

USING THE INTERNET PROTOCOL DETAIL RECORD STANDARD FOR NEXT-GENERATION NETWORK BILLING AND FRAUD DETECTION

MA Bihina Bella¹, JHP Eloff², MS Olivier³

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

¹s20183667@tuks.co.za, +27 12 420 3035, University of Pretoria

²eloff@cs.up.ac.za, +27 12 420 2361, University of Pretoria

³molivier@cs.up.ac.za, +27 12 420 2052, University of Pretoria

ABSTRACT

Fraud is a crucial problem in the telecommunications industry and is expected to increase in future convergent networks, commonly referred to as Next-Generation Networks (NGNs). Indeed due to the convergent nature of NGNs, it is highly likely that fraud from traditionally separate entities will converge and that new forms of fraud targeted at content rather than connection will emerge. Some examples include illegal redistribution of service and unauthorized access to services. Unfortunately, fraud management systems (FMSs) deployed to detect fraud on current networks are not equipped to effectively address this emerging threat and need to be revised accordingly.

As the main source of input data of FMSs is generated by billing systems, determining NGN billing systems requirements is the first step to the design of an FMS suitable for future networks. Some of these requirements have been identified but cannot be satisfied by current billing systems due to the proprietary and static format of their CDRs (Call Detail Records) i.e. the records capturing the service usage of the network users. A promising solution to these problems is the recently developed Internet Protocol Detail Record (IPDR) standard.

This research paper therefore examines the IPDR solution and demonstrates how it can help meet the identified NGN billing requirements. The paper also shows how the IPDR standard can improve the fraud detection success rate of potential fraud types in NGNs.

KEY WORDS

Next-Generation Network (NGN), billing system, fraud management system (FMS), Call Detail Record (CDR), Usage Detail Record (UDR), Internet Protocol Detail Record (IPDR).

USING THE INTERNET PROTOCOL DETAIL RECORD STANDARD FOR NEXT-GENERATION NETWORK BILLING AND FRAUD DETECTION

1 INTRODUCTION

NGN (Next-Generation network) has been a buzzword in the telecommunications industry since 1998. It generally refers to the convergence of telephone and data networks into a single multiservice IP (Internet Protocol) network, which carries voice, video and data over the same infrastructure [Hui99]. Shifting to NGNs will enable the offering of a new class of services that has the potential to increase revenue for operators and enhance customers' experience. However it is highly likely that these new high-value services will attract a large number of criminals and hence favour the rise of fraud.

Telecommunications fraud is the "theft of services or deliberate abuse of voice and data networks" [Jac04]. One popular example of fraud is call selling i.e. the resale of fraudulently obtained telephone services at cheap rates [Jac04]. Fraud is a serious problem continuously faced by carriers since it has been identified as their primary cause of revenue loss. For this reason, it needs to be addressed before NGNs yield the expected benefits.

Fraud is generally managed by fraud management systems (FMSs). 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. In the telecommunications industry billing records are usually called CDRs (Call Detail Records), they are used to generate customer profiles necessary to establish correct thresholds for fraud detection. Since FMSs are usually developed for a specific application they cannot accommodate the new services that will be offered in NGNs and need some revisions [Lun02].

This paper presents the current status of a research project aimed at designing an FMS suitable for NGNs. An overview of the project background and methodology was given in [BEO04]. Since billing records are the main source of input data for FMSs, the examination of billing systems is the first step towards the project goal. Inputting incorrect or outdated billing records into an FMS will indeed only result in the detection of incorrect or outdated fraud cases.

Various modifications are required from traditional service-specific billing systems in order to cater for the new services and associated charging schemes offered in NGNs. Some of these requirements were already mentioned in [BEO04] and have been refined in this paper. The identified requirements cannot be fully satisfied by current billing systems because the format of their CDRs lack flexibility to bill for new service usage attributes and does not allow interoperability between vendors due its proprietary layout. This severely limits the effectiveness of the fraud detection process and indirectly increases the probability of fraud occurrences in NGNs. The emerging IPDR (Internet Protocol Detail Record) standard [Ipd04a] seems a promising solution to this problem.

