Telephony Fraud Detection in Next Generation Networks

Simon Augustin, Carmen Gaißer, Julian Knauer, Michael Massoth, Katrin Piejko, David Rihm and Torsten Wiens
Department of Computer Science
Hochschule Darmstadt
Darmstadt, Germany
senily64dx@googlemail.com, carmen.gaisser@stud.h-da.de, jpk@goatpr0n.de, katrin.piejko@stud.h-da.de,
david.rihm1@freenet.de, michael.massoth@h-da.de, torsten.wiens@h-da.de

***Abstract*—Telephony fraud is a growing problem for telecommunication service providers that operate Next Generation Networks (NGN). This paper describes a framework for a rule-based fraud detection system. The classification of fraudulent calls is based on Call Detail Records (CDR) that are used by telecommunication service providers for billing purposes. By analyzing this data, fraud can be detected efficiently. We propose a method for accomplishing this. The work has been conducted in collaboration with a telephony service provider that made real-life CDR data available for analysis. The main achievement of this paper is the description of a rule-based system that detects telephony fraud using CDR data.**

Keywords-Communication system security; Communication system signaling; Communication system traffic; Computer network management; Next generation networking

I. INTRODUCTION

Telephony fraud is a serious problem for carriers that operate Next Generation Networks (NGN). Attackers regularly try to compromise accounts of users or providers to circumvent charging systems or to cause financial harm to customers. Telephony fraud comprises unauthorized deletion or alteration of billing records, unauthorized bypassing of lawful billing systems, unauthorized billing and the taking of service provider property [1].

A. Current situation

The Communications Fraud Control Association (CFCA) estimated in 2009 that fraud leads to a worldwide annual loss of 74 to 80 billion USD [2]. It is expected that this value will increase in the future. The top three fraud types, as named in their report, are (see Figure 1):

- Subscription or identity theft (22.0 billion USD)
- Compromised Private Branch Exchange (PBX) systems (15.0 billion USD)
- Premium rate service fraud (4.5 billion USD)

Even single fraud attacks may cause significant losses. In one case, an attacker conducted 11,000 calls to Australia, causing an estimated damage of more than 120,000 USD. These calls were made over a period of only 46 hours [3]. These losses could be drastically reduced if effective real-time fraud detection mechanisms were applied.

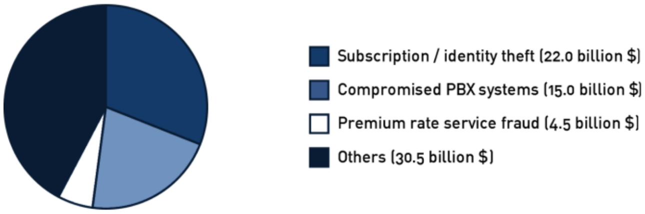

Figure 1. Top three fraud types

This kind of fraud also causes significant economic damage because some small- and medium-sized enterprises (SME) may not be able to deal with the amount of financial damage caused by these attackers, possibly leading to bankruptcy.

B. Challenges in fraud detection

In order to develop well performing fraud detection mechanisms, access to real world data is necessary. However, telecommunication providers are not allowed to expose this data due to privacy reasons. This is caused by national legal limitations, for example the German “Bundesdatenschutzgesetz” (Federal Data Protection Act) [4]. Additionally, fraud detection is not just a binary problem. The precise classification of calls as fraudulent or not with a minimum of false positives is difficult. There are cases that cannot be decided with certainty. Therefore, fraud detection has to be treated as an n-class problem [5].

C. Structure of the paper

This paper is structured as follows: Section II gives an overview on the recent activities in the field of fraud detection. Section III describes the basic concept of fraud detection and our design decisions for the framework. After the fundamentals have been explained, a more detailed description of our approach is given in Section IV. The paper ends with a conclusion and an outlook on future work in Section V. Acknowledgements follow in the last section.

II. RELATED WORK

In this paper, a rule-based system for fraud detection is described. The field of fraud detection can be divided into multiple categories. Two important ones are rule-based approaches and neural networks. There are also additional approaches, for example Bayesian Networks, Support Vector

ISBN: 978-1-61208-199-1

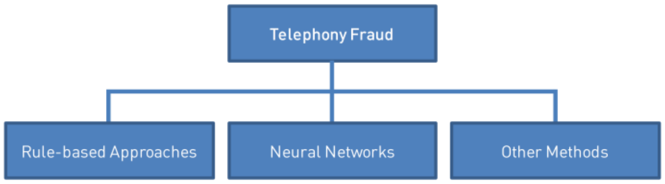

Figure 2. Methods to counter telephony fraud

Machines and Hidden Markov Models. These are described in Section II.C (see Figure 2).

