



HAL
open science

Bypass frauds in cellular networks: Understanding and Mitigation

Anne Josiane Kouam

► **To cite this version:**

Anne Josiane Kouam. Bypass frauds in cellular networks: Understanding and Mitigation. Networking and Internet Architecture [cs.NI]. Ecole Polytechnique (Palaiseau, France), 2023. English. NNT : 2023IPPAX035 . tel-04402681v1

HAL Id: tel-04402681

<https://hal.science/tel-04402681v1>

Submitted on 18 Jan 2024 (v1), last revised 24 Jan 2024 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



INSTITUT
POLYTECHNIQUE
DE PARIS

NNT : 2023IPPAX035

Thèse de doctorat



Bypass frauds in cellular networks: Understanding and Mitigation

Thèse de doctorat de l'Institut Polytechnique de Paris
préparée à l'École polytechnique

École doctorale n°626 École doctorale de l'Institut Polytechnique de Paris (EDIPP)
Spécialité de doctorat : Informatique

Thèse présentée et soutenue à Palaiseau, le 11 Mai 2023, par

ANNE JOSIANE KOUAM

Composition du Jury :

Aurelien Francillon Professeur, EURECOM	Président
Aurelien Francillon Professeur, EURECOM	Rapporteur
Walter Rudametkin Professeur, Université de Rennes 1 et IRISA (DiverSE)	Rapporteur
Konrad Rieck Professor, TU Berlin	Examineur
Oana Goga Chargée de recherche, CNRS - accueillie à INRIA (CEDAR) au LIX	Examineur
Aline Carneiro Viana Directrice de recherche, INRIA (TRiBE)	Directeur de thèse
Alain Tchana Professeur, Grenoble INP ENSIMAG	Co-directeur de thèse
Cedric Adjih Chargé de recherche, INRIA (TRiBE)	Invité
Philippe Martins Professeur, Telecom Paris (INFRES)	Invité

*To my beloved parents,
Jacques and Laure Brigitte Kouam,
who imparted me with love for science.*

Acknowledgements

It is with a heart full of emotions that I would like to thank the many people who have contributed to this thesis since its inception.

My profound gratitude goes to my supervisors, Aline Carneiro Viana and Alain Tchana, who allowed me to start this adventure and held my hand daily until the end. I sincerely believe that I had the best possible guidance and consider it a wink of God that their first names, Aline and Alain, match almost perfectly. I learned a lot from Aline, not only scientifically, and she has become a true role model for me. At the same time, Alain has always uplifted me with his spirit of excellence and unique benevolence. Thank you so much for such inspiration!

I want to thank my jury members: Aurelien Francillon, Cedric Adjih, Konrad Rieck, Oana Goga, Philippe Martins, and Walter Rudametkin. Your research work is a great inspiration for me, and it is an honor to be reviewed by such world-class experts. I will undoubtedly learn a lot from your thoughtful feedback.

Thank you to all my work collaborators, Luca Pappalardo and Leo Ferres, who allowed me to research in another context and continue supporting me. Thanks to Philippe Martins and Cedric Adjih for their advice and generous donations of time, infrastructure, and funding that go straight to my heart.

I would like to particularly thank the members of my follow-up committee Aurelien Francillon and David Bromberg, who took their role very seriously and assisted me during this thesis. Thanks infinitely to Aurelien for his support and recommendations in all my applications.

I thank all the members of the IPP doctoral school and INRIA Saclay, my host laboratory. In particular, the TRiBE team was an ideal framework thanks to Cedric Adjih, Laurence Fontana, Michael Barbosa, Nadjib Achir, and Philippe Jacquet. I cherish all my fellow students on this team for the good moments and the comfort: Abhishek Mishra, Clinton Nyobe, Fernando Ortiz, Iman Hmedoush, Licia Amichi, and Pengwenlong Gu. I also thank other Ph.D. mates and friends I met before and during this thesis and who participated in making it an exciting adventure: Djob Mvondo, Firmin Kateu, Hasnaa Ouadoudi, Kevin Jiokeng, Kevin Nguetchouang, Lionel Gako, Lucien Ndjie, Qiong Liu, Stella Bitchebe, Veronne Yepmo, Yibo Quan.

I cannot but express my deep gratitude to my parents, Jacques and Laure Brigitte Kouam, both university professors who have inspired me to follow this path since childhood. Thank you to my brothers and sisters (Euranie, Antoine, Cathy, and Pagnol), my nephews, the Tamo, and the Nzomigni families for their presence, encouragement, and love. Thank you to my large Christian family, who watched over me with multiple prayers throughout my work. I

especially thank Patrice Nyamy, Moclair and Mireille Kamgaing, Serges and Marie Kalla, Joseph and Larissa Marae, and the Cadres360 team.

I give special thanks to my dear husband, Arnaud Tamo, who has lived this adventure with me and always supported me.

Last but not least, I glorify my Lord Jesus Christ for this thesis. I thank him for both the highs and lows, as they taught me valuable lessons in patience and perseverance. Hence, Prof. Watchman Ndjiteh's quote, "*Learn to make the most you can with the less you have. And you'll forge a character that will never leave you,*" perfectly encapsulates the essence of this thesis.

Abstract

Cellular networks provide digital communications for more than five billion people around the globe. Besides, their openness to the general public, opaqueness, and complexity have exposed cellular networks to attacks that have tremendously grown over the previous decades. According to the Communication Fraud Control Association's 2021 report, worldwide mobile network operators are experiencing as much as \$39.89 billion annually due to illegal activities on their surfaces. Among such illegitimate activities, *SIMBox* international bypass fraud is one of the most prevalent, having a severe impact manifold.

SIMBox fraud involves diverting international cellular voice traffic from regulated routes and rerouting it as local calls in the destination country from a VoIP-GSM gateway (i.e., *SIM-Box*). Affecting countries worldwide, this problem impairs operators' revenues, network quality, networking research, and national security. Mainly in developing countries, up to 70% of incoming international call traffic is terminated fraudulently. Even worse, *SIMBox* fraud allows international terrorists to conduct covert activities, masquerading as national subscribers.

In this context, many challenges are added. First, while mobile network datasets (i.e., Charging Data Records or CDRs) are the primary data type leveraged for operators' fraud detection, they are intrinsically private. CDRs hold sensitive information about subscribers' habits, hardening their shareability to the research community and, at the same time, curbing fraud detection investigations. Second, fraudsters' behavior changes over time to adapt to the target solutions, making detection lag behind. In particular, *SIMBox* fraud increasingly mimics human communication behavior regarding traffic, mobility, and social habits perceptible in CDRs. Third, considering the low related investment, the fraud is quickly profitable. Therefore, the detection time is crucial for effective long-term mitigation.

This thesis tackles international bypass fraud understanding and mitigation while addressing the aforementioned challenges.

- It first deeply surveys both existing literature and the major *SIMBox* manufacturers to shed light on the *SIMBox* fraud ecosystem uncovering fraudulent techniques and their constant evolution through time.
- Second, it significantly contributes to unleashing the barrier of real-world CDRs exploitation for research on *SIMBox* fraud. This includes releasing a scalable simulation environment, i.e., *FraudZen*, that generates realistic CDRs, with fraudulent and legitimate users. To this end, *FraudZen* incorporates (i) *SIMBox* fraud modeling for fraudulent users and

(ii) generative modeling capturing real-world communication behaviors for legitimate users. Applying *FraudZen* capabilities to the in-depth evaluation of ML-based fraud detection literature reveals that the tackled fraud model variation causes a significant discrepancy in detection performance.

- Third, it investigates the use of cellular signaling data for the real-time detection of bypass fraud through experimental analyzes with real *SIMBox* appliances.

Through in-depth evaluations, we validate this thesis's contributions to accomplish a pipeline to handle the fraud: *from Fully understanding SIMBox frauds and detection limitations to Long-term fraud mitigation by anticipation and rapid retort.*

Keywords: Cellular networks, Human mobility and communication behaviors, Deep generative modeling of behaviors, Charging Data Records (CDRs), *SIMBox* fraud modeling and detection, Cellular signaling

Résumé

Les réseaux cellulaires fournissent des services de communication numérique à plus de cinq milliards de personnes dans le monde. En outre, leur ouverture au grand public et leur complexité ont exposé les réseaux cellulaires à des attaques qui se sont considérablement développées au cours des dernières décennies. D'après le rapport de 2021 de la Communication Fraud Control Association, les opérateurs de réseaux mobiles subissent chaque année des pertes s'élevant à 39,89 milliards de dollars en raison d'activités illégales sur leurs surfaces. Parmi ces activités illégitimes, la fraude de contournement internationale à la *SIMBox*, est l'une des plus répandues, ayant un impact sévère multiple.

La fraude à la *SIMBox* consiste à détourner le trafic vocal cellulaire international des routes réglementées et à le réacheminer sous forme d'appels locaux dans le pays de destination à partir d'une gateway VoIP-GSM (c'est-à-dire une *SIMBox*). Touchant des pays du monde entier, ce problème porte atteinte aux revenus des opérateurs, à la qualité des réseaux, à la recherche sur les réseaux et à la sécurité nationale. Principalement dans les pays émergents, jusqu'à 70% des appels internationaux entrants sont terminés frauduleusement. Pire encore, la fraude à la *SIMBox* permet aux terroristes internationaux de mener des activités cachées, en se faisant passer pour des abonnés nationaux.

Dans ce contexte, de nombreux défis s'ajoutent. Tout d'abord, tandis que les jeux de données des réseaux mobiles (Charging Data Records ou CDRs) sont le principal type de données exploité pour la détection de la fraude par les opérateurs, ils sont intrinsèquement privés. Les CDRs contiennent des informations sensibles sur les habitudes des abonnés, ce qui rend leur partage difficile à la communauté scientifique et, en même temps, limite la recherche sur la fraude. Deuxièmement, le comportement des fraudeurs évolue au fil du temps pour s'adapter aux solutions, maintenant la détection en arrière. En particulier, la fraude *SIMBox* imite le comportement de communication humain concernant les habitudes de trafic, mobilité et sociabilité perceptibles dans les CDRs. Enfin, dû au faible investissement correspondant, la fraude à la *SIMBox* est rapidement rentable. Ainsi, le temps de détection est crucial pour une mitigation efficace à long terme.

Cette thèse s'intéresse à la compréhension et à la mitigation de la fraude à la *SIMBox* tout en adressant les défis susmentionnés.

- Tout d'abord, elle étudie en profondeur la littérature existante et les principaux fabricants de *SIMBox* afin de mettre la lumière sur l'écosystème de la fraude en révélant les techniques frauduleuses et leur évolution constante dans le temps.

- Ensuite, elle contribue significativement à relâcher la barrière d'exploitation des CDRs réels pour la recherche sur la fraude à la *SIMBox*. Cela comprend la publication d'un environnement de simulation scalable, *FraudZen*, qui génère des CDR réalistes, avec des utilisateurs frauduleux et légitimes. A cette fin, *FraudZen* intègre (i) une modélisation de la fraude *SIMBox* pour les utilisateurs frauduleux et (ii) une modélisation générative capturant les comportements de communication réels pour les utilisateurs légitimes. L'application de *FraudZen* à l'évaluation approfondie de la littérature sur la détection de la fraude révèle que la variation du modèle de fraude abordé entraîne un écart important dans les performances de détection.
- Troisièmement, elle étudie l'utilisation des données de signalisation cellulaire pour la détection en temps réel de la fraude par contournement, par des analyses expérimentales avec de véritables appareils *SIMBox*.

Par des évaluations approfondies, nous validons les contributions de cette thèse pour accomplir un pipeline traitant la fraude : *de la compréhension complète des fraudes SIMBox et des limites de détection à l'atténuation de la fraude à long terme par l'anticipation et la riposte rapide.*

Mots-clés : Réseaux cellulaires, Comportements humain de mobilité et communication, modèles génératifs profonds de comportements, Charging Data Records (CDRs), Modélisation et détection de la fraude à la *SIMBox*, Signalisation cellulaire

Contents

Acronyms	xi
1 Introduction	1
1.1 Context	1
1.2 Challenges	3
1.3 Contributions	4
1.4 Thesis Outline	8
2 Background: Telephony Ecosystem	11
2.1 Mobile telephony networks	11
2.2 Call routing in cellular networks	13
2.3 Cellular network datasets	15
2.4 Summary	17
3 SIMBox Fraud	20
3.1 General description	21
3.2 The SIMBox architecture	22
3.3 SIMBox fraud detection in the literature	26
3.4 Fraud evolution	30
3.5 Summary	33
4 FraudZen: cellular networks dataset generation	34
4.1 Overview: usage and flexibility	36
4.2 FraudZen Design	36
4.3 Comparison with state-of-the-art simulators	40
4.4 Summary	41
5 Legitimate communication modeling	43
5.1 Zen Overview	44
5.2 Traffic module	47
5.3 Mobility module	51
5.4 Social ties module	53
5.5 CDRs generation inside <i>FraudZen</i>	54

5.6	Evaluations	55
5.7	Related works	61
5.8	Summary	62
6	Modeling <i>SIMBox</i> fraud for effective detection	64
6.1	Formalizing <i>SIMBox</i> fraud models	65
6.2	Defining <i>SIMBox</i> fraud models	67
6.3	<i>SIMBox</i> fraud model effectiveness	69
6.4	Building efficient <i>SIMBox</i> fraud detection	73
6.5	Related works	79
6.6	Summary	80
7	Cellular signaling-based detection	82
7.1	Cellular signaling-based detection	83
7.2	<i>SigN</i> prevention system	86
7.3	Discussion	91
7.4	Summary	92
8	Conclusion	94
8.1	Contributions summary	94
8.2	Limitations	96
8.3	Short-term perspectives	97
8.4	Long-term perspectives	97
	Bibliography	99
	Appendices	
A	<i>FraudZen</i> simulation parameters	115

Acronyms

AKA	Authentication and Key Agreement (<i>p. 89</i>)
ANN	Artificial Neural Network (<i>pp. 29, 75</i>)
AUTN	Authentication Token (<i>p. 89</i>)
CDMA	Code Division Multiple Access (<i>p. 32</i>)
CDR	Charging Data Records (<i>pp. 1, 3, 5, 6, 8</i>)
EMM	EPS Mobility Management (<i>p. 17</i>)
EPS	Evolved Packet System (<i>p. 17</i>)
GAN	Generative Adversarial Network (<i>p. 61</i>)
GBDT	Gradient Boosting Decision Tree (<i>pp. 74–76, 79</i>)
GSM	Global System for Mobile Communications (<i>pp. 1, 11, 12, 17</i>)
HBS	Human Behavior Simulation (<i>pp. 24, 25, 27, 29, 33</i>)
IMEI	International Mobile Equipment Identity (<i>pp. 83, 85</i>)
IMS	IP Multimedia Subsystem (<i>p. 88</i>)
IP-PBX	IP Private Branch Exchange (<i>p. 12</i>)
ITR	International Termination Rate (<i>p. 2</i>)
KASME	Key Agreement Key Stored in the Mobile Equipment (<i>p. 89</i>)
LSTM	Long Short-Term Memory (<i>pp. 48, 49, 55</i>)
LTR	Local Termination Rate (<i>p. 2</i>)
MAC	Media Access Control (<i>p. 17</i>)
MCC	Mobile Country Code (<i>p. 54</i>)
ME	Mobile Equipment (<i>pp. xi, 84, 85, 87</i>)
MME	Mobility Management Entity (<i>p. 88</i>)
MNC	Mobile Network Code (<i>p. 54</i>)

MSC	Mobile Switching Center (<i>pp. 13, 14</i>)
NAS	Non-Access Stratum (<i>p. 17</i>)
NLL	Negative Log Likelihood (<i>p. 56</i>)
PDCP	Packet Data Convergence Protocol (<i>p. 17</i>)
PLMN	Public Land Mobile Network (<i>p. 88</i>)
PSTN	Public Switched Telephone Network (<i>pp. 12, 17</i>)
RAN	Radio Access Network (<i>p. 39</i>)
RF	Random Forest (<i>pp. 29, 75–79</i>)
RLC	Radio Link Control (<i>p. 17</i>)
RRC	Radio Resource Control (<i>p. 17</i>)
SDR	Software-Defined Radio (<i>p. 84</i>)
SGW	Serving Gateway (<i>p. 88</i>)
SMS	Short Message Service (<i>pp. 39, 40</i>)
SVM	Support Vector Machine (<i>pp. 29, 75–79</i>)
TAC	Type Allocation Code (<i>p. 85</i>)
TCG	Test Call Generation (<i>p. 27</i>)
UE	User Equipment (<i>pp. 8, 85, 87–91</i>)
UML	Unified Modeling Language (<i>p. 36</i>)
USRP	Universal Software Radio Peripheral (<i>p. 88</i>)
WCDMA	Wideband Code Division Multiple Access (<i>p. 32</i>)
XRES	Expected Response (<i>p. 89</i>)

Introduction

1.1 Context

Since the first mobile phone was invented in 1973 [60], the past half-century has seen increasingly rapid advances in the innovation of mobile devices and mobile communication technologies. Nowadays, mobile devices are almost indispensable for business and personal lives. As illustration, mobile devices and connections have reached 14.9 billion in 2021; they will be 18.22 billion in 2025 [49].

The ever-higher penetration rate of mobile devices and their continuous interaction with the cellular network infrastructure give mobile network operators the possibility to easily record time-stamped and geo-referenced events of a vast population at a small cost for billing or network management purposes [115]. Human footprints in most operator-collected datasets come from CDRs – Charging Data Records [150], triggered by subscribers' generation of the so-called charging network events, i.e., voice calls, text messages, internet browsing, etc.

In this well-monitored communication environment, mobile network operators are still losing about USD 39.89 Billion annually [35] due to fraudulent and illegal activities. International voice bypass fraud, commonly known as Subscriber Identity Module (*SIMBox*) fraud, is by far one of the most prevalent frauds affecting the telecommunication market, being in the top four of phone system frauds that cause a significant loss to mobile network operators [35].

Fraudulent voice carriers divert the international voice traffic from the regulated routes, through VoIP established links. The diverted traffic is received at the level of a *SIMBox* (i.e., VoIP to GSM gateway equipped with a bundle of SIM cards) in the destination country and re-originated as a national mobile call to its recipient (see Fig. 3.1). Hence, the destination cellular operator does not receive international call termination charges but instead the much lower local termination charges. Beyond a growing revenue loss for operators estimated to \$2.7 Billion in 2019 [34] and \$3.11 Billion in 2021 [35], *SIMBox* fraud negatively impacts the network quality of experience for legitimate consumers as well as the national security. In particular, by creating network hotspots through the injection of vast volumes of hijacked calls

into under-provisioned cells, the fraud directly impacts network availability and reliability. More significantly, *SIMBox* fraud allows attackers to act as national subscribers, which international terrorists could easily exploit to conduct hidden activities. *SIMBox* devices also give the possibility to eavesdrop on call conversations [55] *impeding users' privacy and giving the possibility to do international espionage*. The induced possibilities of terrorist activities attest to the severity of *SIMBox* fraud.

SIMBox fraud development is facilitated by some regulatory, contextual, and contractual factors explaining its prevalence in the developing world: About 78% of African countries and 60% of Middle Eastern countries are fraud destinations [19], and as much as 70% of incoming international call traffic is terminated fraudulently in some of these countries [135].

- First, the fraud is fuelled by the huge difference between calls' International Termination Rates (*ITRs*) and Local Termination Rates (*LTRs*). Notably, in emerging countries, such a marked difference is due to the *general propensity of governments to set high ITRs* for the domestic network's development, combined with *low LTRs urged by local competition*.
- Second, *easy access to prepaid SIM cards* – contrary to postpaid subscriptions – allows fraudsters to manage multiple call flows while limiting their traceability. From this standpoint, Africa and the Middle East are the areas most concerned with, on average, 94% and 80% of prepaid mobile subscriptions, respectively [154].
- Third is the *manifold corruption of the telecom industry*. For instance, fraudsters may collude with re-seller kiosks to acquire huge amounts of SIM cards using fake identity cards (IDs). Also, to be hired by mobile operators, anti-fraud companies may boost *SIMBox* fraud traffic before a solution demonstration to inflate the apparent size of the fraud and ensure instant results of their proposed solution. Even worse, the operator's fraud-prevention team can be corrupted not to block fraudulent SIM cards when detected.
- Last but not least, *the prevalence of different telecommunications regulatory policies impedes any states' cooperation for fraud mitigation*. Indeed, *the notion of legal can greatly vary from one state to another*: on the one hand, there may be a broad regulation enabling to send traffic through VoIP legally, and on the other hand, a strict regulation considering the traffic of only a few legacy operators as legitimate (e.g., USA and India as in [96]). This explains why *SIMBox* manufacturers are free to produce and publicly advertise for their appliances as in [7, 133]. Furthermore, even at a national level, *operators usually cannot share their pricing terms, routing options, or fraud-related findings* due to privacy concerns and competition [138]. Also, sometimes, a competing operator can profit from the losses and the bad reputation induced by the fraud. For all these reasons, *SIMBox* fraud detection *investigation* involves only the destination operator experiencing losses.

1.2 Challenges

Besides the striking impact of *SIMBox* frauds and the related nationwide threat, several challenges are added, making their mitigation complex.

The scarcity of cellular traffic datasets with fraudulent and legitimate users. *SIMBox* fraud traces in cellular networks are captured in datasets (e.g., CDRs or Audio records) holding sensitive information of users' habits, thus intrinsically private. Hence, access to this data is not uniform and generally scant in the research community and often occurs behind restrictive Non Disclosure Agreements (NDAs). The result is that the potential of mobile traffic datasets to feed fraud detection innovation is curbed. This explains why there is very little research in the area: we identified only 14 fraud detection approaches since 2011 (cf. Table 4.1), which is relatively low for a topical security problem of this importance.

Furthermore, research on *SIMBox* fraud requires ground-truth knowledge to guide analyzes. Ground truth describes the known fraudulent and legitimate users in cellular datasets. Mobile operators are generally aware of no or a relative low percentage of fraudulent users compared to the total amount of users in CDRs (cf. Table 4.1), due to their limited detection capabilities. The remaining large percentage of users, non identified as fraudulent, is considered legitimate. *Thus, detection approaches built from such partial ground truth and wrongly considered as the whole CDRs ground truth likely cause many false negatives.*

While another option to obtain required datasets is setting up an environment to generate frauds through the acquisition of *SIMBox* appliances, there are some considerations to bear in mind. First is the legal aspect of manipulating *SIMBox* appliances for research. Ethically and due to interference with deployed operator networks, *SIMBox* experimentation should be carried out inside a shielded environment (e.g., a Faraday or Anechoic shield). *Hence experimentation requires not only the acquisition of SIMBox appliances (accessible in online commercial platforms) but also the set up of a complete mobile operator architecture test-bed, with running call, SMS, and data services.* Second, even with such a caliber, it remains challenging to scale regarding the amount and models of legitimate or fraudulent devices.

The continuous fraud evolution. As in most security problems, the behavior of fraudsters changes over time to adapt to the target detection solutions. Specifically, *SIMBox* appliance's functionalities are constantly refined to evade existing detection solutions, most of which analyze users' behaviors in cellular network traces (e.g., CDRs) to distinguish fraudulent from legitimate subscribers. Fraudsters counteract by developing advanced strategies to *mimic human communication behavior.*

As a result, *SIMBox* fraud is still present despite existing literature detection approaches' very high accuracy level (reported in Table 4.1). Indeed, until now, literature detection works have been trained from operators' past detection inside *considered-to-be CDRs* ground truth. Such methodologies, therefore, do not advance – but only automate – detection capabilities

and fail to uncover newly developed fraud strategies. Besides, *no information is given on fraudsters' behavior in the analyzed datasets*. Such omission directly impacts the interpretation and leveraging of developed detection methods. Precisely, it is unclear whether the obtained performances are due to the tackling of a naive fraud, *easily detectable and expected to evolve*, or the efficiency of detection designs in the choice of parameters *robust to the fraud evolution*.

The need for quick detection. Considering the low investment required to conduct *SIMBox* fraud (i.e., one-time purchase of *SIMBox* appliances, estimated to \$550 per *SIMBox* gateway, and regular purchase of cheap SIM cards), fraudsters quickly benefit from this malicious activity, easily generating gains of \$100/day per *SIMBox* gateway [78]. Accordingly, the time required to acquire relevant insights for detection and achieve SIMs blocking – currently from a day to a week – is enough for fraudsters to cause damage. The obtained substantial gain fosters fraud continuity in substituting blocked SIM cards. *Therefore, efficient SIMBox fraud detection should provide a quick response to distinguish the fraudsters with high precision.*

1.3 Contributions

This thesis's contributions aim at proposing solutions to the aforementioned problems while opening some lines of discussion. We organize them in a progressive way as shown in Fig. 1.1.

1.3.1 Revealing the *SIMBox* fraud ecosystem

First, a clear understanding of what is *SIMBox* fraud is missing from the literature due to the related investigation barriers. Accordingly, we provide all the necessary elements to understand the *SIMBox* fraud problem in its entirety (cf. **Chap. 3, P1**). Precisely:

- We deeply explore beyond the scientific literature, public sources such as articles from private anti-fraud companies, manuals of *SIMBox* manufacturers, fraud businesses, association reports, and articles from news organizations (cf. Table 3.1) to provide comprehensive knowledge on the fraud ecosystem and the system behind the *SIMBox*.
- We thoroughly review the functionalities of all 50 appliances from the major *SIMBox* manufacturers of the international market [58] and acquire some *SIMBox* appliances that we deeply investigate in an in-laboratory deployment. The gotten practical information helps us provide a taxonomist organization of current *SIMBox* functionalities into configuration units common to all *SIMBox* architectures.
- We further examine the temporal evolution of *SIMBox* fraud strategies related to human behavioral simulation yielding to the fraud's evolutionary perspective.

The results listed above are presented in the following publication(s):

- P1** *SIMBox* bypass frauds in cellular networks: Strategies, evolution, detection, and future directions. Anne Josiane Kouam, Aline Carneiro Viana, Alain Tchana. *IEEE Communications Surveys and Tutorials*, 2021.

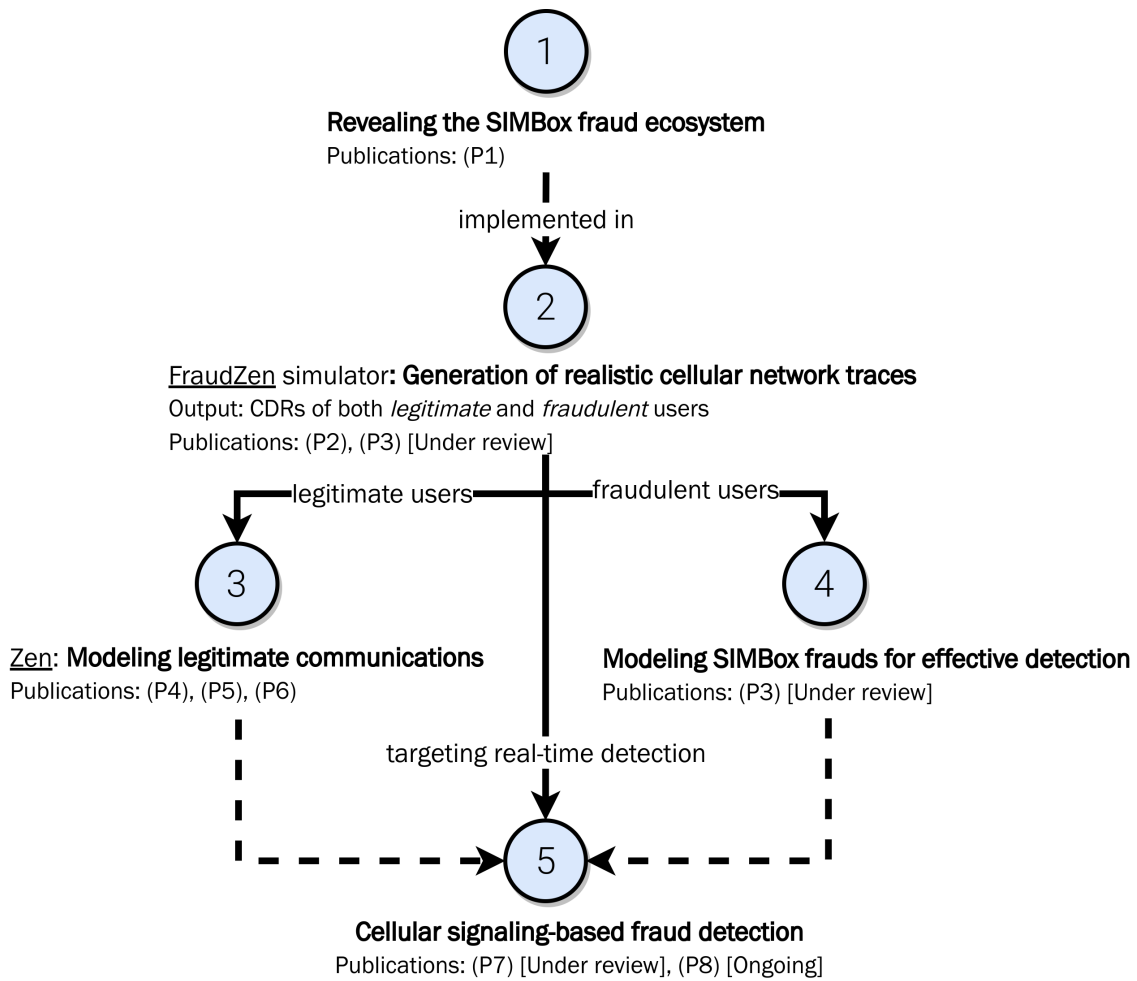


Figure 1.1: Progressive organization of contributions

1.3.2 Generation of realistic cellular network traces

Second, we tackle the barriers related to the exploitation of real-world cellular datasets (i.e., CDRs) for research on *SIMBox* fraud. We propose *FraudZen*: *an environment for the scalable simulation of numerous real fraud strategies*. *FraudZen* overcomes current limitations (i) through the generation of CDRs traces of both legitimate and *SIMBox* fraudulent users in realistic cellular scenarios and (ii) by allowing to reproduce, investigate, and foresee *SIMBox* frauds without purchasing hardware or setting up architectures. (cf. **Chap. 4, P2, P3**). Specifically:

- *FraudZen* implements a realistic cellular networks architecture, reproducing multiple operators' radio-access topology and core networks to provide call/SMS/data services. The implemented architecture allows the creation and configuration of all parties involved in *SIMBox* fraud realization, i.e., *SIMBox* appliances and legitimate users' devices. This enables the generation of innumerable frauds calibrated by the combination of 122 real-world parameters.
- On top of this realistic context, *FraudZen* allows the simulation of various scenarios

involving fraudulent and legitimate users' interaction according to input *communication behaviors* indicating the type (i.e., *what*), the timing (i.e., *when*), the social interaction (i.e., *whom*), and the location (i.e., *where*) related to network events generation. Such communication behaviors are modeled separately for legitimate and fraudulent users in the following two contributions.

- *FraudZen* outputs realistic *CDRs* associated with each simulation scenario, which identifies legitimate and fraudulent users to be used as ground-truth in *SIMBox* fraud on-line/offline detection investigations.

The results listed above are described in the following publication(s):

- P2** Simulating *SIMBox* frauds for detection investigation. Anne Josiane Kouam, Aline Carneiro Viana, Alain Tchana. *ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT) Student Workshop*, 2022.
- P3** [Under Review] *SIMBox* bypass frauds at hand for effective detection. Anne Josiane Kouam, Aline Carneiro Viana, Alain Tchana. *ACM RAID*, 2023.

1.3.3 Modeling legitimate communications

Third, we contribute to modeling legitimate users' behaviors in producing *Zen*. *Zen* is the first-in-the-literature framework capturing real-world legitimate users' communication behaviors. It thus covers the legitimate users' segment of *FraudZen* (cf. **Chap. 5, P4, P5, P6**). Aiming *CDRs* that reliably reproduce real-world *CDRs*' distributions, we make the following:

- Leveraging on a real-world fully anonymized *CDRs* describing users' traffic behavior we propose two modeling of *CDRs* traffic: first using statistical methods (**P4**) and then improving it through deep generative techniques (**P5**). We detail in this thesis only the latter modeling, which captures long-range and inter-features correlations while addressing the population heterogeneity.
- Mobility behaviors of individuals are emulated according to the infrastructure of a real-world metropolitan city. Here, we leverage city planning, transportation information as well literature investigations on laws dictating human mobility [6, 62, 110] to extensively enhance the literature *Working Day Mobility* (WDM) model [45] into *En-WDM*.
- We combine the previous models along with a statistical representation of individual social ties to generate complete *CDRs* describing individual mobility, traffic, pairwise communications, and reproducing daily cellular behaviors of the urban population.

The results listed above are described in the following publication(s):

- P4** Génération de traces cellulaires réalistes. A. J. Kouam, A. C. Viana, A. Garivier, A. Tchana. *Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication (CORES)*, 2022.

P5 LSTM-based generation of cellular network traffic. A. J. Kouam, A. C. Viana, A. Tchana. *IEEE Wireless Communications and Networking Conference (WCNC)*, 2023.

P6 On the intricacies of per individual cellular network datasets generation. A. J. Kouam, A. C. Viana, A. Tchana. Poster presented at *NetSci-X*, 2023.

1.3.4 Modeling *SIMBox* frauds for effective detection

Fourth, we lay the groundwork for *SIMBox* fraud substantive research by addressing the challenges related to the fraud evolution. We propose the first-of-the literature *SIMBox* fraud modeling, grasping fraudsters' intents and enabling fraud design and forecast. By extracting *information used to think like a fraudster*, we thus provide a framework to define meaningful *SIMBox* fraud models, as input to *FraudZen* simulations (cf. **Chap. 6, P3**). Specifically:

- We methodically unravel *SIMBox* appliance's capabilities, obtained from our in-depth *SIMBox* market study (cf. §1.3.1), and extract intuitive and easy-to-interpret *traits encompassing the fraud action areas*, i.e., traffic, mobility, and social communication behaviors. The result is a seminal definition of a *SIMBox fraud model* giving degrees of freedom for *SIMBox* fraud design, reproducibility or anticipation.
- We design a metric to capture a fraud model's *efficiency*, from *FraudZen* generated traces, i.e., *the fraud capability in making fraudulent users blend into legitimate real-world users' crowd*, referred to as *in-crowd-blending capability*. The more efficient the fraud model is, the better it mimics human behaviors, i.e., legitimate users' habits in communication.
- Through realistic *SIMBox* fraud models (from a naive to an advanced one), our designed metric is leveraged to investigate the influence that each fraud model's trait has on fraud efficiency. Results show an average *in-crowd-blending capability* of 99.6% for the advanced fraud model compared to 12.6% for the naive one, validating our framework's ability to define *SIMBox* fraud models of different efficiency levels.
- Further, we use our *SIMBox* fraud model's formalization as a proxy for the in-depth evaluation and interpretation of the 10 ML-based literature works' detection performances. Therefore, we provide takeaways for future detection improvements through *insights on what detection should be aware of and how to react to new fraud models*.

The results listed above are described in the following publication(s):

P3 [*Under Review*] *SIMBox* bypass frauds at hand for effective detection. Anne Josiane Kouam, Aline Carneiro Viana, Alain Tchana. *ACM RAID*, 2023.

1.3.5 Cellular signaling-based fraud detection

Our latest contribution addresses the need for quick fraud detection. We investigate cellular signaling's potential in providing quickly exploitable insights on network devices for *SIMBox*

fraud detection. Hence, we present *SigN*, a novel *SIMBox* detection method to be deployed at the cellular network edge (cf. **Chap. 7, P7, P8**). Precisely:

- We deploy inside a shielded Faraday cage environment with real cellular core and access networks, local and distributed *SIMBox* architectures from the top market manufacturer, and mobile phones from various brands representing legitimate devices.
- *SigN* analyzes the standardized cellular network signaling messages exchanged between user devices and the network in various scenarios and infers a real-time distinction between fraudulent and legitimate devices. In particular, we propose a lightweight and fraudster-unalterable detection approach exploiting UEs (user equipment) signaling latency during the network attachment procedure.
- Preliminary experimental analyses show a *SIMBox* latency overhead in the distributed architecture, on average 40× greater than mobile phones. This paves the way for real-time detection of *SIMBox* appliances at the attachment to the network and thus before any damage.

The results listed above are described in the following publications:

P7 [*Accepted*] Signalisation cellulaire pour la détection des fraudes de contournement. A. J. Kouam, A. C. Viana, P. Martins, C. Adjih, A. Tchana. *CORES*, 2023.

P8 [*Under Review*] You left a SigN in your cellular traffic: International bypass fraud mitigation. Anne Josiane Kouam, Aline Carneiro Viana, Philippe Martins, Cedric Adjih, Alain Tchana. *ACM CCS*, 2023.

1.4 Thesis Outline

The rest of this dissertation is organized in six chapters, as described in the following:

Chapter 2 explains the prerequisite notions about the telephony ecosystem where *SIMBox* frauds are deployed.

Chapter 3 provides a global understanding of *SIMBox* fraud and its context. It makes a comprehensive review presentation of both the fraud system (i.e., the *SIMBox*), the fraud strategies and the literature’s detection contributions. It ends discussing the temporal evolution of the *SIMBox* fraud and the related detection capability.

Chapter 4 details our contribution providing simulation means for the generation of realistic cellular network datasets to unleash research on *SIMBox* fraud detection. It provides a description of the *FraudZen* simulator including components and operation.

Chapter 5 discusses our contribution to *legitimate users behavior modeling*. It details our methodology for capturing traffic, mobility and social aspects of users communication behavior as well as the evaluation of obtained generated CDRs for practical use cases.

Chapter 6 focuses on *fraudulent users behavior modeling*, essential to simulate meaningful frauds. It presents our formal definition of *SIMBox* fraud model and how it is leveraged at the evaluation of literature’s detection performances with related lessons learned.

Chapter 7 describes our contribution on *SIMBox* fraud detection based on cellular signaling data analysis and addressing the need for quick detection approaches. It details *SigN* methodology and presents the related experimental analyzes attesting to its relevancy.

Concluding this dissertation, **Chapter 8** summarizes our findings, details our short-term future works, and discusses long-term perspectives derived from our contributions.

Background: Telephony Ecosystem

Contents

2.1	Mobile telephony networks	11
2.1.1	Calls in cellular networks	11
2.1.2	Calls in VoIP networks	12
2.1.3	VoIP to GSM gateway	12
2.2	Call routing in cellular networks	13
2.2.1	Stakeholders	13
2.2.2	International call	14
2.2.3	Money flow	15
2.3	Cellular network datasets	15
2.3.1	Charging Data Records (CDRs)	15
2.3.2	Cellular signaling	17
2.4	Summary	17

This chapter presents the key elements of telephone networks necessary for understanding *SIMBox* fraud. We focus on the *call service* by first discussing how calls are provided in mobile cellular and VoIP networks as well as the interface between these two networks. Then, we discuss legitimate call routing in cellular networks, including stakeholders, routing schemes, and money flow. We next elaborate on network operators' collected traces (i.e., CDRs and cellular signaling), describing their applicability. At last, we outline our findings.

2.1 Mobile telephony networks

2.1.1 Calls in cellular networks

Call routing is a service provided by 2G, i.e., *GSM* networks, based on establishing a direct circuit between interacting subscribers. Although newer generations of wireless technologies

offer access to a wide range of high-speed data services, they still rely on the 2G circuit-switched architecture to route telephone calls. Therefore, we mainly mention **GSM** networks throughout the manuscript, but more recent generations are also concerned.

For a mobile customer, the *Mobile Equipment* is the entry point to the cellular network. It is uniquely identified by its *International Mobile Equipment Identity* (IMEI) and requires a *Subscriber Identity Module* (SIM) card to access the operator's network services. The SIM card is uniquely identified on the network by its *International Mobile Subscriber Identity* (IMSI) and contains a cryptography key assigned by the operator to encrypt communication.

2.1.2 Calls in VoIP networks

Voice over IP (VoIP) is the technology used to transmit voice over wired (cable/ADSL/optical fiber) or wireless (satellite, Wi-Fi, UMTS or LTE, etc.) IP networks. VoIP network is based on *VoIP servers*, providing authentication, management and routing services to *VoIP clients*, and optionally *VoIP gateways* allowing interconnection with other telephone networks (i.e. *Public Switched Telephone Network* (**PSTN**) and cellular).

VoIP clients are *IP hard-phones*, *IP soft-phones* and even analog **PSTN** phones combined with an *Analog Telephone Adapter*. In companies, they are managed by a central component called **IP Private Branch Exchange** (IP Private Branch Exchange), which allocates an IP phone number to each station and connects internal calls (see Figure 2.1).

