İSTANBUL UNIVERSITY CERRAHPAŞA

**RESEARCH ARTICLE**

Electrica 2021; 21(1): 74-84

# A Case Study on Fraudulent User Behaviors in the Telecommunication Network

**H. Hakan Kilinc**

Department of Research and Development, NetRD Information Technologies and Telecommunications, Istanbul, Turkey

**Cite this article as:** Kilinc HH. A Case Study on Fraudulent User Behaviors in the Telecommunication Network. *Electrica,* 2021; 21(1): 74-84

**ABSTRACT**

In the telecommunications industry, fraud is quite common and fraud detection is similar to looking for a needle in the haystack. In this article, the behavior types of the fraudsters are revealed through a case study and ten types of fraudulent user behaviors are identified by using examples and figures.
**Keywords:** Telecommunication, fraud, security, detection methods, communication service providers

**Corresponding Author:**
H. Hakan Kilinc

**E-mail:**
hakank@netrd.com.tr

**Received:** 12.05.2020

**Accepted:** 30.11.2020

**DOI:** 10.5152/electrica.2021.20050



## Introduction

Telecommunication frauds can be defined as the unauthorized and illegal use of telecommunication services such as cellular network security and infrastructure for an intention of misuse or for earning illegal revenue or for not paying the particular service. Fraud is a serious risk to communication service providers' revenue, and it is difficult to detect especially when, how, or where new fraud methods will emerge. According to the 2019 Global Fraud Loss Survey of the Communications Fraud Control Association (CFCA), it is estimated that the industry is losing $28.3 billion per year from fraud [1].

In this literature, there are proposed studies on behavior analysis for fraud detection in telecommunication networks. Wu et al. [2] proposed the design of an intrusion detection system for Voice over IP (VoIP) systems. The proposed rule-based detection system is effective against Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP)- based attacks such as SIP BYE attack, fake instant messaging, call hijacking, and RTP attack. Olszewski [3] proposed a method that distinguishes normal and fraudulent behavior based on user profiles to detect subscription fraud. Cahill et al. [4] used signature-based, event-driven, and self-initializing methods to prevent subscription fraud.

Hoffstadt et al. [5] analyzed different VoIP attack stages from scanning to toll fraud using a VoIP Honeynet System that recorded over 47.5 million SIP messages in total. In another study after 2 years, Hoffstadt et al. [6] proposed a multilayered solution to detect and prevent fraud and misuse in VoIP networks. They used rule-based user and call profiling, neural network, and velocity trap check methods in their solution.

Guo et al. [7] proposed a model based on Long Short-Term Memory (LSTM) considering the characteristics of behavioral sequence. They also used real telecommunications data sets under both supervised and unsupervised scenarios. Lin et al. [8] modeled user interaction and consecutive behaviors to identify abnormal behavioral patterns.They tested their proposed model with both synthetic and real telecom data.

Estévez et al. [9] proposed a system using fuzzy rules as a classification module and a multilayer perceptron neural network as a detection module to detect subscription fraud. Hilas and Mastorocostas [10] used the multilayer perceptron technique, a class of feed-forward artificial

neural networks as supervised learning, and the hierarchical agglomerative clustering technique as unsupervised learning, to detect superimposed fraud.

In this article, a customer case study is presented to demonstrate fraudulent user behaviors in telecommunication networks. We used the real-world telecommunication data sets that are obtained from one of the Communication Service Providers (CSP) in Turkey.

Using this data analysis study, we aim to detect anomaly on CDR (Call Detail Report) data, perform behavior-based user analysis, detect new fraud behaviors, and offer intrusion detection and prevention rule suggestions for detected fraud behaviors.

In the literature and industry, there are studies on fraud types such as international revenue share fraud, interconnect bypass, and premium rate service as well as fraud methods such as subscription fraud, IP PBX hacking, and phishing [11]. One of the unique aspects of our study is to conduct a statistical analysis on the behavior of fraudulent users, using these fraud types and methods. Successful fraudsters use environments with huge call traffic and target large companies and CSPs. They fail to notice the costs associated with the fraud. It is easy to notice fraudulent behavior that tries to make profiteering in one go and does not achieve its purpose. Fraudsters try different kinds of techniques to hack and manipulate the system. We tried to reveal fraudulent behavior in an environment with high call traffic.

This article is organized as follows. Section II gives background information about telecommunication fraud. Section III discusses the behavior analysis of telecommunication frauds by using a customer case study. Section IV concludes the article.

**Telecommunication Fraud**

It is well-known that there is a variety of telecommunication fraud occuring in the current scenario. Domestic/international revenue share fraud, premium rate service fraud, interconnect bypass fraud and roaming fraud are the main types of fraud that fraudsters mostly prefer [1,11]. For most of the fraud types, while fraudulent users are reducing their cost of getting services or products, service providers are facing the problem of revenue loss owing to these kinds of frauds.

Nowadays, more frauds are occuring since many new technologies are appearing in the market, which are easy to be hacked owing to the lack of robust security systems. New voice technologies are becoming more attractive, and fraudsters can easily infiltrate systems that are not correctly installed. Thus, fraudsters use several fraud combinations that are difficult to be detected by traditional methods, trying to discover previous forms of fraud. Fraud is noticed usually when the phone bill is significantly increased, or when a service provider bypasses international calls or pays significant interconnection charges. In multinational corporations, it is difficult to detect fraudulent calls when international call volumes and charges are high.

In communication networks, VoIP (Voice over Internet Protocol) communication is the root cause of being vulnerable to attacks, especially telecommunication frauds. Difficulties in securing the VoIP network and its services built into a shared IP network are much more complex and difficult than securing the traditional circuit-switched PSTN (Public Switched Telephone Network) voice network. The expected service quality and system reliability cannot be maintained if the VoIP network is not secure enough.

VoIP services are typically provided through Internet Protocol Private Branch Exchanges (IP PBXs) that operate in nonsecure operating systems and unsecured support systems (e.g., databases and web servers). These operating systems and services are affected by attacks that regularly target other types of servers that make IP PBXs more vulnerable than traditional PBX [12].