A. *Rule-based methods*

Rule-based methods are very effective, but hard to manage. Extensive work is required to specify rules for every imaginable fraud case. Another downside is that rule-based fraud detection systems need to be updated frequently to cover new kinds of fraud [6].

Rosset et al. [7] proposed an extension of the C4.5 algorithm that divides a rule-discovery process into two steps. The first step generates a large number of candidate rules. The second step puts together a rule-set from these candidates. Olszewski [8] constructed a detection method based on user profiling by employing the Latent Dirichlet Allocation (LDA). Using the Kullback-Leibler divergence, the participants are classified as “good” or “evil”. Ruiz-Agundez et al. [9] propose an architecture for rule-based mechanisms that can be applied on NGN infrastructures.

B. *Neural networks*

One of the alternatives to rule-based approaches for classification are neural networks. These are more suitable to cover new and unknown attacks. Taniguchi et al. [10] summarize three methods for fraud detection, one being a neural network. They claim that these three types are able to detect 85% of all fraud cases that occurred in their test set.

1. The first method consists of the application of a feed-forward neural network. It is used to learn a discriminative function to classify service subscribers using summary statistics.
2. The second method applies a Gaussian mixture model to determine the probability of the user’s future behavior. This is based on user behavior in the past. The probabilities are used to validate the current behavior in order to detect deviations.
3. The third method uses a Bayesian network. Here, statistical properties of users and of multiple fraud cases are used.

The application of neural networks for fraud detection in mobile communication has been introduced by Qayyum et al. [11]. A disadvantage of their approach is that further adjustments are needed for the system in order to work efficiently.

C. *Other methods*

The pattern recognition skills of the human eye are very powerful. Therefore, Cox et al. [12] proposed to apply humans in the process of fraud detection. They introduced multiple techniques to visualize network traffic in a human readable way. Hollmén and Tresp [13] proposed a system that is based on a hierarchical regime-switching model. This system receives inference rules from a junction tree algorithm and is trained by using the Expectation Maximization (EM) algorithm.

III. CONCEPT AND OVERALL SYSTEM DESIGN

Every internet telecommunication service provider uses charging systems that log each call that was made using the network of the service provider. These log files contain detailed information about calls, and are commonly referred to as Call Detail Records, or sometimes as Call Data Records (CDR). In the CDR, the subscriber numbers of caller and callee, the date and time when the call was made and the call duration are recorded. Therefore, these log files contain valuable information that can be used to detect telephony fraud. Since CDR data is not allowed to be exposed to the public because of German legal regulations, the data provided by the cooperating telecommunication service provider had to be anonymized.

Our system uses CDR files and analyzes them for anomalies (see Figure 3). This is accomplished by different filters. Each filter scans the CDRs using specific rules. If an anomaly is detected, and one of the filters supplies a positive result, there is a strong suspicion that a fraud case has occurred. This fraud case has to be validated by a human and further actions, for example the temporary deactivation of an account, have to be taken. Our framework does not automatically perform these actions, as telephony fraud comprises false positives.

The framework has been implemented in Python 2.7. The decision to use Python resulted from several considerations. First of all, Python can be learned quickly and, due to its code structure, is easy to read. This ensures a quick start of implementation and results in low costs for later maintenance and the addition of extensions. Furthermore, Python is an open source product that is highly portable and runs on almost every operating system [14].

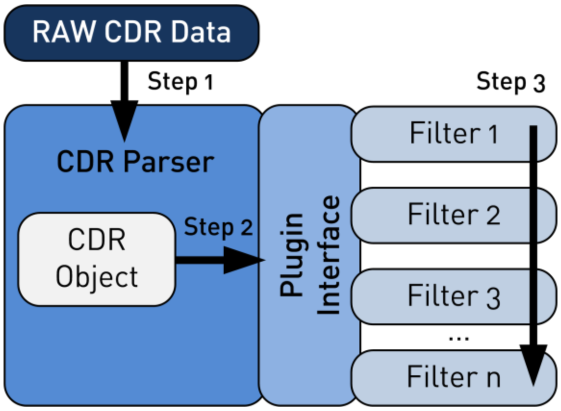

Figure 3. System overview

ISBN: 978-1-61208-199-1

IV. System Components

In this section, the system components are described in detail.

