Toll Fraud Detection in Voice over IP Networks Using Communication Behavior Patterns on Unlabeled Data

Sandra Kübler, Michael Massoth, Anton Wiens and Torsten Wiens
Department of Computer Science
Hochschule Darmstadt – University of Applied Science
Darmstadt, Germany
e-mail: {sandra.kuebler | michael.massoth | anton.wiens | torsten.wiens}@h-da.de

***Abstract*—Widespread monetary losses are known to be caused worldwide by fraud attacks on Voice over IP systems. In 2014, several millions of FRITZ!Box routers have been compromised and used to conduct phone calls to international destinations. By using fraud detection systems, such attacks can be detected. By analyzing Call Detail Records (CDRs), various algorithms can be applied to detect fraud. Unfortunately, this data is mostly unlabeled, meaning no indications on which calls are fraudulent or non-fraudulent exist. In this work, a new method to detect fraud is presented, utilizing the concept of clustering algorithms leading to *behavior pattern recognition* using information retrieved from user profiles. The grouping aspect of clustering algorithms regarding the similarity of objects leads to data depicting the behavior of a user to be matched against behavior patterns. If a deviation from the assigned behavior patterns occurs, the call is considered fraudulent. A prototype has been implemented with two behavior patterns defined, making it possible to detect fraud. It can further be refined by adjusting multiple thresholds, as well as defining more behavior patterns. The prototype is to be integrated in an existing fraud detection system of Hochschule Darmstadt, being developed in cooperation with a small and medium-sized enterprise (SME) telecommunication provider, improving the quality of its VoIP services.**

Keywords-Fraud detection; Voice over IP networks; behavior pattern recognition; unlabeled data; FRITZ!Box.

I. INTRODUCTION

Voice over IP (VoIP) has been well-established as one of the possibilities to perform voice communication. As it uses the internet as a means of data transportation, it also inherits its drawbacks, also concerning its security flaws. These security flaws can be exploited by criminals by, for instance, taking over a private branch exchange (PBX) and performing fraudulent phone calls using a specific user's account. Telecommunication providers, especially small and medium-sized enterprises (SME), suffer from those attacks as they lead to financial losses and a decrease of trust on part of their customers.

Every two years, the Communications Fraud Control Association (CFCA) conducts a survey on global fraud loss. The 2013 survey shows that approximately 46.3 billion USD have been lost due to fraud attacks, denoting an increase of 15% in comparison to 2011 [1].

The actuality of fraud attacks in VoIP is further emphasized by the "FRITZ!Box incident". *AVM FRITZ!Boxes* are multifunctional routing devices, which are very popular in Germany. In February 2014, several million units have been compromised by hackers exploiting security vulnerabilities [2]. For instance, this caused a regional German telecommunication provider financial losses of more than 200,000 € during one month [3].

Meanwhile, the security vulnerabilities have been patched by the manufacturer, but users still can be affected, as it is very likely that sensitive data (e.g., login data) has been stolen as well. If the password has not been changed, the system may still be vulnerable. Furthermore, the update requires manual patching. This is further accentuated in [4], where it is shown that users who did not patch their units are still suffering from attacks.

Fraudulent activities in the telecommunication sector can be countered using various mechanisms. Possibilities range from techniques based on user profiling where deviations from a user's normal behavior are considered fraudulent, using machine learning algorithms or even combining techniques from various fields and developing frameworks with additional features as a means to prevent fraud in the first place [5]-[9].

The *University of Applied Sciences Darmstadt* aims to detect and therefore minimize financial loss with its research project "Trusted Telephony". Furthermore, it intends to provide enhanced security in VoIP telecommunication, leading to a versatile *fraud detection system*, which is currently in development. It utilizes various techniques gained from ongoing research on fraud detection, e.g., using rule-based and user profiling techniques. The work at hand is part of the research project "Trusted Telephony" and is preceded by the works [6][10][11]. The German telecommunication service provider *toplink GmbH* cooperates with the *University of Applied Sciences Darmstadt*, especially providing the necessary data for analysis.

In this paper, a new method to detect fraud in VoIP communication is presented. This new method is intended to be a new component for the fraud detection system. It is based on the findings on fraud detection obtained from preceding work [6], which dealt with the issues of the FRITZ!Box incident as well. A summary of the most important findings concerning an analysis on data obtained during the FRITZ!Box incident is given in Section V.