The VoIP network includes more components and software such as IP PBX, VoIP Servers, Media Gateways, and IP Phones/Soft Phones. More components mean more vulnerabilities. Endpoints, such as IP Phones/Soft Phones, whose security settings are not sufficiently configured, can be captured internally or externally. This will result in exposure to attacks such as traffic fraud, toll fraud, and eavesdropping.

There are various features and real-time requirements specific to VoIP that make security even more difficult. There is no tolerance assured for any delay. There are many application layer firewalls to protect IP PBXs and IP phones against external attacks such as Denial of Service (DoS) and toll fraud, and also to determine whether packages are legitimate [13].

VoIP services are less secure than other traditional IP services, because VoIP includes a large number of standards that are implemented both dynamically and often poorly. There are many VoIP protocols, including SIP, H.323, H.248, and vendor-specific protocols. SIP is the most common protocol used for VoIP. However, it is challenging to secure a SIP system with the current state of SIP implementations. Security requirements in SIP are not fully defined, and therefore vendors themselves define their product security. Most SIP development is focused on feature sets and interoperability, and there is no emphasis on security. Even if a provider's components support security, it is also safe to use all the other elements involved.

**A Case Study**

For our case study, we used the Nova V-GATE product, a system for the detection and prevention of traffic and toll fraud [14]. Figure 1 shows the network topology of CSP and the position of Nova V-GATE. With Nova V-GATE, it is aimed to monitor international call traffic and to detect and prevent toll fraud attacks, which is capable of detecting and preventing online frauds that occurred within a maximum of 3 hours. Data analysis is required for fraud in the longer period and the rules proposed as a result of the analysis can be applied. In the CSP, approximately 420,000 calls, of which 300,000 are international, were collected for 4 months. It is possible to determine fraud and

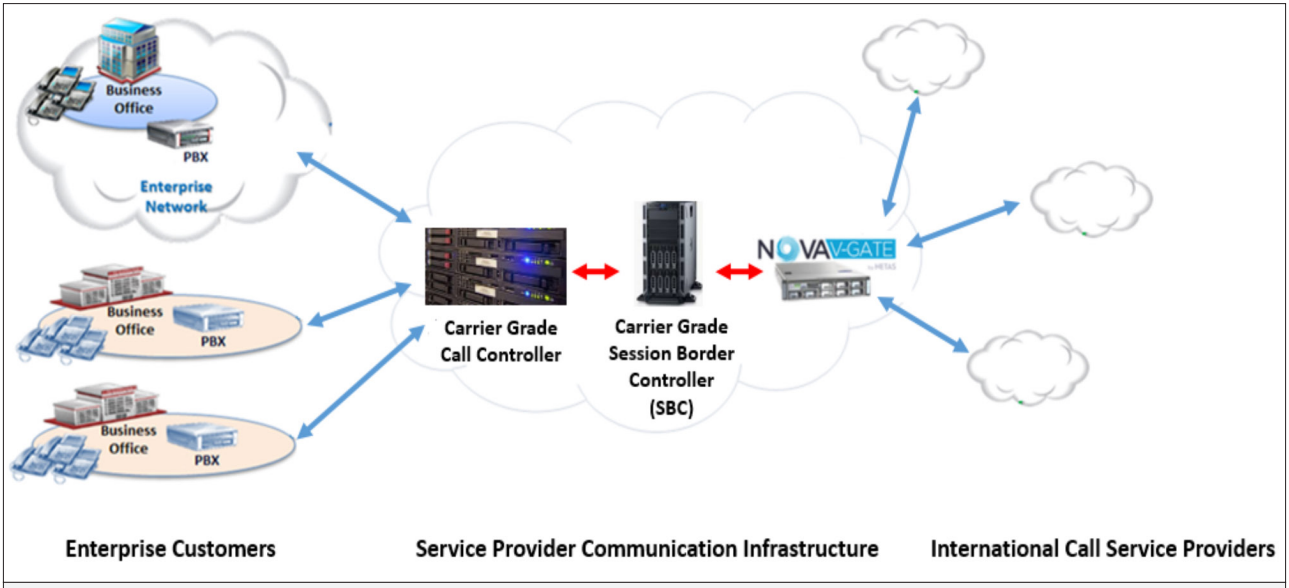


**Figure 1.** Network Topology and Nova V-GATE Position

**Table 1.** Fraudulent User Behaviors

| Fraud Behavior | Fraudulent User Behaviors |
|---|---|
| F1 | A few calls with long duration call |
| F2 | Too many calls with short duration call |
| F3 | Long duration calls in a specific time window |
| F4 | Too many calls in a specific time window to a specific charge rate destination |
| F5 | Long duration calls in a specific time window to a specific charge rate destination |
| F6 | Long duration calls from one user to the same destination in the same time period |
| F7 | Too many calls with short duration from one user to the same destination in the same time period |
| F8 | Too many calls with long duration from one user to the same destination in the same time period |
| F9 | Sparse and short calls to same destination in a wide range time period |
| F10 | Sparse and short calls to different destinations in a wide range time period |

attacks such as fraudulent calls, caller id spoofing, service interruption, making the unauthorized call, dropping the authorized call, unbilled calls, and policy violations by analyzing the collected data in the VoIP infrastructure.

We analyzed the enriched CDR data generated by the NOVA V-GATE to detect the fraudulent calls in the VoIP network of the CSP. Statistical analysis methods were performed in the data to recognize call patterns that act abnormal behavior regarding some call-specific attributes. The attributes used to define user behavior are call type (national, international, mobile, etc.), call date, call duration, call count, and call destination. The source of the call is IP phones and IP PBXs compromised within Turkey. They were seized owing to insufficient security measures and hence the call source was ignored.

First, we only focused on international calls since the majority of the toll frauds were targeting international calls. Secondly, we determined each destination country and destination region by performing the longest match algorithm among destination numbers. We then processed data with statistical analysis methods based on the above call attributes to discover the users' normal and suspected behavior. We also investigated the behavior of some fraud calls reported by the CSP.