A. Structure of a CDR

Each CDR consists of several elements that correspond to different functionalities. These elements indicate the start and the end of a call, among other parameters. Each element contains the date and time when the element was written. The first element, indicating the beginning of a record, contains the unique session ID that identifies a CDR. The elements that are necessary for further analysis are now described in more detail.

The Incoming element of a CDR (called A-element in the CDR specification) contains the properties of an incoming call [15]. For our purpose, only the carrier ID (n-attribute of the A-element) is important.

The Connected element (C-element) only exists if a conversation was established. The C-element consists of several sub-elements. For example, its x-element contains the Session Initiation Protocol-(SIP) data of the connection. The SIP data contains several fields, starting at position zero. The first field corresponds to the number of the callee. The 13th and 25th field both contain the customer ID or the subscriber number. Furthermore, the C-element includes the duration of a call in milliseconds.

If a call lasts longer than 15 minutes, the CDR is split into multiple parts. These parts can be identified by the first number in the S-element. This element is the first element in a CDR, indicating the beginning of the CDR. If the call duration is below 15 minutes, the identifier is set to ”0”. If it indicates the start of a record series, it is set to ”1”. The final part is marked ”3”. All parts in between are set to ”2”.

If a call is finished, the Disconnecting element (D-element) is written. In this element, the reason for the call’s termination is stored. The From-field in this element is also important, as it indicates which party hung up. In a nutshell, the C- and the D-element provide the necessary information to bill a call.

B. Framework

To analyze the CDRs, we developed a framework that is capable of parsing the log files generated by the billing system. The framework consists of multiple parts:

- Classes for CDRs and CDR-elements into which the input data is parsed.
- The main part of the software that controls the application flow.
- Several filters implementing the rules for fraud detection.

Now, the individual parts of the framework are explained in more detail.

1. CDR Classes: The framework contains classes for each CDR element (see previous section). This modular structure provides easy filter access to the different CDR elements.

2. Main part: This part of the software controls the application flow. It starts the application, evaluates the console commands for the input files that are to be parsed and registers the different filters. The filters are organized as a list, which is iterated for each input CDR. To expand the software, more filters can easily be integrated into the analysis process, simply by adding them to the list of registered filters.

The CDR parser starts to read the data from the given input files. Each CDR is parsed from the log files into a CDR object. Each filter expects a CDR object as input and analyzes it. After the input files have been parsed completely, the results from the filters are collected by the main part. If one filter or multiple filters have detected a potential fraud case, the output is saved to a text file. In this case, an operator is alarmed.

The release candidate comes as a console application. A graphical user interface has not been included, since the software is used by the technical staff of the cooperating telecommunication service provider and the systems that process the CDRs are UNIX-based. Hence, a command line interface is sufficient.

C. Filters

The framework includes a filter base class that is inherited by all implemented filters (see Figure 4). This base class contains methods for all filters, e.g., for the formatting of date and time, and a method that returns the results. For each rule, which was defined to detect fraud, a filter is implemented. Each filter analyzes a given CDR, evaluates it for fraud-suspicious data and returns the collected results to the main class.

In general, all filters only regard calls originating from the internet telecommunication service provider's network, as only these calls are charged. These are identified if the callee’s subscriber number corresponds to a customer ID and the carrier ID in the Incoming element of the CDR does not correspond to the service provider’s ID.

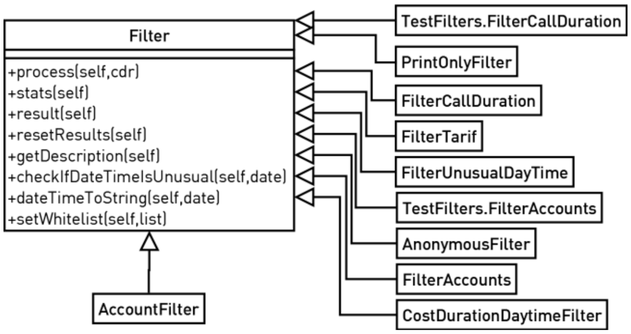

Figure 4. Filter base class and inherited classes

Up to date, four filters have been developed. The first filter regards only single calls of a customer. The second one regards all calls of a specific customer per hour. The third filter scans for signaling errors and suppressed caller IDs, while filter number four considers historical user data.

