Fraud Detection for Voice over IP Services on Next-Generation Networks

Igor Ruiz-Agundez, Yoseba K. Penya, Pablo Garcia Bringas

Fraud Detection for Voice over IP Services on Next-Generation Networks

Igor Ruiz-Agundez, Yoseba K. Penya, and Pablo Garcia Bringas

University of Deusto
Bilbao, Basque Country
{igor.ira,yoseba.penya,pablo.garcia.bringas}@deusto.es
http://www.deusto.es

Abstract. The deployment of Next-Generation Networks (NGN) is a challenge that requires integrating heterogeneous services into a global system of All-IP telecommunications. These networks carry voice, data, and multimedia traffic over the Internet, providing users with the information they want in any format, amount, device, place or moment. Still, there are certain issues, such as the emerging security risks or the billing paradigms of the services offered, which demand deeper research in order to guarantee the stability and the revenue of such systems. Against this background, we analyse the security requirements of NGN and introduce a fraud management system based on misuse detection for Voice over IP services. Specifically, we address a fraud detection framework consisting of a rule engine built over a knowledge base. We detail the architecture of our model and describe a case study illustrating a possible fraud and how our system detects it, proving in this way, its feasibility in this task.

Key words: Next-Generation Networks, Fraud Detection, Voice over IP services, Security requirements

1 Introduction

Next-Generation Networks (NGN) do not belong to the past, and neither solely do they to the far future. This special kind of net has been evolving over the last years, parallel to the evolution the Internet, and, nowadays, they are one of the backbones of the so-called *Future Internet*. Therefore, telecommunication network operators are challenged to shift their current networks to NGN by creating an integrated global system that supplies heterogeneous services across network providers, network backbones, and geographical regions [1].

More accurately, NGN is a broad term describing the telecommunication core and access networks that will be deployed in the next years. They have been progressing to carry voice, data, and multimedia traffic over common transmission links and routers using a packet-based transport method [2]. Their aim is to provide users with the information they want, in any format, device, place or moment and at any quantity [3]. NGN are characterised by the following main features:

– Packet-based transfer of all the data

- Separation of control functions
- Decoupling and aggregation of services providing technologically-independent open interfaces
- Broadband capabilities with *quality of service (QoS)* and transparency
- User mobility and diverse identification schemes with an unified service perception

Some of the services enabled by the apparition of these networks, such as voice telephony or call centres, were already present within traditional telecommunication networks but not in an integrated way, unifying simultaneously all of them. Moreover, NGN also facilitate novel services such as multimedia, virtual private networks, e-commerce, distributed virtual reality, and data connectivity [4]. Unfortunately, the charging models and specifications are not yet completely defined.

In this way, the deployment of NGNs poses a new scenario of risks and security problems. Together with classical security risks (e.g. denial of service (DoS), sniffing, spoofing or spam), which are already adapted to NGN's special conditions, brand new threats will emerge. Standing out in this latter group, fraud is considered to be the most harmful.

Fraud from employees, consumers, third-party, computer crime, insurance or financial fraud increases every year [5]. More accurately, in our target area, telecommunications, the increment reached the 52% from 2003 to 2005 [6].

In order to face these risks, *Fraud Management Systems (FMS)* detect and analyse fraud and suggest counteractions. Traditional FMS, however, are service specific and depend on the underlying network infrastructure. As NGN introduce new services and infrastructures, FMS need to evolve too. They help in the identification of fraud signals using an automate procedure of deceit detection. The also raise alerts and countermeasures based on pre-defined rules.

The FMS collect data from multiple formats and sources, adapting the data to be treated by the system by filtering and assembling processes. When data is normalised, the detection step starts generating alerts on suspicious cases. The detection can be performed by different techniques of Artificial Intelligence.

Against this background, the contribution of this paper is three-fold: First, we present the security requirements of NGN and detail a taxonomy of fraud on telecommunications. Second, we propose an approach that uses a standard rule engine to support fraud detection based on the knowledge provided by an expert on the service to be protected. Last but not least, we describe a case experiment that tests our FMS's ability against fraud attempts and we discuss the obtained results.

The remainder of the paper is structured as follows. Section 2 introduces the related work on security requirements on NGN and defines different approaches to face fraud using a Fraud Management System. Section 3 describes the proposed system architecture and its specific requirements. It details a fraud management system based on misuse detection for Voice over IP services of the NGN. Section 4 presents a case study for the evaluation of the system architecture. Finally, Section 5 concludes and draws the avenues of future work.

