This scam is often associated with call PRS fraud and selling. Subscription fraud is currently the most prevalent form of fraud (Ibbett, 2007).
- **Telemarketing fraud**: "*Any scheme to defraud in which the persons carrying out the scheme use the telephone as the primary means of communicating with prospective victims and trying to persuade them to send money to the scheme*" (Johnson *et al*, 2004). Usually, telemarketing fraudsters use fraudulently obtained telephone lines in order to retain

anonymity. There are many variants of telemarketing fraud, inter alia the prizes/sweepstakes, and the so-called 'half-price scam', a telemarketing scheme that targeted Telkom in South Africa. The two schemes are described below:

– **Prizes/sweepstakes**: An individual receives a call from a telemarketer claiming that he has won a valuable prize. He is required to pay a processing fee or to buy a product before receiving the prize and only obtains a cheap and worthless gift that costs much less than the amount he paid (Johnson *et al*, 2004).

– **Telkom half-price scam**: Masquerading as a Telkom official, the fraudster phones a customer, proposing to write off his telephone bill for that particular month, provided that he pays 50% of the due amount to a specified bank account. After obtaining the customer's consent, the con artist uses a fake cheque to pay Telkom and issues the customer with a receipt as proof of cash payment. The customer then deposits the money into the given bank account and only realises he has been conned once Telkom informs him that the cheque has been rejected and he still owes last month's bill (Telkom, 2004).

3.3.3 Fraud types specific to fixed voice networks

- **Clip-on fraud** (called clip-on in America and teeing-in in the UK): *The physical connection to a legitimate customer's telephone line in order to make free calls at his expense* (Collins, 1999). Basically, customers receive access to telephone services through a pair of wires within a cable connected to the telephone exchange. These cables are usually laid underground up to a distribution point, but are often visible on the outside of buildings for maintenance purposes. The fraudster opens this distribution point to cross connect his line to the victim's line. This is often achieved through the use of some elementary alligator clips (Collins, 1999).
- **Hacking:** *The use of specialised software to obtain access codes to a telecommunications system in order to abuse the network* (TUFF, 2004). Examples of tools that enable this were given in Section 3.2.4.

3.3.4 Fraud types specific to mobile voice networks

- **Cloning**: *The programming of the identification details of a legitimate phone onto the fraudster's phone.* Cloning is still a widespread threat in older analogue networks. Cases of cloning in GSM (Global System for Mobile Communications) systems, the successor of

analogue networks, have also been reported (Isaac, 2004), but GSM cloning is not regarded as a major issue. In analogue networks, the identification details that are reproduced are the Mobile Identification Number (MIN) and the Electronic Serial Number (ESN). The MIN identifies the customer, while the ESN identifies the phone (Ericsson, 2004). Such information is usually obtained through eavesdropping with scanning devices during phone calls or by theft. Fraudsters can also extract ESN/MIN pairs from mobile phones that are being repaired, or steal them from the operator's records (Ericsson, 2004). Calls made on the cloned phone are then charged to the owner of the original phone. A variant of this fraud type is called **tumbling** (Cerebrus Solutions, 2002c), whereby *the identity of many phones is reproduced onto the cloned phone, enabling it to rotate between its different identities each time a call is made*. Cloning is the best-known type of telecommunications fraud (Cerebrus Solutions, 2002c).

- **Handset theft**: Mobile phones are often stolen as they can be resold and can provide access to the network, at least within the time interval when the theft and the barring of the account occur. Stolen handsets are also often used as clones (Cerebrus Solutions, 2002c).
- **Roaming fraud**: *The exploitation of the delay (up to 72 hours or more) to exchange billing information between roaming operators*. For instance, a customer can subscribe to a service in one country and, in a short period of time, make many expensive calls in another country where there is a roaming agreement between his home operator and the local network operator (Meyer, 1997). It is sometimes also possible for the customer to keep on using his mobile phone abroad for a certain period although his account has already been closed in his home country (Ibbett, 2007). Roaming fraud is often a secondary form of attack as the criminal usually uses stolen or cloned phones or has committed subscription fraud to gain access to the service. Roaming fraud is also often associated with PRS fraud (Ibbett, 2007).

3.3.5 Fraud types specific to the Internet

Internet fraud refers to "*any type of fraud scheme that uses email, web sites, chat rooms or message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme*" (Nationmaster.com, 2005).

Contrary to fraud perpetrated on voice networks, fraud over the Internet does not target free access to services, probably because Internet access is relatively inexpensive compared to voice calls. Generally, fraudsters merely use the Internet as a means to easily commit other forms of

'traditional' fraud not related to network technology, such as credit card fraud or identity theft. The Internet offers a target of choice for criminals because it provides anonymity and crosses geographic borders. Nevertheless, examining Internet fraud is important as many of the new NGN services will be carried over the Internet. Some common Internet scams are the following:

- **Credit card fraud**: *the use of a credit card, or credit card details, without the permission of the card's owner* (TUFF, 2004). When referring to the Internet, credit card fraud involves stealing credit card information to perform fraudulent online transactions, such as buying goods or services. Such information can be obtained through copying details from retail sites, through hacking companies' customer databases or from companies' employees who sell customers' credit card details (Nationmaster.com, 2005).
- **E-commerce fraud**: *the non-delivery of merchandise sold through the Internet*. There are many variants of e-commerce fraud but the most reported form is **Internet auction fraud** (Jenamani *et al*, 2007). In this scam, products advertised for sale through an Internet auction site are deliberately misrepresented or simply never delivered to their buyers. In other cases, the items that are up for bid have been fraudulently obtained (e.g. copied software or items bought using stolen credit card numbers). According to various sources (Rusch, 2003; Furnell, 2005; Bradbury, 2006; Jenamani *et al*, 2007), Internet auction fraud is the largest category of all Internet frauds.
- **IP Spoofing:** *the use of a forged source IP address to create IP packets*. Hackers alter the packet headers by using an IP address that belongs to a trusted host in order to obtain unauthorised access to a computer system. Spoofing can also be used to forge an email address in order to make it appear as if it comes from a trusted source. Email-spoofing is very simple for anyone with the appropriate knowledge of the SMTP protocol. This protocol is used for sending e-mails, but does not have a strong authentication mechanism (Thomsen, 1995).
- **Phishing:** It is a fairly new form of fraud which consists of *sending a fraudulent email that appears to be from a legitimate business*, usually a financial institution, to which the recipient is affiliated. This email urges the recipient to visit a fake Web site that appears to belong to the legitimate institution, where he is asked to enter in personal details (e.g. passwords and credit card numbers) purportedly for updating his account. These details are then captured by the criminal and used for identity theft (Eloff & Granova, 2005). Anybody who has a valid email-address can be targeted for phishing. However, email-addresses that are publicly posted on the Internet (e.g. in newsgroups or on web sites) are more exposed to phishing because these addresses can be easily found by spiders (Beal, 2005). Spiders – also

called webcrawlers or robots – are applications that automatically search and index web pages based on their content and keywords (Aljifri & Navarro, 2004). Spiders are normally used to update search engines' databases, but scammers also use them to find as many valid email-addresses as possible (Beal, 2005). Phishing is based on IP spoofing, as the phishers forge both the email-address and the web site address of the real institution in order to lure the victims.

- **Pharming:** *The use of a Trojan Horse to install a keystroke reader or a redirector on a user's machine that enables the fraudster to record user details such as passwords and credit card numbers, when the user performs financial transactions online* (Entrust, 2005). It is also a very new form of fraud and can be classified as a spyware attack as the victim is not aware of the monitoring occurring on his machine. Spyware is any software that secretly gathers information from a computer and transmits it to someone else (Hinde, 2004). Typically, a pharming attack follows one of the following two scenarios:
  - The victim receives a seemingly legitimate email with an attachment. When opened, this attachment secretly installs a keystroke reader that captures the user's login details typed in through the keyboard when he performs online banking. These details are then sent to the criminal who can use them to access the victim's bank account (Entrust, 2005).
  - When a user visits his online-bank, his session is redirected to the fraudster's web site. This can be achieved by either poisoning the DNS server that supplies the bank address or through a redirector that corrupts the user's HOST files. The user unwittingly installs the redirector on his machine when downloading a particular file or when visiting a Web site that has an ActiveX control. The attacker can then retransmit the session to the online-bank while observing all the traffic between the user and his bank (Entrust, 2005).

  Unlike phishing attacks, which are easy to recognise and to shut down, pharming attacks are hard to detect and to prevent.

Other common forms of Internet scams exploit the naivety of their victims by sending fake emails with false hope of making easy money. As some of these scams are sometimes conducted over the phone, either through calls or fax messages, they also belong to the category of telemarketing fraud. Examples of such scams are Nigerian money offers, work-at-home plans, and investment fraud.

- **Nigerian money offer** (also called advance fee fraud or 419 scam due to "the relevant section of the Nigerian criminal code that it violates"): *a scam aimed at extracting funds from selected victims after making them false promises of receiving a huge sum of money*. Although this scam is usually associated with Nigeria, fraudsters are often active also in other African countries including South Africa. More recently the scam has been launched from big cities outside Africa, including London, Amsterdam, Madrid, Toronto and Dubai. The fraudster, masquerading as a rich citizen (usually a government official or a bank manager) from Nigeria or any other poor country, sends an email to a prospective victim based in a rich country, usually in Europe or America, asking for his help to discreetly transfer a large amount of money overseas. The fraudster asks his victim to allow him to deposit the money temporarily into his bank account. The victim is promised a significant share, often 20% to 40% of the money, for his cooperation. Victims are asked to send personal information such as banking details, business letterheads as well as telephone and fax numbers, and to pay for never-ending processing fees before the money can be sent, which obviously never occurs (Nationmaster.com, 2005).
- **Work-at-home schemes:** *online scammers advertise supposedly lucrative work-at-home business opportunities*. They then require interested individuals to purchase the necessary equipment (e.g. envelopes, paper, and even training software) before they can start the job but fail to provide this equipment. In some cases of assembly work, the individual receives the purchased kit and makes the required items (e.g. toys or plastic signs) but the fraudsters pretend that the products do not "meet the company's standards" and refuse to buy them as they had promised (Johnson *et al*, 2004).
- **Investment fraud:** These *stock market manipulation schemes* basically follow two methods. The first technique, called pump-and-dump, sends out false information in chat rooms, forums, emails and message boards, which pushes up the value "of thinly traded stocks or stocks of shell companies". As soon as the price becomes high enough, the criminals sell off their shares to make a significant profit, which decreases the price of the stock and pushes down the investment of the victims of the scam. The second method, known as short-selling or scalping, follows the same strategy but fraudulently attempts to decrease the value of a specific stock in order to buy it at a low cost and resell it at a high price when it returns to its real value (Nationmaster.com, 2005).

The review of all these fraud types shows that fraudsters are ingenious in finding clever ways to con operators and customers. The risk of criminals taking advantage of potential security flaws

in NGN services is therefore high, given the expected high financial value and ease of use of these services.

3.4 Conclusion

Telecommunications fraud is a major and continuously increasing problem that is hard to fight. With the advent of new technologies and services in NGNs, fraud may worsen significantly. The operator is the primary victim of fraud, and therefore also the primary beneficiary of efficient fraud management systems – except in the case of Internet fraud, which mainly targets individuals rather than companies. It is therefore the responsibility of the operator to have such systems in place. However, implementing fraud management solutions necessitates a clear vision of the evolution of fraud in converged networks. This is the subject of the next chapter. Chapter 4 examines the likely NGN fraud types, based on the current situation of fraud presented in this chapter and the security threats of NGNs analysed in the previous chapter.

Chapter 4: Telecommunications fraud: likely evolution in NGNs

4.1 Introduction

NGNs have many security vulnerabilities that may make them susceptible to an increase in fraud and associated financial losses. This chapter analyses the likely evolution of fraud in NGNs, based on these vulnerabilities and the traditional fraud scenarios presented in Chapter 3. The analysis of likely NGN fraud types will illustrate the differences between the new and the old fraud scenarios. These differences constitute the foundations of this research project, which is based on the fact that current FMSs lack flexibility to effectively detect the possible new fraud scenarios associated with new convergent services. The identified differences will be used to generate a suitable solution to this problem in subsequent chapters.

The chapter starts in Section 4.2 with a discussion of the major drivers for the increase in fraud in NGNs. It goes on to describe NGN fraud types in Section 4.3 and first presents likely generic NGN fraud types in Section 4.3.1. This is followed in Section 4.3.2 by a description of some technology-dependent fraud cases that have recently emerged in new network types for the convergent technologies of VoIP, 3G (3rd Generation) and Wi-Fi. These new fraud types serve as an indication of the expected fraud scenarios in NGNs.

4.2 Drivers for the increase of fraud in NGNs

There is general consensus that telecommunications fraud will increase considerably in NGNs due to the numerous security vulnerabilities of converged networks. It is also generally accepted that it will be harder to counteract this crime due to the novelty and increased sophistication of the fraud scenarios (IEC, 2004b). The reasons for these expectations can be summarised under the following headings featured below: new services and technologies, new billing models and new business models (Kvarnstrom *et al*, 2000).

4.2.1 New services and technologies

Possible fraud scenarios depend on the service types and their underlying technologies. This is clearly shown in the previous chapter that classifies common fraud schemes on the basis of their network type. For instance, clip-on fraud can only be committed in fixed voice networks, while

roaming fraud only targets mobile voice networks. For this reason, new forms of fraud can be expected to appear in NGNs as new services and technologies are introduced. Examples of such new NGN services were discussed in Chapter 2, and mention was also made of some new NGN technologies. For instance, new network components (e.g. softswitches and multimedia servers) are required for deploying NGNs. As is the case with every new technology, these components will probably have new weaknesses that may be exploited by fraud.

A simple illustration of the evolution of fraud due to a new technology is cellphone cloning, which emerged with the advent of mobile voice networks. Fraudsters first exploited the fact that identification details were sent in clear text in analog mobile systems to clone the phone. They then managed to clone the SIM (Subscriber Identity Module) card of a GSM mobile phone because of a design flaw in the authentication algorithm – COMP 128 – of GSM systems, despite the fact that authentication details were encrypted (Hynninen, 2001).

The distributed, standards-based, open and flexible architecture of NGNs allows services to be quickly developed and modified. These services are therefore more dynamic with a shorter lifetime, changing frequently according to customers' demands. Fraudsters are able to exploit this situation and continuously find new techniques to steal the new services and remain one step ahead of the fraud managers. Fraud detection techniques clearly need to be more flexible and they need to be updated constantly.

Furthermore – due to their increased sophistication, NGN services are highly likely to have a greater commercial value than traditional telecommunications services that are now seen as commodities (e.g. phone calls). Thus, criminals will be more attracted towards committing fraud, as their profit will be higher.

4.2.2 New billing models

Unlike current voice networks, which have well-established standards for recording service usage and billing customers, no standardised billing scheme exists for the new IP-based services. Therefore, new accounting standards and billing models will be introduced in NGNs. As NGN services will be offered mostly over the Internet, the new charging models are expected to depend on content and quality – in contrast to old pricing schemes that are usually flat-rate or based on distance and time. This will have an impact on the types of fraud perpetrated, as fraud scenarios are

also a factor of billing models (Lundin, 2002). Fraudsters will unquestionably look for means to exploit the new billing parameters in order to steal the services.

To briefly illustrate how charging models affect fraud, let us consider multimedia services offered online (e.g. video-on-demand and music-on-demand). If these services are prepaid online with a credit card, then obviously, subscription fraud cannot be committed. Criminals will rather attempt to use stolen credit card numbers to avoid payment of the services (Karlsson, 2001).

4.2.3 New business models

The provision of sophisticated NGN IP-based services follows a different business model than traditional telecommunications services, as many more actors are involved. These actors may include the customer, the service provider, the content provider, the application service provider, the network operator and the e-payment provider. Each of them constitutes a potential candidate for fraud the moment money flows from one to the other. Fraud investigation is harder in NGNs because data needs to be gathered from many different sources, contrary to traditional telecommunications networks where the main point of fraud is generally between the operator and his customer (Lundin, 2002).

The different fraud actors in NGN online services are illustrated in Figure 4.1. The dashed arrows show the likely fraudulent relations from the third-party fraudster to his victim, while the solid arrows show the normal flow of money, which can also be misused for fraud.

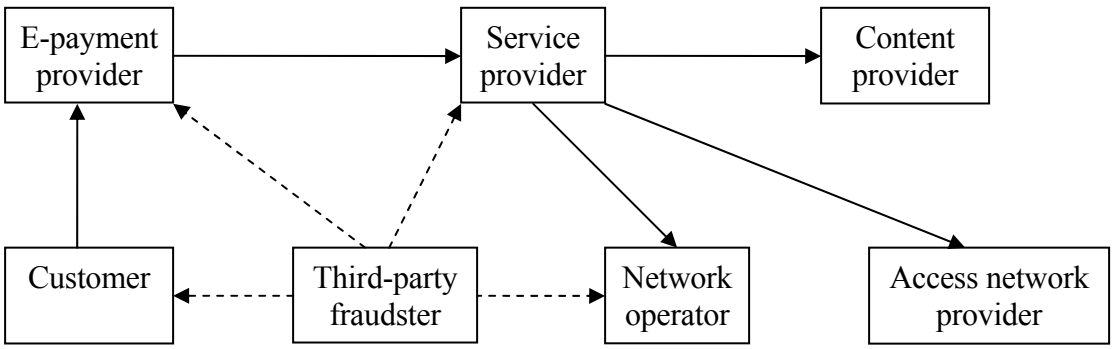

Figure 4.1: Typical fraud relations in NGN services, adapted from Lundin (2002)

Note that this illustration is much more complex than the corresponding diagram in Figure 3.1 (Chapter 3), which showed the different fraud actors in traditional telecommunications networks. It is worth realising that not all these relations are applicable to all NGN services since in certain

services an actor can simultaneously play many roles, such as being both the network operator and the service provider (Lundin, 2002).

An example of the complex situation depicted in the above figure is the so-called "Millionaire" quiz, which is the SMS version of the popular television game show "*Who wants to be a millionaire?*" broadcast in many countries, including South Africa (Wikipedia, 2005b). The SMS-based quiz has many variants but the common rules of this premium-rated game are as follows: The network operator sends out a number of quiz questions to its subscribers via SMS. For each correct answer, the subscriber wins a cash prize but if the answer is incorrect, the operator deducts some money from his account. The quizzes are provided by a specific service provider. In Figure 4.2, the author shows some of the many fraud relations that may result from such a service set-up.

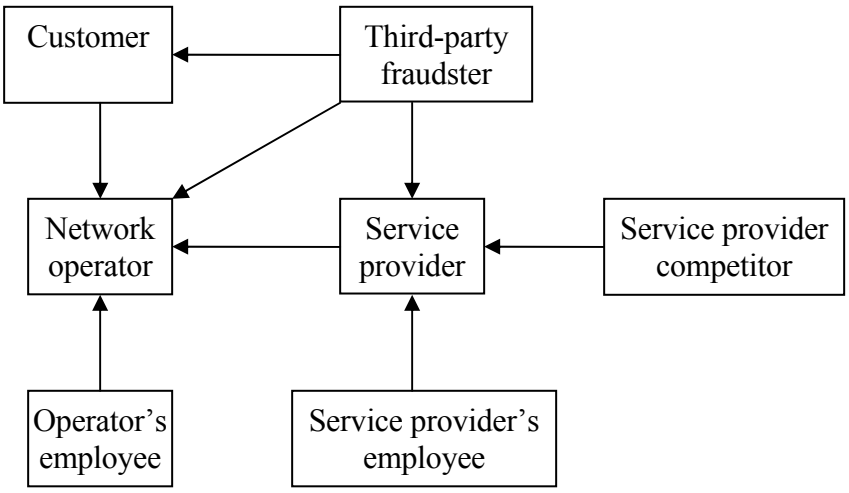

Figure 4.2: Possible fraud relations between actors in the 'Millionaire' game

These different fraud relations are explained below:

- **Customer against network operator**: The customer might commit fraud to get free access to the quiz or to obtain answers to the questions. This can be achieved through subscription fraud, roaming fraud or with the assistance of an insider.
- **Third-party fraudster against customer**: The fraudster will typically commit identity theft, cloning or handset theft to participate in the game at the expense of a legitimate customer.
- **Third-party fraudster against network operator**: The fraudster commits subscription fraud to get access to the game and to play as much as possible before disappearing.

- **Third-party fraudster against service provider**: A criminal hacks into the service provider database to get answers to the quiz questions.
- **Competitor against service provider**: A competing service provider can launch a denial-of-service attack on the active service provider in order to get all the potential customers.
- **Service provider against network operator**: The service provider sends many fraudulent SMSs, typically using a cloned phone, to increase his revenue share from the operator.
- **Network operator against customer**: The operator can defraud the customer by only selecting very hard questions or by falsely declaring that the customer's answer is incorrect. This is done in order to increase the amount of money deducted from the customer's account.
- **Employee against service provider**: The employee gains access to the questions and their answers, and resells them at a high price.
- **Employee against operator**: The employee provides free or cheap SMSs to friends by manipulating billing processes.

The above fraud scenarios result in hard currency loss for the operator, as the latter needs to pay the user for every correct answer obtained fraudulently. They therefore have a high impact, even when perpetrated on a small scale. The fraud scenarios also show that despite the service provided being new, the actual techniques for committing fraud are not. Criminals simply find new ways to use old fraud types, which again highlights the importance of retaining old fraud detection capabilities in the design of an NGN FMS.

In addition to the actors listed above, new players in the telecommunications industry will be involved through mergers, acquisitions and start-up companies. This will certainly generate new points of security vulnerabilities susceptible to malicious activities.

Some speculations on the evolution of fraud in NGNs are offered in the next section.

4.3 NGN fraud types

This section starts with an analysis of the likely general evolution of fraud in NGNs. It is followed by a presentation of some of the fresh application-specific fraud scenarios that operators are facing in respect of recently launched services that offer some form of network convergence.

4.3.1 General evolution of fraud in NGNs

Predicting the future of fraud in NGNs accurately is prone to be wrong and virtually not possible. However, some general trends of the future fraud scenarios can be inferred as follows:

Firstly, fraud scenarios are highly dependent on service offerings as well as business models. For this reason various industry experts estimate that, due to the expansion of m-commerce in NGNs, fraud will target service content (the service or the good purchased) rather than connection (the phone call or Internet access), since the value of the content largely exceeds the cost of the connection (Johnson, 2002a). Content fraud will be most probably initially perpetrated by new entrants in the fraud community, while traditional phreakers will keep on illegally obtaining and selling calls.

Secondly, due to the convergent nature of NGNs, it is highly likely that fraud from various communities (financial, Internet, hackers, telecommunications fraudsters) will converge. Therefore the traditionally separate teams of fraud management, risk management, revenue assurance, network security and credit control need to combine their effort to effectively combat fraud (Johnson, 2002a).

Thirdly, due to the ease of spoofing an IP address, identity theft will increase considerably in NGNs. This is already visible from the sudden rise in new email-based fraud attacks such as phishing and pharming (Dunham, 2004).

However, it is worth mentioning that fraud motives and threats remain generally the same throughout the years, even though technology evolves (Abramowicz & Ledberg, 2002). Criminals merely gain more technology know-how and, hence, use new techniques to perpetrate the same basic types of fraud. For example, clip-on fraud, which first emerged in the 1950s (Collins, 1999) still occurs widely nowadays. Thus it can be assumed that although certain new forms of fraud will appear, a large number of the fraud types in NGNs will be just the same as the current ones, with only slight modifications. It is therefore very important not to overlook old fraud issues in NGNs.

Based on the above speculations, some likely application-independent NGN fraud types are shown in alphabetical order in Table 4.1.

Content fraud types (non-traditional)	Excess download
	Illegal redistribution of service
	Overcharging
	Unauthorised access to resources
New fraud type due to convergence	Money laundering
Traditional fraud types	Credit card fraud
	Identity theft
	Insiders abuse
	IP attacks (e.g. malware, DoS, spoofing)
	PRS fraud
	Subscription fraud

Table 4.1. Likely NGN fraud types

The new fraud types (non-traditional) are described in more detail below.

- **Excess download**: A customer manipulates the billing mechanism for the media content in order to download more data than he is entitled to. This is only applicable to services where billing is based on the amount of data downloaded. This fraud, aimed at the service provider, also indirectly affects the content provider (Abramowicz & Ledberg, 2002). Typically, this will be achieved with the assistance of an insider.
- **Illegal redistribution of service**: A legitimate customer downloads multimedia content (e.g. movies) and illegally redistributes it to other individuals. The redistribution can be free of charge or at a low cost. Redistributing media involves breaking the encryption mechanism used to protect the broadcast material. It is almost impossible to detect occurrence of this fraud by using only network indicators, since the fraudster is likely to reproduce and resell the content on a storage device (e.g. CD-ROM, DVD) instead of redistributing it over the network (Horal, 2000).
- **Overcharging**: An actor in the IP business model charges another actor more than was previously agreed upon. For instance, a service provider tries to overcharge a customer by sending him more data than he requested. To avoid being noticed, the fraud will generally be committed as a so-called *salami* attack, i.e. only a very small amount of money is added to each transaction (Abramowicz & Ledberg, 2002). This fraud can thus be considered as a new form of cramming attack, which was explained in the previous chapter.
- **Unauthorised access to resources**: This refers to obtaining free unauthorised access to multimedia resources by bypassing the authentication mechanism. Unauthorised access can

be the result of hacking, social engineering, shoulder surfing or insider's assistance (Abramowicz & Ledberg, 2002). Depending on their value (e.g. newly released movie or live broadcast of a football match), the resources obtained can be resold either for a small or a significant amount.

- **Money laundering**: Criminals might use m-commerce as a means to commit money laundering. One example is that of a criminal who wants to deposit large sums of illegally obtained money in a bank account without raising suspicion. To that end, he and his accomplices anonymously buy merchandise through m-commerce and legally resell the goods. He can then lodge the money in his bank account claiming that it comes from his legitimate commerce (Johnson, 2002b).

4.3.2 Recent technology-dependent NGN fraud types

New forms of fraud have recently emerged due to the penetration of new convergent network technologies. Two of these technologies are of particular interest with regard to telecommunications fraud, namely VoIP for wireline networks and 3G for mobile wireless networks. Wi-Fi has also recently emerged as a technology of choice for fixed wireless networks and, similar to the other two, presents security vulnerabilities that are exploitable for fraud. Table 4.2 lists some of the recently reported scams associated with these network types. These scams give us an idea of what fraud scenarios might look like in fully convergent NGNs.

Wireline networks: VoIP	Mobile wireless networks: 3G	Fixed wireless networks: Wi-Fi
▪ Caller ID spoofing ▪ VoIP-PSTN termination scam	▪ Cross-over fraud	▪ War driving ▪ Evil twin attack

Table 4.2. Some new fraud types on VoIP and 3G networks

Sections 4.3.2.1 to 4.3.2.3 describe the fraud types associated with VoIP, 3G and Wi-Fi networks respectively.

4.3.2.1 VoIP fraud

VoIP inherits IP-inherent security vulnerabilities in addition to being exposed to new threats, due to the convergence of voice and data on IP networks. Currently, VoIP is still an immature technology and so are its associated fraud types. However, the more VoIP solutions are deployed, the more

they may attract attackers, increasing the risk for harm from Internet attacks. The following is a description of some of the new types of fraud perpetrated over VoIP networks.

Caller ID spoofing

Caller ID spoofing refers to changing the calling number that appears on the call display of the receiving end. This is used to make it appear as if calls originate from a different number, chosen by the caller. Several web sites, such as Spooftel.com, Telespoof.com and Camophone.com, offer this service for free or at low costs (BBCNews, 2005). Caller ID spoofing was initially designed for debt collectors, private investigators and law enforcement agencies in order to entice people into answering the phone. However, criminal use of VoIP caller ID spoofing is increasingly common, often for committing money laundering and phishing (Reuters, 2005).

Caller ID spoofing is used for money laundering in the following way: Criminals use wire-transfer services such as Western Union in the USA to easily transfer illegally obtained funds as an alternative to buying goods and reselling them. Western Union requires its customers to call from their home phone in order to validate money transfer requests. Criminals take advantage of this elementary validation system by forging their calling number in order to make a fraudulent transfer to themselves. The forged number that appears on the Western Union phone actually belongs to the owner of the stolen credit card used to transfer the money. In the case of small amounts, i.e. less than USD 300, Western Union does not call back to verify that the call back number matches the number on the credit card. This enables criminals to eventually transfer large sums of money by making repeated calls (Schuk, 2005).

Criminals also use caller ID spoofing for phishing. This is accomplished as follows: Fraudsters forge the phone number of a trusted financial institution or government agency to which they pretend to belong in order to obtain people's sensitive information such as banking details or ID numbers. This is the phone version of the email-based phishing scam described in the previous chapter (Reuters, 2005).

VoIP-PSTN termination scam

The VoIP-PSTN termination scam targets the settlement principle for calls originating from one operator's network and terminating in another operator's network. According to this agreement, for every call made from operator A's network to operator's B network, operator A must pay a fee to operator B. In this case operator A is the VoIP service provider and operator B is the PSTN

operator. The PSTN operator attempts to defraud the VoIP provider by illegally increasing the number and the duration of calls made to his network. This scam can therefore be considered as a modern form of interconnect fraud. Interconnect fraud was explained in Section 3.3.2 of the previous chapter. In Figure 4.3 the VoIP-PSTN termination settlement is illustrated and the fraud actors are indicated as reported in Schuk (2005).

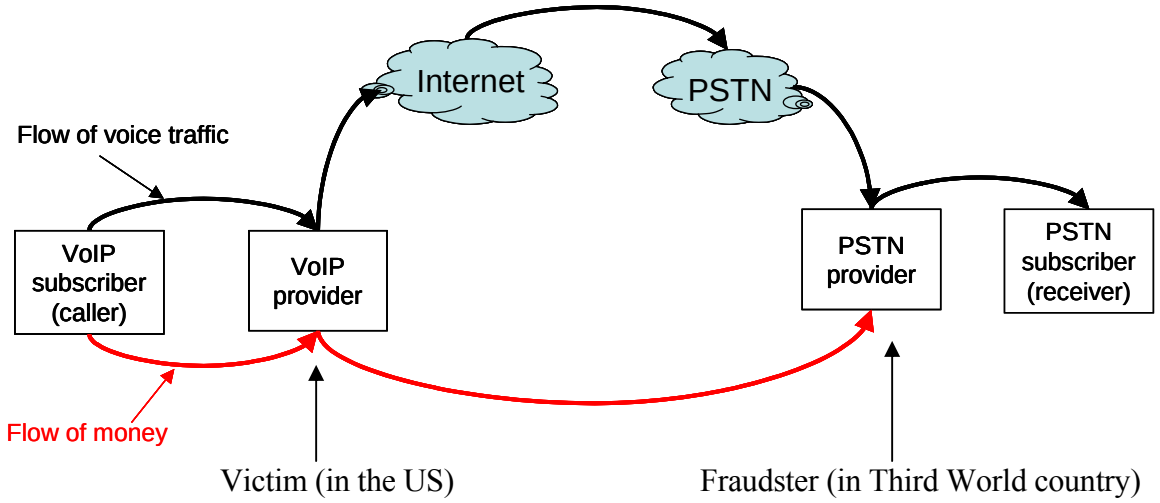

Figure 4.3: VoIP-PSTN termination scam

The above scam works as follows: The fraudster registers as a PSTN provider in a Third World country. In some countries this may simply involve filling out some forms and paying a processing fee. Cases of such scams originating in Afghanistan and Lichtenstein have been reported (Schuk, 2005). Then, the fraudster publishes very high call completion rates (say $1.90 a minute) for a list of customer numbers and creates these virtual numbers. They are nothing but software in some computer, but they actually seem to ring when dialled and they do answer incoming calls. The fraudster then looks for a US-based VoIP provider who does not know about his costly call termination rates and whose call rates are much lower ($.09 a minute). He subscribes to this VoIP provider using a freshly stolen credit card number and creates a list of 'customers' who will make calls. The customers are merely computer programs such as an auto-dialer. The fraudster then places many long duration calls to his own list of numbers via the VoIP provider. At some point in the future, the VoIP provider will receive a huge bill from the 'PSTN provider', while he himself gets paid only a small amount from his customers (the fraudster's computer programs).