The first filter analyzes a single call for the following criteria:

- The duration of the call, depending on the destination pay scale area.
- The date and time when the call was made.

To classify the pay scale area, the destination area code of the callee's subscriber number is analyzed. We defined four categories of pay scale areas:

1. No charges: The first category classifies calls that only cause low charges or none at all. Therefore, these calls are omitted. As the software was developed in cooperation with a German company, the relevant area codes include the German fixed network, Voice over Internet Protocol (VoIP) and national subscriber numbers.
2. Moderately expensive: This category comprises calls destined for the German mobile network. These calls are not very expensive, regarding the charges per minute. In this case, calls lasting for more than a specific threshold are considered unusual.
3. Expensive: To simplify the classification, this category includes all calls that do not belong to one of the other categories. These are calls that are destined for international and special rate numbers. A threshold for the call duration is set accordingly.
4. Very expensive: Satellite calls belong to the most expensive category. These calls may be charged at up to 20 € per minute. Therefore, the threshold in this category is considerably lower than the thresholds in the previous categories. The second criteria for this filter are the date and the time when the call took place. If, for example, a company only has business customers, it can be assumed that calls outside the business hours or on weekends are more suspicious than others.

The second filter regards all calls that are made by a specific customer in a given time frame. The criteria are as follows: If the amount of calls per hour is greater than a specific value or if the overall call duration per hour exceeds a specific threshold, it is assumed that this is a fraudulent usage of the telephony service.

The first and the second filter also include a whitelist for specific customers. Whitelist candidates are customers who would regularly be above the thresholds with their normal call behavior, and therefore would be considered as fraudulent. Those customers are maintained in the whitelist and are ignored by the filters.

The third filter scans the input data for signaling errors and suppressed caller IDs, since these may also denote fraud cases. These parameters are only considered for analysis if they are found on incoming calls. Additionally, data in the CDRs indicating the connection quality is assessed by this filter. One of the typical fraud scenarios consists of routing calls via multiple international service providers. In these cases, connection quality may drop significantly. Therefore, low connection quality may be another indicator for fraud cases.

The fourth filter collects historical user data, for example the total duration of calls made by a single user or by all users. Here, up to seven categories may be included. Additionally, this filter is able to output descriptive statistics and diagrams as a PDF file.

Another interesting information in a CDR is the reason for call termination, which is stored in the D-element. Among the possible reasons, SIP and identity errors are the most interesting ones from the perspective of fraud detection. These reasons can also be used for statistical purposes or to detect internal network errors.

The filter rules and their associated thresholds have been determined by a thorough evaluation of actual fraud cases. This has been actively supported by the collaborating service provider. Unfortunately, it is not possible to describe the rules and thresholds in more detail. A publication of these parameters would give attackers a significant advantage in bypassing the system, which is productively used.

D. Conclusion and future work

In general, the presented rule-based approach for detecting telephony fraud is promising. The described solution performs well on the real-life CDRs delivered by the service provider, regularly classifying about 4% as false positive fraud cases. Additionally, it is almost an order of magnitude faster than the solution previously used, which was script-based. For example, the presented system is able to process typical CDR files in significantly less than one minute, while the old system took more than ten minutes to accomplish this, under identical circumstances. Furthermore, the system did not only detect known fraud attacks, but also discovered yet unknown signaling errors that were caused by other carriers. Future work will comprise an investigation of these signaling errors, since they appear to be potential predictors for telephony fraud. This especially concerns so-called inter-carrier fraud.

Still, the developed system needs more testing. It appears that the thresholds have to be specified more precisely. As these values rely on experiences, the software has to be run in a productive environment with near real-time data to exactly determine the thresholds, in order to increase the detection probability. The final decision, if the results detected by the system are fraud, still relies on a human operator judging each case. Much harm could be done by automatically blocking innocent customers due to false positive classification results. With the presented approach, our system is able to conduct most of the analysis necessary to detect fraud by itself. Therefore, the probability that the delivered results indicate real fraud cases is already high.

