# A fraud detection model for Next-Generation Networks

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

{s20183667@tuks.co.za, molivier@cs.up.ac.za, eloff@cs.up.ac.za,}

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

**Abstract— Telecommunications fraud, already a major threat in currently specialized networks for voice and data traffic, is expected to increase in upcoming converged networks referred to as Next-Generation Networks (NGNs). 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 (FMS) as these systems are highly service-specific. More appropriate tools are therefore needed for improved NGN fraud detection.**

**This paper presents our work-in-progress on designing an FMS suitable for NGNs. The paper provides suggestions on the design of an FMS model to address NGN fraud detection.**

**Index Terms— fraud management system (FMS), Internet Protocol (IP), Next-Generation Network (NGN), telecommunications fraud.**

## I. INTRODUCTION

The term Next-Generation Network (NGN) is used to refer to the future convergence of voice, video and data networks onto the same infrastructure [1]. The migration towards NGNs is mainly motivated by the ever-increasing growth of the data traffic (directly caused by the growth of the Internet) that already exceeds the voice traffic. It therefore becomes sensible to carry voice as an application over the data network instead of maintaining a separate voice network [1]. Besides, operators are facing new customer demands that cannot be provided by today's specialized networks. For instance, 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 [2].

NGNs are based on the Internet Protocol (IP) and can be accessed from various mechanisms. These key characteristics pose new challenges for fraud detection in converged networks. Besides due to the potential high value of the new services offered in NGNs, fraud is likely to increase significantly.

Telecommunications fraud is a worldwide problem that deprives operators of enormous sums of money every year. Consequently, the high probability of the rise of fraud in NGNs is an alarming thought. An even more alarming thought is the absence of adequate NGN fraud management systems (FMS). An FMS is a system designed to detect, manage and assist in the investigation of fraudulent activities through the analysis of customers' usage records generated for billing purposes [3].

FMSs are usually developed for a specific service in a specific environment. Thus, they cannot accommodate the new services and associated fraud types that are likely to appear in NGNs. The design of more general FMSs suitable for NGNs is therefore a necessity and is the main goal of our ongoing research project, which was described in [4]. Previous work such as [5], [6] and [7] has already been conducted in the area of NGN fraud detection. The proposed solutions either focus on identifying more efficient fraud detection techniques or combining aspects of intrusion and fraud detection to enhance the management of fraud in NGNs. However one [5] of these solutions presents a fraud model that can be used to define classes of fraud characteristics that are then implemented in modules and used to design FMSs. As *fraud* specifications require extensive knowledge of the *service* characteristics, we extend the fraud model provided in [5] to design a more general fraud detection model based on *service* specifications.

The goal of this paper is to describe our model for NGN fraud detection. Suggestions on the model are based on the analysis of the potential evolution of fraud in NGNs and the examination of key NGN characteristics that make fraud detection more complex in converged networks.

Section 2 reviews the present fraud issues as well as common fraud types on current networks. Section 3 examines how key aspects of NGNs add complexity to the problem of fraud detection. In Section 4 a vision of the future of fraud in NGNs is presented. Section 5, which is the core of the paper, presents our ideas for the design of the NGN fraud detection model.

## II. FRAUD IN CURRENT NETWORKS

There is currently no standard definition for

"telecommunications fraud". From an industry point of view, fraud managers commonly use this term to refer to the theft by deception or the deliberate misuse of services offered via a telecommunications system [8]. From a legal perspective, the APRI (American Prosecutors Research Institute) defines this type of offense as "the use of telecommunication devices to intentionally deceive or criminally manipulate a person for financial gain" [9].

On an industrial scale, fraud is mainly perpetrated by organised criminal gangs, professional hackers and operators' own employees [10]. In fact, it is estimated that almost 73% of all telecommunications fraud involves some employees of the telecommunications companies [10]. However, due to the availability of numerous hacking and phreaking[1] tools on the Internet, fraud is a widespread crime that can be committed by anybody depending on one's individual goal [8].