VoIP is provided as a cellular network data service through mobile applications referred to as *Over-The-Top* (OTT) apps (e.g., Skype, Discord, Whatsapp). These apps, developed on the top of VoIP protocols, provide cheap call services that attract more users and are seen as a threat by mobile operators [132]. VoIP calls are cheaper than cellular ones because they rely on an IP network's existing service and infrastructure (e.g., the Internet or an Intranet). Voice data is compressed and encapsulated as IP packets before its transmission over the network; this is done by specific algorithms called *codecs*, which determine the sound quality related to the bandwidth usage. On the other hand, VoIP calls quality is generally poor due to bandwidth sharing (for services other than VoIP) and IP network latency. As a result, they are affected by packet losses, delay, and jitter, which cause gaps in the audio flow.

2.1.3 VoIP to GSM gateway

Despite the growing trend of OTT applications, cellular phone calls are still widely used by customers and are, in some cases, requisite. Therefore, to exchange with the cellular network (e.g., a call to a customer or an employee on a mission), companies use VoIP GSM gateways, also known as *SIMBox*. A *SIMBox* manages a set of SIM cards from various mobile operators to ensure the live broadcast of the audio signal from the IP network to the cellular one and vice versa, which significantly extends the voice communication coverage (see Figure 2.1). Hence, each time a call is made from the company's IP hard/soft-phone to the cellular network, a SIM card is automatically allowed by the *SIMBox* to transmit the flow as a cellular phone call

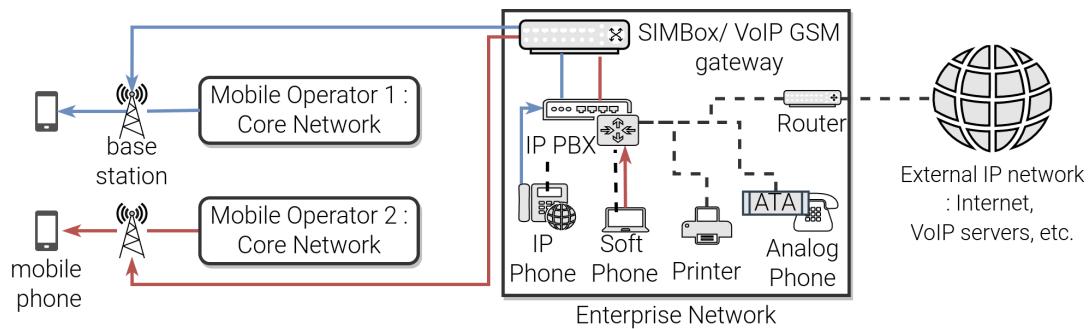


Figure 2.1: Gateway from a company's internal VoIP network to the cellular network

to the called party. For instance, in Figure 2.1, using two SIM cards, the *SIMBox* allows the simultaneous routing of two VoIP calls to subscribers of two different cellular networks.

In large companies and businesses, *SIMBox* equipments have a strong market, for economic and operational reasons, but with a controlled usage by licensed telecommunication providers and regulators. Companies can significantly reduce their telephone expenses to the cellular network with these devices by avoiding roaming charges.

2.2 Call routing in cellular networks

Call routing schemes and involved stakeholders can vastly vary depending on if the call is domestic (within the country) or international; *on-network* or *off-network*. A phone call is said to be *on-network* (on-net) when the caller and the called parties are both customers of the same mobile operator, on the contrary of *off-network* (off-net) calls.

2.2.1 Stakeholders

The following parties may play a role in the termination of a phone call.

End-users emit and receive calls. Using multi-SIM devices, they may have two or three SIM cards from different providers. This is common in developing markets as it helps end-users always get the best offer from competing network operators.

Mobile Operators provide call routing through the traffic relay from the radio access network by the *base station* to the core network. At the core network level, the *Mobile Switching Center (MSC)* establishes a route to the called party. In the case of an off-net call, it transfers the call traffic to the *Gateway MSC* for interconnecting with the destination mobile operator. The interconnection can be a direct link or through *intermediate carriers*.

Intermediate carriers are public (e.g., Tata Communications¹ in India) or private companies (e.g., Belgacom ICS² and Telia Carrier³) offering routes to termination or transit countries that they buy and acquire through partnerships and resell to others. They mainly intervene in international call routing when there is no direct link between the originating and the destination

¹<https://www.tatacommunications.com/>

²<https://bics.com/>

³<https://www.teliacarrier.com/>

operators. Therefore, the route followed by the international call traffic is carrier-to-carrier hops from the originating mobile operator to the destination one.

The interconnection between carriers and operators is governed by agreements that provide the various terms and conditions, including the traffic measurement, the *Points of Interconnection* between carriers, and the quality of service standards [27]. There are numerous technologies of transport links a carrier can use to convey received traffic: satellite links, submarine communication cables, fiber rings, or such, impacting the pricing and the quality of the route. Increasingly carriers also rely on VoIP technology to transmit voice as data packets. Therefore, a hop (in the international termination route) is considered *legal* if the carrier provides a license in its country to use a regulated transport link technology. VoIP links are challenging to regulate and control and therefore present some challenges and risks; Depending on the regulations, they can thus be considered *illegal*. Admittedly, there are three types of international termination routes: *white*, *grey*, and *black* [24]. A route is considered *white* when there is no illegal (black) hop all over the interconnection path. On the contrary, *grey* routes are arrangements where one hop is illegal, i.e., the originating operator sends the traffic to a legitimate carrier, but the traffic is terminated at the destination by an unlicensed carrier. This is the case of most calls from the USA to India [96]. In *black* routes, both source and destination use unconventional interconnections.

The telecommunication market is dynamic. A mobile operator usually has interconnections with several (maybe hundreds) carriers for each destination country and has to choose between them for the termination path. Besides, the quality and the price of these routes may vary weekly for the same carrier. To keep up with changes, *Least Cost Routing* algorithms [37] at the level of the *Gateway MSC* automatically select the most efficient route regarding quality and pricing to ensure the efficient use of the existing network infrastructure and maximize the operators' income.

Regulators, either public (e.g., ministries) or private, rule mobile operators' activities and partnerships in some countries. Indeed, governments usually consider telecommunications an essential public service and want to ensure services are supplied consistently with the national perception of the public interest.

2.2.2 International call

In Figure 2.2 an international call flow is depicted. Phone X calls Phone Y, a customer of operator B abroad. The originating operator (Operator A) transfers the call request through two intermediate carriers, with carrier 1 automatically chosen through least cost routing. Carrier 2, with a direct connection, sends the traffic to operator B's core network, which establishes the call route until Phone Y. This example draws a white call routing as all carrier-to-carrier links are conventional, well-monitored connections specified by contractual engagements. The example assumes there are only two intermediate hops between operator A and operator B, but this value is unknown in practice as call routing is often opaque. Indeed, each carrier only

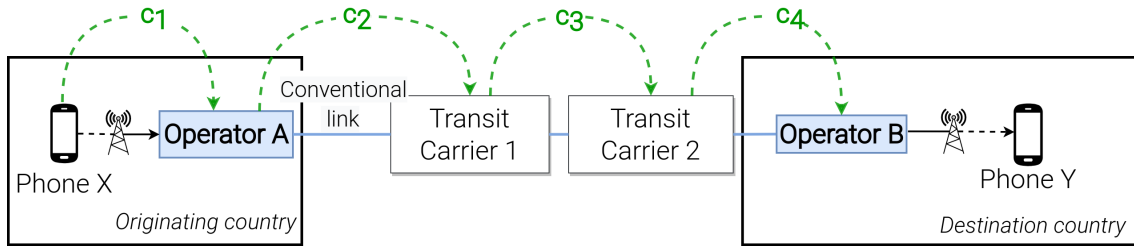


Figure 2.2: International call scheme

knows the previous and the next hops of the termination route, as well as the originating and destination phone numbers [138]. Besides, the originating number can sometimes be missing or incorrect.

2.2.3 Money flow

In all call routing schemes (domestic on-net/off-net and international), the caller pays the call termination fees; however, international calls are generally more high-priced than domestic calls. This is because an international call may travel over multiple intermediate operators before reaching its destination. Therefore, each transit operator gets a share from the call revenue for passing over the call traffic, referred to as *settlement rate*; and the destination operator receives the *call termination fee* for terminating the international call on its network. In Figure 2.2, the green dashed line represents an example of money flow. Operator A bills the end customer a *collection charge* c_1 , including what it retains plus the sum c_2 it pays to carrier 1 for routing the call. Similarly, each transit carrier bill includes its fees and the sum required to ensure call routing to the destination. Lastly, the destination operator (Operator B) charges (c_4) represent the termination fees.

2.3 Cellular network datasets

In the following, we describe two data types related to cellular network traffic that we exploit throughout this manuscript.

2.3.1 Charging Data Records (CDRs)

With mobile devices becoming proxies for human presence and activity, datasets collected by mobile operators, i.e., Charging Data Records (CDRs), are acknowledged as a common tool for studying human mobility, infrastructure usage, and traffic behavior on a large scale [84]. CDRs describe time-stamped and geo-referenced event types (i.e., data, calls, SMS) generated by each mobile device interacting with operator networks (cf. Table 2.1). They comprise city-, region-, or country-wide areas and usually cover long periods (months or years); no other technology currently provides an equivalent per-device precise scope.

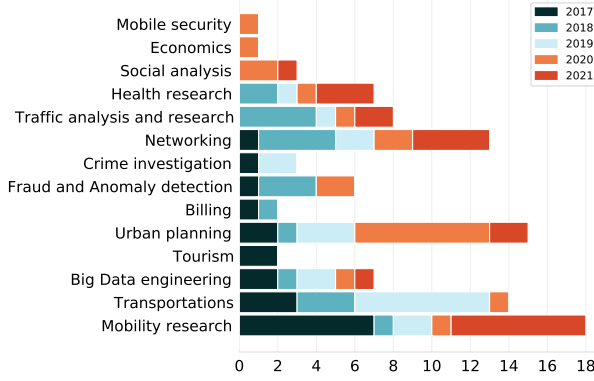


Figure 2.3: Distribution by domain of the last 5-year most relevant publications using CDRs.

Table 2.1: CDRs format.

	CDR field
General	Phone number
	IMEI code
	Timestamp
Traffic	Event-type (call/SMS/data)
	Call duration
	Data session size
Social	Phone number of the correspondent
Mobility	Network cell Id

As such, CDRs datasets have been leveraged in various domains. Especially for *SIMBox* fraud investigations, CDRs are the *de facto* means used in the literature to distinguish fraudulent users from legitimate ones, allowing the inference of manifold communication behaviors. While a powerful asset, this also represents a weakness due to CDRs’ inherent accessibility and usability issues limiting their exploitation and research reproducibility.

CDRs value recognition. Generated by the continuous interaction of a urban-wide population with cellular networks, CDRs represent a rich source of knowledge, valuable to many research communities [115]. For a quantitative appreciation, Fig. 2.3 identifies as many as 14 different research domains leveraging CDRs, among 100 items selected from a 5-year sample set of 1022 CDR-related publications (gotten from Google Scholar). This clearly shows a great diversity of domains on this sample only ($\sim 10\%$) and considering the 5-year period.

Limitations in CDRs exploitation.

Unlike WiFi networks, cellular networks are mobile operators’ exclusive property, hardening outside access to collected CDRs. CDRs access is usually granted through NDAs and is often hardly available for most researchers, time demanding, or imprecise due to privacy laws, bringing *accessibility issues*.

Though strongly necessary, privacy compliance asks for CDRs information aggregation, which hardens their usability and limits the exactness of related investigation. Aggregation usually concerns flows, space, time, and event information in CDRs. For instance, the CDRs available at [80] describe aggregated flows of individuals and their number of generated events per intervals of 10 min and square grids of size 235 meters. This points a lack of *information precision* in available CDRs.

Not surprisingly and justifying the regular CDRs’ imprecision issue, personal details of individuals’ life habits, inferred from CDRs, calls for privacy-strict exploitation rules and impairs data shareability: e.g., when reconstructed [36] or not [107], majority of individuals’ trajectories in CDRs (i.e., higher than 80%) can still be precisely identified, even if anonymized and being sparse in space and coarse in time.

Restricted access to CDRs impacts the *flexibility* of scaling up or adapting CDRs’ research

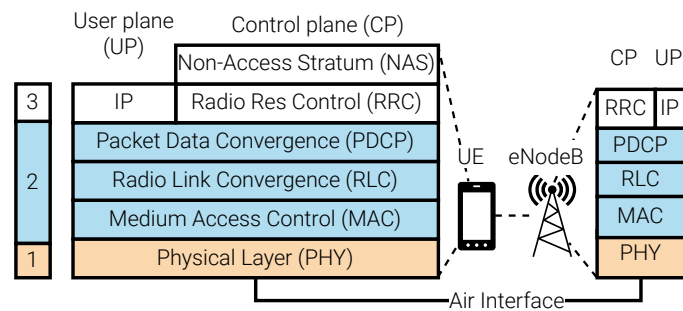


Figure 2.4: 4G (LTE) mobile network protocol stack

results in terms of the population size, the duration, or the covered geographical area, thus limiting advanced research requiring such data richness.

2.3.2 Cellular signaling

As illustrated in Fig. 2.4, the communication between *User Equipment* (UEs) and the mobile core network is framed by a 3-layered protocol stack, i.e., physical, data link, and network layers. Signaling messages are exchanged between UEs and the network, according to such well-defined protocols, with the aim to control the UEs, manage access to the network and services, and monitor terminals in case of mobility.

Mobile network protocols are distributed according to the *Access Stratum* (AS) and the *Non-Access Stratum* (NAS). The AS (RRC, PDCP, RLC, MAC, and PHY) manages the signaling between UEs and base stations for radio resource management, handover, and data encryption/compression. The Non-Access Stratum (EMM and EPS in LTE) manages the signaling between UEs and the core network, including establishing data or call sessions and mobility.

The network attachment procedure, for instance, involves the AS and the NAS. It establishes a new connection between a UE and the network that occurs when the UE is powered on, moves into a new tracking area, or after losing network coverage. In 4G (LTE), the attachment procedure consists of several steps aiming the (i) UE Identity (i.e., IMSI/IMEI code) acquisition, (ii) the mutual UE and network authentication, (iii) the NAS security setup, (iv) the UE location update, and (v) the EPS (Evolved Packet System) session establishment [1].

2.4 Summary

The telephony ecosystem has enormously evolved in recent decades and interconnects billions of user devices worldwide. This chapter showed that such a well-monitored environment builds upon several telephone networks (PSTN, VoIP, GSM, and upper cellular network generations) and specialized equipment able to switch from these networks to others, forming a complex architecture. Not surprisingly, the growing impact of these technologies on consumers has sparked governments' interest in their role of protecting the population's rights and the national economy. However, leading to a large number and variety of operators and service providers, it is impossible to ensure transparency while preserving competition and

liberalization good for the economy. All these hazards of the cellular network ecosystem, challenging to overcome, have favored the proliferation of numerous frauds. In the next chapter, we explore, in particular, *SIMBox* bypass fraud related to the routing of international calls.

SIMBox Fraud

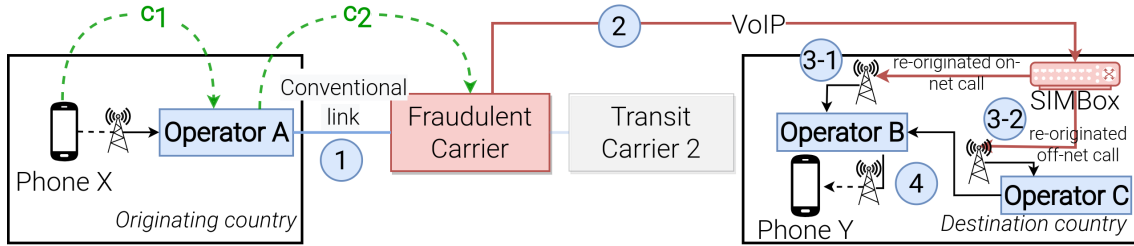
Contents

3.1	General description	21
3.1.1	Fraud schemes	21
3.1.2	How do fraudsters benefit?	22
3.2	The <i>SIMBox</i> architecture	22
3.2.1	<i>SIMBox</i> components	23
3.2.2	<i>SIMBox</i> deployment	23
3.2.3	<i>SIMBox</i> functionalities	24
3.3	<i>SIMBox</i> fraud detection in the literature	26
3.3.1	Test Call Generation (TCG)	27
3.3.2	Rule-based method (RBM)	27
3.3.3	CDR-based approaches	29
3.3.4	Audio-based approaches	29
3.3.5	Signalling data-based approaches	30
3.4	Fraud evolution	30
3.4.1	Hardware evolution	32
3.4.2	Functional evolution	32
3.4.3	Evolution pace	32
3.5	Summary	33

This chapter reports a comprehensive overview of the *SIMBox* fraud from an in-depth review of the scientific literature and specific information collected from various sources, as summarized in Table 3.1. First, we give a general description of the *SIMBox* fraud while explaining the fraud schemes, benefits, and factors (§3.1). Then we explore the system behind the *SIMBox* by commenting on its components, and report *SIMBox* functionalities developed to reduce detection effectiveness (§3.2). Next, in §3.3, we discuss and introduce a categorization

Table 3.1: Classification of surveyed information sources on *SIMBox* fraud

Category	Sources	Total	
Scientific literature	Global information on <i>SIMBox</i> fraud	[24]	4
	<i>SIMBox</i> fraud detection contributions	[46, 132, 102]	
Private anti-fraud companies	[4, 114, 140, 139, 88, 86, 87, 153, 158, 5, 75]	14	
<i>SIMBox</i> manufacturers	[135, 26]	11	
<i>SIMBox</i> fraud businesses	[98, 99, 38, 18, 129, 29, 103]	19	
Association reports and news organizations	[151, 8, 143, 15, 145, 130, 41, 14, 9, 42, 44, 11, 144, 13, 12, 17, 160, 16, 146]	4	
	[57]	6	
	[56, 53, 59]		
	[35],[34],[33]	6	
	[119, 154, 108, 66]		

Figure 3.1: Possible schemes of an international call flow in case of a *SIMBox* fraud

of *SIMBox* detection research conducted in the literature. In §3.4, we uncover and discuss the fraud evolution and its impact on fraud detection capabilities. At last in §3.5, we summarize our findings. All such elements thus provide a complete introductory guide to *SIMBox* fraud investigations.

3.1 General description

SIMBox frauds build upon two main telephone systems' inherent characteristics. First, the possibility of *interconnection between VoIP and cellular networks* is the cornerstone for *SIMBox* fraud. This cannot be circumvented as it provides many benefits for companies besides extending the voice communication range. Second, the *variety of operators and services* offered (transit carriers and VoIP providers) in telephony makes it challenging to ensure each service provider/carrier has good purposes. This point is difficult to tackle without undermining competition and liberalization, thus slowing down service improvement. These root characteristics are the cause of weaknesses exploitable for the spread of fraudulent schemes and techniques.

3.1.1 Fraud schemes

SIMBox fraud consists of deviating call traffic from the conventional routing routes to a VoIP network using the appropriate gateway, i.e., the *SIMBox*. Its scheme can be broken down into four steps, summarized in Fig. 3.1. (1) a call is emitted from one country to another and transits through regulated routes until a fraudulent carrier. (2) The fraudulent carrier uses a gateway to route the traffic through the VoIP network to the destination country where fraudsters' partners have a *SIMBox*, and the traffic is received at the *SIMBox* level. (3) The

SIMBox reconverts the traffic to a mobile call using a SIM card as the call's origination. As distinguished in Fig. 3.1 the re-originated call can be on-net (step 3-1) call or off-net (step 3-2). (4) The call re-originated by the *SIMBox* is terminated to the call recipient.

Domestic on-net. This is the most recurrent case. An on-net termination indicates the SIM card used to re-originate the call is provided by the destination operator (Operator B). It is the most cost-effective case for fraudsters as on-net calls can be almost free charged; minimizing the cost of terminating calls through the *SIMBox* maximizes their revenues.

Domestic off-net. Here, fraudsters use a SIM card from a competing operator to re-originate the call in domestic termination. It may reduce fraudsters' financial outcomes in case of off-net termination charges; however, it makes it harder for operators to track fraudulent activity.

3.1.2 How do fraudsters benefit?

The primary motivation for the *SIMBox* fraud is financial; as estimated in [78], fraudsters can easily generate over \$100/day per *SIMBox* gateway. They are attracted by the difference between International Termination Rates (ITRs) and Local Termination Rates (LTRs), which can be tremendously high in emerging countries (e.g., 2.8 to 28 times higher in Cameroon [118]). To obtain a *share of the termination fees*, fraudsters develop techniques to insert themselves into the voice traffic termination route before sending it to the *SIMBox*.

As in Fig. 3.1, the most classical technique consists of hijacking operators' voice traffic through unfair carrier service. Fraudsters advertise very cheap rates for a destination number range by which they attract operators or transit carriers' international traffic. This is facilitated by a *lack of due diligence* in agreements between carriers and a *lack of transparency* in telephony networks that precludes the verification of a carrier's connectivity to reach a number range.

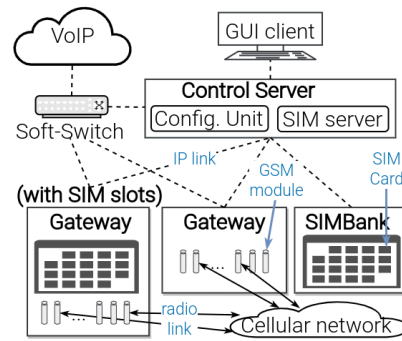
Besides, other bypassing techniques allow fraudsters to divert the traffic directly from subscribers. For instance, fraudsters have been using *override services apps* (e.g., RebTel [133]) that offer low-cost calls by selling minutes or charging monthly. They may also use *international calling cards*, i.e., prepaid cards that give international calling minutes to end consumers at discounted rates.

3.2 The *SIMBox* architecture

Understanding the *SIMBox* architecture and internal functioning is a required step towards comprehending the fraud strategies it can form. There are various *SIMBox* models on the international market, depending on the manufacturer. These models may differ according to the components' appellation, size, or functionalities. We carried out a comprehensive market review encompassing all 50 *SIMBox* appliance from the six major *SIMBox* manufacturers [59], from which we acquired, deployed, and tested five, as summarized in Table 3.2. Our study reveals an organization and functional architecture common to *SIMBox* models. We describe in what follows such an organization including components, deployment, and functionalities.

Table 3.2: Specifications of reviewed market *SIMBox* models

Manufacturer	# gateways	# SIMBank	# Control server
Hybertone	10	2	1
Dinstar	6	1	1
Antrax	2	2	1
Ejoin	8	2	1
Portech	6	2	3
2N VoiceBlue	2	0	0
Acquired devices			
Hybertone	3, i.e., [73]	1, i.e., [74]	1

Figure 3.2: *SIMBox* distributed architecture

3.2.1 *SIMBox* components

The *SIMBox* is a standard appliance operating as a VoIP GSM gateway. It receives diverted call traffic as a VoIP client and terminates it by re-originating cellular mobile calls using numerous SIM cards (e.g., the GoIP324 *SIMBox* model [73] has 128 SIM slots). The *SIMBox* continuously creates "virtual" UEs by associating SIM cards and GSM modules. In this association, the GSM module provides wireless communication with the network and the SIM card identifies and authenticates the formed UE. The *SIMBox* operates through the interaction of three types of hardware components:

- The *gateway* is a rack with a set of GSM modules maintaining the wireless communication inside a given frequency range corresponding to different generations of wireless technologies (2G/3G/4G) (e.g., the GoIP324 model [73]). It receives incoming VoIP traffic and distributes it to the GSM modules.
- The *SIMBank* is an appliance with numerous SIM slots that remotely holds a bundle of SIM cards (e.g., the SMB32 model [74]). It handles the *SIMBox* SIM cards, i.e., their addition, removal, and the transfer of their data and status to other components.
- The *control server* is a web server providing the *SIMBox* control functions, i.e., the binding of SIM cards to GSM modules and the whole architecture's configuration. It can be hosted online to ease remote access from a web GUI client.

From such components we distinguish two *SIMBox* architectures: *standalone* and *distributed*. In the standalone architecture the *SIMBox* consists of a unique gateway equipped with SIM slots, which can thus handle all components' functions at once. The distributed architecture involves several appliances: at least one gateway, at least one SIMBank, and the control server. Fig. 3.2 depicts a distributed architecture with two gateways and one SIMBank.

3.2.2 *SIMBox* deployment

In practice, fraudsters usually follow some conventions when deploying a *SIMBox* architecture in a city for fraudulent termination. First, they have to choose where to locate the different

gateways. Gateway locations must ideally be crowded, such as city centers, market areas, densely residential districts, or call-center areas. Such overcrowded places enable the camouflage of *SIMBox* traffic by the massive flows of calls made in these areas. Fraudsters rent offices or apartments, at these spots, with stable power and Internet access for continuous gateway operation and connection with the *SIMBox* architecture.

On the other hand, the architecture's SIMBank(s) do(es) not emit a cellular signal and can be located anywhere in the country or abroad. Still, the IP connection's quality should be good beyond a certain threshold to allow smooth communication with the gateways. For instance, the Hybertone manufacturer [143] requires a packet delay of less than 300ms and a packet loss rate of less than 1%. The control server is usually hosted on a private server, and its configuration interface is accessible online. Finally, the fraudulent carrier manages the Soft-Switch emitting incoming VoIP calls to the *SIMBox* architecture.

3.2.3 *SIMBox* functionalities

SIMBox fraudsters intercept international calls and then rely on their appliance functionalities to control and re-originate local calls *the most indistinguishable from legitimate traffic*, to avoid being detected. They therefore designed features to mimic the human communication behavior, known in the literature as *Human Behavior Simulation (HBS)* [121].

HBS functionalities are set and applied within configuration units of the *SIMBox* architecture, namely groups of SIM cards (i.e., SIM groups) or of GSM modules (i.e., GSM groups). We classify *SIMBox* functionalities with similar intent into ten categories, from C_1 to C_{10} , and report in Table 3.3 their configurations. Specifically, we distinguish:

C_1 - ***SIM activity limitation***. This category's purpose is to control fraudulent SIM cards from being used excessively or at unusual periods, which would ease their detection. Limitations are of three types. First, *parameter limitation* enforces thresholds to metrics related to SIMs' call behavior (e.g., #calls, total/avg. call duration, etc.). Second, *parameter limitation per period* automatically block SIMs exceeding the threshold value until the end of a specified period. Third, *time limitation* ensures a SIM group operates only at a specified day or week interval.

C_2 - ***SIM-to-module allocation***. This category controls the association between SIM cards and GSM modules for the generation of *virtual* mobile devices. To this end, we distinguish three-fold policies: (i) a *rotation trigger* defining when to change an allocated SIM card to discard the virtual mobile device, (ii) a *rotation policy* defining the next SIM to allocate to a GSM module, and (iii) a *SIM migration policy* determining whether a SIM can be allocated based on its history.

C_3 - ***IMEI modification***. The IMEI (International Mobile appliance Identity) is a unique identification code for mobile devices. This category allows modifying the from-factory and easily detectable IMEI specific to each GSM module. It also helps limiting the number of different mobile devices to which a SIM card is associated in case of mobility, by simulating the whole User Equipment (i.e., SIM card and GSM module) movement. IMEI codes are,

Table 3.3: SIMBox HBS functionalities, Parameters, and Illustrations

HBS functionality	Parameter	Value	Illustrations
C1- SIM activity limitation and C6- Channel control activity	Type of limitation	Parameter limitation	Hybertone [145], Dinstar [42], Ejoin [44], Portech [130]
		Parameter limitation per period	Antrax [14, 9], Dinstar [42]
		Time limitation	Hybertone [145], Antrax [14, 9], Ejoin [44], Dinstar [42], Portech [130]
C2- SIM to module allocation	Rotation trigger	Threshold method	Hybertone [145], Antrax [14, 9], Portech [130]
		Activity script method	Antrax [14, 9]
	Rotation policy	round-robin method	Hybertone [146], Antrax [15]
		random method	Hybertone [145], Portech [130]
		statistic-based factor	Hybertone [145], Antrax [15], Dinstar [41]
		statistic-based factor per period	Antrax [15]
	SIM migration policy	Manually fixed method	Hybertone [145]
		Any except previous	Antrax [11], Hybertone [145]
		Any except previous Zone ID	Hybertone [144]
		Any gateway	Antrax [11]
C3- IMEI modification	Generation rule	Specified order	Antrax [11]
		Fixed frequency	Antrax [13], Dinstar [42], Hybertone [145]
		Threshold on call activity	Dinstar [42]
	Change policy	At counts of SIM rotations	Antrax [13], Dinstar [42]
		Manual modification	Hybertone [145], Ejoin [44], Antrax [13]
		Random IMEI	Antrax [13], Hybertone [145]
		Prefix-based IMEI	Ejoin [44], Antrax [13]
		IMEI from a database	Antrax [13]
		Type Allocation Code	
		prefix-based IMEI	Antrax [13], Dinstar [42], Hybertone [145]
C4- Network activity generation	Generated services	Internet (web browsing)	Ejoin [44], Dinstar [42], Antrax [12]
		USSD commands	Hybertone [145], Ejoin [44], Dinstar [42], Antrax [17], Portech [130] 2N voiceblue [160]
		SMS	Hybertone [145], Ejoin [44], Dinstar [42], Antrax [16], Portech [130] 2N voiceblue [160]
		Calls	Ejoin [44]
C5- Base station selection	Selection policy	Manually	Portech [130]
		Default by the network	Hybertone [145], Ejoin [44], Portech [130], Dinstar [42]
		Fixed	Hybertone [145], Dinstar [42]
		Random	Dinstar [42]
		Poll	Hybertone [145], Ejoin [44]
		Advanced	Hybertone [145], Dinstar [42]
C7- Call routing authentication	Phone number lists	Allow-list	Hybertone [145], Dinstar [42]
		Block-list	Hybertone [145], Dinstar [42], Antrax [10]
C8- Routing policy	Choice of the GSM module to route the call	First-released GSM module	Hybertone [145]
		Balance	Hybertone [145]
		Round-robin	Hybertone [145]
		Random	Hybertone [145]
C9- Call forwarding	Forwarding conditions	Unconditional	Hybertone [145], Dinstar [42]
		Busy	Hybertone [145], Dinstar [42]
		Unreachable	Hybertone [145], Dinstar [42]
		No reply	Hybertone [145], Dinstar [42]

therefore, related either to each GSM module (if set in a GSM group) or *SIMBox* SIM (if set in a SIM group). The defined *generation rule* triggers the change of the IMEI in either case and the *change policy* determines the new IMEI value.

C_4 - Network activity generation. These functionalities generate network traffic other than the *SIMBox* outgoing calls to reproduce human behavior. For instance, SIM cards can automatically initiate calls to each other, web browse, and send SMS. The chosen *application trigger* initiates the operation of the activated *applications* (i.e., call/sms/data).

C_5 - Base station selection. This category simulates virtual devices' neighborhood movements by connecting GSM modules to their surrounding cell towers. The *change trigger* initiates movements and the *selection policy* determines to which cell tower GSM modules connect.

C_6 - Channel activity control. This category controls the quality of the radio channels through appropriate metrics such as the average call duration, or the number of rejected calls, as some detection methods are based on the identification of voice call signal degradations. GSM modules with metrics exceeding a fixed threshold are blocked or allocated to others SIMs.

C_7 - Call routing authentication. It defines how the *SIMBox* handles incoming call traffic from international. GSM modules can accept calls only to a specific format of numbers (e.g., referring to an operator) or make filtering related to block- and allow- lists of numbers. Besides, phone numbers are automatically added to the block-list based on their calling patterns.

C_8 - Routing policy. The routing policy is common to all GSM groups and determines the available *virtual* mobile device to route an incoming call based on the traffic history.

C_9 - Call forwarding. The call forwarding policy allows a call intended for a *SIMBox* SIM card to be forwarded to another phone number so that a human agent can reply.

C_{10} - Voice and codec configuration. Configurations to voice and codecs used in the *SIM-Box* intend to improve the call quality as some detection methods are based on audio call pitfalls (packet losses and jitter) identification. They allow fraudsters to select from a variety of supported codecs, as well as to handle jitter buffer or audio silence suppression.

Additionally, the *SIMBox* provides CDRs (Call Detail Records) for accounting management, which enables specific queries on SIM card traffic. Unfortunately, fraudsters often use these provided CDRs to refine their strategies by exploiting publicly available detection techniques.

3.3 *SIMBox* fraud detection in the literature

Here, we discuss existing literature approaches for *SIMBox* fraud detection, all summarized in Table 3.4. Such approaches are organized in Fig. 3.3 into two categories expressing their operation mode, i.e., active or passive. Active methods (§3.3.1 - §3.3.2) require a permanent human action and significant material resources to be implemented. They represent the first response of mobile operators to the fraud. On the other hand, passive methods are designed to automatically detect fraudulent entities in an operator network, with little human monitoring. We further categorize passive methods into three sub-groups depending on the analyzed data

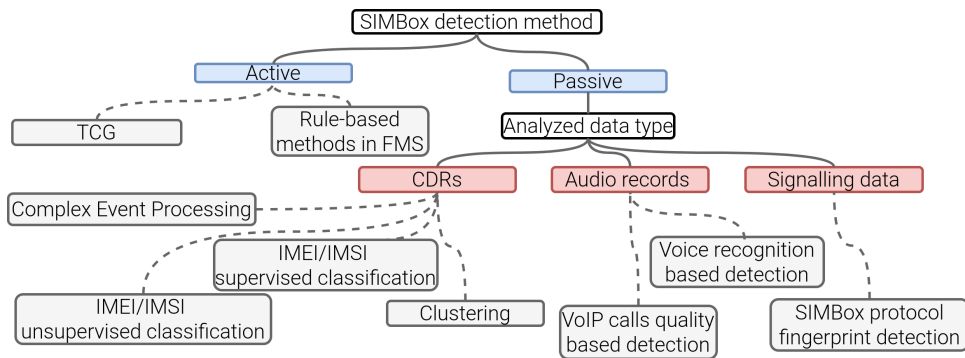


Figure 3.3: Categorization of existing *SIMBox* fraud detection methods.

type: CDR analysis-based approaches (§3.3.3), audio analysis-based approaches (§3.3.4), and signalling data analysis-based approaches (§3.3.5).

3.3.1 Test Call Generation (TCG)

TCG consists of setting up test phone numbers in a target mobile network and making calls to those test numbers from different countries using different interconnect voice routes. This way, a local *Calling Line Identification (CLI)* indicates a *SIMBox* number and can be acted upon accordingly. The call campaign maximizes detection by concentrating on routes detected to have a high volume of *SIMBox* terminations. **TCG** is known for not making false positives, which explains its wide adoption by anti-fraud services [38, 18, 129, 29, 103]. Yet, it is expensive requiring to make several calls, each call being associated with some resource consumption.

TCG worked successfully for many years. Yet, between 2012 and 2013, its effectiveness significantly dropped as fraudsters figured out how to avoid detection. Specifically, they analyze the voice call traffic coming toward their *SIMBox* appliances. Based on usage patterns, they can differentiate calls to real subscribers from those originating from a **TCG** campaign. They can either block such test calls or reroute them to a legitimate carrier. Fraudsters can also allocate pools of SIM cards to be sacrificed by allowing their detection. This makes mobile operators feel confident and deceive their vigilance. Furthermore, the sacrificed SIM cards are chosen to refrain from using **HBS** techniques and, therefore, have an apparent fraudulent profile (i.e., high call traffic and no mobility) that cannot be leveraged to identify other SIMs.

3.3.2 Rule-based method (RBM)

Rule-based method consists of establishing basic rules for subscriber profiling to identify fraudulent SIM cards (e.g., done in [5]). This involves the analysis and monitoring of call patterns (e.g., outgoing call count, cell ids counts, incoming to outgoing call ratio, SMS originating/terminating counts, etc.) of a set of subscribers, looking for an abnormal behavior. Any case identified and validated can then be used to profile and uncover other similar SIM cards. This approach is less costly and has better coverage than **TCG** because once a profile is established, it can be extended over all available subscribers for a wide detection range. However,

Table 3.4: Summary of existing detection work on SIMBox fraud detection classified by category

Category	Detection method	Year	Principle			Countermeasure	Year		
Active	TCG	~2010	Generation test calls from abroad to a target network and CLI verification			HBS - C7 - C9 Sacrifice of naive SIM profiles	2012		
	RBM	/	Basic rules establishment for subscriber profiling			HBS - C1 - C2	2011		
Passive	CDR-based		Data Preparation	Model building and evaluation	Detection time				
		[140]	2013	Call behavior	ANN	A day	HBS - C1 - C2	2011	
		[139]	2014	Call behavior	SVM	A day	HBS -C1 - C2	2011	
		[114]	2014	- Call behavior - Mobility - Entity properties	Linear comb. (RF, ADTree, FTree)	A week	HBS -C1 -C2 -C3	2011	
		[102]	2015	- Call behavior - Mobility - Network usage	Fuzzy logic	/	HBS 1. C1 2. C2 3. C4	2011 (1-2) 2013 (3)	
		[88]	2015	- Call behavior - Mobility	CEP	Real-time	HBS - C1 - C2	2011	
		[4]	2016	- Call behavior - Entity properties	- ANN - SVM - Boosted Trees - Logistic Classifier	A day	HBS - C1 - C2	2011	
		[86]	2018	- Call behavior - Mobility - Network usage - Entity properties	- ANN - RF - SVM	- 4 hours - A day - A month	HBS 1. C1 2. C2 3. C3 4. C4	2011 (1-3) 2013 (4)	
		[87]	2019	/	- ANN - SVM	/	/	/	
		[153]	2020	- Call behavior - Mobility - Network usage	- ANN - RF - SVM	- An hour - 4 hours	HBS 1. C1 2. C2 3. C3 4. C4	2011 (1-3) 2013 (4)	
		[158]	2020	Call behavior	CEP	Real-time	HBS C1	2011	
		Audio-based	[132]	2015	Detection of call audio degradation		Real-time	HBS -C6 -C10	/
			[46]	2017	Recognition of call speakers voices			/	/
Signaling-based	/	/	Intuition: detection of SIMBox fingerprint			/	/		

it has several limitations. First, it causes a non-negligible rate of false positives and requires continuous monitoring and field expert intervention. Second, through time, the whole process of analyzing data gets more complex as rules are added to the system. It increases the detection latency, allowing fraudsters to make enough profit before being blocked.

RBM have been effective in detecting *SIMBox* fraud before the integration of *HBS* techniques (discussed in Section 3.2.3) into *SIMBox* appliances. Such techniques significantly increases the false positive rate, paralyzing the decision to block a suspected SIM card.

3.3.3 CDR-based approaches

Such approaches analyze the content and the occurrences of CDRs, unlike Rule-based methods that only focus on the latter. Most of *SIMBox* fraud detection solutions leverage CDR-typed datasets through Machine Learning or *Complex Event Processing* (CEP). Machine Learning CDR-based solutions correspond to a *classification problem* where the entity to classify is either the *SIM card* or the *mobile device* generating traffic. A standard methodology is thus applied consisting of a *data preparation* step followed by *model building and evaluation*.

Data preparation includes feature selection and any form of data preprocessing. A CDRs dataset has several fields, some of which may not be meaningful for *SIMBox* fraud detection. Aggregating useful CDRs fields yield *detection features* to distinguish fraudulent from legitimate users in terms of call behavior (e.g., #outgoing calls, ratio of outgoing to incoming calls [140, 139], #called contacts, etc.), mobility (e.g., #visited cells [114], #calls with no displacement), network usage (e.g., ratio of #calls to #other services), or entity properties (e.g., #SIM cards per IMEI, account age [114, 86, 153]). Moreover, data preparation often includes sampling to reduce the input data's size to ensure a proper proportionality between fraudulent and non-fraudulent entities, leading to better results. In this vein, the proportionality of 66% normal cases versus 34% fraudulent cases is commonly adopted as in [140, 139, 114].

Model building and evaluation consists of training a machine learning classifier to capture users' communication behaviors from given features and accordingly categorize them as fraudulent or legitimate aiming the lowest error. Several models have been used in the literature for that purpose; [140], [86] and [153] perform a performance comparison of Artificial Neural Network (*ANN*) and Support Vector Machine (*SVM*) models. [86] and [153] also consider a Random Forest (*RF*) model in such a comparison. [114] presents another approach consisting of the linear combination of three models: a Random Forest (*RF*), a Functional Tree (FTree) [50], and an Alternating Decision Tree (ADTree) [71]. The final decision of the classification model is a linear combination of individual model decisions (0/1) according to weight coefficients found by minimizing the classification error in the training dataset. We also note approaches based on Fuzzy logic [102] and Complex Event Processing [158, 88].