2 Related work

Technology and security advance in parallel; this reason complicates foreseeing future risk scenarios and, consequently, the ways to face them. As the technology evolves, so do the security needs. Many taxonomies [7] [8] have tried to classify these threats with different terminology. In this way, we consider that security risks can be catalogued by their effect on the system or the client.

For instance, the system may suffer a service continuity interruption, ranging from attacks as Denial of Service (DoS) or physical attacks to the network or service provider hardware. Moreover, there may be abuses based on logical attacks such as insufficient validation of the services or abuses of functionality (using a service for not expected task). This latter thread is related with information disclosures due to predictable resource location, information leakage, or directory indexing.

Furthermore, intrusions may compromise network systems by executing unauthorised commands, taking advantage from architectural or design vulnerabilities. Privacy of the clients or the stored data may be exposed too by several techniques like sniffing, spoofing, spamming or phising. Access to services can be bypassed with authentication attacks (e.g. brute force or password inference) or with authorization attacks (e.g. credential prediction or insufficient authorization schemes).

Note that we focus here on the possible risks that fraud can cause to service providers, customers and stakeholders. Fraud is defined as *"a deliberate act of obtaining access to services and resources by false pretences and with no intention of paying"* [9]. Other authors [10] define fraud as the intentional act of giving a false statement about an important fact. Whenever such false statement is believed by the victim (a person or an organization), the victim relies and acts upon the untrue representation and, finally, it suffers loss of money or property as a result of relying and acting upon this untrue representation. There are also definitions of fraud [11] that provide formal analyses of notions of fraud using modal operators.

2.1 Approaches to face fraud

Dealing with fraud is a very complex task mainly due to its transversal nature to the operators structure [12]. Traditional fraud techniques are evolving and adapting to the new network infrastructure. We have to consider them because basic ideas remain despite the underlying technology. Moreover, we have to focus on the specific risks around the NGN. Although there is not a standard procedure for classifying the different types of fraud on NGN there have been some attempts [13] to do it.

Deception in telecommunications include subscription frauds, where the cheater accesses the services without being subscribed. Users can also suffer line or identify theft, being charged for services used by others. Telecommunication operators can oversee users that exceed their download quote and rate performing illegal service redistribution, sometimes for an economic profit. Finally, cloning or unauthorised access to services may lead to compromising privacy.

Anyway, the most common types of fraud on telecommunications are subscription fraud and identity theft [14]. After those, voice mail fraud and calling card fraud pre-

vail. The analysis of the different fraud techniques points out that the tendency is a convergence of the fraud, which increases the complexity of its detection [2].

Fraud Management Systems have proved to be a suitable tool to detect fraud in different networks with diverse techniques: *self-organising maps (SOM)* [2], general data mining [15], rule-based systems [16], profiling through Artificial Intelligence techniques like neural networks or decision trees [12], based on the hierarchical regime-switching models [17], Bayesian networks [18], fuzzy rules [19] or other data mining techniques [20]. There also exist works on how to discover new rules to detect fraud in telecommunications [21] and on the privacy concerns of applying detection techniques to users data [22]. Nevertheless, to our knowledge, there is none that works on fraud detection for VoIP services in NGN with use cases.

3 Misuse detection for Fraud Management Systems

Misuse detection in the scope of fraud prevention protects a system from already known fraudulent techniques or attacks [23]. An expert defines the already known vulnerabilities and takes measures to cover these eventualities. Other techniques, based on statistical measures of user behaviour, need to train the systems over a length of time to reach to a certain success threshold.

On the contrary, one of the main advantages of misuse detection is that it does not need any data processing training [24]. On the other hand, the main drawback of this approach is that the expert needs to define the vulnerabilities that the system can manage *in advance*. Nevertheless, the expert can look for known patterns of abuse that might occur by increasing the main sensibility of the system. These patterns depend on the problem environment and the knowledge of the expert is crucial.

3.1 The system architecture

Figure 1 shows the general architecture of the Fraud Management System. The service consumer uses the service elements (e.g. IPTV, VoIP, WLAN, etc.), which generate vendor specific billing data. If needed, this data is transcoded into Internet Protocol Detail Record (IPDR) format and captured by the recorder. When required, these IPDR entries can be stored or transmitted to the business support system.