The contribution of this paper is twofold. Firstly a set of requirements for NGN billing systems is established based on the examination of a typical billing process and its limitations with respect to NGN fraud detection. Secondly the IPDR standard is reviewed in light of the NGN billing requirements for improved fraud detection.

The rest of the paper is organized as follows: Section 2 reviews a standard billing process and presents NGN billing requirements. Section 3 gives an overview of commonly used billing

standards, explains why they are a limiting factor to the identified requirements and shows how these various standards increase the fraud risk in NGNs. Section 4 gives an overview of the IPDR standard. Section 5 demonstrates how using IPDRs for billing can help satisfy the above-mentioned requirements and how this can positively influence the fraud detection process in NGNs based on a small set of potential future fraud types. The paper ends with a conclusion and some thoughts for future work in Section 6.

2 NEXT-GENERATION NETWORK BILLING REQUIREMENTS

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" [NTIA04]. The billing system produces information about financial transactions that helps 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) [Ama03].

UDRs are usually generated by network service elements such as telephone switches, routers or gateways. They can also be produced by a clearinghouse or a third-party service provider for settlement purposes. Each of these sources produces UDRs in a different proprietary format. Therefore the UDRs need to be converted into the billing system internal format before they can be rated. Rating is the calculation of the charges for a service usage [IEC04a]. The UDR format conversion is done by a mediation system and is an inherent part of the billing process [OHL03:9]. Figure 1 shows our representation of a standard billing process and its connection to the FMS.

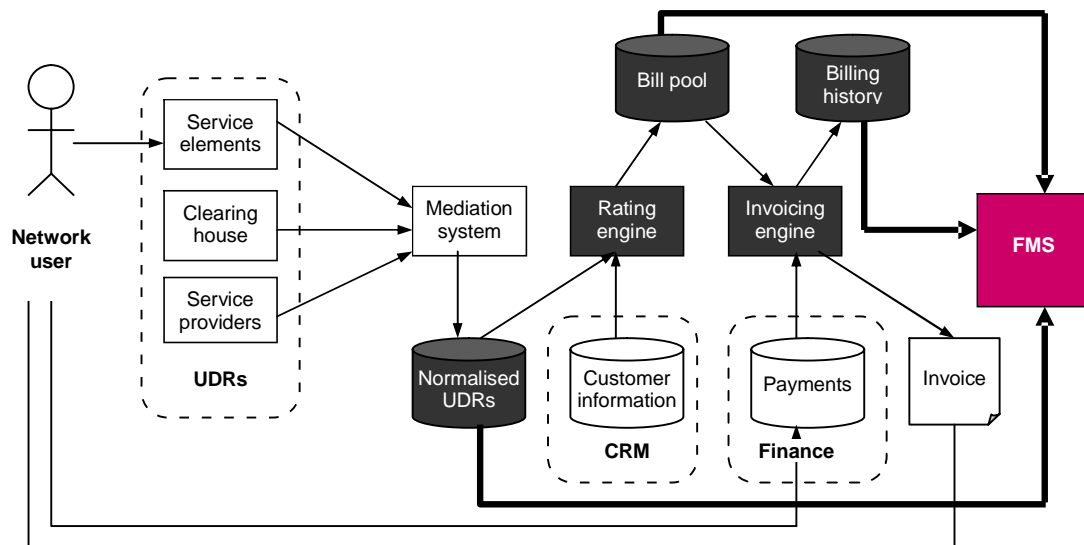


Figure 1. Standard billing process

Except for the FMS, shaded blocks in Figure 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.

Figure 1 shows that as the customer makes use of the network services, the corresponding service elements, service providers and clearinghouses (if applicable) record his activities and create raw (not properly formatted and not rated) UDRs on completion of his usage of the service. The mediation system gathers these raw UDRs, checks their validity, reformats them into the billing system proprietary layout, consolidates related UDRs and stores them in a database. The normalised UDRs can then be sent to the rating engine either periodically or after an event has been triggered (e.g. a certain volume of UDRs has been reached) [OHL03:9]. The rating engine matches UDRs to the user account using the customer information database from the customer relationship

management system (CRM) and calculates service charges for each UDR (excluding promotions). It then stores the rated UDRs into a bill pool until the next billing cycle (usually once a month). When the next billing cycle is run, UDRs are transferred from the bill pool to the invoicing engine, which adds recurring charges (such as monthly fees) in addition to any promotions, discounts and taxes corresponding to the customer account. Then, 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 [IEC04a].