3.3.4 Audio-based approaches

Audio records hold valuable information to obtain attributes such as the origin of a call and to perform analysis and profiling on packet loss and noise. Two research works used audio record

analysis to detect *SIMBox* fraud to the best of our knowledge. Reaves et al. [132] leveraged the fact that calls performed over the VoIP network suffer from audio degradation in terms of packet losses and jitters (as discussed in §2.1.2). Therefore, the authors try to detect calls with such degradations as an indication of a bypass over the VoIP network using a *SIMBox*. The system is designed for deployment at the base station level for the detection of ongoing fraudulent calls. This work is a refinement of the PindrOp system [22] that combats large telephony frauds through audio “fingerprints” built from noise characteristics and indicators of different codecs used by a call routing networks. Elrajubi et al. [46] proposed a voice-recognition-based approach to fraud detection. The solution is based on the fact that fraudulent SIMs are used to terminate traffic that may originate from several different callers to local numbers. Therefore, a SIM associated with a number of unique speakers beyond a given threshold is identified as fraudulent. Although the idea is promising, the system was not implemented due to privacy issues in telephone calls.

3.3.5 Signalling data-based approaches

The analysis of signaling data to detect *SIMBox* fraud has not yet been exploited in the literature. It was mentioned in a 2015 white paper [78] is described as with high potential. The authors in [78] argue that *SIMBox* components generate a specific set of signaling messages that constitute a fingerprint allowing for their distinction. These messages’ data and parameters can be analyzed in real-time. For instance, the *SIMBox* signature may be identified at the SIM card attachment to the network, preventing any use. This technology is, therefore, promising as it may stop fraud before any revenue is lost.

3.4 Fraud evolution

The *SIMBox* has evolved, both in terms of hardware and functionality. We try in this Section to build a chronological sequence of this evolution which is useful threefold: (1) it gives better visibility on the pace at which the *SIMBox* (and therefore, fraud) evolves, (2) it provides insights on the motivations for this evolution, which helps us guess how the fraud can further improve (3) it allows getting a global view of the potential of the *SIMBox* (and therefore, fraud) positioned in time, which can be opposed to the detection potential (detailed in Table 3.4).

Very little information is available on the evolution of *SIMBox* appliances. *We have been able to collect the data presented in Fig. 3.4 by reporting news about the addition or update of components on the websites of the leading SIMBox suppliers.* The Figure gathers the upgrades of four different manufacturers (*Hybertone*, *Dinstar*, *Ejoin*, and *Antrax*). Each line represents upgrades from one category (hardware or functional) provided by one manufacturer. The name and the category of the upgrades are indicated below the line. For the [Antrax: functional] line’s updates, the text is right-aligned for space reasons.

3.4. FRAUD EVOLUTION

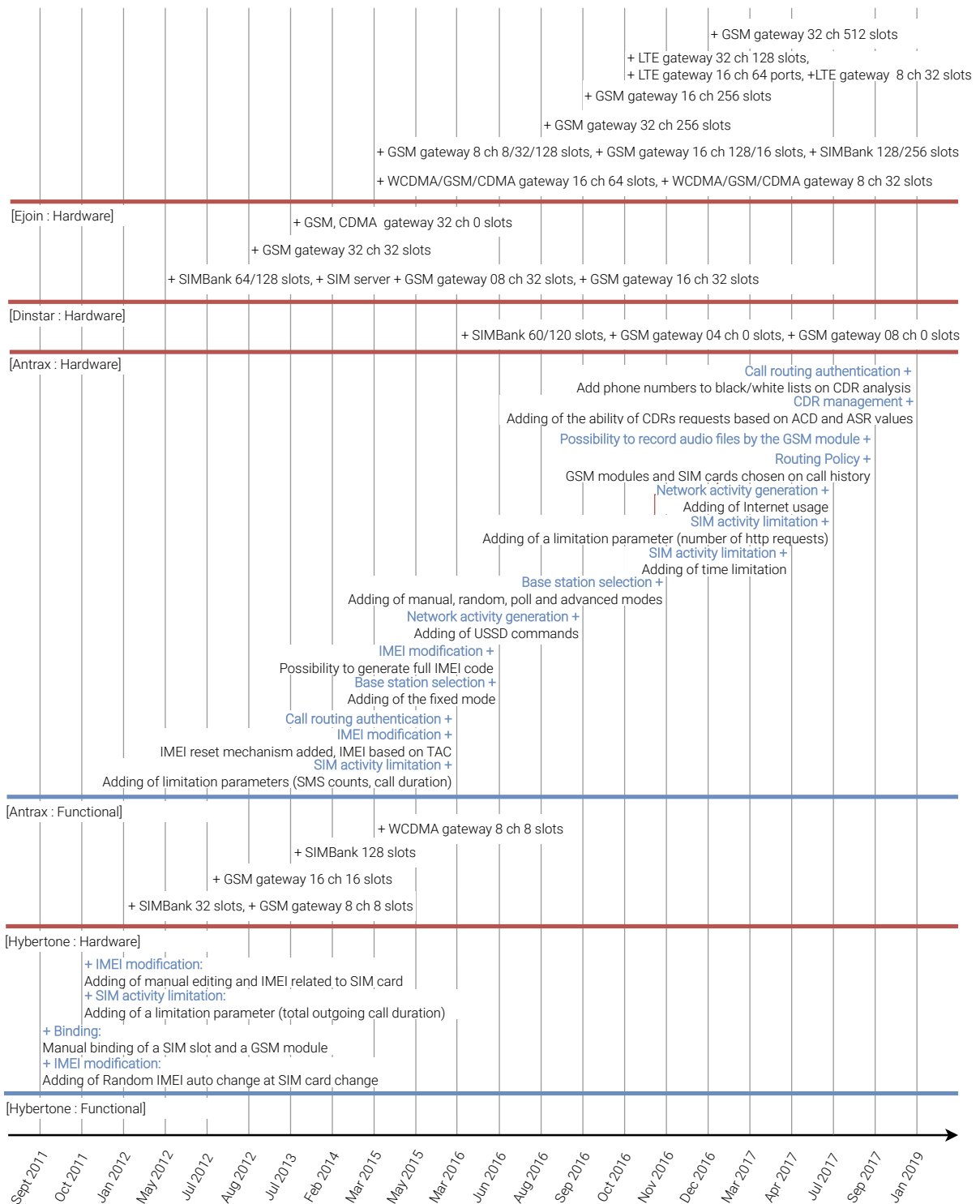


Figure 3.4: Timeline of the SIMBox evolution from material and functional points of view.

3.4.1 Hardware evolution

The SIMBank appears to be the first update for each supplier. Its first occurrence is in 2012 by Hybertone, with the capacity of only 32 SIM slots. Over time its size, i.e., the number of simultaneous SIM cards, evolved very quickly, to the peak of 256 SIM slots from 2015 by Ejoin. The presence of the SIMBank allows the deployment of distributed *SIMBox* architectures. *Therefore, since 2012, fraudsters can manage their gateways remotely and carry out simulated SIM card mobility using at least two gateways.*

On the other hand, gateways' evolution is seen in the number of modules and SIM slots and the supported cellular technologies. Similarly to SIMBank, the number of GSM modules evolves from the value eight by Hybertone in January 2012 to the peak of 32 in 2012 by Dinstar provider. *Therefore, since 2012, it is possible to terminate 32 calls simultaneously using a gateway.*

Over time gateways support new generations of cellular network technologies. In 2013 we had GSM and CDMA gateways, WCDMA in 2015, and LTE in 2016. The more cellular technologies a gateway supports, the more features it offers. For instance, GSM gateways cannot enable data services contrarily to CDMA and WCDMA gateways, and LTE gateways allow higher data rates. *We deduce that since 2013 with the providing of CDMA gateways by Dinstar, fraudsters can make usage of other mobile data services.* Hence manufacturers are providing gateways that support multiple cellular technologies (e.g., Dinstar and Ejoin).

3.4.2 Functional evolution

Information on functional evolution is more challenging to obtain. We were only able to collect them for two manufacturers: *Hybertone* and *Antrax*. Both providers make a point of *IMEI modification* and *SIM activity limitation*. Indeed, since 2011 both features are already supported by *Hybertone* devices. This is expected as the IMEI, if not changed, makes it easy to determine all SIM cards operating in a *SIMBox*' GSM module. Similarly, if the call traffic is not regulated and distributed to the different SIM cards of the architecture, the SIM cards will be easily identifiable. *Antrax* started its activity later in time (in 2015); it added in 2016 the *Call routing authentication* feature to register and block numbers used by operators for test calls and developed many other features above-mentioned. Furthermore, since 2017, the *Antrax SIMBox* model can record audio tracks of calls routed through the *SIMBox*. It represents a real intrusion because fraudsters can eavesdrop on bypassed calls without the call sender and recipient's permission.

3.4.3 Evolution pace

The evolution of the *SIMBox*, both from a hardware and functional point of view, is significant. We notice that during the period we were able to collect information from each provider, the updates are frequent. There is on average one update every six months within a provider, with a maximum of 2 updates per month (e.g., *Hybertone* from Sept 2011 to Oct 2011) and a minimum of one update per year (e.g., *Antrax* from Sep 2017 to Jan 2019). With a comparable

evolution rate, we assume that *SIMBox* nowadays (and therefore, fraud) supports many more features, more accurate than what is available in the literature (i.e., provider websites). For instance, one of the latest functional updates made by Antrax is the possibility to analyze CDRs generated by the *SIMBox*. It paves the way for a wide range of advanced [HBS](#) features based on current AI advances.

3.5 Summary

The *SIMBox* fraud is tricky as it involves economic, technical, and even character factors (people's mentality). Moreover, it evolves by adapting to existing detection solutions and is a real challenge. This chapter surveyed significant public sources, including the *SIMBox* manufacturer's community, to highlight the fraud schemes and various strategies and the scientific literature regarding fraud detection.

We, therefore, report the limitations of existing solutions clarifying why fraud continues to be rampant. First, we notice that CDR-based detection methods are restricted. They are based on prior detection knowledge provided by mobile operators, i.e., ground truth used to train machine learning models. *Such ground truth is unfortunately limited as coming from active detection methods that fraudsters know to delude.* This explains why most CDR-based detection solutions do not consider [HBS](#) features (yet existing long before, as shown in [Table 3.4](#)) but still achieve excellent detection accuracy. *Therefore, CDR-based solutions currently detect only fraudulent SIM cards with apparent fraudulent behaviors* (e.g., limited mobility, a large number of outgoing calls, etc.) Second, *Audio-based solutions are thorny and challenging to explore as they deal with private data.* Although they allow real-time detection, our survey reveals that fraudsters have access to call audio recordings and could modify them to avoid detection. Moreover, recent *SIMBox* appliances support various codecs, *which makes these approaches challenging to scale.* Third, although virtually unexplored, signaling data-based solutions promise *more efficient and accurate SIMBox fraud detection regardless of the strategy used.* This provides a great incentive to investigate solutions based on this data type.

In the next chapter, we leverage all information described on *SIMBox* architecture and fraud strategies to the implementation of a scalable simulator of *SIMBox* fraud in a realistic mobile network environment. We claim such a tool is key to research advances in this field for its ability to generate datasets valuable for detection investigation, whose access is currently curbed. We thus discuss its functioning and the potential it unleashes for future works.

FraudZen: cellular networks dataset generation

Contents

4.1	Overview: usage and flexibility	36
4.2	<i>FraudZen</i> Design	36
4.2.1	The <i>SimulationManager</i>	38
4.2.2	The <i>NetworkManager</i>	39
4.2.3	The <i>TrafficManager</i>	39
4.2.4	The <i>MobilityManager</i>	40
4.3	Comparison with state-of-the-art simulators	40
4.4	Summary	41

This chapter introduces the design of the *FraudZen* as a solution to tackle the scarcity of cellular network datasets required for *SIMBox* fraud mitigation (cf. §2.3.1). *FraudZen* reproduces the realistic cellular network architecture of a *SIMBox* fraud’s target area (the destination country in Fig. 3.1), and simulates the network usage and interactions of legitimate and *SIMBox* fraudulent users on top of this architecture. *FraudZen*’s resulting CDRs convey users’ communication behavior at individual fine-grained precision.

Researchers and mobile operators can use this tool to (i) inject fraudulent traffic to their CDRs and check the validity of their designed solutions, (ii) analyze the impact of the so-far-unreachable *SIMBox* ecosystem, i.e., *SIMBox* architecture and fraud parameters, (iii) reproduce and explore off-net fraud mechanisms, and (iv) design and investigate new fraud schemes. The full control and flexibility related to the simulation environment guarantee complete and large fraudulent CDRs ground truth for detection models’ training. Moreover, *FraudZen* allows anticipating the fraud evolution, freeing research from the past/current fraud capabilities and allowing the incorporation of not-yet-existing *SIMBox* functionalities in foresight.

Table 4.1: Literature’s *SIMBox* fraud detection

Id	Reference	Date	Datatype	#Total users	#Fraudulent users	Reported Avg. Accuracy
1	[140]	2013	CDRs	6415	2126	98.71%
2	[114]	2014	CDRs	93500	500	99.95%
3	[139]	2014	CDRs	6415	2126	98.8%
4	[132]	2015	Audio	Public Audio data corpus [51]		87%
5	[102]	2015	CDRs	Unspecified	0	No evaluation
6	[88]	2015	CDRs	2487556	40	99.99%
7	[4]	2016	CDRs	30198	19816	83.34%
8	[76]	2017	CDRs	Unspecified		No evaluation
9	[46]	2017	Audio	No test data available		No evaluation
10	[86]	2018	CDRs	25 million	5000	83.2%
11	[75]	2019	CDRs	720	20	99.9%
12	[87]	2019	CDRs	8745	50	99.3%
13	[158]	2020	CDRs	No test data available		No evaluation
14	[153]	2020	CDRs	20000	5000	95.55%

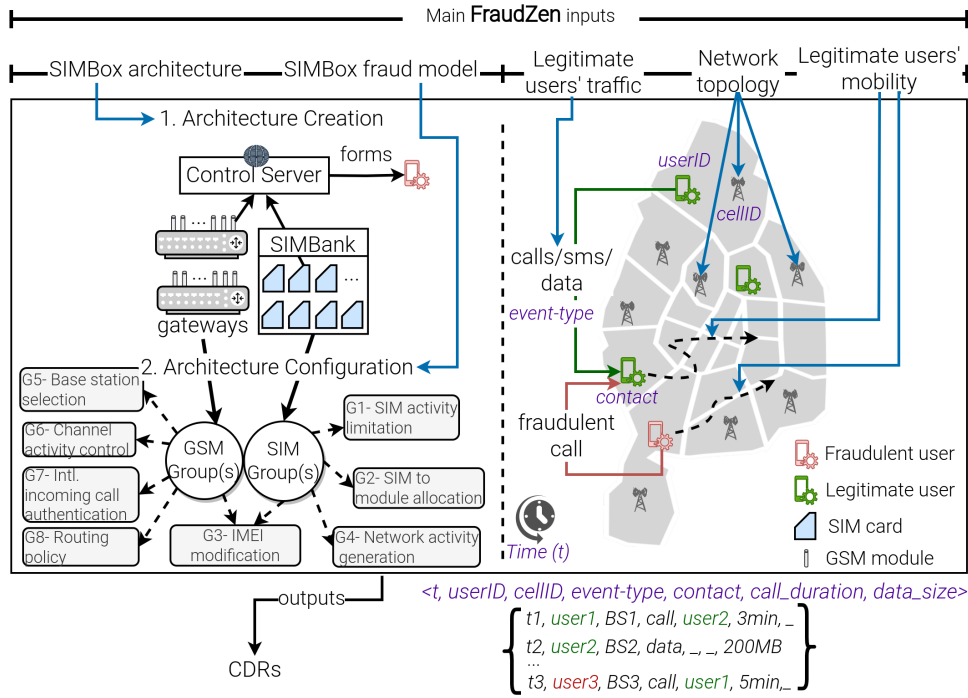


Figure 4.1: *FraudZen* pipeline: from *SIMBox* architecture implementation to ground-truth CDRs generation.

We will release *FraudZen*’s code and generated datasets for broad use in the research community.

In the following, we first give in §4.1 an overview of *FraudZen* discussing its practical usage. Then in §4.2 we present *FraudZen* design and components. We next discuss in §4.3 the related works and we summarize our findings in §4.4.

4.1 Overview: usage and flexibility

As depicted in Fig. 4.1, *FraudZen* intakes from a configuration file, the choices of legitimate users' traffic and mobility behaviors, the fraud model (i.e., policies) to be simulated, along with a set of scenario parameters (e.g., network topology, duration, number of operators). From these configurations, *FraudZen* outputs realistic CDRs of legitimate and fraudulent communication behaviors aiming to be used as ground-truth in *SIMBox* detection investigations.

We use experimentation as well as our in-depth survey of the fraud ecosystem reported in chapter 3 to bring high fidelity to our simulation. Precisely, the related insights on *SIMBox* functionalities are used to calibrate the simulator, which goes beyond experimentation's scalability and accessibility limits.

As to ensure high simulation performance, we build *FraudZen* to meet the following properties: (i) *flexibility* to generate multiple frauds, (ii) *modularity* to facilitate extension with new fraud functionalities, (iii) *efficiency* to generate, in a short time, CDRs covering a significant period, and (iv) *ease of use* to facilitate the configuration of simulation scenarios. Therefore, *FraudZen* has been written in C++, using the object-oriented paradigm as an event-driven simulator. Currently, the simulator comprises 90 classes, 247 files, and approximately 19,000 lines of code. In addition, it offers a configuration file of 122 parameters, allowing for the simulation countless frauds. Fig. 4.2 shows the UML (Unified Modeling Language) class diagram of the most important classes implemented, highlighting their most important methods and variables. Note that *SIMBox*-related classes are represented with a dashed border.

To ensure ease of use, running a simulation only needs filling in a user configuration file, whose parameters are provided in the appendix (cf. Fig. A.1). Although *FraudZen* configuration file has several parameters to provide great flexibility, default values allow a naive user to modify only the essential parameters, i.e., (i) legitimate users' mobility and (ii) traffic models (cf. Fig. A.2), (iii) *SIMBox* architecture (cf. Fig. A.2), and (iv) *SIMBox* strategy given by SIM and GSM groups creation and configuration (cf. Figs. A.3 and A.4). These parameters' value is set by a keyword referring to a model/class implemented in the simulator. For instance, the "trace-based" value for the parameter "regularTrafficStrategy" calls for the traffic strategy class that reads an external traffic file. Similarly, extending the simulator only needs inheriting existing classes and referencing the corresponding keywords in the configuration file.

4.2 *FraudZen* Design

FraudZen is constituted by four modules : the *SimulationManager*, the *NetworkManager*, the *TrafficManager*, the *MobilityManager*. Each module performs a key role in the simulation, as described in Table 4.2. While the *SimulationManager* and the *NetworkManager* each correspond to a class with a single instance, following the Singleton design pattern, *TrafficManager* and *MobilityManager* modules consist of a set of classes. We use the notations *Class::object* and *Class::function()* to indicate an *object* attribute and a *function()* defined into the *Class*.

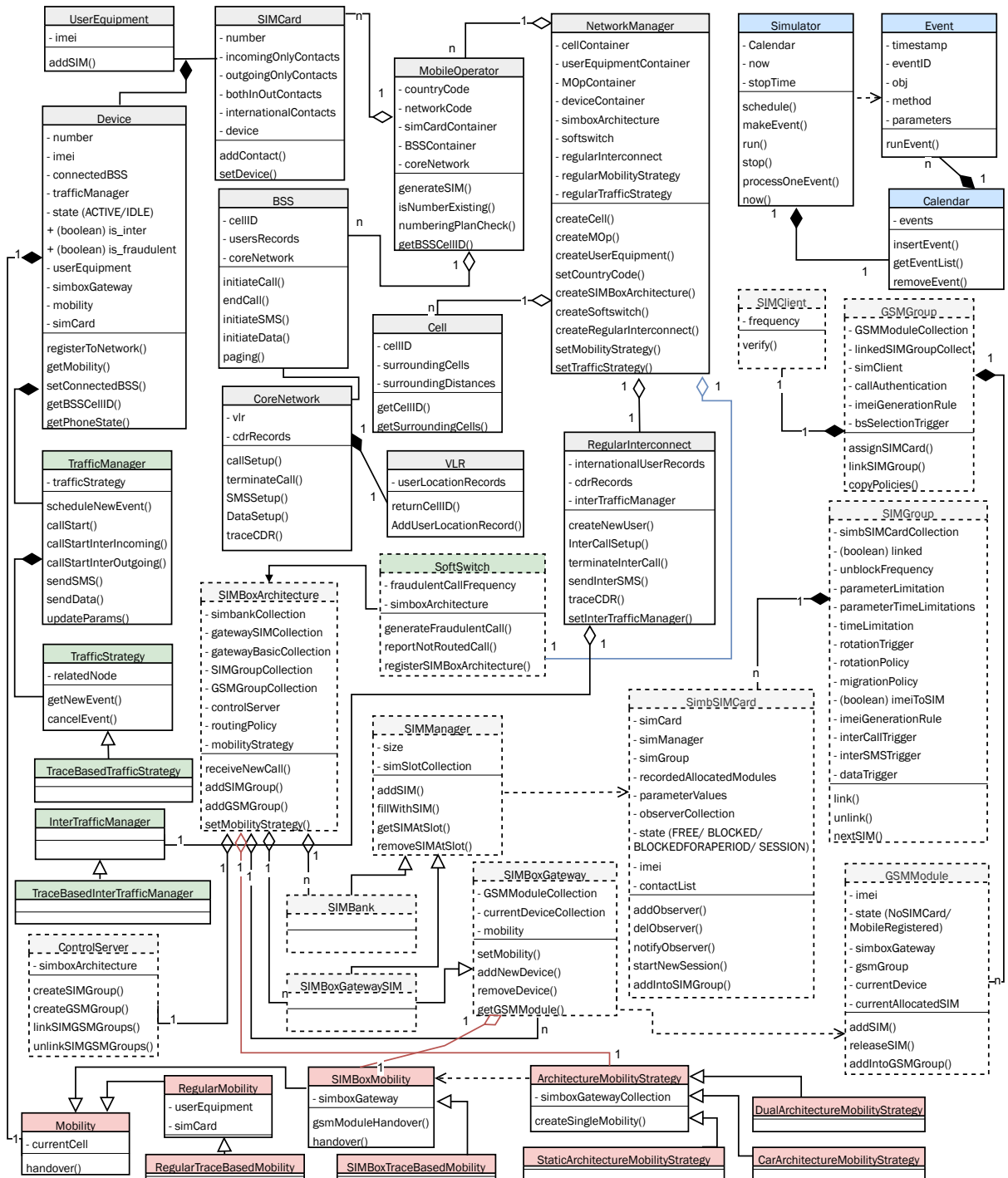


Figure 4.2: FraudZen simulator class diagram (better seen in color)

Table 4.2: *FraudZen* simulator modules and description

Module	Functions	Important methods/classes	Method description
<i>Simulation Manager</i>	- Creates/Handles/Ends an event - Manages simulation time	(method) schedule	Creates a new event and insert into the calendar
		(method) processOneEvent	Executes the earliest calendar event
		(method) run/ stop	Starts/ Ends the simulation
		(method) now	Gives the current simulation date and time
<i>Network Manager</i>	- Creates the network infrastructure and devices (Mobile Operators, Cells, UEs, <i>SIMBox</i> architecture, etc.)	(method) createSIMBoxArchitecture	Creates all equipment of a <i>SIMBox</i> architecture
		(method) setMobilityStrategy	Set legitimate users' mobility model
		(method) setTrafficStrategy	Set legitimate users' traffic generation model
<i>Traffic Manager</i>	- Handles regular and fraudulent traffic generation	(class) TrafficManager	Handle network events scheduling for each user
		(class) TrafficStrategy	Define legitimate users' traffic generation
		(class) InterTrafficManager	Handle legitimate intl. incoming traffic scheduling
		(class) SoftSwitch	Generate fraudulent intl. incoming traffic routed to the <i>SIMBox</i>
<i>Mobility Manager</i>	- Handles regular and fraudulent mobility	(class) RegularMobility	Handle mobility (i.e., handovers) scheduling for each legitimate user
		(class) ArchitectureMobilityStrategy	Define the mobility of the <i>SIMBox</i> architecture
		(class) SIMBoxMobility	Handle mobility (i.e., handovers) scheduling for each <i>SIMBox</i> gateway

A *FraudZen* simulation is done by reading the configuration file in the following steps. (i) First, *SimulationManager* and *NetworkManager* singleton objects are created. (ii) The *SimulationManager* configures the simulation duration and sets the stop time accordingly. (iii) The *NetworkManager* creates all network cells and simulation operators. (iv) *NetworkManager*'s `setMobilityStrategy()` and `setTrafficStrategy()` methods are used to define traffic and mobility models of legitimate users. Follows the creation of the *RegularInterconnect* object for incoming international traffic scheduling. (v) Then, the *NetworkManager* creates all User Equipment (UEs) and SIM cards to form regular devices. (vi) Next, the *NetworkManager* creates the *SIM-Box* architecture and sets its configurations and policies. Finally, *SimulationManager::run()* method launches the chronological execution of events scheduled in the calendar through the steps above. We hereafter, describe each *FraudZen* module.

4.2.1 The *SimulationManager*

FraudZen is event-driven. It chronologically executes timestamped events created by simulation objects throughout the simulation duration. The *SimulationManager::Calendar* sorts events in chronological order, according to their timestamps. *SimulationManager::Schedule()* adds a new event in the calendar and *SimulationManager::ProcessOneEvent()* executes the earliest event in the calendar. An event execution runs a function into a specific object (e.g., *mobility::handover()*) and can generate the scheduling of new events.

4.2.2 The *NetworkManager*

This module is responsible for creating the cellular network infrastructure, the user devices, and the fraud architecture (cf. Fig. 4.1), all described in the following.

Network infrastructure. The mobile cellular network, as designed in *FraudZen*, is multi-operator. Each operator provides its subscribers with communication services through voice, text messages, and mobile data to or from external networks (i.e., local or international operators). The network architecture deployed by each operator is based on the standards. It comprises two main sections: the Radio Access Network (RAN), and the core network. The RAN provides wireless access to mobile devices. It is constituted by a set of base stations, each deployed in a network cell; here, we make the realistic assumption that the RAN is shared by all operators who therefore have the same network topology. The function of each base station is to transmit service initiation requests to the core network and to perform paging, i.e., indicate the position of a device in its cell as well as its status (idle or active). The core network provides, in addition to network communication services, control operations, namely authentication and mobility management. Each operator's core network continually records in a file timestamped network service usage events yielding CDRs.

Network devices. A network device is formed by adding a SIM card to a user's cell phone. Such a partition between SIM cards and user equipments allows for distinguishing legitimate devices from virtual devices *SIMBox* created. Each legitimate device has a mobility component and a traffic component. The mobility component keeps up-to-date devices' connected base station by scheduling handovers, i.e., movements between the network cells, according to the chosen mobility model. Similarly, the traffic manager schedules each device's traffic generation according to the defined traffic model. Devices abroad (emitting or receiving international calls) have no mobility or operator; they generate traffic according to an input policy.

SIMBox architecture. From inputs such as the number of SIMBank, gateways, and SIM/GSM groups, *FraudZen* builds a *SIMBox* architecture and creates related configuration units (i.e., SIM and GSM groups). The *SIMBox* operates with SIM cards provided by the simulation operators, from which it forms *SIMBox* SIM cards (i.e., *SimbSIMCard*). Each *SimbSIMCard* has a state (e.g., Free/Blocked) and a set of parameters related to its traffic (e.g., call count, total call duration), allowing the control of its activity. Each SIM and GSM group works according to a set of functionality configurations given as the fraud strategy/model (cf. Fig. 4.1). Once the *SIMBox* architecture is formed and configured, it continually receives, with a fixed frequency, international traffic to be routed as local calls to legitimate users.

4.2.3 The *TrafficManager*

This module handles traffic generation for legitimate and fraudulent devices. For legitimate devices, traffic events are repeatedly generated according to the input traffic model. Each traffic event has the attributes: timestamp, event type (call, international call, SMS, or data), metric (i.e., call duration or data size), and contact if applicable. *FraudZen* currently includes

a trace-based traffic model, reading traffic events from an input file. For legitimate users, the *TrafficManager::scheduleNewEvent()* method repeatedly requests the next traffic event generation. This is done by calling the *TrafficStrategy::getNewEvent()* recursive method, returning a traffic event with the attributes timestamp, event type (call, international call, SMS, or data), metric (i.e., call duration or data size), and contact in case of a call. The *TrafficStrategy* class implements the legitimate users' traffic generation model and can be inherited to define new algorithms. The current version of *FraudZen* simulator includes a trace-based *TrafficStrategy*. Based on the returned event type, legitimate devices transmit a call/SMS/data service request to their connected base station. Fraudulent devices make use of these same requests to generate traffic; however, this is coordinated by *SIMBox* architecture's network activity generation and routing policies.

4.2.4 The *MobilityManager*

This module handles legitimate and fraudulent devices (i.e., users) cell-granularity displacements during the simulation. Legitimate users have a mobility attribute implementing the input specified mobility model. On the other hand, the mobility of a fraudulent device matches the movements of its belonging gateway. Such movements are governed by a strategy defined at the level of the whole *SIMBox* architecture. As this can be easily extended, *FraudZen* currently includes mobility models/strategies for both legitimate and fraudulent users based on existing mobility traces.

4.3 Comparison with state-of-the-art simulators

Fraud simulations are mandatory to conduct research in domains where datasets are intrinsically private and hard to get, such as cellular networks. However, despite a large number of available cellular network simulators, none is intended for cellular fraud simulation.

As part of the development and standardization of 4G(LTE/LTE-A) and 5G networks, several open-source mobile network simulators have been proposed in the literature to test and optimize algorithms and procedures. The objective of these tools is to evaluate network performance either at the radio link level [104, 77, 61, 111, 91, 127] or the network application level ([128, 159, 23, 117, 126, 83]). In the former, these simulators model the PHY or MAC protocol layers with a high level of fidelity to measure physical layer quantities, such as signal-to-interference-to-noise ratio (SINR) or spectral efficiency as a function of physical layer designs. Evaluations are typically performed in an individual cell, with one or many UEs potentially moving around a base station. In the latter, simulations are instead aimed at the performance of application-level metrics (e.g., end-to-end delay, user transaction throughput, packet loss rate, etc.) based on upper-layer designs (e.g., an admission control scheme or a radio scheduling algorithm). These simulators provide more network features and include models of application logic, Layer 4, Layer 3, and Layer 2 protocols, and network equipment running these protocols.

The test scenarios are based on a network layout with multiple cells, mobile UEs, and traffic generators.

Our *FraudZen* simulator differs from the above-mentioned in that it does not aim at testing the network's performance but allows to obtain realistic spatio-temporal characterizations of the network usage that can be leveraged for many use cases, especially *SIMBox* fraud investigations. For instance, most simulators employ user mobility and network traffic as load generators. Therefore, they use non-realistic models such as random direction or random walk for mobility and constant bit rate for traffic. Conversely, our simulator is not designed to represent detailed transmissions between UEs and the network through the implementation of layered protocol stacks. *FraudZen* abstracts these aspects to reproduce network users' behavior when generating traffic on the top of these layers.

4.4 Summary

In this chapter, we identified and discussed limitations related to real-world CDRs exploitation and their impact fraud *SIMBox* fraud investigations. To fill this gap, we proposed a simulation framework, i.e., *FraudZen*, designed for realistic CDRs self-generation by the research community. We believe *FraudZen* is indispensable for research in this field, where raw datasets are intrinsically private. *FraudZen* simulator surpasses this fundamental need by enabling the advancement of fraud detection capabilities so far restricted to past operators' detection automation. Through fraud anticipation and results reproducibility, mobile operators and researchers have within their grasp the capability to investigate the whole fraud ecosystem and get relevant insights for long-term fraud mitigation.

We conduct two-fold *FraudZen* validation in the next chapters:

- On the one hand, we need to validate *FraudZen* ability to generate realistic *legitimate* CDRs. As shown in Fig. 4.1, *FraudZen* legitimate users' communication behaviors highly depend on the input mobility and traffic models, which can be trace-based. We have adopted this design to allow mobile operators to replay their CDRs traces in the simulator while injecting only fraudulent traffic. Accordingly, in the next chapter, we present traffic and mobility input models to *FraudZen* that experimenters with no CDRs may use. And we validate their ability to generate realistic, legitimate CDRs by comparison with real-world CDRs.
- On the other hand, validating *FraudZen* fraud generation does not fit with the classical approach of comparing *FraudZen* generated *fraudulent* CDRs to real-world ones to prove their "*realisticness*." Indeed, this would demand real-world fraudulent CDRs with multiple fraud behaviors *without the reach of mobile operators due to their limited detection*. Besides, it would not guarantee *FraudZen* capability to advance fraud-related research with novel fraud models. *Faced with this, we instead want to validate the ability of FraudZen to generate efficient frauds*. We pursue this objective in chapter 6. Although seemingly simple, this task requires defining frauds meaningfully, raising the question: *what is the intent of SIMBox fraud? And how to measure fraud effectiveness?*

Legitimate communication modeling

Contents

5.1	<i>Zen</i> Overview	44
5.1.1	Architecture	44
5.1.2	Real-world reference datasets	45
5.1.3	<i>Zen</i> CDRs attributes	45
5.2	Traffic module	47
5.2.1	Event-type modeling	48
5.2.2	Inter-event time modeling	48
5.2.3	Correspondent modeling	49
5.2.4	Metric modeling	50
5.3	Mobility module	51
5.3.1	Mobility generator	51
5.3.2	Topology builder	53
5.3.3	Position-to-cellId module	53
5.4	Social ties module	53
5.5	CDRs generation inside <i>FraudZen</i>	54
5.6	Evaluations	55
5.6.1	Traffic module	55
5.6.2	Mobility module	58
5.6.3	<i>Zen</i> CDRs use cases	59
5.7	Related works	61
5.8	Summary	62

As the previous chapter introduces, the ability for self-realistic CDRs generation is our proposed solution to the challenging access to real-world CDRs for research. First, a high-fidelity reproduction of *SIMBox* appliances' functionalities allows the generation of realistic *fraudulent CDRs*. However, producing realistic, *legitimate CDRs* is a more complex task reflecting the hard-to-predict trends of human communication behavior as captured in CDRs.

From another point of view, "*legitimate CDRs*", which we will refer to as "CDRs" throughout this chapter, offer a wide range of possible applications beyond *SIMBox* fraud research (cf. §2.3.1). Accordingly, to ensure such broad applicability and reliably reproduce real-world CDRs, we should conform to essential attributes, namely, *completeness*, *realisticness*, *fine-grained description*, and *privacy*. Unfortunately, those attributes make the generation of realistic CDRs challenging and complex (cf. §5.1.3).

This chapter presents *Zen*, the first-of-the-literature modeling framework for the generation of realistic, legitimate Charging Data Records (CDRs) datasets that fulfills the above-mentioned attributes. First we give an overview in §5.1, then discuss *Zen*'s components from §5.2 to §5.5. In §5.6, we validate *Zen* CDRs ability of reproducing daily cellular behaviors of the urban population and its usefulness in practical networking applications such as dynamic population tracing, Radio Access Network's power savings, and *SIMBox* fraud as compared to real-world CDRs. At last we discuss the related works and summarize our findings.

5.1 *Zen* Overview

In the following, we provide an overview of *Zen* architecture and describe the different real-world datasets we leverage. We then elaborate on the requirements generated CDRs should meet to ensure broad applicability and reliably reproduce real-world CDRs and discuss how *Zen*'s generated CDRs meet such requirements.

5.1.1 Architecture

Mobile traffic generation involves synthesizing timestamped datasets (from x_0 to x_T) only from a given context taken as a parameter, which is much complex traffic prediction, i.e., estimating the next data value at time T based on records from $t = 0$ to $T - 1$. Hence, a generative framework should be expressive enough to fully learn from provided datasets as a training phase, infer the inherent data distributions, and produce new datasets with identical distributions, i.e., realistic.

According to an input context, *Zen* generates realistic CDRs through four phases, each implemented in a module of its architecture (cf. Fig. 5.1). *Zen* architecture consists of (1) a *traffic module*, (2) a *mobility module*; (3) a *social-ties module*, and (4) a *CDR-combiner* module.

The *traffic module* (§5.2) leverages *Long-Short-Term Memory neural networks (LSTM)* jointly with statistical analysis to model users' traffic behavior from real-world CDRs. It provides answers to *what*, *when*, with *whom*, and *how* to generate events. The *mobility module* (§5.3) (i) emulates users temporal displacements on a real-world geographical map over a selected

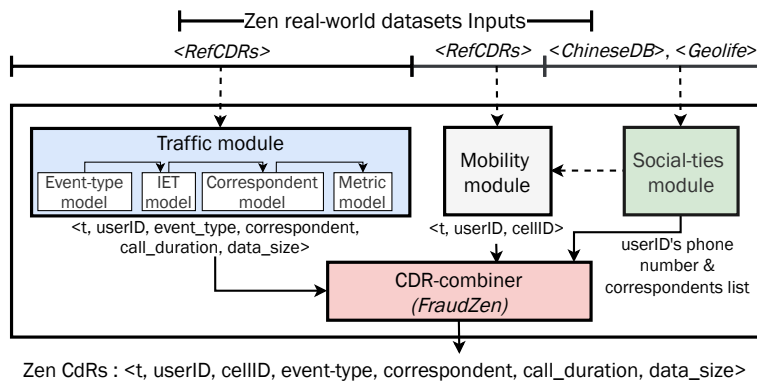


Figure 5.1: Zen architecture.

Table 5.1: Review of CDRs completeness

	Mobility features	Traffic features		
		Call	SMS	data
[113]	x	✓	x	x
[149]	x	✓	x	x
[72]	x	✓	x	x
[109]	x	x	x	✓
[32]	✓	x	x	x
[79]	✓	x	x	x
[167]	✓	x	x	x
[95]	✓	x	x	x
Zen	✓	✓	✓	✓

period, and (ii) associates corresponding users positions with a real-world cellular topology. This dataset feeds the *social-ties module* (§5.4) that builds the network social structure on top of which users’ communication interactions occur by building users’ phonebooks, i.e., list of phone numbers a user is likely to contact. Finally, all the previous modules’ outputs are provided as input to the *FraudZen* simulation framework combining them to produce realistic CDRs per network operator over a specified duration and particular urban area (§5.5).

5.1.2 Real-world reference datasets

Zen models real-world datasets to produce realistic outputs. In particular, as depicted on top of Fig. 5.1, *Zen* uses three real-world reference datasets described in what follows.

RefCDRs are used by both the *traffic* and the *social-ties* modules. *RefCDRs* refer to a fully-anonymized CDRs dataset collected by a major mobile network operator in Africa. They describe 1-month (*from 2018-06-01 to 2018-06-30*) per-user traffic resulting in about 3 million timestamped events generated by 186,738 distinct phone numbers, where about 17,000 are from the *RefCDRs*’ operator. *RefCDRs* are incomplete; they lack mobility features and incoming-SMS traffic type (i.e., only have outgoing SMS). Still, there is no information on the size of sessions in the data traffic type. *RefCDRs* provide each user’s operator network code. We leverage this information to identify the list of operators appearing in the datasets.

On the other hand, the *mobility module* leverages the *ChineseDB* [6] and *Geolife* [166] datasets, by extracting statistics of real-life mobility behavior of users. *ChineseDB* (non-public and fully anonymized mobility CDRs) contains trajectories of 642K users during two weeks. In particular, we did not have access to *ChineseDB* but only to related statistics available in [6]. *Geolife* (public and anonymized GPS dataset) contains trajectories of 182 users during 64 months.

5.1.3 Zen CDRs attributes

We present hereafter the positioning of *Zen* generated CDRs with respect to our goals:

Completeness: Complete CDRs comprise mobility and traffic features and should, thus, include, in addition to user positions (i.e., network cell Ids), all event types, namely data, call, and SMS. Achieving CDRs completeness thus requires (i) either real-world complete CDRs

datasets (hard to obtain) describing mobility, traffic, and pairwise users communications or (ii) to cope with the difficulty in modeling the intrinsic correlations between information describing users' behaviors in space, time, and social communication. Here, the limited access to complete real-world CDRs hardens the modeling and reproduction of complete CDRs. *Zen* circumvents this limitation and provides complete CDRs by jointly modeling individual CDRs features to capture the implicit correlations between them: e.g., the choice of *whom* to communicate with is generally time (*when*) and event (*what*) dependent. Hence, Table 5.1 shows *Zen* yields complete CDRs compared to most state-of-the-art contributions instead providing only one CDRs feature, either mobility or an event type.

Realisticness: CDRs directly reflect the collecting network topology (*users' cell-tower locations*) and organization (*operators*). Hence, there is a strong dependency between operators' CDRs and their network architecture, which has to be captured to produce realistic CDRs. Achieving CDRs' *realisticness* thus implies considering real-world cellular network complexities (architecture and topology) at all levels of the generation process. Related to that, *Zen* modeling integrates a real telecom network topology (*inducing users' cell-tower locations*) as opposed to a biased theoretical one (with identical hexagonal-shaped cells). In addition, *Zen* considers a realistic network organization in multi-operators allowing to capture inter-operator interaction's patterns. valuable for *SIMBox* fraud investigation for instance [93].