The FMS is hosted in this business support system and receives data in IPDR format for its analysis, starting in this way the fraud detection process. Each IPDR is sent to the rule engine that contains the expert knowledge on fraud in order to detect possible violations using misuse detection techniques. If the FMS suspects a possible fraud, it reports the incident to the response module. As seen in section 3.3, this final module can trigger a fraud notification alarm to the system operator or it can block all the present and future connections of a suspicious client.

3.2 The Internet Protocol Detail Record

The Internet Protocol Detail Record (IPDR) intends to be the standard protocol for exchanging service usage and for managing control information between IP networks,

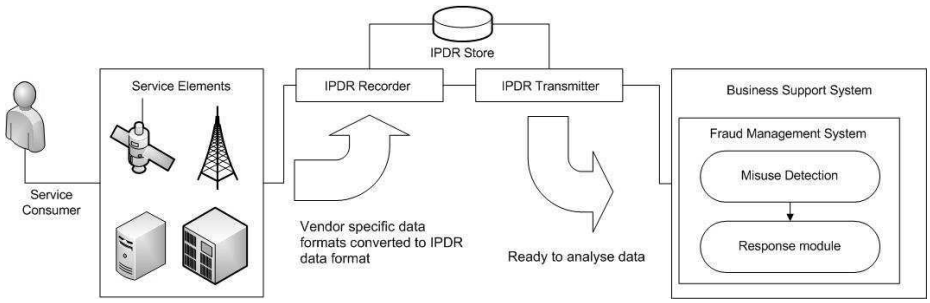

Fig. 1. Schematic architecture of the system

hosting elements and operations or business support systems. It provides a standardised framework that enables Next-Generation Network providers to operate efficiently [25].

This standard is defined by the Internet Protocol Detail Record Organization and the TeleManagement Forum. It is designed to enable cost-effective usage measurement and exchange for next-generation services across the entire value chain.

Moreover, the IPDR covers the billing requirements of NGN providing converged billing, avoiding provider dependence and reducing the required interfaces. Real-time billing is allowed, and therefore charging is performed faster. Finally, it offers great flexibility to represent existing and future services with scalability possibilities.

As fraud detection is closely related to billing, IPDR is also used for fraud detection [26]. Since it is the most adequate format to represent the obtained data, it is the base of the fraud detection analysis.

IPDRs are mainly generated at the end of each call or connection resulting in either a normal or abnormal completion of the call. Alternatively, they may be generated during the progress of call or connection. This generation is triggered by events at the beginning of a call, the answer of a call, during long calls, etc.

According to its service specifications [25], IPDR is capable of collecting usage characteristics of any IP-based network or application service. All service specifications have five common attributes in their records. The first one describes the person in charge of the usage of a service, defining user identification. The second attribute tells when a certain service is used. The third attribute defines what service is being measured (e.g. quality of service, state information, event codes, connection state, etc.). The next attribute contents information to allow traceability by providing context, source, and destination, defining in this way the place the service is consumed. The final attribute informs about the reason that triggered the event.

Even though IPDR specifies services for Internet Protocol Television (IPTV), Public Wireless LAN (WLAN) access, Streaming Media (SM), Voice over IP (VoIP) or any other service specified by the service designer, in this paper we focus on the service specification of VoIP.

Specifically, a VoIP call is started by a calling party or initiator and received by one or more call parties or recipients. The participating elements for the call include service elements, gatekeepers, and endpoints or users.

The VoIP IPDRs contain the identifiers of all call participants, the time the call was started and ended, the call progress state, the final call completion codes for each call, and the call payment type. Section 4 presents real examples of VoIP IPDR.

3.3 Task environment of the system

We will define the task environment as shown in Table 1, which outlines the challenge we are facing: defining the Performance, Environment, Actuator and Sensors (also known as PEAS) [27]. First, we specify the performance measure of the system. We will consider that the actions performed by the system will be resolved with efficacy if we are able to detect fraudulent data records in our system. In the case of the efficiency, we will consider that the problem is resolved efficiently if we are able to detect a fraud in our system with the maximum certainty, with the minimum possible computational cost, and with the minimum response time. However, maximum certain ability and minimum possible cost may be goals in conflict, so there are trade-offs involved.