The main motivation to commit fraud is to make money (*revenue fraud*). This can be achieved by selling fraudulently obtained services at cheap rates or by selling critical company information to other criminals [11]. Other reasons to commit telecommunications fraud (*non revenue fraud*) include:
- to avoid or reduce payment of services used
- to maintain anonymity while committing other crimes
- to demonstrate ability to outmaneuver [1]the operator's system security [12].

Both the operator and the customer suffer from fraud. The operator suffers from damaged reputation and substantial loss of revenue, usually between 3% and 8% of their annual income [13]. This amounts to almost USD 40 billion globally [14] and to USD 700 million in Africa alone [8]. The customer can suffer from loss of privacy and negative credit rating due to identity theft. He can also experience overcharged bills due to the illegal access and use of his account by criminals.

The International Data Corporation has identified more than 200 forms of telecommunications fraud [8]. Most of them are perpetrated using the following two basic strategies: the fraudster either impersonates someone or technically deceives the network systems [9]. Table 1 shows common fraud types on current telecommunications networks. Fraud types are sorted alphabetically.

Some of these fraud types are described below:
- Subscription fraud: It is 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 in a short period of time before disappearing. This scam is often associated with call selling i.e. the resale at discounted rates of fraudulently obtained telephone services. Subscription fraud is currently the most prevalent form of fraud [11].
- Premium rate service (PRS) fraud: a PRS number is a number with higher than normal call rates because this number gives access to special services such as weather forecasts or entrance to prize-winning competitions. In

such a service set-up, income from calls received is shared by the network operator and the premium rate service provider, 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 dialed fraudulently by people who want to use the service without paying. Secondly they are sometimes illegally dialed by the service provider himself (or his accomplices) in order to increase the number of calls made to his own PRS numbers and consequently raise his revenue from the operator [15].

- Cloning, still a widespread threat in older analogue networks especially in developing countries, is the programming of the Mobile Identification Number (MIN) and the Electronic Serial Number (ESN) of a legitimate phone onto the fraudster's phone. The MIN identifies the customer while the ESN identifies the phone [15]. Such information is usually obtained through eavesdropping with scanning devices during phone calls or by theft. Calls made on the cloned phone are then charged to the owner of the original phone. A variant of this fraud type is *tumbling* [11], 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. Cases of cloning in GSM (Global System for Mobile Communications) systems, the successor of analogue networks, have also been reported [16] but GSM cloning is not regarded as a major threat. Cloning is currently the best-known type of telecommunications fraud [11].

TABLE 1
SOME CURRENT COMMON FRAUD TYPES

| All voice networks | Fixed voice networks | Mobile voice networks | Data network (Internet) |
|---|---|---|---|
| Call selling | Hacking | Cloning and tumbling | Credit card fraud |
| Calling cards fraud | Teeing-in (or clip-on fraud) | Handset theft | E-commerce fraud |
| Insiders abuse | | Roaming fraud | IP attacks (denial of service, virus, spoofing) |
| Interconnect fraud | | | Phishing and pharming |
| PBX (private branch exchange) fraud | | | |
| PRS (premium rate service) fraud | | | |
| Subscription fraud | | | |

Detecting fraud is a challenging task as hackers are getting more and more technology savvy and constantly change their fraud tactics. With the advent of new services and technologies, fraud detection in NGNs could be even more challenging.

III. THE PROBLEM OF FRAUD DETECTION IN NGNS

As mentioned in Section I, NGNs have two main characteristics that create new security vulnerabilities and make fraud detection more difficult:
1. IP-centric. IP is the underlying protocol for NGNs.
2. Many access mechanisms (e.g. wired, wireless, cable and modem).

## A. IP-centric

- Since all gateways of the converged networks are connected to the Internet, NGNs will inherit IP inherent security vulnerabilities. Due to their open architectures IP networks suffer from many vulnerabilities and can be easily exploited for fraudulent actions such as IP spoofing (the use of a stolen IP address for impersonation) making it easier to conceal fraud [3].

- The provision of sophisticated NGN IP-based services follows a different business model than traditional telecommunications services, as many more actors are involved. Such actors may include the customer, the service provider, the content provider, the application service provider, the network provider and the e-payment provider. Each of these actors is a potential candidate for fraud. This makes fraud investigation harder in NGNs as data need to be gathered from many different companies [5]. A simplified example for such a scenario is the previously described PRS fraud. If the content of the premium rate service is offered by a specialised content provider and necessitates a specific application service provider, then fraud detection becomes much more complex.