Fine-grained description: This relates to the realistic reproduction of the individual users behaviors in terms of mobility and traffic, beyond the global behavior of the population. While mobility modeling and reproduction is well covered in literature, individuals' cellular traffic reproduction still lacks detailed investigations. In particular, daily individuals' cellular traffic presents a notable heterogeneity that challenges its reproductions. As an illustration, Fig. 5.2 (left) shows a daily traffic (i.e., sequence of events per user) of 100 randomly selected users from a real-world CDRs. We can see a great diversity of users regarding events generation. For instance, while some users make predominantly local calls, others make only data; some do not make international calls, and others make it frequently. Statistical approaches (see Fig. 5.2 (center)), as commonly used in the state-of-the-art [92, 149, 109], are limited in reproducing such traffic dynamics as they do not allow per-user modeling but per-user profile (i.e., group of users with similar behavior). Improving this result, the approach we use in *Zen* better captures such individuals heterogeneity (see Fig. 5.2 (right)).

Privacy compliance: Generated traces should be *privacy-compliant* to avoid backtracking real users' identities, most often done through their mobility information. Here, *Zen* leverages *refCDRs* with no geographical information associated with traffic events. From such CDRs, *Zen* uniquely captures and reproduces individuals' traffic behavior in time, which can be then associated with any modeling of individuals' daily urban mobility. In *Zen*, mobility behavior is emulated as realistically as possible. Such disjoint modeling hides real individuals' spatiotemporal daily-life habits in routine and leisure times (e.g., home/work, nightlife), bringing the privacy-preserving capability to the produced CDRs.

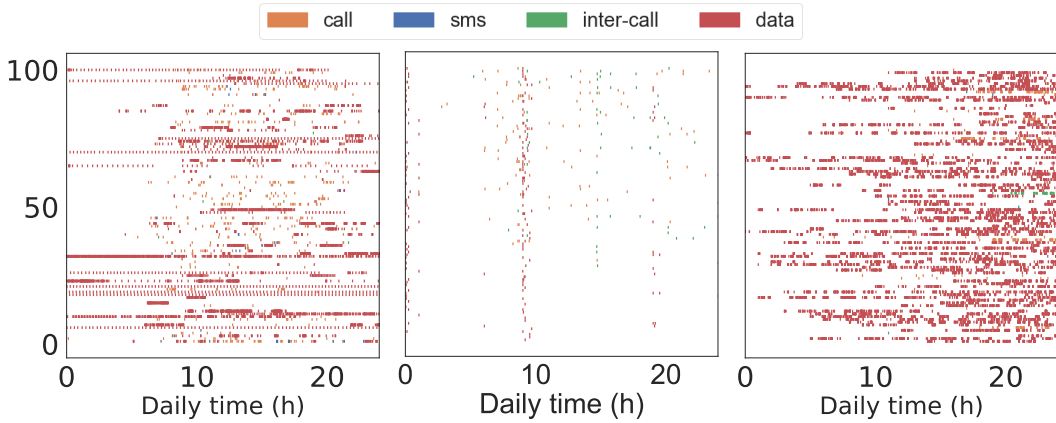


Figure 5.2: Temporal event sequences of 100 users for: (left) a real-world, (center) a statistically-generated and (right) the *Zen*-generated CDRs.

5.2 Traffic module

We describe here the generative modeling used to reproduce CDRs traffic behavior. Our generative model has enough expressive power to capture inter-CDRs feature correlations while considering individual users' behavior. In particular, we leverage an enhanced *recurrent neural network* (RNN), named *Long-Short-Term Memory* (LSTM), known for its ability to generate complex, realistic long-range sequences [70].

Our model is trained from *RefCDRs* which report a set of timestamped events generated by several users. Each CDRs' event (or a line) includes the following information: start time, user id (i.e., phone number), event-type (i.e., data, SMS, call), corresponding user id (for calls and SMS), call duration (for calls only), and data volume (for data only).

We organize *RefCDRs* by user: the set of events chronologically generated by the user u throughout the trace forms a sequence of events $(e_1^u, e_2^u, e_3^u, \dots, e_{N_u}^u)$ of size N_u , which is the model basis. Hence, data reproduction is done in a sequential order, i.e., from time step 1 to N_u . The generation of an event in a sequence is a four-stage process, where each stage relies on the previous output.

Stage 1: at step t , we predict the next event-type e_{t+1}^u a user will perform, using the *event-type model* (cf. §5.2.1).

Stage 2: given the event-type, the *inter-event time (IET) model* generates the IET value used to deduce the starting time for the predicted event-type e_{t+1}^u (cf. §5.2.2).

Stage 3: the *correspondent model* predicts which of its correspondent a user will interact with for the next event e_{t+1}^u (§5.2.3). This model is executed only if e_{t+1}^u is a call or SMS, i.e., the only events requiring correspondent interactions.

Stage 4: Finally, the *metric model* refers to how the events are generated: For call events, it generates its duration, while for data events, it produces the data volume (§5.2.4). Note that the temporal information is not constant throughout the pipeline. From stages 1 to 2, we use the temporal information of the event-type at step t to predict the one of the event-type at

step $t + 1$, then used in stage 3.

5.2.1 Event-type modeling

The *event-type model* predicts the next event-type a user will generate from four types of events: data, local calls (uniquely outgoing), international calls (outgoing or incoming), and local SMS (uniquely outgoing). Local incoming calls and SMS are modeled here as they are induced from outgoing calls and SMS during the generation. Modeling international calls separately from local calls, rather than having a unique "call" event-type and determining probabilistically if it is local or international, allows distinguishing different user behaviors towards international calls. As shown in Fig. 5.2, some users may not make international calls while others make them frequently. Finally, we did not model international SMS event-type because it is rare and not present in *RefCDRs*.

The event-type model. We model sequences of event-types using an **LSTM**. At step t , the **LSTM** takes as input a vector of features x_t and generates a vector of four scores, $y_t = (y_t^1, y_t^2, y_t^3, y_t^4)$. These scores parameterize a multinomial distribution $Pr(\hat{e}_t^u | y_t)$ for the next event-type \hat{e}_{t+1}^u , through a softmax function: $Pr(\hat{e}_t^u | y_t) = \frac{\exp(y_t^k)}{\sum_{k'=1}^4 \exp(y_t^{k'})}$.

When training, the true previous event-types at step t are encoded as input for the next step. Network parameters' training is done according to the standard approach of minimizing the negative-log-likelihood of the training data. We compute the gradient of this loss with respect to our network parameters through backpropagation.

Features x_t . At step t , we distinguish four features for predicting e_{t+1}^u : the event-type at step t (one-hot encoded) and its temporal features, i.e., Day-of-Week (**DOW**, one-hot encoded), Hour-of-Day (**HOD**, one-hot encoded), and Second-of-Day (**SOD**, cyclical encoded). A one-hot encoding represents the i th of N features using a N -sized vector of all zeros, except for the i th element, which is set to 1. A cyclical encoding maps a continuous inherently-cyclical feature into two dimensions using a sine and cosine transformation. The **HOD** and **DOW** features capture the seasonality and regularity of mobile traffic (less activity at night and during weekends [30]). The fine-grained encoding of time as **SOD** is used to capture the very short temporal difference between consecutive events (e.g., tens of seconds for data events).

5.2.2 Inter-event time modeling

The *IET model* returns the possible time values between a sequence's events with a confidence interval. It works in two steps: first, we use an **LSTM** to parameterize a multinomial distribution over a discrete set of time bins. Then, we use statistical methods to sample a continuous value inside a predicted time bin. In the following, we present our considerations for discrete IET estimation, then the detail of our **LSTM** network, and finally, our methodology for sampling an IET value given an IET bin.

Discrete IET estimation. IET are divided into discrete bins, b_1, \dots, b_J , representing J consecutive intervals of time. To determine the bin boundaries, [97] recommends setting boundaries

at evenly-spaced quantiles of time in training data. We found that, in our case, such a setting results in tiny intervals for the smallest values of IET due to the IET’s heavy-tailed distribution. For instance, considering the 4-quantiles, there are as many elements in $[1s - 20s[$ as in $[20s - 72s[$. A division at the 20s could distort the model’s accuracy while being acceptable for realistic CDRs. Thus, we chose the IET bins empirically to make the model less complex and easier to train without increasing the reconstruction error in mapping back to continuous values. We, therefore, divide IET into three intervals: $[0s - 30min]$, $]30min - 24h]$, and $> 24h$.

The IET LSTM model. The LSTM network takes at each step, t , as input a feature vector, x_t and generates as output a vector of scores y_t , with one score for each possible IET bin. As with the *event-type model*, these scores are used as logits in a softmax to get a multinomial distribution over the time bins. To train the network parameters, we minimize the negative-log-likelihood of the training data.

Features x_t . At each step t , we consider as features, the temporal information of e_t^u (§5.2.1) as well as the predicted event-type e_{t+1}^u , one-hot encoded.

Continuous estimation. Generating CDRs traffic requires knowing the precise starting time of the next event of the sequence, which is used for further predictions. Therefore, we convert the predicted discretized IET bins to real-values. We apply to each IET bin the KS statistic test to estimate the distribution and related parameters best fitting the corresponding empirical distribution in *RefCDRs*. Table 5.2 shows the fitted distributions to sample an IET value per bin. The model returns the median value and the confidence interval of the values obtained after n sampling (by default $n = 1$).

5.2.3 Correspondent modeling

The *correspondent model* applies only for event-types requiring interaction with a correspondent (i.e., SMS and local or international calls). We first define the notion of *friendship degree* (fd), intuitively capturing the friendship strength of a user with each of its correspondents. Let u be a user, with $\#c_u$ correspondents over the considered period, we then call $\#e_c^u$ the number of events the user u had with his correspondent c . We increasingly order the correspondents of u according to their corresponding number of events such that $\#e_1^u \leq \#e_2^u \leq \dots \leq \#e_j^u \leq \dots \leq \#e_{\#c_u}^u$. The *friendship degree* of the correspondent c of u is the rank j of c in this order. Hence, at step t , the *correspondent model* returns a predicted *friendship degree* \widehat{fd}_t^u for the correspondent with whom the event e_t^u is done.

Correspondent LSTM model. The *correspondent model* is also a LSTM network that takes as input at step t , a feature vector x_t per user. It generates as output the predicted *friendship degree* \widehat{fd}_t^u . The network parameters training minimizes the Mean Absolute Error (MAE) of the training data.

Features x_t . At step t , the features are: the temporal information of e_t^u (cf. §5.2.1) except the SOD, the one-hot encoded event-type e_t^u , and the number of correspondent of u , $\#c_u$. This

Table 5.2: IET distribution and parameters per bin

IET bin	Distrib.	Parameters
[0s – 30min]	Lognormal	$\sigma = 1.798$ $\mu = 4.04$ $x_0 = 0.99$
]30min – 24h]	Lognormal	$\sigma = 1.731$ $\mu = 8.59$ $x_0 = 1749.08$
> 24h	Exponential	$\lambda = 6.21e - 6$ $x_0 = 86401$

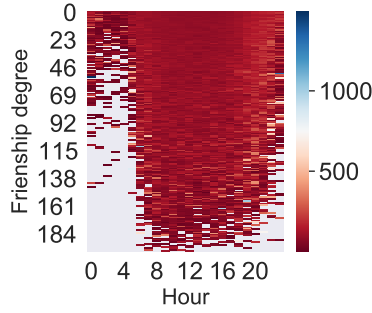
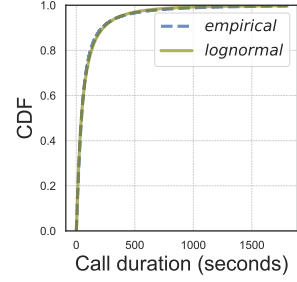


Figure 5.3: Avg call duration (s).

Figure 5.4: Call duration CDF for *RefCDRs*.

later is constant throughout a user sequence and is essential to help the model captures that $\widehat{fd}_t^u \leq \#c_u$. Accordingly, it is not encoded and is left to its actual value.

5.2.4 Metric modeling

This section presents the models used to generate the metrics (i.e., a model per metric) associated with events generation, namely the call duration and the data volume.

Call duration We use a statistical method to model the call duration. In fact, contrary to the previously modeled parameters, we found no explicit feature dependency or variability (and therefore, no complexity) regarding call durations, which implies that a used RNN could hardly train. Precisely, Fig. 5.3 shows a minor variation of the average call duration per hour and per friendship degree over the entire dataset. We can see that overall, call duration does not vary much, and thus, there is no particular correlation between these parameters. Moreover, the per-user behavior regarding call duration (easily assessed through the average call duration per user) closely depends on the number of calls each user makes over the CDRs duration, which is opportunely already captured by the *IET model*. Accordingly, the *call duration model* corresponds to the estimation of the parameters of the continuous distribution that best fits the empirical distribution of call duration, as shown in Fig. 5.4. Applying the Kolmogorov–Smirnov statistical test, we found this distribution to be Lognormal of parameters $\sigma = 1.29$, $\mu = 3.78$, $x_0 = -0.47$.

Data volume. The *data volume model* returns a data volume value for each data event. According to 3GPP standards, each data-typed CDRs line corresponds to the generation of a data session by a user. Unfortunately, as *RefCDRs* lack this information, we rely on the study done in [109] to design the *data volume model*. To the best of our knowledge, [109] is the only work that conducts a thorough characterization of data volume usage per session and per user over time extracted from real-world CDRs, as well as designs a generator of realistic CDRs that conforms to these characterizations.

Oliveira et al. ([109]) profiled users’ data usage over time according to their generated amount of data (*volume profile*, i.e., Light, Medium, or Heavy) and to how often they generate data sessions (*frequency profile*, i.e., Occasional or Frequent). Besides, it extracted from real-world CDRs the distributions of data session volume according to a user’s profile and the day period

(peak or off-peak hours) and the percentage of users per profile. We use such percentages to first assign a *volume profile* to each user in *Zen*. As the *frequency profile* could be inconsistent with the frequency of data event-type as predicted by the *event-type model*, we attribute to each user, in *Zen* the *Occasional frequency profile*. In fact, the distribution of the number of data sessions per day and user from *RefCDRs* shows the majority of the population to be of this latter profile. Finally, we sample from the distributions found in [109] to get a data session volume.

5.3 Mobility module

The *Zen's mobility module* produces realistic CDRs mobility traces in three steps each covered by a sub-module. The *mobility-generator* (§5.3.1) emulates a population urban mobility in a real-world city map, with users displacements generated according to public sources [123] and describing city planning and transportation information [81]. Next, from the input city map, the *topology-builder* (§5.3.2) builds a realistic cellular topology using cell towers' positioning of mobile operators deployed in the considered real-world city, gotten from OpenCellID [122]. This topology is then used in the *position-to-cellId module* (§5.3.3) to map the mobility traces produced by the *mobility-generator* to the cell granularity.

5.3.1 Mobility generator

The *mobility-generator* inherits the highly configurable capability of the *Opportunistic Network Environment* (ONE) [89] simulator. Specifically, it enhances the *Working Day Mobility* model (WDM) [45] of ONE into a model named *En-WDM*, and generates CDRs of format `<Timestamp, userId, lat, lon>`.

Our motivation to use WDM as a foundation is twofold. First, contrary to similar models [141, 161], WDM originality comes from the combination of various mobility aspects present in people daily life (e.g., home and workplaces, day periods). Second, WDM closely reproduces wireless interactions (i.e., inter-contact and contact time) distributions found in two real-world measurement experiments (i.e., iMote and Dartmouth), asserting modeling generality.

Nevertheless, WDM is limited in capturing some fine-grained real mobility habits or fine-tuning. *En-WDM* tackles such limitations and strengthens the model with additional literature's intuitions on laws dictating human mobility behavior, such as preferential attachment, regular daily behavior, transportation-dependent shortest-path preferences, and most importantly, uncertainty (i.e., novelty-seeking behaviors) and heterogeneity. Specifically:

- *Inherited functionalities*: *En-WDM* models week working days' movements into three activities and their transitions, i.e., "home", "working", and "night activity". The night activity corresponds to leisure-related times spent in preferred spots of friends groups.
- *Exploration profiling*: Users in *En-WDM* simulation decide in a probabilistic-way whether to go home or to a night activity. To setup such probabilities, we rely on the exploration

phenomenon profiling conducted in [6] and define three mobility profiles: *scouters* are more inclined to explore and discover new places to visit, *routiners* rarely explore and prefer to stay among their familiar and few known places, and *regulars* constantly alternate between exploration and routine. We then accordingly classify users given by the *ChineseDB* dataset [6] in these three profiles. Results describe a population with 20.27% of *scouters*, 54.75% of *regulars*, and 24.98% of *routiners*. After this classification, we assign to users in each profile, a probability indicative of their propensity to go for a "night activity": 0.8 for *scouters*, 0.5 for *regulars*, and 0.2 for *routiners*.

- *Clusters and popularity*: Rather than considering home/office locations' (lat, lon) coordinates, *En-WDM* associates each location coordinate to the center of a cluster of rectangular shape and configurable size. A user is first assigned a home/office cluster and then, chooses her exact home/office location randomly inside the cluster. Moreover, we added the notion of *cluster popularity*, which represents the probability for a user to choose a given cluster as a home/office cluster or, in the case of night activity spots, the probability of going to this location for her evening activity.
- *Distance-based profiling*: *En-WDM* enables the definition of cities' artificial communes or districts (hereafter, areas) to replicate the real world. Accordingly, we associate each user to one of the three profiles representing area displacements: *Profile1* inside a single area, *Profile2* among two areas, and *Profile3* in the whole map. To get the population percentage to be considered in each profile, we profile *Geolife's* users resulting in: *Profile1* including 72% of users whose maximum distance is less than 1/3 of the maximum observed distance D_{max} ($\approx 2.49 \times 10^3 km$). *Profile2* with 19% of users with a maximum distance between 1/3 and 2/3 of D_{max} , and *Profile3* including 9% of users with a maximum distance greater than 2/3 of D_{max} .
- *Simple parameterization*: We report all the key configuration parameters needed for *En-WDM* simulation. Table 5.3 summarizes them. We use italic style for those we used the default value and regular one for those we modified. We fixed all temporal parameters, i.e., *workDayLength*, *officeMinWaitTime*, *officeMaxWaitTime*, *minAfterShoppingStopTime* to be close to real-world scenario. The parameters for which minimum and maximum values are set are uniformly random sampled in the interval unless another distribution is mentioned (e.g., the office waiting time follows a Pareto distribution). Parameters in bold (*homeRange* and *officeRange*) are those we added for clusters implementation. In particular, the ratio between the *worldSize*, *officeSize*, and cluster sizes as well as the *ProbOwnCar* parameter may vary depending on the simulated city. These parameters values in Table 5.3 are adapted for a simulation in the city of Helsinki.

Table 5.3: Description and settings of parameters for *En-WDM* simulation.

<i>En-WDM</i> Parameter	Description	Used value	Default
<i>workDayLength</i>	length of time spent at work each day	28800s = 8h	28800s = 8h
<i>officeWaitTimeParetoCoeff</i>	coefficient of the Pareto distribution giving users' pause time inside the office	0.5	0.5
<i>officeMinWaitTime</i>	minimum value for users' pause time inside the office	3600s = 1h	10s
<i>officeMaxWaitTime</i>	maximum value for users' pause time inside the office	28800s = 8h	Inf
<i>officeSize</i>	size of the office squared-shaped side	50	40
<i>minGroupSize</i>	minimum size of a friends group for evening activities	1	1
<i>maxGroupSize</i>	maximum size of a friends group for evening activities	5	3
<i>minAfterShoppingStopTime</i>	minimum value for evening activities duration	3600s = 1h	3600s = 1h
<i>maxAfterShoppingStopTime</i>	maximum value for evening activities duration	14400s = 4h	7200s = 2h
<i>walkingSpeed</i>	(minimum, maximum) value of speed when walking	(0.8, 1.4) m/s	(0.8, 1.4) m/s
<i>probOwnCar</i>	probability for a user to own a car	0.19	0.5
<i>busSpeed, carSpeed</i>	(minimum, maximum) value of speed by car or bus	(7, 10) m/s	(7, 10) m/s
<i>busWaitTime</i>	(minimum, maximum) of bus wait time at a stop	(10, 30) s	(10, 30) s
<i>worldSize</i>	(width, height) in meters of the simulation area	(10000, 8000)	(10000, 8000)
homeRange	(width, height) in meters of a home cluster	(50, 30)	N/A
officeRange	(width, height) in meters of an office cluster	(1000, 900)	N/A

5.3.2 Topology builder

The *topology-builder* uses the geographical positions of base stations (BS) in the emulated area, as given by *OpenCellId* [122], and performs a Voronoi tessellation. The tessellation produces a cellular network topology with heterogeneous cell sizes close to reality, containing each input BS. Each Voronoi cell defines the communication boundaries of an input BS. For generality and simplicity reasons, we include all operators' base stations given by *OpenCellId* in a bigger architecture to derive the Voronoi topology. This unique topology is assigned to all operators considered in *Zen*'s process. In practice, sharing BSs between different operators is commonly done for cost savings.

5.3.3 Position-to-cellId module

The *position-to-cellId* module assembles the modeled users' mobility and the designed Voronoi cellular topology. For this, each user's geographical position given by the *mobility-generator* traces is mapped to the corresponding *OpenCellId*'s BS identifier, i.e., *cellID*, in the Voronoi topology. It outputs mobility CDRs in the format <Timestamp, userID, cellID> describing users' spatiotemporal daily mobility in a real city map and adapted to a real network topology. Despite the realism given by such leveraged real-world information, the generation of users' mobility has a realistic and not a real nature since no ground-truth information on users' real-life routine is available. This brings privacy benefits to *Zen* CDRs.

5.4 Social ties module

Zen CDRs generation lays on the *social-ties* module providing the network social structure. This structure yields phone numbers from users of the mobility CDRs and builds the network social graph by creating per user's phonebook, i.e., list of correspondents.

Mobility users to phone numbers. From the number of network's operators and the users distribution per operator (taken as parameter or induced from *OpenCellId*[122]), the *social-ties* module assigns an operator per user and generates a phone number in the format <MCC><MNC>

<5 random digits>, where **MCC** and **MNC** describe the mobile code for country and the operator network code within the country, respectively.

Network social graph. Reproducing the social graph of users' interactions implies answering the following three questions.

(Q1) how many correspondents does each user have? To answer this question, the *social-ties* module relies on the distribution of correspondents per user from *RefCDRs*. Let $u \in U$ be a user with $\#c_u$ correspondents; we consider the non-parametric distribution $P_{\#c} = P(\#c_u = \#c) \forall \#c \in [1, MAX]$. Thus, for each generated user u' , its number of correspondents $\#c_{u'}$ is obtained with the multinomial distribution of parameters $P_{\#c}$.

We then define four disjoint categories of correspondents: international correspondents (c_{inter}), outgoing local correspondents (c_{out}), incoming local correspondents (c_{in}), and both outgoing and incoming local correspondents (c_{both}). Thus, $\forall u \in U$, $\#c_u = \#c_{inter,u} + \#c_{out,u} + \#c_{in,u} + \#c_{both,u} = (x_{inter,u} + x_{out,u} + x_{in,u} + x_{both,u}) \times \#c_u$. We export the average values $\overline{x_{cat,u}} \forall cat \in \{inter, out, in, both\}$. Then, we use the multinomial distribution of $P = \overline{x_{cat,u}}$ to induce the number of correspondents, in each category, of each user.

(Q2) how do we choose these correspondents? We create user phonebooks by implementing a variant of the configuration model algorithm [162], which allows building a graph from given users degrees. We apply this algorithm by correspondents' category so that each user is an c_{in} correspondent of its c_{out} correspondents and a c_{both} of its c_{both} correspondents. Moreover, we add a heuristic to choose users' correspondents based on their relationship type, (i.e., neighbors, colleagues, or friends) extracted from the generated mobility dataset (cf. §5.3) as follows. users located inside the same home/work cluster between *1am to 4am* and *10am to 2pm*, over the whole dataset duration, are considered neighbors and colleagues, respectively. As well, users in the same group for night activities, when they occur, are considered friends. Hence, a user's correspondents are selected according to defined probabilities (taken as parameters) from its list of neighbors, colleagues, friends, and other users until we reach the fixed number of the user's correspondents.

At last, the *social-ties* module outputs each user's list of correspondents organized in the categories c_{out} , c_{both} , and c_{inter} , while c_{in} category is induced from the c_{out} one.

(Q3) how does a user interact with all of its correspondents? While (Q1) and (Q2) are tackled by the *social-ties module*, question (Q3) is addressed through the *correspondent model* of the *traffic module* detailed in section 5.2.3.

5.5 CDRs generation inside *FraudZen*

FraudZen integrates all modules' outputs to produce realistic CDRs, as follows. First, the simulation is initialized with network users creation. Each user includes its list of correspondents per category as indicated by the *social-ties* module.

Using *event-type* and *IET* models from the *traffic module*, *FraudZen* generates timestamped

sequences of events over the total considered duration. For each call/SMS event-type, the *correspondent* model indicates the correspondent to reach for the event processing. In particular for calls events, the call duration metric relates only to available correspondents of users. We do not consider unavailable users' correspondents (i.e., already in an ongoing communication) at the caller-callee association. Hence, for available correspondents, a call duration value is sampled from the *call duration* model distribution. As well, for data events, the data volume metric is assigned according to the *data volume* model.

Following, *FraudZen* integrates at each event-type generation the spatial information, i.e., corresponding users' cell Ids at the corresponding timestamp (resulting from the *mobility module*). Users' network event generation are recorded per network operator resulting in complete and realistic CDRs traces in the format specified in Table 2.1.

5.6 Evaluations

This section confirms *Zen*'s validity by evaluating traffic and mobility modeling separately, then their merging into CDRs.

5.6.1 Traffic module

Hereafter, we evaluate the accuracy and the performance of predictions resulting from the *traffic module*'s stages. As there is no similar contribution in the literature, we compare *Zen*'s models to designed baseline predictors. Table 5.4 summarizes all comparison metrics and provides their distributions on the right of each evaluation result.

5.6.1.1 Experimental datasets

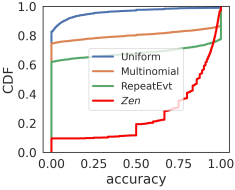
We train and evaluate our models on *RefCDRs* after some data handling. First, we only consider events of *users subscribed* to the operator network collecting *RefCDRs*. Then, we filter out users having less than 3 generated events in the whole period of 4 weeks and those with more than one event at the same timestamp. Those manipulations result in the selection of nearly 6000 users totalizing 1,782,829 events or CDRs entries, i.e., 77.8% of the *RefCDRs*' initial size. We then use as *training set* the first two weeks of the dataset, the 3rd week as *validation set*, and the 4th week as the *test set*. Because our traffic predictions are user-based, the non-filtered remaining users compose all the three previous sets and only their event sequences varies according to the week considered in each set.

5.6.1.2 Models training and Hyper-parameters

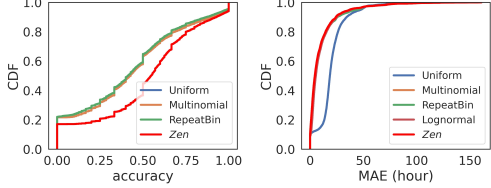
We used a 2-layer *LSTM* with 50 hidden units per layer for the *event-type model* and 100 hidden units per layer for the two other models. To avoid over-fitting the training dataset, we used a dropout regularization with $p = 0.2$. The *LSTM* losses are iteratively minimized using mini-batch gradient descent with the Adam optimizer. Each mini-batch contains 64 sequences of events (i.e., users). We chose event sequences' lengths of 302 for training, 157 for validation,

Table 5.4: Traffic LSTM models evaluation results.

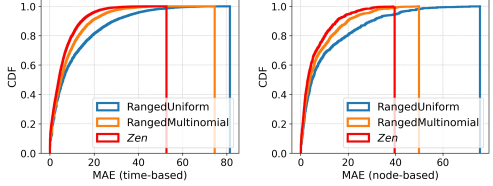
Event-type model		
Predictor type	NLL	Accur.
Uniform	0.27	2.91%
Multinomial	0.21	38.97
RepeatEvt	N/A	43.27
Zen	0.037	91.82



IET model						
Predictor type	NLL	Accur.	MAE			MAE
			[0, 30 min] (82.8%)]30min, 24h] (15.45%)	>24h (1.75%)	
Uniform	0.215	64.56	1097	1033	1120	2319
Multinomial	0.165	64.56	231	68	334	2877
RepeatBin	N/A	58.05	239	73	347	2871
Lognormal	N/A	N/A	249	78	361	2973
Zen	0.118	69.25	185	16	295	2904



Contact model								
Predictor type	MAE (time-based)				MAE (user-based)			
	All	[1,6]]6,21]	>21	All	[1,6] (50%)]6,21] (30%)	>21 (20%)
Ranged-Uniform	25.12	1.17	5.04	29.57	26.38	1.08	4.53	31.17
Ranged-Multinomial	15.78	0.91	3.87	18.42	17.28	0.81	3.41	20.38
Zen	11.81	0.65	3.02	13.77	13.23	0.63	2.57	15.68



159 for test, sampled from the distribution of the number of events generated by users in each experimental set. Therefore, we pad all sequences to the sequence length in each experimental set to homogenize datasets and ease the training. We use a masking layer to tag added values in each sequence to ignore them in the loss calculation. Besides, we fixed a gradient clip value of 0.01 to avoid "exploding gradients" prone to affect RNN.

5.6.1.3 Event-type model

We compare our *event-type model*'s predictions (cf. §5.2.1) to the ones of the following baselines: *Uniform* – each event-type is equally likely to occur at each time step; *Multinomial* – each event-type probability is given by its empirical count in training data; *RepeatEvt* – the next event-type is always predicted to be the same as the previous one. We use the following evaluation metrics: (*NLL*) Negative-log-likelihood of next-step probabilities, and (*Accuracy*) next-step 1-best correct classification rate (for this metric, the traditional Multinomial approach always output the most frequent event-type). Results are presented in Table 5.4. Selecting event-type according to *Multinomial* is significantly more predictive than the *Uniform*, but worse than *RepeatEvt*. Our *Zen*'s *event-type model* works the best. For both *NLL* and *Accuracy*, *Zen* is much better than *RepeatEvt*, i.e., the most probable event-type is not always the prior one.

5.6.1.4 IET model

As before, we compare the acuteness of our model in predicting the next IET Bin (cf. §5.2.2) with the corresponding above-defined baselines. Table 5.4 shows that for both metrics, *NLL*

and Accuracy, the performance of *Zen's IET model* is much higher than *RepeatBin* (that simply repeats the previous IET Bin), followed by the Uniform and the *Multinomial* baselines. Disregarding the prediction approach, we compute the discretized probabilities of IET Bins and map them to IET values in a continuous domain: named *Bin sampling* mapping. To evaluate how efficient *Zen's* and baselines' *Bin sampling* are, we compare them to the *Overall sampling* mapping, both described next.

- *Bin sampling*: At each Bin, the IET value is obtained after averaging $n = 500$ samplings of the corresponding continuous IET distribution (see §5.2.2). We apply this approach to all the previously Bin-based models, i.e., *Zen's IET model*, Uniform, Multinomial, and RepeatBin predictors.
- *Overall sampling*: We perform a fitting of the empirical IET distribution (i.e., with no bins) and obtain a Lognormal distribution with $\sigma = 2.67, \mu = 4.97, x_0 = 1$. Then, we straightly predict continuous values by sampling the resulted fitted IET distribution. We name this prediction *Lognormal*.

The Mean Absolute Error (MAE) of the IETs in minutes is used as the comparison metric. It estimates the average distance between actual and predicted IET. From Table 5.4, we can notice that the *Bin-sampling* of *Multinomial* and *RepeatBin* have comparable MAE performances, followed by the *Overall-sampling Lognormal* predictor. This behavior is also verified per Bin (three last columns). Overall, *Zen* works the best. In the first bin $]0, 30min]$, which is the most sensitive, we note that except for the *Zen*, all models on average predict an IET value outside the initial interval.

5.6.1.5 Correspondent model

At last, we evaluate the *correspondent model* (cf. §5.2.3) by comparing its predictions to the following baselines:

- *RangedUniform*: Per user u , correspondents $c_i, \forall i = 1, 2, \dots, \#c_u$ are equally likely to be predicted at each sequence step.
- *RangedMultinomial*: Per user u , each correspondent c_i is chosen with a probability ($p_i^u, 1 \leq i \leq \#c_u$) extracted from the procedure as follows:

Let U be the set of users and u a user in U . We recall that $\#e_{c_i}^u$ refers to the number of events u made with his correspondent c_i . From this definition, we derive $P_{c_i}^u$ the proportion of events made by u with its correspondent c_i : $P_{c_i}^u = \#e_{c_i}^u / \sum_i \#e_{c_i}^u$.

For all $i = 1, 2, \dots, MAX(\#c_u)$ we extract the mean values $\overline{P_{c_i}} = \overline{P_{c_i}^u} \forall u \in U$. Hence, for a user u , the probabilities ($p_i^u, i = 1, 2, \dots, \#c_u$) is obtained by normalizing the first $\#c_u$ mean values ($\overline{P_{c_i}}, i = 1, 2, \dots, \#c_u$) such that $\sum_i p_i^u = 1$.

The evaluation metric is the MAE of the predictions \widehat{fd}_t in the test dataset. We found that as we train the *correspondent model* with chronologically-separated experimental windows (defined

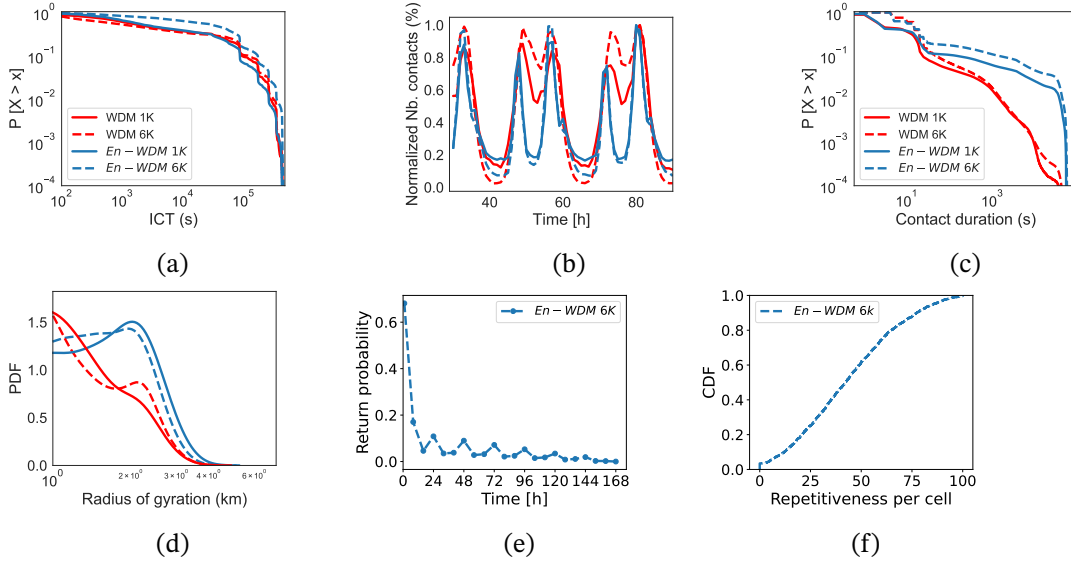


Figure 5.5: Mobility metrics compared with initial WDM: (a) Inter-contact time CCDF (b) Normalized number of contacts per hour (c) Contact duration CCDF (d) Radius of gyration CDF (e) Return probability (f) Per-cell repetitiveness CDF

in §5.6.1.1), the MAE loss value continually increases in the validation dataset. This is due to the fact that in the training period (i.e., first two weeks), users only interact with some of their correspondents, making it difficult for the model to generalize. To fix this issue, we instead split training, validation, and test datasets by selecting users traffic over the whole dataset period (4 weeks). The training dataset includes 60% of the users, while the validation and test datasets each represent 20%. Results in Table 5.4 show the *RangedMultinomial* predictor has significantly better results compared to the *RangedUniform* predictor.

Overall, *Zen* is the modeling that best performs, showing its ability to capture users interaction with their correspondents. In particular, the detailed distribution plots show *Zen* presents for 80% of users (i) more than 95% and 75% of accuracy for respectively, the event-type and IET models, and (ii) less than 6.68% and 12.5% of MAE maximum values for respectively, the IET and correspondent models.

5.6.2 Mobility module

We validate our *En-WDM* mobility model by comparing it to its original version, the WDM [45]. We rely on WDM results closely following real-world measurement datasets distributions (i.e., iMote [142] or Dartmouth [148]). Since *En-WDM* adds new functionalities in modeling mobility to WDM, we are not looking for identical results from both models but for similarities in terms of distributions and curve behaviors.

Fig. 5.5 shows well-known metrics for characterization of wireless networking meetings (inter-contact and contact time) and the tendencies in human mobility, i.e., confinement (radius of gyration) and repetitiveness (probability to return to previously visited places). As for WDM, we emulate a scenario with 1000 and 6000 users, moving in the Helsinki city center

area with roughly 7×8.5 km for 5.10^5 s and with the same arrangement of home/work and POIs. We use the same representation of results for comparison reasons.

We can see that *En-WDM*'s inter-contact time distribution (cf. Fig. 5.5a) closely follows the ones of WDM, attesting the realistic modeling of such metric at population scale and the capability of reproducing heterogeneity to mobility decisions. The number of contacts per hour (Fig. 5.5b) follows the same cyclical trend. However, *En-WDM*'s off-peak periods are more downward, as a larger percentage of the population (routiners and regulars) do little activity at night. Interestingly, realistic mobility profiling of users adds heterogeneity to mobility decisions and consequently conducts to real-life daily repetitiveness and temporal regularities as well as to better opportunities for opportunistic data exchanges (Fig. 5.5c). At last, we evaluate the capability of the two models in reproducing seminal literature analytical human mobility laws [62, 6, 110]. The radius of gyration (Fig. 5.5d) estimates the area size mostly covered by daily displacements of a user. In *En-WDM*, the radius of gyration is globally smaller due to routiners and regulars (79.73% of the population) who have more confined displacements, consistent with real-life mobility behavior [6]. Moreover, the average return probability (Fig. 5.5e) and per-cell repetitiveness (Fig. 5.5f) results show that users have a regular and periodical spatial mobility behavior with a higher probability of returning to a previous small set of visited locations, as shown in [62, 110].

5.6.3 Zen CDRs use cases

We evaluate the complete CDRs resulting from *Zen* framework as compared to *RefCDRs* when applied to three use cases. As *RefCDRs* lack ground-truth in mobility information, we enrich them with *Zen* CDRs' emulated user trajectories as described in ref. §5.5; we name it *M-RefCDRs*. Based on the confirmed *Zen* performance in reproducing human mobility laws, we focus our use-cases analysis on the reproduction of cellular traffic behavior for which we have a ground-truth. We generate *Zen* CDRs with 6000 users, corresponding to the same number of users in *RefCDRs* (see §5.6.1.1) and consider a week-long period.

Dynamic urban tracking. Real-time population density tracking is a key functionality to support adaptive urban and transport planning. As shown in [90], such density at time t can be derived from the corresponding network activity load at t computed as the mean number of network events (here ongoing calls, exchanged SMS, and established data sessions) per individual. Following this methodology, Fig. 5.6 shows the spatial distribution (values in the color bar) of people presence in network cells of an Helsinki area (2.2 km \times 3.6 km), at four representative time hours of individuals' routine, obtained with *M-RefCDRs* and *Zen* CDRs. As in *M-RefCDRs*, we see that people presence at the office period (8h-12h) is concentrated in specific zones corresponding to defined Helsinki business neighborhoods. In contrast, the after-work period (18h-22h) includes displacements times and night activities not made at specific spots (e.g., groups of users can walk down the streets for their night activity), explaining people presence is spread over a broader zone. Besides, we notice that people presence is captured equivalently in *M-RefCDRs* and *Zen*'s CDRs, especially in working period (8h-12h).