Figure 1 also shows that the FMS can collect billing records from three different sources: the database of normalised but not rated UDRs (to monitor user's most recent activity), the bill pool (for rating details) and the billing history (to profile customer past usage behaviour).

An analysis of this diagram reveals the following shortcomings of standard billing processes in relation to NGN fraud detection:

- The billing system operates in batch mode: UDRs are stored for some time before being periodically 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 making it impossible to stop ongoing fraudulent activity and making it more difficult to catch the fraudster [IEC04b]. 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 only accessed during the rating phase, thus after the service has been consumed [Luc04]. 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 the revenue loss due to fraud.
- The billing system has a centralized architecture. This means that all UDRs are processed by only one rating engine and only one invoicing engine. This limits the billing system scalability. The provision of sophisticated NGN services usually necessitates the partnership of several service providers. This will significantly augment the volume of business transactions in NGNs [Luc04]. 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 [Ama03].
- Although it is not visible from the diagram, billing systems are usually service specific [IEC04b]. 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 capable to accommodate NGN usage-sensitive and content-based pricing models, which are expected to replace current flat-rate charging models [IEC04b].

Four major requirements for NGN billing systems can be inferred from the above discussion:

- Real-time billing is an imperative for timely fraud detection. Various industry experts agree that real-time billing "is the only practical solution to the increasing problem of risk management" [Luc04]. True real-time billing already exists but only for prepaid services [OHL03:6].
- High-level of scalability is a necessity to support an ever-increasing number of customers and inter-carrier settlement activities [IEC04b].

- Convergent billing i.e. the aggregation of the charges for all the different types of services used by one customer onto a single invoice [IEC04b], is needed for effective fraud detection. It 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 [Luc04].

Some propositions to address some of these requirements have been made and, in some cases, have already been implemented. One such proposition is to move the rating engine out of the billing system and to integrate it with the mediation system to enable real-time rating and upgrades to rating plans without jeopardising the billing flow [Luc04]. Another suggestion is to use a modular architecture for added scalability [Luc04]. 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 the FMS can only be as good as its input data. It is therefore necessary to review current billing standards since they define UDR content and format.

3 BILLING STANDARDS

Billing standards define the measurement, format and transmission methods of UDRs [OHL03:25]. Reviewing common billing standards is necessary to select a proper UDR format and transmission protocol that can help satisfy the billing requirements established in the previous Section. UDRs contain details about a service usage. These details include 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), why (cause of event recording) [Ipd04a]. UDR formats are generally quite static, meaning that only specific service usage attributes can be recorded.

There exist many billing standards currently in use and they all depend on a specific type of application and network environment. There also exist different billing standards for usage data (between an operator and his end-users) and settlement data (between an operator and his partners). This means that there is no universal format for UDRs and no uniform protocol for UDR transmission.

Traditionally, UDRs have been generated by telephone switches using the Automatic Message Accounting (AMA) process developed by the Bell telephone company in the 1940s. UDRs were then formatted using Telcordia Technologies' Billing AMA Format (BAF), which defines a binary coded decimal format for UDRs [Bor01]. BAF is still in use today, especially in North America, but its implementation varies from one switch manufacturer to the other [OHL03:10]. Some recent variations of the BAF format are the ACDR (an ASCII AMA format) and the XCDR (an XML AMA format) [OIF02]. Other service elements such as softswitches generally produce UDRs in comma-delimited format or in table format [OIF02].

A multitude of billing standards for transmitting UDRs is also in use. Some examples are:

- 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) [ATIS04].
- MXP (Mobile Xchange Protocol), defined by CiberNet, a division of CTIA (Cellular Telecommunications Industry Associations) to bill for wireless non-voice services [PRT02].
- OSP (Open Settlement Protocol) defined by ETSI (European Telecommunications Standards Institute) for the exchange of pricing data between IP telephony operators [Bor01].

These various application-dependent billing standards are a limiting factor to the effectiveness of conventional billing systems for NGNs as they prevent them from meeting the four requirements determined previously:

- Convergent billing: UDRs have vendor-specific formats and are exchanged through service-dependents 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. Therefore operators either try 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. These security holes can then be easily exploited for fraud [NT04].