As indicated in Table 1, we discovered ten behaviors of fraudulent user behaviors as a result of our investigation for determining user call behaviors. At the first stage, we cannot determine if these call scenarios were exactly fraud, but we can accept them as suspicious calls. Fraudulent user behaviors are characterized by the unexpectedly high values of call counts or/and call duration within a period.

The CSPs categorize each international numbers based on the billing price. While Category K5 is assumed as the most expensive international region, Category K1 is the least. The "GSM" suffix in categories means the Global System for Mobile Communications (GSM). Fraudsters naturally prefer the most expensive and poorly regulated international call region to maximize their profits.

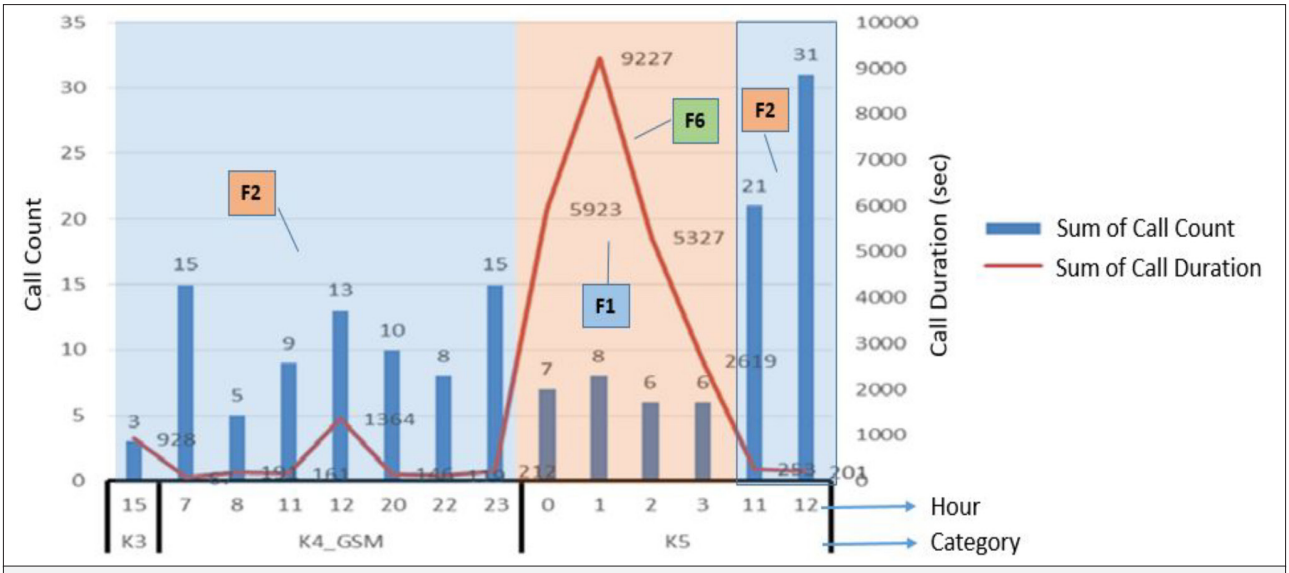


**Figure 2.** The number and duration of suspicious calls by category and hour

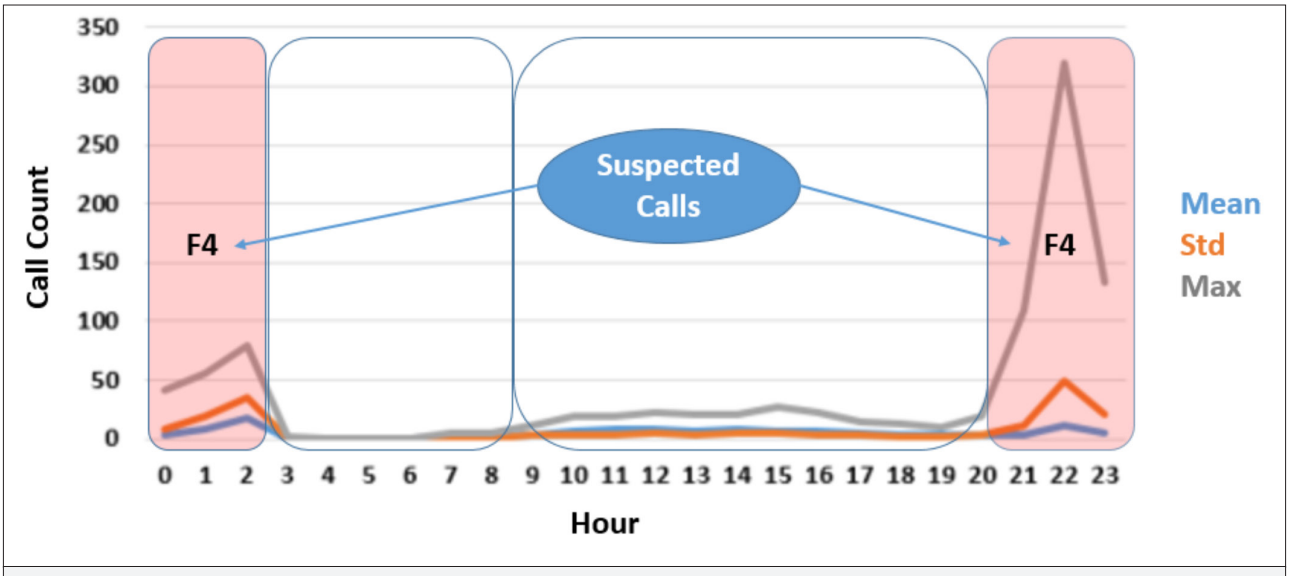


**Figure 3.** The number and duration of suspicious calls by category and hour

With examples and figures, we need to clarify the concepts such as short, long, a few, too many, sparse in the table and explain how we detect fraud behavior. The specific values of these concepts vary depending on the use case.