One victim, a VoIP provider company called NuFone, lost more than $400,000 through this scam, while another, LiveVoIP, was declared bankrupt (Schuk, 2005). This scam is greatly facilitated by the weak control over the communications systems in some countries. It is also facilitated by the

growth of identify theft, since scammers usually use stolen credit card numbers to sign up contracts with VoIP providers.

4.3.2.2 3G fraud

3G (short for third-generation wireless) is the emerging standard for mobile wireless technology and uses packet-switched technology with an emphasis on broadband data rather than voice services (Hearne, 2004). 3G networks offer greater opportunities for fraud and revenue leakage because they give users access to m-commerce and premium multimedia content. They also generate significantly more volume of data for users' transactions, making fraud detection harder (Hearne, 2004). One of the much feared scams in respect of 3G networks is cross-over fraud, which is described below.

Cross-over fraud

The fraudster, a PRS service provider, sends a Trojan horse to a subscriber. This Trojan horse causes the subscriber's mobile phone to automatically dial the fraudster's own premium rate number. This enables the PRS provider to increase his revenues at the expense of the customers (Hearne, 2004). An example of such a scenario already occurred in Japan. Emails containing malicious embedded java scripts or HTML hyperlinks were sent to mobile phones of I-mode customers of NTT DoCoMo, the Japanese leader in mobile Internet and data. The malicious code caused handsets to dial Japan's emergency number. Other emails caused the phone to freeze or to dial random numbers or numbers found in the user's phone book (Fitchard, 2001).

4.3.2.3 Wi-Fi fraud

Wi-Fi stands for Wireless Fidelity and broadly refers to any type of wireless network based on the IEEE 802.11 standard. It is currently the leading technology for fixed wireless communications (HP, 2005). Wi-Fi offers convenient wireless access to the Internet from fixed access points known as "hot spots" – increasingly common in public places such as airports, hotels and coffee shops. However, because Wi-Fi was not designed to protect against more than casual eavesdropping, it presents many security flaws that can be used with a malicious intent (HP, 2005). Two of the reported security attacks affecting Wi-Fi users are war-driving and the so-called evil twin attack. A description of these scams follows.

War-driving

War-driving is a fairly recent practice that involves driving through an area, equipped with a laptop and possibly an antenna and some special software, searching to discover unprotected Wi-Fi networks. Such software can be downloaded freely from the Internet (Tyler, 2003). War driving is facilitated by the poor security measures taken by Wi-Fi users. Many users, including big private organisations, do not change or even activate the default security settings of their Wi-Fi systems. It is however also true that these security features provide only minimal protection against intrusions. For example, it is a well-known fact that WEP (Wired Equivalent Privacy), the standard encryption algorithm for IEEE 802.11-based networks, can easily be broken (Tyler, 2003).

War-driving is not a crime *per se*, but it can be used to get free access to another person's Internet connection, with the added advantage of almost complete anonymity, as it leaves no trace of the hacker. Any criminal activity perpetrated by the war-driver will then be linked to his victim's Internet account (Associated Press, 2004). In one instance, a man in Southern California, USA, pleaded guilty of using unprotected access points accessed from his car to send unsolicited emails that advertised adult content web sites (Schim, 2004). Other cases of crime involving war-driving have also been reported (Schim, 2004). War-driving enables a hacker to penetrate wireless networks that can then be exploited to access private company information or to commit identity theft.

Evil twin attack

An evil twin attack, also known as access point phishing (AirDefense, 2005), is a new technique devised by identity thieves to get hold of user's personal details. It involves luring Wi-Fi users in a busy public place into connecting to a hacker's Wi-Fi-equipped computer, such as a laptop or PDA (personal digital assistant), by spoofing a legitimate access point (Wickham, 2005). There are many ways in which the hacker can pose as a legitimate hotspot. First he sets his service identifier to be the same as the local hotspot, thus creating the so-called evil twin. Then he could launch a denial-of-service attack against this access point, create interference around it, or send out a stronger radio signal near the wireless client. This forces users to lose their connection to the legitimate hot spot and to unknowingly reconnect to the fake access point (Goldstein, 2005). Once a user connects to this forged hotspot, the computer of the fraudster sends him phony login prompts in order to obtain his user name, password and even his credit card details before redirecting him to the Internet. In sophisticated attacks, the evil twin can redirect the user to fake web pages that look like the legitimate ones the user visits regularly. The fraudster is then able to

see all the information accessed or entered by the user and to track all his activities on the Internet, such as reading an email or filling a web form for registration or login purposes (Biba, 2005). In a freshly reported version of this attack (AirDefense, 2005), after connecting to the evil twin, the user was presented with a mouse-enabled web page that would trigger an automatic downloading of malware, irrespective of where the user clicked on the page.

So far, no large-scale occurrence of this attack has been reported. However, because it is quite easy to perpetrate such a scam, it constitutes a real threat to the Wi-Fi community (Wickham, 2005). This scam also illustrates the evolution of fraud scenarios due to new technology, as the evil twin attack is merely a new form of phishing.

Many of the attacks presented in Section 3 above have not yet been reported on a large scale and some of them, although doable, still belong to the domain of fiction. For this reason, the present dissertation focuses only on three real NGN fraud types that have already been committed in several instances and that are highly likely to greatly increase in fully convergent NGNs due to the growth of m-commerce. Besides, these three usually result in hard currency loss in the business-sharing model of NGN services. They are subscription fraud, unauthorised access to resources and illegal redistribution of services. The three fraud types have also been represented in the fraud relations described in Figure 4.2 in respect of the *Millionaire* game. They will be used to illustrate the benefits of the solutions that are proposed for NGN fraud detection in subsequent chapters.

4.4 Conclusion

New fraud types have been emerging in the latest convergent technologies and more sophisticated ones are likely to appear in fully convergent NGNs. The ease with which these attacks can be performed *and* concealed makes them a big threat to the evolution of the telecommunications industry. Users will be deterred to use the new services and technologies due to the lack of security, and operators and service providers will therefore lose their investment in these new products. In order to find appropriate solutions to these scams, it is important to take note of previous work in the field of NGN fraud detection. Such work is reviewed in the next chapter, which presents a summary of related research previously conducted to fight NGN fraud.

Chapter 5: Review of previous work in NGN fraud management

5.1 Introduction

The area of NGN fraud management has not received much attention to date and there is not an extensive body of literature available on this topic. Although some work has been performed by industry since the year 2000, most results have not been made publicly available due to their sensitive nature. Fortunately, due to the participation of academia in these research projects, some of these results have been published.

A review of these solutions lays the foundation for future development of a suitable FMS for NGNs, which is the main goal of this dissertation. Knowledge about previous work allows us to incorporate and possibly improve in our FMS architecture the solutions suggested by previous researchers. It also facilitates the identification of the areas of fraud detection that have been overlooked and need further investigation. This chapter therefore reviews public reports on NGN fraud management and also contrasts previous work to the approach used in the current research. In this dissertation, the researcher uses requirements for billing systems as the basis for the design of an FMS architecture for NGNs. This approach differs significantly from previous work in this field as little has been done to date to combine the areas of NGN fraud management systems and NGN billing systems.

The chapter is structured as follows: Section 5.2 provides a survey of previous work done in NGN fraud detection, while Section 5.3 conducts a critical analysis of this survey and highlights the major difference between previous research projects and the current project.

5.2 Previous work in NGN fraud detection

Although several research documents on NGN fraud detection are available, they are mostly from or based on the EURESCOM (the European Institute for Research and Strategic Studies in Telecommunications) project P1007 (Eurescom, 2002). Apart from the EURESCOM project, two other projects worth mentioning are the research conducted at the Swedish Royal Institute of Technology (Abramowicz & Ledberg, 2002) and the study at the Waterford Institute of

Technology in Ireland (McGibnet & Hearne, 2004). The EURESCOM project is discussed in Section 5.2.1, while the other two projects are described in Sections 5.2.2 and 5.2.3.

5.2.1 Eurescom project P1007 (2000 – 2002)

The EURESCOM project P1007 (Application of intelligent techniques to telecommunications fraud detection), which was carried out between 2000 and 2002, is currently the most significant contribution to the area of NGN fraud detection. The project involved numerous European telephone companies and the Department of Computer Engineering at Chalmers University of Technology, Sweden, sponsored by Telia AB. Telia AB is the former leading operator in Sweden, and is currently known as TeliaSonera since its merger in December 2002 with Sonera, a former operator in Finland (Budde, 2002). The project focused on the investigation of intelligent techniques for fraud detection in future high-value IP services. It looked at how intelligent techniques from the domains of learning, personalisation and data-mining could improve fraud detection and analysis for new types of fraud. Not surprisingly, the main outcomes of this extensive research involve confidential information and therefore are not publicly accessible. Various public reports and dissertations nevertheless resulted from this project. Dissertations from Chalmers University of Technology are discussed in Section 5.2.1.1 and an independent report from EURESCOM is described in Section 5.2.1.2.

5.2.1.1 Research from Chalmers University of Technology

Chalmers University of Technology in Sweden was an active participant of the EURESCOM project P1007. Master's students from this university published several theses on the subject of IP fraud detection, and below the results of these studies are discussed in chronological order.

5.2.1.1.1 Master's thesis by Mikael Horal (2000)

In his Master's thesis published in 2000, Mikael Horal studied fraud in IP multicast services (e.g. digital television and video), arguing that IP multicast is the best solution for future Internet broadcasting. The thesis examines how fraud can be committed in IP multicast and also how to detect it. This is illustrated by the description and implementation of a software prototype for a post-paid IP multicast audio service, whereby a user logs onto an application server to access MP3 audio data transmitted over an IP network by radio stations. The research determines not only detailed fraud scenarios that may occur on such a service, but also their fraud indicators and uses the software prototype to confirm these results.

However, no FMS architecture or new fraud detection method is proposed. Fraud is detected using traditional threshold-based detection techniques and data is collected for analysis from network sniffers, application servers and routers.

5.2.1.1.2 Dissertation by Cecilia Karlsson (2001)

Another interesting work from the EURESCOM P1007 project is a dissertation by Cecilia Karlsson published in January 2001, which focuses on combining fraud and intrusion detection techniques in a single system for IP-based multimedia services. The logic behind this idea is based on the belief that unlike telephone companies, which are mainly concerned with fraud occurrences, companies offering multimedia services in data networks will probably want to address all types of events that affect their services. They will thus benefit from a combination of IDS (intrusion detection system) and FMS capabilities, instead of having them as separate systems. An IDS is a security system that gathers and analyses information from various areas within a computer or a network to identify possible intrusions. An intrusion is an attempt to gain unauthorized access to a system in order to test its level of security, modify or steal information or render a system to be unreliable or unusable (Arvidson, & Carlbark, 2003).

In order to identify methods for both intrusion and fraud detection for IP multimedia services, Karlsson needed to determine what fraud attempts and intrusions were likely to occur in such services. To this end, she used a commercial multimedia system and investigated how it could be misused for fraud and intrusion attacks. The multimedia system used was Oracle Video Server, which is known today as Thirdspace OVS (SGI, 2002). The outcome of the research was the determination and evaluation of a set of methods capable of efficiently detecting the identified intrusion and fraud scenarios. Identified methods are Predictive Patterns Generation, Neural Networks, Belief Networks and Decision Networks.

As is the case for Horal's research, Karlsson's report does not propose a new FMS architecture. The suggested fraud detection methods are compared to a set of predefined criteria such as flexibility and false alarm rate based on information gained from research papers. No actual experiment is conducted to test the selected methods and confirm the results of the analysis. However, some suggestions on how to conduct the experiment are provided.

5.2.1.1.3 Thesis of Emilie Lundin (2002)

A year after Karlsson's report presentation, Emilie Lundin published a thesis (Lundin, 2002) under the EURESCOM P1007 project that also suggested the combination of fraud and intrusion detection techniques for future fraud scenarios. However, this suggestion was for all types of emerging telecommunications services, such as online gambling and media-on-demand services. In her thesis, Lundin argues that as more and more telecommunications services are getting computerised, it is pure common sense to integrate an FMS and an IDS into a single system. She also states that since an FMS can be considered as an application-specific IDS, fraud detection systems can and should greatly benefit from intrusion detection technologies, seeing that they were developed and matured well before the public started showing interest in fraud management.

The focus of her thesis was to find aspects of "cross-fertilisation", as Lundin calls it, between intrusion and fraud detection, in other words how advances and solutions in one area can be used to solve problems and improve the other area. The outcome of the research was threefold. Firstly, a method for generating artificial test data for fraud detection was suggested and illustrated to show how it can benefit intrusion detection as well. Secondly, some solutions were proposed to the problem of breach of privacy in anomaly-based intrusion detection, and their use in fraud detection was explained. Thirdly, a survey of research in the intrusion detection area was conducted.

According to Lundin, the goal of her research project goal is not to improve the fraud detection capabilities of existing FMSs. She prefers to focus on combining fraud and intrusion detection functionality to solve other overlooked issues such as invasion of user's privacy and unavailability of quality test data for FMSs. For this reason, Lundin does not propose any fraud detection methods or any FMS architecture.

5.2.1.2 Study by EURESCOM (2002)

Also in 2002, another study (Biscaia, 2002) from the EURESCOM project investigated the Emerging Pattern Detection (EPD) area, an innovative intelligent detection method for IP fraud. Not many details are known about this technique, but basically the algorithm works as follows: The fraud detection engine is presented with two data sets, one without fraud and another one supposedly containing fraudulent records. It then compares the two data sets in order to identify patterns recurring in the second data set but which are not present in the first data set. The goal of this algorithm is to detect new forms of fraud.

Results from the study were encouraging as they proved that the number of detected fraud cases could be improved by combining the EPD with more traditional fraud detection techniques. However, one possible drawback of this solution is that the user must know or at least assume that fraud exists in one data set prior to the investigation. This implies that some knowledge about the new fraud scenarios already exists.

Two other research projects that were not sponsored by EURESCOM will next be reviewed below. They are the thesis prepared by Abramowicz and Ledberg in 2002 and Hearne's dissertation completed in 2004.

5.2.2 Master's thesis by David Abramovicz and Per Ledberg (2002)

The Master's thesis by David Abramowicz and Per Ledberg from the Swedish Royal Institute of Technology (Abramowicz & Ledberg, 2002) investigates the fraud types that are likely to prevail in IP networks and whether FMSs are as much needed for data networks as they are for voice networks. The research was sponsored by Visual Wireless, a Sweden-based revenue assurance company that develops and sells an FMS called VCDR (short for Visual CDR).

Abramowicz and Ledberg identified a set of likely IP fraud types, including denial-of-service, excess download and illegal redistribution of service, and tested the efficiency of VCDR in detecting these fraud scenarios. The experiment used IP data as input to VCDR. The IP data was acquired by setting up a virtual video-on-demand service using the free evaluation version of Real Network's Video-on-demand server (RealNetworks.com, 2006). Employees of Visual Wireless were then asked by the researchers to temporarily use this service. Three other systems were also included in the experiment to make the IP service more realistic. They are the following:

- Version 1.8.7 of an open source IDS called Snort (Snort.org, 2006), used to monitor the network traffic around the server.
- Version 1.3.20 of the Apache web server (Apache, 2006), to allow user's access to the service through a web interface.
- MySQL database (MySQL, 2006), used as a billing database.

Results of the experiment concluded that fraud would be a huge problem in IP networks and that VCDR and similar products would require various improvements mainly in the area of input data collection to cater for the future fraud types. Abramowicz and Ledberg therefore proposed a list of

commercial products that could assist VCDR in the aggregation of IP data and the identification of IP users, namely NetFlow, NetCounter, XACCT, Switch Port Mapper and URT (Abramowicz & Ledberg, 2002).

However, neither any new fraud detection technique nor any new FMS architecture was proposed. It is worth mentioning that this research extensively used results from the EURESCOM project as the latter was practically the only available source of documentation on IP fraud.

5.2.3 Master's thesis by Sean Hearne (2004)

The other research project on NGN fraud not sponsored by EURESCOM is the Master's thesis by Sean Hearne (Hearne, 2004) at the Waterford Institute of Technology in Ireland. In the thesis that was published in 2004, Hearne addresses the problem of fraud management for emerging converged networks and propose a rule-based FMS capable of analysing data in flexible formats for NGN fraud detection. A high-level architecture as well as a prototype evaluation for the proposed FMS is provided. This work is part of the *Converge* project funded by the Irish Department of Education and Science (Strand III) and Enterprise Ireland's Research Innovation Fund. The *Converge* Project from the Telecommunications Software and Systems Group (TSSG) is concerned with quality of service, security and accounting in convergent IP networks. It was planned to run from 2001 to 2004.

The architecture proposed by Hearne does not present any novelty, except for the fact that the rule engine of the system contains rules specific to each service offered. The obvious disadvantage of this approach is that knowledge about the fraud type is needed to be able to define appropriate rules. Thus it does not allow the detection of unknown fraud types.

5.3 Critical assessment of previous work in NGN fraud management

One commonality of many of the above-mentioned projects is the importance of incorporating the functionality of an IDS into the fraud detection process for NGNs. The previous researchers all have different reasons for this suggestion, but it can be argued that since NGNs can be accessed from different mechanisms, the effective detection of fraud necessitates the comparison of all network traffic, as explained in Chapter 2. Thus, using information generated by an IDS is a good mechanism to have a broad view of all traffic flowing through the network.

It is also clear from all the above projects that although some work has been done regarding FMSs for NGNs, research mostly focused on the detection engine of the FMS. All these projects are limited to identifying NGN fraud types and determining appropriate techniques to recognise them. The earlier researchers do not propose a new FMS architecture to address the lack of flexibility of existing FMSs. Besides, these projects do not take into consideration the changes that are required of the billing systems processes when designing a solution for NGN fraud detection. This fact is somewhat surprising, as the billing systems constitute the main source of input data for FMSs. Modification of the billing systems to accommodate the new charging models of NGN services will certainly have an impact on the FMS. However, some of the surveyed reports do mention that the selected billing model has a definite impact on the fraud types encountered and therefore on the fraud detection techniques.

For instance, Karlsson (2001) clearly states in her thesis that since an FMS is mainly fed by billing data, different charging models for multimedia services will result in different fraud methods. She gives some examples of various charging models and their associated fraud cases. She also mentions the problem of the non-existence of a standard for billing records of IP-based services and how this may impact on the efficiency of the FMS, but she clearly states that solving these issues is beyond the scope of her work. In fact, she states that her work is based on the assumption that an appropriate billing structure is already in place before proceeding to fraud management for IP multimedia services. Nevertheless, she very briefly refers to the existence of ongoing work from a standardisation body called IPDR.org to solve the IP billing issues.

Abramovicz and Ledberg (2002) also mention IPDR.org's ongoing work of defining IP billing standards. The standard mentioned is called IPDR or Internet Protocol Detail Record. Abramowicz and Ledberg's dissertation is the first research document that actually expressly refers to IPDR as a viable solution for IP billing and that provides results of using this record format in an FMS prototype for IP networks. However – the IPDR standard is used for billing record format only, and no mention is made of its possible usage in the billing process.

Similarly, Hearne (2004) uses billing records in IPDR format in his FMS prototype, but does not comment on the required changes of the billing system.

It is worth mentioning at this point that at the time these papers were published, the IPDR standard was not widely known and this probably influenced its low usage for NGN billing systems. However, it is clear that the billing model has a direct impact on the FMS capabilities. It therefore constitutes the foundation of the current dissertation and aspects of combining NGN billing systems requirements into the design of an NGN FMS are investigated in detail. The current dissertation also uses the following results from the earlier completed research projects due to their relevance for the project goal:

- Incorporating the functionality of an IDS into the FMS architecture.
- Hearne's suggestion of having service-specific fraud detection modules.
- Further investigation of the work of IPDR.org and the IPDR standard.

5.4 Conclusion

A review of previous research in fraud management for NGNs reveals two important requirements for effective fraud detection: combining IDS and FMS functionality, and considering the impact of the billing process in the design of the FMS architecture. The latter requirement is at the core of this research project and constitutes the topic of the next chapter. Chapter 6 determines the limitations of current billing systems with regard to NGN services and identifies some requirements to overcome these limitations.

Chapter 6: Billing systems: overview and NGN requirements

6.1 Introduction

The provisioning of new NGN services involves many more revenue-sharing operators and necessitates changes to traditional billing models. This implies some modifications to legacy billing systems. As billing systems are the main source of input data for FMSs, determining the required qualities of NGN billing systems is the first step in this research project towards the design of an NGN FMS. Indeed, the FMS can be only as good as the billing records that were used as input data. If these records contain incorrect information or are received by the FMS long after being generated, the end result will be incorrect or outdated fraud detection. For this reason, the suitability for NGNs of both current billing records contents (determined by billing standards) and billing processes needs to be analysed.

This chapter examines the limitations of current billing systems and billing standards with regard to NGN services. It subsequently determines the impact of these limitations on fraud detection for NGNs and identifies necessary changes of billing processes to overcome these obstacles.

The structure of Chapter 6 is as follows. Section 6.2 describes a typical billing system and presents its shortcomings in relation to NGN fraud detection. These shortcomings are used to establish NGN billing requirements in Section 6.3. Section 6.4 explains how currently used billing standards are a limiting factor to the identified requirements and proceeds to motivate the adoption of a unified standard for NGN billing.

6.2 Description of a typical billing system

The identification of requirements for NGN billing systems first necessitates a thorough understanding of standard billing processes. It also requires the analysis of the impact of NGNs on these processes. This section therefore begins with a definition of a billing system. This is followed by the description of a typical billing system as currently deployed in the telecommunications industry and an analysis of the limitations of such a system in relation to NGNs.

6.2.1 Definition of a billing system

The American National Telecommunications and Information Administration defines a billing system as a "system that tracks customer usage of services, and calculates the impact on a customer's account, based on the price of the services" (NTIA, 2004). This definition is adopted throughout this dissertation. The billing system produces information about financial transactions that help determine the level of productivity and profitability of a company. In the traditional telephony industry this information is usually called CDR (Call Detail Record), but a more general term used to accommodate recent non-voice services is UDR (Usage Detail Record) (Amat, 2003).

6.2.2 The billing process

In Figure 6.1, the author illustrates a standard billing process and its connection to the FMS.

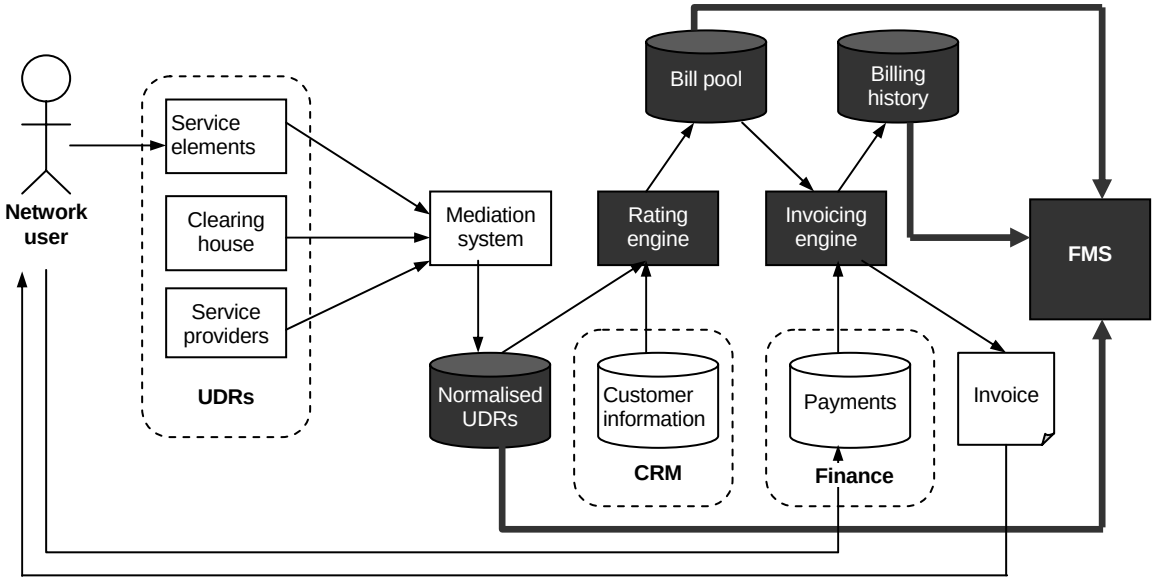

Figure 6.1: Standard billing process

Except for the FMS, shaded blocks in Figure 6.1 represent components of the billing system whereas the unshaded blocks are entities that do not belong to the billing system although they are used during the billing process. The billing process basically consists of three phases – mediation, rating and invoicing (IEC, 2004c) – which are described in the following sections as explained in Ofrane & Harte (2003).

6.2.2.1 Mediation

Figure 6.1 shows that as the customer makes use of the network services, the corresponding network service elements such as telephone switches, routers or gateways record his activities and create UDRs on completion of his network usage. Other UDRs can also be produced by a

clearinghouse or a third-party service provider for settlement purposes. Since each of these sources produces UDRs in a different proprietary format, the UDRs need to be converted into the billing system's internal format before they can be rated. The UDR format conversion, called normalisation, is done by a mediation system. The mediation system first gathers the raw UDRs – not properly formatted and not rated – and checks their validity. This involves checking for various errors such as duplicate UDRs or missing details in the records. Invalid UDRs are sent to an error file for processing. The mediation system then normalises the valid UDRs, consolidates related UDRs and stores them in a database.

6.2.2.2 Rating

Rating lies at the core of the billing system. It is the calculation of the charges for a service usage. Normalised UDRs are sent to the rating engine either periodically or after an event has been triggered (e.g. a certain volume of UDRs has been reached). They can also be sent following a request from the billing system. The rating engine matches identification information in the UDR, such as the calling number, to a user account in the customer database of the CRM (Customer Relationship Management system). Initial service charges for each UDR can then be calculated based on the rating plan of the user and various parameters (e.g. distance, time of day, day of the week). The rating engine subsequently stores the rated UDRs in a bill pool until the next billing cycle, which usually occurs once a month (Ofrane & Harte, 2003, p.9). In case the user is not identified as part of the network's customer database, the UDR is transmitted to his home operator to be billed.

6.2.2.3 Invoicing

When the next billing cycle is run, UDRs are transferred from the bill pool to the invoicing engine. Note that billing cycles differ from one group of customers to another. This avoids overloading the billing system since not all customers are billed at the same time (Ofrane & Harte, 2003, p.22). The invoicing engine adds to the rated UDRs recurring charges such as monthly maintenance fees, in addition to any promotions, discounts and taxes corresponding to the customer account. Next, the invoicing engine produces an invoice that is sent to the customer. Finally invoice details along with received payments information from the financial system are archived in the billing history database.

Figure 6.1 also shows that the FMS can collect billing records from three different sources: the database of normalised UDRs in order to monitor users' most recent activity, the bill pool to obtain rating details and the billing history to profile customer past usage behaviour.

6.3 Shortcomings of the standard billing process with regard to NGNs

An analysis of the diagram in Figure 6.1 reveals a number of shortcomings of standard billing processes in relation to NGN fraud detection, namely batch-mode processing, centralised architecture and service specificity. These characteristics directly affect the quality of the rated UDRs in terms of timeliness and content. They therefore have a strong negative impact on the fraud detection process since the rated UDRs are used as input to the FMS. A discussion of each of these limitations follows below.

6.3.1.1 Batch-mode processing

The billing system operates in batch mode and UDRs are stored for some time before periodically being transferred to the FMS. Moreover, UDRs are only generated after completion of a service usage. Consequently fraud, such as call selling, can only be detected a relatively long time after it has been committed. This makes it impossible to stop ongoing fraudulent activity and even more difficult to catch the fraudster (IEC, 2004a). In addition, batch-mode billing does not allow for fraud prevention. The operator cannot determine whether the customer is able to pay for services such as video-on-demand or gaming before granting access to the network, since customer account details are accessed only during the rating phase – thus after the service has been consumed (Lucas, 2004). Batch-mode billing is going to be a bigger problem in NGNs due to the potential high value of the new services rendering significantly higher revenue loss due to fraud.

6.3.1.2 Centralised architecture

The billing system has a centralised architecture. This means that all UDRs are processed by only one rating engine (with a single module) and only one invoicing engine. This limits the billing system scalability. Sophisticated NGN services usually necessitate the partnership of several service providers, which will significantly augment the volume of business transactions in NGNs (Lucas, 2004). Conventional billing systems will not be able to support the resulting growing number of UDRs. This could result in more revenue leakage, knowing that operators admit

generally losing between 2% and 5% of their revenue due to lost billing records or incorrect transmissions from service elements to billing systems (Amat, 2003).

6.3.1.3 Service specificity

Although it is not visible from the diagram, billing systems are usually service specific (IEC, 2004c). Introducing a new service usually implies deploying a new billing system. In NGNs, the FMS will therefore need to collect UDRs from a large number of billing systems to accommodate new services. Given that the FMS can retrieve UDRs from three different databases in one billing system, the FMS will have a considerable number of UDR sources for a single customer subscribed to various services. Consolidating these disparate data to create an accurate user profile is likely to be a challenging task. Besides, because of their lack of flexibility, conventional billing systems will not be able to accommodate NGN usage-sensitive and content-based pricing models (IEC, 2004a).

The shortcomings discussed above are used as the basis to identify key requirements of NGN billing systems. These required qualities are determined in the following section.

6.4 Requirements for NGN billing systems

The following four major requirements for NGN billing systems can be inferred from the discussion in Section 6.2.3:

- **Real-time billing** is an imperative for timely fraud detection. It involves authenticating and authorising the user, accounting and rating his network usage, as well as advertising his service charges at the time of service request. In near real-time billing, which is the best many operators have managed so far, these operations are performed very shortly after the usage event, generally within five minutes (Nexus Telecom, 2004). Various industry experts agree that real-time billing is "the only practical solution to the increasing problem of risk management" (Lucas, 2004). Real-time billing may also assist in avoiding bad debt from careless customers by advertising the cost of the services before service delivery (Lucas, 2004). True real-time billing already exists but only for prepaid services (Ofrane & Harte, 2003, p.6).
- High-level of **scalability** is essential to support an ever-increasing number of customers and inter-carrier settlement activities. Besides, due to their highly distributed architecture, IP networks have the potential to significantly increase the volume of usage records generated for a single service (IEC, 2004b).

- **Convergent billing,** in other words the aggregation of the charges for all the different types of services used by one customer onto a single invoice (IEC, 2004a), is a further requirement for effective fraud detection. The aggregated invoice details per customer should be stored in a single billing history database. This will give a unified view of the activities of one customer and facilitate customer profiling.
- High **flexibility** to bill for existing and new services. The rating engine should also be capable to modify rating plans quickly without major interruption to the billing process (Lucas, 2004).

Solutions to address some of these requirements have been proposed and are available today. Since rating constitutes the main process of the billing system, these solutions revolve around the positioning of the rating engine. The following explains some of these suggestions (Lucas, 2004).

- Moving the rating engine out of the billing system and integrating it with the mediation system. A similar approach is to build the rating engine as a stand-alone application, with interfaces to both the mediation system and the billing system. Both these solutions enable real-time rating and upgrades to rating plans without jeopardising the billing flow.
- Embedding rating in separate network systems that interact with the service elements. Implementing rating within the network enables real-time rating at session set-up and provides high availability and scalability of the rating devices.
- Implementing rating as a process on the network device itself (e.g. handset, gaming device, computer). The rating processors communicate with the network at predefined intervals to harmonise and balance information and update rating plans. This solution is particularly beneficial for wireless services as it enables portability of the rating engine and real-time charging. Besides, this approach is highly scalable as each rating processor handles only one subscriber account.

Although these solutions are viable, none of them simultaneously covers all four requirements and none of them can solve the billing system service-specificity problem. Before looking for alternative solutions, a logical step to resolve these issues is the examination of UDRs because they have a direct impact on the effectiveness of the FMS. It is therefore necessary to review current billing standards since they define UDR content and format. This is the topic of the next section.

6.5 The impact of billing standards on NGN billing requirements

This section starts with a definition of a billing standard. It then reviews common billing standards and explains why these standards are a limiting factor to the billing requirements established previously and why they negatively affect fraud management.

6.5.1 Definition of a billing standard

Billing standards specify the measurement, format and transmission methods of UDRs (Ofrane & Harte, p.25). They are defined by various regulation bodies depending on the application type and network environment. UDRs contain details about a service usage, which include the following five essential elements: who (identification of the user), when (start and end times of service usage), what (type of service used), where (UDR source identifier), and why (cause of event recording) (Ipdr.org, 2004a). UDR formats are generally quite static, meaning that only specific service usage attributes can be recorded. Figure 6.2 below shows the basic structure of a raw UDR for a fixed-line phone call.