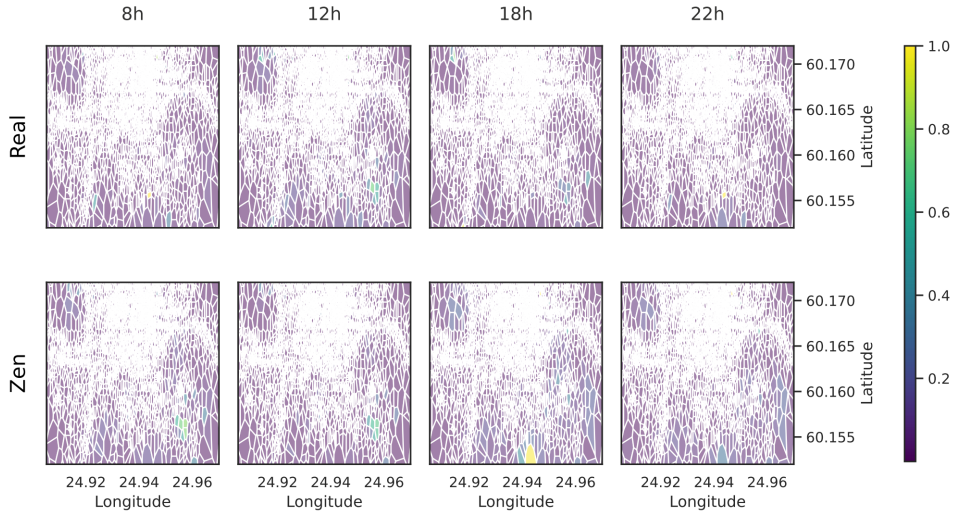


Figure 5.6: Dynamic people presence estimated at four daily time in Helsinki for real-world and *Zen* traffic.

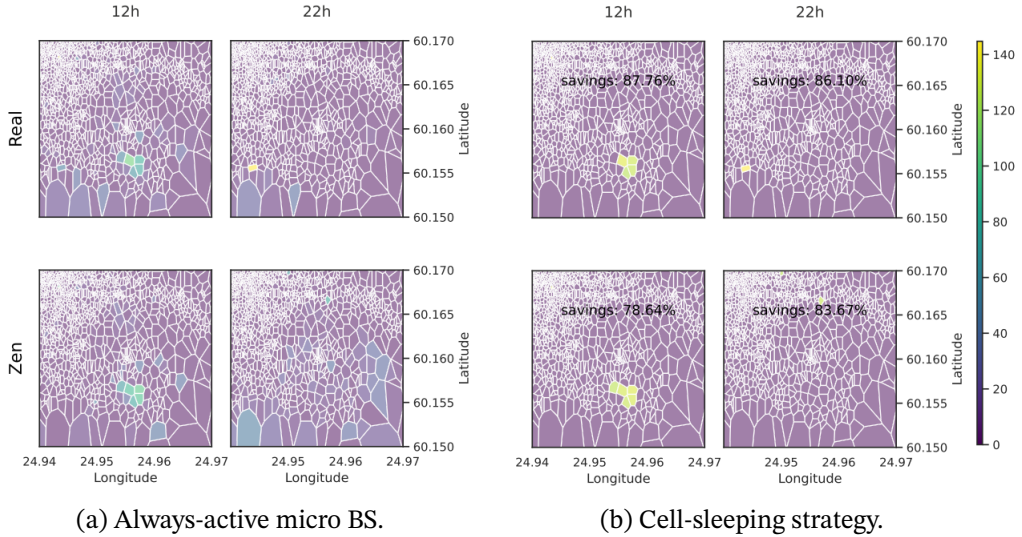


Figure 5.7: Power consumption per cell (a) for always-active micro BS and (b) with a cell-sleeping strategy.

We believe the resulting few dissimilarities, particularly for the after-work period (18h-22h), are mainly due to the non-deterministic association of user's traffic to trajectories in *Zen*.

Data-Driven Micro BS Sleeping. Numerous works studied power savings in Radio Access Networks (RAN). Inspired by [164], we investigate how a traffic-aware Base Station (BS) on/off-switching strategy [157] performs when informed with *Zen* CDRs compared to *M-RefCDRs*. We assume an heterogeneous RAN deployment where each cell is served by a separate micro BS, whereas macro BSs provide umbrella coverage to a larger area. Specifically, we consider a grid tessellation of 5X5 macro BSs in the considered zone. The power needed to the operation of a BS at time t is $P(t) = N_{trx}(P_0 + \Delta_p P_{max} \rho(t))$, $0 \leq \rho(t) \leq 1$, where $\rho(t)$ is the relative traffic load at time t with P_0, N_{trx}, P_{max} and Δ_p being constants defined for micro and macro BSs in [164]. Then, if $\rho(t) \leq \rho_{min} = 0.37$ as considered in [39] the micro BS offloads its local traffic

to the macro BS and goes into sleep mode, where it consumes negligible power. Accordingly, Fig. 5.7 shows the power consumption ($P(t)$ values in the color bar) of each cell’s micro BS at two hours in Helsinki (a zoomed-in area of $2.2\text{km} \times 1.6\text{km}$) with and without such a strategy implemented. We can see that comparable cells are kept on, while the strategy brings similar energy savings.

Anomaly detection. Beyond global population-related applications, the fine-grained state of *Zen* CDRs allows for the investigation of per-user spatiotemporal behavior for cellular anomaly detection. Such anomalies can be unusual events possibly generated by some security incidents (e.g., stolen account, malware device infection) [52] or users with a fraudulent behavior profile. As an instance of the latter, we assess the utility of *Zen* CDRs for investigating *SIM-Box* fraud by applying a user profiling method where traffic or mobility users’ behaviors are leveraged to classify a user as fraudulent or not. To this end, we apply for both *Zen* and real ones, a DBSCAN clustering to a set of per-user traffic-related features specific to detect *SIM-Box* fraudulent behavior as described in Table 1 of [139]. Results show a similarity between *Zen* CDRs and real-world ones: while *M-RefCDRs*’ estimated number of clusters and outliers are 10 and 1241, *Zen* CDRs’ confidence intervals for these metrics are 9.1 ± 1.66 and 1122.3 ± 35.02 for 10 samples of *Zen* CDRs’ call duration feature (ref. §5.2.4).

5.7 Related works

CDRs’ inaccessibility has pushed researchers to generate their own synthetically, commonly using features modeling. This leads to either mobility- or traffic-specific CDRs, often with grouped-based analysis of individuals’ behavior. *Zen* tackles such lacks by empowering the scientific community with the autonomy needed for the generation of realistic, complete, precise, and flexible CDRs.

Traffic-related: Instead of aggregated network traffic generation as done in [100, 164, 163], we focus here on per-individual CDRs generation that tackles different challenges. In this domain, literature’s synthetic CDRs lack completeness in describing both call [113, 149, 72] and mobile data [109] usages, and to the best of our knowledge, pay no attention to SMS usage. Murtić et al. [113] used Social Network Analysis to reproduce call behaviors’ features (i.e., temporal likelihood of calls and call duration distribution) per user profile, extracted from real-world CDRs. Nevertheless, the work did not include any validation. In the same vein, Songailaitė et al. [149] statistically model key parameters from real CDRs to produce realistic CDRs. Calling behaviors is simulated based on the empirical fitting of call duration, call count, call likelihood per hour, and weekdays similarity in behaviors. However, simulation relies on a simplistic and randomly-built network social structure leveraging static parameters such as the maximum number of friends and acquaintances. Using a *GAN* generative model, Hughes et al. [72] show the deep learning models’ capability to learn inherent and complex distributions from real CDRs. Unfortunately, real and generated CDRs included only two features: the starting call hour and duration in minutes, revealing a limited extent of modeled features compared to

complete CDRs. Finally, Oliveira et al. [109] focused on the data-traffic profiling, modeling, and generation from real CDRs. Their model allows generating data usage's timestamped records per profiled user. Although providing flexible settings for profiles' granularity, this work also has the drawback of modeling only data traffic features, lacking thus real-world CDRs' completeness.

Mobility-related: Synthetically generated mobility traces are regular in literature and frequently extracted from models implemented in ONE [89], BonnMotion [20], or SUMO [101] realistic simulators. Several works on mobility modeling actually focus on the generation of synthetic traces that capture specific features in human mobility that are often domain-specific: e.g., MANETS and DTNs (e.g., inter-contact and contact time) [141, 112], Disaster Management [124, 21] or Sociology [28]. Still, a few works such as [45, 64, 125, 85] aim to model real-life mobility and propose more complex models, valuable for more applications. This paper leverages the [45]'s originality in combining various mobility aspects and realistically modeling them. Other strategies rely on recurrent neural networks [95] or statistical generative models based on real mobility traces such as Markov models [32], spatiotemporal empirical distributions [79] or travel demand [167]. Yet, only a few works [105, 65] address the privacy issues of generated mobility traces, which is however crucial.

5.8 Summary

This chapter presented *Zen*, the first framework allowing the autonomous generation of complete and realistic CDRs in an individual basis. To this end, we relied on a fully anonymized and incomplete (only traffic-related) CDRs datasets and provide the first literature modeling that captures long-range and inter-CDRs traffic features correlation, individuals heterogeneity and social-ties in communication. The disjoint modeling of realistic emulated mobility and captured real-world traffic behaviors hides real individuals' daily-life habits in routine and leisure times (e.g., home/work, nightlife, etc.), bringing the privacy-preserving capability to the produced *Zen* CDRs. Finally, we validate *Zen* CDRs (i) realisticness in reproducing daily cellular behaviors of urban population and (ii) usefulness in practical networking applications such as dynamic population tracing, network power savings, and anomaly detection as compared to real-world CDRs.

In the next chapter, we elaborate on *FraudZen* validation with respect to *SIMBox* fraud generation. Specifically, we propose and validate a *SIMBox* fraud modeling leveraged at the deep evaluation of literature detection approaches.

Modeling *SIMBox* fraud for effective detection

Contents

6.1	Formalizing <i>SIMBox</i> fraud models	65
6.2	Defining <i>SIMBox</i> fraud models	67
6.3	<i>SIMBox</i> fraud model effectiveness	69
6.3.1	In-crowd-blending capability	69
6.3.2	Experimental setup	70
6.3.3	Assessment results and discussion	71
6.4	Building efficient <i>SIMBox</i> fraud detection	73
6.4.1	Literature on <i>SIMBox</i> fraud detection	74
6.4.2	Impact of the detection model	75
6.4.3	Impact of the aggregation period	76
6.4.4	Impact of the features set	77
6.4.5	Impact of the frequency of incoming traffic	77
6.4.6	Impact of the <i>SIMBox</i> fraud model	78
6.4.7	Fraud model mobility uniqueness	79
6.5	Related works	79
6.6	Summary	80

The *FraudZen* framework enables the simulation of numerous *SIMBox* frauds by tweaking *SIMBox*-implemented functionalities. In this chapter, we deal precisely with *how such SIMBox functionalities can be exploited to create meaningful and ready-to-test frauds*. Depending on the chosen functionalities, the generated fraud can be more or less elaborate in human behavior mimicking, directly affecting its detectability and accordingly, the efficiency of the applied detection techniques. This leads us to investigate the questions of *what characterizes a SIMBox fraud and how such characteristics can impact fraud efficiency*, as follows.

1. First, we name the notion of *fraud model* as a way for implementing a specific fraud, i.e., the set of functionalities that can be chosen to perform a *SIMBox* fraud. Hence, by scrutinizing the intuition behind the *SIMBox* functionalities (cf. §3.2.3), we provide in §6.1 a formal definition of a *SIMBox fraud model* given by its characteristics.
2. Second, in §6.2, we define realistic fraud models from naive to advanced ones, following our formalization. Such fraud models are designed to enable the investigation of each fraud model’s characteristic on its effectiveness.
3. We introduce in §6.3, the *in-crowd-blending* metric as a practical tool to measure the effectiveness of a *SIMBox* fraud model from *FraudZen*’s generated CDRs. Our designed metric captures “*how effective are the means employed by a thief to escape the police control*”, which for *SIMBox* fraud means “*the capability of a fraudster to blend into the crowd of legitimate users*”. We use this metric at the evaluation of our defined fraud models to (1) validate *FraudZen*’s capability of efficient frauds generation and (2) assess the impact of each fraud behavioral feature on the fraud efficiency.
4. Following, we leverage *FraudZen* and our fraud modeling to conduct an in-depth evaluation of current literature detection. We first identify the main features in their design. We then vary such features to obtain a set of detection approaches that we apply to *SIMBox* fraud models of different *in-crowd-blending* capabilities. Based on the obtained results, we provide *quantitative and qualitative insights* takeaways for future detection improvements on what detection should be aware of and how to react to new fraud models (§6.4).
5. At last we discuss the related works in §6.5 and summarize our findings in §6.6.

6.1 Formalizing *SIMBox* fraud models

Fraudsters aim to maximize their profit by committing efficient frauds. Here, *fraud efficiency means mimicking human communication behavior as well as possible, blending among legitimate telecom users while being undetectable*. Accordingly, human communication behavior, commonly inferred from operators’ CDRs [40, 68], has always driven *SIMBox* functionalities. Henceforth, we identify, in Table 6.1, the four main components in human communication behavior that also characterizes the fraud behaviors the *SIMBox* functionalities try to reproduce. For clarity reasons, we only reference in the table the most detailed literature works, which are also considered in §6.4.

(1) Traffic behavior. User traffic behavior relates to the type of generated network events (*ETy* i.e., incoming or outgoing, national, or international calls and SMS, data), the timing of these events (*ETi* i.e., when they occur), and the associated metrics (*EM* i.e., call duration or data session size). For instance, a user generating only outgoing calls or with important traffic at night would be easily identified as fraudulent. Fraudsters define these patterns using *SIM activity limitation* and *network activity generation* functionalities.

Table 6.1: SIMBox fraud models description and examples.

Behavioral traits	Traits-related features	SIMBox functionalities for traits mimicking	SIMBox mimicked traits' options	fraud models' examples
Traffic behavior				
Event types (ETy)	<ul style="list-style-type: none"> - ratio of incoming calls to outgoing calls [102, 86, 114] - nb. of outgoing calls for users not making other events (out_calls_no_evt) [102] - total nb. of out. calls [139, 114, 88, 86, 153] - total nb. of in. calls [139, 114, 88, 86, 153] - total nb. of outgoing intl. calls [114] - total nb. of in. intl. calls [114] - ratio of intl. calls to total calls [114] - total nb. of outgoing SMS [86] 	<ul style="list-style-type: none"> - Network activity generation 	ETy1- outgoing calls only ETy2- out.&in. calls only ETy3- all event types, i.e., out.&in. calls, sms, data	<ul style="list-style-type: none"> - fd_naive ETy1+ETi1+EM1+SP1+SD1+MU1+CN1+RI1+DU1 - fd_traffic ETy3+ETi2+EM2+SP1+SD1+MU1+CN1+RI1+DU1
Event time (ETi)	<ul style="list-style-type: none"> - nb. of calls at night (0-5AM) [102, 139] - total night call duration [139] - total nb. of unique contacts called at night [139] - average inter-call time [86] 	<ul style="list-style-type: none"> - SIM activity limitation - Network activity generation 	ETi1- no restriction ETi2- no activity at night and inter-event time distribution	<ul style="list-style-type: none"> - fd_mobility ETy1+ETi1+EM1+SP3+SD2+MU2+CN1+RI1+DU1
Event metrics (EM)	<ul style="list-style-type: none"> - total call duration [139, 153] - avg. call duration [139] - max. call duration [88] 	<ul style="list-style-type: none"> - SIM activity limitation 	EM1- no call duration limit EM2- max. nb. of calls per day	<ul style="list-style-type: none"> - fd_social ETy1+ETi1+EM1+SP1+SD1+MU1+CN2+RI2+DU1
Mobility behavior				
Stay Points (SP)	<ul style="list-style-type: none"> - nb. of unique visited cell Ids [114, 88, 86] - ratio of the nb. of cell Ids to the nb. of calls [86] 	<ul style="list-style-type: none"> - SIM to module allocation - Base station (BS) selection 	SP1- gateways located in popular cells SP2- gateways are associated in groups of 2 corresponding to home and work locations SP3- each gtw. is moved by car	<ul style="list-style-type: none"> - fd_all ETy3+ETi2+EM2+SP3+SD2+MU2+CN2+RI2+DU2
Stay Duration (SD)	<ul style="list-style-type: none"> - nb. of calls without mobility [102] - nb. of calls in the most recurrent cell Id [88] 		SD1- gateways are static SD2- gateways are at home in 7pm-8am, at work in 9 am-7pm, and make small movements in the neighborhood from 7-8pm	
Mobility Uniqueness (MU)	<ul style="list-style-type: none"> - avg. nb. of users making calls in the same cell Id [102] 	<ul style="list-style-type: none"> - SIM to module allocation - BS selection - SIMBox architecture 	MU1- all SIMs are in the same gtw. MU2- 2 SIMs per gtw.	
Social behavior				
Contact Nb. (CN)	<ul style="list-style-type: none"> - total nb. of unique called [139, 88, 86] - total nb. unique callers [88] 	<ul style="list-style-type: none"> - Routing policy - Incoming intl. call authentication - Network activity generation 	CN1- no maximum CN2- max. nb. of contacts	
Relationships (RI)	<ul style="list-style-type: none"> - ratio of the nb. of unique contacts called to the total nb. of calls [139] 	<ul style="list-style-type: none"> - Routing policy - Network activity generation 	RI1- none RI2- cliques of fraudulent SIMs	
Device type				
Device Uniqueness (DU)	<ul style="list-style-type: none"> - nb. of SIM per device (IMEI identified) [114] 	<ul style="list-style-type: none"> - IMEI modification 	DU1- no IMEI modification DU2- one SIM per IMEI	

(2) Mobility behavior. User mobility is identified in operators' traces by the position of the cell tower relaying a generated event and the trajectory formed by a sequence of these positions. Therefore, a user's mobility behavior is reflected by the charge (relative high traffic or not) and the number of network cells where the user appears (*SP*), as well as his visiting duration at each cell related to the time of the day (*SD*). Such elements must be meaningful with respect to the daily habits commonly governing people mobility (e.g., commuting to work, shopping, meeting friends), which are mirrored in CDR-like trajectories of people. Accordingly, a user appearing in an individual cell or a small number of nearby cells over a long period has a dubious mobility behavior. Fraudsters set such behavior through *base station selection* and *SIM to module allocation* functionalities. They can also transport gateways by car or bike. A latter important aspect of the mobility behavior is the uniqueness amongst others is an individual trajectory (*MU*), which is an indicator of the fact that the individual most of the time moves alone and not with a group as with a *SIMBox* (i.e., a box of SIM cards). Fraudsters can alter this by setting the number of SIM cards allocated to each *SIMBox* gateway: the more it is, the more the *SIMBox* generates group mobility.

(2) Social behavior. Calls and SMS events directly reveal inter-user interaction and social life. Specifically, the number of contacts a user has (*CN*) and the weight and direction (outgoing/incoming) of its interactions with these contacts are indicative of its social behavior. Further, such interactions, generally modeled in the literature as mobile call graphs [82, 165], often reflect meaningful relationships between users (*RI* e.g., family, group of friends) through the identification of cliques of varying sizes [116]. Fraudsters use three strategies for building such behavior. First, with *routing policy* and *call routing authentication* functionalities (cf. §3.2.3), calls from international users can be preferentially terminated by specific *SIMBox* users, limiting users' number of contacts. Besides, *network activity generation* functionalities allows inter-calls and SMS of *SIMBox* users, simulating close users groups.

(3) Device type. The device type refers to the number of SIM cards a user's device operates with, which is limited to one or two for legitimate users. Accordingly, each *SIMBox* user has to mimic a usage in a unique mobile device (*DU*). For instance, a SIM card (identified by an IMSI code) connected to several mobile devices in a short period is likely to be fraudulent, revealing the presence of a *SIMBox* with hardware capability to manage many SIMs having many GSM modules. Fraudsters leverage *IMEI modification* functionalities to hide such noticeable behavior.

6.2 Defining *SIMBox* fraud models

In practice, a multiplicity of *SIMBox* fraud models can be formed following the formalization given in §6.1. An Internet-available *SIMBox* equipment, can be purchased and configured by non-expert and beginner fraudsters giving rise to naive strategies as well as by traffic termination businesses such as [7, 57] giving rise to advanced strategies close to legitimate users' behavior. Accordingly, we introduce five fraud models, designed for evaluating the significance

of each behavioral feature introduced in the previous section, at the fraud efficiency.

Table 6.1 shows how we build such fraud models from the *SIMBox* functionalities implemented in *FraudZen*. Precisely, we vary the configurations of the *SIMBox* functionalities associated to each fraud model's behavioral feature (cf. third column in Table 6.1), to generate examples of attacks from simple to advanced ones (cf. fourth column of Table 6.1). Some of these configurations are based on statistics from a real-world anonymized CDRs of legitimate users, described in §6.3.1.

This results in five representative fraud models (cf. last column of Table 6.1). From the simplest to the most advanced model, they are named: *fd_naive*, *fd_traffic*, *fd_mobility*, *fd_social*, and *fd_all*. It is worth mentioning behavioral features related to *device type* have been little investigated and considered in fraud detection literature. Therefore, we opt to not consider them in our fraud models' design. We hereafter elaborate on each fraud model.

fd_naive. performs fraud with no effort to mimic human behavior. The *SIMBox* is therefore limited to routing incoming international calls, generating only outgoing call events at all day periods as long as there is traffic to terminate. Concerning mobility, the *SIMBox* gateways are each installed in a crowded place in the city, and SIMs are allocated only once to each GSM module resulting in virtual devices that never move. In addition, all *SIMBox* SIM cards are installed in a unique gateway. The social behavior doesn't limit the number of contacts *SIMBox* devices can have. Finally, the device type configuration keeps the factory IMEI assigned to each GSM module.

fd_traffic. simulates a traffic behavior close to human behavior while keeping the other behavioral features naive. Thus, the *SIMBox* virtual devices generate, in addition to outgoing calls, data traffic, SMS, and incoming calls through inter-calls and SMS. Moreover, concerning events timing, they make no traffic at night and respect legitimate users' Inter-Event Time distributions in generating traffic (incoming calls, data, and SMS) during the active period. Finally, these devices are configured to make a maximum number of calls per day set to the mean of the distribution of the number of calls per day for legitimate users.

fd_mobility. adopts for each *SIMBox* architecture's gateway, mobility modeled on human behavior based on the realistic Working Day Mobility model (WDM) [45] and keeps the other behavioral features naive. Therefore, each gateway moves by car between its associated home and workplaces occupied according to the time of day. Besides, the fraud model creates some reduced movements (in the neighborhood) in the evening that errands or activities could induce. To ensure mobility uniqueness, this fraud model allocates only two SIM cards to each *SIMBox* gateway.

fd_social. solely modifies the social behavior of users. Hence, an history-based call routing policy is used to limit the number of fraudulent call destinations, i.e., contacts. Similarly, the number of contacts making inter-calls is restricted from legitimate users' contacts statistics.

fd_all. at last, includes all advanced configurations related to each behavioral feature.

All such fraud models are included in *FraudZen* as scenarios given by configuration files.

6.3 SIMBox fraud model effectiveness

This section presents the *in-crowd-blending capability* as a metric to estimate the effectiveness of a SIMBox fraud model from FraudZen’s generated CDRs (§6.3.1). We use this metric in §6.3.3 at the evaluation of our defined fraud models to (1) validate FraudZen’s capability of efficient frauds generation and (2) assess the impact of each fraud behavioral feature on the fraud efficiency.

6.3.1 In-crowd-blending capability

The *In-crowd-blending capability* of a SIMBox fraud model refers to its ability to make fraudulent users blend in the crowd of legitimate ones. It comes from the intuitive idea that the more a fraud model yields fraudulent users’ behaviors close to human ones, the harder it is to detect such fraudulent users. To infer such capability, we consider the FraudZen CDRs generated from a given fraud model fm . From these traces, we get for each user a vector of features reflecting its communication behavior:

$$V_f = \{P_{1,ETy}, \dots, P_{k,ETy}, P_{1,ETi}, \dots, P_{l,ETi}, P_{1,EM}, \dots, P_{m,EM}, \\ P_{1,SP}, \dots, P_{n,SP}, P_{1,SD}, \dots, P_{p,SD}, P_{1,MU}, \dots, P_{q,MU}, \\ P_{1,CN}, \dots, P_{r,CN}, P_{1,RI}, \dots, P_{s,RI}, P_{1,DU}, \dots, P_{t,DU}\}$$

where $P_{i,BT}$ refers to i th feature of the behavioral trait BT (cf. Table 6.1). In particular, we use a comprehensive list of features reported from the SIMBox detection literature in 2nd column of Table 6.1. We then apply a multi-variate unsupervised clustering (e.g., DBSCAN) to the gotten users’ feature vectors to group users with similar cellular communication behavior. The users populating the same behavioral group define a particular cluster.

As in Fig. 4.1, we distinguish three categories of fraudulent users: (i) isolated users (named *outlier cluster*, i.e., OC), (ii) users in the same clusters as legitimate users (named *hybrid cluster*, i.e., HC), and (iii) users in a cluster of only fraudulent users (named *fraudulent-only cluster*, i.e., FC), described hereafter. The distribution of users into the three aforementioned categories reveals how efficient each SIMBox fraud model fm is in blending into the legitimate crowd. We compute such *in-crowd-blending capability*, $ICB(fm)$, as:

$$ICB(fm) = \frac{|HC|}{|HC| + |FC| + |OC|} \quad (6.1)$$

- **Hybrid cluster - HC**: shows its fraudulent users’ behaviors are similar to legitimate ones. Such users have a high *in-crowd-blending capability*, making them hardly detectable. *A fraud model’s best efficiency is thus a majority of fraudulent users in the hybrid cluster.*

- **Fraudulent-only cluster - FC**: identifies fraudulent users with similar behaviors isolated from legitimate ones. Such users have a low *in-crowd-blending capability*, making them easily detectable. *A sparse fraudulent-only cluster thus reveals an efficient fraud model.*

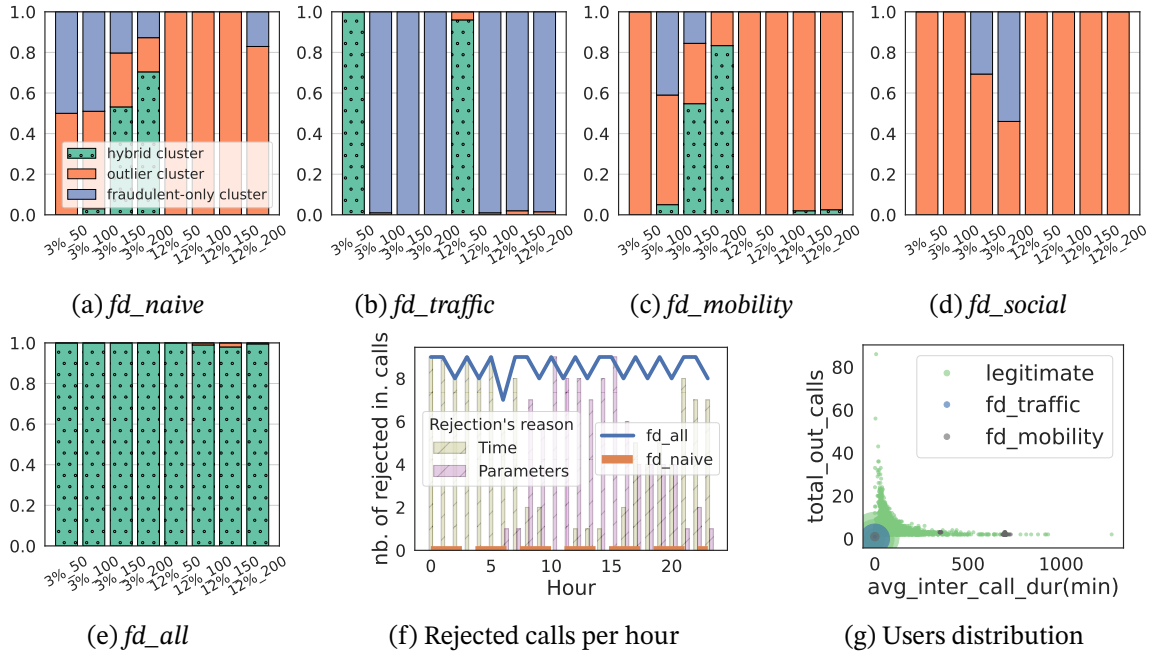


Figure 6.1: (a)-(e) In-crowd-blending metric per fraud model. (f) *SIMBox* rejected calls per hour in 3% scenario and 200 Fraudulent users. (g) *fd_traffic* to *fd_mobility* comparison in 3% scenario and 200 Fraudulent users.

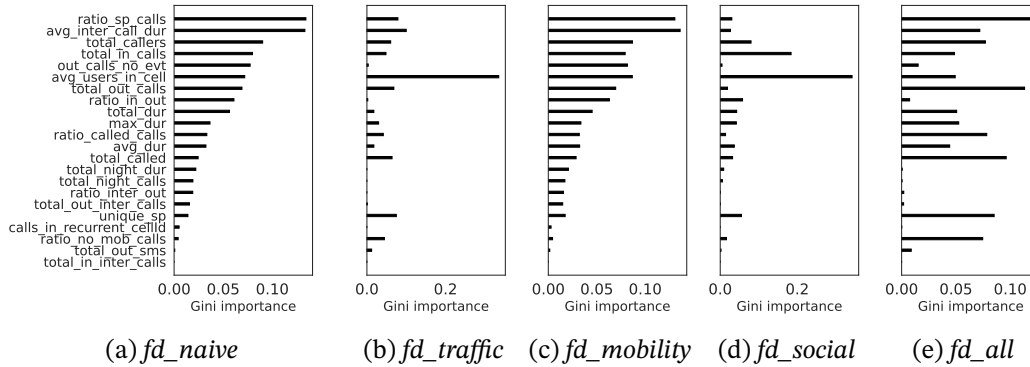


Figure 6.2: Average relative importance of trait-related features per fraud model.

- **Outlier cluster - OC:** similarly to the fraudulent-only cluster, fraudulent outliers are isolated, thus vulnerable and not resilient to detection, having thus, a low *in-crowd-blending capability*. Hence, a low number of outliers is also indicative of an efficient fraud model.

6.3.2 Experimental setup

For the numerical assessment of define fraud models, we constitute 40 *FraudZen* simulation scenarios differently configured to simulate heterogeneous behaviors of legitimate and fraudulent users, as shown in Table 6.2.

Generating legitimate behavior. At the generation of legitimate cellular traffic, we leverage the traffic behavior as described in real-world, non-public, and fully anonymized CDRs

Table 6.2: *FraudZen* simulation scenarios.

	Parameter	Value(s)	Number of scenarios	
<i>Legitimate behavior</i>	Local traffic model	Trace-based from real-world traffic CDRs	1	Total=40
	Inter. incoming traffic model			
	Mobility model			
<i>Fraudulent behavior</i>	<i>SIMBox</i> fraud model	<i>fd_naive, fd_traffic, fd_mobility, fd_social, fd_all</i>	5	
	% inter. incoming calls	3% =>one call/7min, 12% =>one call/2min	2	
	Number of fraudulent SIMs	50, 100, 150, 200	4	

from a major telecom operator, i.e., *RefCDRs* as presented in §5.1.2. It describes one month of per-user traffic (local and international outgoing calls and SMS, data) in about 3 million time-stamped events generated by 28K users from the provider operator. We filter out users interacting with other operators’ phone numbers (i.e., 7000 users), and build our simulation scenarios with a unique operator and 21K legitimate users.

Because the leveraged CDRs lack daily spatiotemporal mobility information of users (i.e., users’ cell ID positions), we assign realistic trajectories to every 21K users generated by our *En-WDM* mobility emulator (cf. §5.3). This association is made according to the algorithm presented in §5.5. Accordingly, we end up with complete CDRs describing real-world users’ traffic, mobility, and social behaviors.

Note that the lack of mobility information in the used raw CDRs and its enrichment with *as-realistic-as-possible* spatiotemporal trajectories do not impact the numerical assessment of fraud models presented next. *Indeed, the configuration offered by WDM brings the flexibility to add physical organization and daily behaviors of an actual city and its inhabitants, which constitutes the underlying structure required to play the designed fraud models, (most importantly) leveraging in-market SIMBox functionalities.*

Generating fraudulent behavior. We simulate each of the five fraud models of §6.2 in 8 scenarios, obtained through different values of the (i) percentages of incoming international traffic and (ii) numbers of SIM cards in the fraudulent architecture. First, the percentage of incoming international traffic varies from operator to operator and impacts the number of calls the *SIMBox* has to route. We consider in the simulation two percentage values (i.e., 3% and 12%) inspired by a statistical report [134] of a victim telecom operators. Hence the percentage of international traffic diverted to the *SIMBox* is deduced by deducting from the considered rates (i.e., 3% and 12%) the actual rate of international incoming in our legitimate CDRs. From such values, the fixed frequency of diverted international incoming calls is 7min and 2min, respectively. Second, the number of SIM cards in the fraudulent architecture directly impacts the efficiency of the implemented fraud. Therefore, we consider four values of SIM cards’ number in our analyzes: 50, 100, 150, and 200 (cf. Table 6.2).

6.3.3 Assessment results and discussion

Fig. 6.1 shows the in-crowd-blending capability per fraud model and under the scenario configurations described in Table 6.2. Besides for explainability, Fig. 6.2 presents per fraud model

the average impact, over all implemented scenarios, of each *feature* $P_{i,BT}$ (cf. 2nd column of Table 6.1) on the clusters generation. To get such result, we train a Random Forest with the behaviors of users composing each cluster as described by the corresponding trait-related features. Then, we estimate the relative importance of each *feature* $P_{i,BT}$ in determining the clusters composition using the *Gini importance* metric. The Gini importance measures the contribution of each feature in a decision tree or random forest model by calculating how much each feature reduces the amount of uncertainty or randomness in the model. However, it can favor features with many unique values or categories with high cardinality due to the more significant number of possible splits.

The insights drawn from both Fig. 6.1 and Fig. 6.2's results are as follows.

fd_naive (Fig. 6.1a) This fraud model makes no human mimicking effort; however, we observe that for 3% of incoming international traffic, the value of *hybrid_metric* increases when the number of fraudulent SIMs grows. This is because the same amount of incoming diverted traffic is distributed to more fraudulent users, i.e., each user makes less traffic. With 12%, we observe the same pattern but with much more generated traffic (1 call/2min), which explains why despite the increase in the number of users, we have a majority of outliers. Fig. 6.2a confirms this interpretation: the most important features are the ratio of unique stay points to the number of outgoing calls (*ratio_sp_calls*) and the average inter-call duration (*avg_inter_call_dur*). Since for all naive users, the number of unique stay points is fixed at one as they are static, the values of *ratio_sp_calls* increase with the number of fraudulent users and approach those of legitimate users. Similarly, the values of *avg_inter_call_dur* increase as the number of individual calls decreases.

fd_traffic (Fig. 6.1b) As shown in the figure, the results produced by this fraud model are counter-intuitively worse than those of fraud model *fd_naive*, in which there is no effort to defraud. When the number of fraudulent users is low, with 3% and 12% of incoming international calls, the fraud model simulates a human-like behavior as shown by its large hybrid cluster. When the number of users increases, all these users form a fraudulent-only cluster making them easily detectable. Fig. 6.2b shows this is mainly due to the mobility behavior which remains naive: the value of *avg_users_in_cell* is very high for all fraudulent users compared to the legitimates because they are all allocated to a single gateway that never moves.

fd_mobility (Fig. 6.1c) The results of this fraud model are very similar to those of *fd_naive* but are improved: more populated *hybrid cluster* and less *fraudulent-only's* overall. Hence, improving mobility rather than traffic has a better impact on the effectiveness of fraud strategies. To better explore this, we make bubble plots of legitimate users (not outliers), *fd_traffic* users, and *fd_mobility* users for traffic behavioral features (Fig. 6.1g). *fd_traffic* users are concentrated in a density different from legitimate users distribution. On the contrary, *fd_mobility* users are spread with majority remaining similar to the density of legitimate users.

fd_social (Fig. 6.1d) The results of this fraud model are the worst in terms of human behavior reproduction. The more fraudulent users there are, the greater is the *fraudulent-only* cluster; but there is no hybrid cluster compared to the *fd_naive* fraud model. The feature with the

Table 6.3: Designed *SIMBox* fraud detection models and evaluation parameters.

ML model	Hyper-parameter values used for tuning	Detection features set	Aggregation period	Evaluation metrics
ANN [139, 86, 153]	- #hidden layers: 1, 2, 3 - #nodes in hidden layers: 5, 9, 18 - learning rate: 0.1, 0.3, 0.6, 0.9 - optimizer: RMSProp, SGD, Adam	- traffic_detection - traffic+social - traffic+mobility - all_detection	- a day [139, 86, 153] - a week [114]	- accuracy - f1 score - precision - recall - training time
SVM [139, 86, 153]	- kernel: RBF, polynomial - gamma: 0.125, scaled - degree: 2,3 - C: 1, 10, 100, 1000			
RF [114, 86, 153]	#trees: 1, 2, 5, 10, 20, 50, 100, 200, 500			
Gradient Boosting Decision Trees (GBDT)	- #trees: 1, 2, 5, 10, 20, 50, 100, 200, 500 - learning rate: loguniform(0.01, 1)			

greatest impact on this classification, as depicted in Fig. 6.2d, is *avg_users_in_cell* as in the case of the *fd_traffic* fraud model. But differently, the feature *total_in_calls* has more impact. With further investigation, we found this is because, although generating a number of callers for fraudulent users (*total_callers*) that is similar to legitimate, the *fd_social* fraud model does not control the incoming traffic generated, the value of *total_in_calls* becomes too large, allowing its distinction.

fd_all (Fig. 6.1e) This fraud model yields all fraudulent users in hybrid clusters regardless of the scenario. This proves that it is possible, with the current in-market *SIMBox* functionalities, to generate frauds very close to human behavior. We can see from Fig. 6.2e that this result is mainly based on features *ratio_sp_calls*, *total_out_calls*, *ratio_called*, and *unique_sp* (i.e., unique number of stay points), which relate to all the behavioral features of a *SIMBox* fraud model. We also note that some features are of little importance, i.e., (*ratio_night_dur*, *total_inter_calls*, *total_in_inter_calls*, and *total_out_sms*); it is therefore not essential to include them in the *SIMBox* fraud model for effective fraud.

On the other hand, Fig. 6.1f shows that configurations associated with the *fd_all* fraud model cause the *SIMBox* to reject the majority of fraudulent calls from abroad. This is due to fraud model’s restrictions on the event time (i.e., no operation at night) and parameters (i.e., maximum number of calls per day). In comparison, the *fd_naive* fraud model routes all incoming calls as it has no restrictive policy. *Therefore, although the fd_all fraud model is effective, it allows fraudsters to make limited financial gains due to rejected calls, given the level of investment* (e.g., an architecture with 200 SIMs requires 100 gateways to maintain a fair mobility uniqueness, i.e., 2 SIMs/gateway).

6.4 Building efficient *SIMBox* fraud detection

This section relies on *FraudZen* to provide an in-depth evaluation of literature *SIMBox* fraud detection techniques, giving essential insights to improve future research on the domain. Precisely, we analyze detection’s performance metrics (cf. last column of Table 6.3), while varying parameters of *detection* and *fraud* models.

While the analysis of *detection parameters* guides the choice of the best options for designing efficient fraud detection, *fraud-related parameters* allow assessing how detection performs in different fraud scenarios, uncovering detection's weaknesses. Thus, from our literature review in §6.4.1, we identify and consider three *detection parameters*: the ML model, the aggregation period, and the feature set (cf. §6.4.2, 6.4.3, and 6.4.4). Besides, we consider three *fraud-related parameters*: the fraud model, the frequency of incoming traffic, the SIMBox mobility behavior (cf. §6.4.5, 6.4.6, and 6.4.7).

6.4.1 Literature on SIMBox fraud detection

CDR-based literature SIMBox fraud detection approaches typically use ML classification models on supervised CDRs preprocessed into detection features describing users communication behavior. We narrow our selection to some of the most recent or high-ranked published works providing description of the used parameters, allowing reproduction. Hereafter, we discuss the identified detection parameters reported in Table 6.3.

ML classification model. At the core of detection approaches, ML models are trained from a set of fraudulent and legitimate users in the CDRs ground truth. They capture users' communication behaviors and accordingly categorize them as fraudulent or legitimate aiming the lowest error. Our review reports comparative analysis of the following models: Artificial Neural Network (ANN) and Support Vector Machine (SVM) [140, 86, 153]; Random Forest (RF) [86, 153, 114]; as well Alternating Decision Tree [114, 71]. Focusing on the models' classification performance, we consider in our analysis the Gradient Boosting Decision Tree (GBDT) model, an evolution of the Alternative Decision Tree (no longer used in literature). GBDT combines several decision trees using the boosting method. Because the unfeasible replicability of the selected detection approaches (i.e., unavailable training datasets), we conduct a hyper-parameter tuning to determine the best model in each scenario.

Aggregation period. It defines the amount of timestamped data in CDRs to be considered for the detection features computation, i.e., how frequent a detection will be carried out (e.g., daily, weekly). This period directly impacts the amount of information collected to differentiate between fraudulent and legitimate users. On the other hand, the lower the detection frequency, the higher the fraudsters' profit due to more extended fraud operations.