Figure 2 shows the number and duration of suspicious calls by category and hour. Calls that are made between different hours in the K4 category, calls between 11.00 and 13.00 hours in the K5 category, and calls between 15.00 and 16.00 in the K3 category consist of too many calls (5 calls and more) with short duration (about 1000 seconds or less) like F2 fraud behavior. Also, calls that are made between 00.00 am and 04.00 am in the K5 category includes a few calls (10 calls and less) with long duration call (2000 seconds and more) like F1 fraud behavior.

Another feature of calls that are made between 00.00 am and 04.00 am in the K5 category is multiple calls with long duration from the same user toward the same destination at the same time as F6 fraud behavior. It can be ascertained that there is an intersection of F1 and F6 fraud behaviors occuring between 00.00 am and 04.00 am.

Figure 3 shows a large number of calls (50 calls and more) toward a specific category (K5) within a specific slice of time (between 21.00 and 03.00 am) like F4 fraud behavior.

Figure 4 shows long duration calls toward a specific category (K5) within a specific slice of time (between 22.00 and 00.00 am) such as F5 fraud behavior. We will discuss Figure 3 and

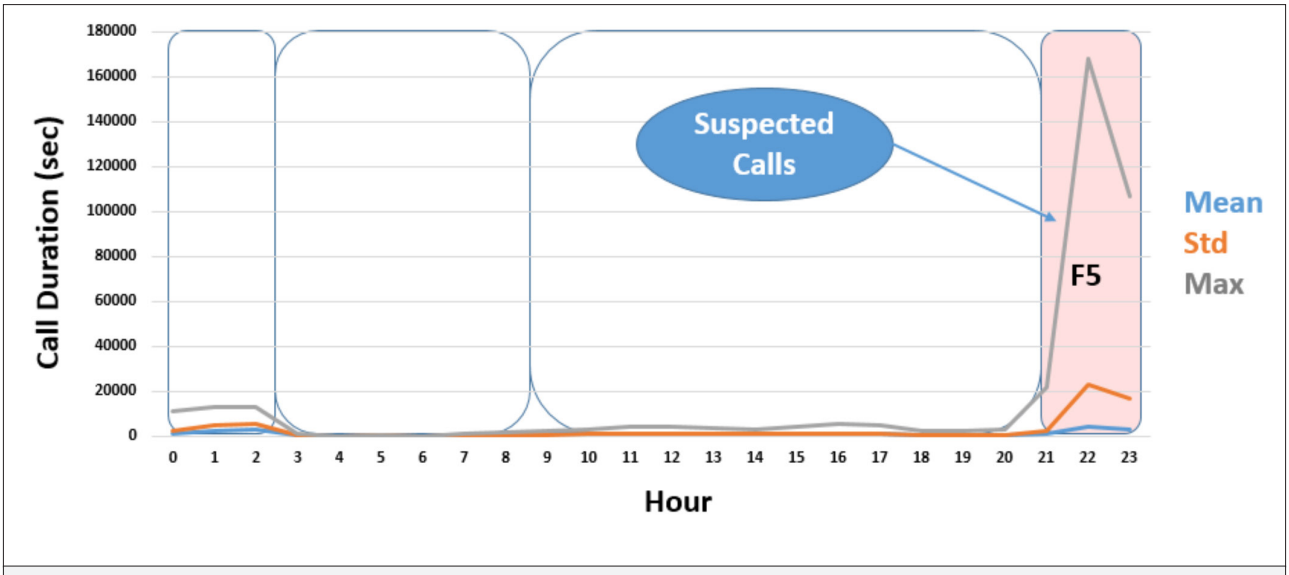


**Figure 4.** The duration of suspicious calls in a specific time window towards a specific category

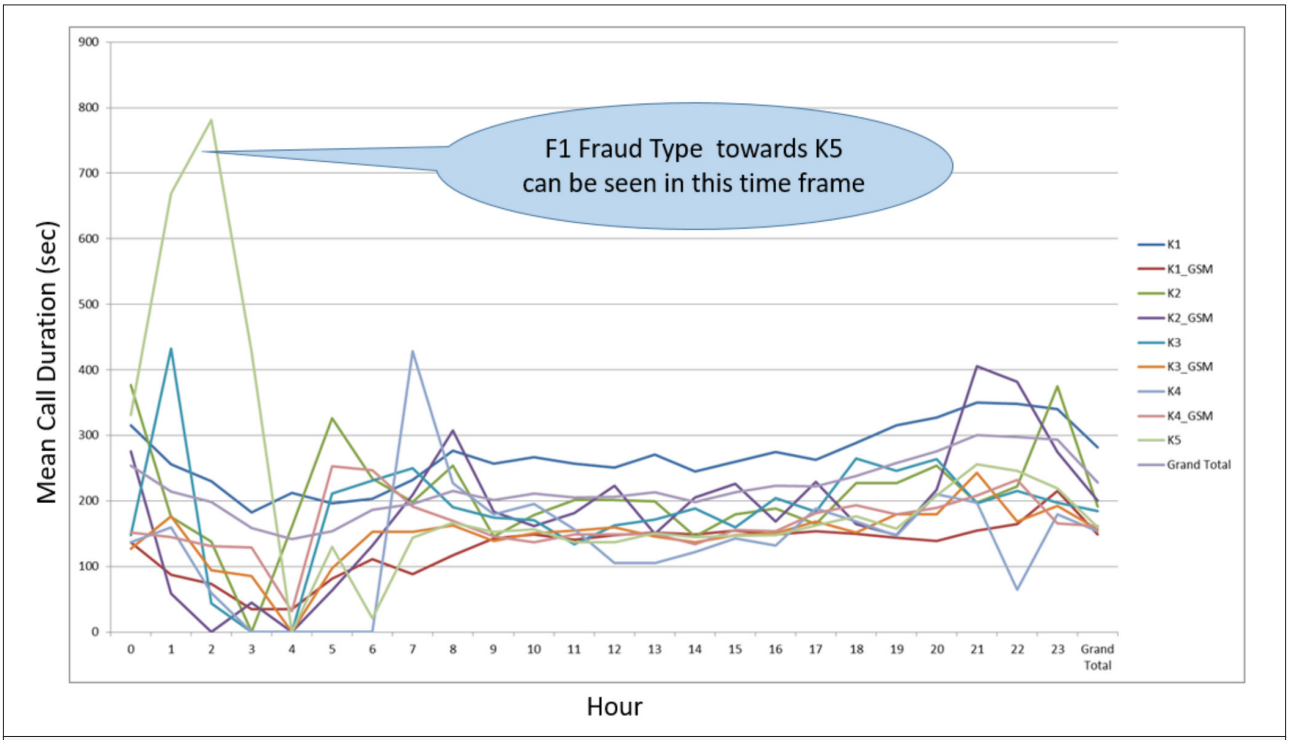


**Figure 5.** Hourly average call duration based on call destination category

Figure 4 in more detail in the Solution Approaches section later.

Figure 5 gives the average call duration for international calls made toward each call destination category. It is shown that a peak in call duration of calls occurs toward K5 between 00.00 am and 04.00 am. This situation is a typical F1 fraud behavior that points out the small number of long duration calls. Fraudsters prefer out-of-business hours to make long-duration calls toward the high-cost destination numbers.

Figure 6 indicates the most observed fraud behaviors and rates. It seems that fraudulent users tend to make small numbers of long duration calls like F1 fraud behavior, and long duration calls within a specific period like F3 fraud behavior. Also, they tend to make a large number of calls with a short duration like