The idea of the new approach is to adapt the idea of the concept of *clustering* ("grouping" of data based on the

 ISBN: 978-1-61208-398-8

similarity of an object) from machine learning and combine it with *user profiles*, leading to an approach based on *behavior pattern recognition* using pieces of information retrieved from user profiles. The thought of potentially using clustering algorithms in the first place arose because no labeled data was available. Therefore, techniques not solely relying on the existence of labeled data became more interesting to the project.

A. Call detail records

In this work, the data provided by *toplink GmbH* is in the form of Call Detail Records (CDRs). These text files contain call parameters, e.g., caller- and callee-party parameters, starting time and call duration.

B. Structure of the paper

The introduction is followed by an overview of related work in Section II. Section III gives a brief overview of unsupervised learning, as it is relevant for the concept to detect fraud cases. The basic idea of user profiling is described in Section IV. Section V describes the data collected during the FRITZ!Box incident, followed by a use case of the presented method in Section VI. The concept of *communication behavior patterns* using data from user profiles is described in detail in Section VII. The prototypical implementation is described in Section VIII, including information about the utilized data set, the experimental setup and its results. A conclusion to this paper is presented in Section IX, being followed by possible future work in Section X.

II. Related Work

As a means to visualize user accounts, self-organizing maps (SOM) are used in [5]. This visualization is used to differentiate between normal and fraudulent ones. Three features are extracted from the CDR data and used for analysis: Call destination, call start time and call duration. According to the authors, the method has a true positive rate (TPR) of 90% and a false positive rate (FPR) of 10%.

In order to cluster probabilistic models, a framework for self-organizing maps has been developed by Hollmén, Tresp and Simula [12]. User profiles using data of mobile communication networks have been used for test runs of the system. The output is presented visually, so that the fraudulent calls can be distinguished from normal ones.

The authors of [7] focus on the detection of superimposed fraud using two signature methods, each summarizing a user's behavior. The first presented approach is based on a deviation of the user's current behavior and his signature, while the second is based on a dynamic clustering analysis. In the second approach, a sudden change or "shift" of a user's signature from one cluster to another is the criterion for a classification as fraud. The similarity between a signature and a cluster centroid, which in itself is defined as a signature, is crucial for such a shift. The detection rates of both methods have been estimated: The first one promises a TPR of 75% and the second one a TPR of 91%. Also, a combination of both approaches is examined.

The framework *SUNsHINE*, which is able to detect and prevent VoIP fraud by combining real-time capable components with an offline statistical analysis, is presented in [9]. Multiple data sources, network traffic data and CDRs, can be used. Different algorithms and techniques are used, e.g., rule sets, profiling, neural networks and clustering. No estimations concerning the detection rate are given.

As some of the related work is using neural networks or variations of these, it should be further pointed out that one of the major drawbacks of using neural networks lies in the necessity of having labeled data for training. While it is possible to use SOMs in the sense of clustering, these still require some kind of "training" or evaluation.

The preceding works [11] and [6] as part of the research project had to deal with this problem as well. In [11], a detailed list regarding related work based on user profiling is provided and a method based on statistical user profiling is presented. Two user profiles containing statistical features are generated, representing the past (Past Behavior Profile, PBP) and the present (Current Behavior Profile, CBP), using a significant deviation of a user's behavior in contrast to his past behavior as an indication for possible fraud. The idea of using two user profiles is based on [8] and [13], which both use a user profile history and a current user profile. In [11], a TPR of 90% and a FPR of 1.22% is estimated.

The successor of the approach described above is using an enhanced approach in order to deal with the fraud cases acquired during the FRITZ!Box incident [6]. Distributed fraud attacks, as described therein, can be detected by profiling the destination numbers instead of a user as it is normally done when using the principles of user profiling. The approach described in [6] differs in the *point of view* of the data in contrast to this work. The work at hand has been inspired by the concept of clustering algorithms, as the aspect of *finding similarities* has been adopted.

III. Unsupervised Learning

One conceptual requirement for the component being developed for this work is to be able to detect fraud without using labeled data. Hence, algorithms based on unsupervised learning immediately suggest themselves [14][15]. Clustering techniques, grouping similar objects, are most commonly used. The similarity function used depends on the type of clustering algorithm, e.g., hierarchical or centroid based methods. Further information on clustering algorithms can be found in [15].

In this work, as a means to perform unsupervised learning, user profiling is being applied (see Section IV) for fraud detection. Applying user profiles proved successful in previous work on the fraud detection system [6][11], as the data is put into a user context which is missing otherwise. This context is important as not every user behaves the same.