- 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 [6]. This security feature is lost in IP networks as their open interfaces are well documented and understood by many more people. Therefore attacking previously highly protected systems is much easier [18].

- The PSTN (Public Switched Telephone Network) follows a centralized 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 decentralized 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 [5].

## B. Many access mechanisms

- The possibility to use various mechanisms to access the network enables fraud to be committed from various 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 [2]. This 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) [2].

Although converged networks face the security issues mentioned above, operators are eager to deploy NGNs due to the reasons previously explained in Section I. In fact, migration from traditional telephone networks to NGNs is already underway in developed telecommunications markets [17]. As NGNs imply the development of new technologies and services, new forms of fraud might therefore appear.

## IV. EVOLUTION OF FRAUD IN NGNs

Fraud scenarios depend on the service types and their underlying technologies. For this reason fraud will evolve in NGNs as new services and technologies are introduced. New usage-sensitive and content-based billing models are expected to replace current flat rate-charging schemes. This will also have an impact on the types of fraud perpetrated [12]. Some speculations on the evolution of fraud in NGNs are given below.

Firstly, because fraud scenarios highly depend on service offerings as well as business models, 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 [12]. 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 [12].

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 of new email-based fraud attacks such as phishing [18] whereby the scammer mimics the email-address of a trusted party in order to obtain the victim's personal information such as his bank details.

However it is worth mentioning that fraud motives and threats remain generally the same throughout the years, even though technology evolves [7]. Criminals merely become more technology savvy and hence, use new techniques to perpetrate the same basic types of fraud. For example, teeing-in (physically connecting to a legitimate customer's phone line in order to make free calls at his expense), which first appeared in the 1950s is still widely spread nowadays [19]. It can thus be assumed that although some new forms of fraud will appear, a large number of the fraud types in NGNs will just be the same as the current ones with slight modifications. It is therefore very important not to overlook old fraud issues in NGNs.

Based on the above speculations, some potential NGN fraud types are shown in Table 2 in alphabetical order.

TABLE 2
LIKELY NGN FRAUD TYPES

| Content fraud types | Excess download |
|---|---|
| | Illegal redistribution of service |
| | Overcharging |
| | Unauthorized access to resources |
| New fraud type due to convergence | Money laundering |
| Traditional fraud types | Credit card fraud |
| | Identity theft (email-based) |
| | Insiders abuse |
| | IP attacks |
| | PRS fraud |
| | Subscription fraud |

Some of the new fraud types are described below.

- 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 in a bank account large sums of money illegally obtained 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 his money in his bank account claiming that it comes from his legitimate commerce [20].
- Excess download: A customer manipulates the billing mechanism for the media content in order to download more data than he is entitled to [7].
- Overcharging: An actor in the IP business model charges another actor more than previously agreed upon. For instance a service provider tries to overcharge a customer by sending him more data than he requested [7].

These new forms of fraud and the increased complexity of fraud detection in NGNs necessitate more general FMSs. A formal fraud detection model independent of any service type or network environment would therefore be beneficial.

## V.  THE FRAUD DETECTION MODEL

As NGNs enable the provision of dynamic services, which may change quickly according to new customer requirements, effectively managing NGN fraud detection requires FMSs that are highly flexible and can support any type of service. Thus the FMS needs a modular architecture where components and data analysis techniques can be quickly added, removed or modified [7]. The FMS also needs to be able to scale to support an increasing number of business transactions due to the new business model of IP-based services. Another key requirement is the real-time operability of the FMS. As explained previously, IP fraud can originate from several access points at the same time, which requires the quick exchange and analysis of relevant information to detect and possibly stop fraud as soon as possible. Issues to look at when designing our FMS are:
1. The collection and the format of the input data
2. The identification of fraud indicators
3. The fraud detection technique
4. The deployment of the FMS
   A discussion of each of these issues follows.