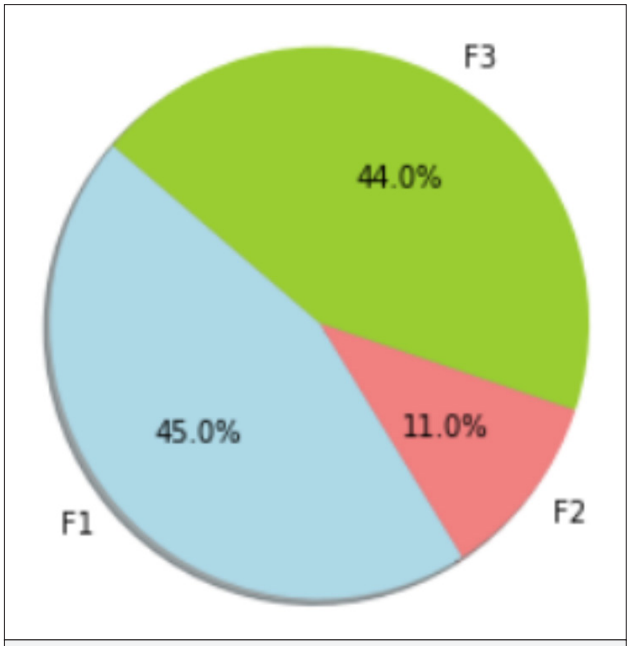


**Figure 6.** Fraud calls percentage based on fraud behaviors

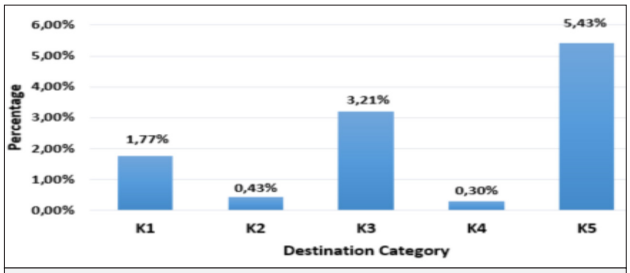


**Figure 7.** Percentage of fraud calls based on category

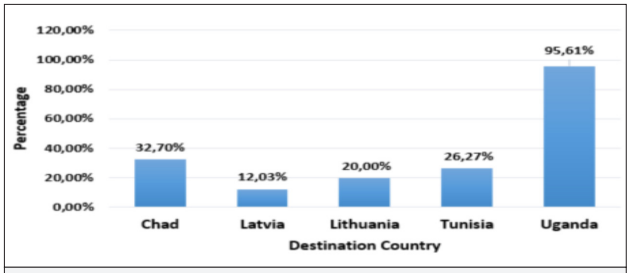


**Figure 8.** Percentage of fraud calls based on destination country

F2 fraud behavior. The fraudulent user behaviors that were detected between F4 and F10 were not approved by CSP, therefore they were not added to this figure. The approximate percentages of these behaviors are too small.

As shown in Figure 7 and Figure 8, prevented fraudulent calls are mostly made toward highly charged regions. It is inferred from both the figures that K5 as a destination category and Uganda as a destination country is the most targeted destination points by the fraudulent users.

F7 and F8 types are fraud behaviors that have note been observed in this data set, but we think that they are observable. For F9 and F10 fraud behaviors, we need to use the data set with a wider time interval. In the data set we selected, we observed short calls in the same or different directions, but are there similar patterns in previous periods? For this, studies based on event-based multiple change-point models should be conducted in a data set with wider time intervals. We plan to work on this topic in the future.

The customer recorded most fraudulent calls that surpassed the length or amount of calls within one or two hours. As the core outcomes of our data analysis, one of the typical fraudulent behaviors is that fraudsters prefer making a significant amount of multiple simultaneous calls within 1 hour. However, even if all the fraud attacks happened within an hour, the total call duration of multiple calls is much more than 2 hours. Fraudsters prefer off hours to make long duration calls to high-cost areas. They also tend to make the small number of long duration calls, long duration calls in specific period of time, and large numbers of short duration calls. In the next subsection, details of the Intrusion Detection and Prevention System (IDPS) rules that can be created based on the analysis results will be discussed.

**Solution Approaches**

Solution approaches to detect these fraud scenarios are suggested as follows.