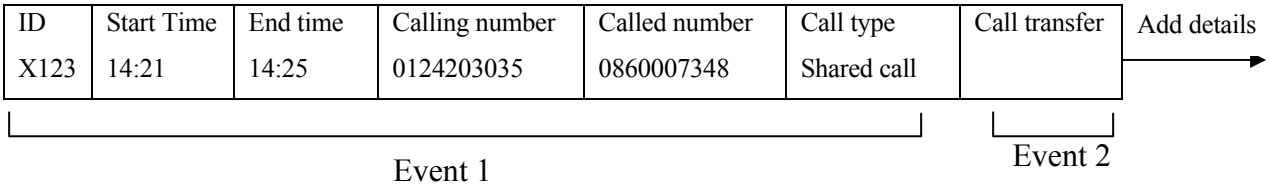

Figure 6.2: Basic structure of a UDR, adapted from Ofrane & Harte (2003, p12)

The UDR starts with an identification number. The recorded call contains two events: a shared call of four minutes and a call transfer. Figure 6.2 shows that the UDR "grows" as more details about the second event become available. The UDR records these two events as separate entities and each of them is rated individually. This explains why billing can be a very lengthy process: each call can have many events and in some cases, each event can generate several UDRs (Ofrane & Harte, 2003, p.13). This also explains why real-time billing is such a challenging task.

Reviewing common billing standards is necessary to select a proper UDR format and transmission protocol to help satisfy NGN billing requirements.

6.5.2 Commonly used billing standards

Many proprietary billing standards are currently in use and all of them are application-specific. Due to the regular introduction of new services, billing standards are frequently revised. This implies

that companies often use many different billing standards and several versions of one standard. For this reason, clearinghouses often act as translators between various billing standard formats (Ofrane & Harte, 2003, p.25). There are also different billing standards for usage data and for settlement data. Usage data corresponds to billing records generated by an operator's service elements to bill his end-users, while settlement data refers to billing records exchanged between an operator and his partners (Ipdr.org, 2004a). This means that there is no universal format for UDRs and no uniform protocol for UDR transmission.

6.5.2.1 Billing standards for usage data

Traditionally, UDRs were generated by telephone switches using the Automatic Message Accounting (AMA) process developed by the Bell telephone company in the 1940s (Borthick, 2001). UDRs were then formatted using Telcordia Technologies' Billing AMA Format (BAF), which defines a binary-coded decimal format for UDRs (Borthick, 2001). BAF is still in use today, especially in North America, but its implementation varies from one switch manufacturer to the next (Ofrane & Harte, 2003, p.10). Some recent variations of the BAF include the ACDR, which is an ASCII AMA format, and the XCDR, which is an XML AMA format (OIF, 2002). Other service elements such as softswitches generally produce UDRs in comma-delimited format or in table format (OIF, 2002).

6.5.2.2 Billing standards for settlement data

A multitude of billing standards for transmitting UDRs are also in use. The following are examples of such standards:

- EMI (Exchange Message Interface), used to support customer billing and exchange messages between operators and billing companies. It is defined by the Ordering and Billing Forum committee of ATIS (Alliance for Telecommunications Industry Solutions) (ATIS, 2004). EMI records are generated from UDRs in BAF format (Borthick, 2001). The billing records can be exchanged electronically, by magnetic tape or CD ROM (Ofrane & Harte, 2003, p.26).
- CIBER (Carrier Inter-Exchange Billing Exchange Record), defined by CiberNet, a division of CTIA (Cellular Telecommunications Industry Associations) for inter-carrier roaming between wireless telephone systems (Cibernet, 2006). There exist ten types of CIBER records to transmit different sets of charges. For instance, a type 10 record is used to uniquely transmit air charges, while a type 20 record is used for sending both air and toll charges (Cibernet, 2006). Figure 6.3 shows some of the parameters of a CIBER record.

- MXP (Mobile Xchange Protocol), also defined by CiberNet to bill for wireless non-voice services, such as m-commerce, messaging, and data exchange (Ponnavaikko *et al*, 2002). MXP focuses on wholesale billing between revenue-sharing wireless operators and content providers. It therefore has a wide set of validation rules to verify the identity of a third-party wireless operator and to reject incorrectly formatted billing records. The standard comprises three record types for usage data, settlement data and rejects. MXP supports various units of measure for duration, volume and content. The records can be exchanged in near real-time or in batch mode and are defined in XML format (Schwartz, 2003).
- TAP (Transferred Accounting Procedure), defined by the GSM Association to exchange roaming billing information in GSM systems. Many versions of TAP are currently in use: TAP II, TAP II+, NAIG TAP II and TAP 3. In addition to the basic subscriber and network identification parameters, TAP records also cater for exchange rates between different currencies because GSM systems are deployed globally (Gullstrand, 2005).
- OSP (Open Settlement Protocol) defined by ETSI (European Telecommunications Standards Institute) for the exchange of charging data between IP telephony operators. OSP also specifies mechanisms to exchange information for interdomain pricing, routing and authorisation (Borthick, 2001). OSP records follow the MIME (Multipurpose Internet Mail Extensions) specifications, which produce messages in XML format. MIME specifies "mechanisms to combine individual components of arbritray format (e.g. text, graphics, audio information, binary data) into a single message". OSP usage records include a source and a destination IP address (ETSI, 2000).

These various proprietary and application-dependent billing standards are a limiting factor to the effectiveness of conventional billing systems for NGNs. They prevent billing systems from meeting the four requirements determined previously. This is further explained in the following section.

Home Carrier SID/BID	Caller ID
MIN/IMSI	Called number
ESN/IMEI	Time zone indicator
Serving carrier SID/BID	Air connect time
Total charges and taxes	Air chargeable time
Total local tax	Air rate period
Call date	Toll connect time
Call direction	Toll chargeable time
Call completion indicator	Toll carrier ID
Call termination indicator	Toll rate class

Note
SID/BID: System ID/Billing ID

MIN/IMSI: Mobile Identification Number/International Mobile Subscriber Identity

ESN/IMEI: Electronic Serial Number/ International Mobile Equipment Number

Figure 6.3: Sample fields of a CIBER record, adapted from Ofrane & Harte (2003, p.27)

6.5.3 Billing standards as a limiting factor to NGN billing requirements

- **Convergent billing**: UDRs have vendor-specific formats and are exchanged through service-dependent protocols – thus no interoperability is possible between billing systems used for different types of services.
- **Real-time billing**: The time-consuming normalisation process required for UDRs in different formats does not allow for real-time billing.
- **Flexibility**: Due to their static format, UDRs lack flexibility to bill for non-conventional usage attributes (e.g. quality of service or latency) that are likely to describe NGN services and do not permit the introduction of new billing schemes.
- **Scalability**: Various UDR formats have a high level of information density, which decreases the scalability of the billing systems.

In addition to limiting the effectiveness of billing systems, UDR shortcomings increase the fraud risk in NGNs as explained below.

Due to increased competition in the deregulated telecommunications industry, NGN value-added services are launched as quickly as possible. Unfortunately they are often deployed without the proper billing structure in place. Operators therefore try either to adapt their existing inflexible billing systems or to rapidly build service-specific billing systems. This results in costly maintenance, as many billing systems need to interoperate through many interfaces. This disparate

infrastructure severely lacks stability, reliability and security, and these security holes can easily be exploited for fraud (Nexus Telecom, 2004).

In view of the above, it is obvious that the global adoption of a common billing standard is essential for effectively billing NGN services and thus decreasing the fraud risk in NGNs. It can also be argued that a single billing standard will facilitate fraud detection as it allows for real-time billing and convergent billing, which both reduce the time to transmit billing records from the billing system to the FMS.

6.6 Conclusion

Traditional billing systems suffer from many limitations that make them unsuitable for NGNs and increase the challenge of effectively detecting NGN fraud. Various modifications are required from these systems in order to cater for the new services and associated charging schemes offered in NGNs. Current billing systems cannot satisfy the identified requirements fully because the formats of their CDRs lack flexibility to bill for new service usage attributes and do not allow interoperability between vendors due their proprietary layout. This severely limits the effectiveness of the fraud detection process and indirectly increases the probability of fraud occurrences in NGNs. Therefore, in order to satisfy NGN billing requirements, a flexible service and network-independent UDR format is needed. This implies the universal adoption of one billing standard for all types of NGN services. The author has selected IPDR (Internet Protocol Detail Record) as such a standard. An overview of the IPDR standard is provided in the next chapter.

Chapter 7: Using the IPDR standard for NGN billing and fraud detection

7.1 Introduction

This chapter presents the IPDR standard as a contribution to the process of finding solutions to the problem of fraud detection in NGNs. The IPDR standard is used to address the four requirements for NGN billing systems that are identified as a prerequisite for effectively detecting fraud in NGNs. These requirements that were established in the previous chapter – namely real-time billing, convergent billing, scalability and flexibility – help overcome the limitations of current billing systems with regard to NGN services. As billing records are the main input data for FMSs, the quality of the output of the FMS is a reflection of the quality of the billing records. For this reason, improving NGN billing processes will also improve NGN fraud detection. The four requirements consequently constitute the starting point in the design of the NGN FMS architecture proposed in this dissertation.

In the previous chapter it was demonstrated that these requirements can only be fully achieved with the usage of a single billing standard for all types of NGN services. The IPDR has been selected as the preferred standard for such a purpose for various reasons discussed in this chapter. This chapter also demonstrates how using IPDR for NGN billing positively affects the detection of NGN fraud.

The chapter is structured as follows. Section 7.2 gives background information on IPDR and on its regulation body. Background information on this organisation is necessary to establish the credibility of the standard. Section 7.3 provides a detailed description of the IPDR standard, and Section 7.4 demonstrates how IPDR can help satisfy NGN billing requirements.

7.2 Background information on IPDR

This section first defines the IPDR standard and then presents its regulation body called IPDR.org.

7.2.1 Definition of the IPDR standard

IPDR is an acronym for Internet Protocol Detail Record. Initially designed for IP-based services, IPDR records – subsequently called IPDRs – are effectively IP UDRs but they can be used to bill for different types of existing as well as new services, whether they are IP-based or not. IPDRs can

be used for all the processing stages of traditional UDRs, from UDR generation to rating and invoicing. They can also be used both for usage data and settlement data, and therefore require few interfaces between different billing systems. The IPDR standard is defined by an organisation called IPDR.org (Heintz, 2002).

7.2.2 Overview of IPDR.org

IPDR.org is a consortium of leading service providers, system integrators and vendors of network equipment, billing systems and mediation systems, established in the United States in 1999. Its objective is to reduce the time and cost of usage measurement and to promote interoperability for the exchange of billing records between telecommunications systems for NGN services. This is achieved through the definition and deployment of open standards for IP-based services (Heintz, 2002). IPDR.org has five working groups, each with its own focus: business requirements, protocol, interoperability, marketing and WLAN (Wireless Local Area Network) accounting and settlement (IPDR.org, 2005b). IPDR.org has more than 20 member companies among which are Cisco, Hewlett-Packard and Motorola. Table 7.1 lists current IPDR.org members (IPDR.org, 2004a).

Charter members	**Supporting members**	**Associate members**
Amdocs	Arris	Active Broadband Networks
Billing Concepts	BigBand Network	DISA
Cisco Systems	CGI-AMS	MetraTech Corp
Hewlett-Packard	Coastal Technologies Group	Primal Solutions
Narus	CSG Systems	
Rogers AT&T Wireless	Infosys Technologies	
Sprint PCS	Motorola	
VeriSign	SBC Technologies	
	Syniverse Technologies	
	TeleStrategies	

Table 7.1. IPDR.org members (IPDR.org, 2004a)

In Table 7.1 members are classified alphabetically according to their category – charter, supporting or associate – with charter members having the highest level of rights and privileges regarding the definition of the standard (IPDR.org, 2004a).

7.3 Description of the IPDR solution

According to the latest version (3.5.0.1) of its "map and overview" document released in November 2004, the IPDR standard is based on four components (Cotton, 2004):

- A reference model that specifies the relationships between the IP network and service elements as well as the support systems.
- Service specifications guidelines to describe usage and settlement data.
- A file encoding format to encode usage information.
- A transport protocol to specify how billing records are exchanged between network systems.

A description of each of these components is provided below. This is followed by an overview of current achievements of IPDR.org to spread the adoption of their standard.

7.3.1 IPDR.org reference model

The IPDR.org reference model is based on the TeleManagement Forum's (TMF) Enhanced Telecommunications Operations Map (eTOM), the most widely used framework for business processes in the telecommunications industry. The IPDR.org reference model extends the NDM (Network Data Management) component of the eTOM. This is why IPDR is often referred to as NDM-U (Network Data Management Usage). The reference model specifies interfaces to exchange IPDR records between IPDR-enabled devices or systems (IPDR.org, 2004c). This model is shown in Figure 7.1.

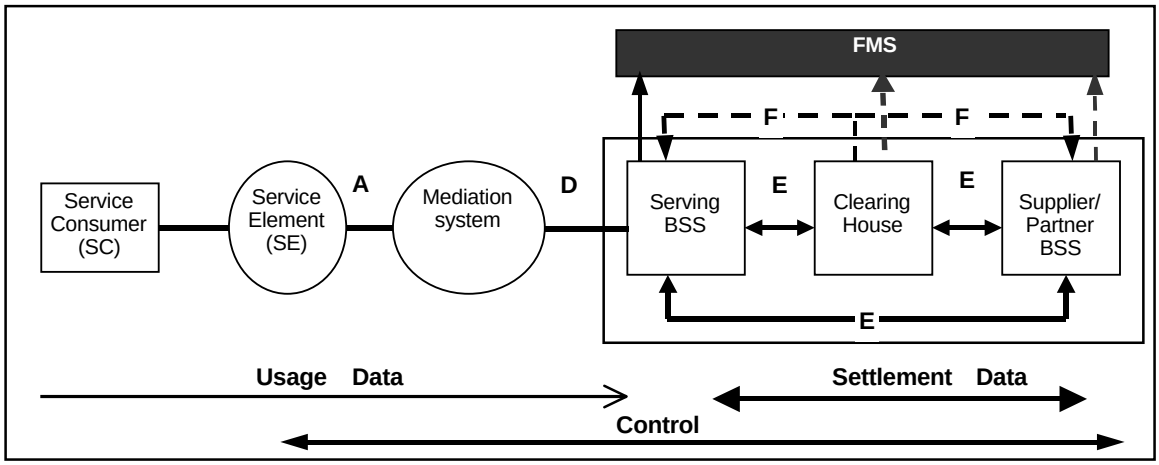

Figure 7.1: IPDR.org reference model, adapted from IPDR.org (2004c)

In Figure 7.1, BSS stands for business support system. A BSS is a system used to support customers, such as a billing system or a customer relationship management system (Lucas, 2005). The model indicates the flow of IPDRs from the service elements to the business support systems of the network operator and of the operator's partners. The model also indicates the key interfaces to exchange IPDRs within a network, namely A, D, E and F. A dash arrow represents a potential information flow, while a contiguous line is a typical exchange path of billing records. The model

serves as a guideline and does not constrain implementations to be exactly as it is depicted in the diagram (IPDR.org, 2004c).

The author has added a separate shaded block (FMS) and its associated arrows to the diagram in Figure 7.1 to illustrate the positioning of one FMS within this model. The FMS spans over the operator's BSSs, the clearinghouse and the third-party suppliers' BSSs, from which it can receive billing records for inspection.

7.3.2 IPDR.org service specifications

Service specifications define the contents and layout of an IPDR for a specific service type. They may be defined by IPDR.org working groups or by independent third parties after approval and review by the relevant committee of IPDR.org.

Every IPDR contains the so-called "5Ws" attributes explained in the previous chapter: who, when, what, where, why. Additional service-specific attributes can be added (e.g. quality of service, bandwidth, and latency). Related IPDRs for a specific time interval are packaged into one IPDR document. A master schema specifies the general structure of an IPDR document and is used as a template for all service-specific IPDR schemas (IPDR.org, 2004c). Figure 7.2 shows a graphical representation of the IPDR master schema.

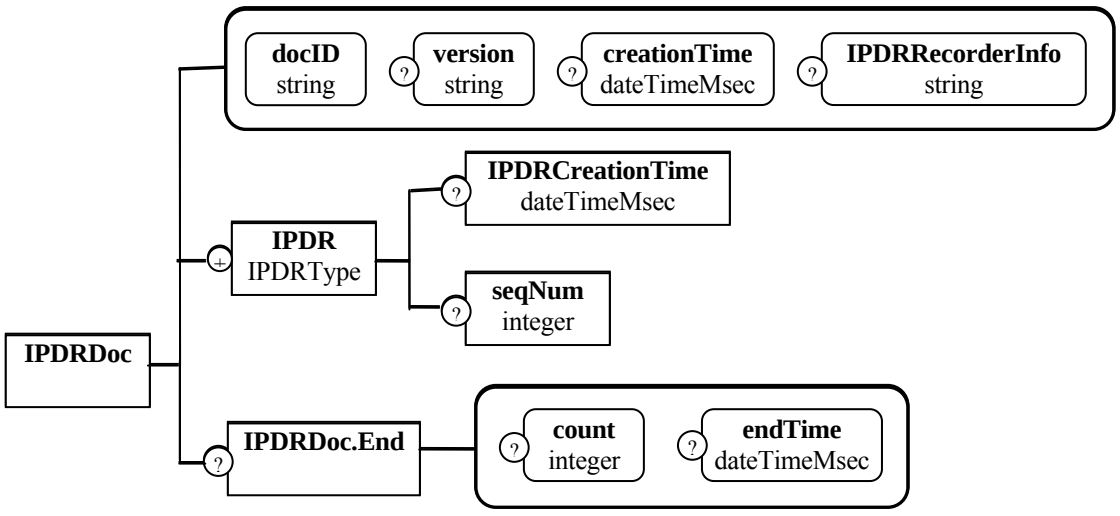

Figure 7.2: IPDR master schema, adapted from IPDR.org (2004d)

Figure 7.2 shows that every IPDR document (IPDRDoc) starts with identification details: a unique identifier, the version of the master schema used in the document, the creation time of the file and information about the network device that recorded the individual IPDRs contained in the

document. Identification details are followed by one or several IPDRs describing the usage of a single service type. They may represent discrete events or parts of a session in progress. Each IPDR includes its creation time and its sequence number in the document. The IPDR document may end with an optional ending block that contains a count of the number of IPDRs stored in the file, followed by the end time of the file generation.

Currently specifications are available for the following services: streaming media (e.g. media on demand); VoIP; Email; ASP (Application service provision); DOCSIS (Data over cable service interface specifications); public WLAN access; content delivery and wholesale bandwidth (Cotton, 2004). These specifications are sufficient to describe currently available IP-based services such as video-on-demand and online gambling, and are flexible enough to represent any new NGN service.

7.3.3 IPDR file encoding format

Two formats are available for encoding IPDR documents: XML and XDR (External Data Representation).

- XML has the advantage of being human-readable and highly flexible. It can be extended to the definition of web services and legacy UDR transmission protocols. However, it suffers from a high level of information density. In Figure 7.3, the researcher shows a simple IPDR record in XML format for an incoming email.
- XDR has been developed to solve the information density issue of XML. It is binary and much more compact and efficient than XML. Conversion between the two formats is easy and straightforward (IPDR.org, 2004b).

Using either XML or XDR does not have an impact on the outcome of this research project, as both formats provide the same usage information required to detect fraud. Thus, the selected IPDR encoding format does not affect the architecture of the NGN FMS proposed later in the dissertation. However, for a possible future implementation of the FMS, both XML and XDR formats are used to encode IPDRs. XML is only used for external visualisation of the billing records, while XDR is the actual internal format used to transfer the records between the billing system and the FMS and to process the records.

```
<?xml version="1.0"?>
<IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr"
xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:schemaLocation="http://www.ipdr.org/namespaces/eMail3.0-A.0.xsd"
docId="g8e0ca84-2222-11b2-85ef-fd66246596bb"
IPDRRecorderInfo ="SNMPServer.myisp.com"
version="3.0-A.0">
<IPDR>
<seqNum>1</seqNum>
<IPDRCreationTime>2005-04-06T02:38:00Z</IPDRCreationTime>
<userLoginName>b60rose </userLoginName>
<userLoginLocation>137.215.41.53</userLoginLocation>
<providerName>Star ISP</providerName>
<providerLocation>212.95.58.66</providerLocation>
<eventType> incoming </eventType>
<size> 14000</size>
<eventTime> 2005-04-06T02:35:00Z </eventTime>
<emailSubject> ICSA meeting </emailSubject>
<emailOriginator> bella@tuks.co.za</emailOriginator>
</IPDR>
</IPDRDoc>
```

Figure 7.3: Instance IPDR document for incoming email in XML format

7.3.4 IPDR transport protocol

Two mechanisms exist for transmitting IPDRs: file-based transport protocol and streaming protocol. They are briefly described below.

7.3.4.1 File-based transport protocol

The file-based transport protocol is a batch-mode mechanism for transferring IPDRs. Its specifications make provision for the following three models of IPDR transmission (IPDR.org, 2004d):

- IPDR Transmitter Push, whereby the IPDR generators, i.e. either the service elements or the mediation system, deliver IPDR documents to a business support system (BSS).
- BSS Pull, where the business support system requests the IPDR documents from the IPDR generators.
- Demand poll, which is a combination of the previous two mechanisms. The IPDR generators inform the BSS of the availability of the IPDR documents and the BSS is then responsible for fetching them.

However, only the Pull model is described in the current standard specifications. In the Pull model, the IPDR generator allocates IPDR documents to one or more groups, depending on the local network policy. For instance, groups can be created based on service type or customer name. This makes it easy for the relevant system to retrieve only specific IPDR documents. Information about groups and group allocation policy is stored in a capability file. Each group is managed by a control file, which keeps track of all the IPDR documents placed in the group. The control file contains the

name and the location of each IPDR document. Control files are changed periodically, based on the network "aging" policy, which is usually time dependent (e.g. every hour or every day). Old control files and their associated documents are therefore deleted on a regular basis. This allows the relevant system to only pull the most recent IPDR documents. This is accomplished by either copying or ftp-ing IPDR documents from a group. Naming conventions for the groups, the control files and the capability files are specified in the IPDR standard (IPDR.org, 2004d).

Due to its batch mode process, the file-based transport protocol is not used in the NGN FMS design but rather the streaming protocol, as explained next.

7.3.4.2 Streaming protocol

Contrary to the file-based protocol, the streaming protocol operates in real-time and provides a fast and reliable mechanism to send IPDRs. It is primarily designed for time-critical service elements such as softswitches, VoIP gateways, firewalls, web servers, content delivery servers, application servers, game servers and location-based wireless services (Cotton, 2006).

The streaming protocol is based on template negotiation between the IPDR exporter (the service elements) and the IPDR collector (the mediation or billing system). A template defines "the structure of a data message payload by describing the data type, meaning, and location of the fields in the payload". It is an ordered list of identifiers of service attributes referencing a service specification document. Template negotiation enables the collector to know how to process the received data records. This allows a reduction of the amount of bandwidth required to transmit records, as attributes are sent without their descriptors. Besides, fields in the template can be disabled so that only required attributes are sent based on prior agreement between the collector and the receiver (Cotton, 2006).

Basically, the exporter informs the collector of its template set through user configuration prior to the delivery of accounting records. Template negotiation may then occur, whereby the collector and the receiver negotiate a set of fields to be sent. All streaming records are XDR-encoded, which further reduces the volume of the data sent (Cotton, 2006).

In this study, the streaming protocol is preferred as it operates in real-time. It thus addresses the problem of time delay experienced with current batch-mode billing processes.

7.3.5 IPDR.org current achievements

Already 14 leading billing and mediation systems vendors, including Marconi, Cisco and Hewlett-Packard (IPDR.org, 2005a) have implemented the IPDR standard specifications, using either version 3.1 (in 2002) or version 3.5.0.1 (in 2005). IPDR-compliant products have therefore been successfully sold worldwide for years. However the only services that have been tested by IPDR-compliant vendors are streaming media, VoIP (mainly), WAP and DOCSIS. Both XML and XDR encoding/decoding have been implemented and both the file transport protocol and the streaming protocol have been deployed (IPDR.org, 2005a). Specifications for both the usage data (D interface) and settlement data (E interface) are available. An open-source reference library for reading and writing IPDRs is provided in C and Java (Heintz, 2002).

Table 7.2 shows some IPDR compliant vendors, their products and customers. Vendors have been classified according to their products type – mediation or billing systems. IPDR.org refers to mediation systems as IPD producers and to billing systems as IPDR consumers (IPDR.org, 2005a).

PRODUCER: mediation system		
COMPANY	PRODUCTS	CUSTOMERS
DIGITAL ROUTE	MediationZone™ 3.0	Meteor (Ireland) Cerebrus Solutions (UK) Tunisiana (Tunisia)
CONSUMER: billing system		
CSG SYSTEMS	CSG Kenan®/BP	Bharti Televentures (India) Telemobil Romania (Romania) British Telecom (UK)
PRODUCER/CONSUMER		
CONVERGYS	Mediation Manager Geneva	EINSTEINet (Germany) Telenor Mobil (Norway) Arsenal Digital (US)

Table 7.2. Some IPDR-compliant vendors and their customers

Table 7.2 illustrates how IPDR-compliant products are deployed globally from Europe to America, Asia and Africa.

In addition, IPDR.org has established some partnerships with standardisation bodies including the following:

- ITU-T, the standard body of the International Telecommunications Union. In 2002 it formally approved IPDR.org as a recognised institution for cooperation and exchange of information (Denis *et al.*, 2002).
- Wi-Fi Alliance, the international organisation that certifies interoperability of WLAN products based on IEEE 802.11 specification. A formal partnership was signed in December 2003 to enable inter-operator settlement for "universal single-bill access to public WLAN hotspots" (Jenkinson, 2003).
- In August 2002 ATIS created a working group to define mapping of the IPDR service specifications to the EMI format (IPDR.org, 2002), and to develop standardised transport protocols and record format for billing and settlement of VoIP services in October 2004 (Gessner, 2004).
- CableLabs, the research and development consortium for cable telecommunications technologies, included IPDR Streaming Protocol as a mandatory element in their DOCSIS 2.0 in January 2005. DOCSIS describes the interface specification adopted by the international digital cable industry (Jenkinson, 2005a).
- TeleManagement Forum. Collaboration was established in November 2005 to address interoperable provisioning and billing for IP television services (Jenkinson, 2005b).

It is clear from the above analysis that the IPDR standard is a promising solution for NGN services billing. It provides specifications for most IP services that are currently available and the service definition can easily be extended for new services. Besides, various leading standardisation organisations have joined IPDR.org and many telecommunications companies worldwide have adopted the standard.

The features of the IPDR standard that are directly relevant for this research project can be summarised as follows: IPDR is flexible enough to define *any* type of service; it offers the possibility of transferring billing records in real-time; and its XDR encoding format is very compact – which facilitates scalability of the billing system. These benefits make IPDR the standard of choice for NGN billing. The next section further discusses these benefits and illustrates to what extent IPDR can help meet NGN billing requirements and assist in NGN fraud detection.

7.4 Using IPDR for NGN billing and fraud detection

This section starts with a demonstration on the effectiveness of the IPDR standard with regard to NGN billing and then illustrates the positive impact of the standard on fraud detection.

7.4.1 Using IPDR for NGN billing

Based on the above description of IPDR, it can be inferred that this standard can help satisfy the NGN billing requirements identified in the preceding chapter in the following way:

- **Convergent billing**: IPDRs stop vendor-format dependency and reduce interfaces through standardisation. The use of the popular XML language facilitates billing system interoperability. It also enables the mapping of the IPDR format to the format of older billing standards. IPDR thus enables the FMS to collect records from different billing systems in the same format. Fully convergent billing provides a single point of source data to the FMS.
- **Real-time billing**: Real-time billing is enabled through the streaming protocol. Besides, IPDRs can be generated periodically while a service is in use and not only for completed usage data. If the service elements generate usage records directly in IPDR format, no normalisation is required, which further reduces delays in the billing process and enables the billing records to be analysed by the FMS in real-time.
- **Flexibility**: It is possible to represent existing and emerging services, whether IP-based or not. New service usage attributes can be measured and charged for without extra overheads. The new attributes can provide additional fraud indicators for the FMS. Besides, XML tags can be added and removed quickly as service features constantly change in a highly dynamic NGN environment.
- **Scalability**: IPDRs can be represented in a compact XDR format, which enables the billing system to support an increasing number of billing records. This increased scalability also applies to the FMS.

Adopting the IPDR standard can therefore greatly enhance the effectiveness of the billing systems for convergent networks. This improved effectiveness should also be reflected in the fraud detection process for NGNs, which is further explained in the following section.

7.4.2 Using IPDR for NGN fraud detection

This section shows how using billing records in IPDR format can have a positive impact on fraud detection. Three highly likely NGN fraud types are used as examples: subscription fraud,

unauthorised access to resources and illegal redistribution of services. Some of their fraud indicators are listed and a brief demonstration of how IPDRs can help in the detection of these indicators is provided.

- **Subscription fraud**.

Indicators:

1- A high number of expensive services are requested in quick succession.

2- A customer receives unusually large bills although his service usage has not changed.

Correlation between the customer information database and the IPDRs generated in real-time can give a prompt indication of (1) and stop ongoing fraud. By comparing IPDRs from the billing history database to the ones in the bill pool, suspicious activity can be detected quickly in the case of (2).

- **Unauthorised access to resources**.

Indicators:

1- An individual receives resources without corresponding billing records in the billing system.

2- Many costly downloads are performed.

In the case of (1), periodic IPDRs from the service elements will show that the network resources are in use although no record is present in the billing system. This will help investigate fraud quickly before a significant amount of money is lost. In the case of (2), real-time billing increases the chance of quickly detecting fraud.

- **Illegal redistribution of service**.

Indicators:

1- A live event is downloaded at the same time as a significant volume of data is uploaded.

2- Downloaded and uploaded data have the same characteristics.

Real-time billing can allow timely fraud detection for (1). In the case of (2), relevant attributes can be analysed for signs of fraud (e.g. exact same quality of service and network performance metrics for uploaded and downloaded data).

It is clear that if billing records are represented in IPDR format, the probability can be greatly increased of detecting the fraud occurrences mentioned above and catching the fraudster before significant damage has been done.

A common format also enables the easy exchange of usage records between the various business support systems used by the distinct teams of network security, risk management and fraud management. This facilitates collaboration between these separate groups for enhanced fraud detection in NGNs. A unique layout and transmission protocol also assists in the quick exchange of billing records between an operator and his numerous associated service providers in an NGN environment. This facilitates the timely detection and impediment of fraud scenarios that exploit the delay in exchanging settlement data, such as roaming fraud.

Besides, IPDRs can be quickly generated and aggregated at frequent intervals to allow the rapid detection of ubiquitous fraud cases, which are likely to be committed on convergent IP networks.

A possible shortcoming of the IPDR standard is that it is not very specific. It provides a common framework but allows a large margin of freedom on its implementation. This may lead to different implementations of the standard from one operator to the next. It could also jeopardise the expected interoperability between service providers that motivated the creation of the standard in the first place. IPDR.org would thus benefit from more specific guidelines on the actual usage of the standard.

7.5 Conclusion

In this chapter the emerging IPDR standard has been proposed as a solution to the inadequacy of current billing systems for NGN fraud detection. The IPDR solution has been described in detail and the advantages of using IPDR to satisfy the billing requirements determined in Chapter 6 have been evaluated. Some examples have also been provided to illustrate the added benefits of IPDR on NGN fraud detection. It is worth mentioning that IPDR is not a silver bullet for NGN billing systems, but rather a step in the right direction. It needs to be implemented in conjunction with other solutions, such as the propositions mentioned in Section 6.3 of the previous chapter.

As billing records constitute the main source of information for FMSs, selecting an appropriate format and transmission method for NGN billing records was the first step towards achieving the main goal of this research project: designing an FMS suitable for NGNs. The next step is to identify an appropriate fraud detection technique. This will be the main focus of the next chapter, which provides a critical assessment of current fraud detection techniques.