Second, we will study our knowledge about the environment. We know that our environment is formed by the specification of the IPDR. The previous Section 3.2 gives a detailed description of this data records and in Section 4.2 and Section 4.3 we present two separate examples of this records. This data is encoded in XML format and it is transferred to an environment class created with an object-oriented representation. We also know the effects that the possible actions may have in the system. So far, the FMS can send a fraud notification alarm to the system operator or block all the present and future connections of a suspicious client.

Third, we will study FMS actuators, which send a notification alarm and block connections. Sensors, on the contrary, are the information that the system receives from the out site. In our case, the inputs are the set of IPDRs that the system collects from the billing information. Section 4.1 describes how the dataset of the performed experiments is obtained.

Table 1. PEAS description of the task environment for the Fraud Management System based on Misuse Detection for Next-Generation Networks

Agent Type	Fraud Management System
Performance Measure	Fraud detection Certainty Computational cost Response time
Environment	Specification of the IPDR
Actuators	Notification alarm Blocking connections
Sensors	IPDR collector

3.4 The structure of the system

So far, we have described the FMS from the point of view of its behaviour. Now, we will address the design of the program that implements the system function by mapping perceptions into actions. We also know that our FMS works on a computing device or architecture. This architecture provides perceptions from the sensors to run an appropriate process that chooses which actuator to run from the available ones.

The skeleton of our system is based on agent programs, also known as autonomous software programs [28], which uses the current perceptions as input from the sensors and returns an action to the actuators. This agent selects an action to perform on the basis of the current perception, the current IPDR. We can catalogue the agent as a simple reflex agent because its decision making is based only on the current input data [27].

Listing 1.1 shows the program of the agent. Even though the proposed agent is very simple, it works according to the performance measure, because the decision making is made only on the basis of the current perception (the environment is fully observable).

```
1  // KB, a knowledge base. Based on rules, a set of condition−action rules t,
2  // a counter, initially 0, indicating time
3  // @param p,
4  // @return Action
5  public Action KB−AGENT(Percept percept) {
6    TELL(KB, makePerceptSentence(percept,t));
7    action = ASK(KB, makeActionQuery(t));
8    TELL(KB, makeActionSentence(action,t));
9    t = t + 1;
10   return Action;
11 }
```

Listing 1.1. Knowledge-based FMS

3.5 Rule engine

Our system uses an existing framework, Drools, that provides a full set of tools to define our knowledge base. Drools is a rule engine that uses a rule-based approach to implement an expert system and can be more accurately classified as a production rule system.

The term rule engine is sometimes considered ambiguous [29] because any system using rules, in any form, can be seen as a rule engine. Nevertheless, we understand it as a full production rule system, this is, a Turing-complete system that represents knowledge with propositional and first-order logic (which is sufficiently expressive to represent a good deal of common-sense knowledge [27]). The core of the system is an inference engine that processes rules and facts by matching them with production rules in order to infer conclusions.

The production rules include a condition clause and an actions clause that will trigger when the conditions clause happens to be true. In our experiment, the person in

charge of defining the rules is an expert in the domain of the security in telecommunications. Therefore, these rules are defined with previous knowledge and are limited to the scope of the misuse detection in this specific domain. Anomaly detection, or other boundary cases, is not under the scope of this experiment.

The rules are stored in a production memory and the facts, or input data, in a working memory. Facts are asserted in the working memory, where they may then be modified or retracted. If the system has a large number of rules, many rules may happen to be true. In this case, an agenda manages the execution order of the rules in conflict.

4 Case study

In this section, we describe the experiment performed with the FMS. Section 4.1 presents the design of this case study. Section 4.2 details a legitimate use case example. Section 4.3 describes a fraudulent use case example. Finally, section 4.4 discusses the results of the experiments.

4.1 Design

The purpose of this experiment is the definition of a case study based methodology [30] which can be applied to any fraudulent scenario. We have considered that there are prefixed use case scenarios on the use of the VoIP services. The input data to the FMS follows the schema of the service specifications [31].

VoIP service sessions have two or more participants over a partial or complete Internet-based connection. The session or call is started by one of the participants (call initiator) and it is received by one or more participants (call recipients). The call is managed by different elements, such as services, gatekeepers and endpoints (or end users).

These sessions can be IP to IP, Public switched Telephone Network (PSTN) to IP, IP to PSTN, cellular to IP or any other combination. In each use case the resulting IPDR is different but maintains a fixed structure. Based on this structure, we have inferred general use cases for each scenario.