- F1, F2, and F3 fraud behaviors can be detected by the rule-based systems and prevented with VoIP IDPS tools. Since these behaviors occurred within a maximum of 3 hours, it was possible to apply the IDPS rules for online detection and prevention.
- After the fraud behaviors between F4 and F8 were detected by data analysis, it was possible to establish IDPS rules. It is possible to inference from the sample in a specific time window, because the relationships between the variables can be detected in this time window.
- We think that F9 and F10 fraud behaviors can be found by machine learning approaches, but it is difficult to estimate that sparse and short calls over a wide period of time are normal calls. It is necessary to make the most accurate estimate possible.

Regarding the data analysis process and the rules that can be proposed, we present the following examples. Figure 9 shows the hourly distribution of calls made toward the K5 category in the 4-month dataset. There are four different behavioral time intervals toward the K5 category. Time intervals and maximum call numbers are as Table 2 in below.

According to these values, rules can be established for international calls to determine whether the number of calls in the last [1–3] hours has exceeded the maximum number of calls in the relevant time range.

**Table 2.** Time Intervals and Max Call Numbers toward the K5 Category in the 4-month Dataset

| Time Interval | Maximum Call Number |
|---|---|
| [0-2,8] | 120 |
| [3-7] | 29 |
| [9,17,18,19,20,21,23] | 448 |
| [10-16,22] | 780 |

**Table 3.** Time Intervals and Max Call Number in the 1 Hour toward the K5 Category

| Time Interval | Maximum Call Number |
|---|---|
| [0-2] | 80 |
| [3-8] | 5 |
| [9-20] | 27 |
| [21-23] | 319 |

**Table 4.** Time Intervals and Max Call Duration toward the K5 Category in the 4-month Data set

| Time Interval | Maximum Call Duration |
|---|---|
| [0-2,8] | 352 minutes |
| [3-7] | 65 minutes |
| [9, 17-21] | 1198 minutes |
| [10-16, 23] | 1951 minutes |
| [22] | 3913 minutes |

**Table 5.** Time Intervals and Max Call Duration in the 1 Hour toward the K5 Category

| Time Interval | Maximum Call Duration |
|---|---|
| [0-2,21] | 21405 seconds (356 minutes) |
| [3-8] | 1830 seconds (30 minutes) |
| [9-20] | 5335 seconds (89 minutes) |
| [10-16, 23] | 168239 seconds (2804 minutes) |

It is clearly mentioned that Figure 3 shows the mean, standard deviation and maximum number of calls on an hourly basis toward the K5 category. Based on this figure, four different behavioral time intervals vary according to the total number of calls. These time intervals and the maximum number of calls in the last 1 hour in these time intervals are as Table 3 in below.

According to these values, rules can be created for international calls in the last 1 hour based on the maximum number of calls in the appropriate time intervals.

Figure 10 indicates the hourly distribution of the duration of calls made to the K5 category in the 4-month data set. Five different behavioral time intervals were observed toward K5 category. These time intervals and max call durations in these time intervals are presented in Table 4 below.

As stated in these values, rules can be created for international calls in cases where the maximum call duration is exceeded in the relevant time interval (T1–T5).

In Figure 4, the average, standard deviation and maximum values of call duration are shown according to the hours toward the K5 category. According to this figure, four different behavior time intervals toward K5 direction change according to the total value. These time intervals and the maximum call duration in the last 1 hour in these intervals are provided in Table 5 below.

According to this, the rules that can be written for international calls in the last 1 hour may be based on exceeding the maximum call duration in each time interval.

Evaluating Figure 3 and Figure 9 together can help create more accurate IDPS rules. Likewise, evaluating Figure 4 and Figure 10 together can allow creating more accurate IDPS rules. Time intervals with high standard deviation are intervals indicating suspicious calls. Figure 9 and Figure 10 show a normal distribution during business hours and their standard deviations at these hours are very low. In non-business hours, however the parts with high standard deviation are remarkable.The standard deviations in the time intervals [0–2] and [21–23] in Figure 3 are high. In Figure 4, the standard deviations in the time intervals [0–3] and [21–23] are high. In these time intervals, it is understood that expensive international calls to the K5 category should be restricted by both the number of calls and the call duration.

In summary, rules can be written according to many parameters on VoIP IDPS. In the above examples, rules that can be created by subtracting the characteristics of the calls according to call duration and number of calls on a category basis are proposed.

**Detecting Suspicious Calls with Machine Learning Models**

In this section, we will detect suspicious calls by applying machine learning models to our data set and compare them with the results we obtained with statistical methods.

Since we do not have labeled data, we labeled calls that show abnormal behavior with the Local Outlier Factor model, an unsupervised outlier detection method that calculates the local density deviation of a given data point relative to its neighbors [15]. After running this model, 6,698% of the calls are labeled