Chapter 8: Fraud detection techniques for the NGN FMS

8.1 Introduction

The collection of properly formatted billing records by the FMS is the first step in the fraud detection process. It therefore constitutes an important issue to be addressed in the design of the NGN FMS architecture proposed later in this dissertation. The second step in the fraud detection process is the inspection of billing records by means of an appropriate technique. This constitutes the topic of this chapter, which provides a critical review of fraud detection methods used in existing commercial FMSs. Techniques deemed most suitable for detecting NGN fraud are then selected based on that review.

The remainder of Chapter 8 is structured as follows. Section 8.2 provides a general overview of fraud detection and explains the different approaches to identify fraud indicators as well as the type of detection errors that may occur. This information provides a basis for classifying existing fraud detection techniques. Section 8.3 reviews the fraud detection techniques that are currently available in commercial FMSs. These techniques are categorised on the basis of the fraud detection approaches described in Section 8.2. Section 8.4 highlights the limitations and advantages of the reviewed techniques in relation to NGN fraud detection, and suitable techniques for detecting NGN fraud cases are subsequently selected.

8.2 Overview of fraud detection

This section reviews various aspects of fraud detection generally used in the examination and selection of fraud detection techniques to suit a specific operator's needs. The fraud detection aspects that are reviewed include fraud indicators (in Section 8.2.1), fraud detection approaches (in Section 8.2.2) and fraud detection errors (in Section 8.2.3). The section focuses on fraud detection approaches as they are used by the researcher to classify existing fraud detection techniques.

8.2.1 Fraud indicators

The detection of telecommunications fraud relies on the analysis of the field values in Call Detail Records (CDRs) to discover suspicious calling patterns indicative of fraud. In addition to usage data, the FMS also uses customer data and billing history data to identify fraud indicators (Horal, 2000). Fraud indicators in traditional telephony are often high-usage related and include the

following as mentioned in Horal (2000), Abramowicz and Ledberg (2002), as well as Hearne (2004):

- High call frequency
- Long duration calls
- Expensive calls (especially when they have a long duration)
- High ratio between outgoing/incoming calls
- Simultaneous or overlapping calls from the same number (e.g. in case of cloning or clip-on fraud)
- Calls to so-called "hot" numbers, that is numbers often associated with fraud (e.g calls to specific destinations).
- Calls to black-listed numbers

These fraud indicators can be detected using either one of the two approaches mentioned in the next section.

8.2.2 Fraud detection approaches

Moreau *et al* (1996) mention the existence of 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. Since existing fraud detection techniques use either absolute analysis or differential analysis, knowledge about these two approaches is important in order to select appropriate fraud detection techniques for NGNs. To this end, classifying fraud detection techniques according to their analysis approach would be beneficial. However, the available literature on fraud detection such as Kou *et al* (2004); Abramowicz and Ledberg (2002); Hearne (2004) and IEC (2004b) does not provide such a classification. All of these papers discuss common techniques for detecting fraud without categorising them.

Moreau *et al* (1996) and IEC (2004b) talk about user profiling, threshold-based analysis, rule-based analysis and neural networks. Hearne (2004) presents the same techniques but refers to profile-based analysis as statistical analysis based on the argument that user profiling is usually performed with statistical tests. Abramowicz and Ledberg (2002) review the same techniques but specify that user profiling can be done with either statistical analysis or neural networks. In Kou *et al* (2004), which provides a survey of fraud detection techniques, visual data mining is mentioned as an

additional method for detecting telecommunications fraud. An application of visual data mining is documented in Cox *et al* (1997), but only as a research prototype. The techniques recurrent in all papers and available in existing FMSs are therefore user profiling, threshold-based analysis, rule-based analysis and neural networks. In Table 8.1 the author proposes a classification of these common techniques based on their analysis approach.

Absolute analysis	Differential analysis
▪ Threshold-based ▪ Rule-based	▪ Profile-based ▪ Neural networks

Table 8.1. Common fraud detection techniques

Both fraud detection approaches try to minimise the number of errors that may occur during the detection process. Potential fraud detection errors are briefly explained in the next section.

8.2.3 Fraud detection errors

Fraud detection errors can be of two kinds: false positives and false negatives. A false positive, also known as a false alarm, 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 (Arvidson & Carlbark, 2003). False alarms generate more workload for the fraud analysts, while false negatives result in revenue loss (Abramowicz & Ledberg, 2002). The latter are therefore usually far more threatening for the operator.

Knowledge about fraud detection errors is used to calculate the success rate of an FMS. The success rate refers to the proportion between the number of correctly detected fraud cases and the number of detection errors. It is an important criterion to consider when selecting a fraud detection method. Differential analysis often produces more detection errors than does absolute analysis, because the exact definition of a fraud pattern is not known in advance. The detection errors are usually false positives generated after a slight but non-fraudulent modification of the normal calling pattern of a user. On the contrary, absolute analysis results in many false negatives when new fraud attacks are committed, since it looks only for known fraud patterns. Many false positives are also generated when the definition of the fraud attack is so generic that it may also include normal behaviour. Absolute and differential analysis techniques listed in Table 8.1 are reviewed in the next section.

8.3 Review of current fraud detection techniques

This section reviews common fraud detection techniques classified in Section 8.2.2 as based on either absolute or differential analysis. Absolute analysis techniques are examined in Section 8.3.1 and differential analysis methods are discussed in Section 8.3.2. In order to illustrate the application of each technique, the author uses the example of the video-on-demand (VoD) service illustrated in Figure 8.1 throughout this section. The example of a VoD service is quite applicable because it is an IP-based service and indicators for some of its related fraud cases were previously described in Chapter 7. For the sake of clarity, these fraud indicators are repeated here. An example of the most suitable fraud detection technique is subsequently provided for each applicable fraud type.

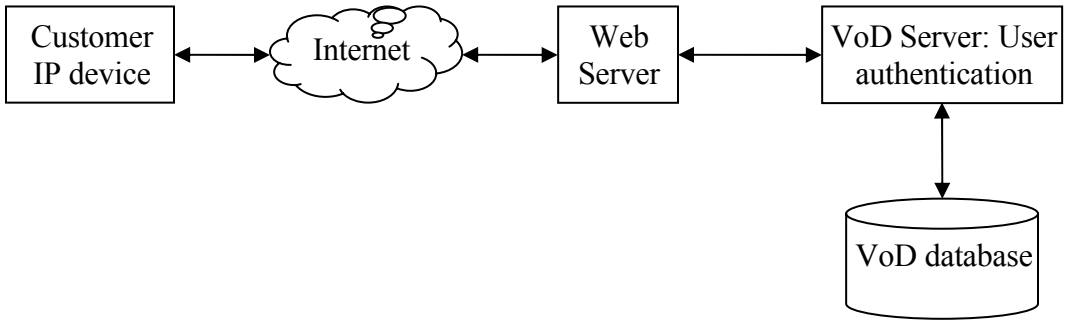

Figure 8.1: Video-on-demand model

The VoD service shown in Figure 8.1 works as follows. The customer connects to the VoD server via the web using his PC or other IP-enabled device. After entering his username and password, he is presented with a list of available videos that he may view. Videos are stored in categories with different associated prices: movies, music videos and live events. The categories also have subcategories such as romantic comedy or drama for the movies category and sport or festival for the live events category. The selected video is then downloaded or broadcasted to the user device where he can view it, as well as pause or rewind. The customer is billed on a post-paid basis. His service usage is recorded for a month and he receives the bill at the end of the month.

Possible fraud types that may occur in this VoD service set-up include subscription fraud, unauthorised access to and illegal redistribution of the videos.

- **Subscription fraud**. Indicators:
  1- A high number of expensive videos are quickly requested (fraudster against operator)
  2- A customer receives unusually large bills although his service usage has not changed (fraudster against customer).

- **Unauthorised access to the videos**. Indicators:
  1- An individual receives videos without corresponding billing records in the billing system.
  2- Many costly video downloads are performed.
- **Illegal redistribution of the videos**. Indicators:
  1- A live event is downloaded at the same time as a significant volume of data is uploaded.
  2- Downloaded and uploaded data have the same characteristics.

8.3.1 Absolute analysis

The most common techniques used in absolute analysis are threshold-based analysis and rule-based analysis. These are described in Section 8.3.1.1 and in Section 8.3.1.2 respectively.

8.3.1.1 Threshold-based analysis

8.3.1.1.1 Overview of threshold-based analysis

In threshold-based fraud detection, a sequence of call records is compared to fixed predefined thresholds. If details about the calls (e.g. call duration) exceed (or sometimes go below) the thresholds, an alarm is generated (IEC, 2004b).

Threshold-based fraud detection is based on the idea that most fraud losses result from revenue fraud perpetrated on a large scale. For this reason, thresholds are usually set to high values (IEC, 2004b). For the same reason, the FMS does not inspect individual CDRs, but only a time-based summary of a sequence of CDRs for every account. For instance, statistics such as average call duration and number of calls to specific destinations can be computed for the past hour or day. Account summaries are then periodically compared to the thresholds. When a threshold is exceeded, the account is queued for further analysis based on its priority level (Cahill *et al*, 2002). Parameters used to define account summaries are specified by fraud experts and thresholds can be chosen manually by means of trial and error (Cahill *et al*, 2002).

With reference to the VoD service explained above, threshold-based analysis is most suitable to detect subscription fraud using Indicator 1 as it only requires the detection of high service usage: a high number of expensive services are quickly requested. An example of possible thresholds to detect this fraud case is provided in Figure 8.2.

account_activation_duration < 3 months
Total number of downloaded videos > 100
Total_video_cost > R1000

Figure 8.2: Thresholds to detect subscription fraud on video-on-demand service

8.3.1.1.2 Advantages and disadvantages of threshold-based analysis

Threshold-based fraud detection tools are very popular because the algorithm is very quick, efficient and easy to implement (IEC, 2004b). However, threshold-based fraud analysis unfortunately also has many disadvantages, including the following (IEC, 2004b; Cahill *et al*, 2002):

- Thresholds only work well for detecting the extremes of fraudulent events and thus cannot detect many fraud types. This results in many false negatives for the less severe fraud attacks.
- Thresholds are not generic enough since they must be fine-tuned for every account to avoid generating too many false positives. This fine-tuning may be dependent on various parameters such as the time of day and the type of call, which implies that many different thresholds may be needed for a single account. It may require a high number of interacting thresholds that need to be regularly updated to cater for changing customers' calling patterns.
- Thirdly, as the fraud detection is performed only periodically, it cannot detect or stop ongoing fraud. This delay is worsened by the usually high values of thresholds, which only allow the detection of fraud cases after considerable damage has been done.
- Finally, experienced fraudsters can easily limit their activities to levels below or above known threshold values, thereby largely reducing the possibility of being caught.

8.3.1.2 Rule-based analysis

8.3.1.2.1 Overview of rule-based analysis

Rule-based fraud detection attempts to find a match between the activities of a customer and known fraud patterns stored as rules. Fraud rules or signatures specify characteristics of a specific fraud type. They usually consist of a series of events that indicate fraud when occurring in a predefined timeframe (Abramowicz & Ledberg, 2002). Rule-based fraud detection is an improvement over threshold-based analysis (Cortes & Pregibon, 2001). Unlike threshold-based analysis which uniquely compares a series of CDRs to fixed numeric values, rule-based analysis

allows CDRs to be individually compared to various types of criteria, including numeric thresholds.

Fraud rules are usually written as a set of conditions represented by "if-then statements". All conditions need to be met for the rule to fire (Hearne, 2004). The rules specify which action to take once all the conditions have been satisfied and they are manually written by a fraud expert, based on the analysis of past fraud scenarios. The rules can subsequently be processed by an expert system fed with input data labelled as fraudulent. An expert system is a computer program used to simulate the decision-making process of a human expert in a specialised subject and knowledge about the subject area is stored in the expert system database (Jackson, 1990:3).

With reference to the VoD service mentioned previously, Figure 8.3 shows an example of a fraud rule using Indicator 1 to detect the illegal redistribution of a live video. This rule requires the prior detection by a network element (e.g. a router) of a video upload on the network. Rule-based analysis is appropriate in this case as this indicator (a live event being downloaded at the same time as a significant volume of data is uploaded) contains several characteristics that can be easily modelled as rules (e.g. video type = "Live", downloading time = uploading time). Besides, this indicator does not require many numeric thresholds, which makes the use of threshold-based analysis unsuitable.

```
IF video uploading recorded on network traffic
AND video_type = "Live"
AND uploading IP address = downloading IP address
AND downloading_time = uploading_time
AND uploaded volume > 2 x downloaded volume
THEN alert on likely illegal redistribution of video broadcasting
Process for further investigation
```

Figure 8.3: Fraud rule example to detect the illegal redistribution of a video broadcast

8.3.1.2.2 Advantages and disadvantages of rule-based analysis

Commercial FMSs rely heavily on rule-based fraud detection because the latter generates a fairly low number of false positives. An exact match between the rule and the user's activities must be found for the rule to fire. Rule-based analysis also provides detailed information about the fraud, which makes it very easy for the fraud analyst to respond appropriately to the attack (Hearne, 2004).

Like threshold-based analysis, rule-based analysis has the obvious disadvantage of being unable to detect new fraud attacks. Only those fraud scenarios stored in the rule database can be identified. Moreover, fraud rules can only detect a limited number of fraud types, because many complex fraud scenarios cannot be modelled as if-then expressions. For instance, they cannot detect the unauthorised use of someone else's account, unless the perpetrator exhibits an unusual calling pattern corresponding to a known fraud signature. This inevitably results in a large number of false negatives.

Another problem with rule-based fraud detection is the definition of the attack signatures. As is the case in threshold-based analysis, if the signatures are too narrow an attacker can easily evade the FMS by just slightly modifying the attack pattern. If, instead, the signatures are too generic, it could result in too many false alarms (Arvidson & Carlbark, 2003). This implies that fraud rules must be constantly updated to reflect changes in fraud patterns, which makes rule-based analysis difficult to manage (Kou *et al*, 2004). In addition, rule-based analysis does not allow a high level of scalability, as the performance of the FMS is significantly reduced when more rules are added to the detection engine (IEC, 2004b).

8.3.2 Differential analysis

Differential analysis is also called anomaly detection (Hearne, 2004). It is usually performed with one of the following two techniques: profile-based analysis or neural networks. Both techniques are discussed below.

8.3.2.1 Profile-based analysis

8.3.2.1.1 Overview of profile-based analysis

Profile-based fraud detection assumes that a fraud attack can be detected by observing a deviation from the normal calling behaviour of a customer, which is stored as the customer profile (Debar *et al*, 1999). A customer profile, also called an account signature, specifies expected usage patterns based on the observation of past legitimate calling patterns of that customer. The usage patterns include values such as number of calls, call frequency, call times and days, called destinations and payment methods (Cahill *et al*, 2002). This expected behaviour is compared to the current user activity to identify anomalies. When a significant deviation is observed, the FMS generates an alert and the relevant CDRs are sent to a case management tool for further analysis. In other words,

anything that does not correspond to a previously learned behaviour is considered suspicious (Debar *et al*, 1999).

Various statistical tests can be performed to estimate whether the deviation from the normal account signature is significant enough to be considered fraudulent. According to Stallings (2003:302) they are as follows.

- **Mean and standard deviation**: The mean value and the standard deviation of a parameter are determined after the parameter's examination over a period of time. The current customer behaviour is compared against these values to determine if it falls within a normal range.
- **Multivariate**: This involves the analysis of events to identify normal or abnormal correlations between various variables. For example, service cost should be proportionate to service usage for every customer.
- **Markov process**: The Markov process is a statistical method that determines the probability of transitioning from one state to another. For instance, it can be used to determine the likelihood for one customer to use one command after another, in order to detect fraudulent activities.
- **Time series**: The time series model determines time intervals between events. It can be used to detect suspicious timings between events, such as a very high call frequency.

The following paragraph shows how profile-based analysis can be used to detect subscription fraud (Indicator 2) on the VoD service described earlier. Indicator 2 of subscription fraud requires prior knowledge of the customer usage pattern, making profile-based analysis the most suitable technique to use in this case.

Indicator 2 for subscription fraud is the following: a customer receives unusually large bills although his service usage has not changed. This implies that an unusually high service usage is recorded on the customer's account. This fraud scenario requires a fraudster to first commit identity theft to impersonate a legitimate customer. One way to detect this indicator is to use a time series model that determines the frequency of downloading movies. For instance, if the customer suddenly goes from watching one video a week to ten videos a week, this could indicate that fraud is occurring. Another possibility is to use a Markov process that determines the probability of switching from one video type to another. For example, the customer suddenly switches from relatively old and inexpensive dramas to expensive movie premieres or live events.

8.3.2.1.2 Advantages and disadvantages of profile-based analysis

The main advantage of profile-based fraud detection is that it can detect new forms of fraud attacks by identifying unusual calling patterns. It can even produce information that can be used to define signatures for new types of fraud (Hearne, 2004). In addition, profile-based fraud detection is able to detect a wider range of fraud attacks than rule-based or threshold-based analysis as the fraud scenarios detected through absolute analysis also exhibit a significant deviation from normal usage behaviour. In this sense, it can be argued that absolute analysis is included in differential analysis (Burge *et al*, 1997).

The high false alarm rate is generally cited as the main drawback of profile-based fraud detection, since the FMS needs to learn all possible forms of normal usage behaviour and might well fail to do so. Also, behaviour can change over time, which implies that the system must be regularly updated with the new behaviour profile. Fraud can occur at the very time the FMS is learning the behaviour. This will result in the FMS containing fraudulent behaviour, which is not detected as suspicious (Debar *et al*, 1999). Another problem with profile-based fraud detection is that it cannot provide enough information about an alert. When an absolute analysis method triggers an alert, the signature that detected the event is usually associated with some kind of attack information. In contrast, profile-based analysis can only tell what is not normal and not what caused the attack. This makes the task of the fraud analyst more difficult since he does not know the exact cause of the alarm and therefore does not know how to respond to it (Arvidson & Carlbark, 2003).

8.3.2.2 Neural networks

8.3.2.2.1 Overview of fraud detection using neural networks

Artificial neural networks are a computational method designed to emulate the functioning of the human brain. In the brain, a biological neural network consists of a set of neurons interconnected through synapses. Electrochemical signals are sent to transmit information through the network. Artificial neural networks simulate this process (Cerebrus Solutions, 2002b). In other words, artificial neural networks have the following properties that resemble the human brain (Hearne, 2004):

- They are formed of many interconnected computational units that work in parallel. The network units represent the neurons. Each unit receives some input (the signal), processes it through a mathematical function (called a learning function) and produces an output.

- The units are connected through weighted links organised in specific patterns. The links represent the synapses.

Most neural networks have many layers of connected neurons for increased computational power. Each layer can have a different number of neurons and a different learning function. These details, as well as the number of layers and the connection patterns between layers specify the network architecture. The architecture design depends on the problem to be solved.

Neural networks are essentially pattern recognition tools. In fraud detection, neural networks are used to recognise the calling pattern of a customer and classify it as either fraudulent or non-fraudulent. The main difference between artificial neural networks and other fraud detection techniques is that knowledge about fraud is acquired through learning instead of programming. Instead of writing rules and algorithms that are programmed to recognise fraud cases, neural networks learn to classify on their own input data as fraud or non-fraud. For this reason, they are referred to as *self-learning* methods (Cerebrus Solutions, 2002b). The learning process of a neural network is called training (Hearne, 2004).

There are many types of neural networks – depending on their architecture and on their learning function – but they are all trained using either of the following training methods: supervised training or unsupervised training (Cerebrus Solutions, 2002b).

In supervised training, the neural network is trained with data of known behaviour. The neural network is provided with a sequence of input patterns and their corresponding target output patterns. A learning algorithm then repeatedly modifies the weights until the network output corresponds to the target output (Caudill & Butler, 1992:8). For instance, with reference to the VoD service mentioned earlier, supervised training can be used to detect unauthorised access to the videos using Indicator 2, namely ‘many costly downloads are performed’. Indicator 2 is used as it can be easily recognised by the values of the CDR parameters. The training process to detect this fraud type is explained below.

The neural network is presented with a large training data set of pre-labelled CDRs. Some CDRs represent normal behaviour and are labelled as “normal”, while other CDRs are fraudulent and labelled as “Unauthorised access to videos”. The fraudulent CDRs have the following characteristics:

- The selected video types correspond to expensive video categories such as a live event or a newly released movie.
- The required quality of service is very high.
- The number of the selected videos is high.
- The duration of the session is largely above average.
- The associated cost is high.

Obviously, low and high values are already predefined by the fraud analyst. In this case, the input pattern corresponds to the CDR field values and the target output is the correct labelling of the CDR. The neural network then learns to recognise fraudulent and non-fraudulent events when fed with data of similar patterns as the training set. For every CDR subsequently processed by the neural network, its field values are analysed and the CDR is labelled accordingly. The label is compared to the expected label of the CDR and in case it is not correct, the weights of the neural network are adjusted. Most of the successful applications of neural networks in commercial FMSs use supervised training because it allows the use of previously acquired knowledge in the learning process (Cerebrus Solutions, 2002b).

In unsupervised training, learning is performed without any training data; thus the output of the neural network is not known in advance. The network receives some input vectors and modifies their weights so that input vectors with the most similar characteristics are grouped together. Using the same example as above, unsupervised training can also be used to detect unauthorised access to the videos through the process described below.

The neural network is presented with a set of unlabelled CDRs. The network then identifies patterns in the CDRs (the parameter values) and groups CDRs with similar patterns together. The number of groups depends on the number of different patterns identified. Thus, in case the network analyst wants to differentiate between a CDR describing a normal behaviour and a CDR representing unauthorised access to the videos, he only presents a data set of these two types of CDRs (unlabelled) to the neural network. Depending on how disparate the parameter values are, more than two groups can be formed by the neural network. For instance, one group may contain CDRs with very low values for the number of selected videos, the duration of a session and the video costs, while another group will have medium values and a third one will have very high values.

Unsupervised training is most often used for clustering, that is, categorising input vectors based on discovered patterns in the data set (Engelbrecht, 2003:55). Unsupervised neural networks are powerful classification tools but their usage in fraud detection is rather limited because they require the fraud analyst to manually analyse their results in order to understand the identified patterns (Cerebrus Solutions, 2002b).

8.3.2.2.2 Advantages and disadvantages of using neural networks for fraud detection

The advantages of neural networks are manifold.

- Firstly, they are very effective for analysing complex data that cannot be processed efficiently with rigid rules and algorithms.
- Secondly, they produce very few errors once correctly trained.
- Thirdly, they are optimised for processing very large data sets, which is ideal for handling large volumes of network traffic.
- Besides, because they identify patterns in data, they can discover previously unknown calling patterns indicative of new fraud scenarios.
- Finally, as self-learning tools, neural networks can easily adapt to changing customer behaviour (Cerebrus Solutions, 2002b).

However, a major drawback of neural networks is their construction time, which can be significant. It takes a lot of time to properly train the network as well as to design its architecture (Horal, 2000). Besides, profile-based analysis and neural networks display the same shortcoming – they do not explain their results. Data is classified automatically without any justification.

8.4 Selection of fraud detection techniques for NGNs

The review conducted above provides the necessary knowledge to choose appropriate fraud detection techniques for an NGN FMS. The selected techniques are presented in this section and a justification of the researcher's choice is attempted. Section 8.4.1 first establishes some criteria that the researcher identified as necessary for effective fraud detection techniques for NGNs. The most appropriate fraud detection techniques are then selected in Section 8.4.2 based on the established criteria.

8.4.1 Requirements for NGN fraud detection techniques

Criteria for suitable techniques to detect NGN fraud have been determined on the basis of the above review as well as knowledge gained from previous chapters. These are, in particular, Chapter

2 which analysed NGN security vulnerabilities, Chapter 4 which described likely NGN fraud types and Chapter 6 which identified requirements for NGN billing systems. Many of the requirements are also taken from previous researchers in the field of NGN and IP fraud detection as explained below.

Moreau *et al* (1996) mention the need for intelligence in the FMS to accommodate the "heterogeneity and multiplicity" of the IP fraud scenarios. They also require flexibility and adaptability of the FMS to accommodate new fraud patterns. Horal (2000) likewise requires flexibility and adaptability. The FMS needs to be flexible in order to be modified easily to detect fraud on a new service and it should be adaptive to new technologies and changing customer behaviour. In addition to flexibility and adaptability, Horal (2000) identifies real-time fraud analysis and the ability to detect old as well as new, interesting and abnormal patterns as critical requirements for future FMSs. Hearne (2004) also talks about the need for near real-time analysis of CDRs and mentions that the FMS must be able to cater for many services with the ability to easily add or remove services.

In addition to these requirements, the author identified accuracy and scalability as necessary qualities of an effective NGN FMS. The combined requirements for NGN fraud detection techniques are therefore the following.

- **Flexibility**: The fraud detection technique must be very flexible to easily accommodate changing customer behaviour, services and fraud scenarios.
- **Coverage**: The FMS must be able to detect both new fraud types and existing, traditional fraud attacks as all of these are expected to be carried out in NGNs as long as their associated services are offered. It is therefore important to retain existing fraud detection algorithms that effectively detect current fraud attacks.
- **Intelligence**: The fraud detection algorithm should preferably be able to adapt without manual intervention of the fraud analyst, since he does not know the calling patterns associated with the new fraud scenarios. Some level of intelligence is therefore required.
- **Accuracy**: The FMS needs to generate as few errors (both false positives and false negatives) as possible. The fraud detection methods must therefore display a high level of accuracy.
- **Timeliness**: Fraud needs to be detected as quickly as possible. Ideally, this would happen in real-time to detect and stop ongoing fraud attacks which could be extremely costly in an NGN environment.

- **Scalability**: A high level of scalability is required from the FMS. The FMS should be able to handle large volumes of network traffic. The performance of the fraud detection technique should not be affected when the volume of data to analyse increases significantly (which is expected in NGNs due to the introduction of new services).

8.4.2 Selected NGN fraud detection techniques

In light of the above discussion, it is obvious that a combination of both absolute and differential analysis techniques is needed to tackle NGN fraud effectively. No single fraud detection approach can satisfy all the requirements listed above. Similarly, no single technique can meet all the required criteria. Consequently, complementary techniques are needed. Absolute and differential techniques both have advantages and disadvantages with regard to NGN fraud detection. Their respective benefits and shortcomings are briefly recapitulated below.

Absolute analysis techniques have the advantage of being fairly accurate since they have a low false alarm rate. They also provide detailed information about an attack, which makes it easier for the fraud analyst to respond appropriately to the attack. This is particularly important in NGNs where inappropriate responses to fraud can result in huge financial losses in the case of hard currency fraud. Hard currency fraud in particular is expected to prevail in NGNs due the high number of cost-sharing service and network providers. Disadvantages of absolute analysis techniques include their need to be regularly updated in order to detect new fraud scenarios that are not yet stored in their knowledge base. Maintenance of the knowledge base of the FMS is a time-consuming task as it requires careful analysis of each new attack (Axelsson, 2000). This is a serious drawback in NGNs, where many new fraud scenarios are expected to emerge. Existing FMSs, which are heavily based on absolute analysis techniques, will therefore not be able to detect the new fraud types.

The main advantage of differential analysis is its flexibility, which is a key requirement for an NGN FMS. Differential analysis techniques can adapt to evolving customer behaviour and are able to uncover new fraud types. A major problem with differential analysis methods is that, unlike absolute analysis techniques, they cannot give enough details about an alert. They can only tell what is abnormal and not which fraud type occurred (Arvidson & Carlbark, 2003).

For the purpose of this dissertation, the author has decided to select rule-based fraud detection together with unsupervised neural networks. In doing so, most of the requirements identified above are covered. Rule-based fraud detection provides accuracy and timeliness, while unsupervised neural networks give flexibility, intelligence and scalability. Furthermore, combining these two methods gives satisfactory fraud coverage to the FMS. The exact implementation of these methods in the NGN FMS architecture is provided in Chapter 10.

Rule-based fraud detection is used to identify known (i.e. current and past) fraud scenarios. Most of them can be easily modelled as rules, since their exact characteristics are well known. The rules also include known fraud thresholds. This implies that both rule-based and threshold-based fraud detection techniques are in fact implemented.

Unsupervised neural networks are used to identify patterns in call records that may indicate fraud cases not detected by the rules. The author decided not to use supervised neural networks because they require prior knowledge of the fraud patterns and will merely reproduce most of the results of the rule-based fraud detection process. Neural networks are preferred over statistical profile-based fraud detection as they can handle large volumes of data and are self-learning. A specific type of unsupervised neural network called a Self-Organising Map (SOM) is used. The SOM algorithm is described in the next chapter. Reasons for using a SOM are also provided in that chapter.

8.5 Conclusion

This chapter has reviewed common fraud detection techniques currently in use in commercial applications. Such analysis has been conducted in order to identify suitable fraud detection methods for the NGN FMS architecture that is proposed in this dissertation. From the review, the author concluded that a combination of methods implementing both absolute and differential analysis is needed. The methods that were selected are rule-based fraud detection for known fraud scenarios and the SOM for unknown fraud types. The implementation of the selected methods into the NGN FMS architecture is explained in Chapter 10. The following chapter describes the SOM algorithm and justifies its selection for detecting NGN fraud.

Chapter 9: Overview of Self-Organising Maps

9.1 Introduction

The previous chapter provided a critical review of current fraud detection techniques, after which techniques deemed appropriate for the NGN FMS proposed later in this dissertation were selected based on that review. A major shortcoming of these existing methods is that they lack the flexibility to accurately detect previously unknown fraud types. For this reason the author proposes in this chapter the use of a Self-Organising Map (SOM) – an existing powerful data visualisation tool – for detecting new NGN fraud scenarios. As explained in the previous chapter, the ability to discover new fraud patterns is a key requirement for any fraud management solution for NGNs due to the novelty of the convergent network technologies and services, and consequent novel forms of fraud attacks.

This chapter is structured into two sections. Section 9.2 describes the SOM algorithm, while Section 9.3 analyses the advantages of using a SOM for the detection of NGN fraud cases.

9.2 Description of the SOM algorithm

9.2.1 Background on the SOM algorithm

The Self-Organising Map (SOM) or Self-Organizing Feature Map (SOFM) is a model of unsupervised neural networks used for the analysis and visualisation of multi-dimensional data (Engelbrecht, 2003:63). The SOM algorithm was created by Teuvo Kohonen in the early 1980s, which is why it is often referred to as the *Kohonen network* (Picton, 1994:107).

Like other unsupervised neural network algorithms, the SOM classifies input data based on the similarity of the input vectors. Similar vectors are grouped into the same cluster. However, the distinguishing feature of a SOM is that its neurons represent a topological system (usually a two-dimensional rectangular or hexagonal map) and they are arranged in an ordered and structured way based on their weights (Hollmén, 2000). Neurons with close weight vectors are situated close to one another while neurons with very different weights are physically far apart (Engelbrecht, 2003:63). The goal of the SOM algorithm is to train the network so that nearby output vectors correspond to nearby input vectors. Since nearby vectors in the input data set have similar features,

the SOM learns the distribution as well as the topology of the input data. For this reason, the SOM is also known as a *topology preserving map* (Fausett, 1994:168).

9.2.2 Description of the SOM algorithm

A SOM has two components: the sample data to be trained on and the weight vectors (Kohonen 1999). The sample data can be of any dimension but the SOM algorithm will project it into a low-dimension plane (usually 2D or 3D maps) for better visualisation and understanding. Thus, a SOM is also a data reduction tool. Each weight vector in turn also has two elements: its data and its spatial location. The data of a weight vector has the same dimension as the sample vectors.

Like other unsupervised neural networks, the SOM is based on *competitive learning*, which is the process of updating only the weight of the neuron closest to the sample vector. This increases the probability of this neuron to win again the next time a vector with similar patterns is shown. The winner outputs a "1" when such a vector is presented and a "0" otherwise. This process is repeated many times. The end result is that there will be a winning neuron associated with every group of similar input vectors, enabling the neural network to learn how to categorise input data (Fausett, 1994:16). Basically, the SOM algorithm works as follows:

1. Initialise the weight vectors of the SOM with random numbers.
2. Randomly select a sample input vector *x*.
3. For every neuron of the SOM, calculate the Euclidian distance (Picton, 1994:108) between *x* and the neuron's weight vector.
4. Determine the neuron *y* associated with the shortest distance; it is called the winner or best matching unit (BMU).
5. Decrease the weight of *y* and of its neighbours to make them closer to *x*.
6. Repeat steps 2 to 6 for every sample input vector.