The new component should be integrated into an existing framework, which should function in nearly real-time. The authors decided to use clustering algorithms as a "preprocessing step" during the data analysis, as opposed to related work, e.g., [5]. This is due to the fact that a lot of data has to be processed and the clustering algorithms have to be evaluated. Additionally, clustering algorithms can also be

 ISBN: 978-1-61208-398-8

time-consuming. The pieces of information obtained through clustering are used to obtain indications of the definition of behavior patterns and thresholds. The definition of behavior patterns is a key part in the work at hand, as each pattern describes a distinct behavior of a user and as the matching to a behavior pattern and its growth are used for the actual fraud detection. For the preprocessing step, clustering algorithms (k-means, unsupervised SOM) as they are implemented in the tool WEKA, which provides machine learning algorithms for data mining tasks [16], are applied. Furthermore, ideas derived from clustering techniques in general influenced the actual concept of *communication behavior patterns* using data from user profiles as described in Section V.

IV. USER PROFILING

Two types of analysis exist: absolute and differential [17]. While an absolute analysis is retrieving pieces of information directly from CDRs and therefore is in need of having a firm understanding of fraud patterns, a differential analysis summarizes the retrieved information into statistical features over a distinct period of time. The latter is also called *behavior-* or *user profiling*. Utilizing this profile, it is possible to identify a change in a user's behavior over a given period of time. The utilization of user profiling, varying in its concept and features used, is addressed in related work [6][8][11][18][19], which partially use the common features *duration per call*, *number of calls per customer* and *costs per call*.

V. FRITZ!BOX INCIDENT DATA

Fraud cases originating from the FRITZ!Box incident share some common characteristics. These characteristics have been described in detail in [6] and will be briefly summarized, as well as complemented in the following. A description of how these units could have been taken over is given in [6]. Occurring attack patterns are as follows:

- Different and numerous international numbers have been dialed in rapid succession which were either not connected (call attempts) or having a short duration (call connects).
- From the user's perspective, only one international number has been dialed either resulting in a call attempt or a call connect. From the call destinations' perspective, up to eight different users dialed the number. The numbers have been dialed in rapid succession (at night-time in one-second intervals), having a mean duration of approximately 7-8 minutes.
- A user dials several, mostly international numbers. A destination number is being dialed by 3 users on average.
- While national numbers have been dialed, call attempts, as well as call connects to international numbers were made nearly simultaneously.
- Most fraudulent calls were made between afternoon and early morning, showing a peak in the night-time.

Especially countries from zones 2 (mostly Africa) and 3 (mostly Europe) have been called numerously. The listed criteria can occur combined. The amount of call attempts outweighs the amount of call connects. The duration of the phone calls ranges from approximately 30 ms up to 11 minutes.

VI. USE CASE – COUNTRY PROFILING

In the following, a use case for the concept of *communication behavior patterns* using information from user profiles is depicted (see Fig. 1).

A customer of a telecommunication provider – in most cases in the given data set, a customer equals a company – conducts business calls to various foreign countries. These international calls are further described as matches to behavior patterns of the customer, each being a differentiation of a behavior pattern describing international calls in general. In Fig. 1, the size of each ellipse surrounding a country A to E indicates how many calls are usually – i.e., as it had been profiled during the initialization phase – conducted to the destination. Now, a new behavior pattern reflecting the behavior to conduct calls to country E emerges. During a short time span, e.g., of one hour, the number of matches to this new behavior pattern grows, indicating that distinctly more calls have been conducted to country E. Furthermore, this new behavior pattern and the growth of the match to it over a short period of time could indicate fraudulent calls, as typically, the customer does not conduct that many calls to country E so that a match to such a behavior pattern could be justified.

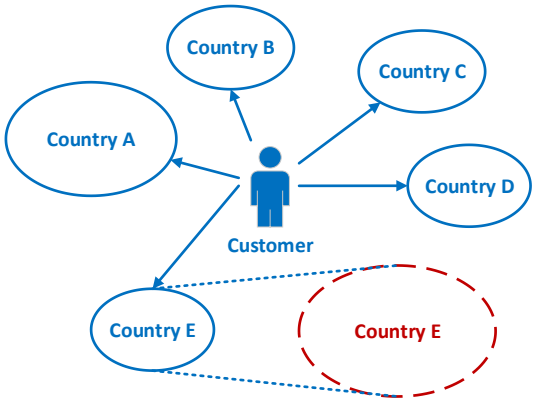

Figure 1. Depiction of the use case with a customer having his international groups and a new one growing over a short time interval, indicating fraud.