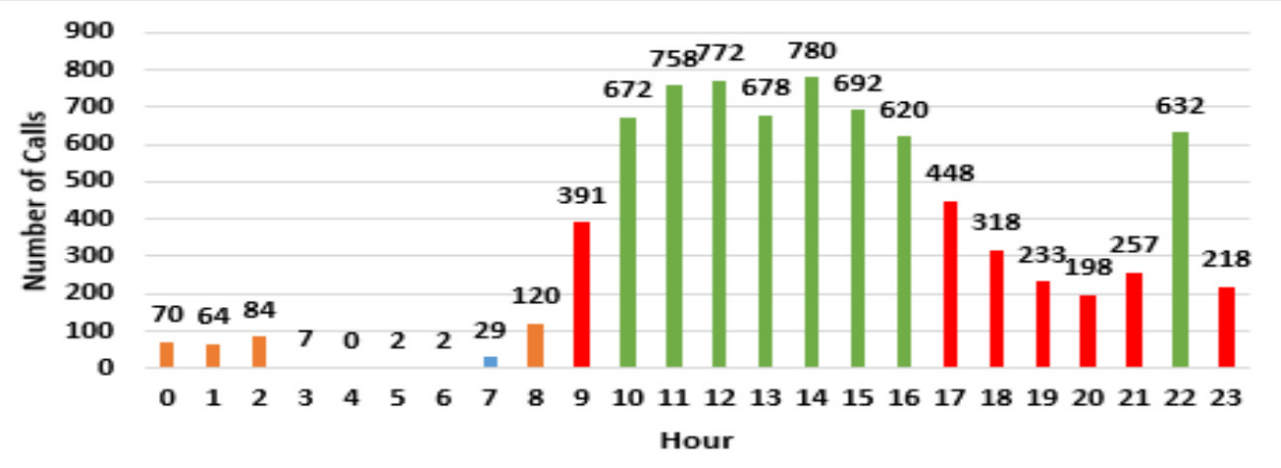


**Figure 9.** Hourly calls toward K5 category

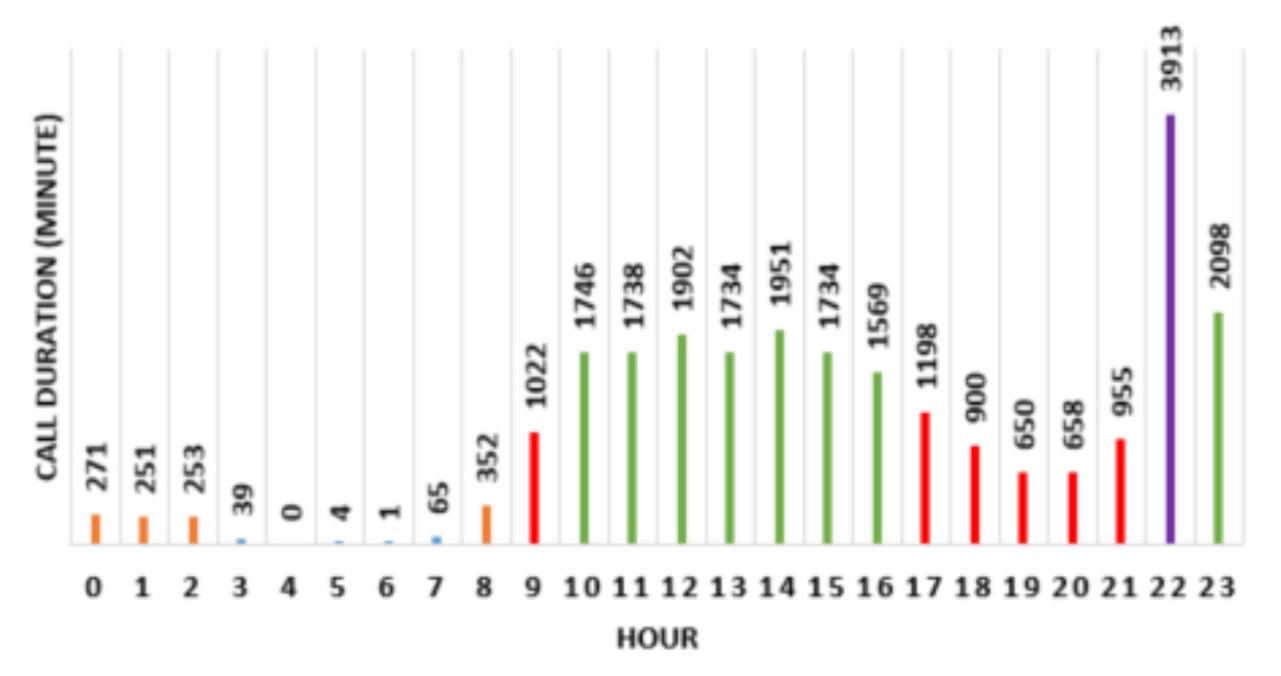


**Figure 10.** Hourly call duration toward K5 category

as suspicious. The data labeled as suspicious were used to train the supervised learning classifiers that were chosen. The selected supervised algorithms are as follows.

- Decision Tree classifier [16].
- Gaussian Naive Bayes classifier [17].
- Ada Boost classifier [18].

In addition to these, a mixture model was created by taking the averages of three supervised models. We separated the data set, 30% as test and 70% as training. In Fraud detection systems, both false positive and false negative values are significant. For this reason, besides the accuracy of the model, recall and precision values are also essential. Although the Decision Tree classifier has a high accuracy (93%), the recall value (4%) is quite low, as shown in Table 6. It is also noted that the precision value is 69%. In this case, false negative is expected to be higher than false positive. In other classifier, it is observed that the models approached the targeted accuracy, but their precision and recall values were far below the desired aspect.

According to the majority of the 5 models we have used, the rate of the number of calls found to be suspicious by getting 3 points out of 5 is 0.68% and 280 suspicious calls were detected. The percentage of suspicious calls based on destination country is as Figure 11.

**Table 6.** Classification report for supervised classifiers

| Classifier | Accuracy | Precision | Recall |
|---|---|---|---|
| Decision Tree | 0,93 | 0,69 | 0,04 |
| Naïve Bayes | 0,88 | 0,15 | 0,19 |
| Ada Boost | 0,93 | 0,46 | 0,02 |
| Mixture Model | 0,89 | 0,15 | 0,13 |

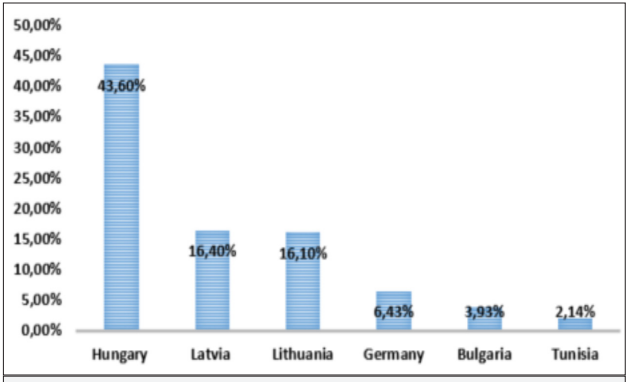


**Figure 11.** Percentage of suspicious calls based on destination country

When the results obtained by machine learning models were compared with the results determined by statistical approaches, it was observed that the suspicious call rates of Latvia, Lithuania, and Tunisia were high in both approaches.