Note that neighbours are updated based on their distance to the winner. The further they are from the winning neuron, the less their weight is modified. This process is performed a large number of times for every sample vector. Winners differ from one sample vector to another (Kohonen, 1999). During learning, the neighbourhood distance is decreased over the successive iterations of the algorithm until it reaches a null value (Hollmén, 2000). The SOM ends up mapping output nodes to patterns in the input data.

Like other neural network algorithms, the SOM has two successive operating modes, as explained in Orr (1999).

- **The training process** where the map is constructed through competitive learning. This phase requires a very large number of input vectors to accurately represent all or most of the patterns to be identified.
- **The mapping process** where a new input vector is quickly and automatically assigned a location on the map, based on its feature.

Usually, a SOM can be graphically visualised by displaying a unified distance matrix (U-matrix) that shows the different clusters identified in the input data. The U-matrix calculates the distance between the map units and a colour is assigned to each unit based on this distance. Close units have similar colours (Hollmén, 2000). In case the identified patterns are labelled, their label can also be displayed on the associated map unit. Other SOM visualisation techniques are discussed in Vesanto (1999).

9.3 Advantages of the SOM algorithm for fraud detection

The SOM algorithm has been around for a relatively long period of time and it has been successfully applied in various areas including image processing, industrial process monitoring, speech recognition (Kohonen, 1999) and flaw detection in machines (Hsu, 2006). More recent applications of SOMs include financial analysis (Kaski *et al*, 2001) and medical diagnosis (Chan *et al*, 2000). However, its application in telecommunication fraud detection is not available in commercial FMSs due to the main disadvantage of differential analysis that was explained previously: it does not explain its results. However, the algorithm has several advantages that make it suitable for use in fraud detection for NGNs.

Firstly, the algorithm is very fast. It has a high processing speed for massive data sets, which makes it a perfect candidate for real-time fraud detection. Secondly, the SOM algorithm is simple and very popular as evidenced by its success record and by the large body of knowledge available on the topic. It is an efficient method of classifying data. Thirdly, and most importantly, it is highly visual. A SOM can be easily visualised with coloured maps that are easy to read. It reduces the complexity of a large data set to a few patterns that are quickly identifiable (Hsu, 2006).

A SOM is a data classification and visualisation tool. It is not a fraud detection technique *per se*. As such, unlike current fraud detection methods, it applies neither absolute nor differential analysis when used for detecting fraud. This is because the algorithm is not based on the knowledge of either normal or fraudulent behaviour. This gives the SOM its flexibility and power as no *a priori* knowledge about the usage data is required to identify fraud. The algorithm does not detect fraud but relies on the experience and visual analytical ability of the fraud manager. It greatly assists the fraud analyst in detecting suspicious usage patterns by presenting massive volumes of usage data in a simple and structured way. In addition to suspicious behaviour, other interesting patterns in the data set can be identified – such as the (normal or abnormal) correlation between several parameters (e.g. time of day and intensity of service usage). This information can provide more insight into customer usage patterns, which could subsequently be used to prevent service abuse or to define new fraud rules.

However, a major issue with a SOM is the need for massive training data sets to generate accurate results. Fortunately, this does not constitute a problem in this research project as the researcher managed to obtain data sets of considerable volume to train the performance of the algorithm in a real-life scenario. This experiment is described in detail in Chapter 11, which explains how the SOM algorithm was tested to verify the efficiency of the proposed NGN FMS architecture.

9.4 Conclusion

This chapter presented the SOM algorithm as an appropriate tool for detecting unknown patterns of fraud in NGNs. In the NGN FMS architecture proposed in the next chapter, the SOM is used in conjunction with other techniques reviewed in Chapter 8 to enable the detection of both known and unknown fraud types. The description of this FMS architecture constitutes the topic of Chapter 10.

Chapter 10: The NGN FMS architecture

10.1 Introduction

In Chapter 8 existing fraud detection techniques were reviewed and techniques deemed most appropriate for NGNs were selected. Chapter 9 presented the SOM algorithm, the original data analysis technique selected for identifying unknown NGN fraud scenarios. Determining suitable fraud techniques was the fourth step in this research, aimed at designing an FMS architecture to address the lack of flexibility and the application-specificity of existing FMSs with regard to NGNs. This chapter, which is the next step of the research, presents the original high-level FMS architecture proposed as a solution to these issues. The proposed architecture combines the various partial solutions determined in the previous chapters in relation to the types of fraud to be detected, the source and format of the FMS input data, and the fraud detection techniques to be used. In addition, some features of the architecture have been inspired by results of previous research projects in NGN fraud management reviewed earlier in the current dissertation.

The chapter is structured as follows. Section 10.2 presents requirements identified by the researcher as necessary for an effective NGN FMS. These requirements form the basis of the design of the NGN FMS architecture. In Section 10.3, the NGN FMS architecture proposed to satisfy these requirements is described in detail. Section 10.4 examines how the presented architecture can satisfy the requirements for NGN FMSs.

10.2 Requirements for NGN FMSs

This section discusses the requirements for an NGN FMS. Some of these requirements are similar to the required criteria defined for fraud detection techniques in Chapter 8 because the detection methods constitute the core of the FMS. The requirements are the following.

- **Application-independency and 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 traffic coverage:** The FMS needs to analyse all the data flowing through all the different access points in NGNs. As explained in Chapter 2, the fact that

NGNs have many access mechanisms, allows fraud attacks to be launched from various points simultaneously.

- **Timeliness:** Like the billing system, the FMS needs to process data as soon as it is received. However, the FMS should also allow batch mode processing to cater for fraud types that can only be detected after the observation of a sequence of billing records (e.g. call-selling fraud).
- **Scalability:** New fraud scenarios will be committed, which implies that more fraud rules will be added to the detection engine of the FMS. In addition, the number of billing records to be analysed by the FMS will also increase due to the new services offered**.** Old fraud attacks might again disappear in time when their associated services are no longer offered. The FMS architecture needs the ability to easily scale up or down to accommodate the dynamic NGN environment.

The FMS architecture designed to satisfy the above requirements is presented in the next section.

10.3 Description of the NGN FMS architecture

This section describes the architecture proposed for an effective NGN FMS. The architecture consists of several interdependent components each processing the usage records from the billing system. The billing records are in the IPDR format and are analysed in several stages for signs of fraud. For every stage, only billing records not identified as suspicious go through the next analysis phase. An alarm is generated for suspicious IPDRs.

The FMS is designed to accommodate any type of service. However, for the purpose of this dissertation, the author focuses on two types of services: phone calls and media-on-demand services. Phone calls are traditional voice services and media-on-demand is 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 VoD service presented here refers to the VoD service described in Chapter 8, together with some related fraud types: subscription fraud, unauthorised access to the videos and illegal redistribution of the videos. The videos are accessible from the operator's website and can be downloaded to the user's mobile phone.

The key components of the FMS are the modules used to analyse the IPDRs with the techniques selected in Chapter 8, namely rule-based analysis and the Self-Organising Map algorithm. The modules that perform rule-based analysis are named Service-specific Fraud Detectors and the module that implements the SOM algorithm is called the SOM Analyser. Another key component is the Intrusion-based Fraud Detector which integrates the functionality of an Intrusion Detection System (IDS) into the FMS. A UML (Unified Modelling Language) diagram of these components is shown in Figure 10.1. The diagram is designed with the UML notation because the UML is a standard system modelling language used worldwide (Fowler and Scott, 2000).

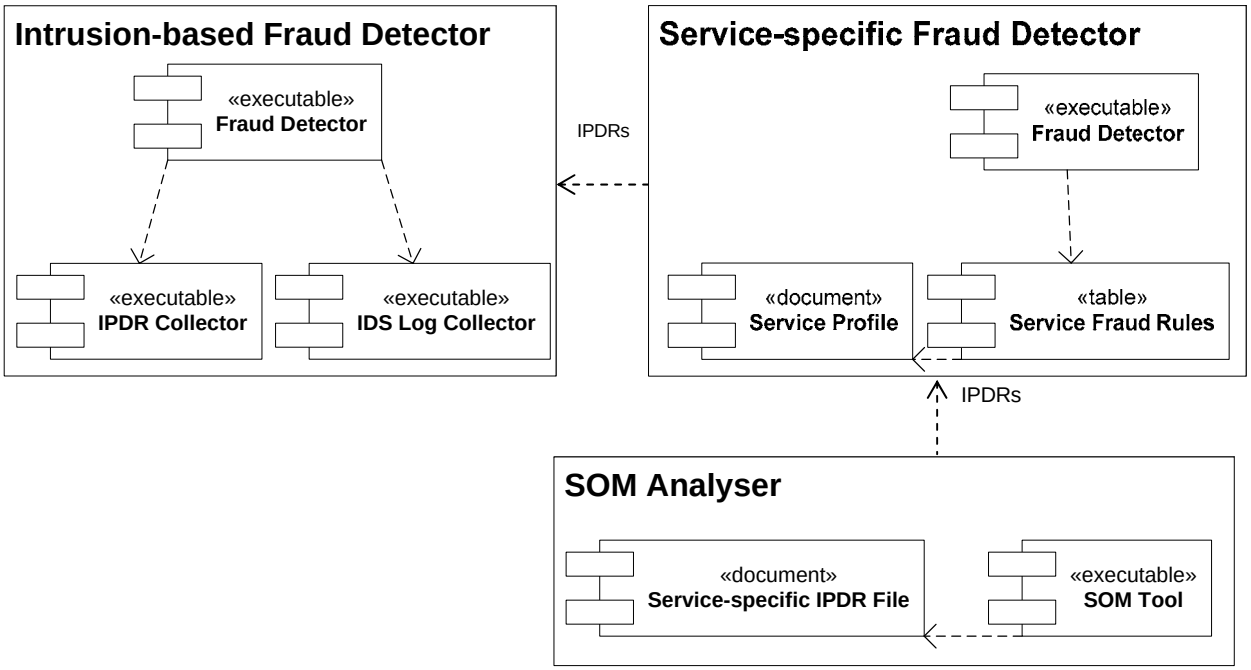

Figure 10.1: UML diagrams of the key components of the NGN FMS architecture

Figure 10.1 shows the component diagrams of the Intrusion-based Fraud Detector, a Service-specific Fraud Detector and the SOM Analyser. Each of these components is made of several sub-components. This is modelled by a big rectangle containing smaller rectangles. Each rectangle represents a component and has the name of the object it represents. Except for the container components, a component is modelled as a rectangle with two smaller rectangles on the left side. Each component also has a textual stereotype indicating its type: a document file, an executable file, or a database table. Dashed arrows represent a dependency between a client and a supplier. The client (source component) needs information from the supplier (target component). For instance, the SOM Analyser requires IPDRs processed by the Service-specific Fraud Detector,

which analyses IPDRs initially processed by the Intrusion-based Fraud Detector. A description of these main components follows.

10.3.1 The Intrusion-based Fraud Detector

The Intrusion-based Fraud Detector provides the first analysis phase for 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 (Arvidson, & Carlbark, 2003). The Intrusion-based Fraud Detector has three sub-components: the IPDR Collector, the IDS Log Collector and the Fraud Detector.

- The IPDR Collector retrieves IPDR records 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 IPDR records. Indeed, for every intrusion detected by the IDS, an alarm is generated in the FMS and the corresponding IDS entry is pulled by the IDS Log Collector. 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.

10.3.2 The Service-specific Fraud Detector

There is one Service-specific Fraud Detector for each different service offered by the operator. Each Service-specific Fraud Detector – 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 rules.
- The Fraud Detector applies the fraud rules to the IPDRs to detect any fraudulent activity.

Thus, the MobileCalls-specific Fraud Detector has fraud rules for, for instance, call selling, premium rate service fraud, cloning and roaming fraud (as specified in Table 3.1 in Chapter 3). It also has a service profile that specifies values for the average and standard deviations in respect of the duration, the number, the frequency, the cost and the time of the calls. The VoD-specific Fraud Detector has a table with rules for the frauds mentioned earlier: subscription fraud, unauthorised access to the videos and illegal redistribution of the videos. Indicators for these fraud types were mentioned in Chapter 8. The service profile of the VoD-specific Fraud Detector 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.

10.3.3 The SOM Analyser

The SOM Analyser processes the IPDRs with the SOM algorithm described in Chapter 9. It is used to detect unknown fraud patterns once the IPDRs have been analysed with known intrusion and fraud rules. The SOM Analyser consists of 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 hours). Each file contains IPDRs that were produced over the last specified time interval and that were not identified as suspicious by either the Intrusion-based Fraud Detector or the relevant Service-specific Fraud Detector. The files are deleted after the SOM analysis when no suspicious activity is found.
- The SOM Tool uses Service-specific IPDR Files as input to generate service-specific maps. The maps show clusters of the usage records, based on the similarity of the values of their parameters. The fraud analyst analyses the map to identify outliers or unusual patterns that may indicate suspicious activity. A detailed description of the SOM Analyser is provided in its prototype implementation in the next chapter.

In addition to the three key components described above, the NGN FMS has other modules that are necessary to correctly dispatch the IPDRs to the appropriate Service-specific Fraud Detector; to notify the fraud manager when suspicious activity is detected, and to confirm or refute fraud attacks from the suspicious IPDRs. They are the IPDR Dispatcher, the Alert Manager and the Case Manager. The NGN FMS also has a General Fraud Detector to detect general fraud rules applicable to all service types. This is done in order to avoid redundancy in various Service-specific Fraud

Detectors. The complete NGN FMS architecture is illustrated in the UML component diagram in Figure 10.2 and explained in the remainder of this section.

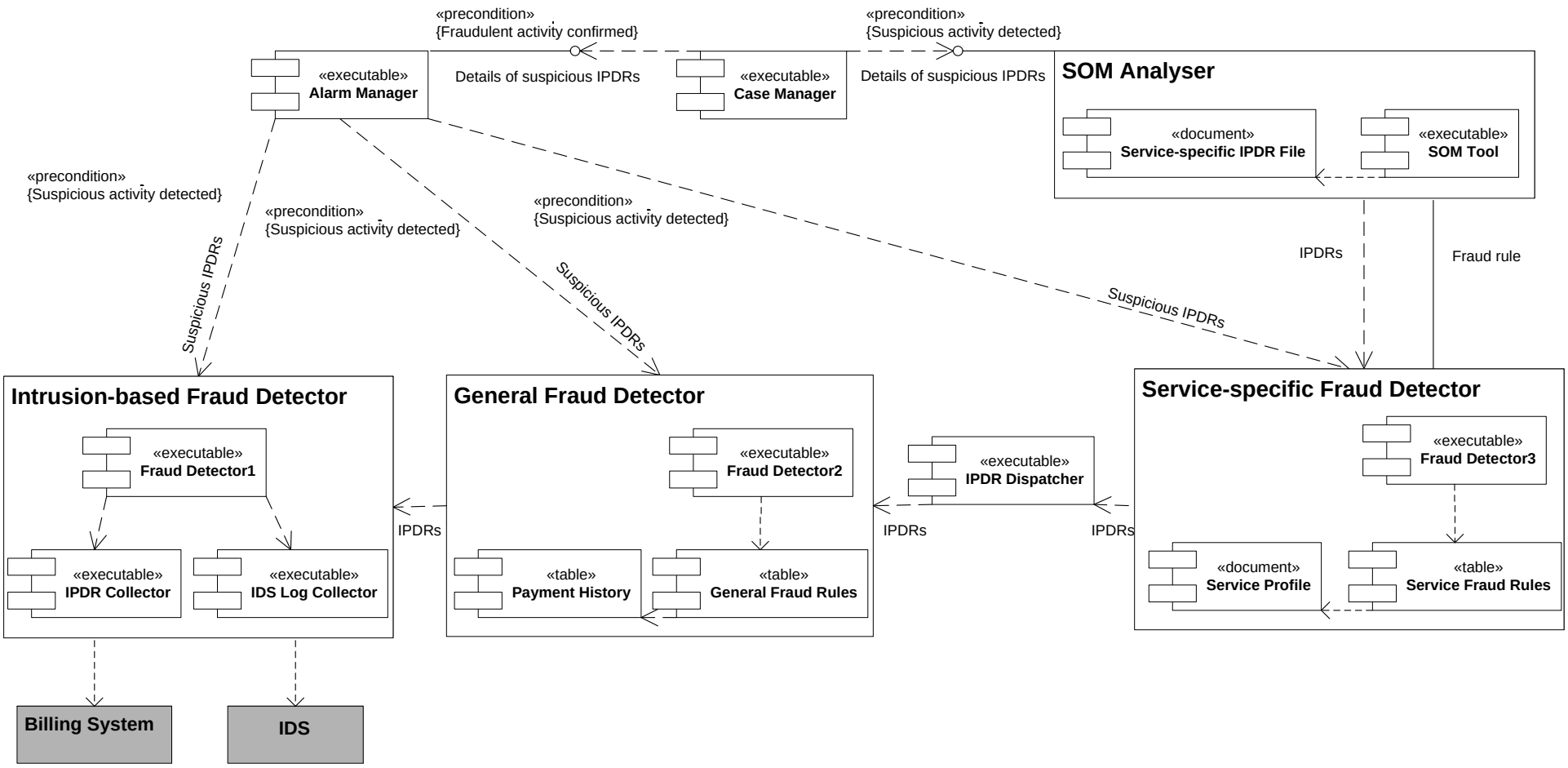

Figure 10.2: UML component diagram of the NGN FMS architecture

Only the unshaded blocks in Figure 10.2 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. The paragraph below explains the UML notation used in Figure 10.2.

- As explained in Figure 10.1, dashed arrows in Figure 10.2 represent a dependency between components. Some dependencies are subject to some conditions. For instance, the Alarm Manager can only obtain IPDRs from the Intrusion-based Fraud Detector if suspicious activity has been detected by that component.
- The 'lollipop' notation represents a dependency upon an interface. Thus, the Case Manager is dependent on the output of the SOM Analyser upon an interface. Indeed, when the fraud analyst recognises a possible fraud occurrence in a SOM-generated map, he manually opens a case in the Case Manager interface and enters all the information he gathered from the SOM analysis. If information entered on that interface is modified, it will affect the output of the Case Manager.
- The continuous line between the SOM Analyser and the Service-specific Fraud Detector indicates an association between these components. The information obtained from the SOM analysis can be used to detect new fraud scenarios and to define corresponding fraud rules subsequently added to the associated Service-specific Fraud Detector.

Figure 10.2 shows that the NGN FMS architecture has a multi-stage detection process. The reasoning behind this architecture is to go from a very general to a very specific fraud detection process. The IPDRs are first compared to known intrusions in the Intrusion-based Fraud Detector, and to general fraud scenarios in the General Fraud Detector. Then, they are analysed with fraud rules specific to each service type. At any of the above stages, in case some IPDRs are identified as suspicious, they are not sent to the next module but to the Alarm Manager which raises an alarm. Finally, the IPDRs are processed by a SOM to identify anomalies suggestive of unknown fraud scenarios. The Case Manager is used to conduct further investigation on a likely fraud attack, either from the alarms generated by the Alarm Manager or the suspicious patterns revealed by the SOM Analyser.

A more detailed description of the additional components of the architecture shown in Figure 10.2 (the General Fraud Detector, the IPDR Dispatcher, the Alarm Manager and the Case Manager) follows.

10.3.4 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 service types. It has three sub-components:

- The General Fraud Rules table stores the fraud rules.
- The Payment History database 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 quickly identify obvious cases of fraud. Examples of fraud cases that are 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 database.
- Blacklisted customer: The calling number or source IP address matches an entry in a blacklist of the operator.
- Collision: Simultaneous calls or logins from the same number or user account.

10.3.5 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 service types offered by the operator. 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 Figure 10.3 which shows the entries in that component.

```
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
```

Figure10.3: Illustration of the entries in the IPDR Dispatcher

10.3.6 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, sms, pop-up screen).

The Alarm Manager 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.

10.3.7 The Case Manager

The Case Manager is a graphical user interface used to conduct further investigation on 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 the fraud scale and impact (hard currency or soft currency) as explained in Chapter 3, Section 3.2.3. For instance, roaming fraud, which results in hard currency, has a higher impact and therefore a higher priority level than cloning, which is a soft currency fraud.
- For unknown suspicious fraud patterns detected by the SOM Analyser, other criteria are used to assign a priority level. This includes 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. The fraud analyst can also compare the fraud case at hand to similar past fraud cases to find

recurring fraud patterns. If the investigation from the Case Manager proves that no fraud attack occurred (false alarm), the suspicious IPDRs are deleted.

The flow of the different processes in the NGN FMS is summarised in the UML activity diagram in Figures 10.4a and 10.4b.

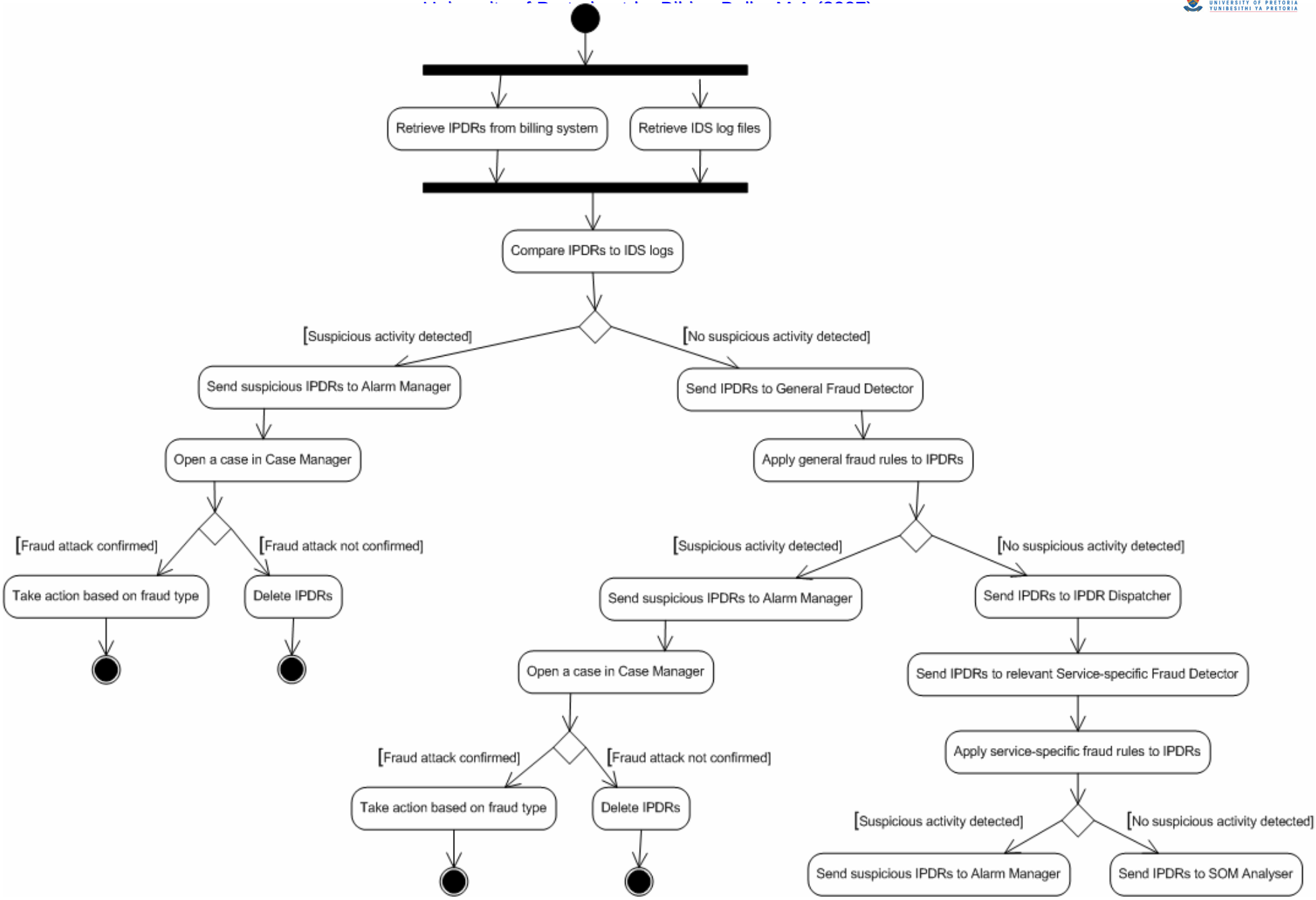

Figure 10.4a: UML activity diagram of the NGN FMS

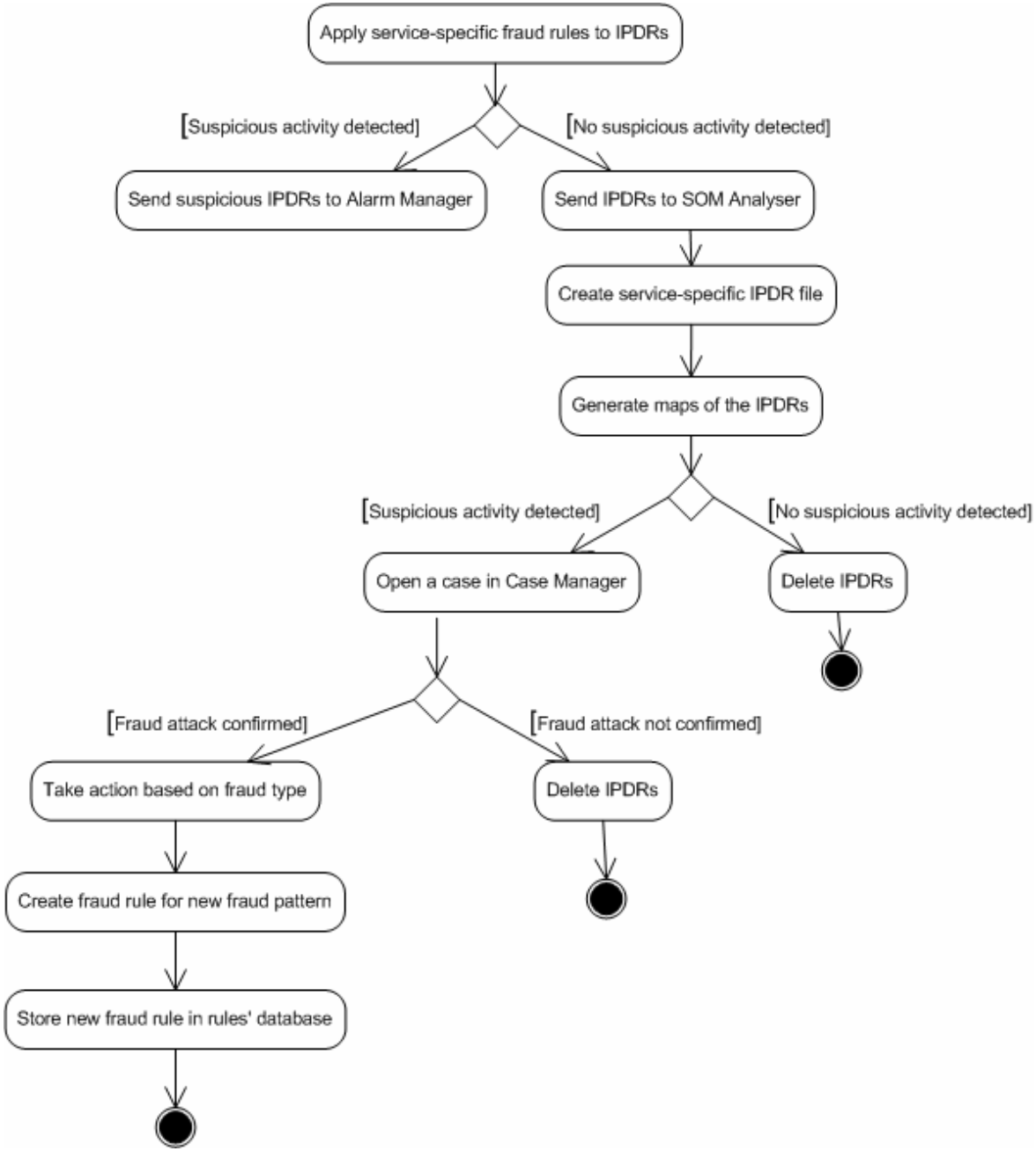

Figure 10.4b: UML activity diagram of the NGN FMS (following)

10.4 Examination of the proposed architecture

This section examines how well the proposed architecture satisfies the requirements for NGN FMSs identified earlier in Section 10.2.

- **Application-independency and flexibility**: Using the flexible IPDR format for the billing records enables any type of service to be recorded in that format and to be processed by the FMS. 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. Fraud rules are not interdependent and can thus be easily added or removed from the relevant modules, which provides flexibility to the FMS. In addition, using the SOM algorithm can help identify previously unknown fraud scenarios not stored in the rule database, adding flexibility to the FMS.
- **Complete network traffic coverage**: Combining intrusion and fraud detection gives a good overview of all the network traffic. It can also help prevent future fraud attacks by detecting some abuse of the network vulnerabilities that could be used for fraud (as shown earlier with the example of a hacking attack).
- **Timeliness**: The IPDRs are analysed as soon as they are collected by the FMS, although batch mode processing is also enabled for the SOM Analyser. The separation of billing records according to their service type also speeds up the fraud detection process because all the Service-specific Fraud Detectors work in parallel and have a reduced number of records to process and a limited number of rules to go through.
- **Scalability**: The modular architecture enables the FMS to easily scale down or up. Service-specific Fraud Detectors can be easily added or removed to accommodate a dynamic service offering in NGNs. Scalability is also enforced in the SOM Analyser, which only needs to analyse 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 increased scalability of the FMS.

10.5 Conclusion

This chapter has provided a high-level description of the original NGN FMS architecture that has been proposed to overcome the limitations of existing commercial FMSs. The proposed architecture has the potential to satisfy the requirements of flexibility, coverage, timeliness 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. A description of the prototype that was developed to test the viability of the SOM Analyser component of the architecture is given in the next chapter.

Chapter 11: Prototyping the SOM Analyser of the NGN FMS

11.1 Introduction

This chapter documents the prototype implementation of the SOM Analyser of the NGN FMS architecture which was presented in the previous chapter. The prototyping focuses on the SOM Analyser as it is the key novelty of the architecture and the tool used to detect unknown NGN fraud scenarios. The goal of the prototype implementation was to assess the viability of using a SOM to detect suspicious usage patterns. This was achieved through the processing of a set of usage records with a SOM implementation tool. Chapter 11 first presents a detailed architecture design of the SOM Analyser and then documents the prototyping of this component.

The remainder of the chapter is structured as follows. Section 11.2 provides a detailed design of the SOM Analyser. The design is used as the basis for the prototype implementation. Section 11.3 gives an overview of the preliminary work that was performed to set up the lab environment. This involved designing a testing plan, obtaining an appropriate training data set and selecting the proper SOM training software. The section explains how each of these phases was performed and how they all contribute to the success of the prototype implementation. The complete implementation of the SOM Analyser prototype – from the data pre-processing to the output maps – is detailed in Section 11.4. Finally, the outcome of the prototype implementation is discussed in Section 11.5.

11.2 Designing the SOM Analyser

This section explains the detailed design of the SOM Analyser. A high-level design of this component was provided in the NGN FMS architecture diagram in Figure 10.2 in Chapter 10. For clarity, this diagram is reproduced in Figure 11.1.The SOM Analyser is the block with thick lines on the figure. It uses non-suspicious IPDRs from Service-specific Fraud Detector modules as input to create service-specific IPDR files. It then outputs maps of the usage patterns in the IPDRs using a SOM tool that applies the SOM algorithm to the IPDR files. A detailed UML class diagram of the SOM Analyser is shown in Figure 11.2.