Detection features set. Classification features are obtained by aggregating CDRs fields to capture users' communication behavior. Considered features define the representation of each user provided to the classification model; a representation that is not good enough to distinguish fraudulent from legitimate users, limits the classification performance. Literature works considered various sets of features (cf. Table 6.1). Here, we focus on the impact of communication behavior (i.e., traffic, mobility, or social) to the detection. Accordingly, we group all detection features by behavior, which bring us to distinguish four sets (cf. Table 6.3): traffic features only (*traffic_detection*), traffic with social features (*traffic+social*) [139], traffic with mobility features (*traffic+mobility*) [114], and all features, i.e., traffic with social and mobility (*all_detection*) [86, 153]. Hence, each feature set targets the detection of the behaviors

Table 6.4: Detection models’ performance per fraud model, 3% of intl. calls, and all_detection feature set.

Model	#fraudulent users	fd_naive			fd_all			fd_traffic			fd_mobility			fd_social		
		balanced acc	precision	recall	balanced acc	precision	recall	balanced acc	precision	recall	balanced acc	precision	recall	balanced acc	precision	recall
ANN	200	0.99	0.95	0.99	0.57	0.21	0.16	1	1	1	0.57	0.5	0.14	1	1	1
	50	1	1	1	0.5	0	0	0.89	0.67	0.8	0.98	0.94	0.96	0.99	1	0.98
SVM	200	0.98	0.82	0.97	0.56	0.37	0.14	1	1	1	0.62	0.76	0.24	0.99	0.99	0.99
	50	0.97	1	0.94	0.49	0	0	0.99	0.84	1	0.98	0.88	0.96	0.97	0.96	0.94
RF	200	0.94	0.93	0.88	0.80	0.82	0.64	1	1	1	0.66	0.63	0.34	0.99	0.99	0.98
	50	0.97	1	0.94	0.49	0	0	0.99	0.97	1	0.96	0.98	0.92	0.98	0.93	0.96
GBDT	200	0.99	0.94	0.99	0.70	0.88	0.41	1	1	1	0.62	0.82	0.25	0.99	0.99	0.99
	50	0.98	0.92	0.96	0.5	0	0	0.99	0.92	1	0.97	0.94	0.94	0.97	0.92	0.94

it considers.

Evaluation metrics. we consider five evaluation metrics obtained with a 10-fold cross validation: (1) The *balanced accuracy* – rather than the classical one, as legitimate users outnumber fraudulent ones – is defined as the average of recall obtained on each class. (2) The *recall* is the ability of the classifier to find all the scenario’s fraudulent users, giving its capacity to resolve the fraud. (3) The *precision* is the ability of the classifier to not label as fraudulent a user that is not one, giving the confidence level in blocking a detected fraudulent user. (4) The *F1-score* indicates the overall performance of the classifier. (5) The *training time* of each model is a relative indicator of the required resources for operation, a critical metric when dealing with hundreds of thousands of subscribers.

6.4.2 Impact of the detection model

Considering the *all_detection* features set, Table 6.4 shows the evaluation metrics’ results for the five fraud models (cf. Table 6.1), for 50 and 200 fraudulent users, and considering 3% of incoming intl. traffic. With the *fd_naive* fraud model, all detection ML models have comparable performance and do quite well for 50 and 200 fraudulent users, with at least 97% of accuracy and 82% precision. With the *fd_all* fraud model, all ML models poorly perform when there are 50 fraudulent users, with 0 recall and precision, indicating that all fraudulent users are misclassified as legitimate and no user is classified fraudulent. However, when the number of users is higher, **RF** and **GBDT** perform better than **ANN** and **SVM**. Although **GBDT** precision is higher than the **RF** one, the balanced accuracy and recall of **RF** are globally higher: the **RF** detects more fraudulent users (i.e., 64%) than other ML models, with a pretty good precision (i.e., 82%). These tendencies are also moderately observable with *fd_traffic*, *fd_mobility*, and *fd_social* fraud models.

Furthermore, we report in Fig. 6.3 the distribution over all scenarios of considered detection models’ training time. We can see that the **GBDT** is unsurprisingly the best model w.r.t. the training time as it combines shallow decision trees that are easy to train. On the other hand, the **ANN** model is relatively the longest to train due to the high number of layers and, therefore, parameters it may have. At the same time, the **SVM** can present very high training time values depending on the scenario.

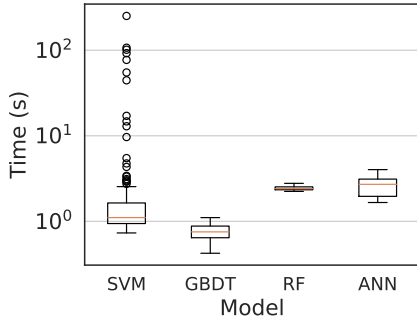


Figure 6.3: Training time (s) of considered ML detection models.

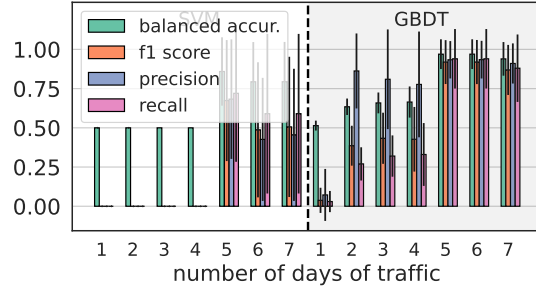


Figure 6.4: Evaluation metrics w.r.t. the aggregation period in 3% scenario, 100 Fraudulent users, and all_features set.

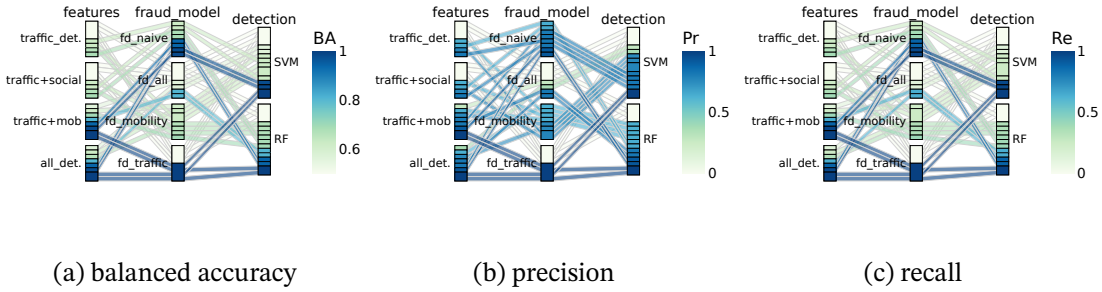


Figure 6.5: Evaluation metrics w.r.t. the features set in 3% scenario and 200 Fraudulent users.

1st Insight: A combination of simple decision rules (as done in *RF* and *GBDT*) based on individual’s behavioral features is more efficient than classifying users based on their global behavior (as done in *SVM*). We therefore recommend for an efficient detection to leverage tree ensemble models or a linear combination of such models which however, requires more training time.

6.4.3 Impact of the aggregation period

As shown in Fig. 6.4, increasing the aggregation period from 1 to 7 days impacts the detection performance of *SVM* (of average performance) and *GBDT* (efficient) models. Such results consider the *fd_all* fraud model with 100 fraudulent users and 3% of incoming intl. traffic. For *SVM*, we see a significant performance increase only after five days. Unfortunately, considering the low initial investment on SIM cards acquisition, such time is enough for fraudsters to generate substantial gains before replacing the SIMs detected as fraudulent. Also, for both models we notice that beyond five days, the performance (e.g., the precision), slightly decreases each day. Indeed, by increasing the aggregation period we include more legitimate users of heterogeneous communication behaviors, increasing their probability of being misclassified.

2nd Insight: Aggregation period enlargement does not straightly improve detection performances. Accordingly, we recommend to apply detection while considering many aggregation periods; for instance, (i) daily features and (ii) 3 to 5 days aggregated ones. Such a design can increase detection precision for more efficiency.

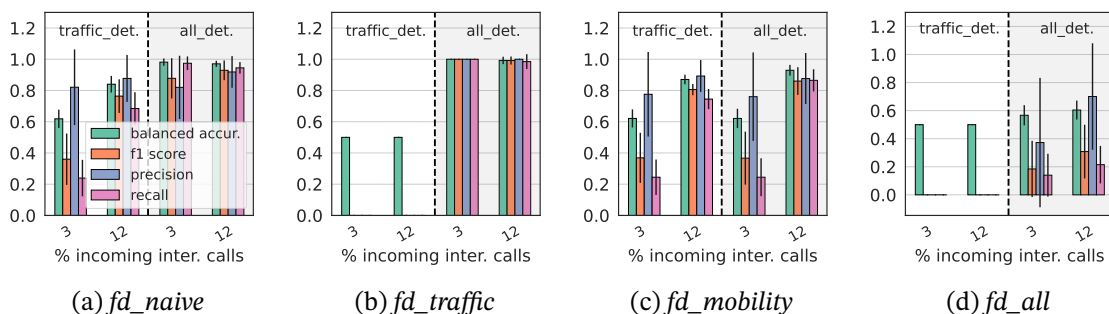


Figure 6.6: Evaluation metrics w.r.t. the percentage of fraudulent incoming traffic. #Fraudulent users: 200 Model: SVM.

6.4.4 Impact of the features set

Fig. 6.5 shows the impact of detection features on the detection performance of both SVM and RF models, for 3% of incoming intl. traffic and 200 users. We consider all fraud models but the *fd_social* one, as it causes no dynamics to fraud detection (cf. § 6.3.3). Overall, results show the values of balanced accuracy, precision, and recall are the lowest with *traffic_detection* and *traffic+social* feature sets: the addition of social features to the detection add no difference. Instead, the addition of mobility detection features creates a shift in the detection performance, according to the fraud model: for *fd_traffic*, the performance increase is the most important, followed by *fd_naive*, *fd_all*, and finally, *fd_mobility*, for which there is almost no influence. We also notice the impact of the mobility detection features is more important for the precision metric than for the balanced accuracy and recall. Finally, the detection made with *all_detection* features slightly increases evaluation metrics compared to the *traffic+mobility* features.

3rd Insight: Compared to traffic and social behaviors, users’ mobility behavior presents the best facet to distinguish between fraudulent and legitimate users. *We therefore recommend a deeper exploitation of detection features based on mobility behavior.*

6.4.5 Impact of the frequency of incoming traffic

We can see from Fig. 6.6 how detection performances vary when we increase the amount of incoming international traffic the SIMBox has to route, from 3 to 12%. The results are presented for an SVM detection with *traffic_detection* and *all_detection* feature sets in a scenario with 200 fraudulent users. As for previous section, we do not consider the *fd_social* model in results computation. Globally, the upsurge of incoming traffic increases all the evaluation metrics for all the fraud models. In particular, for the *fd_naive* and *fd_mobility* fraud models, we observe a change from 62% to 83% accuracy when the detection is only on the traffic features. For the *fd_all* and *fd_traffic* fraud models, there is no impact in *traffic_detection*. However, there is a slight increase of accuracy with *all_detection* due to impact on the fraud mobility behavior. Indeed, *as the inter-call time is reduced due to a higher call frequency, the number of unique cell ID positions recorded in CDRs for each fraudulent user tends to diminish, denoting a lack of mobility.* Such an effect is more apparent for *fd_all* users as they make very few calls to simulate

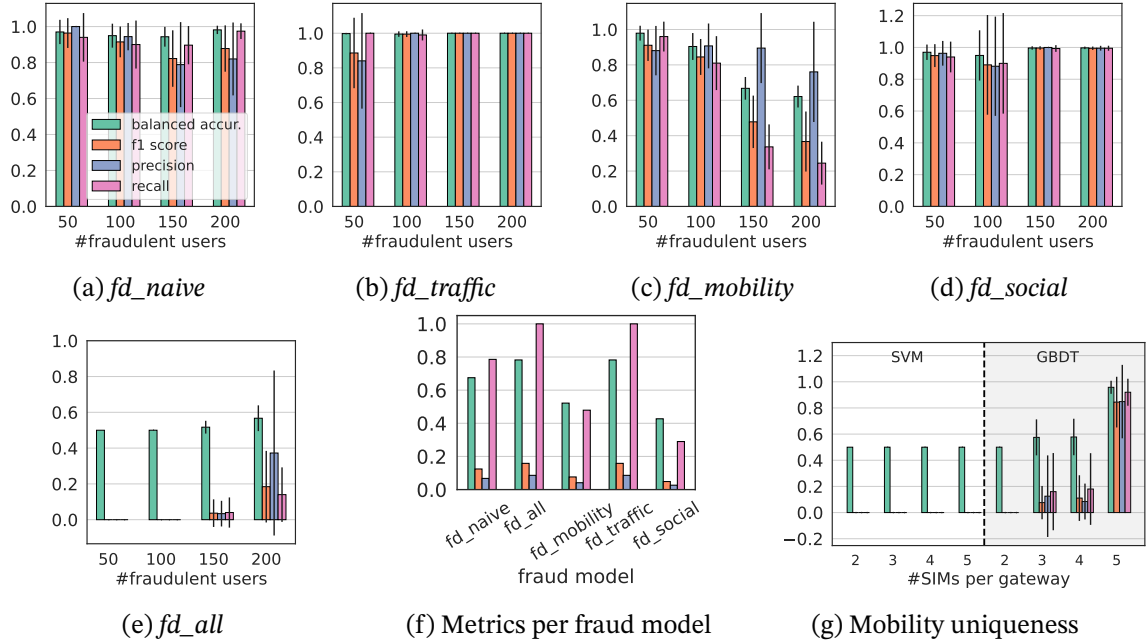


Figure 6.7: (a)-(e) Evaluation metrics *w.r.t.* the number of fraudulent users. Scenario: 3%. Model: SVM. Features set: *all_features*. (f) Multi-fraud models detection in 3% scenario, 200 Fraudulent users, and *all_features* set. (g) Evaluation metrics *w.r.t.* the mobility uniqueness. fraud model: *fd_all*. Features set: *all_features*. Scenario 3%. #Fraudulent users: 200

real users' traffic behaviors. Yet, enabling to configure a minimum inter-call time value in the *SIMBox* could make this effect disappear.

4th Insight: *The more calls the SIMBox has to route, the more difficult it is to disguise the resulting traffic while imitating human behavior. Although this is within fraudsters' reach, it requires more resources (i.e., SIM cards and gateways) in the architecture.*

6.4.6 Impact of the *SIMBox* fraud model

Figure 6.7 shows the performance of the SVM model (middle performing) against our five fraud models while varying the number of fraudulent users. We fix in *FraudZen* the incoming traffic to 3% and report metrics with *all_detection* features.

Results for *fd_naive* and *fd_mobility* fraud models are highly correlated with statistics obtained in §6.3.3 with the in-crowd-blending metric: As the number of fraudulent users increases, fraudulent users blend in with legitimate ones, and the detection accuracy and recall drop, though the precision value is maintained high ($\geq 80\%$). On the other hand, for *fd_all* and *fd_traffic* fraud models, *the increase of fraudulent users causes an overall improvement in detection performances*. At last, the *fd_social* fraud model is easily detectable compared to *fd_naive*.

5th Insight: *The variation of the tackled fraud model causes an important discrepancy in detection performance; attesting fraudsters have genuine control over their traceability.*

At last, Fig. 6.7f gives an idea of how the detection could be in real-world scenarios where the data includes several attack patterns that are not a priori known. Here, we apply the RF

model with the *all_detection* feature set, to a dataset containing 5000 legitimate users and 200 fraudulent users per fraud model, i.e. 1000 fraudulent users. **RF** is trained on 80% of the dataset, without any knowledge on the fraud model's choice. We report the classification performances on each fraud model in the test set, i.e., the remaining 20%. The results show poor precision for all fraud models but a significant recall, especially for the fraud models *fd_all* and *fd_traffic*. These latter two models generate fraudulent users with homogeneous behaviors, compared to the other fraud models (cf. Figs 6.1b, 6.1e). The detection thus mostly learn their behaviors as fraudulent, which also explains why many legitimate users are misclassified.

6th Insight: *Considering several fraud models at once negatively impacts detection performances, especially in the presence of advanced fraud models inducing a loss in precision. This result suggests to handle separately each fraudulent behavior in detection. FraudZen offers the means to generate enough data to train detection models before applying them to uncontrolled scenarios.*

6.4.7 Fraud model mobility uniqueness

Following the 3rd insight drawn in §6.4.4, we deeper investigate the impact of the fraud's mobility behavior on detection. Here we consider *fd_all* and vary only the number of SIMs per gateway of the architecture, referring to the fraud model's *mobility uniqueness* (cf. Table 6.1). Precisely, this parameter directly influences the mobility detection feature *avg of users in cell ID* whose average value for legitimate users in our scenarios is 2.06. Note that such a value is lower than in real-world scenarios as we simulate mobility with a lower population density than in Helsinki city to meet the number of users of our provided CDRs.

Hence, we perform **SVM** and **GBDT** detection on the *fd_all* fraud model while varying the number of SIMs per gateway from 2 to 5 in a scenario with 200 fraudulent SIMs and 3% of incoming international traffic. Results in Fig. 6.7g show that although there is no impact on **SVM** detection, the **GBDT** model is very sensitive and reaches a balanced accuracy of 100% for 5 SIMs per gateway. Hence, the smaller is this parameter, the better it is for fraudsters.

7th Insight: *The number of SIMs per gateway parameter defining the fraud model's mobility uniqueness can largely influence fraud detection. Moreover, fraudsters can hardly control its impact, which varies with the mobility zone and the behavior of the legitimate users in this zone. Hence we recommend future detection to increase features distinguishing this fraud behavior.*

6.5 Related works

As most security problems are evolving, a lot of works in the literature leverage an attack formalization identified as "threat model" [31, 69, 156, 136] or "attack model" [25, 155, 43]. Such formalization is essential to define the attacker's capabilities and evaluate related defense efficiency. Regarding *SIMBox* bypass frauds, this work presents the first attempt in attack modeling.

6.6 Summary

Despite its huge impact on operators' revenue and national security, *SIMBox* bypass fraud is an open issue in cellular networks. This chapter addressed one major challenge hindering its investigation: the difficulty of leveraging detection due to a lack of clarity on fraud behavior in analyses. By methodically unraveling the *SIMBox* appliances' functionalities, we extracted intuitive and easy-to-interpret traits encompassing the fraud action areas and defining a *SIMBox* fraud modeling. Henceforth, we established the groundwork for fraud detection evaluation by using our *SIMBox* fraud modeling as a proxy for performance investigation of literature detection approaches. Our provided detection-related insights attest to the *FraudZen* capability of generating efficient *SIMBox* fraud traces allowing new venues for future fraud detection investigations.

In the next chapter, we explore a novel cellular data type in the *SIMBox* detection literature: cellular signaling data. Through experimental analyses, we show its usefulness for real-time *SIMBox* fraud detection. Therefore, we propose a detection framework exploiting such insights to be deployed at the network edge.

Cellular signaling-based detection

Contents

7.1	Cellular signaling-based detection	83
7.1.1	Motivation	83
7.1.2	Literature limitations	83
7.1.3	Goal	86
7.2	<i>SigN</i> prevention system	86
7.2.1	Intuition	86
7.2.2	Experimental setup	88
7.2.3	Network attachment latency	88
7.2.4	Prevention algorithm	89
7.3	Discussion	91
7.4	Summary	92

At this level, we consider two findings from previous studies: First, CDR-based methodologies, as currently designed, are unfortunately not robust to the constant fraud evolution. Second, the time required to infer detection insights from CDRs datasets leads to coarse-grained detection frequency (e.g., at most once a day), giving time to fraudsters to profit from their light initial investment. As a bridge to the gap of such limitations, this chapter explores a relatively novel data type in the *SIMBox* fraud detection literature, i.e., cellular signaling traces valuable for their (i) robustness to the fraud evolution and (ii) ability for real-time detection.

We introduce *SigN*, a novel *SIMBox* detection system intended to be deployed at the cellular network edge. *SigN* analyzes the standardized cellular network signaling messages exchanged between user devices and the network, from a real cellular core and access networks deployed inside a Faraday Cage. From such analyzes it infers a real-time distinction between fraudulent and legitimate devices based on the latency of the network attachment procedure.

In the following sections, we elaborate on *SigN* methodology and the related experimental analyses as a follow-up to an overview of cellular signaling-based detection.

7.1 Cellular signaling-based detection

This section introduces the analysis of signaling messages for *SIMBox* fraud detection. It first discusses the corresponding motivation, then elaborates on related literature limitations to spotlight the requirements of signaling-based detection.

7.1.1 Motivation

Cellular signaling, unlike call audio, has the advantage of being *easily accessible as logs* recorded at multiple nodes in an operator network. Besides, it is framed by the 3GPP standards for mobile network security and operation and conveys user devices' information that, although *not private*, can serve to identify the fraud. Such thorough standardization causes *fraudsters to have limited control* over such datasets, mainly involving the operators' components (i.e., Operator-provided SIM cards inside the *SIMBox* and Operator's cellular antennas). Furthermore, signaling data is generated at the network protocol level, prior to any traffic (call/SMS/data) generation and thus to any induced communication behavior. Therefore, unlike CDRs, cellular signaling is *utterly resilient to all advanced fraud techniques* that aim to disguise fraudulent users' communication behavior. At last, cellular signaling procedures are speedy in the range of milliseconds so as not to be perceptible to the end-users, *paving the way for "real-time" detection* to stop the fraud before any damage.

7.1.2 Literature limitations

Here we narrow our focus to the only work of the literature that similarly considers signaling data for *SIMBox* fraud detection. Oh, et al. [120] has been recently published in a top-ranked security venue and proposes a fingerprint-based prevention methodology to mitigate *SIMBox* appliance (i.e., precisely gateways) access to the network. In the following, we use the term "ACL" to refer to this methodology.

7.1.2.1 Description

ACL analyzes signaling messages generated during the LTE attachment procedure. From the extraction of as many as 31,118 Mobile Equipment (ME) models software and firmware-related features inside the "Attach request" and "UECapabilityInformation" messages, it empirically shows that smartphones are fingerprintable. Likewise analyzing LTE *SIMBox* gateways and IoT devices, the paper concludes that *"without the supplier's support or using the same chipset of smartphones"* reproducing smartphones' fingerprints will be difficult for fraudsters. Yet, the impersonation of IoT devices is more accessible. Based on that, the authors propose a two-stage access-list policy strictly enforcing IoT devices to get registered at the operator before attachment. First, the approach compares ME fingerprint and **IMEI** codes to those recorded in a database. Then, in phase 2, ACL rejects non-registered IoT devices with voice call subscriptions.

Table 7.1: Fingerprint differing field's values

Mobile Equipment (ME)	Release Year	NAS			RRC				
		UE network capability (A)	access Stratum Release	ue-Category	supported ROHC profiles	supported BandList EUTRA	supported BandList UTRA-FDD	supported BandList GERAN	nonCritical Extension Parameters (B)
Samsung Galaxy S3 (S3)	2012	$A_{S3} = \{\dots\}$	rel9	3	None	3, 7, 20	I, V, VIII	gsm850, gsm900E, gsm1800, gsm1900	$B_{S3} = \{\dots\}$
<i>SIMBox</i> Hybertone LTE GoIP8 (GoIP8)	2012	$A_{GoIP8} = A_{S3} + 128\text{-EEA2} + 128\text{-EIA2}$	rel10	4	RTP(1), UDP(2)	3, 7, 20, 1, 28, 8	I, VIII	gsm900E, gsm1800	$B_{GoIP8} = B_{S3} + \text{loggedMeasurementsIdle-r10} + \text{standaloneGNSS-Location-r10}$
Samsung ZFold 5G (ZFold)	2020	$A_{ZFold} = A_{S3} + 128\text{-EEA2} + 128\text{-EIA2}$	rel15	4	RTP(1), UDP(2)	3, 7, 20, 1, 28, 8, 41, 38, 2, 4, 12, 13, 17, 18, 19, 25, 26, 39, 40, 64	I, II, IV, V, VIII	gsm850, gsm900E, gsm1800, gsm1900	$B_{ZFold} = B_{S3} + \text{loggedMeasurementsIdle-r10} + >200 \text{ other parameters (including 63 CA-related ones)}$

7.1.2.2 Limitations

We identified a set of limitations to ACL effective capability to mitigate the fraud, discussed hereafter:

- First, ACL considers a *mild threat model* in which fraudsters cannot collaborate with the *SIMBox* appliance providers, thus limiting their capabilities to modify their fingerprint. Such collaborations are, however, regular in practice. For instance, GoAntiFraud [57] is a cloud-based service assisting *SIMBox* termination businesses. Since 2013 they have helped over 2000 fraudsters in more than 31 countries. In addition, they have partnerships with various *SIMBox* manufacturers from which they can obtain and configure such devices' software according to their client (i.e., *SIMBox* fraudsters) needs. More critically, Antrax [7] is a company that covers all stages of the international termination business, from *SIMBox* manufacture to the hiring and assistance of *SIMBox* fraudsters. They provide "*specialty tailored world-known hardware and software for ready-made call termination business*" and thus can modify both *SIMBox* firmware and software, adjusting their generated fingerprint.
- The previous more severe *yet actual* threat model considers fraudsters can access any phone's fingerprint using an open-source LTE stack and an SDR-based eNB as done in [120]. *SIMBox* fraudsters are thus able to precisely determine what to modify to reproduce a specific phone's fingerprint, which would guarantee not to be detected by ACL. Accordingly, although ACL fingerprint includes device's capabilities information that might cause network communication failure if modified, we assess how feasible it would be for a fraudster to copy a phone fingerprint.

ACL's fingerprint includes "[NAS] attach request," relating to the core network **ME**'s functions, and "[RRC] UECapabilityInformation," relating to the **ME**'s radio-access capabilities, such as the supporting radio frequency, carrier aggregation (CA) configuration and radio resource scheduling. As highlighted in [120], the latter capabilities are the best facet to distinguish *SIMBox* appliances, with a unique antenna per baseband, compared to smartphones, supporting carrier aggregation (CA), i.e., multiple frequencies simultaneously. From such

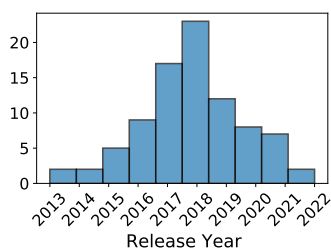


Figure 7.1: Distribution of release year of ACL’s tested phones.

observation, we reason that *SIMBox* fraudsters would, therefore, preferably copy old or “non-smart” phones not supporting advanced radio-access capabilities. Furthermore, as Fig. 7.1 confirms that all ACL’s tested phones were released from 2013 to 2021, we compared, using the testbed described in §7.2.2, the fingerprint of (i) a 2012-released phone (i.e., Samsung Galaxy S3/S3), (ii) a 2012-released *SIMBox* gateway (i.e., Hybertone LTE GoIP8/GoIP8) and (iii) a 2020-released phone in the device set of ACL (i.e., Samsung ZFold 5G/ZFold). Table 7.1 reports fields with differing values for the 2012-phone and the 2012-*SIMBox* gateway. First, apart from two bits, all NAS-mandatory information in ACL’s fingerprints are similar for both MEs. Regarding RRC, the difference is light regarding the number and content of the fields relative to the 2020-phone. Generally, the 2012-phone-supported capabilities are included in the *SIMBox* gateway ones, easing required adjustments by the fraudulent parties. Also, the last column highlights that the 2020-phone supports many more capabilities than the 2012-phone, including 63 more CA-related features, justifying conclusions drawn in [120]. Our study demonstrates it is manageable for *SIMBox* fraudsters to reproduce an old phone fingerprint and thus circumvent ACL control.

- Third, a significant limitation of ACL is that the considered fingerprint is based on 3GPP specifications, [3] for NAS and [2] for RRC, which are constantly evolving. Such an evolution directly impacts ACL’s scalability, whose first phase is manually checking these specifications to identify the information expected from UEs. Specifically, a study of these specifications updates in the last five years, as depicted in Fig. 7.2, shows an update on average every three months. Therefore, the manual checking of specifications implies searching at each update through the whole voluminous document or its numerous references to the introduced modifications. Moreover, several releases of a specification can be maintained simultaneously, as shown in Fig. 7.2b, giving each UE a choice to dock to a release that ACL should be able to track. All these considerations make ACL implementation difficult in practice.
- At last, ACL is vulnerable to *unknown* cases. Indeed, it relies on a database of fingerprints with corresponding device model identifiers (i.e., the first eight digits of the IMEI, called Type Allocation Code/TAC). Unfortunately, the detection decision is incapacitated if an attaching device model’s TAC and corresponding fingerprint are not yet in the database. Hence, using new *SIMBox* models not yet known in the market or simply modifying to new

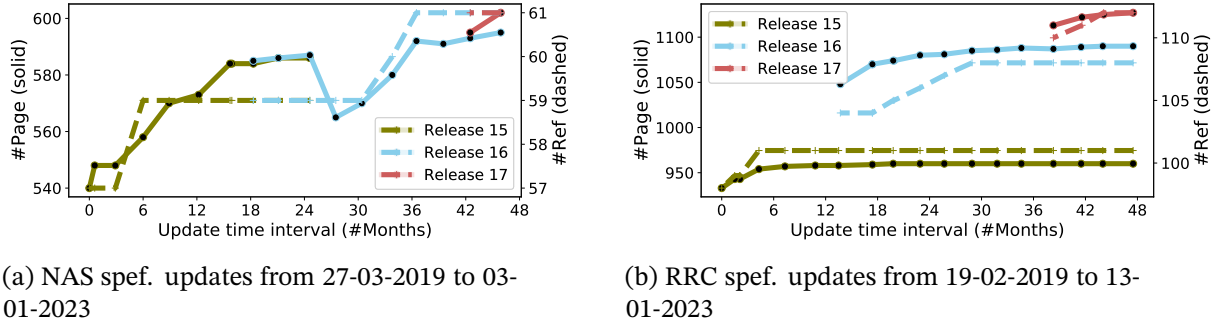


Figure 7.2: NAS[3] and RRC[2] protocol specifications size

existing fingerprints is enough for fraudsters to evade ACL.

7.1.2.3 Summary

From the above analysis, we conclude that although exploiting cellular signaling, ACL methodology has two main shortcomings: (i) *it relies on features that fraudsters can alter*, i.e., the network capabilities of the *SIMBox* appliances they produce, and (ii) *it is complex to implement requiring constant maintenance* in terms of protocol specifications and phone models updates, without which its effectiveness is significantly reduced.

Given these limitations, the following section highlights the requirements for a suitable signaling-based *SIMBox* fraud detection solution.

7.1.3 Goal

The threat model we consider does not limit fraudsters' hardware and software adaptation capabilities. Therefore we aim to develop detection solutions with in mind the following properties: (1) solutions should *remain efficient regardless of fraud enhancement*, thus relying on factors beyond the reach of fraudsters. (2) solutions should be *based on properties whose ease of modification severely limits the fraud effectiveness*, thus facilitating its detection. (3) solutions should be *simple* and require little nonconstant effort on the operator side to be widely deployed on the network surface.

7.2 SigN prevention system

Responding to highlighted detection goals, we propose *SigN*, a *SIMBox* fraud detection system based on the cellular signaling latency perceived at the network edge. This section first presents *SigN* intuition describing how it meets identified goals, then describes our experimental setup, and at last discusses obtained results.

7.2.1 Intuition

Our detection intuition is based on *SIMBox appliances signaling having relatively high latency compared to regular devices due to the SIMBox architecture*.

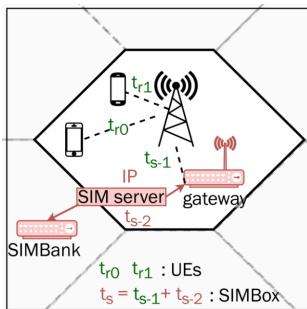


Figure 7.3: Regular and *SIMBox* UEs signaling latency.

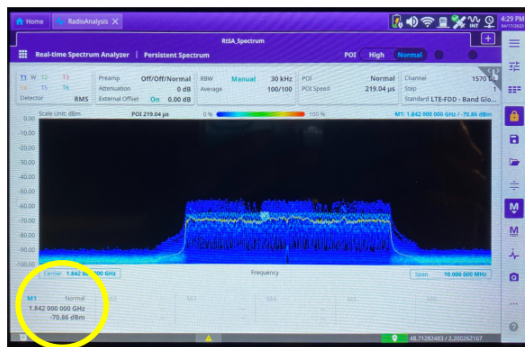


Figure 7.4: Analysis of received signal power inside the testbed (y-axis: signal power (dBm); x-axis: frequency)

Indeed, *UEs* in cellular networks are a combination of the *ME* and the *SIM* with an active subscription for interaction with the cellular network. For the *SIMBox UEs*, the combination of the *ME* (gateway) and *SIM* cards is either *manual* in the standalone *SIMBox* architecture or *logical* at the level of the *SIM* server in the distributed architecture. Yet, most *SIMBox* deployments are distributed due to the limitations induced by *SIMBox* standalone architecture described below. Thus, as shown in Fig. 7.3, the communication latency of *SIMBox UEs* $t_s = t_{s-1} + t_{s-2}$ where $t_{s-1} \approx t_{r0} \approx t_{r1}$ is the regular latency due to signaling operations processing and wireless signal propagation within the cell. On the other hand, t_{s-2} is the latency overhead experienced by *SIMBox* due to the interaction of its components in an *IP* network.

Such latency overhead may be identified at the network's base station. Thus *SigN* detection method based on signaling latency analysis fulfills goals (1), (2), and (3) as follows.

- (1): Fraudsters can hardly prevent their signaling latency overhead, depending on parameters out of their reach, such as the size of standardized cellular signaling messages or the required number of signaling exchanges between the *ME* and the *SIM* card. Moreover, vagaries related to Internet link quality between *SIMBox* appliances may also impact.
- (2): Although such a detection intuition is based solely on the distributed architecture of *SIM-Box*, switching to a standalone architecture would be very costly for fraudsters. Not only does this limit the number of calls that can be hijacked to the features of a single *SIMBox* gateway, but it also makes it impossible for fraudsters to apply human mobility simulation to their *SIM* cards [54], yielding straightforward detection through literature CDR-based approaches.
- (3): Inspecting signaling latency is straightforward and has already been implemented as timers for other purposes in LTE. For instance, the timer T300 [2] is used by the eNodeB to keep track of the RRC Connection Request messages it receives from the *UE* and determine whether it should initiate the RRC connection setup procedure. Such *SigN* lightness guarantees its ease of implementation at the eNodeB nodes.

In an effort to validate such detection intuition, we experimentally analyze cellular signaling latency per *UE* to build the *SigN* detection approach. Precisely, *SigN* focuses on the *UEs'* latency during the network attachment procedure, that fraudster should mandatorily carry

out to connect to the network.

7.2.2 Experimental setup

The testbed used in this study relies on a 4G Amarisoft suite deployed inside an $30m^2$ Faraday shield. The specifications of used components are detailed in Table 7.2. We use a single PC to host the base station and core network nodes (MME, IMS, and SGW). This PC is in charge of the baseband processing, while the Software-Defined Radio (SDR) processing is handled by a USRP B210 [48] connected to the PC through an USB3 interface. The baseband processing communicates with SDR via a libuhd 4.3.0 TRX API.

The testbed deploys a single 4G cell whose radio parameters are described in Table 7.2. Using a VIAVI Radio spectrum analyzer [147], we validate the Reference Signal Received Power (RSRP) at the level of UEs to be around -71dBm (cf. Fig. 7.4) reflecting an excellent signal quality in real urban scenarios measurements [94].

Our testbed includes 12 phones from six distinct vendors and 7 SIMBox appliances from two manufacturers. Such devices are equipped with Sysmocom programmable SIM cards [152], whose PLMN is set to the one of the shielded LTE network. SIMBox control server software is hosted in LAN-connected Ubuntu-Server and Windows 7 PCs according to Hybertone and Portech requirements. Such PC hardware specifications are described in Table 7.2. We use the acronyms SIMBoxHYB_std and SIMBoxPOR_std to refer to the deployment of the standalone architectures of the Hybertone and Portech SIMBox models respectively, as well as SIMBoxHYB_dis and SIMBoxPOR_dis for the corresponding distributed architectures.

7.2.3 Network attachment latency

Methodology. For each phone type and SIMBox architecture, we carry out 50 executions of the attach procedure. The generated cellular signaling logs from such attach procedures are collected at the level of the eNodeB. For each message we use the following associated fields for latency computation: time layer direction ue_id message. The direction, i.e., Uplink/Downlink, indicates the message originator as the UE/the network, respectively. We consider NAS-layer messages only, as they provide information of the signaling between the UE and the core network during the attach procedure (cf. Table 7.3). Therefore, we compute the latency of each step as $L_i = T_i - T_{i-1}$, i.e., the delta time between the arrival of a message i and its previous one $i - 1$. Depending on the message direction, L_i refers to the network's or the UE's processing time along with the message transmission time to the eNodeB. The total attach procedure latency of an UE is thus $\sum_{i=1}^{10} T_i - T_{i-1}$.

Results. Table 7.3 reports the obtained latency's average values and standard deviation for each step of the network attach procedure. A particular interest is on the lines where the UE responds to a network request (text in column 2 in red), enabling us to determine and compare the processing time per UE type. Note that some UEs (e.g., SIMBoxPOR) may not execute the identity request if their attach request already includes the UE's identifier (IMSI).

Table 7.2: Testbed components specifications

Parameters		Values
Host PC (BS, MME, SGW)		Intel(R) Core(TM) i9-10900K CPU@3.70GHz, 16GB RAM, Gigabit Ethernet controller
Cell	Bandwidth	5MHz FDD
	Configuration	SISO
	Frequency	Downlink center frequency: 1845 MHz, Band 3
Programmable SIM card		SysmoSIM-SJS1 de Sismocom
Mobile phones	Samsung Galaxy Note 4 (x3)	
	Samsung Galaxy S3	
	Xiaomi Redmi Note 9	
	Xiaomi 10 Lite 5G (x2)	
	FairPhone 4 5G	
	OnePlus Nord Model 5G	
	Sony XPERIA	
	Samsung galaxy Z Fold2 5G	
SIMBox appliances	Hybertone - SIMBank: SMB32 - Gateway: GoIP8 (x2) - Server v. 2022-5-11 (Host PC: Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz, 8GB RAM, Gigabit Ethernet controller)	
	Portech - SIMBank: SBK-32 - Gateway: MV-374 - Server SS-128 (Host PC: Intel(R) Core(TM) i7-4610M CPU @ 3.00GHz, 16GB RAM, Gigabit Ethernet controller)	

Similarly, the network determines the ESM information request inclusion in case of the need for additional information about the UE, such as its supported EPS bearers or QoS parameters. Regardless of the phone type, all phones have comparable latencies per step, similar to the *SIMBox* standalone architectures. However, distinguishing from those mentioned above, the latency overhead in distributed architectures of the two *SIMBox* types is significantly higher compared to the related standalone architectures ($\approx 9\times$ for Hybertone and $\approx 5\times$ times for Portech). Such overhead emerges at step 4 (authentication response), which consists of mutual authentication of the network and UE, following the AKA procedure in LTE [131]. It requires the UE to send in response to the network the authentication vectors (RAND, AUTN, XRES, KASME) from an internal computation of the SIM card (in the SIMBank) as requiring its secret key K_i . In this step, the time t_{s-2} of inter-*SIMBox* component IP communication is thus necessarily imputed, explaining the overhead.

7.2.4 Prevention algorithm

SigN implementation in an operator network monitors user devices' authentication response latency. According to LTE specifications [47], this is already done through the timer T3460 attesting to the lightness of *SigN* methodology and guaranteeing its potential for real-time large-scale deployment. In the following, build upon LTE timing mechanisms to propose a *SigN* algorithm adapted to *SIMBox* fraud mitigation.