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. IPDR has been identified as such a standard.

4 AN OVERVIEW OF THE IPDR STANDARD

IPDR is an acronym for Internet Protocol Detail Record. Initially designed for IP-based services, IPDRs are more general UDRs thus enabling to bill for different types of existing as well as new services. IPDRs can be used for usage data as well as for settlement data, and therefore require few interfaces between different billing systems. This standard is defined by IPDR.org.

IPDR.org is a consortium of leading service providers 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. IPDR.org has more than 20 member companies among which Cisco, Hewlett-Packard and Marconi. [Ipd04a].

According to the latest version (version 3.5.0.1) of its “map and overview” document [Ipd04b], released in November 2004, the IPDR solution relies on a reference model that specifies interfaces to exchange IPDRs between IPDR-enabled devices or systems. This model is shown in Figure 2.

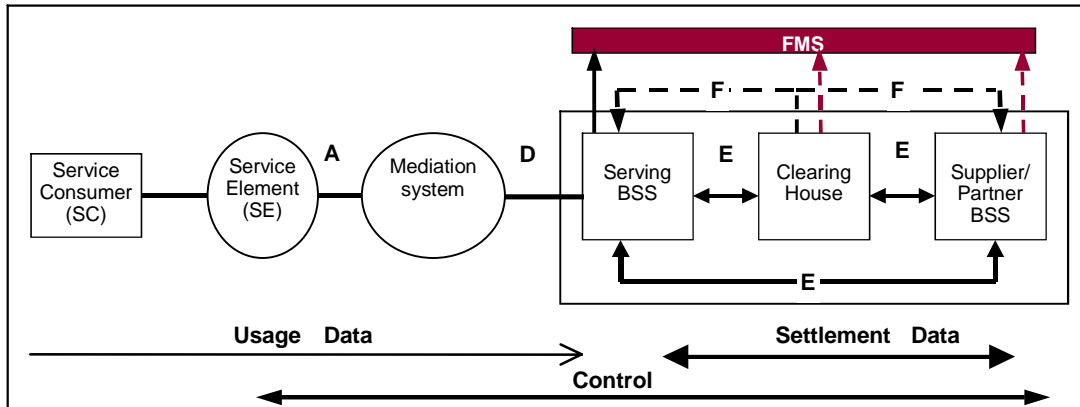


Figure 2. IPDR.org reference model [Adapted from Ipd04b]

In Figure 2 BSS stands for business support system. A BSS is a system that supports business operations (e.g. a billing system or a customer relationship management system). We have added a separate shaded block (FMS) and its associated arrows to the diagram to illustrate the positioning of one FMS within this model. The FMS spans over the operator's BSSs, namely the billing system, the clearinghouse and the suppliers' BSSs, from which it can receive billing records for inspection.