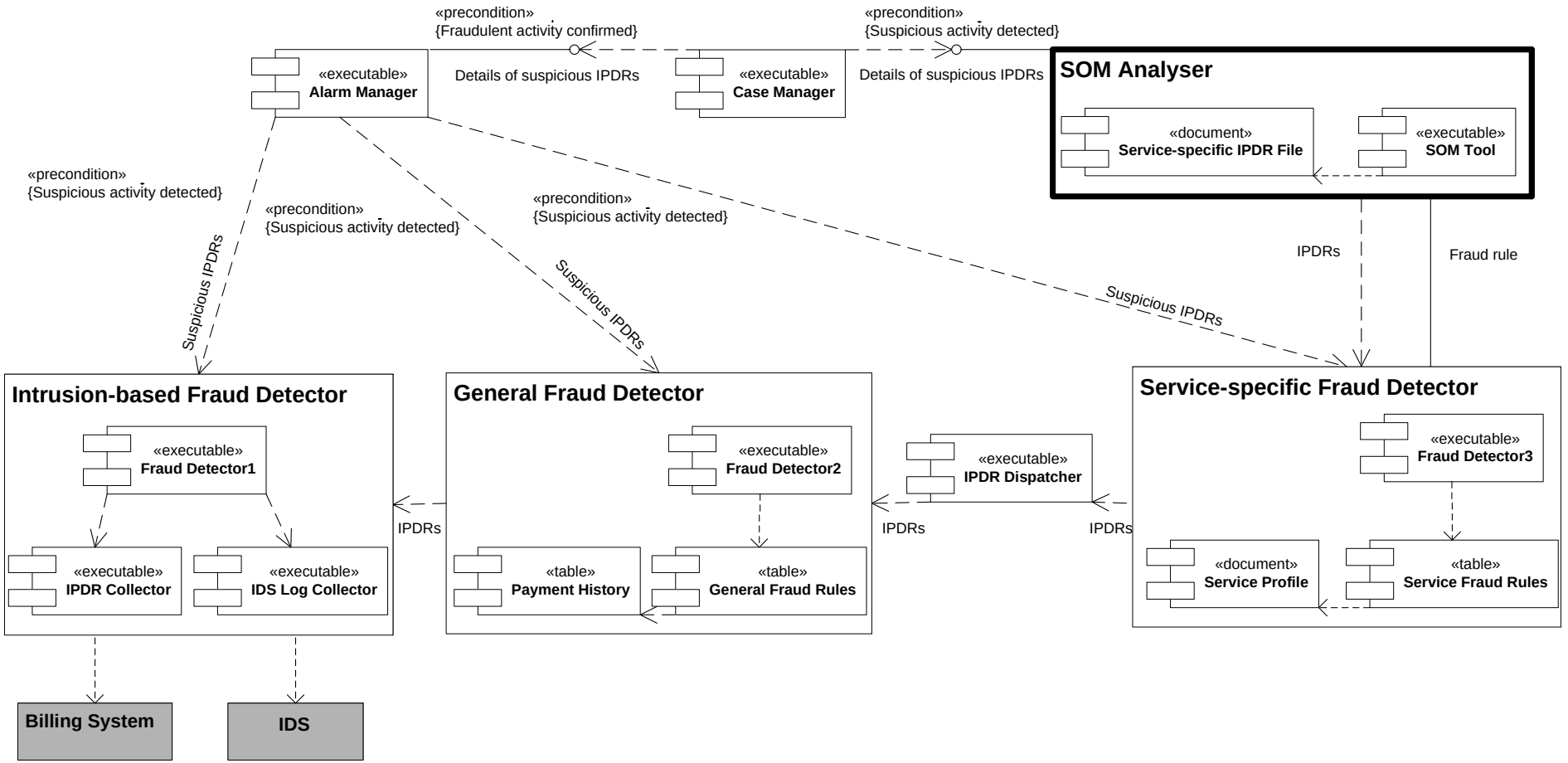

Figure 11.1: Component diagram of the NGN FMS architecture

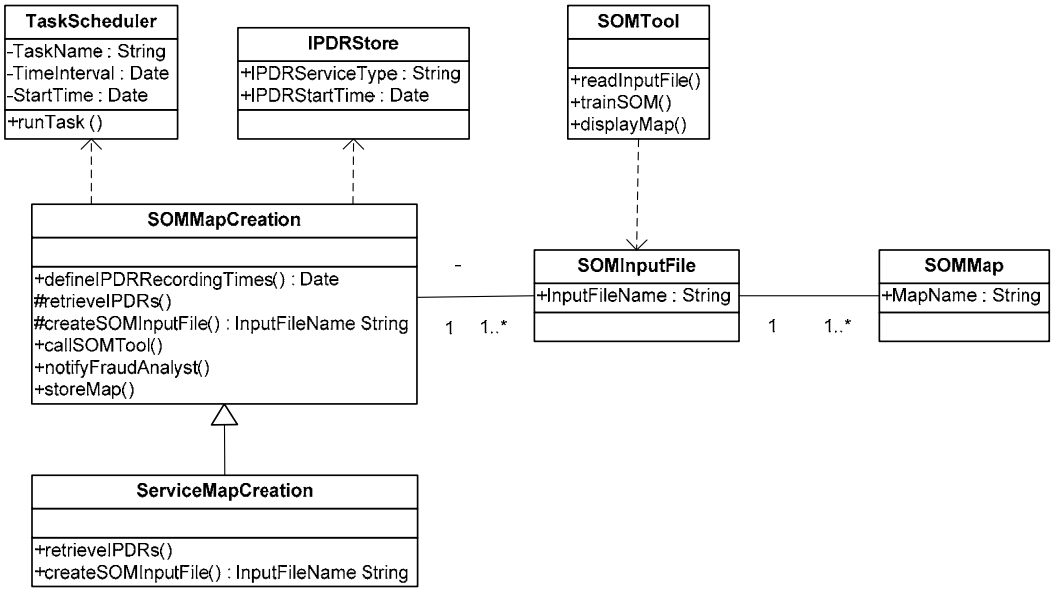

Figure 11.2: Class diagram of the SOM Analyser

Figure 11.2 shows the seven different classes that constitute the SOM Analyser, as well as their parameters and methods. As explained in Figure 10.2 in Chapter 10, dashed arrows indicate dependencies between classes: the source class depends on the target class. The arrow with a white tip indicates a realisation: the source class inherits and implements the functions of the target class. The seven classes are used as explained below. Note that as for the FMS architecture in Chapter 10, the description of the SOM Analyser is based on two service types: mobile calls and video-on-demand (VoD).

11.2.1 IPDRStore

The IPDRStore stores IPDRs identified as non suspicious by the Service-specific Fraud Detectors. Typically, it is implemented as a database containing different tables for each service type. Each Service-specific Fraud Detector sends its "normal" IPDRs to the associated table. The IPDRs are retrieved at specified time intervals by the SOMMapCreation class to create service-specific input files for the SOM.

11.2.2 SOMMapCreation

The SOMMapCreation class is the core module of the SOM Analyser. It is responsible for creating input files for the SOM, calling the SOMTool class to process the input files, notifying the fraud analyst once the SOM output maps are created, and storing the maps. It is typically implemented as a batch file called at regular time intervals by the TaskScheduler. The different functions of this class are performed in the following sequence:

- `DefineIPDRRecordingTimes()` defines the time interval (start and end times) used to retrieve the most recent IPDRs from the IPDRStore. Only IPDRs whose recording start time falls within that time interval are retrieved. For instance, if the FMS is programmed to generate SOM maps every four hours, then the end and start times for the very last four-hour interval will be defined as follows:

```
endTime = current time;
startTime = endTime – 4 hours;
```

- `retrieveIPDRs()`extracts IPDRs from the IPDRStore according to the criteria (time interval) defined above. Only parameters relevant for fraud detection are retrieved. For example, with reference to the `startTime` and `endTime` variables defined above, the SQL code to extract the relevant IPDRs from the VoD table in the IPDRStore is as follows:

```
SELECT video-type, file-size, bandwidth AND price FROM VoD_table WHERE
IPDRStartTime >= startTime AND IPDRStartTime <= endTime;
```

- `createSOMInputFile()` creates a text file from the extracted IPDRs in the format specified by the SOMTool class. The text file is stored in the SOMInputFile class.
- `callSOMTool()` calls the SOMTool class to process the file stored in SOMInputFile using the SOM algorithm.
- `notifyFraudAnalyst()` alerts the fraud analyst (e.g. sms or pop-up screen) once the SOM tool generates output maps from the input file.
- `storeMap()` stores the output maps as image files in the SOMMap class.

11.2.3 ServiceMapCreation

ServiceMapCreation is a child class of SOMMapCreation. There is one ServiceMapCreation class for each service type (e.g. MobileCallsMapCreation class for the mobile calls service and VoDMapCreation class for the VoD service). IPDRs from different service types have different parameters that can be used for fraud detection. For instance, parameters used for detecting fraud include the calling number, the called number, the call duration and the call rating for mobile calls, while fraud detection on a VoD will use the video type, the video file size, the bandwidth used and the video price. Therefore, the functions retrieveIPDRs() and createSOMInputFile() in SOMMapCreation have different implementations from one service type to another. For this reason, they are defined as abstract functions in SOMMapCreation and implemented in ServiceMapCreation classes.

11.2.4 SOMTool

The SOMTool class implements the SOM algorithm. It reads the input files stored in SOMInputFile, trains the SOM to cluster the values of the IPDR parameters based on their similarity and displays some coloured maps that show the identified clusters.

11.2.5 SOMInputFile

The SOMInputFile class stores input files created by ServiceMapCreation classes.

11.2.6 SOMMap

The SOMMap class stores the output maps of the SOM. The maps are analysed by the fraud analyst to identify suspicious usage patterns based on service profiles stored in the Service-specific Fraud Detectors.

11.2.7 TaskScheduler

The TaskScheduler is a generic class that automatically runs tasks (in the form of executable files) at predefined time intervals. It requires the task name, a specified time interval and the start time to run the task using the runTask() function which calls the specified file, in this case the SOMMapCreation batch file. The TaskScheduler can be implemented using the Windows built-in Scheduled Tasks application.

The different processes of the SOM Analyser explained above are summarised in the sequence diagram in Figure 11.3.

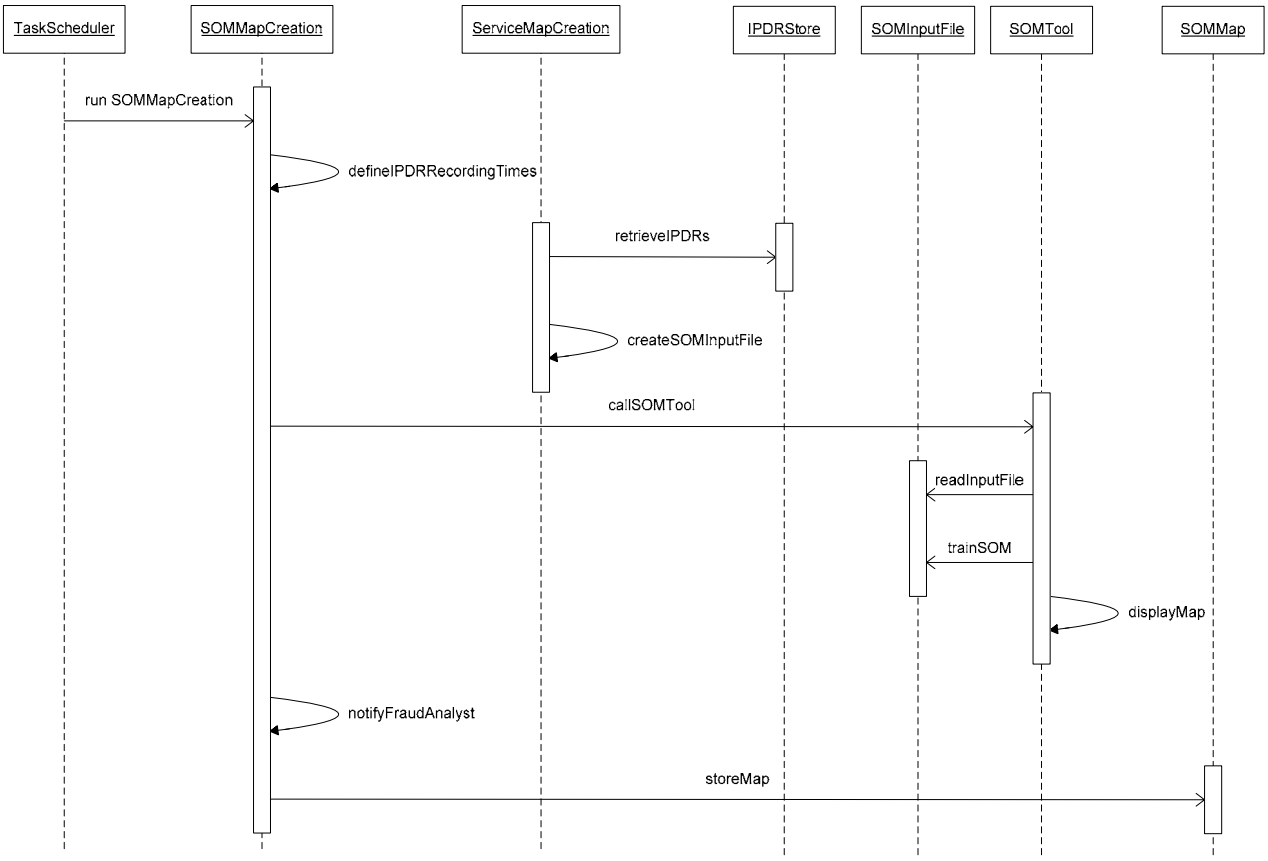

Figure 11.3: SOM Analyser sequence diagram

11.3 Setting up the lab environment

The goal of the prototype implementation was to verify whether using a SOM was a viable method for detecting fraud. For this reason, the researcher followed the main processes illustrated in Figure 11.3, namely create some files of service-specific usage records, process them with a SOM implementation tool and generate some service-specific maps. Some service profiles were also needed to identify suspicious activities from the maps. The prototype implementation required some test data, a SOM implementation tool and a testing plan, described in Sections 11.3.1, 11.3.2 and 11.3.3 respectively.

11.3.1 The training data set

A set of usage records was required to train the SOM. The ideal set-up was to use real customer usage data flowing from a network service. It would enable the obtainment of usage patterns and service profiles that are as realistic as possible and allow the testing of the timeliness of the fraud analysis process. All this could be achieved by setting up an IP service environment such as a media-on-demand server using a free trial version available on the Web. Unfortunately, setting up

such a lab environment proved to be time and resource consuming and subject to many errors. Therefore, static usage records were used instead. As real data was required to obtain realistic results, the researcher asked Telkom's fraud management team for a file containing records from past customer usage. Telkom is a major fixed-line operator in South Africa. Because Telkom does not use the IPDR standard yet, the records provided were not in the IPDR format but rather in Telkom own's internal format. Fortunately, this did not affect the prototyping because all the necessary usage fields were present.

Telkom gave a Microsoft Excel file of 2 595 CDRs generated from an SS7 gateway. The CDRs were produced over 242 seconds or 4 min (between 12:34:40 PM and 12:38:42 PM) on Friday, 3 June 2005. The CDRs had 16 parameters but only the following nine were used in the prototype implementation as they provided all the necessary information:

- StartTime
- Duration (in seconds)
- Destination
- Reference (calling number)
- B_Curr_Type (Telkom internal classification code indicating the call type)
- B_Curr_N2 (country code for international call)
- Rating (approximate call cost, no unit specified)
- A_NP_Curr (area code of calling number)
- B_Curr_N1 (prefix indicating call type, e.g. 09 for international call)

Figure 11.4 shows a few CDRs from the CDR file. For privacy, the destination and reference numbers have been modified. For the same reason, the CDR source and parameters, as well as the call types recorded in the file had been carefully selected by Telkom.

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

Figure 11.4 Sample CDRs from the test data set

11.3.2 Selection of the SOM software

MATLAB (MathWorks, 2006) was used as the software application to apply the SOM algorithm to the provided data set. MATLAB is a commercial product used for technical computation. It enables one to easily compute, visualise and program solutions and algorithms for mathematics and data

analysis problems. It is also often used for modelling and prototyping. The software has built-in functionality for many complex mathematical functions including neural network algorithms. MATLAB was chosen because it was readily available in the computer lab of the Mathematics Department at the university and the researcher had some prior experience of using that tool. Besides, it is a well-known and recognised application used as the tool of choice for research and analysis, both in academia and in industry.

After a thorough review of the SOM functionality offered by MATLAB, the researcher decided to incorporate a MATLAB add-on, the SOM Toolbox (CIS, 2006), due to the limited visualisation features of the built-in SOM module of MATLAB. The SOM Toolbox package is freely available online on the website of the Laboratory of Computer and Information Science (CIS) at the Helsinki University of Technology (CIS, 2006). In addition to its ability to train SOMs, the SOM Toolbox has very powerful and flexible functions to visualise the trained networks. The Toolbox allows the user to display various types of maps and visualisation features, including the following:

- **A U-matrix**: The U-matrix shows distance values between cells in the map. Each cell or unit represents an input vector in the data set. In this case, an input vector is a CDR. The distance between input vectors indicates how close input vectors are from one another and is therefore used to show the clusters in the data set.
- **Component maps for each input field**: The component map shows on a colour bar the scale of the values in the field and also represents clusters in that field. In this discussion an input field corresponds to a CDR parameter. Each component map is automatically assigned a title based on the information provided in the input field. The user can specify which component map he wants to display. Note that the values on the colour bar are not always accurate and representative of the values in the input file. The colour bar merely represents the distribution of the values in the input file and not the actual values. However, it is possible to get a fairly accurate indication of the values in the data set by displaying some hits, as explained below.
- **Empty maps**: They have the same topology as the component maps and can be used to display various visualisation attributes including labels and hits. Hits are coloured dots on the map units that show how well the values on the map match the corresponding values in the data set. Hits and labels can also be added to the component maps.
- The user can modify the default settings for maps and visualisation attributes such as font size; type and colour for the legend and the title; colour range for the colour bar; colours for labels and hits; and map size and shape (e.g. 2D or 3D).

11.3.3 The prototype implementation plan

In order for the SOM analysis to be a viable approach towards fraud detection, the researcher identified the following three key requirements that it needs to satisfy:

- Firstly, the algorithm must produce accurate results. In other words, the clusters displayed on the map must correctly reflect the patterns in the input data.
- Secondly, the algorithm must be scalable to correctly process data sets of varying sizes. This is especially crucial for data sets of large volumes as is usually the case in real-life network environments.
- Thirdly, the algorithm must be fast enough to quickly process the data at specified time intervals. The output maps should be generated within a few minutes after the SOM tool has been invoked.

The researcher opted for the following series of tests to assess these criteria:

- **Testing the accuracy of the data clustering**

Since the researcher had absolutely no prior knowledge of the calling patterns in the data set, she decided to test the SOM functionality by first processing the data with a familiar software application and then checking whether the SOM would provide similar results. If maps were generated solely with the SOM Toolbox, she would not be able to confirm the accuracy of the results. As the initial data set was provided as a Microsoft Excel file, it was processed with that software application (Microsoft Excel) as indicated later in Section 11.4.1.

- **Testing the scalability of the SOM algorithm**

In addition to the initial data set of 2 595 CDRs, the researcher fed the SOM Toolbox with other data sets of increasing sizes to determine the scalability of the algorithm and its performance level in a real-life environment.

- **Testing the processing speed of the algorithm**

As with the test conducted for the scalability of the SOM, the researcher used different data sets of varying sizes and monitored the elapsed time between the reading of the input file and the generation of the output map.

Section 11.4 provides a thorough explanation of how each of these tests was conducted.

11.4 Description of the prototype implementation

This section describes the experiment conducted to prototype the SOM Analyser described in Figure 11.2. The prototyping followed the plan outlined above: testing the accuracy of the data clustering (Section 11.4.1); testing the scalability of the SOM algorithm (Section 11.4.2); and testing its processing speed (Section 11.4.3).

11.4.1 Testing the accuracy of the data clustering

As mentioned previously, two series of analyses were performed to test the accuracy of the SOM data clustering. Firstly a statistical analysis of the test data was conducted with Excel, and then the data was processed with the SOM Toolbox to confirm the results. These phases are described in Section 11.4.1.1 and Section 11.4.1.2 respectively.

11.4.1.1 Statistical analysis with Excel

The goal of the statistical analysis was to identify call patterns that could subsequently be confirmed with the SOM analysis. To this end, the researcher first determined general trends in the data set and then created service "profiles" to obtain detailed call patterns. Since the Excel file only contained CDRs for one service type (phone calls from a fixed line), the call types were considered as different services. Note that, since the test data possibly contained fraudulent CDRs, the profiles did not indicate normal user behaviour as is the case in the proposed NGN FMS architecture. They merely indicated the trends of user activity for each service type.

In order to obtain general calling trends, a Pivot Table was created using all the CDRs to determine the distribution of the different call types in the data set. The Pivot Table, displayed in Figure 11.5, showed the count and percentage of calls for each call type (B_Curr_Type parameter), as well as the overall average call duration and call rating. Basic service profiles were also included in the table. For each call type, the average, minimum and maximum values for the calls' duration and rating were calculated.

	Description	B_Curr_Type	Count	Percentage	Avg_duration	Min_duration	Max_duration	Avg_Rating	Max_rating	Min_rating
3	International call	16	1237	47.67	49	5	220	287	2046	0
4	Shared call	9	775	29.87	58	5	229	96	248	62
5	FreeCall	3	204	7.86	54	5	204	0	0	0
6	Fax to Email	21	147	5.66	53	6	168	335	992	62
7	MaxiCall	10	141	5.43	56	5	206	196	620	62
8		5	24	0.92	80	12	228	0	0	0
9	Call to a competition line	2	16	0.62	12	5	90	93	558	62
10	MaxiNet (ISP)	15	15	0.58	36	15	75	66	124	62
11		-1	12	0.46	59	9	138	93	186	0
12	Call to an information line	22	12	0.46	91	35	174	439	930	186
13		11	4	0.15	16	11	19	0	0	0
14	Call to a competition line	18	4	0.15	80	21	124	481	744	124
15	Virtual Fax deposit	13	3	0.12	48	31	73	124	186	62
16	Call to VoiceLink	14	1	0.04	17	17	17	62	62	62
17										
18		**Grand Total**	**2595**		**53**			**162**		

Figure 11.5: Profiles of call types based on Excel analysis

In Figure 11.5, highest values for call duration and rating are highlighted in blue. The top five call types according to their percentage in the data set are highlighted in yellow. Although very elementary, this analysis reveals important information about calling trends in the data set as explained below:

- There are 14 call types recorded in the data set. A description of some of these call types could not be found, hence the empty cells in the Description field.
- The large majority of calls are international calls (47.67%), followed by shared calls (29.87%). Other popular call types are free calls (7.86%), fax to email (5.66%) and MaxiCalls (5.43%).
- Calls are usually short, with an overall average of 53 s. The longest calls are generally calls to information lines (average of 91 s) and calls to competitions lines (average of 80 s). Note that the shortest call duration is 5 s and the longest is 229 s (a Shared call).
- Calls are usually inexpensive with an average rating of 162. The longest calls are also the most expensive, with an average rating of 439 for calls to information lines and of 481 for calls to competition lines. The minimum rating value is 0 (for free calls) and the maximum is 2046 (an international call). Note the extent to which this value is an outlier in the data set.

After a general overview of the call patterns had been obtained from all the CDRs, more detailed profiles were created using only service-specific CDRs. Results of the analysis that was conducted for international calls are presented in Figure 11.6. The focus was on international calls because they are usually more prone to fraud attacks than other call types. The parameter B_CURR_N2 (country code for international call) was used to calculate the count of each country code (i.e. the number of calls made to this country), its percentage in relation to all international calls, as well as the average duration and rating of the calls per country code. The country or destination corresponding to each code was also indicated.

1	Count and percentage of dialled international numbers based on destination country					
2	Nr of different destinations is 100, Max avg call duration is 220s (to 223-Mali), min is 5 (to 1813)					
3	Count of B_CURR_N2					
4	B_CURR_N2	Total	Percentage	Avg duration	Avg rating	Country or destination
5		1335				
6	44	342	27.14	31	161	UK
7	263	105	8.33	63	287	Zimbabwe
8	264	103	8.17	57	264	Namibia
9	267	98	7.78	53	248	Botswana
10	258	91	7.22	50	368	Mozambique
11	268	69	5.48	50	241	Swaziland
12	266	47	3.73	54	255	Lesotho
13	49	34	2.70	46	259	Germany
14	265	33	2.62	68	333	Malawi
15	260	24	1.90	70	434	Zambia
16	88233	19	1.51	34	0	Mobile Satellite service
17	234	17	1.35	65	554	Nigeria
18	31	15	1.19	52	298	Netherlands
19	9	15	1.19	36	66	MaxiNet ISP (0899)
20	91	15	1.19	61	380	India
21	254	14	1.11	45	283	Kenya
22	33	14	1.11	45	221	France
23	244	12	0.95	59	362	Angola
24	39	10	0.79	35	229	Italy
25	86	10	0.79	63	601	China

Figure 11.6: International call trends in test data

Figure 11.6 shows the top 20 international destinations in terms of the percentage and number of calls. The top five destinations are highlighted in blue: UK, Zimbabwe, Namibia, Botswana and Mozambique. Except for the UK (which is largely dominant), the other top four entries are all neighbouring countries to South Africa, which is not surprising. A surprising finding is however that although the UK is the most popular destination, calls to this country are the shortest (average duration of 31 s) and the cheapest (average rating of 161).

Equipped with the knowledge gained from the statistical analysis, the researcher proceeded to the SOM analysis, which is described in the next section.

11.4.1.2 The SOM analysis

The goal of the SOM analysis was twofold: firstly, to verify the results of the Excel analysis and secondly, to identify suspicious call patterns. The SOM Toolbox was used for both these objectives. The basic usage of the SOM Toolbox involves the five steps (CIS, 2006) depicted in Figure 11.7 below.

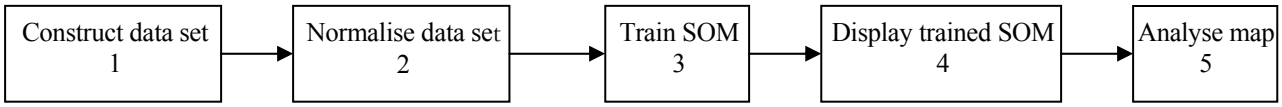

Figure 11.7: SOM Toolbox usage procedure

These steps can be grouped into the following phases: some preprocessing of the data (step 1); the actual SOM processing (steps 2, 3 and 4); and the analysis of the generated maps (step 5). These phases are described in Sections 11.4.1.2.1, 11.4.1.2.2 and 11.4.1.2.3 respectively.

11.4.1.2.1 Preprocessing

As a computational method, the SOM can only process numerical data. The data must be in a column format where each column corresponds to one input field of numerical values. Although represented as a string of digits, values in several fields in the Excel file were not numeric. For instance, the destination number 0860123456 has no numerical value for the SOM algorithm as it cannot be quantified (e.g. it is not smaller than 0860123457 or greater than 0860123454). This number represents a code and is considered as a text by the SOM. Some preprocessing of the Excel file was therefore needed to retain only numeric fields. However, since the SOM Toolbox allows the use of symbolic values for labelling the numeric fields, non-numeric attributes were also kept, but only as labels. Preprocessing involved the following steps:

- Select numeric fields: The only numeric values in the CDR file were the duration and the rating of the calls and thus, they were the only numeric input fields to the SOM.
- Select non-numeric fields: The non-numeric fields that were used were the call type, the calling number, the called number, the calling area and the country code of the dialled international number. For an easier understanding, call type codes were replaced by a shortcut of their textual description. For instance, “i” was used for international call, “fr” for free call, “s” for shared call, “m” for MaxiCall, “fe” for Fax to email and “if” for call to information line.
- Create a text file: After selecting numeric attributes, a text file was created from the Excel file to comply with the file types that can be recognised by the SOM Toolbox.
- Format the text file according to the SOM Toolbox specifications: In the first line of the file the number of numeric fields was specified and in the second line the field names. This was followed by the field values, starting with numeric fields. Column fields were separated by tabs.

Figure 11.8 shows the top entries of the formatted input file.

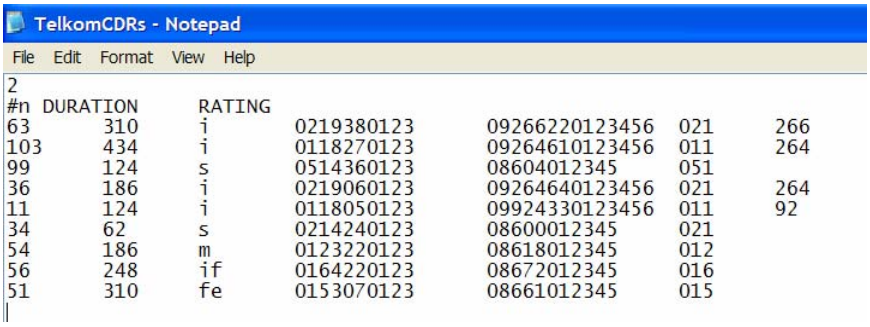

Figure 11.8: Top entries of the formatted input file

11.4.1.2.2 The SOM processing

Once the data set is created, the basic three operations that constitute the SOM processing (normalise the input vectors, train the map, visualise the map) are straightforward; each can be executed with a single command. In addition to these operations, the user must specify the input file name and the type of maps he wants to generate, as well as other optional features (e.g. on which map he wants the labels to be displayed).

As with the statistical analysis, the researcher first determined general patterns by generating some maps of all the CDRs. Next, service-specific input files were created and service-specific maps were produced. The following commands were used to create some maps of all the CDRs, using default attributes. Comments are provided for each command. The resulting maps are described in the next section.

```
sD = som_read_data('TelkomCDR.txt'); % read the input file
sD = som_normalize(sD, 'var'); % normalize the input vectors (input fields)
sM = som_make(sD); % initialize and train the SOM
sM = som_autolabel(sM, sD, 'vote'); %Add the labels to the maps
som_show(sM, 'umat', 'all', 'comp', 1:2, 'empty', 'Call type', 'norm', 'd');
%Specify SOM visualization features: display a U-matrix of all the components (
input fields), then display components maps for each input field and an
additional empty map entitled “Call type”; use the ‘denormalised’ values on the
maps, i.e. the original input values.
som_show_add('label', sM, 'subplot', 4); % Add the labels to the 4th map, in
this case the empty map that was created just for labelling.
```

11.4.1.2.3 Analysis of the SOM output

This section describes the output of the SOM processing in the form of coloured maps. The four maps created from the initial SOM processing are shown in Figure 11.9. MATLAB displays all maps on the same plan, in the order specified by the user: first the U-matrix, then the first and second component maps and finally the empty maps with labels. An explanation of the maps follows.