Each structure has the same flow and the same IPDR attributes. In our experiments, we are only interested in the IPDRs; hence, we have studied the attributes involved in each use case. These attributes have a wide range of possible valid values and their presence is known beforehand.

In this way, based on the structure of each use case, we study the attributes and their possible values in order to simulate the content of the IPDR and obtain valid data for our experiment.

4.2 Legitimate use

One of the use cases we have considered in our experiment is the legitimate use of the VoIP services. In particular, we have performed a use case in which the call initiator has a cellular phone and the call recipient has an IP telephone [31]. The basic flow of this example is similar to the one presented in Section 4.3.

Listing 1.2 shows an example of the IPDR for this use case. In our scope of fraud detection, the main attributes of this record are the destination identification, the unique call identification, the personal identification number, the start access time and end time, the call duration, the average latency and the incoming codec.

```
<IPDR>
  <IPDRCreationTime>2009−07−07T13:21:08.031+02:00</IPDRCreationTime>
        <seqNum>1</seqNum>
        <subscriberID>Vendor Phone−1027365692</subscriberID>
        <hostName>author.gateway.123</hostName>
        <ipAddress>192.168.1.197</ipAddress>
        <startTime>2009−07−07T18:29:35.448+02:00</startTime>
        <endTime>2009−07−07T18:51:31.448+02:00</endTime>
        <timeZoneOffset>60</timeZoneOffset>
        <callCompletionCode>CC</callCompletionCode>
        <originalDestinationId>555−066−0023</originalDestinationId>
        <uniqueCallId>52s70uj5−1507−2954−xspx−7b86x2a23q66</uniqueCallId>
        <imsiIngress>445594063997989</imsiIngress>
        <esnIngress>49916516</esnIngress>
        <disconnectReason>NormalCallClearing</disconnectReason>
        <ani>555−467−0100</ani>
        <pin>6333276</pin>
        <serviceConsumerType>EU</serviceConsumerType>
        <startAccessTime>2009−07−07T18:29:14.448+02:00</startAccessTime>
        <callDuration>1337000</callDuration>
        <averagePacketLatency>105</averagePacketLatency>
        <type>V</type>
        <feature>H</feature>
        <incomingCodec>G726</incomingCodec>
        <ipAddressEgressDevice>192.168.1.205</ipAddressEgressDevice>
        <portNumber>4724</portNumber>
        <homeLocationIdEgress>MT43AGR5</homeLocationIdEgress>
</IPDR>
```

Listing 1.2. Cellular to IP use case IPDR

4.3 Fraudulent use

In order to test our FMS against illegitimate use we implemented one of the classical telephone service fraud, inspired on the *blue box* phreaking tool.

This tool is an electronic device that simulates a telephone operator's dialling console [32]. Originally it was used to replicate telephone tones to switch log-distance calls and to route the user's call bypassing the normal switching mechanism. The main use of the blue box was to make free telephone calls. These systems are nowadays based on digital technologies and they do not use in-band signalling, which the blue box originally emulated. Nevertheless, for the purpose of our experiment, we have assumed that the essential idea of this tolls is still working in spite of the underlying technology has changed.

Based on this box principle, we address the following scenario. There is a client that is going to commit fraud in a voice service call. We suppose that he makes a phone call and does not pay for it, or at least he pays less time of consumption than the real amount he really has consumed.

Figure 2 illustrates the basic flow of this example. It starts with the call of the client to the local access number for the gateway (1). The gateway queries a network element that verifies the subscribers account (2-3). The user is asked to enter a PIN and a destination phone number (4-5). After that, the gateway consults the gatekeeper on ways to route the call and establishes a connection between the terminal and gateway (6). The gateway places the call to the PSTN by out-pulsing the destination number (7). At this point, the client tries to commit fraud by deceiving the gateway and by making it think that he hangs down (8). However, the connection is still alive and the fraudulent user is able to maintain a conversation with the destination number without being charged or being charged less than what it should.