Every IPDR contains the "5Ws" elements: who, when, what, where, why. Additional service-specific attributes can be added (e.g. quality of service, bandwidth and latency). IPDRs can be encoded using two available formats: 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. Figure 3 shows a simple IPDR document in XML format for an incoming email.

```
<?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 3. Instance IPDR document for incoming email in XML format

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. IPDRs can be created and transmitted at regular intervals for ongoing service usage to cater for "always on" IP connections in NGNs.

Already twelve leading billing and mediation systems vendors – including Amdocs, Hewlett-Packard and Marconi – have implemented version 3.1 of the IPDR specifications released in 2002. They have been successfully selling IPDR-compliant products worldwide for three years. In

addition, IPDR.org has established some partnerships with standard bodies such as: ITU-T, the standard body of the International Telecommunications Union (in June 2002), Wi-Fi Alliance (in December 2003), ATIS (in October 2004) and, recently, CableLabs (January 2005) [Ipd04a].

The above analysis clearly shows that the IPDR standard is a promising solution for NGN services billing and consequently also for NGN fraud detection.

5 USING IPDR FOR NGN BILLING AND FRAUD DETECTION

Based on the above-mentioned description of IPDR, it can be inferred that this standard can help satisfy NGN billing requirements identified in Section 2 the following way:

- **Convergent billing:** IPDRs stop vendor-format dependency and reduce interfaces through standardization. The use of the popular XML language facilitates billing system interoperability.
- **Real-time billing:** real-time billing is facilitated since IPDRs can be generated periodically while a service is in use and not only for completed usage data. Besides, if the service elements generate usage records directly in IPDR format, no normalization is required which 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 overhead. Besides XML tags can be quickly added and removed 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.

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. Some speculations on the future of fraud in NGNs is summarised in the following paragraph.

Various experts [Joh02] claim that with the expansion of m-commerce in NGNs, fraudsters are likely to target service content (the service or good purchased) rather than connection (the phone call or Internet access). However they also state that, although some new forms of fraud might appear in NGNs, current fraud types will still prevail but will be committed with new technologies. Besides, due to the convergent nature of NGNs, it is highly likely that fraud from various communities (financial, Internet, IT hackers, telecommunications fraudsters) will converge. Therefore joint work between the separate fraud management, security, risk management, revenue assurance, network security, and credit control teams is a necessity [Joh02]. Based on these assumptions, some highly potential NGN fraud types and their fraud indicators, as described by [AL02] are as follows:

- **Subscription fraud:** it is the subscription to a service with no intention to pay by either using his own identity (slightly modified) or impersonating someone else. It is currently the most common fraud type [Jac04] and will most probably remain so in NGNs. Some of its fraud indicators are the following: (1) a high number of expensive services are quickly requested, (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 quickly detected in case of (2).
- **Unauthorised access to resources:** This refers to obtaining free unauthorised access to resources. Some indicators for this fraud type are: (1) an individual receives resources without

corresponding billing records in the billing system, (2) many costly downloads are performed. In 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 case of (2) real-time billing increases the chance of quickly detecting fraud.

- Illegal redistribution of service: a customer legally or illegally downloads material (e.g. movies) and redistributes it to other individuals. Some pointers for this form of fraud are: (1) a live event is downloaded at the same time as a significant volume of data is uploaded, (2) downloaded and uploaded data have same characteristics. Real-time billing can allow timely fraud detection for (1). In 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 of detecting the above-mentioned fraud occurrences and catching the fraudster before significant damage is done can be greatly increased.

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, due to their highly distributed architecture IP networks enable fraud to be committed from various points simultaneously. This necessitates the constant exchange of information between all service elements and network devices [IEC04c]. IPDR records can thus 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-based networks.

6 CONCLUSION AND FUTURE WORK