This use case illustrates the *potential* of the concept of *communication behavior pattern recognition* with information from user profiling, as it is described in detail in the following section, and how it can be used for fraud detection. Instead of profiling by country, it would also be possible to profile by telecommunication providers, as our data suggest.

VII. CONCEPT OF COMMUNICATION BEHAVIOR PATTERNS

The idea behind the concept of using *behavior patterns* with information from user profiles is to adapt the principle

 ISBN: 978-1-61208-398-8

of *clustering* algorithms, combined with the usage of *user profiles* (differential analysis). Thus, the requirement of the concept to function with unlabeled data can be met. The concept itself can therefore be categorized as an unsupervised classification method.

Similar objects following similar patterns are to be assigned into the same behavior pattern. To associate with a behavior pattern, each shall have its own criteria, where similar groups possess similar criteria. In this work, user profiles, using the information retrieved from the CDRs as a base for their features, are used as objects. In order to describe the behavior concerning a distinct aspect of a user or a group of users, the calls of a user profile are matched against predefined behavior patterns. A user is able to have matches to several behavior patterns.

To obtain an indication for the thresholds and to search for behavior patterns, clustering algorithms from WEKA were used.

A. Data preparation

Only a fraction of the information contained in the CDRs is used as input for a user profile, as not all information concerning a VoIP connection is necessary for analysis, as shown in [11]. The important pieces of information extracted from a CDR are the following attributes A_1 to A_4:

A_1 User ID
A_2 Timestamp of the call
A_3 Duration of the call
A_4 Destination number

The session ID is not used for the construction of a user profile, but as a unique identifier of the corresponding CDR. The information obtained from A_4 is further categorized into its call region *national*, *mobile* and *international*. The information whether the call had been connected or was merely a call attempt is being retrieved from A_3.

A_2 is further processed and divided into more fine-grained pieces of information, namely whether or not the call occurred on a weekend and if the call has been made during work hours (7:00 am to 18:59 pm) or after hours (19:00 pm to 6:59 am) with a time span of 12 hours each. This segmentation is done because of findings from the analysis described in Section V, as a considerable amount of fraudulent calls, especially call attempts, has been conducted at night. Furthermore, this allows for a more versatile definition and use of behavior patterns without being too complex.

B. User profiles

A user profile contains data extracted from CDRs (see above) related to a user over a certain period of time *t*.

After being filled with data accumulated during *t*, a *user profile* is considered ready to test for fraud. For *t*, at least one week is considered appropriate [6][7][8][9][11], as substantial data about the normal behavior of a user has to be gathered, resulting in a "training phase" of a user profile.

CDRs outdating *t* are removed from a profile. Based on the data contained in a profile, features can be extracted.

C. Behavior patterns

As mentioned before, a *behavior pattern* reflects a distinct behavior or rather a behavior in a specific context of a user. For instance, if a user is calling international destinations often, this user matches the behavior pattern "International Calls". Another specific context is that calls have been made on weekend or during work hours. It is possible for a user to *match* one or more behavior patterns.

1) Features

A behavior pattern has its own defining set of features *F* called *feature vector*, with comparable behavior patterns having similar defining features. As these features are highly dependable on the context or rather the criteria of a behavior pattern, an overall definition for a feature vector cannot be given. The features are derived from the data contained in a user profile. Essentially, there are two types of features: numeric and Boolean (true/false).

Examples for two behavior patterns, their criteria and therefore feature vectors:

- *"International Calls After Hours"*: The criteria for this pattern are: The call has to be connected, the call region is *international* and the call is made *after hours*.
- *"Weekend Calls"*: The only criterion is for the calls to be made on a weekend.

For both behavior patterns applies that the single numerical value in the feature vector is the accumulation of the respective calls during a time span t_{BP}. For t_{BP}, a value of one hour has been chosen, as this time span is neither too short nor too long.

2) Criteria for a behavior pattern match

In order for a *user* to *match* a behavior pattern, every feature of a feature vector, depending on its type, has to meet its criteria:

- Numeric: A statistical or numeric feature has to pass a *threshold*.
- Boolean: A Boolean feature has to have the value *true*.