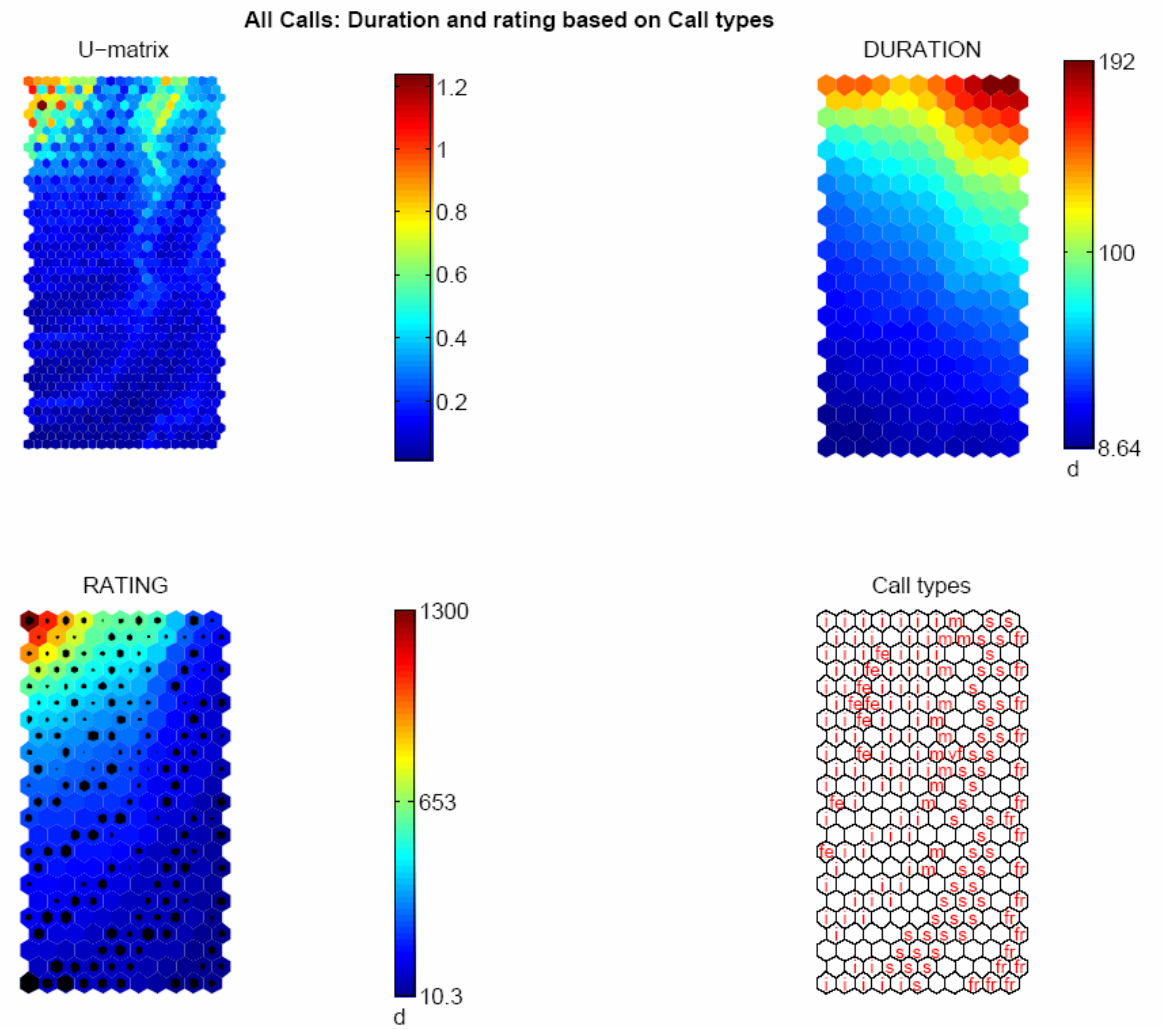

Figure 11.9: Maps of the duration and rating of all calls in the data set

- U-matrix: This is a visualisation of the clusters in the data set based on the duration and the rating of the calls. As mentioned previously, it shows distance values between input vectors. High values (shown on the colour bar) indicate a high distance between vectors and thus represent cluster borders. As can be seen, almost the entire map is blue, which means that there is a strong correlation between the duration and the rating of all the calls in the data set. In other words, rating is generally proportional to duration. There are a few exceptions where the colour is different, but no definite cluster can be inferred. The data set is therefore generally uniform.
- Duration map: It shows the scale of the values for the duration of the calls, which is roughly between 8 s and 192 s. This is rather close to the range of 5 s to 229 s obtained with the Excel analysis. As shown on the map, most of the calls are short (in blue). This corresponds to the results obtained from the statistical analysis. However, a small number of calls are

relatively long (in red). The map shows the existence of three clusters: short calls in blue, medium-duration calls in light blue and green, and long calls in orange and red.

- Rating map: This map shows that only a very small percentage of the calls are expensive (in red in the top left corner). Note the disparity within the range of values shown on the colour bar, from 10.3 to 1 300. The highest value (the dark red unit in the top left corner) is 100 times the size of the smallest one and is much larger than any of the others! The researcher also added some hits (the black spots) that show how well the values on the map match the corresponding values in the data set. The hits also show how the data is spread throughout the map. The following commands were used to display the hits:

```
h = som_hits(sM, sD); % create hits
som_show_add('hit',h,'Subplot',3); % display the hits on the 3rd map.
```

The proportion between the size of a map cell and the size of the associated hit reflects the proportion between the cell value on the map and the real rating value of the corresponding CDR in the data set. The bigger the dot, the closer the two values. For instance, the cell with the highest rating value has a hit that covers about half of the cell, implying that the real rating value of the corresponding CDR is twice as much as the value displayed on the map. The colour bar indicates that this value is equal to 1 300. Therefore, the corresponding value in the input file should be approximately equal to 2 600. This corresponds exactly to the outstanding rating value revealed from the statistical analysis mentioned earlier.

- Note that the topology of all the component maps is the same. Therefore, the cell at the top left of the Rating map (in dark red) corresponds to the same CDR as the cell in the same position on the Duration map. A strange pattern is that some of the calls with very long duration (in red on the Duration map) are also very inexpensive with a low rating (in blue on the Rating map). *This visualisation shows how quickly one can identify anomalies in the data*.
- In order to identify the call types and their distribution, the researcher generated an empty map using the call types as labels. Only the following call types appear on the map: international (i), shared call (s), MaxiCall (m), free calls (fr) and fax to email (fe). There are obviously other call types in the data set but only the most prevalent ones are displayed on the map. This shows that most of the calls are international, followed by Shared and Free Calls, exactly as revealed by the analysis in Excel. This added information also explains the strange results mentioned above. The calls with long duration and low rating are either shared calls or free calls, which is normal.

Based on the above results, the researcher generated two other labelled component maps for call duration and rating in order to find additional correlation patterns between the two fields. The calling areas were subsequently added on the duration map and the call types on the rating map. Figure 11.10 shows these two maps.

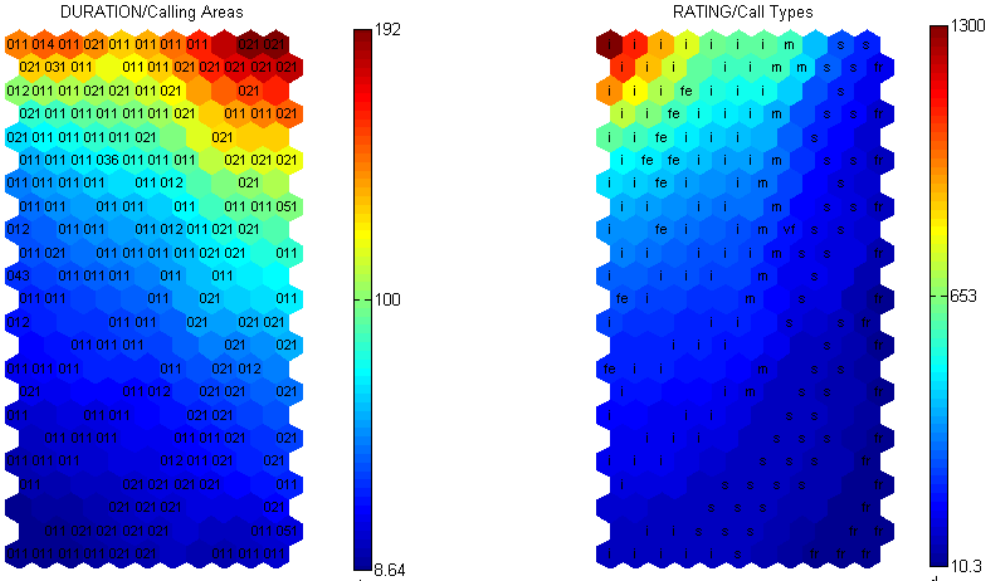

Figure 11.10: Duration and rating of calls based on calling area and call type

In Figure 11.10, the labels on the duration map show the most popular calling areas: Johannesburg (011) and Cape Town (021). Almost all the calls originate from these two cities. This is probably due to the fact that they are the main business cities in the country. The maps in Figure 11.10 also show an additional calling trend in the data set, which would have been hard to pick up from the statistical analysis. One can easily see that most of the Shared calls ("s") are from Cape Town (021) and that most of the international calls and faxes to email are from Johannesburg (011). *Such information could eventually be used to locate fraud areas.*

After generating maps for the whole data set, some service-specific maps were created to verify if the service profiles obtained from the SOM would match the profiles obtained with Excel. The researcher also looked for unusual trends indicative of fraud. In order to generate those maps, some other text files containing only data specific to each call type were created. Figure 11.11 shows the maps generated for international calls.

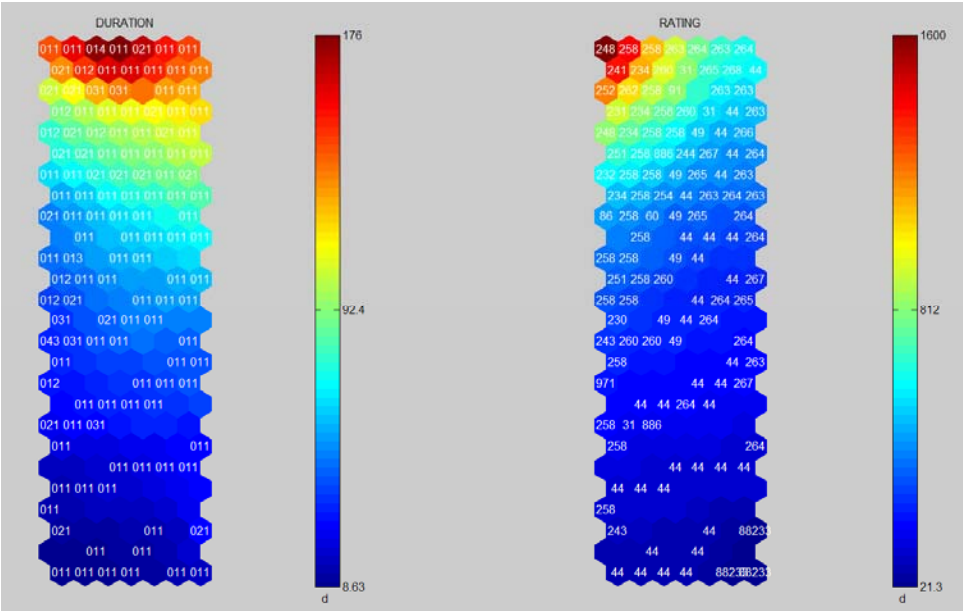

Figure 11.11: Duration and rating of international calls

Some interesting findings in the above maps are the following:

- A large number of the calls are to the UK (44), which corresponds to the results of the statistical analysis. Those calls mainly come from Johannesburg.
- Some long international calls are rather cheap (the top three rows of the maps, on the right-hand side of the maps), and this looks quite suspicious. However, a closer look reveals that they are to neighbouring countries, which is understandable. The calls were made to Zimbabwe (263), Namibia (264), Malawi (265), etc,, exactly as was revealed by the statistical analysis.

The researcher also generated a few maps from aggregate values that were obtained from a manual calculation in Excel. This was done in order to get different input fields and hopefully find other suspicious patterns. Some interesting results were obtained from the calculation of 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 maps are displayed in Figure 11.12.

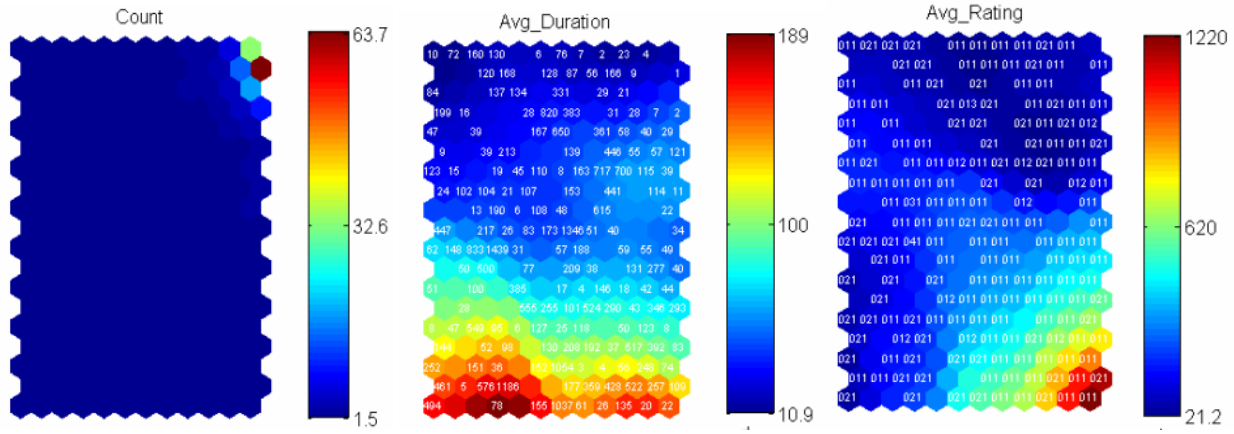

Figure 11.12: Count, average duration and rating of calls from each calling number

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

The first map is very uniform except for one outlier (the red cell), which really stands out. The outlier corresponds to calling number 1 (on the second map) and comes from Johannesburg (on the third map). The map shows a count of 1.5 for most of the calls and of 63.7 for the outlier. However, further manual analysis revealed that most of the calling numbers were used only once or twice (as shown on the map), but calling number 1 was used 229 times in just 4 minutes! Besides, all the calls from that number were made to the UK. This does not necessarily imply fraud, as all depends on the payment history of the corresponding subscriber and its usage profile. Some of the Telkom analysts suggested that this might indicate a telemarketing activity, since almost all the calls were very short (less than 20 s) and to different numbers (more than 100). These details were discovered when further analysis was done. *However, it shows how quickly one can identify outliers.*

After generating service-specific maps, the researcher proceeded to testing the scalability of the SOM.

11.4.2 Testing the SOM scalability

This section describes the second SOM analysis performed with a bigger data set to test the scalability of the algorithm.

The maps generated with the initial data set of 2 595 CDRs were all fairly accurate compared to the results obtained with Excel. The high density of the hits (on the Rating map in Figure 11.9), as well as their relatively big size (many of them cover a large portion of the associated cells), also showed that the values in the file were well distributed in the maps. Besides, the maps were all easily readable. This proved that the patterns displayed by the SOM were correct. However, it did not give any indication of the level of correctness of the SOM output in a real-life environment. Indeed, the 2 595 records were far from the few millions of CDRs that are usually generated daily on an operator's network. Therefore, the scalability of the SOM needed to be tested. To this end, the researcher requested another data set, much bigger than the first one.

Telkom gave two other Excel files: one file containing 84 750 CDRs all from Johannesburg, and another file containing 179 917 CDRs all from Limpopo, a rural province. All the calls were made between 11 AM and 2 PM (a peak-time period), on Monday, December 12, 2005. The researcher then merged the two files into one to obtain a bigger data set and got 264 667 CDRS. Although 264 667 CDRs are still 10 times less than the average 2 to 3 million CDRs produced daily on Telkom's network, it is much closer to a real-life scenario. Besides, as the SOM Analyser of the proposed architecture only processes CDRs for the same service type at regular intervals, it is unlikely to have to process millions of CDRs at the same time. The researcher therefore estimates that 264 667 CDRs represent a close value to the maximum number of CDRs that will need to be processed by the SOM at any given time.

The maps generated from the combined file did not reveal any suspicious activity. Nevertheless, it showed the low density of the hits, which in turn indicate a low distribution of the values in the input file. Only highly recurrent labels were displayed. Due to the limited readability of the labels, these maps are unfortunately not shown in this report. However, Figure 11.13 shows the maps that were created from the separate files for the calls from Johannesburg (011) and from Limpopo (015) as they revealed interesting features. A comparison between the maps from Johannesburg and the maps from Limpopo shows distinct calling trends in the two areas as summarised in Table 11.1. Note the low density of the hits on the Duration map for Johannesburg.

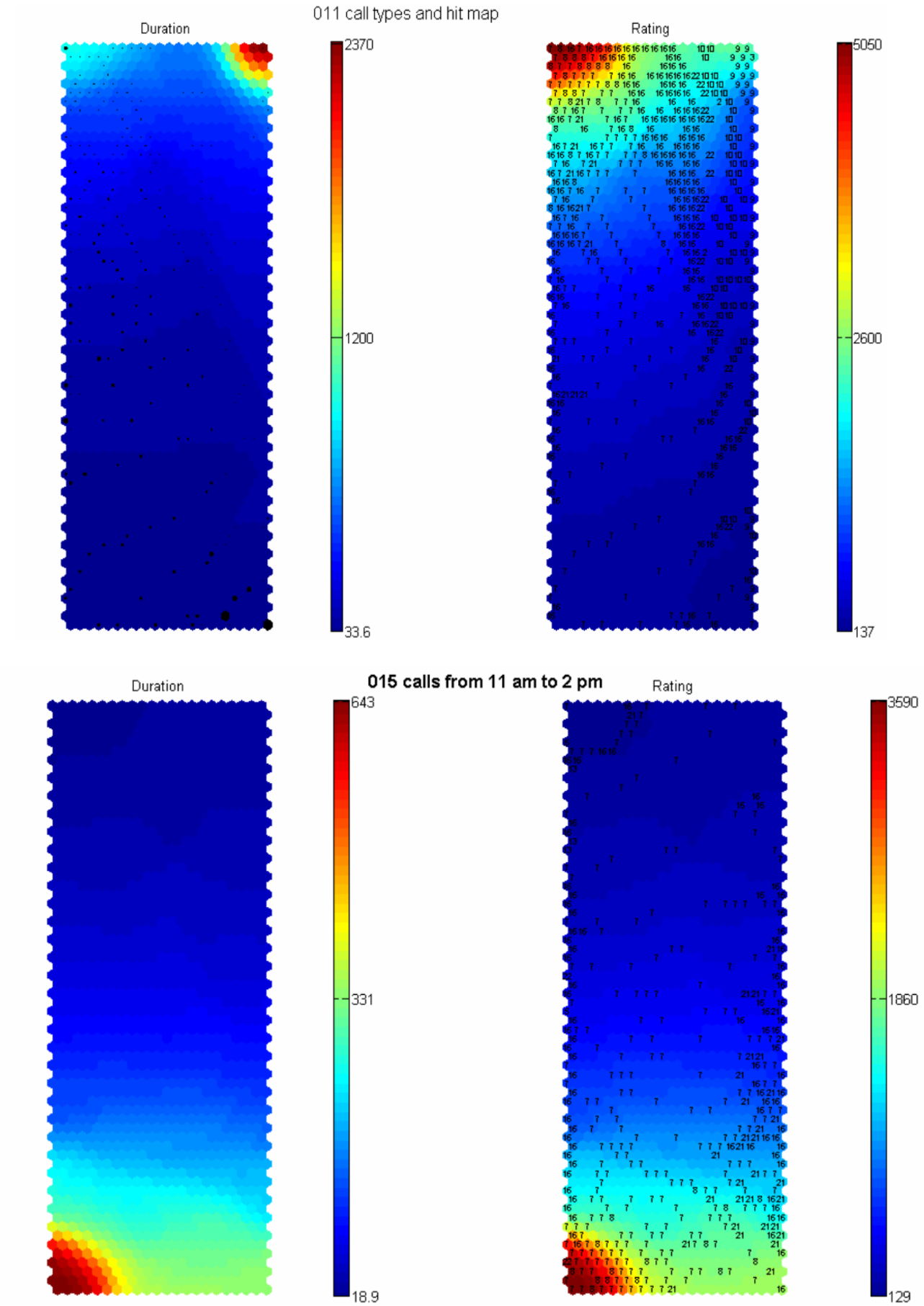

Figure 11.13: Duration, rating and types of calls from Johannesburg and Limpopo

Johannesburg	Limpopo
Duration scale	
between 33 s and 2370 s (≈39 min)	between 18.9 s and 643 s (≈10 min)
Median call duration	
1200 s (20 min)	331 s (≈ 5min)
Rating scale	
between 137 and 5050	between 129 and 3590
Median call rating	
2600	1860
Top 5 call types in order of prevalence	
- 16 (international call) - 7 (call to a Vodacom number) - 10 (0861 – MaxiCall) - 9 (0860 – shared call) - 22 (information line)	- 7 (call to a Vodacom number) - 16 (international call) - 21 (0866 – FaxToEmail) - 8 (call to an MTN number) - 13 (virtual Fax deposit)

Legend
Vodacom: largest mobile operator in South Africa
MTN: 2nd largest mobile operator in South Africa

Table 11.1: Comparison of call patterns from Johannesburg and from Limpopo

Although the maps do not show any suspicious calling pattern, they provide information useful for profiling. For example, unlike Limpopo, calls from Johannesburg are mainly business related (international calls, MaxiCalls, shared calls and calls to information lines). Another feature visible from the map and hard to determine with statistical analysis is that call duration and rating have almost exactly the same distribution in Limpopo (both maps have strikingly similar patterns). The SOM can therefore be used to profile each calling area and each call type. Any map displaying very different patterns from the normal profile can indicate that suspicious activity is going on. One example is the case where the duration and the rating of calls from Limpopo show very different patterns while they normally are almost exactly the same.

The last test that was performed was to evaluate the processing speed of the SOM. A description of this test is given in the following section.

11.4.3 Testing the SOM processing speed

The processing speed of the SOM was tested simultaneously with its scalability and the accuracy of its output map. In other words, as maps were generated with different input files, the researcher monitored the elapsed time between the reading of the file and the display of the map. The results are summarised as follows.

The maps created with the first data set of 2 595 CDRs were all generated within 5 seconds, i.e. almost instantaneously. The creation of service-specific maps was even quicker because fewer CDRs were in the corresponding input files. The quick processing speed was very promising, but the researcher suspected it was due to the small size of the input file.

The time required to process the second data set was observed next. The file containing 84 750 CDRs uniquely from Johannesburg took 29 seconds to train the SOM, and the other file with 179 917 CDRs from Limpopo took 110 seconds, which was still very quick. As explained in the previous section, the two files were then combined, which resulted in 264 667 CDRS. This required 8 minutes to train the SOM. As also discussed in the previous section, it was believed that 264 667 CDRs correspond well to the number of records that the SOM will have to process in one batch in a real-life environment. Consequently, the processing speed of 8 minutes is acceptable, given that there is a relatively long time interval between the SOM processing of consecutive CDR batches. The fraud analyst therefore has enough time to read and analyse a map before the next one is generated.

Section 11.4 described the prototype implementation of the SOM Analyser. The results of the prototyping are now discussed in the next section.

11.5 Discussion of the test results

This section examines the results of the prototype implementation described above. Firstly, the validity of the results is discussed in Section 11.5.1. Then Section 11.5.2 examines how well the SOM meets the required criteria tested in the experiment. Finally, the limits of the SOM processing discovered from the prototype implementation are explained in Section 11.5.3.

11.5.1 Validity of the test results

The results from the SOM testing have the advantage of being valid for a real-life environment for the following reasons:

- Real CDRs generated from real customer calls were used. Therefore, although biased, the call patterns revealed by the SOM reflect real usage patterns. Note that, as expected, the percentage of suspicious activity is very small compared to the normal usage patterns. Besides, suspicious activity detected by the SOM is not sufficient to ascertain that fraud occurred. Like in real-life, further analysis is required.

- The test data set (especially the second one) was large enough to provide valid results.
- The researcher worked with professional and experienced fraud analysts who confirmed the correctness of the results.

11.5.2 Advantages of the SOM processing

Although the SOM analysis that was performed did not actually detect any definite fraud attack, it provided some insight on its viability based on the following three requirements identified early in this chapter and tested during the prototype implementation:

- Accuracy: The accuracy of the SOM output was checked by first conducting an elementary statistical analysis of the test data with a familiar software application. Although not as accurate as the statistical analysis, the SOM output matched the statistical results. Using a SOM is therefore a valid method to get a correct overview of the patterns in the usage records.
- Scalability: The series of tests that was conducted showed that the SOM is capable of processing large volumes of CDRs. However, the bigger the input file, the less detailed the output maps. Only highly prevalent values are displayed on the maps. This nonetheless still provides a good overview of the trends in the input file and allows the quick identification of unusual usage patterns.
- Processing speed: The SOM proved to be fast, even for large input files. This ensures its viability for use in fraud detection, which is a time-critical operation.

In addition to the above advantages, the experiment demonstrated other benefits of using a SOM for fraud detection. These are discussed below.

- As mentioned in Chapter 9, the SOM is very visual. It enables one to visualise on a single map the correlation between many dimensions or parameters such as the duration, the rating, the call type and the calling area for a high number of CDRs. For instance, the SOM shows that calls from Johannesburg are usually short and inexpensive and that they are mostly either calls to the UK or local business calls (MaxiCalls and shared calls). Such a correlation is hard to display with statistical tests and impossible to define as a set of rules.
- The SOM assists in profiling by displaying trends in the data set. The displayed patterns can be used to define profiles for various types of entities such as a service type, a calling area or even a subscriber. Unlike statistical profiling, profiling with a SOM does not require any calculation and provides a good overview of the activities of one entity.

- The SOM enables the quick identification of suspicious or complex usage patterns that may indicate unknown fraud scenarios and may be used to define new fraud rules. For example, referring to Figure 11.12, in case the identified outlier was indeed a fraud attack, a new rule to detect the recurrence of such a fraud scenario could be defined, as shown in Figure 11.14. The fraud rule will be applied to a set of CDRs generated over a predefined time interval (e.g. 30 minutes) and rule parameters will be adjusted according to that interval. In Figure 11.14, fraud parameters are defined based on the 4-minute period in the test data.

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 min; frequency is 57/min, use 50/min as threshold.

Count of dialled numbers: number of dialled phone numbers; 100 different numbers were dialled from the same number, use 50 as threshold.

Figure 11.14: Fraud rule to detect new telemarketing scam

11.5.3 Limitations of the SOM processing

The main limitations of the SOM processing that were discovered from the prototype implementation are the following.

- Lack of accuracy: The values displayed by the SOM are not very accurate. Although it is possible to use hits to get an approximation of the correct values, determining the ratio between a hit and its associated map unit is not always straightforward, especially when the hit is very small. This is conducive to many estimation errors.
- SOM Toolbox not interactive and 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 (Eudaptics.com, 2006).
- Limited readability: When the map contains a large number of labels or when the labels are long words, they are not displayed properly and their readability is limited.

11.6 Conclusion

This chapter described in detail the prototype implementation of the SOM Analyser of the NGN FMS architecture designed in Chapter 10. The prototype was implemented to test the viability of using a SOM for fraud detection. The implementation used real call records obtained from Telkom and was conducted with a free add-on product of MATLAB, the SOM Toolbox. 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 FMS architecture proposed for NGN fraud detection. The next and final chapter summarises and concludes the dissertation.

Chapter 12: Conclusion

12.1 Introduction

This dissertation discussed the limitations of currently available FMSs with regard to NGNs and proposed an original FMS architecture to address these shortcomings. The key component of the architecture is the SOM Analyser that is used to identify previously unknown suspicious patterns by applying the SOM algorithm to the usage records. In the previous chapter, a prototype of that component was implemented to test the viability of using a SOM for fraud detection. The prototype implementation was the final step of the research. This chapter summarises the dissertation (Section 12.2), critically reviews the results of the research (Section 12.3) and discusses the possible direction of future research in NGN fraud detection (Section 12.4).

12.2 Research summary

The present dissertation addressed the problem of fraud detection in emerging IP-based NGNs. Due to the expected high value of new NGN services and the vulnerabilities of new networking technologies, fraud attacks perpetrated against telecommunication networks are likely to increase in NGNs. This security threat is exacerbated by the lack of adequate FMSs to effectively detect the new fraud scenarios. The main limitation of traditional FMSs is their application-specificity, which prevents them from accommodating new services and new fraud types. The goal of this research was therefore to design a new flexible FMS architecture capable of handling new NGN services and of effectively detecting their associated fraud types. In order to design such an architecture, the following steps were taken:

- Analysis of the likely evolution of fraud in NGNs to examine how NGN fraud scenarios could affect current fraud detection processes. This was based on the analysis of the security vulnerabilities of NGNs and on the review of current fraud types prone to be affected by new NGN business models and services.
- Identification of the most appropriate sources of input data to the FMS, in other words data that will provide all the information necessary to detect the identified NGN fraud types. To this end, a critical review of traditional billing systems was conducted, as they are the main source of input data of current FMSs. The format and the content of billing records used for traditional telecommunication services were examined and a suitable billing standard for IP-based services – the IPDR standard – was selected.

- Identification of suitable fraud detection techniques for NGNs based on a review of techniques currently used in commercial FMSs. The two techniques selected were rule-based analysis to detect known fraud patterns and Self-Organising Maps, a type of unsupervised neural network, to discover unknown fraud scenarios.
- Design of the NGN FMS architecture, based on the outcome of the previous phases.
- Prototype implementation of the SOM Analyser component of the proposed architecture to test the viability of using a SOM for identifying suspicious activity. The prototype implementation used real customer records provided by Telkom, a major fixed-line operator in South Africa.

The proposed FMS architecture described in Chapter 10 follows a 4-step fraud detection process, whereby the IPDRs from the billing system are first compared to log files of an Intrusion Detection System (IDS), then analysed with fraud rules, and finally processed with a SOM. The rule-based analysis is performed in two steps. Firstly, general fraud rules applicable to all services offered by the operator are applied to the records and then service-specific fraud rules associated with each type of service are used. Each of the four steps is performed by a different module. The architecture also has a module for handling fraud alarms so as to notify the fraud analyst of suspicious activities and a Case Manager to query various systems to obtain more information about a suspected fraud case.

The proposed modular architecture boosts a high level of flexibility as it can accommodate any type of service. Modules for service-specific rule-based fraud detection can be added or removed as needed. The prototype implementation addressed the SOM analysis of the FMS and showed that it was a viable method to detect previously unknown suspicious usage patterns.

12.3 Review of the research outcome

This section reviews the outcome of the research. Section 12.3.1 examines how well the problem stated in Chapter 1 was solved and Section 12.3.2 elaborates on the contributions to the field of fraud detection made by the results of the study.

12.3.1 Solutions to the problem statement

The steps mentioned in Section 12.1 above were performed to answer the various questions that constituted the problem statement defined in Section 1.2 in the first chapter. Based on the outcome

of the research, it is now possible to answer these questions to determine how well the problem addressed by the research was solved.

12.3.1.1 What is the likely evolution of fraud in NGNs?

The research has determined that many of the current fraud types perpetrated on traditional telecommunication networks will still be committed in NGNs as long as their associated services are still offered. In addition to old fraud types, new fraud scenarios targeting service content such as multimedia content will emerge. Likely new fraud types are listed below:

- Illegal redistribution of service
- Unauthorised access to resources
- Overcharging
- Excess download
- Money laundering

Note that the identified fraud types are not dependent on any specific service or application.

12.3.1.2 What is (are) the most suitable source(s) of information for an FMS for NGNs?

This question was broken up into the following three sub-questions.

- **Which information is required to detect NGN fraud?**

Customer usage records generated for billing purposes, as well as entries from an IDS, were identified as necessary for detecting NGN fraud attacks. Combining billing records' information with IDS logs was required to provide a good coverage of the data flowing through the network.

- **In which format should fraud-detection information be provided?**

The billing records should be provided in the IPDR format, an emerging billing standard specifically designed for IP-based services. The key quality of the IPDR standard is its high level of flexibility that allows for it to be used for recording any type of service, including traditional telecommunication services and new IP services.

- **How should fraud-detection information be collected by the FMS?**

The IPDR standard enables the transmission of IPDR records in real time from the billing system to other systems, including the FMS. Real-time collection of billing records by the FMS is therefore the preferred transmission method for obvious reasons. However, the FMS should also allow the collection of billing records in batch mode to cater for fraud types that can only be identified after the examination of a series of billing records over a specified time frame (e.g. call selling).

12.3.1.3 Which data analysis technique(s) is (are) required for detecting NGN fraud?

Two complementary approaches to fraud detection were selected: absolute analysis and differential analysis. Differential analysis was implemented with rule-based analysis to detect known fraud scenarios. The Self-Organising Map algorithm was used for absolute analysis. The SOM was used to assist in the detection of unknown NGN fraud scenarios.

It can now be stated that the problem defined in Chapter 1 has been solved, since answers to all the above questions have been provided by the results of the research. However, it is not possible to guarantee the effectiveness of the proposed architecture and all its features, since the viability of only one component (the SOM Analyser) has been tested. The author's choice of the input data source, contents and format, as well as the flow of the different data analysis processes cannot be confirmed as effective unless a prototype for the complete architecture is implemented. Nevertheless, it can be argued that the results of the research provided various contributions to the field of NGN fraud detection as explained next.

12.3.2 Research contributions

The main contributions of the research are the analysis of the likely evolution of fraud in NGNs, the design of a new NGN FMS architecture and the publication of several papers.

12.3.2.1 Analysis of the likely evolution of fraud in NGNs

The study provided a thorough analysis of likely NGN fraud trends. Cases for some of the NGN fraud types described in the dissertation have already been reported while others still belong to the domain of fiction. However, the patterns described give a good indication of where the serious fraud threats lie. This information can be used to tighten the security features of the targeted services to prevent considerable financial loss due to fraud attacks. One example is to use strong encryption mechanisms to prevent the illegal copying and distribution of multimedia content.