## Conclusions

In fraud detection, first of all, it is necessary to identify fraud scenarios and reveal the behavior patterns of fraudsters, which have been identified using real telecommunication data, and solution approaches have been proposed to detect these patterns. It is not possible to detect and prevent identified fraud scenarios and behavior patterns only with basic rule-based methods. Some patterns of behavior can be detected by statistical data analysis in detail, but it is important to detect this before the event or at the beginning of the event.

More advanced and sophisticated detection systems and approaches are needed to prevent more complex attacks. Machine learning is one of the intelligent approaches that can be very fruitful for the detection of fraudulent users in real time.

Our future work will be on big data security analytics studies using machine learning techniques specific to the telecom/unified communication domain. In our future work, we will focus on the following topics.

- Automated suspected call detection and IDPS rule detection with the user behavior model.
- Automated real-time detection and prevention of the suspected calls with the user behavior model.
- Machine learning study integration with fraud detection and prevention system.

**Peer-review:** Externally peer-reviewed.

**Conflict of Interest:** The author has no conflicts of interest to declare.

**Financial Disclosure:** The author declared that the study has received no financial support.

## References

1. Communications Fraud Control Association, (2020), Global Fraud Loss Survey 2019, Available from: https://www.cfca.org/
2. Y. Wu, S. Bagchi, S. Garg, N. Singh, "SCIDIVE: A stateful and cross protocol intrusion detection architecture for Voice-over-IP environments", International Conference on Dependable Systems and Networks, Florence, Italy, 2004, pp. 433-442.
3. D. Olszewski,"A probabilistic approach to fraud detection in telecommunications", Knowledge-Based Systems, vol. 26, pp. 246-258, February 2012. [Crossref]
4. M. H. Cahill, D. Lambert, J. C. Pinheiro, D.X. Sun, "Detecting fraud in the real world", Handbook of Massive Data Sets, Springer, Boston, USA, vol 4, pp. 911-929, 2002. [Crossref]
5. D. Hoffstadt, S. Monhof, E. Rathgeb, "SIP trace recorder: monitor and analysis tool for threats in SIP-based networks", 8th International Wireless Communications and Mobile Computing Conference (IWCMC), Limassol, Cyprus, pp. 631-635, 2012. [Crossref]
6. D. Hoffstadt, E. Rathgeb, M. Liebig, R. Meister, Y. Rebahi, T.Q. Thanh, "A comprehensive framework for detecting and preventing VoIP fraud and misuse.", The IEEE International Conference on Computing, Networking and Communications (ICNC), Honolulu, USA, pp. 807-813, 2014. [Crossref]
7. J. Guo, G. Liu, Y. Zuo, J. Wu,"Learning sequential behavior representations for fraud detection", IEEE International Conference on Data Mining (ICDM), Singapore, pp. 127-136, 2018. [Crossref]
8. H. Lin, G. Liu, J. Wu, Y. Zuo, X. Wan, H. Li, "Fraud detection in dynamic interaction network", in IEEE Transactions on Knowledge and Data Engineering, vol. 32, no. 10, pp. 1936-1950, Oct. 2020. [Crossref]
9. P. A. Estévez, C. M. Held, C. A. Perez, "Subscription fraud prevention in telecommunications using fuzzy rules and neural networks", Expert Systems with Applications, vol.31, no. 2, pp. 337-344, Aug. 2006. [Crossref]
10. C. S. Hilas, P. A. Mastorocostas, "An application of supervised and unsupervised learning approaches to telecommunications fraud detection", Knowledge-Based Systems, vol. 21, no. 7, pp. 721-726, Oct. 2008. [Crossref]
11. M. Sahin, A. Francillon, P. Gupta, M. Ahamad, "SoK: Fraud in Telephony Networks", IEEE European Symposium on Security and Privacy (EuroS&P), Paris, 2017, pp. 235-250. [Crossref]
12. E. Herrell, "Resolving security risks for IP Telephony; what companies need to consider when deploying voice on data networks", Forrester Research Inc., Cambridge, MA, USA, 2004.
13. M. D. Collier, "Enterprise telecom security threats", SecureLogix, San Antonio, TX, USA, 2004.
14. NOVA Cyber Security Solutions, (2020), Nova V-Gate, Available from: http://novacybersecurity.com/en/products/nova_vgate
15. M. M. Breunig, H. P. Kriegel, R. T. Ng, J. Sander, "Lof: Identifying density-based local outliers", ACM SIGMOD Record, vol. 29, no. 2, pp. 93-104, June 2000. [Crossref]
16. L. Breiman, J. Friedman, R. Olshen, C. Stone, "Classification and Regression Trees", Taylor & Francis, Belmont, CA, 1984.

17. T. F. Chan, G. H. Golub, R. J. LeVeque, "Updating formulae and a pairwise algorithm for computing sample variances", Technical Report STANCS-79-773, Stanford University, Department of Computer Science, 1979.

18. Y. Freund, R. Schapire, "A decision-theoretic generalization of on-line learning and an application to boosting", Journal of Computer and System Sciences, vol.55, no.1, Aug. 1997. [Crossref]

H. Hakan Kılınç is working as R&D Strategies and Innovation Project Manager for NetRD since December 2019. He worked as cybersecurity product line manager for Netas between 2014 and 2019. He received his B.S. degree in Mathematics and Computer Science from Ege University, Izmir, Turkey, in 1997. He received his M.S. degree in 2001 in the Department of Computer Engineering at the Izmir Institute of Technology. He worked as a visiting scholar at the University of Texas at Dallas between 2009 and 2011. He holds Ph.D. about the security of SIP (Session Initiation Protocol) in the Department of Electronics Engineering at the Gebze Technical University in 2014. He worked as analyst, application developer, project manager, presales and product manager in a wide variety of business applications such as credit & credit card application and evaluation, value added services, alternative distribution channels, call centers, geographic information systems. His research interests are in the areas of big data security analytics, ID-based cryptography, reputation management, overlay and p2p networks and their securities with emphasis on mathematical modelling and performance analysis.