For every defined behavior pattern, the criteria are tested. This way, it is possible for a CDR of a user to lead to a match to more than one behavior patterns.

3) Metric for a match

All calls matching a distinct behavior pattern are stored in respective lists. Over time, the length of such a list - and, therefore, the *grade* of a match - can diminish or grow. This is further denoted as a *growth* of a match to a behavior pattern.

The *growth G* of a match to a behavior pattern over a timespan is measured as:

$$G = \frac{C_L}{\bar{x}\,(C_P)} \quad (1)$$

C_L denotes a list of all connected calls during the current (latest) hour and C_P a list of all connected calls in the past.

 ISBN: 978-1-61208-398-8

For both C_L and C_P, calls from the list of matches are used. $\bar{x}$ denotes the arithmetic mean over the respective list.

4) Change of a match

The *growth G* of a match to a behavior pattern described above is further used as a criterion to mark a current call as *fraudulent*, as it is defined in the following case differentiation:

$$Fraud = \begin{cases} true, G > T_{BP} \\ false, otherwise \end{cases} \quad (2)$$

T_{BP} denotes a threshold for the growth of a match to a behavior pattern. If T_{BP} is passed, the current call, which had been causal for *passing* the threshold, is the first call to be considered fraudulent. All subsequent calls which are still triggering *true* are considered fraudulent as well. Additionally, a *weight* can be assigned to every behavior pattern, indicating how much a growth of a match influences the assignment of a call as fraudulent. This leads to an enhancement of the case differentiation (2):

$$Fraud = \begin{cases} true, G \cdot w > T_{BP} \\ false, otherwise \end{cases} \quad (3)$$

VIII. PROTOTYPE

The concept described in Section VII has been implemented as a prototype. The description of the prototype consists of the used data set (Subsection A), the experimental setup (Subsection B) and the results (Subsection C).

A. Used data

Real life traffic data over a time span of seven weeks provided by *toplink GmbH* has been used to test the prototypical implementation. For the initialization of the user profiles, as well as behavior patterns of a user, the data of the first week has been used, as they contained no known fraudulent activity. Out of the seven weeks, there is at least one week included with definite fraud attacks having the pattern described in Section V. The rest of the data shows partial signs of the FRITZ!Box fraud attack pattern as well.

The data set comprises 10,401,547 CDRs. As only outgoing calls, as well as successfully connected calls (call connects) are of importance, 2,749,860 CDRs were left.

B. Experimental setup

For the prototypical implementation, two simple behavior patterns have been defined:

- *IntCallsPattern*: All connected calls having an international destination match the behavior pattern.
- *IntCallsAfterHoursPattern*: All connected calls having an international destination and having been conducted in the after hours match this behavior pattern.

The thresholds for the statistical features for both behavior patterns, as well as indications about the thresholds concerning the change of a match to a behavior pattern have been derived using clustering algorithms from WEKA. The applied clustering algorithms were k-means, EM and an implementation of a SOM as a clustering algorithm.

C. Results

Determining a True and False Positive Rate (TPR and FPR) poses a difficult task if only unlabeled data is available. Due to the analysis performed on the data retrieved during the FRITZ!Box incident, an approximation concerning the TPR was possible. Nevertheless, not all fraudulent data has been known during the evaluation of the prototype. The data set described in Section VIII.A has been used. The following steps have been applied:

1. Apply the thresholds and weight values retrieved from clustering algorithms and given from experience, respectively.
2. Run the prototype with the defined two behavior patterns.
3. Analyze the results utilizing the knowledge derived from the analysis of the data, as well as from *toplink*.

In total, 17,110 fraud cases were reported and analyzed. During the analysis, one customer was noticeable in his behavior to conduct calls to foreign destinations very often, even not during the timeframe of the FRITZ!Box incident. Therefore and because of other aspects found in our analysis, this customer can be considered being a call center. Such a call center is a likely candidate to be added to a whitelist and thus can be ignored, leading to a total of 13,503 reported fraud cases if subtracted. The TPR measured is *98.4%*. The TPR would vary if this specific customer would be taken into account, but this type of customer could easily be excluded in preprocessing via whitelisting. The measured FPR is below 0.01 %.

Surely not all fraud instances of the FRITZ!Box incident could be found. This can be said even though not enough labeled data existed, as valuable time – and therefore, CDRs - passes in order for a user to match a behavior pattern and be associated with the described behavior. Afterwards, a threshold concerning the growth of a match has to be passed, resulting in an equivalent to a "settling-in phase". Thus, it is possible that not all fraudulent instances were detected.