### A.  The collection and the format of the input data

Collecting data for analysis is the first step in the fraud detection process. Typically, CDRs (call detail records) generated by network elements such as telephone switches for billing purposes, are the main source of input data for current FMSs [5]. These records contain all the necessary details for identifying and charging the customers for their usage of the network services. The main problem with CDRs in respect to NGN fraud detection is that they lack flexibility to reliably describe NGN services and they have proprietary formats, which does not allow for the interoperability of network elements [6]. Another problem with CDRs is that they are only generated after completion of a service usage and are processed in batch-mode, which makes real-time fraud detection impossible [6]. We therefore choose to use emerging IPDRs (Internet Protocol Detail Records) [21] as these billing records are highly flexible, allow interoperability between different network elements and systems and can be generated for ongoing service usage. A detailed discussion on IPDRs and their benefits over CDRs for NGN fraud detection can be found in our previous paper [22].

In an NGN environment usage records are not the only valuable source of information for detecting fraud. Analysis of network traffic is also crucial as fraud can be ubiquitous in an all IP network.  Network traffic analysis can also be used to compare how much data is sent to the user and how much he actually pays for it [3]. Information about the network traffic can be obtained from a network device such as a router but also from Intrusion Detection System (IDS) log files. Basically an IDS is a network node that inspects network traffic and identifies suspicious patterns that may indicate an attack [7]. Combining IPDRs and IDS log files might give a good coverage of the data flowing through the network and that need to be analysed for signs of fraud.

### B.  The identification of fraud indicators

Fraud indicators are details about the service usage that may indicate that fraud is perpetrated [5]. In the traditional voice networks usual indicators of fraud include long duration calls, large number of calls from the same account and calls to blacklisted numbers [6]. These indicators are used to create fraud rules or signatures that are characteristics of a fraud type. Fraud rules need to be updated continuously as fraud types evolve. An alternative to defining fraud signatures is the creation of customer profiles [7]. A customer profile defines the individual pattern of normal usage for a customer. By comparing the current usage to the stored profile, fraud can be detected without the need for specifying rules for specific fraud scenarios.

This approach works well for traditional networks where a limited set of services are offered and a user profile can reliably describe normal behaviour for this set of services. However this will not be effective in NGNs where services are very dynamic, new ones constantly appear and old ones disappear to reflect changing customer demands and technologies. Keeping up-to-date with a customer's usage pattern becomes more problematic and can probably result in inaccurate or outdated profiles. The FMS will therefore

generate many false alarms. For instance if a new service is introduced, the first time the customer makes use of this service an alarm will be triggered as this does not correspond to his normal profile. This is bound to happen as often as new services are offered.

Our suggestion is therefore to create a *service* profile that describes how the service is normally used by the average user. This service profile is also used to create service-specific fraud rules used to detect suspicious events. The profile will answer questions such as: how much is usually spent on this service, at what time and for how long is the service usually used? Answers to these questions enable the creation of groups of users for a specific service. For instance, it is possible to create different profiles for different times of the day or week (e.g. peak time, night, week-end). The billing records are then sent to the relevant group profile based on the time of the service usage. The service profiles are stored in modules that can be added and removed from the FMS as needed.

### C. The fraud detection technique

Various data analysis techniques are in use by FMSs. The most recurrent techniques are threshold-based, rules-based and the use of neural networks [6].

In threshold-based fraud analysis, details about the call (e.g. call duration) are compared to fixed criteria called triggers. If the value of the call detail exceeds that trigger, an alarm is generated [6]. Threshold based detection tools are simple, efficient but only work well for detecting the extremes of fraudulent events as triggers are usually set to high values.

In rules-based analysis, fraud patterns are defined as rules and call records are analysed against these rules to spot fraud [6]. The main drawback of rules-based analysis is that it can only detect known fraud scenarios.

Neural networks are an artificial intelligence technique that is based on the fact that fraud attempts display significant change from previous legitimate behaviour [6]. As neural networks are self-learning tools that can adapt to changing legitimate behaviour they are the ideal technique for detecting new forms of fraud not described by our service-specific fraud rules.

NGN FMS as it is not possible to accurately describe future NGN fraud patterns and to use them as a training data set. Our suggestion is to use a SOM (Self-Organising Map) [6] as this type of unsupervised neural network can provide a graphical representation of the analysis, highlighting outliers that may suggest suspicious activity.