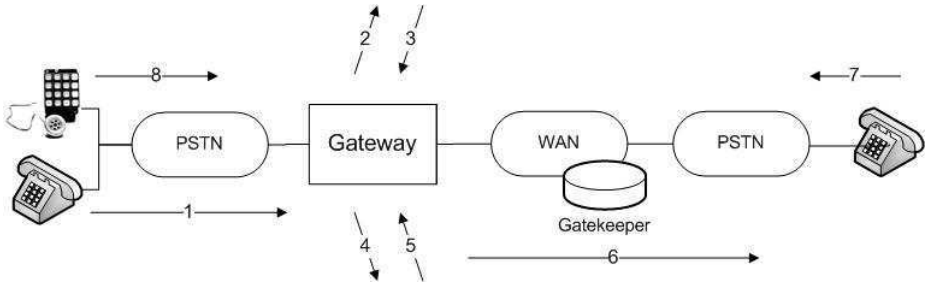

Fig. 2. Fraudulent use case

Listing 1.3 shows the IPDR of this use case. The main attributes that indicate fraud in this record are the start access time, the end time, and the call duration. The goal of this fraud is to falsify the ending time of the call, making it briefer than it real was. Nevertheless, and in this use case, the call duration will represent the real call duration value. If we use these three variables and analyse non correspondences between them, we are able to detect fraudulent use cases.

```
<IPDR>
  <IPDRCreationTime>2009−07−07T13:21:08.078+02:00</IPDRCreationTime>
        <seqNum>3</seqNum>
        <subscriberID>Vendor Phone−573460227</subscriberID>
        <hostName>author.gateway.123</hostName>
        <ipAddress>192.168.1.210</ipAddress>
        <startTime>2009−07−07T20:42:36.053+02:00</startTime>
        <endTime>2009−07−07T20:56:42.053+02:00</endTime>
        <timeZoneOffset>60</timeZoneOffset>
        <callCompletionCode>CC</callCompletionCode>
        <originalDestinationId>555−680−9802</originalDestinationId>
```

```
        <uniqueCallId>12l93my3−1546−3231−rmoi−2h61q7z54l47</uniqueCallId>
        <imsiIngress>861425764477418</imsiIngress>
        <esnIngress>59148223</esnIngress>
        <disconnectReason>NormalCallClearing</disconnectReason>
        <ani>555−906−5415</ani>
        <pin>2315855</pin>
        <serviceConsumerType>EU</serviceConsumerType>
        <startAccessTime>2009−07−07T20:41:40.053+02:00</startAccessTime>
        <callDuration>66666666</callDuration>
        <averagePacketLatency>80</averagePacketLatency>
        <type>V</type>
        <feature>H</feature>
        <incomingCodec>G711Alaw</incomingCodec>
        <ipAddressEgressDevice>192.168.1.244</ipAddressEgressDevice>
        <portNumber>15745</portNumber>
        <homeLocationIdEgress>OS38SJT3</homeLocationIdEgress>
</IPDR>
```

Listing 1.3. Fraudulent use case IPDR

Listing 1.4 shows a rule to detect this fraudulent use of a phone service. It is based on the incoherence of the call duration time. For this case, it checks that the difference between the start access time and the ending time have the same value as the call duration attribute. If the values are not equal the system detects a fraudulent use of the voice service.

Other rules could be applied to this IPDR, looking for other fraud evidences. The attributes subscriberID, callCompletionCode, incomingCodec or any other could be combined in many different ways creating new heuristic rules to feed the FMS.

```
rule "Incoherent CallDuration time"
  when
    // Variable declaration
    $ipdrVoIPType : EnlargeIPDRVoIPType( )
    // Get the call duration and check that does NOT equals to endTime− startAccessTime
    eval(!($ipdrVoIPType.getCallDuration().equals($ipdrVoIPType.checkCallDuration())))
  then
    System.err.print( "Alert! Incoherent CallDuration time for the IPDR with " );
    System.err.print( "seqNum " + $ipdrVoIPType.getSeqNum() + " and uniqueCallId " +
        $ipdrVoIPType.getUniqueCallId() );
end
```

Listing 1.4. Incoherent call duration time detection rule

4.4 Results

In order to assess the validity of the proposed architecture in section 3.1, we have performed different kinds of tests in our test-bed environment. Since synthetic fraud data has been proved to be more suitable than authentic data when it comes to testing and training of fraud detections systems [33], we have tested a representative subset of VoIP

IPDR records, both legitimate and fraudulent cases from a generated dataset. This generation followed a structured process to ensure the data validity.

Table 2 shows a partial outcome, with three data records, of a bigger execution result. The system inserts a VoIP IPDR record into the system for its analysis. Once the system performs the analysis, it reports the result based on the expert knowledge represented within the rule-set.