TABLE I. FPR AND TPR COMPARISON WITH RELATED WORK

	TPR	**FPR**
This work	98.4%	< 0.01%
Previous work [6]	95% (100%)	0.7%
Previous work [11]	90%	1.22%
Related work [5]	90%	10%

Table I. shows a comparison of the TPR and FPR with related work. Concerning the results in [6], the TPR had been reduced from 100% to 95% by the authors, based on a qualified estimation, as it is possible that not all fraudulent calls in the dataset are known. Concerning the work at hand and the dataset used, this could be very likely, too.

 ISBN: 978-1-61208-398-8

IX. CONCLUSION

It is possible to detect fraud attacks using the presented approach. Regarding the FRITZ!Box data, it is comparable in quality to the approach presented in [6]. With the possibility to define behavior patterns, it has the additional potential to be more versatile. Currently, there are only two behavior patterns defined, but with the addition of more behavior patterns and better regulated thresholds, the results can be improved as more fraud patterns could be detected. Also, more heterogeneous patterns could be found.

X. FUTURE WORK

One possibility to improve the detection rate is to increase the time span for the initialization phase. Behavior patterns relating to weekends or workdays are only meaningful for a stable analysis if there are at least three weeks of data given.

The importance of whitelisting is shortly mentioned in Section VIII.C, as a customer being most likely a call center causes the TPR to differ significantly.

Furthermore, the idea of including a "global trend" arose, similar to the one presented in [11] where a global profile possessing the CDRs of all users has been included in order to balance fluctuations in the data. In the work at hand, the growth of lists of calls matching distinct behavior patterns can be monitored globally. Concerning the users, two possibilities have to be considered:

- The user only just did not meet the requirements of having enough matches to a behavior pattern to be associated with a pattern and
- The user has enough matches to a behavior pattern to be associated with it, but only just did not pass the threshold concerning the growth and therefore the call is not considered fraudulent.

If such a distinct behavior pattern shows fraudulent activity originating from several users, this "global trend" can influence the result concerning the aforementioned users.

Including information given by call attempts and call termination cause codes can further improve the detection result. They can provide insight whether a fraudulent attack is currently prepared or conducted. Additionally, "normal" behavior patterns - e.g., "National Calls" - have to be considered as well. Their sole existence can be used as a further criterion for other behavior patterns.

Furthermore, the possibility of conflicting behavior patterns can be considered as well. For instance, a user usually calls on weekends and this behavior had been learned during the initialization phase. Suddenly – e.g., during one hour – a new matching of a behavior pattern reflecting workday calls emerges. In this case, the existence of the workday behavior pattern matching conflicts with the weekend pattern matching and can be considered suspicious behavior.

Regarding the machine learning part of this concept, further clustering algorithms are currently being evaluated to improve the process of retrieving the thresholds, as well as the values themselves. Furthermore, techniques like *Principal Component Analysis* (PCA) ought to be used for first-step data analysis, as preliminary tests on raw CDR data suggest.

ACKNOWLEDGMENT

We want to express our gratitude to the State of Hesse, Germany and its research program LOEWE for providing funding. Additionally, we want to thank *toplink GmbH* (Darmstadt, Germany) for their cooperation and for providing the data for our research project.

REFERENCES

[1] Communications Fraud Control Association, "Global Fraud Loss Survey," October 2013. [Online]. Available from: http://www.cfca.org/pdf/survey/CFCA2013GlobalFraudLossSurvey-pressrelease.pdf 2014.11.17.

[2] R. Eikenberg, "Hack on AVM routers: Fritzbox breach disclosed, millions of routers at risk," 07 03 2014. [Online]. Available from: http://www.heise.de/security/meldung/Hack-gegen-AVM-Router-Fritzbox-Luecke-offengelegt-Millionen-Router-in-Gefahr-2136784.html 2014.11.19.

[3] R. Eikenberg, "Change VoIP password now: criminals exploit captured Fritzbox data," 26 03 2014. [Online]. Available from: http://www.heise.de/security/meldung/Jetzt-VoIP-Passwort-aendern-Kriminelle-nutzen-erbeutete-Fritzbox-Daten-aus-2155168.html 2014.12.08.

[4] WAZ (DerWesten), "AVM warns against attacks on its Fritzbox routers," 29 09 2014. [Online] Available from: http://www.derwesten.de/ratgeber/avm-warnt-vor-angriffen-auf-seine-fritzbox-router-id9881008.html 2014.11.26.