### D. The deployment of the FMS

Currently this issue is not addressed by our model but will be investigated at a later stage.

Having looked at the FMS design issues, a description of our fraud detection model follows as a solution to these issues.

### E. High level description of the fraud detection model

A high level diagram of our proposed fraud detection model is shown in Figure 1.

Fraud detection follows a three-stage process. In the first phase IDS logs are compared to IPDRs for signs of general fraud cases such as receiving a resource without paying for it. The 2nd step compares the IPDRs of a specific service to its corresponding fraud rules to identify fraud cases that are unique to this service. This will be done through rules-based analysis. In the 3rd phase the IPDRs are compared to the service profile to detect fraud cases that are not stored in the rules database. This analysis is performed by a neural network tool. If suspicious activity is detected at any of these stages, the analysis does not proceed to the following stage but is sent to a case manager for manual inspection. One suggestion is to automatically notify the user and asks for a confirmation of normal activity from his side.

This model offers many advantages over current FMSs.

Firstly it is flexible as fraud rules and service profiles can be updated as needed. Fraud rules and service profiles can be defined during the design phase of a new service and from past fraud scenarios of similar service types. Frauds specifications can be established based on service contents, billing model, service components and involved actors as explained in the fraud model provided in [5].
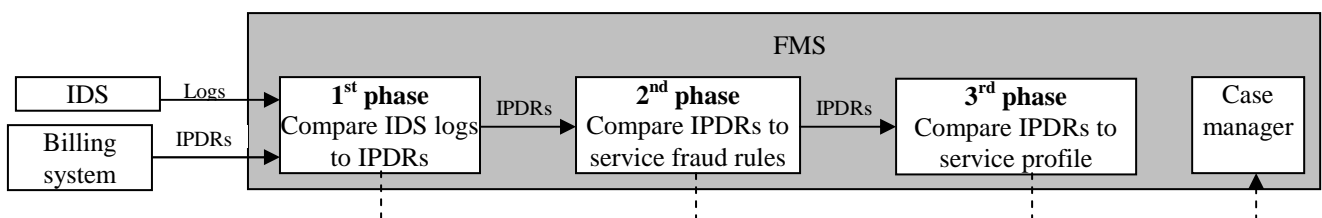


Fig.1. NGN fraud detection model

There exist two main types of neural networks: supervised and unsupervised [6]. Supervised neural networks are trained to look for similarity between the input data and a training data set that was already classified as either "normal" or "abnormal". On the other hand, unsupervised neural networks can automatically identify patterns of similar behaviour in the input data without the need of a training set [6]. They are therefore the best solution for our

Secondly it saves memory and resources because the number of different services and associated features offered by an operator is very small compared to the number of customers using these services. Creating, storing and updating service profiles is therefore much less time and resource consuming than maintaining a very large number of individual customer profiles.

Thirdly by combining IDS logs and usage records

analysis, we are likely to discover a higher number of fraud attacks as such attacks in IP-based services often involve some form of network misuse (e.g. Denial of service). Besides IDS logs might help uncover network security flaws that might be exploited for fraud and hence, help in the definition of new fraud signatures.

In addition, the system has a modular architecture, which facilitates its scalability. Besides, the use of IPDRs enables near real-time fraud detection as these records can be generated on the fly for ongoing service usage.

## VI. CONCLUSION AND FUTURE WORK

This paper has presented a model for an FMS for NGNs. The proposed model has the potential to mitigate the problem of fraud detection in NGNs and can satisfy our identified requirements for NGN fraud management systems. The model is independent of any service or environment and general enough to accommodate any type of existing or future service.

The model has been designed based on the examination of the evolution of fraud in NGNs and the new challenges that NGNs pose for fraud detection.

The model is still in its infancy and necessitates more research. Future work would consist on testing the viability of such a model through the implementation and testing of an appropriate prototype.