Given the modular implementation, the system can be easily extended. More rules, that is to say more filters, can be integrated with no effort. The more distinct the filters are that analyze the incoming data, the more likely it is to detect fraud before too much damage is done.

Granted that the presented system is tested more thoroughly, it will be capable to be used on a Next Generation Network for performant fraud detection. Its application will possibly improve the detection of telephony fraud, and it is worth considering for use by telecommunication service providers. From the collaborating service provider's perspective, the presented approach represents a major achievement concerning fraud detection in their practice, compared to the previously used solution.

ACKNOWLEDGMENT

This work has been performed for the “Fraud Detection” project of Hochschule Darmstadt - University of Applied Sciences. The project is partially funded by the “Bundesministerium für Bildung und Forschung” (BMBF) and supported by ”Center for Advanced Security Research Darmstadt” (CASED). The authors additionally would like to acknowledge the support of toplink GmbH, which made this work possible.

REFERENCES

[1] Zar, J. et al., "VOIPSA - VoIP security and privacy threat taxonomy, public release 1.0", http://www.voipsa.org/activities/taxonomy.php, October 2005.

[2] Communications Fraud Control Association, “2009 global fraud loss survey,” http://www.cfca.org/, 01. 09. 2011.

[3] S. Tindal, “VoIP hackers strike perth business,” ZDNet, Jan. 2009. http://www.zdnet.com.au/voip-hackers-strikeperth-business-339294515.htm, 05. 08. 2011.

[4] Bundesministerium der Justiz, „Bundesdatenschutzgesetz in der Fassung vom 14. Januar 2003, zuletzt geändert am 14. August 2009,“ Berlin, 2009.

[5] T. Padmaja, N. Dhulipalla, R. S. Bapi, and P. R. Krishna, “Unbalanced data classification using extreme outlier elimination and sampling techniques for fraud detection,” in: Proceedings of the 15th International Conference on Advanced Computing and Communications (ADCOM 2007). IEEE Computer Society, 2007; pp. 511–516.

[6] Y. Kou, C.-T. Lu, S. Sirwongwattana and Y.-P. Huang, “Survey of fraud detection techniques,” in: Proceedings of the 2004 IEEE International Conference on Networking, Sensing and Control (ICNSC 2004). IEEE, 2004; pp. 749–754.

[7] S. Rosset, U. Murad, E. Neumann, Y. Idan and G. Pinkas, “Discovery of fraud rules for telecommunications challenges and solutions,” in: Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD 1999). ACM, 1999; pp. 409–413.

[8] D. Olszewski, “Fraud detection in telecommunications using Kullback-Leibler divergence and latent Dirichlet allocation,” in: Proceedings of the 10th International Conference on Adaptive and Natural Computing Algorithms (ICANNGA 2011). Springer, 2011; pp. 71–80.

[9] I. Ruiz-Agundez, Y. Penya and P. Garcia Bringas, “Fraud detection for voice over ip services on next-generation networks,” in: Proceedings of the 4th Workshop in Information Security Theory and Practice (WISTP 2010). Springer, 2010; pp. 199–212.

[10] M. Taniguchi, M. Haft, J. Hollmén and V. Tresp, “Fraud detection in communication networks using neural and probabilistic methods,” in: Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 1998). IEEE, 1998; pp. 1241–1244.

[11] S. Qayyum, S. Mansoor, A. Khalid, K. Khushbakht, Z. Halim and A. Baig, “Fraudulent call detection for mobile networks,” in: Proceedings of the 2010 International Conference on Information and Emerging Technologies (ICIET 2010). IEEE, 2010.

[12] K. C. Cox, S. G. Eick, G. J.Wills and R. J. Brachman, “Visual data mining: Recognizing telephone calling fraud,” in: Data Mining and Knowledge Discovery, vol. 1, no. 2, pp. 225–231, Jun. 1997.

[13] J. Hollmén and V. Tresp, “Call-based fraud detection in mobile communication networks using a hierarchical regime-switching model,” in: Proceedings of the 1998 Conference on Advances in Neural Information Processing Systems 11 (NIPS 1999). Morgan Kaufmann, 1999; pp. 889–895.

[14] P. S. Foundation, “Python programming language - official website,” http://www.python.org, 1990-2011.

[15] TELES, “Teles.icdr, S48-S2000 series,” Teles Communication Systems, 2006.