Table 2. Execution results

Sensors		**Actuators**
uniqueCallId	**Other parameters**	**Notification alarm**
52s70uj5-1507-2954-xspx-7b86x2a23q66	See IPDR in Listing 1.2	no action
12l93my3-1546-3231-rmoi-2h61q7z54l47	See IPDR in Listing 1.3	triggered
55r56gz4-3990-6841-xywy-4b38l1e72i58	Yet another IPDR	no action

In the case of these experiments, if the call duration is coherent, the system informs that the record is valid. In case of an incoherent call duration, the system prompts an alert and takes the pertinent measures through its actuators as described in section 3.3.

Since the results confirm that the proposed system is valid to perform misuse detection for Voice over IP services, the architecture design is ratified. Therefore, the fraud management system works as expected detecting fraud based on the expert knowledge. The system expansion is guaranteed by adding more rules by the domain expert. Other rules would use different attributes and relations, enabling new detection capabilities.

5 Conclusion

In this paper, we introduce a misuse-detection-based system to detect fraud on Voice over IP services on Next-Generation Networks, in order to improve fraud management systems for NGN. We believe that detecting potential security risks contributes to the deployment of these networks by providing extra stability. Besides, the investments on infrastructures and development by telecommunication operators are stepped up.

This approach relies on a previous analysis of NGN security requirements. To this end, we present the related work on security requirements on NGN and define different approaches to face fraud.We have also studied all the existing specifications of IPDR, from the Internet protocol television to the Voice over IP. We believe that misuse detection is the best approach to build a fraud management system that controls these risks. Our analyses show that this paradigm is suitable and is able to react when a fraud attempt occurs.

Future work will focus on the automatic modelling of more use cases and on the automatic generation of new detection rules. Furthermore, as the architectural design of our fraud management system is modular, we intend to spread the system detection capabilities to other services besides the Voice over IP services.

References

1. Mao, Z., Douligeris, C.: A distributed database architecture for global roaming in next-generation mobile networks. IEEE/ACM Trans. Netw. **12**(1) (2004) 146–160
2. Bella, M.B., Eloff, J., Olivier, M.: A fraud management system architecture for next-generation networks. Forensic Sci Int **185**(1) (March 2009) 51–58
3. Liu, Y., Liang, X.: New regulations to the next generation network. In: Communications and Mobile Computing, 2009. CMC '09. WRI International Conference on. Volume 2. (Jan. 2009) 172–174
4. Crimi, J.C.: Next Generation Network (NGN) services. In: Telcordia Technologies. (2000)
5. KPMG Forensic: Fraud survey. http://www.kpmg.com/
6. Communications Fraud Control Association: Global telecom revenues increase 12% and fraud increases 52% from 2003-2005. http://www.cfca.org/ (2006)
7. Web Application Security Consortium: Threat classification. http://www.webappsec.org/
8. Howard, J., Longstaff, T.: A common language for computer security incidents. Technical Report Sandia Report: SAND98-8667, Sandia National Laboratories (1998)
9. Kvarnstrom, H., Lundin, E., Jonsson, E.: Combining fraud and intrusion detection - meeting new requirements. In: Fifth Nordic Workshop on Secure IT systems (NordSec2000). (2000)
10. Simmons, M.R.: Recognizing the elements of fraud. http://www.facilitatedcontrols.com/fraud-investigation/fraudwww.shtml (1995)
11. Mcnamara, P., Firozabadi, B.S., hua Tan, Y., Lee, R.M.: Formal definitions of fraud. In: Norms, Logics and Information Systems - New Studies in Deontic Logic and Computer Science, IOS Press (1999) 275–288
12. Cortesao, L., Martins, F., Rosa, A., Carvalho, P.: Fraud management systems in telecommunications: A practical approach. (April 2005)
13. Bihina Bella, M.A., Olivier, M.S., Eloff, J.H.P.: A fraud detection model for Next-Generation Networks. In Browne, D., ed.: Southern African Telecommunication Networks and Applications Conference 2005 (SATNAC 2005) Proceedings. Volume 1., Champagne Castle, South Africa (September 2005) 321–326
14. Communications Fraud Control Association: Announces results of world wide telecom fraud survey. http://www.cfca.org/ (3 2003)
15. Alves, R., Ferreira, P., Belo, O., Lopes, J., Ribeiro, J., Cortesao, L., Martins, F.: Discovering telecom fraud situations through mining anomalous behavior patterns. In: Workshop on Data Mining for Busines Applications, 12th ACM SIGKDD International Conference on Knowledge Discovery Data Mining. (August 2006)
16. McGibney, J., Hearne, S.: An approach to rules-based fraud management in emerging converged networks. In: IEEE/IEI Irish Telecommunications Systems Research Symposium. (2003)
17. Hollmén, J., Tresp, V.: Call-based fraud detection in mobile communication networks using a hierarchical regime-switching model. Advances in Neural Information Processing Systems (1999) 889–895
18. Kou, Y., Lu, C., Sirwongwattana, S., Huang, Y.: Survey of fraud detection techniques. In: Proceedings of IEEE Intl Conference on Networking, Sensing and Control. (2004)
19. Estévez, P., Held, C., Perez, C.: Subscription fraud prevention in telecommunications using fuzzy rules and neural networks. Expert Systems with Applications **31**(2) (2006) 337–344
20. Weiss, G.: Data mining in telecommunications (2005)
21. Rosset, S., Murad, U., Neumann, E., Idan, Y., Pinkas, G.: Discovery of fraud rules for telecommunications—challenges and solutions. In: KDD '99: Proceedings of the fifth ACM SIGKDD international conference on Knowledge discovery and data mining, New York, NY, USA, ACM (1999) 409–413