## REFERENCES

[1] C. Huitema, 1999, "Challenges of the next generation networks", *Keynote for Internet'99 conference, Moscow, October 25-28.*

[2] A. R. Modaressi, and S. Mohan, "Control and management in Next-Generation Networks: challenges and opportunities", IEEE Communications Magazine, vol 38, issue 10, pp. 94-102, October 2000.

[3] IEC - The International Engineering Consortium. (2004). Fraud analysis in IP and Next-Generation Networks. Web ProForum Tutorials. Available: http://www.iec.org/tutorials/fraud_analysis/.

[4] M. Bihina, J. Eloff and M. Olivier, M, "Requirements for Next-Generation Networks billing systems", in Proc. SATNAC 2004: the Southern African Telecommunications Networks and Applications Conference, Stellenbosch, South Africa. September 6-8.

[5] H. Kvarnstrom, E. Lundin and J. Erland, "Combining fraud and intrusion detection - meeting new requirements", in proc. Fifth Nordic Workshop on Secure IT Systems (NordSec), Reykjavik, Iceland, October 12-13, 2000.

[6] S. Hearne. "A Fraud Detection Framework for Next-Generation Telecommunications Networks", M S. thesis. Waterford Institute of Technology. August 2004.

[7] D. Abramowicz, D and P. Ledberg. "IP fraud: Methods and algorithms for detecting IP-based fraud". M S. thesis. Swedish Royal Institute of Technology. Göteborg, Sweden. 01 December 2002.

[8] R. Jacobs. (2002). "Telecommunications fraud". Dimension data white paper. Available: http://www.didata.com/services/white_papers/Fraud_White_Paper.pdf.

[9] APRI. (September 2004). "If it sounds too good to be true – local prosecutors' experiences in fighting telecommunications fraud". Available: http://www.ndaa-apri.org/pdf/sounds_too_good.pdf.

[10] Beck Computer Systems. (2003). "Breaking the back of telephone fraud". Available: http://www.cto-ict.org/index.php?dir=04&sd=30&aid=1020

[11] Cerebrus Solutions. (November 2002). Fraud Primer. Issue 2.3. Available: http://cerebrussolutions.com/pdf/Fraud_Primer-Nov02.pdf

[12] M. Johnson. (January 2002). "Future Frauds: Telecom fraud in Next Generation Services". Available: http://www.cto-ict.org/index.php?dir=04&sd=30&aid=1012.

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

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

[15] Ericsson. 2004. "Categorising telecommunications fraud – an introduction for those new to the subject". Available: http://www.cto-ict.org/index.php?dir=04&sd=30&aid=1018.

[16] ISAAC- Internet Security, Applications, Authentication, and Cryptography. GSM Cloning. Computer Science Division, University of California, Berkeley. Available: http://www.isaac.cs.berkeley.edu/isaac/gsm.html

[17] P. Falshaw, "Next generation networks and services", in proc. PTC2001, the Pacific Telecommunications Council, 15-17 January 2001.

[18] K. Dunham. "Phishing Isn 't So Sophisticated: Scary!". *Information Systems Security; May/Jun2004, Vol. 13 Issue 2, p2-7.*

[19] M. Collins, "Telecommunications crime – Part 1". *Computers & Security. vol. 18, p 577-586. 1999.*

[20] M. Johnson. (October 2002). "Revenue Assurance, fraud and security in pre-paid 3G services". Visual Wireless white paper.

[21] IPDR.ORG. (November 2004). Document map and overview. Version 3.5.0.1. Available: http://www.ipdr.org/public/DocumentMap/DMO3.5.0.1.pdf.

[22] M. A. Bihina Bella. J.H.P. Eloff and M.S. Olivier, "Using the IPDR standard for NGN billing and fraud detection". Submitted for publication. April 2005.

**M. A. Bihina Bella** is currently a member of the ICSA (Information and Computer Security Architectures) research group at the University of Pretoria pursuing an MSc in Computer Science. The goal of her research project is to design a fraud management system for Next-Generation networks.

MA Bihina Bella, MS Olivier and JHP Eloff, "A fraud detection model for Next-Generation Networks," in D Browne (ed), *Southern African Telecommunication Networks and Applications Conference 2005 (SATNAC 2005) Proceedings*, Vol 1, 321-326, Champagne Castle, South Africa, September 2005