12.3.2.2 Design of a new FMS architecture

A new FMS architecture was designed. Although some of the features of the architecture are derived from previous work in IP fraud detection, the overall architecture design is completely original. Its main novelty is the inclusion of the SOM algorithm to help uncover new fraud patterns and its interaction with other components in the architecture. The SOM is implemented in the SOM Analyser, which receives input data from Service-specific Fraud Detector modules. Results of the

SOM analysis are sent back to the Service-specific Fraud Detectors to define rules for new fraud scenarios and to create profiles for average service usage. Although the SOM algorithm is not new, it has not been used in the field of telecommunication fraud detection and it is not available in commercial FMSs. As the prototype implemented in Chapter 11 demonstrated the viability of the SOM analysis, commercial FMSs could benefit from incorporating this technique in their functionality.

12.3.2.3 Published papers

Results of the research have been published in the following peer-reviewed papers:

Bihina Bella, M.A., Olivier, M.S. and Eloff J.H.P. *A Fraud Management Framework for Next-Generation Networks*. Refereed poster and paper in Proceedings of the South African Institute of Computer Scientists and Information Technologists (SAICSIT) 2005 conference, 20-22 September 2005, White River, South Africa.

Bihina Bella, M.A., Olivier, M.S. and Eloff J.H.P. *A fraud detection model for Next-Generation Networks*. In Proceedings of the 8th Southern African Telecommunications Networks and Applications Conference (SATNAC 2005), 11-14 September 2005, Central Drakensberg, South Africa.

Bihina Bella, M. and Johnson, M. *VoIP and fraud*. African telecoms billing and revenue management conference (IIR telecoms & technology), 05-09 September 2005, Cape Town, South Africa.

Bihina Bella, M.A., Olivier, M.S. and Eloff J.H.P. *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, 29 June-1 July 2005, Sandton, South Africa.

Bihina Bella, M. and Johnson, M. *NGN services and fraud*. Telecoms fraud – Africa conference (IIR telecoms & technology), 24-26 May 2005, Cape Town, South Africa.

Bihina Bella, M.A., Olivier, M.S. and Eloff J.H.P. *Requirements for Next-Generation Network billing systems*. Work-in-progress paper. In Proceedings of the 7th Southern African

Telecommunications Networks and Applications Conference (SATNAC 2004), 6-8 September 2004, Cape Town, South Africa.

12.4 Conclusion and future work

This chapter reviewed the results of the research conducted in the present dissertation, namely the design of an NGN FMS architecture and the prototype implementation of its SOM Analyser component. Areas for improvement include the implementation of a complete prototype to test the viability of the entire FMS architecture.

A potential avenue for future work is the investigation of more appropriate sources of input data for the FMS as the research revealed that it was one area neglected by previous researchers and that it had a strong impact on the quality of the FMS output. The current dissertation suggests the extraction of usage records from the billing system as it contains most of the information required for fraud detection, including service usage charges. Besides, this information is presented in a standard format. However, using usage records directly from the recording network devices seems a faster solution, which allows true real-time fraud detection. The downside to this approach is the raw format of records generated by the network devices and their lack of knowledge about service rates. This was visible in the test data set obtained from Telkom. The usage records were produced by an SS7 gateway and had no real rating. Only approximate rating values with no unit were included in the records. This information is however of crucial importance for an FMS whose main functionality is to reduce revenue leakage. A possibility that was mentioned in Chapter 6 and that needs further research is to implement rating on the network devices.

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 has proved very effective and other methods to display service usage patterns can also be beneficial to detect known 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

ABRAMOWICZ, D. & LEDBERG, P. 01 December 2002. *IP fraud – Methods and algorithms for detecting IP-based fraud*. MSc thesis. Swedish Royal Institute of Technology, Göteborg, Sweden.

AIRDEFENSE. 10 May 2005. "AirDefense Discovers New Version of "Evil Twin" Attack at Interop 2005". AirDefense press release. http://www.airdefense.net/newsandpress/05_10_05.shtm. Accessed: 13 February 2006.

ALJIFRI, H. & NAVARRO, D.S. 2004. Search engines and privacy. *Computers & Security*, vol. 23, pp. 379-388.

AMAT, J. 2003. Charging data collection: the key to revenue generation. *Alcatel telecommunications review*, 3rd Quarter 2003, pp. 1-5.

APACHE. 2006. Apache website home page. www.apache.org. Accessed : 11 April 2006.

ARVIDSON, M. & CARLBARK, M. 25 February 2003. *Intrusion Detection Systems – Technologies, Weaknesses and Trends*. Licentiate thesis. Department of Electrical Engineering, Linköping University, Stockholm, Sweden.

ASSOCIATED PRESS. 30 May 2004. Security-Free Wireless Networks. *Wired News* article. http://www.wired.com/news/wireless/0,1382,63667,00.html. Accessed: 11 February 2006.

ATIS – Alliance for Telecommunications Industry Solutions. 2004. "ATIS Publishes Exchange Message Interface Guidelines". ATIS press release. http://www.atis.org/PRESS/pressreleases2004/022704b.htm. Accessed: 30 March 2005.

AXELSSON S. March 2000. *Intrusion Detection Systems: A Taxomomy and Survey*. Technical Report No 99-15, Department of Computer Engineering, Chalmers University of Technology, Sweden.

AZURE SOLUTIONS. 2006. "Fraud Control". Product information. http://www.azuresolutions.co.uk/fraud_control.asp?id=611&sec_id=222. Accessed: 13 February 2006.

BAUMGARTNER, J. 01 March 2002. Network evolution: the ties that bind. *Communications Engineering & Design Magazine,* March 2002 issue, electronic version. http://www.cedmagazine.com/ced/2002/0302/03b.htm. Accessed: 07 June 2004.

BEAL, V. 21 January 2005. "All about phishing". Webopedia online dictionary article. http://www.webopedia.com/DidYouKnow/Internet/2005/phishing.asp. Accessed: 27 June 2005.

BECK COMPUTER SYSTEMS. 2004. "Breaking the back of telephone fraud". CTO (Commonwealth Telecommunications Organisation) article. http://www.cto-ict.org/index.php?dir=04&sd=30&aid=1020. Accessed: 12 April 2004.

BIBA, E. 15 March 2005. "Does your Wi-Fi Hotspot Have an Evil Twin?". *PC World Magazine*, online article. http://pcworld.about.com/news/Mar152005id120054.htm. Accessed: 10 February 2006.

BISCAIA H, ALEXIOU S, PAVON F, HULTHEN R. 2002. Do intelligent techniques aid fraud detection? *EURESCOM Mess@ge*, vol. March 2002, issue. 1, pp. 17-19.

BORTHICK. S. August 2001. Call accounting and billing for IP services. *Business Communications Review*, vol. 31, issue 8 – Aug 2001, pp. 28-33.

BRAD, O. 2001. Cyber Crime: How Technology Makes It Easy and What to Do About It. *Information Systems Security*, vol. 9, issue 6, Jan/Feb2001, pp. 45-51.

BRADBURY, D. September 2006. Going, going, gone. *Digital Investigation*, vol.3, issue 3, pp. 112-114.

BURGE, P., SHAWE-TAYLOR, J., COOKE, C., MOREAU, Y., PRENEEL, B. & STOERMANN, C. 1997. Fraud detection and management in mobile telecommunications networks. *Proceedings: European Conference on Security and Detection ECOS 97*, pp. 91-96, London, UK, 28-30 April 1997.

CAHILL, M.H., LAMBERT, D., PINHEIRO, J.C. & SUN, D.X. 2002. "Detecting Fraud in The Real World". In *Handbook of massive data sets.* Edited by J. Abello, P.M. Pardalos and M.G.C. Resende. Kluwer Academic Publishers, Norwell, MA, USA (2002), pp. 911–929.

CAUDILL, M. & BUTLER, C. 1992. *Understanding Neural Networks – Computer explorations, Volume 1: Basic Networks*. A Bradford Book, the MIT Press, Massachussetts Institute of Technology.

CEREBRUS SOLUTIONS. November 2002b. "Neural Network Primer", issue 2.2. Cerebrus Solutions white paper. http://www.home.agilent.com/. Accessed: 22 April 2005.

CEREBRUS SOLUTIONS. November 2002c. "Fraud Primer", issue 2.3. Cerebrus Solutions white paper: http://www.home.agilent.com/. Accessed: 13 April 2005.

CFCA. March 2003. "Communications Fraud Control Association (CFCA) announces results of worldwide telecom fraud survey". CFCA press release. http://cfca.org/pressrelease/FraudLoss%20%20press%20release%203-03.doc. Access: 8 May 2004.

CHEN, D.R., CHANG, R.F. & HUANG, Y.L. 2000. Breast cancer diagnosis using self-organizing map for sonography. *Ultrasound in Medicine and Biology*, vol. 1, no. 26, pp. 405-411.

CIBERNET. 2006. "CIBER records". Product information. http://www.cibernet.com/clearing/ciber.htm. Accessed: 26 February 2007.

CIS. 2006. "SOM Toolbox 2.0". Product information. http://www.cis.hut.fi/projects/somtoolbox. Accessed: 31 July 2006.

CODEGODS.NET. 2005. "CIDMage. Caller ID generator/analyst". Product information. http://codegods.net/cidmage/cidmage1.htm. Accessed: 14 November 2005.

COLLINS, M. 1999. Telecommunications crime – Part 1. *Computers & Security*, vol. 18, pp. 577-586.

CORTES, C. & PREGIBON, D. July 2001. Signature-Based Methods for Data Streams. *Data Mining and Knowledge Discovery*, vol. 5, issue 3, pp. 167-182.

COTTON, S. 25 August 2006. "IPDR/Streaming protocol specification" - Version 2.2. IPDR.org technical specification document. http://www.ipdr.org/public/DocumentMap/SP2.2.pdf. Accessed: 26 February 2007.

COTTON, S. November 2004. "Document map and overview" - Version 3.5.0.1. IPDR.org technical report. http://www.ipdr.org/public/DocumentMap/DMO3.5.0.1.pdf. Accessed: 4 April 2005.

DEBAR H., DACIER M. & WESPI A. 1999. Towards a taxonomy of intrusion-detection systems. *Computer Networks*, vol. 31, issue 8, pp. 805-822.

DENIS, C., JENKINSON, M., WEBER, M. & ZHAO, H. 09 December 2002. "IPDR Organization Presents NDM-U to UN International Telecommunications Union". IPDR.org press release. http://www.ipdr.org/news/releases/300400.html. Accessed: 04 April 2005.

DUNHAM, K. 2004. Phishing Isn't So Sophisticated: Scary! *Information Systems Security*, May/June 2004, vol. 13, issue 2, pp.2-7.

DWAN, B. December 2000. The Computer Virus — From There to Here: An Historical Perspective. *Computer Fraud & Security*, vol. 2000, issue 12, pp.13-16.

DWAN, B. March 2004. The Malapropisms of Malware. *Computer Fraud & Security*, vol. 2004, issue 3, pp. 13-16.

ELOFF, J.H.P. & GRANOVA, A. 2005. A legal overview of phishing. *Computer Fraud & Security*, vol. 2005, issue 7, July 2005, pp. 6-11.

ENGELBRECHT, A.P. 2003. *Computational Intelligence: An Introduction*. John Wiley & Sons, Ltd.

ENTRUST. 01 April 2005. "Phishing is yesterday's news – Get ready for pharming". Bitpipe white paper. http://www.bitpipe.com/data/detail?id=1115137448_814&type=RES&src=KA_R. Accessed: 20 May 2005.

ERICSSON. 2004. "Categorising telecommunications fraud – an introduction for those new to the subject". CTO (Commonwealth Telecommunications Organisation) article. http://www.cto-ict.org/index.php?dir=04&sd=30&aid=1018. Accessed: 07 March 2004.

ETSI – European Telecommunications Standards Institute. 24 August 2000. "ETSI TS 101 321 v2.1.1 - Telecommunications and Internet Protocol Harmonization over networks (TIPHON): Open Settlement Protocol (OSP) for inter-domain pricing, authorization, and usage exchange". ETSI technical specification document. http://pda.etsi.org/pda/queryform.asp. Accessed: 27 February 2007.

EUDAPTICS.COM. 2006. "Viscovery® SOMine® - Self-Organizing Maps". Product information. http://www.somine.info/. Accessed: 02 August 2006.

EURESCOM. 2002. "P1007: Application of Intelligent Techniques to Telecommunications Fraud Detection". Project information. http://www.eurescom.de/public/projects/P1000-series/P1007/. Accessed: 16 February 2006.

FALSHAW, P. 2001. Next generation networks and services. *Proceedings: PTC2001, the Pacific Telecommunications Council*, Honolulu, Hawaii, 15-17 January 2001.

FAUSETT, L. 1994. *Fundamentals of neural networks – Architectures, algorithms, and applications*. Prentice Hall.

FITCHARD, K. 23 July 2001. Exposed to infection. *Telephony Online* magazine, July 23, 2001 issue. http://telephonyonline.com/mag/telecom_exposed_infection/. Accessed: 11 February 2006.

FOWLER M and SCOTT K. 2000. *UML Distilled: A Brief Guide to the Standard Object Modeling Language (2nd Edition)*. Addison-Wesley.

FURNELL, S. July 2005. Internet threats to end-users: Hunting easy prey. *Network Security*, vol. 2005, issue 7, pp. 5-9.

GAO. 27 July 1999. Telecommunications: State and Federal Actions to Curb Slamming and Cramming: RCED-99-193. GAO (US General Accounting Office) technical report.

GENTRY, M. 2001. "Next-generation networks and the Defense Department's command, control, communications, computers, intelligence, surveillance and reconnaissance abilities". *Army Communicator* magazine, Spring 2001 edition, vol. 26, no.1. http://www.gordon.army.mil/AC/Spring/Spring%2001/NEXTGEN.HTM. Accessed: 07 June 2004.

GESSNER, T. 12 October 2004. "ATIS and IPDR.org to Coordinate Efforts for Data Interchange Standards". IPDR.org press release. http://www.ipdr.org/news/releases/310400.htm. Accessed: 04 April 2005.

GILLWALD, A. July 2003. National convergence policy in a globalised world: preparing South Africa for next generation networks, services and regulation. *Policy Research Paper No 4, LINK Centre,* Graduate School of Public and Development Management, University of Witwatersrand, Johannesburg, South Africa.

GOLDSTEIN, M. November 2005. Better Safe Than Sorry. *Sales & Marketing Management*, vol. 157, issue 11, p23.

GROSSMAN, W. M. 1 January 1998. *Net.Wars*. New York University Press.

GULLSTRAND, P. 2005. "Tapping the potential of roaming". GSM WORLD article. http://www.gsmworld.com/using/billing/potential.shtml. Accessed: 30 March 2005.

GULYANI, M. & GAUTIER, Y. 16 September 2003. Network evolution: network domain layer convergence. *Alcatel Telecommunications review* – 3rd Quarter 2003.

HACKERSCATALOG.COM. 2005. "Hacking software CD-ROM Index". Product information. http://www.hackerscatalog.com/Products/CD-ROM_Index/index.html. Accessed: 05 September 2005.

HALL, P., DELANEY, J. & HOLMES, J. 2000. "Next-generation services: impacts on the industry and markets". *Telecommunications Development, Asia-Pacific,* Internet Networks and Services series.

HANRAHAN, H. 2002. Convergence, digitization and new technologies: towards the Next Generation Network. *The Southern African Journal of Information and Communications,* vol. 2, no. 1, LINK Centre, Graduate School of Public and Development Management, University of Witwatersrand, Johannesburg, South Africa.

HEARNE, S. August 2004. *A Fraud Detection Framework for Next-Generation Telecommunications Networks*. MSc thesis, Telecommunications Software & Systems Group, Waterford Institute of Technology, Ireland.

HEINTZ, A. 2002. "IPDR.org: standardizing next-generation accounting". IPDR.org company information. http://www.itu.int/itudoc/itu-t/ifs/072003/pres_org/ipdr.html. Accessed: 25 February 2005.

HINDE, S. 2004. Spyware: the spy in the computer. *Computer Fraud & Security*, vol. 2004, issue 12, December 2004, pp. 15-16.

HOATH, P. 1998. Telecoms fraud, the gory details. *Computer Fraud & Security.* January 1998, pp. 10-14.

HOLLMEN, J. December 2000. *User profiling and classification for fraud detection in mobile communication networks*. PhD thesis, Laboratory of Computer and Information Science, Department of Computer Science and Engineering, Helsinki University of Technology, Finland.

HORAL, M. 2000. *Fraud detection in IP multicast applications.* MSc thesis. Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden.

HP – HEWLETT-PACKARD. 2003. "Fraud Management System (FMS)". Product information. http://h71028.www7.hp.com/enterprise/downloads/HP_FraudMgmtSol_SB_9-02-03.pdf. Accessed: 15 June 2006.

HP – HEWLETT-PACKARD. 2005. "Practical Wi-Fi security". HP IT guide white paper. http://www.hp.com/sbso/productivity/howto/it_wifisecurity/it_wifisecurity.pdf. Accessed: 27 January 2006.

HSU, C. March 2006. Generalizing Self-organizing Map for Categorical Data. *IEEE Transactions on Neural Networks*, vol. 17, no. 2.

HUITEMA, C. 1999. Challenges of the next generation networks. *Keynote for MIC'99* - First IEEE/POPOV Joint Conference on Internet Technologies and Services, Moscow, Russia, October 25-28.

HYNNINEN, J. 2001. Experiences in Mobile Phone fraud. Seminar on Network Security, Department of Computer Science and Engineering. Helsinki University of Technology, Finland.

IBBETT, G. January 2007. Top Telco Frauds and How to Stop them. *Billing world and OSS today* magazine, 2007 edition, issue 1, electronic version. http://www.billingworld.com/secondary.cfm?page=detail&archiveId=7824. Accessed: 05 March 2007.

IEC – The International Engineering Consortium. 2004a. Billing in a 3G environment. *Web ProForums* White Paper tutorial. http://www.iec.org/tutorials/billing_3g/topic03.html. Accessed: 07 May 2004.

IEC – The International Engineering Consortium. 2004b. Fraud analysis in IP and Next-Generation Networks. *Web ProForums* White Paper tutorial. http://www.iec.org/tutorials/fraud_analysis/. Accessed: 07 May 2004.

IEC – The International Engineering Consortium. 2004c. Telephony billing. *Web ProForums* White Paper tutorial. http://www.iec.org/online/tutorials/tele_bill/. Accessed: 07 May 2004.

INTEL. 2001. "An introduction to Next-Generation Network Services: the next big opportunity on the web". Intel white paper. http://www.intel.com/network/csp/resources/white_papers/6942web.htm. Accessed: 01 June 2004.

INTEL. 2002. "Modular network voice building blocks". Intel white paper. http://www.intel.com/network/csp/pdf/7299.pdf. Accessed: 01 June 2004.

IPDR.ORG. 1 August 2002. "ATIS's Ordering and Billing Forum and IPDR.org Join Forces to Map IPDR, EMI Billing Records". IPDR.org press release. http://www.ipdr.org/news/releases/290100.html. Accessed: 04 April 2005.

IPDR.ORG. 2004a. "Member list". IPDR.org company information. http://www.ipdr.org/member-list/charter.html. Accessed: 02 January 2006.

IPDR.ORG. November 2004b. "IPDR/XML file encoding format - Version 3.5.01". Technical specification document. http://www.ipdr.org/public/DocumentMap/XML3.5.0.1.pdf. Accessed: 04 April 2005.

IPDR.ORG. November 2004c. "IPDR business solution requirements – Network data management-usage (NDM-U) -Version 3.5.01". Technical specification document. http://www.ipdr.org/public/DocumentMap/BSR-NDM-U3.5.0.1.pdf. Accessed: 06 June 2004.

IPDR.ORG. November 2004d. "IPDR/File Transfer Protocol - ersion 3.5.0.1". Technical specification document. http://www.ipdr.org/public/DocumentMap/File3.5.0.1.pdf. Accessed: 01 April 2004.

IPDR.ORG . 2005a. "IPDR Compliant™ Program". IPDR.org company information. http://www.ipdr.org/compliant-program/index.html. Accessed: 03 January 2006.

IPDR.ORG. 2005b. "Working groups". IPDR.org company information. http://www.ipdr.org/working-groups/index.html. Accessed: 02 January 2006.

ITU – International Telecommunications Union. 03 March 2004. "NGN working definition". Next Generation Networks (NGN) 2004 Project information.

http://www.itu.int/ITU-T/studygroups/com13/ngn2004/working_definition.html. Accessed: 14 June 2004.

ISAAC – Internet Security, Applications, Authentication, and Cryptography. 2004. "GSM Cloning". Press release. *Computer Science Division, University of California, Berkeley, USA.* http://www.isaac.cs.berkeley.edu/isaac/gsm.html. Accessed: 03 March 2004.

JACKSON, P. 1990. *Introduction to Expert Systems – Second edition*. Addison-Wesley Publishing Company.

JACOBS, R. 2004. "Telecommunications fraud". Dimension Data white paper. http://www.dimensiondata.com/NR/rdonlyres/85DC1F7A-0B17-4A87-84F9-328ACF33A670/409/TelecommunicationsFraudWhitePaper1.pdf. Accessed: 07 May 2004.

JENAMANI, M., ZHONG, Y. & BHARGAVA, B. 2007. Cheating in online auction – Towards explaining the popularity of English auction. *Electronic Commerce Research and Applications*, vol.6, issue 1, pp. 53 – 62.

JENKINSON, M. 03 December 2003. "New Standard Enables Wi-Fi® Roaming Cash Flow". IPDR.org press release. http://www.ipdr.org/news/releases/310100.htm. Accessed: 04 April 2005.

JENKINSON, M. 10 January 2005a. "CableLabs® Mandates IPDR Streaming". IPDR.org press release. http://www.ipdr.org/news/releases/310500.htm. Accessed: 04 April 2005.

JENKINSON, M. 08 November 2005b. "IPDR.org Collaborates with TeleManagement Forum in Catalyst Industry Initiative". IPDR.org press release. http://www.ipdr.org/news/releases/310800.htm. Accessed: 02 January 2006.

JOHNSON, J.L., MILLER, M.L., MULLER, S., MORGAN, S. & FANFLIK, P.L. September 2004. "If it sounds too good to be true – local prosecutors' experiences in fighting telecommunications fraud". *APRI (American Prosecutors Research Institute) Special Topics Series,* report in White Collar Crimes series.

JOHNSON, M. January 2002a. "Future Frauds: Telecom fraud in Next Generation Services". CTO (Commonwealth Telecommunications Organisation) article. http://www.cto-ict.org/index.php?dir=04&sd=30&aid=1012. Accessed: 12 April 2005.

JOHNSON, M. October 2002b. "Revenue assurance, fraud and security in pre-paid 3G services". Visual Wireless White Paper.

KARLSSON, C. 3 January 2001. *Methods for intrusion and fraud detection in IP-based multimedia services*. MSc thesis. Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden.

KASKI, S., SINKKONEN, J. & PELTONEN, J. July 2001. Bankruptcy analysis with self organizing maps in learning metrics. *IEEE Transactions on Neural Networks*, vol.12, no. 4, pp. 936-947.

KOHONEN, T. 1999. Analysis of processes and large data sets by a self-organizing method. *Proceedings: Second International Conference on Intelligent Processing and Manufacturing of Materials IPMM'99,* Honolulu, Hawaii, 10 -15 July 1999.

KOU, Y., LU, T., SIRWONGWATTANA, S. March 2004. Survey of fraud detection techniques. *Proceedings: 2004 IEEE International conference on Networking, Sensing and Control,* Taipei, Taiwan, 21-23 March 2004.

KROGFOSS, B. & PIROT, J. 2001. Next generation networks: enablers for new business models. *Alcatel Telecommunications Review,* 2nd Quarter 2001, pp. 91-93.

KVARNSTROM, H., LUNDIN, E. & JONSSON, E. 2000. Combining fraud and intrusion detection – meeting new requirements. *Proceedings of the fifth Nordic Workshop on Secure IT Systems (NordSec),* Reykjavik, Iceland, October 12-13, 2000.

LAMPARTER, B. & WESTHOFF, D. 2002. Security challenges in the future mobile Internet. *PAMPAS'02: Workshop on Requirements for Mobile Privacy & Security*, Royal Holloway, University of London, UK, September 16 - 17, 2002.

LUCAS, M. October 2004. Where rating should be implemented? *Billing world and OSS today* magazine, 2005 edition, issue 10, electronic version. http://www.billingworld.com/rev2/portal/main/search.cfm. Accessed: 24 March 2005.

LUCAS, J. February 2005. ISS Meets IPDR. *Billing world and OSS today* magazine, edition 2005, issue 2, Editorial, electronic version. http://www.billingworld.com/rev2/portal/main/search.cfm. Accessed: 29 March 2005.

LUNDIN, E. 2002. *Aspects of employing fraud and intrusion detection systems.* Licentiate thesis. Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden.

MARSHALL, S. 1 April 2002. "Locking out the intruders – Special Report: Next-Generation fraud". *CommunicationsWeek International* journal, April 1, 2002 issue, electronic version. http://findarticles.com/p/articles/mi_m0UKG/is_2002_April_1/ai_85368014. Accessed: 02 June 2004.

MATHWORKS.COM. 2006. "MATLAB". http://www.mathworks.com/products/matlab/. Product information. Accessed: 31 July 2006.

MELAMED, H. September 2005. The Rise And Fall Of Centrex Services. *Internet Telephony* Magazine, September 2005 issue, feature article, electronic version. http://www.tmcnet.com/voip/0905/featurearticle-rise-and-fall-of-centrex.htm. Accessed: 28 February 2007.

MEYER, H. June 1997. Telecoms fraud in the cellular market: how much is hype and how much is real? *Computer Fraud & Security*, vol. 1997, issue 6, pp. 11-14.

MODARESSI, A., R. & MOHAN, S. 2000. Control and Management in Next-Generation Networks: challenges and opportunities. *IEEE Communications Magazine,* vol. 38, issue 10, October 2000, pp. 94-102.

MOGAKI, I. 17 January 2005. "Network fraud still costs Telkom millions". ITWeb article. http://www.itweb.co.za/sections/telecoms/2005/0501171201.asp?S=Legal%20View&A=LEG&O=TE. Accessed: 22 November 2005.

MOREAU, Y., PRENEEL, B., BURGE, P., SHAWE-TAYLOR, J., STOERMANN, C. & COOKE, C. 1996. Novel techniques for fraud detection in mobile telecommunication networks. *Proceedings: ACTS (Advanced Communications Technologies and Services) Mobile Summit,* Grenada, Spain, 27-29 November 1996.

MYSQL. 2006. Website: http://www.mysql.com/products/. Product information. Accessed: 24 April 2006.

NATIONMASTER.COM. 24 June 2005. "Encyclopedia: Internet fraud". http://www.nationmaster.com/encyclopedia/Internet-fraud. Accessed: 27 June 2005.

NEXUS TELECOM. 2004. "Next-Generation Networks: billing challenges". Product information. http://www.nexus-ag.com/billing.0.html. Accessed: 01 June 2004.

NTIA – National Telecommunications and Information Administration. 2004. "Technical and Economic Assessment of Internet Protocol Version 6 (IPv6): Glossary". http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/draft/draftglossary.htm. Accessed: 04 May 2005.

OIF – Optical Internetworking Forum. 2 April 2002. "Call detail records for UNI 1.0 billing". Technical specification document. http://www.oiforum.com/public/documents/OIF-CDR-01.0.pdf. Accessed: 04 March 2005.

OFRANE, A., HARTE, L. 2003. *Introduction to telecom billing*. ALTHOS Publishing.

PALSHIKAR, G.K. 28 May 2002. "The hidden truth - Data analysis can be a strategic weapon in your company's management and control of fraud". *Intelligent Enterprise Magazine*, vol. 5, No 9, Feature article, electronic version. http://www.intelligententerprise.com/020528/509feat3_1.jhtml. Accessed: 10 May 2004.

PICTON, P. 1994. *Introduction To Neural Networks*. Macmillan.

PONNAVAIKKO, P., RAJAGOPALAN, S. & TUNGGAL, G. 12 December 2002. *Will security and billing issues push Wi-Fi down?* Capstone paper for Masters in Interdisciplinary Telecommunications, University of Colorado, Boulder, USA.

REALNETWORKS.COM. 2006. RealNetworks website home page. http://www.realnetworks.com/. Accessed: 22 April 2006.

RESEARCH AND MARKETS. February 2002. "US Next Generation Networks 2002". *Research and Markets* report. http://www.researchandmarkets.com/reports/294/. Accessed: 14 June 2004.

REUTERS. 20 March 2005. "Phishing by phone – VoIP raises security concerns". *ZDNet News* article. http://news.zdnet.com/2100-1009_22-5627631.html. Accessed: 26 July 2005.

RUSCH, J.J. June 2003. Computer and Internet Fraud: A Risk Identification Overview. *Computer Fraud & Security,* vol. 2003, issue 6, pp. 6-9.

SCHIM, R. 30 September 2004. "'Wardriving' conviction is first under Can-Spam". *ZDNet News* article. http://news.zdnet.com/2100-1035_22-5390722.html. Accessed: 15 February 2006.

SCHUK, C. 01 July 2005. VoIP Fraud: The Industry's Best-Kept Secret. Voxilla article. http://voxilla.com/voxstory166.html. Accessed: 26 July 2005.

SCHWARTZ, S. August 2003. Standards Watch: Cibernet Releases MXP Standard for Mobile IP Revenue Settlement, *Billing World and OSS today*, issue 8, August 2003, electronic version. http://www.billingworld.com/rev2/portal/main/search.cfm. Accessed: 29 March 2005.

SGI. 2002. "Thirdspace OVS for the SGI® Origin® 300 Server: A Streaming Server for Broadband iTV and VOD Broadcast Systems". Product information. http://www.sgi.com/pdfs/3064.pdf. Accessed: 22 February 2006.

SMITH, F.B. 1 August 1998. 'Cramming' telephone bills. *Consumer's Research Magazine*, vol.81, issue 8, pp 34-35.

SNOPES.COM. 12 July 2004. "Call forwarding scam". http://www.snopes.com/inboxer/scams/forward.asp. Accessed: 23 November 2005.

SNORT. ORG. 2006. Snort website home page. http://www.snort.org. Accessed: 12 April 2006.

STALLINGS, W. 2003. *Network Security Essentials: Applications and Standards*. Prentice Hall.

STEVENSON, I., DELANEY, J. & PUGH, T. March 2001. "Softswitches: the keys to the next-generation IP network opportunity". Technical report. Ovum Ltd.

STONES, L. March 2003. "Check that phone bill before you pay". Business Day article. http://www.businessday.co.za/Articles/TarkArticle.aspx?ID=723082. Accessed: 10 February 2007.

SWEENEY, T. 2001. Next Generation Networks: the future of business. *NewsLink – Alcatel International Magazine*, 2nd Quarter 2001, vol. 9, no 2, pp. 13-17.

TEKELEC. 14 February 2001. "Next-Generation Networks: Migration from Circuit to Packet – An overview". Tekelec white paper. http://www.tekelec.com/ss7/NGN-Overview.pdf. Accessed: 07 June 2004.

TELKOM. 18 May 2004. "Telkom busts half-price fraud syndicate". ITWeb article. http://www.itweb.co.za/sections/telecoms/2004/0405180752.asp?S=Legal%20View&A=LEG&O=FRGN. Accessed: 22 November 2005.

THOMSEN, D. March 1995. IP spoofing and session hijacking. *Network Security*, vol. 1995, issue 3, pp. 6-11.

TUFF – TELECOMMUNICATIONS UNITED KINGDOM FRAUD FORUM. 2004. *Accreditation training – Telecom fraud professionals,* version 2.0. CD-ROM.

TYLER, G. November 2003. Go on a War Drive. *Management Services*, vol. 47, issue 11, pp. 20-23.

VESANTO, J. 1999. SOM-Based Data Visualization Methods. *Intelligent Data Analysis,* vol. 3, No. 2 ,1999.

WICKHAM, R. 15 February 2005. Evil Twin Poses Wi-Fi Worry. *Wireless Week*, vol. 11, issue 4, p4.

WIKIPEDIA. 30 November 2005b. "Who wants to be a Millionaire?". http://en.wikipedia.org/wiki/Who_Wants_to_Be_a_Millionaire? Accessed: 02 December 2005.

WIKIPEDIA. 6 March 2007. Phone fraud. http://en.wikipedia.org/wiki/Phone_fraud. Accessed: 06 March 2007.

WU, N., QIAN, Y. & CHEN G. 2006. A Novel Approach to Trojan Horse Detection by Process Tracing. *Proceedings of the 2006 IEEE International Conference on Networking, Sensing and Contro*l, Ft. Lauderdale, Florida, USA, 23-25 April 2006, pp. 721-726.