In this paper the IPDR standard has been proposed as a solution to the inadequacy of current billing systems for NGN fraud detection. As billing records constitute the main source of information for fraud management systems, identifying an appropriate format and transmission method for NGN billing records is the first step towards our research project main goal: designing a fraud management system suitable for convergent networks. This paper has reviewed the limitations of current billing systems and billing standards with regard to NGN fraud detection and evaluated the advantages of using IPDR to overcome these weaknesses. 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 2.

Future work will consist of testing the added efficiency of fraud detection for NGNs by analyzing a database of billing records in IPDR format for signs of fraud. This will serve as a proof-of-concept for the statements made in this paper. Such statements can be summarized as follows: NGNs imply *networks convergence*. Therefore we must expect *fraud convergence* and have *convergent billing* through *convergent usage records* for effective *convergent fraud management*.

7 REFERENCES

[AL02] ABRAMOWICZ, D & LEDBERG, P. 01 December 2002. IP fraud – Methods and algorithms for detecting IP-based fraud. Master thesis. Swedish Royal Institute of Technology. Göteborg, Sweden.

[Ama03] AMAT, J. 2003. "Charging data collection: the key to revenue generation". *Alcatel telecommunications review*. 3rd Quarter 2003. Strategy white paper. p. 1-5. [Online]. Available:

http://www.alcatel.com/doctypes/articlepaperlibrary/pdf/ATR2003Q3/S0309-Data_Collection-EN.pdf. [Cited 24 March 2005].

[ATIS04] ATIS. 2004. "ATIS Publishes Exchange Message Interface Guidelines". [Online]. Available: <http://www.atis.org/PRESS/pressreleases2004/022704b.htm>. [Cited 30 March 2005]

[BEO04] BIHINA, M. ELOFF, J & OLIVIER, M. Requirements for Next-Generation Networks billing systems. *Proceedings of SATNAC 2004: the Southern African Telecommunications Networks and Applications Conference*. Stellenbosch, South Africa. September 6-8.

[Bor01] BORTHICK, S August 2001. Call accounting and Billing for IP services. *Business Communications Review*. August 2001 issue. [Online]. Available: <http://www.bcr.com/bcrrmag/2001/08/p28.php>. [Cited 31 March 2005].

[Hui99] HUITEMA, C. 1999. Challenges of the next generation networks. *Keynote for Internet'99 conference, Moscow, October 25-28*. [Online]. Available: <http://www.huitema.net/papers/challenges/challenges99.html>. [Cited 07 May 2004].

[IEC04a] IEC - The International Engineering Consortium. 2004a. Telephony billing. *Web ProForum Tutorials*. [Online]. Available: http://www.iec.org/online/tutorials/tele_bill/. [Cited 07 May 2004].

[IEC04b] IEC - The International Engineering Consortium. 2004c. Billing in a 3G environment. *Web ProForum Tutorials*. [Online]. Available: http://www.iec.org/tutorials/billing_3g/topic03.html. [Cited 07 May 2004]

[IEC04c] IEC- The International Engineering Consortium. 2004. Fraud analysis in IP and Next-Generation Networks. *Web ProForum Tutorials*. [Online]. Available: http://www.iec.org/tutorials/fraud_analysis/. [Cited 07 May 2004]

[Ipd04a] IPDR.ORG website. <http://www.ipdr.org>. [Cited 02 February 2005]

[Ipd04b] IPDR.ORG. November 2004b. Document map and overview. Version 3.5.0.1. [Online]. Available: <http://www.ipdr.org/public/DocumentMap/DMO3.5.0.1.pdf>. [Cited 4 April 2005]

[Jac04] JACOBS, R. 2004. "Telecommunications fraud". Dimension Data white paper. [Online]. Available: http://www.didata.com/services/white_papers/Fraud_White_Paper.pdf. [Cited 07 May 2004].

[Joh02] JOHNSON, M. January 2002. "Future Frauds: Telecom fraud in Next Generation Services". The Commonwealth Government and business guide to Information and Communication Technology. [Online]. Available: <http://www.cto-ict.org/index.php?dir=04&sd=30&aid=1012>. [Cited 24 February 2005].

[Luc04] LUCAS, M. October 2004. "Where rating should be implemented?". *Billing world and OSS today*. [Online]. Available: <http://www.billingworld.com/archive-print.cfm?ArchiveId=7618>. [Cited 24 March 2005].

[Lun02] LUNDIN, E. 2002. *Aspects of employing fraud and intrusion detection systems*. Thesis for the degree of Licentiate of Engineering. Department of Computer Engineering, Chalmers University of technology, Göteborg, Sweden.

[NT04] NEXUS TELECOM. 2004. Next-Generation Networks: billing challenges. [Online]. Available: <http://www.nexus-ag.com/billing.0.html>. [Cited 01 June 2004].

[NTIA04] NTIA – National Telecommunications and Information Administration. 2004. Technical and Economic Assessment of Internet Protocol Version 6 (IPv6): Glossary. [Online]. Available: <http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/draft/draftglossary.htm>.

[OHL03] OFRANE, A. HARTE & LAWRENCE. 2003. Introduction to telecom billing. ALTHOS Publishing.

[OIF02] OIF - Optical Internetworking Forum. 2 April 2002. Call detail records for UNI 1.0 billing. Online. Available: <http://www.oiforum.com/public/documents/OIF-CDR-01.0.pdf>. [Cited 04 March 2005].

[PRT02] PONNAVAIKKO, P. RAJAGOPALAN, S. & TUNGGAL, G. 12 December 2002. *Will security and billing issues push Wi-Fi down?* University of Colorado, Boulder. Online. Available: http://www.mobilein.com/WiFi_Security_Billing.pdf. [Cited 04 March 2005].

MA Bihina Bella, JHP Eloff and MS Olivier, "Using the IPDR standard for NGN billing and fraud detection," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Research in progress paper, published electronically)

©The authors

Source: <http://mo.co.za>