In LTE, the network initiation of an authentication procedure is associated with the start

Table 7.3: Latency (in ms) per UE model reported per network attachment step

Step	Direction	FairPhone 5G	GalaxyA90	GalaxyNote4	GalaxyS3	GalaxyZfold2 5G	OnePlus Nord	Sony XPERIA	Xiaomi10 Lite5G	Xiaomi9 Pro5G	SIMBoxHYB_std	SIMBoxHYB_dis	SIMBoxPOR_std	SIMBoxPOR_dis
0. Attach request	UE \Rightarrow eNB	0	0	0	0	0	0	0	0	0	0	0	0	0
1. Identity request	UE \Leftarrow eNB	1 \pm 0	1 \pm 0	1 \pm 0	0.9 \pm 0.3	1 \pm 0	1 \pm 0	1 \pm 0	1 \pm 0	1 \pm 0	1 \pm 0	0.9 \pm 0.2	/	/
2. Identity response	UE \Rightarrow eNB	31 \pm 0	27 \pm 6	38.3 \pm 2.3	31.0 \pm 10.4	31 \pm 0	31.8 \pm 2.4	25.0 \pm 6.4	31 \pm 0	31 \pm 0	31.8 \pm 3.5	31.0 \pm 4.3	/	/
3. Authentication request	UE \Leftarrow eNB	1 \pm 0	1 \pm 0	1.0 \pm 0.3	1 \pm 0	1 \pm 0	1 \pm 0	1 \pm 0	1 \pm 0	1 \pm 0	1 \pm 0	0.9 \pm 0.3	0.9 \pm 0.1	1 \pm 0
4. Authentication response	UE \Rightarrow eNB	57.6 \pm 11.4	74.1 \pm 22.1	84.5 \pm 36.5	67.9 \pm 12.2	70.2 \pm 18.2	69.8 \pm 10.0	69.1 \pm 5.9	69.9 \pm 8.2	67.9 \pm 16.2	71.7 \pm 10.8	2122.7\pm309.9	71.2 \pm 10.7	1640.2\pm286.7
5. Security mode command	UE \Leftarrow eNB	1 \pm 0	1 \pm 0	1 \pm 0	1 \pm 0.1	1 \pm 0.1	1 \pm 0	1 \pm 0	1 \pm 0	1 \pm 0	1 \pm 0	0.9 \pm 0.3	1 \pm 0	1 \pm 0
6. Security mode complete	UE \Rightarrow eNB	20.5 \pm 3.2	19.3 \pm 1.6	37.0 \pm 6.3	33.0 \pm 9.5	21.8 \pm 14.3	31.3 \pm 12.5	19.6 \pm 2.6	21.9 \pm 4.6	21.8 \pm 10.5	22.4 \pm 5.9	20.1 \pm 3.7	19.7 \pm 2.7	21.1 \pm 5.8
7. ESM information request	UE \Leftarrow eNB	1 \pm 0	1 \pm 0	0.9 \pm 0.2	/	1 \pm 0	1 \pm 0	1 \pm 0	1 \pm 0	0.9 \pm 0.1	1 \pm 0	1.0 \pm 0	/	/
8. ESM information response	UE \Rightarrow eNB	19 \pm 0	19.7 \pm 2.6	37.3 \pm 5.5	/	22.8 \pm 21.4	26.2 \pm 9.3	19.6 \pm 2.3	22.6 \pm 5.6	20.7 \pm 4.2	22.9 \pm 5.8	20.6 \pm 3.9	/	/
9. Attach accept	UE \Leftarrow eNB	50.4 \pm 4.8	48.7 \pm 2.5	66.2 \pm 6.8	56.9 \pm 8.7	50.0 \pm 4.4	66.5 \pm 14.3	50.9 \pm 5.9	48.8 \pm 3.9	49.3 \pm 4.3	46.9 \pm 10.3	43.7 \pm 9.3	50.7 \pm 6.8	57.9 \pm 26.1
10. Attach complete	UE \Rightarrow eNB	32.4 \pm 1.9	32.8 \pm 3.4	49.7 \pm 7.1	60.1 \pm 1.1	34.3 \pm 6.0	35.5 \pm 8.2	54.5 \pm 6.4	38.8 \pm 3.9	33.5 \pm 4.1	57.3 \pm 10.1	53.2 \pm 9.5	78.5 \pm 6.8	52.2 \pm 4.7
Total		215.0 \pm 21.3	225.6 \pm 38.2	316.8 \pm 65.5	251.9 \pm 42.4	234.2 \pm 64.6	256.6 \pm 44.8	242.8 \pm 29.5	237.1 \pm 33.5	228.2 \pm 38.5	257.1 \pm 42.7	2295.5\pm341.7	253.9 \pm 31.3	1773.5\pm323.3

of the timer T3460, whose default value is 6s. Therefore the UE shall respond with an "authentication response" message within T3460. On the first expiry of the timer T3460, the network retransmits the "authentication request" message as well as resets and starts timer T3460. This retransmission is repeated four times, i.e., on the fifth expiry of timer T3460, the network aborts the authentication procedure and releases the NAS signaling connection. To the best of our knowledge, LTE standards give no support to the default T3460 value of 6s, which can be easily modified by any operator. For instance, Amarisoft 4G suite provides a configuration file in which the value of T3460 can be set.

According to our experimental evidence, such a default value is large enough for a seamless connection to the network of SIMBox fraudulent devices. Hence, the algorithm 1 introduces a threshold range of $[T3460_1 = 500ms, T3460_2 = 1000ms]$ for authentication response latency. The network operator initiates the authentication procedure with T3460 set to $T3460_2 = 1000ms$. It next sends a maximum of 5 authentication requests waiting in case of timer expiry and then stops the signaling connection. However, if an authentication time is more than $T3460_1 = 500ms$, instead of a direct authentication, it makes three other authentication requests and counts the number of times such authentications take more than 500ms. If this number exceeds 2, the UE can be considered dubious and is refused to join the network.

Here, we choose the value of 500ms as being the maximum phone-related time (transmission and processing combined) in our measurements. Similarly, the timer value of 1000ms is empirically defined by all SIMBox authentication times greater than 1000ms. The adjustable threshold frame is, therefore, to minimize possible (yet unlikely) false positives. As a result, such an algorithm has a 100% accuracy, recall, and precision from our testbed measurements.

Algorithm 1 SigN authentication procedure

```

1: procedure AUTHENTICATIONPROCEDURE( $T_{3460_1} = 500ms, T_{3460_2} = 1000ms$ )
2:    $retry \leftarrow 0$ 
3:    $timeoutCount \leftarrow 0$ 
4:   while  $retry < 5$  do
5:      $startTime \leftarrow \text{CURRENT\_TIME}$ 
6:     SEND_AUTHENTICATION_REQUEST
7:      $response \leftarrow \text{WAIT\_FOR\_RESPONSE}(T_{3460_2})$ 
8:      $elapsedTime \leftarrow \text{CURRENT\_TIME} - startTime$ 
9:     if  $response$  is not None and  $elapsedTime \leq T_{3460_1}$  then
10:      return  $response$ 
11:     else if  $response$  is not None and  $elapsedTime > T_{3460_1}$  then
12:        $i \leftarrow 0$ 
13:       while  $i < 3$  do
14:         SEND_AUTHENTICATION_REQUEST
15:          $response_i \leftarrow \text{WAIT\_FOR\_RESPONSE}(T_{3460_1})$ 
16:         if  $response_i$  is None then
17:            $timeoutCount \leftarrow timeoutCount + 1$ 
18:         end if
19:          $i \leftarrow i + 1$ 
20:       end while
21:       if  $timeoutCount \geq 2$  then
22:         return None
23:       else
24:         return  $response_i$ 
25:       end if
26:     end if
27:      $retry \leftarrow retry + 1$ 
28:   end while
29:   return None
30: end procedure

```

7.3 Discussion

The preliminary experimental analyses of UE's network attachment latency confirm a *SIMBox* latency overhead in the distributed architecture, primarily at the authentication phase. Despite being straightforward, SigN algorithm and results are impactful as described in the following:

- First, despite relying only on the UE's authentication computation, SigN ensures multiple opportunities to detect SIMBox appliances. Indeed, *SIMBox* distributed architectures generate regular attach procedures to the network. Precisely, each simulation of human movement by logically binding a SIM card to another cellular antenna triggers a new connection to the network. Such simulated movements occur several times weekly for a realistic mimicking of human mobility, evading CDR-based literature detection. In addition, an operator network has the flexibility to initiate at any time an authentication procedure when a signaling connection exists [47].

- Second, *SigN* related facilities of implementation and wide deployment for the operators are enormous and will allow important economic spin-offs as compared to state-of-the-art solutions.
- Second, although *SigN* intuition is uniquely related to distributed *SIMBox* architectures, the standalone architecture is very costly for fraudsters. Not only does it limit the number of calls that can be diverted to the capabilities of a single gateway, but it also prevents the application of *SIMBox* SIM card migration and rotation techniques, ensuring direct detection by CDR-based approaches in the literature.
- Last but not least, *SIMBox* fraudsters can hardly evade this solution. *SigN* robustness relies on parameters out of fraudsters' reach, such as the standardized number of *SIMBox* components interactions and processing as well as the quality of the Internet connection between such components, which varies depending on the provider and the location.

The future steps of this work are to inspect *SigN* pinpointed latency overhead to provide explainability and verify its generability regardless of the considered *SIMBox* model. On the other hand, we plan to delve deeper into legitimate signaling latency to spotlight its boundaries.

7.4 Summary

This chapter presented practical evidence of cellular signaling data relevance for *SIMBox* fraud detection, highlighting its capabilities for real-time distinction and resilience to *SIMBox* human behavior simulation functionalities. Through an in-depth investigation of the related work limitation, we came out with essential requirements of a cellular signaling-based detection solution, namely (i) to rely on fraudsters-unalterable properties, (ii) to rely on properties costly to circumvent, and (iii) simplicity. We subsequently proposed *SigN* as a straightforward and efficient detection system of *SIMBox* frauds in the network edge based on the cellular signaling latency during the authentication phase. Future work will investigate the generality of *SigN* efficiency in broader realistic scenarios.

Conclusion

Contents

8.1	Contributions summary	94
8.2	Limitations	96
8.3	Short-term perspectives	97
8.4	Long-term perspectives	97

This thesis has focused on *SIMBox* bypass frauds in cellular networks, tackling its understanding and mitigation. Hereafter we draw the related conclusions.

8.1 Contributions summary

Faced with the severe impact of *SIMBox* bypass fraud on several scales (network operator revenues, network quality and research, humanitarian risk related to covert terrorism), this thesis' contributions can be summarized in three main objectives:

Goal 1: Facilitate research on *SIMBox* fraud. We first identified that research on the domain was paralyzed by the inherent privacy of the datasets holding *SIMBox* fraud traces. The induced difficulty in such datasets sharing has hindered the fraud's in-depth knowledge and the development of detection solutions.

Thus, we surveyed significant sources beyond the scientific literature to provide all the elements for an utter understanding of the fraud ecosystem. This survey revealed how fraud techniques evolve over time to oppose detection. Active detection methods (i.e., Test call generation and Rule-based management) are mastered and manipulated by fraudsters to their advantage (cf. §3.3). And, fraudsters have been innovating in the artificial reproduction of human communication behavior known as Human Behavior Simulation, to counter passive detection techniques.

This led us to focus on the Charging Data Records (CDRs) datasets primarily used in the literature for *SIMBox* fraud investigations. Accordingly, we implemented a scalable *SIMBox* simulation environment, i.e., *FraudZen*, to provide broad access to CDRs with realistic, legitimate, and fraudulent profiles. The faithful reproduction of *SIMBox* appliances' functionalities and their related strategies guarantee the realism of the *fraudulent traffic* generated in *FraudZen*. Moreover, we designed, traffic and mobility models of legitimate users, i.e., *Zen*, based on real-world traffic CDRs and mobility traces. Using *Zen* modeling inside the simulator, we validated the ability of *FraudZen* to generate realistic, *legitimate traffic* valuable for real applications beyond *SIMBox* fraud research.

This contribution equips the scientific community with complete CDRs traces free of past/current fraud strategies, giving the flexibility to anticipate the fraud evolution to advance research.

Goal 2: Develop detection resilient to the fraud evolution. We pointed out one major challenge to the fraud investigation, which is the constant evolution of *SIMBox* appliances capabilities making it difficult to leverage the proposed detection approaches. To fill this gap, we introduced a new paradigm that considers detection methods not only in terms of accuracy and precision *but also values their resilience to the evolution of fraud*. For this purpose, we proposed the first-of-the-literature *SIMBox* fraud modeling as a framework allowing the definition of a fraud's behavior ahead of its simulation in *FraudZen*. Furthermore, by calibrating the efficiency of defined fraud models by our conceived "*in_crowd_blending_capability*" metric, we evaluated the impact of various fraud and detection parameters on the detection performances.

For instance, the distinction of each assessed behavior (traffic, mobility, and social) in fraud detection showed us that compared to traffic and social behaviors, users' mobility behavior presents the best facet to distinguish between fraudulent and legitimate users (cf. §6.4.4). We further highlighted that the *mobility uniqueness* behavioral trait is a vulnerability to fraud, being hardly counterfeited by *SIMBox* architectures (§6.4.7). We therefore recommend a deeper exploitation of detection features based on such mobility behaviors.

Added to that, we could assess how the percentage of fraudulent incoming traffic (cf. §6.4.5) and the tackled fraud model efficiency (cf. §6.4.6) affects fraud detectability. We also studied how detection performs in realistic scenarios where datasets may include several attack patterns that are not a priori known. Our study revealed that considering several fraud models at once negatively impacts detection performances, especially in the presence of advanced fraud models inducing a loss in precision. Therefore we suggested exploiting *FraudZen* capabilities to handle each fraudulent behavior in detection separately.

Goal 3: Introduce manageable real-time solutions to the fraud. Motivated by the criticality to consider the in detection design as a response to the rapid fraud earnings, we explored a novel type of data in the *SIMBox* fraud detection literature. Precisely, we experimentally investigated on-top-of an established Faraday cage test-bed a detection track based on cellular signaling latency. Using 10 mobile phones from five different vendors and three *SIMBox*

appliances from the most prevalent manufacturer of the international market, we built proof-of-concept validations of such tracks while discussing their applicability in real-world deployments. Our study revealed that the *SIMBox* distributed architectures have an average latency 40 times higher than conventional phones, allowing distinguishing such devices at the cellular network attachment easily.

8.2 Limitations

Despite their broad applicability, this thesis's contributions present some limitations we want to highlight in this section.

Complete datasets unavailability: The work we conducted in modeling and validating legitimate and fraudulent CDRs exploited an incomplete CDRs dataset missing mobility context (cf. §5.1.2). Indeed, mobility-related data contain potentially sensitive professional and personal information; they are among the most sensitive data currently being collected [106]. For instance, solely relying on location data, a person's home location, attendance to a particular religious or political building, or presence in a motel or abortion clinic can be inferred [106]. As such, even anonymized mobility information is scarcely shared, preventing us from benefiting from their related preciseness in the framework of our study. The direct implication in *Zen* CDRs generation is that our modeling could not capture the implicit correlations between mobility and traffic information. We separately built realistic and well-validated models for users' traffic and mobility. However, the combination of such separated models was based on simplistic heuristics and ought to be improved in future works. In the same vein, such simplification impacts fraud-related analyses to some extent. Even though mobility-related insights compared fraudulent and legitimate users relative to the same (simplified) context, there is still a reasonable bias, related to the realism of users' mobility decisions according to their traffic behavior, with a bounded effect on our conclusions.

Lack of fraudulent ground truth: A bounce-back effect of limited operator detection capability is that they are often unable to indicate any ground truth knowledge on which users are fraudulent in the provided dataset. Accordingly, our *FraudZen* contribution (combined with our *SIMBox* fraud modeling) could not undergo a first-step validation of analogizing the generated CDRs to real-world fraudulent ones. This would have, however, served as a direct attestation of the high fidelity of *SIMBox* appliances implementation inside *FraudZen*. Yet, we could circumvent this shortcoming by showing that the generated CDRs for the advanced fraud models effectively counter the most prominent detection of the current literature. Considering the nowadays operators' incomplete awareness of fraudulent behavior presence in their CDRs, *FraudZen* is the first and unique (to the best of our knowledge) way to investigate *SIMBox* fraud evolution and implication on implementable detection strategies.

Experimentation generality: In spite of the evidence of drawn conclusions regarding the timely distinction between *SIMBox* appliances and legitimate ones by leveraging cellular signaling data, one can still question the generality of such results. Indeed, our experiment set

included a unique *SIMBox* vendor, gateway, and *SIMBank* models. Although such a vendor is acknowledged as the most prevalent in the international market, there is no strict guarantee that other vendors or models will yield the same results. As underlined in the related chapter (cf. chap 7), our analyses, therefore, serve as a proof-of-concept that still compels to be generalized in future works.

8.3 Short-term perspectives

Capturing real-world mobility to traffic correlations: As mentioned early, the mobility generation in *Zen* modeling is still open for improvement. Notably, the generation of complete CDRs, including a realistic correlation of users' trajectories to traffic generation habits, has never been tackled in the literature. Such an interesting problem requires generative models with enough expressive power (i) to track both users' mobility and traffic sequences, (ii) tackle CDRs mobility temporal and spatial heterogeneity, and (iii) adapt to irregularities in telecom network topologies and population lifestyle context.

Leveraging gotten detection insights: Following our second goal, i.e., develop detection resilient to the fraud evolution, we shed light on several insights for future research guidance. The next step consists of leveraging such experience in designing and validating efficient detection approaches.

Exploiting the "box of SIMs" architecture in detection: As shown in our studies, one of the fraud weaknesses is the rugged camouflage of multiple SIMs handling, from which the appellation *SIMBox* derives. However, until now, the literature on detection has always been built on distinguishing each fraudulent user individually, even though they are part of a set. Therefore, we envision a future direction to exploit the utter controllability offered by *FraudZen* to introduce a new approach in *SIMBox* fraud research: Considering that one or a few fraudulent SIM cards have been detected, how can it be exploited to uncover other SIM cards of their belonging architecture?

Alternative modeling approaches: LSTMs are perhaps the simplest neural network architecture (in terms of manual tuning) that can reliably model long-term dependencies and has the flexibility to be used jointly with other more complex architectures. For example, a Generative Adversarial Network (GAN) [164, 67] uses paired generator/discriminator networks to enable very realistic output. Our work provides the generator neural network that can be used inside the GAN in future investigations.

8.4 Long-term perspectives

Privacy vs individual precision: Although presenting ground truth modeling and validation opportunities, individual-based mobility modeling of real-world CDRs brings important privacy issues: As users' actual habits in mobility can be captured in the model, the generated CDRs have the weakness of revealing aspects in users' daily-life routine, such as important

locations (e.g., home/work), regular trajectories (e.g., preferred places for leisure, etc). Accordingly, to what extent *model extraction attacks*, in which an adversary can collect data through query access to a victim model, can be effective to such human mobility generative models is worth investigating. Also, the tradeoff between privacy compliance and preciseness in mobility modeling of CDRs is a relevant topic we let for future work.

Assessing the generality of SIMBox fraud modeling: Our proposed modeling of SIMBox frauds proved effective for generating advanced fraud models with an in-crowd-blending capability of 99.6% on average. However, such a result was obtained while comparing generated fraudulent behavior with a "unique crowd" of legitimate users from the CDRs dataset we analyzed. Therefore, further investigation would assess the generality of such modeling by applying it to legitimate users' datasets collected in different contexts. This will help uncover whether and to what extent fraudsters must adapt their communication behaviors to a target zone or if a fraud model's efficiency is identical regardless of the considered legitimate crowd.

Boosting with adversarial ML defenses: In adversarial machine learning terms, SIMBox fraudsters are persistently generating *adversarial examples* [63] to fool trained detection models with fraudulent users profiles seemingly legitimate. Faced with this, our proposed SIMBox fraud modeling, capturing the fraud action areas, can be leveraged in future works for the application of well-known literature defenses such as adversarial training, i.e., train the model to distinguish adversarial examples, or defensive distillation, i.e., train "distilled" models based on detection uncertainties.

Bibliography

- [1] 3GPP. *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access*. Tech. rep. TS 23.401. 3GPP, 2022. URL: https://www.3gpp.org/ftp/Specs/archive/23%5C_series/23.401/23401-i00.zip (cit. on p. 17).
- [2] 3GPP. *LTE RRC Protocol Specification*. Tech. rep. TS 36.331. 3rd Generation Partnership Project (3GPP), 2023. URL: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2440> (cit. on pp. 85–87).
- [3] 3GPP. *Non-Access-Stratum (NAS) Protocol for Evolved Packet System (EPS); Stage 3*. Tech. rep. TS 24.301. 3rd Generation Partnership Project (3GPP), 2023. URL: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1072> (cit. on pp. 85, 86).
- [4] M. R. AlBougha. “Comparing Data Mining Classification Algorithms in Detection of Simbox Fraud”. MA thesis. St. Cloud State University, 2016-12 (cit. on pp. 21, 28, 35).
- [5] Y. Alraouji and A. Bramantoro. “International Call Fraud Detection Systems and Techniques”. In: *Proceedings of the 6th International Conference on Management of Emergent Digital EcoSystems*. MEDES '14. Buraidah, Al Qassim, Saudi Arabia: Association for Computing Machinery, 2014, pp. 159–166. ISBN: 9781450327671. DOI: [10.1145/2668260.2668272](https://doi.org/10.1145/2668260.2668272) (cit. on pp. 21, 27).
- [6] L. Amichi, A. C. Viana, M. Crovella, and A. A. Loureiro. “Understanding Individuals’ Proclivity for Novelty Seeking”. In: *SIGSPATIAL '20*. Seattle, WA, USA: Association for Computing Machinery, 2020, pp. 314–324. ISBN: 9781450380195. DOI: [10.1145/3397536.3422248](https://doi.org/10.1145/3397536.3422248) (cit. on pp. 6, 45, 52, 59).
- [7] ANTRAX. *Smart GSM Termination with ANTRAX Solutions*. Webpage. 2022. URL: <https://en.antrax.mobi/> (cit. on pp. 2, 67, 84).
- [8] Antrax. Webpage. URL: <https://en.antrax.mobi/> (cit. on p. 21).
- [9] Antrax. *Activity Period Script*. Commit hash ee1d40cf. Antrax. 2017-07. URL: <https://gitlab.com/flamesgroup/antrax/-/blob/master/doc/manual/scripts/activity-period-script.md> (cit. on pp. 21, 25).

- [10] Antrax. *Call Filter*. Commit hash ee1d40cf. Antrax. 2017-07. URL: <https://gitlab.com/flamesgroup/antrax/-/blob/master/doc/manual/scripts/call-filter.md> (cit. on p. 25).
- [11] Antrax. *Gateway Selector Script*. Commit hash ee1d40cf. Antrax. 2017-07. URL: <https://gitlab.com/flamesgroup/antrax/-/blob/master/doc/manual/scripts/gateway-selector-script.md> (cit. on pp. 21, 25).
- [12] Antrax. *HTTP request*. Commit hash ee1d40cf. Antrax. 2017-07. URL: <https://gitlab.com/flamesgroup/antrax/-/blob/master/doc/manual/scripts/business-activity-scripts/http-request.md> (cit. on pp. 21, 25).
- [13] Antrax. *IMEI Generator Script*. Commit hash ee1d40cf. Antrax. 2017-07. URL: https://gitlab.com/flamesgroup/antrax/-/blob/master/doc/manual/scripts/imei_gen_script.md (cit. on pp. 21, 25).
- [14] Antrax. *Session Period Script*. Commit hash ee1d40cf. Antrax. 2017-07. URL: <https://gitlab.com/flamesgroup/antrax/-/blob/master/doc/manual/scripts/session-period-script.md> (cit. on pp. 21, 25).
- [15] Antrax. *Sim Server Factor Script*. Commit hash ee1d40cf. Antrax. 2017-07. URL: <https://gitlab.com/flamesgroup/antrax/-/blob/master/doc/manual/scripts/sim-server-factor-script.md#sim-server-factor-script> (cit. on pp. 21, 25).
- [16] Antrax. *SMS*. Commit hash ee1d40cf. Antrax. 2017-07. URL: <https://gitlab.com/flamesgroup/antrax/-/blob/master/doc/manual/scripts/business-activity-scripts/sms.md> (cit. on pp. 21, 25).
- [17] Antrax. *USSD*. Commit hash ee1d40cf. Antrax. 2017-07. URL: <https://gitlab.com/flamesgroup/antrax/-/blob/master/doc/manual/scripts/business-activity-scripts/ussd.md> (cit. on pp. 21, 25).
- [18] Araxxe. Webpage. URL: <https://www.araxxe.com/p/our-services/global-transaction-verification/global-transaction-verification/test-call-generator-outsourcing.html> (cit. on pp. 21, 27).
- [19] *Articles*. <https://goantifraud.com/en/blog/categories/article>. Accessed: 2020-09-03 (cit. on p. 2).
- [20] N. Aschenbruck, R. Ernst, E. Gerhards-Padilla, and M. Schwamborn. “BonnMotion: A Mobility Scenario Generation and Analysis Tool”. In: *Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques*. SIMUTools ’10. Torremolinos, Malaga, Spain: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2010. ISBN: 9789639799875. DOI: [10.4108/ICST.SIMUTOOLS2010.8684](https://doi.org/10.4108/ICST.SIMUTOOLS2010.8684) (cit. on p. 62).

- [21] N. Aschenbruck, E. Gerhards-Padilla, M. Gerharz, M. Frank, and P. Martini. “Modelling Mobility in Disaster Area Scenarios”. In: *Proceedings of the 10th ACM Symposium on Modeling, Analysis, and Simulation of Wireless and Mobile Systems*. MSWiM '07. Chania, Crete Island, Greece: Association for Computing Machinery, 2007, pp. 4–12. ISBN: 9781595938510. DOI: [10.1145/1298126.1298131](https://doi.org/10.1145/1298126.1298131) (cit. on p. 62).
- [22] V. A. Balasubramanian, A. Poonawalla, M. Ahamad, M. T. Hunter, and P. Traynor. “PinDrOp: Using Single-Ended Audio Features to Determine Call Provenance”. In: *Proceedings of the 17th ACM Conference on Computer and Communications Security*. CCS '10. Chicago, Illinois, USA: Association for Computing Machinery, 2010, pp. 109–120. ISBN: 9781450302456. DOI: [10.1145/1866307.1866320](https://doi.org/10.1145/1866307.1866320). URL: <https://doi.org/10.1145/1866307.1866320> (cit. on p. 30).
- [23] N. Baldo, M. Miozzo, M. Requena-Esteso, and J. Nin-Guerrero. “An Open Source Product-Oriented LTE Network Simulator Based on Ns-3”. In: *Proceedings of the 14th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. MSWiM '11. Miami, Florida, USA: Association for Computing Machinery, 2011, pp. 293–298. ISBN: 9781450308984. DOI: [10.1145/2068897.2068948](https://doi.org/10.1145/2068897.2068948) (cit. on p. 40).
- [24] K. Baskar. “A study on internet bypass fraud: national security threat”. In: *Forensic Research & Criminology International Journal* 7 (1 2019-09), pp. 31–35 (cit. on pp. 14, 21).
- [25] A. Benslimane and H. Nguyen-Minh. “Jamming Attack Model and Detection Method for Beacons Under Multichannel Operation in Vehicular Networks”. In: *IEEE Transactions on Vehicular Technology* 66.7 (2017), pp. 6475–6488. DOI: [10.1109/TVT.2016.2645478](https://doi.org/10.1109/TVT.2016.2645478) (cit. on p. 79).
- [26] Black Swan Telecom Journal. *Mapping the Interconnect Resale Routes of Fraudsters: How a Global Robot Network Detects Voice and SMS Bypass*. Article. 2015-06. URL: http://bswan.org/interconnect_fraud_routes.asp (cit. on p. 21).
- [27] C. Blackman and L. Srivastava. *Telecommunications Regulation Handbook : Tenth Anniversary Edition*. World Bank Publications 13278. The World Bank, 2011-06. URL: <https://ideas.repec.org/b/wbk/wbps/13278.html> (cit. on p. 14).
- [28] V. Borrel, F. Legendre, M. D. de Amorim, and S. Fdida. “SIMPS: using sociology for personal mobility”. In: *IEEE/ACM Transactions on Networking* 17.03 (2009-05), pp. 831–842. ISSN: 1558-2566. DOI: [10.1109/TNET.2008.2003337](https://doi.org/10.1109/TNET.2008.2003337) (cit. on p. 62).
- [29] Calltic. Webpage. URL: <https://www.calltic.com/> (cit. on pp. 21, 27).
- [30] J. Candia, M. C. González, P. Wang, T. Schoenharl, G. Madey, and A.-L. Barabási. “Uncovering individual and collective human dynamics from mobile phone records”. In: *Journal of Physics A: Mathematical and Theoretical* 41.22 (2008-05), p. 224015. ISSN: 1751-8121. DOI: [10.1088/1751-8113/41/22/224015](https://doi.org/10.1088/1751-8113/41/22/224015) (cit. on p. 48).

- [31] R. Canillas, R. Talbi, S. Bouchenak, O. Hasan, L. Brunie, and L. Sarrat. “Exploratory Study of Privacy Preserving Fraud Detection”. In: *Proceedings of the 19th International Middleware Conference Industry*. Middleware ’18. Rennes, France: Association for Computing Machinery, 2018, pp. 25–31. ISBN: 9781450360166. DOI: [10.1145/3284028.3284032](https://doi.org/10.1145/3284028.3284032) (cit. on p. 79).
- [32] J. G. Cárcamo, R. G. Vogel, A. M. Terwilliger, J. Leidig, and G. Wolffe. “Generative models for synthetic populations”. In: *SummerSim*. 2017 (cit. on pp. 45, 62).
- [33] CFCA. *CFCA 2017 Fraud Loss Survey*. Report. 2017. URL: <https://cfca.org/document/cfca-2017-fraud-loss-survey-pdf/> (cit. on p. 21).
- [34] CFCA. *CFCA 2019 Fraud Loss Survey*. Report. 2019. URL: <https://cfca.org/document/cfca-2019-fraud-loss-survey-pdf/> (cit. on pp. 1, 21).
- [35] CFCA. “Communications Fraud Control Association 2021 Fraud Loss Survey”. In: (2021). URL: <https://cfca.org/wp-content/uploads/2021/12/CFCA-Fraud-Loss-Survey-2021-2.pdf> (cit. on pp. 1, 21).
- [36] G. Chen, A. Carneiro Viana, M. Fiore, and C. Sarraute. “Complete Trajectory Reconstruction from Sparse Mobile Phone Data”. In: *EPJ Data Science* (2019-10). DOI: [10.1140/epjds/s13688-019-0206-8](https://doi.org/10.1140/epjds/s13688-019-0206-8). URL: <https://hal.inria.fr/hal-02286080> (cit. on p. 16).
- [37] P. Cholda, M. Kantor, A. Jajszczyk, and K. Wajda. “NGL01-1: Least Cost Routing in Inter-Carrier Context”. In: *IEEE Globecom 2006*. IEEE, 2006, pp. 1–5. DOI: [10.1109/GLOCOM.2006.243](https://doi.org/10.1109/GLOCOM.2006.243) (cit. on p. 14).
- [38] CSGi. Webpage. URL: <https://www.csgi.com/portfolio/digital-wholesale/assure/assure-sim-box-detection/> (cit. on pp. 21, 27).
- [39] M. Dalmasso, M. Meo, and D. Renga. “Radio Resource Management for Improving Energy Self-Sufficiency of Green Mobile Networks”. In: *SIGMETRICS Perform. Eval. Rev.* 44.2 (2016-09), pp. 82–87. ISSN: 0163-5999. DOI: [10.1145/3003977.3004001](https://doi.org/10.1145/3003977.3004001) (cit. on p. 60).
- [40] M. L. Damiani, A. Acquaviva, F. Hachem, and M. Rossini. “Learning Behavioral Representations of Human Mobility”. In: *Proceedings of the 28th International Conference on Advances in Geographic Information Systems*. SIGSPATIAL ’20. Seattle, WA, USA: Association for Computing Machinery, 2020, pp. 367–376. ISBN: 9781450380195. DOI: [10.1145/3397536.3422255](https://doi.org/10.1145/3397536.3422255) (cit. on p. 65).
- [41] Dinstar. *Instructions for Using Multi-SIM Function of DWG*. Dinstar. 3 pp. URL: <https://www.dinstar.com/WEB/files/48826/2019-05-22/Multi-SIM%5C%20of%5C%20DWG%5C%20Instruction.pdf> (cit. on pp. 21, 25).

- [42] Dinstar. *UC2000-VE/F/G GSM/CDMA/WCDMA VoIP Gateway User Manual*. Version 2.2. Dinstar. 2017-02. 121 pp. URL: <https://www.dinstar.com/WEB/files/47154/2019-04-30/UC2000-VE&VF&VG%5C%20GSM&CDMA&WCDMA%5C%20VoIP%5C%20Gateway%5C%20User%5C%20Manual.pdf> (cit. on pp. 21, 25).
- [43] X. Dong, F. Wu, A. Faree, D. Guo, Y. Shen, and J. Ma. “Selfholding: A combined attack model using selfish mining with block withholding attack”. In: *Computers Security* 87 (2019), p. 101584. ISSN: 0167-4048. DOI: <https://doi.org/10.1016/j.cose.2019.101584> (cit. on p. 79).
- [44] Ejoin. *EJOIN ACOM5xx VoIP Gateway User Manual*. Version 1.4. Ejoin. 2019-10. 32 pp. URL: <https://fr.scribd.com/document/484621350/ACOM5xx-User-Manual-V1-4-1> (cit. on pp. 21, 25).
- [45] F. Ekman, A. Keränen, J. Karvo, and J. Ott. “Working Day Movement Model”. In: *Proceedings of the 1st ACM SIGMOBILE Workshop on Mobility Models*. MobilityModels ’08. Hong Kong, Hong Kong, China: Association for Computing Machinery, 2008, pp. 33–40. ISBN: 9781605581118. DOI: [10.1145/1374688.1374695](https://doi.org/10.1145/1374688.1374695) (cit. on pp. 6, 51, 58, 62, 68).
- [46] O. M. Elrajubi, A. M. Elshawesh, and M. A. Abuzaraida. “Detection of bypass fraud based on speaker recognition”. In: *2017 8th International Conference on Information Technology (ICIT)*. 2017, pp. 50–54. DOI: [10.1109/ICITECH.2017.8079914](https://doi.org/10.1109/ICITECH.2017.8079914) (cit. on pp. 21, 28, 30, 35).
- [47] ETSI. *Universal Mobile Telecommunications System (UMTS); LTE; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3*. ETSI Technical Specification 124 301 V15.17.0. European Telecommunications Standards Institute, 2021. URL: https://www.etsi.org/deliver/etsi_ts/124300_124399/124301/15.04.00_60/ts_124301v150400p.pdf (cit. on pp. 89, 91).
- [48] Ettus Research *USRP UB210 Kit*. <https://www.ettus.com/all-products/ub210-kit/>. Accessed on March 8th, 2023 (cit. on p. 88).
- [49] *Forecast number of mobile devices worldwide from 2020 to 2025 (in billions)*. URL: <https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/> (visited on 2023) (cit. on p. 1).
- [50] J. Gama. “Functional Trees”. In: *Machine Learning* 55 (2004-06), pp. 219–250. DOI: [10.1023/B:MACH.0000027782.67192.13](https://doi.org/10.1023/B:MACH.0000027782.67192.13) (cit. on p. 29).
- [51] J. S. Garofolo, L. F. Lamel, W. M. Fisher, J. G. Fiscus, D. S. Pallett, N. L. Dahlgren, and V. Zue. “TIMIT Acoustic-Phonetic Continuous Speech Corpus”. In: *Philadelphia: Linguistic Data Consortium* (1993) (cit. on p. 35).

- [52] P. Giura, I. Murynets, R. Piqueras Jover, and Y. Vahlis. “Is It Really You? User Identification via Adaptive Behavior Fingerprinting”. In: *Proceedings of the 4th ACM Conference on Data and Application Security and Privacy*. CODASPY ’14. San Antonio, Texas, USA: Association for Computing Machinery, 2014, pp. 333–344. ISBN: 9781450322782. DOI: [10.1145/2557547.2557554](https://doi.org/10.1145/2557547.2557554) (cit. on p. 61).
- [53] GoAntiFraud. *10 Misconceptions about GSM Termination*. Article. Accessed: 2020-04-24. 2016-11. URL: <https://goantifraud.com/en/blog/368-10-misconceptions-about-gsm-termination.html> (cit. on p. 21).
- [54] GoAntiFraud. “5 Efficient Ways to Bypass Antifraud Systems”. In: *GoAntiFraud Blog* (2021). URL: <https://goantifraud.com/en/blog/433-5-efficient-ways-to-bypass-antifraud-systems.html> (visited on 2023-03-08) (cit. on p. 87).
- [55] GoAntiFraud. *Call Recording*. <https://goantifraud.com/en/ejointech-skyline-gsm-termination-solution#call-recording>. accessed 2023-03 (cit. on p. 2).
- [56] GoAntiFraud. *GoAntiFraud GSM termination in Africa: TOP 5 destinations in 2020*. Article. Accessed: 2020-02-20. 2020-02. URL: <https://goantifraud.com/en/blog/1186-gsm-termination-in-africa-top-5-destinations-in-2020.html> (cit. on p. 21).
- [57] GoAntiFraud. *GoAntiFraud is a cloud service for efficient GSM Termination*. Article. Accessed: 2020-04-24. 2016-11. URL: <https://goantifraud.com/> (cit. on pp. 21, 67, 84).
- [58] GoAntiFraud. *Top 5 Popular GSM Gateway Manufacturers*. <https://goantifraud.com/en/blog/818-top-5-popular-gsm-gateway-manufacturers.html>. accessed 2023 (cit. on p. 4).
- [59] GoAntiFraud. *TOP-5 Popular GSM Gateway Manufacturers*. Article. Accessed: 2020-02-23. 2018-02. URL: <https://goantifraud.com/en/blog/818-top-5-popular-gsm-gateway-manufacturers.html> (cit. on pp. 21, 22).
- [60] G. Goggin. “Cell Phone Culture: Mobile Technology in Everyday Life”. In: *Cell Phone Culture: Mobile Technology in Everyday Life* (2012-01), pp. 1–255. DOI: [10.4324/9780203827062](https://doi.org/10.4324/9780203827062) (cit. on p. 1).
- [61] D. González, S. Ruiz, M. García-Lozano, J. Olmos, and A. Serra. “System level evaluation of LTE networks with semidistributed intercell interference coordination”. In: *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*. 2009, pp. 1497–1501. DOI: [10.1109/PIMRC.2009.5449773](https://doi.org/10.1109/PIMRC.2009.5449773) (cit. on p. 40).
- [62] M. C. González, C. A. Hidalgo, and A.-L. Barabási. “Understanding individual human mobility patterns”. In: *Nature* 453.7196 (2008-06), pp. 779–782. DOI: [10.1038/nature06958](https://doi.org/10.1038/nature06958) (cit. on pp. 6, 59).

- [63] I. J. Goodfellow, J. Shlens, and C. Szegedy. *Explaining and Harnessing Adversarial Examples*. 2014. DOI: [10.48550/ARXIV.1412.6572](https://doi.org/10.48550/ARXIV.1412.6572) (cit. on p. 98).
- [64] M. Gorawski and K. Grochla. “The real-life mobility model: RLMM”. In: *Second International Conference on Future Generation Communication Technologies (FGCT 2013)*. 2013, pp. 201–206. DOI: [10.1109/FGCT.2013.6767180](https://doi.org/10.1109/FGCT.2013.6767180) (cit. on p. 62).
- [65] M. Gramaglia, M. Fiore, A. Furno, and R. Stanica. “GLOVE: Towards Privacy-Preserving Publishing of Record-Level-Truthful Mobile Phone Trajectories”. In: *ACM/IMS Trans. Data Sci.* 2.3 (2021-08). ISSN: 2691-1922. DOI: [10.1145/3451178](https://doi.org/10.1145/3451178) (cit. on p. 62).
- [66] S. Guerraoui. *Morocco banned Skype, Viber, WhatsApp and Facebook Messenger. It didn't go down well*. Article. Publisher: Middle East Eye. 2016-03 (cit. on p. 21).
- [67] J. Gui, Z. Sun, Y. Wen, D. Tao, and J. Ye. “A Review on Generative Adversarial Networks: Algorithms, Theory, and Applications”. In: *IEEE Transactions on Knowledge and Data Engineering* (2021), pp. 1–1. DOI: [10.1109/TKDE.2021.3130191](https://doi.org/10.1109/TKDE.2021.3130191) (cit. on p. 97).
- [68] J. Gui, Z. Zheng, X. Zhao, and Z. Qin. “Statistical Properties and Temporal Properties of Calling Behavior”. In: *2019 IEEE 5th International Conference on Computer and Communications (ICCC)*. 2019, pp. 1940–1944. DOI: [10.1109/ICCC47050.2019.9064375](https://doi.org/10.1109/ICCC47050.2019.9064375) (cit. on p. 65).
- [69] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar. “Machine Learning Models for Secure Data Analytics: A taxonomy and threat model”. In: *Computer Communications* 153 (2020), pp. 406–440. ISSN: 0140-3664. DOI: <https://doi.org/10.1016/j.comcom.2020.02.008> (cit. on p. 79).
- [70] S. Hochreiter and J. Schmidhuber. “Long Short-term Memory”. In: *Neural computation* 9 (1997-12), pp. 1735–80. DOI: [10.1162/neco.1997.9.8.1735](https://doi.org/10.1162/neco.1997.9.8.1735) (cit. on p. 47).
- [71] G. Holmes, B. Pfahringer, R. Kirkby, E. Frank, and M. Hall. “Multiclass Alternating Decision Trees”. In: *Machine Learning: ECML 2002*. Ed. by T. Elomaa, H. Mannila, and H. Toivonen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 161–172 (cit. on pp. 29, 74).
- [72] B. Hughes, S. Bothe, H. Farooq, and A. Imran. “Generative Adversarial Learning for Machine Learning empowered Self Organizing 5G Networks”. In: *2019 International Conference on Computing, Networking and Communications (ICNC)*. 2019, pp. 282–286. DOI: [10.1109/ICCNC.2019.8685527](https://doi.org/10.1109/ICCNC.2019.8685527) (cit. on pp. 45, 61).
- [73] Hybertone. *GSM VoIP Gateway Model GoIP324*. 2022. URL: http://www.hybertone.com/en/pro%5C_detail.asp?proid=63 (cit. on p. 23).
- [74] Hybertone. *Remote SIM Bank*. 2022. URL: http://www.hybertone.com/en/pro%5C_detail.asp?proid=43 (cit. on p. 23).
- [75] N. A. Ibrahim Soliman Alsadi. “Study to use NEO4J to analysis and detection SIM-BOX fraud”. In: *Journal of Pure & Applied Sciences* 17.4 (2019-01), pp. 31–35. ISSN: 2521-9200 (cit. on pp. 21, 35).