[5] D. Olszewski, J. Kacprzyk, and S. Zadrożny, "Employing Self-Organizing Map for fraud detection" The 12th International Conference on Artificial Intelligence and Soft Computing (ICAISC 2013), June 2013, pp. 150-161, ISBN: 978-3-642-38657-2.

[6] A. Wiens, T. Wiens, and M. Massoth, "Approach on fraud detection in Voice over IP networks using call destination profiling based on an analysis of recent Attacks on Fritz!Box units" The Sixth International Conference on Emerging Network Intelligence (EMERGING 2014) IARIA, Aug. 2014, pp. 29-34, ISSN: 2326-9383, ISBN: 978-1-61208-357-5.

[7] R. Alves et al., "Discovering telecom fraud situations through mining anomalous behavior patterns". Proceedings of the DMBA Workshop on the 12th ACM SIGKDD, 2006.

[8] C. S. Hilas and P. A. Mastorocostas, "An application of supervised and unsupervised learning approaches to telecommunications fraud detection," Knowledge-Based Systems, vol. 21, issue 7 , pp. 721-726, Oct. 2008, doi:10.1016/j.knosys.2008.03.026.

[9] D. Hoffstadt et al., "A comprehensive framework for detecting and preventing VoIP fraud and misuse," 2014 International Conference on Computing, Networking and Communications (ICNC), Feb. 2014, pp. 807-813, doi:10.1109/ICCNC.2014.6785441.

[10] S. Augustin et al., „Telephony fraud detection in Next Generation Networks" The Eighth Advanced International Conference on Telecommunications (AICT 2012) IARIA, May 2012, pp. 203-207, ISSN: 2308-4030, ISBN: 978-1-61208-199-1.

[11] A. Wiens, T. Wiens, and M. Massoth, "A new unsupervised user profiling approach for detecting toll fraud in VoIP networks" The Tenth Advanced International Conference on Telecommunications (AICT 2014) IARIA, July 2014, pp. 63-69, ISSN: 2308-4030, ISBN: 978-1-61208-360-5.

[12] J. Hollmén, V. Tresp, and O. Simula, "A Self-Organizing Map for clustering probabilistic models" Ninth International Conference on Artificial Neural Networks (ICANN) vol. 2,

1999, pp. 946-951, ISSN: 0537-9989, ISBN: 0-85296-721-7, doi:10.1049/cp:19991234.

[13] P. Burge and J. Shawe-Taylor, "An unsupervised neural network approach to profiling the behavior of mobile phone users for use in fraud detection" Journal of Parallel and Distributed Computing 61, 2001, pp. 915-925, doi:10.1006/jpdc.2000.1720.

[14] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: a survey" ACM Computing Surveys (CSUR), vol. 41, issue 3, pp. 15:1-15:58, Jul. 2009, doi:10.1145/1541880.1541882.

[15] N. Grira, M. Crucianu, and N. Boujemaa, "Unsupervised and semi-supervised clustering: a brief survey" A Review of Machine Learning Techniques for Processing Multimedia Content, Report of the MUSCLE European Network of Excellence (6th Framework Programm), 2005.

[16] WEKA, Machine Learning Group at the University of Waikato, official homepage. [Online] Available from: http://www.cs.waikato.ac.nz/ml/weka/ 2014.12.15.

[17] P. Burge et al., "Fraud detection and management in mobile telecommunications networks" European Conference on Security and Detection (ECOS97) Incorporating the One Day Symposium on Technology Used for Combatting Fraud, 1997, pp. 91-96, doi:10.1049/cp:19970429.

[18] Y. Moreau, H. Verrelst, and J. Vandewalle, "Detection of mobile phone fraud using supervised neural networks: a first prototype" 7th International Conference on Artificial Neural Networks (ICANN), 1997, pp. 1065-1070, ISSN: 0302-9743, ISBN: 978-3-540-63631-1, doi:10.1007/BFb0020294.

[19] M. Taniguchi, M. Haft, J. Hollmén, and V. Tresp, "Fraud detection in communication networks using neural and probabilistic methods" Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing, 1998, vol. 2, pp. 1241-1244, ISSN: 1520-6149, ISBN: 0-7803-4428-6, doi:10.1109/ICASSP.1998.675496.

 ISBN: 978-1-61208-398-8