22. Lundin, E., Jonsson, E.: Anomaly-based intrusion detection: privacy concerns and other problems. Computer Networks **34**(4) (2000) 623–640
23. Jones, A., Sielken, R.: Computer system intrusion detection: A survey. University of Virginia, Computer Science Department, Tech. Rep (1999)
24. Kumar, S., Spafford, E.: A pattern matching model for misuse intrusion detection. In: In Proceedings of the 17th National Computer Security Conference. (1994)
25. TeleManagement Forum: IPDR Service Specification. Design Guide. http://tmforum.org/edn. (September 2008)
26. McGibneya, J., Schmidtb, N., Patelb, A.: A service-centric model for intrusion detection in next-generation networks. Computer Standards & Interfaces **27**(5) (2005) 513–520
27. Russell, S., Norvig, P.: Artificial Intelligence: A Modern Approach. Prentice Hall (2003)
28. Wooldridge, M., Jennings, N.: Intelligent agents: Theory and practice. Knowledge engineering review **10**(2) (1995) 115–152
29. Chisholm, M.: How to Build a Business Rules Engine Extending Application Functionality through Metadata Engineering. Elsevier Inc. (2004)
30. Kitchenham, B., Pickard, L., Pfleeger, S.: Case studies for method and tool evaluation. IEEE software **12**(4) (1995) 52–62
31. TeleManagement Forum: Service Specification - Voice over IP (VoIP). http://tmforum.org/edn. (November 2004)
32. Goldstein, E.: The Best of 2600: A Hacker Odyssey (Kindle Edition). Wiley (June 2008)
33. Lundin, E., Kvarnstrom, H., Jonsson, E.: A synthetic fraud data generation methodology. In: Proceedings of the 4th International Conference on Information and Communications Security, Springer-Verlag (2002) 277
34. Axelsson, S.: Intrusion detection systems: A survey and taxonomy. Chalmers University of Technology, Dept. of Computer Engineering, Göteborg, Sweden, Technical Report 99–15
35. Baluja, W., Llanes, A.: Estado actual y tendencias del enfrentamiento del fraude en las redes de telecomunicaciones. Ingeniería Electrónica, Automática y Comunicaciones **XXVI** (2005) 46–52
36. Bihina Bella, M.A., Eloff, J.H.P., Olivier, M.S.: Using the IPDR standard for NGN billing and fraud detection. Research in progress paper, http://mo.co.za/abstract/ipdrfraud.htm (June/July 2005)
37. Choi, M.J., Hong, J.W.K.: Towards management of next generation networks. IEICE Trans Commun **E90-B**(11) (2007) 3004–3014
38. Hearne, S., McGibney, J., Patel, A.: Addressing fraud detection and management in next-generation telecommunications networks. (2004)
39. JBoss: Drools documentation. http://jboss.org/drools/
40. Takuji, T.: Backend systems architectures in the age of the next generation network. NEC Technical Journal **1**(2) (May 2006) 51–55
41. Vincent, J., Mintram, R., Phalp, K., Anyakoha, C.: AI solutions for MDS: Artificial Intelligence techniques for Misuse Detection and localisation in telecommunication environments (2007)