- [76] I. Ighneiwa and H. Mohamed. “Bypass Fraud Detection: Artificial Intelligence Approach”. In: *ArXiv abs/1711.04627* (2017-11) (cit. on p. 35).
- [77] J. C. Ikuno, M. Wrulich, and M. Rupp. “System Level Simulation of LTE Networks”. In: *2010 IEEE 71st Vehicular Technology Conference*. 2010, pp. 1–5. DOI: [10.1109/VETECS.2010.5494007](https://doi.org/10.1109/VETECS.2010.5494007) (cit. on p. 40).
- [78] T. R. Institute. *Network Protocol Analysis: A New Tool for Blocking International Bypass Fraud Before Revenue is Lost*. Tech. rep. LATRO Services, 2015. URL: <https://knowledgecenter.latro.com/hubfs/pdfs/Whitepaper-Network%5C%20Protocol%5C%20Analysis-2093.pdf> (cit. on pp. 4, 22, 30).
- [79] S. Isaacman, R. Becker, R. Cáceres, M. Martonosi, J. Rowland, A. Varshavsky, and W. Willinger. “Human Mobility Modeling at Metropolitan Scales”. In: *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*. MobiSys ’12. Low Wood Bay, Lake District, UK: Association for Computing Machinery, 2012, pp. 239–252. ISBN: 9781450313018. DOI: [10.1145/2307636.2307659](https://doi.org/10.1145/2307636.2307659) (cit. on pp. 45, 62).
- [80] T. Italia. *Telecommunications - SMS, Call, Internet - MI*. Version V1. 2015. DOI: [10.7910/DVN/EGZHFV](https://doi.org/10.7910/DVN/EGZHFV) (cit. on p. 16).
- [81] A. Jaakola, T. Vass, S. Saarto, and L. Haglund. *Helsinki facts and figures 2019*. Tech. rep. Helsinki, Finland, 2019 (cit. on p. 51).
- [82] K. Janakiraman and S. Motahari. “How Are You Related? Predicting the Type of a Social Relationship Using Call Graph Data”. In: *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*. 2012, pp. 111–116. DOI: [10.1109/SocialCom-PASSAT.2012.79](https://doi.org/10.1109/SocialCom-PASSAT.2012.79) (cit. on p. 67).
- [83] C.-K. Jao, C.-Y. Wang, T.-Y. Yeh, C.-C. Tsai, L.-C. Lo, J.-H. Chen, W.-C. Pao, and W.-H. Sheen. “WiSE: A System-Level Simulator for 5G Mobile Networks”. In: *IEEE Wireless Communications* 25.2 (2018), pp. 4–7. DOI: [10.1109/MWC.2018.8352614](https://doi.org/10.1109/MWC.2018.8352614) (cit. on p. 40).
- [84] S. Jiang, G. A. Fiore, Y. Yang, J. Ferreira Jr, E. Frazzoli, and M. C. González. “A review of urban computing for mobile phone traces: Current methods, challenges and opportunities”. In: *Proceedings of the 2nd ACM SIGKDD international workshop on Urban Computing*. ACM. 2013, p. 2 (cit. on p. 15).
- [85] S. Jiang, Y. Yang, S. Gupta, D. Veneziano, S. Athavale, and M. C. González. “The TimeGeo modeling framework for urban mobility without travel surveys”. In: *Proceedings of the National Academy of Sciences* 113.37 (2016), E5370–E5378. DOI: [10.1073/pnas.1524261113](https://doi.org/10.1073/pnas.1524261113) (cit. on p. 62).
- [86] H. Kahsu. “SIM-Box Fraud Detection Using Data Mining Techniques: The Case of ethio telecom”. PhD thesis. School of Electrical and Computer Engineering Addis Ababa Institute of Technology, 2018-11 (cit. on pp. 21, 28, 29, 35, 66, 73, 74).

- [87] M. Kashir and S. Bashir. “Machine Learning Techniques for SIM Box Fraud Detection”. In: *2019 International Conference on Communication Technologies (ComTech)*. 2019-04, pp. 4–8. DOI: [10.1109/COMTECH.2019.8737828](https://doi.org/10.1109/COMTECH.2019.8737828) (cit. on pp. 21, 28, 35).
- [88] K. Kehelwala, H. Bandara, R. Yasaratne, P. De Almeida, I. Ilesinghe, and P. Wickramasinghe. *REAL-TIME GREY CALL DETECTION SYSTEM USING COMPLEX EVENT PROCESSING*. Tech. rep. Sri Lanka: IET, 2015. URL: <http://theiet.lk/wp-content/uploads/2017/10/22-p7.pdf> (cit. on pp. 21, 28, 29, 35, 66).
- [89] A. Keränen, J. Ott, and T. Kärkkäinen. “The ONE Simulator for DTN Protocol Evaluation”. In: *Simutools '09*. Rome, Italy: ICST (Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), 2009. ISBN: 9789639799455. DOI: [10.4108/ICST.SIMUTOOLS2009.5674](https://doi.org/10.4108/ICST.SIMUTOOLS2009.5674). URL: <https://doi.org/10.4108/ICST.SIMUTOOLS2009.5674> (cit. on pp. 51, 62).
- [90] G. Khodabandelou, V. Gauthier, M. Fiore, and M. A. El-Yacoubi. “Estimation of Static and Dynamic Urban Populations with Mobile Network Metadata”. In: *IEEE Transactions on Mobile Computing* 18.9 (2019), pp. 2034–2047. DOI: [10.1109/TMC.2018.2871156](https://doi.org/10.1109/TMC.2018.2871156) (cit. on p. 59).
- [91] Y. Kim, J. Bae, J. Lim, E. Park, J. Baek, S. I. Han, C. Chu, and Y. Han. “5G K-Simulator: 5G System Simulator for Performance Evaluation”. In: *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. 2018, pp. 1–2. DOI: [10.1109/DySPAN.2018.8610404](https://doi.org/10.1109/DySPAN.2018.8610404) (cit. on p. 40).
- [92] A. J. Kouam, A. Carneiro Viana, A. Garivier, and A. Tchana. “Génération de traces cellulaires réalistes”. In: *CORES 2022 - 7ème Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication*. Saint-Rémy-Lès-Chevreuse, France, 2022-05. URL: <https://hal.science/hal-03658019> (cit. on p. 46).
- [93] A. J. Kouam, A. C. Viana, and A. Tchana. “<italic>SIMBox</italic> Bypass Frauds in Cellular Networks: Strategies, Evolution, Detection, and Future Directions”. In: *IEEE Communications Surveys Tutorials* 23.4 (2021), pp. 2295–2323. DOI: [10.1109/COMST.2021.3100916](https://doi.org/10.1109/COMST.2021.3100916) (cit. on p. 46).
- [94] N. Krawczeniuk. “Analysis of LTE network RF performance in a dense urban environment”. Undergraduate thesis. Pace University, 2019. URL: https://digitalcommons.pace.edu/honorscollege_theses/269 (cit. on p. 88).
- [95] V. Kulkarni and B. Garbinato. “Generating Synthetic Mobility Traffic Using RNNs”. In: *Proceedings of the 1st Workshop on Artificial Intelligence and Deep Learning for Geographic Knowledge Discovery*. GeoAI '17. Los Angeles, California: Association for Computing Machinery, 2017, pp. 1–4. ISBN: 9781450354981. DOI: [10.1145/3149808.3149809](https://doi.org/10.1145/3149808.3149809) (cit. on pp. 45, 62).

- [96] H. Kumar. *TECHNICAL NOTE ON ILLEGAL INTERNATIONAL LONG DISTANCE TELEPHONE EXCHANGE IN INDIA*. Tech. rep. Meerut, India: ITS, 2012-08 (cit. on pp. 2, 14, 21).
- [97] H. Kvamme and Ø. Borgan. “Continuous and discrete-time survival prediction with neural networks”. In: *Lifetime Data Analysis 27.4* (2021-10), pp. 710–736. DOI: [10.1007/s10985-021-09532-6](https://doi.org/10.1007/s10985-021-09532-6) (cit. on p. 48).
- [98] S. Limited. *Bypass Fraud - Are you getting it right?* White Paper. 2011. URL: https://www.subex.com/pdf/Bypass_Fraud.pdf (cit. on p. 21).
- [99] S. Limited. *Subex Wholesale Fraud Management Survey 2013 Is the industry ready to tackle a growing issue?* Survey. 2013. URL: <https://billingviews.com/wp-content/uploads/delightful-downloads/2013/09/Subex-Wholesale-Fraud-Management-Survey-2013.pdf> (cit. on p. 21).
- [100] Z. Lin, A. Jain, C. Wang, G. Fanti, and V. Sekar. “Using GANs for Sharing Networked Time Series Data: Challenges, Initial Promise, and Open Questions”. In: *Proceedings of the ACM Internet Measurement Conference*. IMC ’20. Virtual Event, USA: Association for Computing Machinery, 2020, pp. 464–483. ISBN: 9781450381383. DOI: [10.1145/3419394.3423643](https://doi.org/10.1145/3419394.3423643) (cit. on p. 61).
- [101] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. Wießner. “Microscopic Traffic Simulation using SUMO”. In: *The 21st IEEE International Conference on Intelligent Transportation Systems*. IEEE, 2018, pp. 2575–2582. DOI: [10.1109/ITSC.2018.8569938](https://doi.org/10.1109/ITSC.2018.8569938) (cit. on p. 62).
- [102] H. M. Marah, O. M. Elrajubi, and A. A. Abouda. “Fraud detection in international calls using fuzzy logic”. In: *International Conference on Computer Vision and Image Analysis Applications*. 2015, pp. 1–6. DOI: [10.1109/ICCVIA.2015.7351891](https://doi.org/10.1109/ICCVIA.2015.7351891) (cit. on pp. 21, 28, 29, 35, 66).
- [103] MediaFon. Webpage. URL: <https://www.mediafonts.lt/> (cit. on pp. 21, 27).
- [104] C. Mehlführer, M. Wrulich, J. C. Ikuno, D. Bosanska, and M. Rupp. “Simulating the Long Term Evolution physical layer”. In: *2009 17th European Signal Processing Conference*. 2009, pp. 1471–1478 (cit. on p. 40).
- [105] D. Mir, S. Isaacman, R. Caceres, M. Martonosi, and R. Wright. “DP-WHERE: Differentially private modeling of human mobility”. In: 2013-10, pp. 580–588. DOI: [10.1109/BigData.2013.6691626](https://doi.org/10.1109/BigData.2013.6691626) (cit. on p. 62).
- [106] Y.-A. Montjoye, S. Gambs, V. Blondel, G. Canright, N. Cordes, S. Deletaille, K. Engø-Monsen, M. García-Herranz, J. Kendall, C. Kerry, G. Krings, E. Letouzé, M. Luengo-Oroz, N. Oliver, L. Rocher, A. Rutherford, Z. Smoreda, J. Steele, E. Wetter, and L. Bengtsson. “On the privacy-conscious use of mobile phone data”. In: *Scientific Data* 5 (2018-12), p. 180286. DOI: [10.1038/sdata.2018.286](https://doi.org/10.1038/sdata.2018.286) (cit. on p. 96).

- [107] Y.-A. Montjoye, C. Hidalgo, M. Verleysen, and V. Blondel. “Unique in the Crowd: The Privacy Bounds of Human Mobility”. In: *Scientific reports* 3 (2013-03), p. 1376. DOI: [10.1038/srep01376](https://doi.org/10.1038/srep01376) (cit. on p. 16).
- [108] D. Morrow. *Telco Corruption Fuels SIMbox Frauds*. Article. Publisher: Comms Risk. 2017-07. URL: <https://commsrisk.com/telco-corruption-fuels-simbox-frauds/> (cit. on p. 21).
- [109] E. Mucelli Rezende Oliveira, A. Carneiro Viana, K. Naveen, and C. Sarraute. “Mobile data traffic modeling: Revealing temporal facets”. In: *Computer Networks* 112 (2017), pp. 176–193. ISSN: 1389-1286. DOI: <https://doi.org/10.1016/j.comnet.2016.10.016> (cit. on pp. 45, 46, 50, 51, 61, 62).
- [110] E. Mucelli Rezende Oliveira, A. Carneiro Viana, C. Sarraute, J. Brea, and I. Alvarez-Hamelin. “On the regularity of human mobility”. In: *Pervasive and Mobile Computing* 33 (2016), pp. 73–90. ISSN: 1574-1192. DOI: <https://doi.org/10.1016/j.pmcj.2016.04.005> (cit. on pp. 6, 59).
- [111] M. Müller, F. Ademaj, T. Dittrich, A. Fastenbauer, B. Elbal, A. Nabavi, L. Nagel, S. Schwarz, and M. Rupp. “Flexible multi-node simulation of cellular mobile communications: the Vienna 5G System Level Simulator”. In: *EURASIP Journal on Wireless Communications and Networking* 2018 (2018-09). DOI: [10.1186/s13638-018-1238-7](https://doi.org/10.1186/s13638-018-1238-7) (cit. on p. 40).
- [112] A. Munjal, T. Camp, and W. C. Navidi. “SMOOTH: A Simple Way to Model Human Mobility”. In: *MSWiM '11*. Miami, Florida, USA: Association for Computing Machinery, 2011, pp. 351–360. ISBN: 9781450308984. DOI: [10.1145/2068897.2068957](https://doi.org/10.1145/2068897.2068957) (cit. on p. 62).
- [113] A. Murtić, M. Maljić, S. L. Gruičić, D. Pintar, and M. Vranić. “SNA-based artificial call detail records generator”. In: *International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. 2018. DOI: [10.23919/MIPRO.2018.8400222](https://doi.org/10.23919/MIPRO.2018.8400222) (cit. on pp. 45, 61).
- [114] I. Murynets, M. Zabaranin, R. P. Jover, and A. Panagia. “Analysis and detection of SIMbox fraud in mobility networks”. In: *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*. 2014-04, pp. 1519–1526. DOI: [10.1109/INFOCOM.2014.6848087](https://doi.org/10.1109/INFOCOM.2014.6848087) (cit. on pp. 21, 28, 29, 35, 66, 73, 74).
- [115] D. Naboulsi, M. Fiore, S. Ribot, and R. Stanica. “Large-Scale Mobile Traffic Analysis: A Survey”. In: *IEEE Communications Surveys Tutorials* 18.1 (2016-Firstquarter), pp. 124–161. ISSN: 2373-745X. DOI: [10.1109/COMST.2015.2491361](https://doi.org/10.1109/COMST.2015.2491361) (cit. on pp. 1, 16).
- [116] A. A. Nanavati, S. Gurusurthy, G. Das, D. Chakraborty, K. Dasgupta, S. Mukherjea, and A. Joshi. “On the Structural Properties of Massive Telecom Call Graphs: Findings and Implications”. In: *Proceedings of the 15th ACM International Conference on Information and Knowledge Management*. CIKM '06. Arlington, Virginia, USA: Association

- for Computing Machinery, 2006, pp. 435–444. ISBN: 1595934332. DOI: [10.1145/1183614.1183678](https://doi.org/10.1145/1183614.1183678) (cit. on p. 67).
- [117] G. Nardini, D. Sabella, G. Stea, P. Thakkar, and A. Viridis. “Simu5G—An OMNeT++ Library for End-to-End Performance Evaluation of 5G Networks”. In: *IEEE Access* 8 (2020), pp. 181176–181191. DOI: [10.1109/ACCESS.2020.3028550](https://doi.org/10.1109/ACCESS.2020.3028550) (cit. on p. 40).
- [118] NCC. *AN ASSESSMENT OF INTERNATIONAL VOICE TRAFFIC TERMINATION RATES*. Report. 2015-07. URL: <https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/681-the-principles-of-international-termination-rate/file> (cit. on p. 22).
- [119] OECD. “International Traffic Termination”. In: *OECD Digital Economy Papers* 238 (2014). DOI: [10.1787/5jz2m5mnlvkc-en](https://doi.org/10.1787/5jz2m5mnlvkc-en) (cit. on p. 21).
- [120] B. Oh, J. Ahn, S. Bae, M. Son, Y. Lee, M. Kang, and Y. Kim. “Preventing SIM Box Fraud Using Device Model Fingerprinting”. In: *Network and Distributed Systems Security (NDSS) Symposium*. 2023 (cit. on pp. 83–85).
- [121] F. Okumbor N. Anthony and A. A. J. Olokunde. “Grappling with the Challenges of Interconnect Bypass Fraud”. In: *IOSR Journal of Mobile Computing and Application (IOSR-JMCA)* 6 (1 2019-01), pp. 35–41. ISSN: 2394-0050 (cit. on pp. 21, 24).
- [122] OpenCellID. *The world’s largest Open Database of Cell Towers*. 2022. URL: <https://www.opencellid.org/> (cit. on pp. 51, 53).
- [123] OpenStreetMap contributors. *Planet dump retrieved from https://planet.osm.org*. <https://www.openstreetmap.org>. 2017 (cit. on p. 51).
- [124] C. Papageorgiou, K. Birkos, T. Dagiuklas, and S. Kotsopoulos. “Modeling Human Mobility in Obstacle-Constrained Ad Hoc Networks”. In: *Ad Hoc Netw.* 10.3 (2012-05), pp. 421–434. ISSN: 1570-8705. DOI: [10.1016/j.adhoc.2011.07.012](https://doi.org/10.1016/j.adhoc.2011.07.012) (cit. on p. 62).
- [125] L. Pappalardo and F. Simini. “Modelling individual routines and spatio-temporal trajectories in human mobility”. In: *CoRR* abs/1607.05952 (2016). arXiv: [1607.05952](https://arxiv.org/abs/1607.05952). URL: <http://arxiv.org/abs/1607.05952> (cit. on p. 62).
- [126] N. Patriciello, S. Lagen, B. Bojovic, and L. Giupponi. “An E2E simulator for 5G NR networks”. In: *Simulation Modelling Practice and Theory* 96 (2019), p. 101933. ISSN: 1569-190X. DOI: <https://doi.org/10.1016/j.simpat.2019.101933> (cit. on p. 40).
- [127] G. Piro, N. Baldo, and M. Miozzo. “An LTE Module for the Ns-3 Network Simulator”. In: *Proceedings of the 4th International ICST Conference on Simulation Tools and Techniques*. SIMUTools ’11. Barcelona, Spain: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2011, pp. 415–422. ISBN: 9781936968008 (cit. on p. 40).
- [128] G. Piro, L. A. Grieco, G. Boggia, F. Capozzi, and P. Camarda. “Simulating LTE Cellular Systems: An Open-Source Framework”. In: *IEEE Transactions on Vehicular Technology* 60 (2011), pp. 498–513 (cit. on p. 40).

- [129] Pixip. Webpage. URL: <https://www.pixip.net/index.php/solutions/test-call-generation.html> (cit. on pp. 21, 27).
- [130] Portech. *SIM Server User Manual*. Version 2.0.1. Portech. 29 pp. URL: <https://www.portech.com.tw/data/SIM%5C%20Server%5C%20User%5C%20Manual%5C%20V2.pdf> (cit. on pp. 21, 25).
- [131] 3. G. P. Project. *3G Security; Security architecture (Release 16)*. Technical Specification TS 33.102. European Telecommunications Standards Institute (ETSI), 2020. URL: https://www.etsi.org/deliver/etsi%5C_ts/133100%5C_133199/133102/16.03.00%5C_60/ts%5C_133102v160300p.pdf (cit. on p. 89).
- [132] B. Reaves, E. Shernan, A. Bates, H. Carter, and P. Traynor. “Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge”. In: *Proceedings of the 24th USENIX Conference on Security Symposium*. SEC’15. Washington, D.C.: USENIX Association, 2015-08, pp. 833–848. ISBN: 978-1-939133-11-3. DOI: [10.5555/2831143.2831196](https://doi.org/10.5555/2831143.2831196) (cit. on pp. 12, 21, 28, 30, 35).
- [133] RebTel. *How Does Rebtel Work?* Webpage. 2023. URL: <https://www.rebtel.com/en/about-us/how-it-works/> (cit. on pp. 2, 22).
- [134] A. de Régulation des Télécommunications Cameroun. *INFORMATIONS STATISTIQUES*. Tech. rep. Cameroon, 2018 (cit. on p. 71).
- [135] Revector. *SIMBox fraud and OTT bypass biggest threats to mobile operator revenues*. Article. 2016-11 (cit. on pp. 2, 21).
- [136] S. Rizvi, R. Pipetti, N. McIntyre, J. Todd, and I. Williams. “Threat model for securing internet of things (IoT) network at device-level”. In: *Internet of Things 11 (2020)*, p. 100240. ISSN: 2542-6605. DOI: <https://doi.org/10.1016/j.iot.2020.100240> (cit. on p. 79).
- [137] M. Sahin, A. Francillon, P. Gupta, and M. Ahamad. “SoK: Fraud in Telephony Networks”. In: *2017 IEEE European Symposium on Security and Privacy (EuroSP)*. 2017-04, pp. 235–250. DOI: [10.1109/EuroSP.2017.40](https://doi.org/10.1109/EuroSP.2017.40) (cit. on p. 21).
- [138] M. Sahin. “Understanding Telephony Fraud as an Essential Step to Better Fight It”. PhD thesis. TELECOM ParisTech, 2017-09 (cit. on pp. 2, 15).
- [139] R. Sallehuddin, S. Ibrahim, A. Zain, and A. Elmi. “Detecting SIM Box Fraud by Using Support Vector Machine and Artificial Neural Network”. In: *Jurnal Teknologi*. Vol. 74. 2015-04, pp. 137–149. DOI: [10.11113/jt.v74.2649](https://doi.org/10.11113/jt.v74.2649) (cit. on pp. 21, 28, 29, 35, 61, 66, 73, 74).
- [140] R. Sallehuddin, S. Ibrahim, A. Zain, and A. Elmi. “Detecting SIM Box Fraud Using Neural Network”. In: *IT Convergence and Security 2012*. Ed. by K. J. Kim and K.-Y. Chung. Dordrecht: Springer Netherlands, 2013, pp. 575–582. ISBN: 978-94-007-5860-5. DOI: [10.1007/978-94-007-5860-5_69](https://doi.org/10.1007/978-94-007-5860-5_69) (cit. on pp. 21, 28, 29, 35, 74).

- [141] M. Schwamborn and N. Aschenbruck. “Introducing Geographic Restrictions to the SLAW Human Mobility Model”. In: *2013 IEEE 21st International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems*. 2013, pp. 264–272. DOI: [10.1109/MASCOTS.2013.34](https://doi.org/10.1109/MASCOTS.2013.34) (cit. on pp. 51, 62).
- [142] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau. *CRAWDAD dataset cambridge/haggle* (v. 2009-05-29). Downloaded from <https://crawdad.org/cambridge/haggle/20090529/imote>. traceset: imote. 2009-05. DOI: [10.15783/C70011](https://doi.org/10.15783/C70011) (cit. on p. 58).
- [143] L. Shenzhen HyberTone Technology Co. Webpage. URL: <http://www.hybertone.com/en/> (cit. on pp. 21, 24).
- [144] L. Shenzhen HyberTone Technology Co. *Gateway Selector Script*. Version 1.01.1. Shenzhen HyberTone Technology Co., Ltd. 18 pp. URL: <http://www.hybertone.com/uploadfile/download/20171222180904804.pdf> (cit. on pp. 21, 25).
- [145] L. Shenzhen HyberTone Technology Co. *GoIP User Manual*. Version 1.5. Shenzhen HyberTone Technology Co., Ltd. 2016-06. 69 pp. URL: <http://www.hybertone.com/uploadfile/download/20140304125509964.pdf> (cit. on pp. 21, 25).
- [146] L. Shenzhen HyberTone Technology Co. *GoIP32-X4 Quick Setup Manual*. Shenzhen HyberTone Technology Co., Ltd. 17 pp. URL: <http://www.hybertone.com/uploadfile/download/20180913163352145.pdf> (cit. on pp. 21, 25).
- [147] V. Solutions. *RF Spectrum Analyzers*. <https://www.viavisolutions.com/en-us/products/rf-spectrum-analyzers>. Accessed on March 8th, 2023 (cit. on p. 88).
- [148] L. Song and D. F. Kotz. “Evaluating Opportunistic Routing Protocols with Large Realistic Contact Traces”. In: *Proceedings of the Second ACM Workshop on Challenged Networks*. CHANTS ’07. Montreal, Quebec, Canada: Association for Computing Machinery, 2007, pp. 35–42. ISBN: 9781595937377. DOI: [10.1145/1287791.1287799](https://doi.org/10.1145/1287791.1287799) (cit. on p. 58).
- [149] M. Songailaitė and T. Krilavičius. “Synthetic call detail records generator”. In: *CEUR Workshop proceedings (2021)* (cit. on pp. 45, 46, 61).
- [150] *Specifications-3GPP*. URL: <http://www.3gpp.org/specifications> (cit. on p. 1).
- [151] Sysmaster. Webpage. URL: http://www.sysmaster.com/products/gsm_termination.php (cit. on p. 21).
- [152] *SysmoUSIM - Sysmocom*. <https://www.sysmocom.de/products/lab/sysmousim/index.html>. Accessed: March 8, 2023 (cit. on p. 88).
- [153] F. Tesfaye. “Near-Real Time SIM-box Fraud Detection Using Machine Learning in the case of ethio telecom”. PhD thesis. School of Electrical and Computer Engineering Addis Ababa Institute of Technology, 2020-02 (cit. on pp. 21, 28, 29, 35, 66, 73, 74).

- [154] Y. Theodorou, K. Okong'o, and E. Yongo. *Access to Mobile Services and Proof of Identity 2019: Assessing the impact on digital and financial inclusion*. Tech. rep. GSMA, 2019. URL: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofOfID_R_WebSpreads.pdf (cit. on pp. 2, 21).
- [155] H. Tu, Y. Xia, C. K. Tse, and X. Chen. “A Hybrid Cyber Attack Model for Cyber-Physical Power Systems”. In: *IEEE Access* 8 (2020), pp. 114876–114883. DOI: [10.1109/ACCESS.2020.3003323](https://doi.org/10.1109/ACCESS.2020.3003323) (cit. on p. 79).
- [156] F. Valenza, E. Karafli, R. V. Steiner, and E. C. Lupu. “A hybrid threat model for smart systems”. In: *IEEE Transactions on Dependable and Secure Computing* (2022), pp. 1–14. DOI: [10.1109/TDSC.2022.3213577](https://doi.org/10.1109/TDSC.2022.3213577) (cit. on p. 79).
- [157] G. Vallerio, D. Renga, M. Meo, and M. A. Marsan. “Greener RAN Operation Through Machine Learning”. In: *IEEE Transactions on Network and Service Management* 16.3 (2019), pp. 896–908. DOI: [10.1109/TNSM.2019.2923881](https://doi.org/10.1109/TNSM.2019.2923881) (cit. on p. 60).
- [158] B. Veloso, S. Tabassum, C. Martins, R. Espanha, R. Azevedo, and J. Gama. “Interconnect bypass fraud detection: a case study”. In: *Annals of Telecommunications* 75 (2020-10), pp. 583–596. DOI: [10.1007/s12243-020-00808-w](https://doi.org/10.1007/s12243-020-00808-w) (cit. on pp. 21, 28, 29, 35).
- [159] A. Viridis, G. Stea, and G. Nardini. “SimuLTE — A Modular System-Level Simulator for LTE/LTE-A Networks Based on OMNeT++”. In: *Proceedings of the 4th International Conference on Simulation and Modeling Methodologies, Technologies and Applications. SIMULTECH 2014*. Vienna, Austria: SCITEPRESS - Science and Technology Publications, Lda, 2014, pp. 59–70. ISBN: 9789897580383. DOI: [10.5220/0005040000590070](https://doi.org/10.5220/0005040000590070) (cit. on p. 40).
- [160] 2. VoiceBlue. *2N VoiceBlue Enterprise User Manual*. Version 1.11. 2N VoiceBlue. 143 pp. URL: http://www.mpinetworks.com/images/catalogue/id_13/images/22_VoiceBlue_Enterprise_-_User_Manual_EN.pdf (cit. on pp. 21, 25).
- [161] V. Vukadinovic, Ó. R. Helgason, and G. Karlsson. “An analytical model for pedestrian content distribution in a grid of streets”. In: *Math. Comput. Model.* 57 (2013), pp. 2933–2944 (cit. on p. 51).
- [162] Wikipedia. *Configuration Model*. 2022. URL: https://en.wikipedia.org/wiki/Configuration_model (cit. on p. 54).
- [163] K. Xu, R. Singh, H. Bilen, M. Fiore, M. K. Marina, and Y. Wang. “CartaGenie: Context-Driven Synthesis of City-Scale Mobile Network Traffic Snapshots”. In: *2022 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. 2022, pp. 119–129. DOI: [10.1109/PerCom53586.2022.9762395](https://doi.org/10.1109/PerCom53586.2022.9762395) (cit. on p. 61).

- [164] K. Xu, R. Singh, M. Fiore, M. K. Marina, H. Bilen, M. Usama, H. Benn, and C. Ziemlicki. “SpectraGAN: Spectrum Based Generation of City Scale Spatiotemporal Mobile Network Traffic Data”. In: *Proceedings of the 17th International Conference on Emerging Networking EXperiments and Technologies*. CoNEXT ’21. Virtual Event, Germany: Association for Computing Machinery, 2021, pp. 243–258. ISBN: 9781450390989. DOI: [10.1145/3485983.3494844](https://doi.org/10.1145/3485983.3494844) (cit. on pp. 60, 61, 97).
- [165] Y. Yang, X. Du, Z. Yang, and X. Liu. “Android Malware Detection Based on Structural Features of the Function Call Graph”. In: *Electronics* 10.2 (2021). ISSN: 2079-9292. DOI: [10.3390/electronics10020186](https://doi.org/10.3390/electronics10020186) (cit. on p. 67).
- [166] Y. Zheng, X. Xie, and W.-Y. Ma. “GeoLife: A Collaborative Social Networking Service among User, location and trajectory”. In: *IEEE Data(base) Engineering Bulletin* (2010-06). URL: <https://www.microsoft.com/en-us/research/publication/geolife-a-collaborative-social-networking-service-among-user-location-and-trajectory/> (cit. on p. 45).
- [167] M. Zilske and K. Nagel. “Studying the Accuracy of Demand Generation from Mobile Phone Trajectories with Synthetic Data”. In: *Procedia Computer Science* 32 (2014-12), pp. 802–807. DOI: [10.1016/j.procs.2014.05.494](https://doi.org/10.1016/j.procs.2014.05.494) (cit. on pp. 45, 62).

FraudZen simulation parameters

Figures [A.1](#), [A.2](#), [A.3](#), and [A.4](#) present JSON configuration lines of a *FraudZen* simulation scenario.

```
1 {  
2 |   "simulationName": "name",  
3 |   "simulatedDuration": 30,  
4 |   "start_hour": 0,  
5 |   "date": "2021-03-17",  
6 |   "mcc": "244",  
7 |   "nbOp": 1,  
8 |   "mnCodes": [  
9 |     "005"  
10 | ],
```

Figure A.1: General *FraudZen* simulation parameters

```
11 "interCallStrategy": "trace-based",
12 "regularMobilityStrategy": "trace-based",
13 "regularTrafficStrategy": "trace-based",
14 "simbox_fraud": true,
15 "frauded_call_frequency": 3,
16 "simbox_architecture": {
17     "gateways1": [8, 8],
18     "gateways2": [],
19     "gateways2_sims": [],
20     "simbanks": [54],
21     "fillingPercentages": [1],
22     "controlServer": true,
23
24     "fraudulentMobilityStrategy": "trace-based:static",
25     "groupSize": 0,
26
27     "routingPolicy": "inTurn",
28
29     "probabilisticCalls": true,
30
```

Figure A.2: *FraudZen* simulation parameters related to (Lines 11-13) Legitimate users' mobility and traffic and (Lines 14-30) *SIMBox* architecture creation

```
32 "nbSimGroup": 1,
33 "simGroup0":
34 {
35     "location": [[0, 54, 1]],
36     "unblockFrequency": 20,
37     "parameterLimitation": {
38         "state": false,
39         "parameters": ["callCount", "totalCallDur"],
40         "values": [-1, -1, 61]
41     },
42     "timeParameterLimitation":
43 > { ...
44     },
45     "timeLimitation": { ...
46     },
47     "rotationTrigger": { ...
48     },
49     "rotationPolicy":
50 > { ...
51     },
52     "migrationPolicy":
53 > { ...
54     },
55     "imeiGenerationRule":
56 > { ...
57     },
58     "networkActivityGeneration":
59 > { ...
60     }
61 },
62
```

Figure A.3: *FraudZen* simulation parameters related to *SIMBox*' SIM groups creation and configuration

```
148     "nbGSMGroup": 2,  
149     "GSMGroup0":  
150     {  
151         "location": [[0, 8, 1]],  
152         "simCheckFrequency": 20,  
153         "imeiGenerationRule":  
154 >     { ...  
163     },  
164     "baseStationSelection":  
165 >     { ...  
174     },  
175     "copy": false,  
176     "copyFromGroupId": 0  
177     },  
178     "GSMGroup1":  
179     { ...  
180 >     },  
206     },  
207     "linkage": [[0, 0], [1, 0]]  
208 }
```

Figure A.4: *FraudZen* simulation parameters related to *SIMBox*' GSM groups creation and configuration

Titre : Fraudes de contournement dans les réseaux cellulaires : compréhension et mitigation

Mots clés : Réseaux cellulaires, Comportements humain de mobilité et communication, modèles génératifs profonds de comportements, Charging Data Records (CDRs), Modélisation et détection de la fraude à la *SIMBox*, Signalisation cellulaire

Résumé : Les réseaux cellulaires fournissent des services de communication numérique à plus de cinq milliards de personnes dans le monde. En outre, leur ouverture au grand public et leur complexité ont exposé les réseaux cellulaires à des attaques qui se sont considérablement développées au cours des dernières décennies. D'après le rapport de 2021 de la Communication Fraud Control Association, les opérateurs de réseaux mobiles subissent chaque année des pertes s'élevant à 39,89 milliards de dollars en raison d'activités illégales sur leurs surfaces. Parmi ces activités illégitimes, la fraude de contournement internationale à la *SIMBox*, est l'une des plus répandues, ayant un impact sévère multiple.

La fraude à la *SIMBox* consiste à détourner le trafic vocal cellulaire international des routes réglementées et à le réacheminer sous forme d'appels locaux dans le pays de destination à partir d'une gateway VoIP-GSM (c'est-à-dire une *SIMBox*). Touchant des pays du monde entier, ce problème porte atteinte aux revenus des opérateurs, à la qualité des réseaux, à la recherche sur les réseaux et à la sécurité nationale. Principalement dans les pays émergents, jusqu'à 70% des appels internationaux entrants sont terminés frauduleusement. Pire encore, la fraude à la *SIMBox* permet aux terroristes internationaux de mener des activités cachées, en se faisant passer pour des abonnés nationaux.

Dans ce contexte, de nombreux défis s'ajoutent. Tout d'abord, tandis que les jeux de données des réseaux mobiles (Charging Data Records ou CDRs) sont le principal type de données exploité pour la détection de la fraude par les opérateurs, ils sont intrinsèquement privés. Les CDRs contiennent des informations sensibles sur les habitudes des abonnés, ce qui rend leur partage difficile à la communauté scientifique et, en même temps, limite la recherche sur la fraude. Deuxièmement, le comportement des fraudeurs évolue au fil du temps pour s'adapter aux solutions, maintenant la détection en arrière. En particulier, la fraude *SIMBox* imite le comportement de

communication humain concernant les habitudes de trafic, mobilité et sociabilité perceptibles dans les CDRs. Enfin, dû au faible investissement correspondant, la fraude à la *SIMBox* est rapidement rentable. Ainsi, le temps de détection est crucial pour une mitigation efficace à long terme.

Cette thèse s'intéresse à la compréhension et à la mitigation de la fraude à la *SIMBox* tout en adressant les défis susmentionnés.

- Tout d'abord, elle étudie en profondeur la littérature existante et les principaux fabricants de *SIMBox* afin de mettre la lumière sur l'écosystème de la fraude en révélant les techniques frauduleuses et leur évolution constante dans le temps.

- Ensuite, elle contribue significativement à relâcher la barrière d'exploitation des CDRs réels pour la recherche sur la fraude à la *SIMBox*. Cela comprend la publication d'un environnement de simulation scalable, *FraudZen*, qui génère des CDR réalistes, avec des utilisateurs frauduleux et légitimes. A cette fin, *FraudZen* intègre (i) une modélisation de la fraude *SIMBox* pour les utilisateurs frauduleux et (ii) une modélisation générative capturant les comportements de communication réels pour les utilisateurs légitimes. L'application de *FraudZen* à l'évaluation approfondie de la littérature sur la détection de la fraude révèle que la variation du modèle de fraude abordé entraîne un écart important dans les performances de détection.

- Troisièmement, elle étudie l'utilisation des données de signalisation cellulaire pour la détection en temps réel de la fraude par contournement, par des analyses expérimentales avec de véritables appareils *SIMBox*.

Par des évaluations approfondies, nous validons les contributions de cette thèse pour accomplir un pipeline traitant la fraude : *de la compréhension complète des fraudes SIMBox et des limites de détection à l'atténuation de la fraude à long terme par l'anticipation et la riposte rapide.*

Title : Bypass frauds in cellular network: understanding and mitigation

Keywords : Cellular networks, Human mobility and communication behaviors, Deep generative modeling of behaviors, Charging Data Records (CDRs), *SIMBox* fraud modeling and detection, Cellular signaling

Abstract : Cellular networks provide digital communications for more than five billion people around the globe. Besides, their openness to the general public, opaqueness, and complexity have exposed cellular networks to attacks that have tremendously grown over the previous decades. According to the Communication Fraud Control Association's 2021 report, worldwide mobile network operators are experiencing as much as \$39.89 billion annually due to illegal activities on their surfaces. Among such illegitimate activities, *SIMBox* international bypass fraud is one of the most prevalent, having a severe impact manifold.

SIMBox fraud involves diverting international cellular voice traffic from regulated routes and rerouting it as local calls in the destination country from a VoIP-GSM gateway (i.e., *SIMBox*). Affecting countries worldwide, this problem impairs operators' revenues, network quality, networking research, and national security. Mainly in developing countries, up to 70% of incoming international call traffic is terminated fraudulently. Even worse, *SIMBox* fraud allows international terrorists to conduct covert activities, masquerading as national subscribers.

In this context, many challenges are added. First, while mobile network datasets (i.e., Charging Data Records or CDRs) are the primary data type leveraged for operators' fraud detection, they are intrinsically private. CDRs hold sensitive information about subscribers' habits, hardening their shareability to the research community and, at the same time, curbing fraud detection investigations. Second, fraudsters' behavior changes over time to adapt to the target solutions, making detection lag behind. In particular, *SIMBox* fraud increasingly mimics human communication behavior regarding traffic, mobility, and social habits

perceptible in CDRs. Third, considering the low related investment, the fraud is quickly profitable. Therefore, the detection time is crucial for effective long-term mitigation.

This thesis tackles international bypass fraud understanding and mitigation while addressing the aforementioned challenges.

- It first deeply surveys both existing literature and the major *SIMBox* manufacturers to shed light on the *SIMBox* fraud ecosystem uncovering fraudulent techniques and their constant evolution through time.
- Second, it significantly contributes to unleashing the barrier of real-world CDRs exploitation for research on *SIMBox* fraud. This includes releasing a scalable simulation environment, i.e., *FraudZen*, that generates realistic CDRs, with fraudulent and legitimate users. To this end, *FraudZen* incorporates (i) *SIMBox* fraud modeling for fraudulent users and (ii) generative modeling capturing real-world communication behaviors for legitimate users. Applying *FraudZen* capabilities to the in-depth evaluation of ML-based fraud detection literature reveals that the tackled fraud model variation causes a significant discrepancy in detection performance.
- Third, it investigates the use of cellular signaling data for the real-time detection of bypass fraud through experimental analyzes with real *SIMBox* appliances.

Through in-depth evaluations, we validate this thesis's contributions to accomplish a pipeline to handle the fraud: *from Fully understanding SIMBox frauds and detection limitations to Long-term fraud mitigation by anticipation and rapid retort.*

