SIMBox fraud: How well can they mimic your communication behavior?

Anne Josiane Kouam, Aline Carneiro Viana, Alain Tchana

SIMBox fraud: How well can *they* mimic *your* communication behavior?

Anne Josiane Kouam*, Aline Carneiro Viana*, Alain Tchana†
* INRIA, France. † Grenoble INP, France.
E-mail: {anne-josiane.kouam-djuigne, aline.viana}@inria.fr*, alain.tchana@grenoble-inp.fr†

***Abstract*—Being one of the most prevalent scams in cellular networks, *SIMBox* fraud causes a significant financial loss, national security threats, and phone conversation privacy breaches. Yet, *SIMBox* fraud is still an open issue being little addressed and hardly detected by operators due to: (c1) the scarcity of ground-truth fraudulent datasets and (c2) the constant evolution of fraudulent strategies aiming to disguise by mimicking legitimate communication behaviors. This paper introduces the *FraudZen* framework to tackle (c1) by generating mobile communication datasets (i.e., Charging Data Records/ CDRs) with realistic fraudulent ground truth. Such CDRs are associated with explicit knowledge of a *fraud model*, thus filling the gap for tackling challenge (c2). Through *FraudZen*, we show fraudsters can mimic legitimate communication behaviors from literature almost perfectly, raising the need to advance current detection.**

I. Problem statement

SIMBox fraud consists of diverting the international voice traffic from the regulated routes through VoIP established links [1]. The diverted traffic is received at the level of a *SIMBox* (VoIP to GSM gateway) in the destination country and re-originated as a national mobile call to its recipient. Hence, destination mobile operators perceive national termination fees instead of international ones, which are much higher. The impact is enormous, affecting states' and operators' revenues with a loss estimated to USD 3.11 Billion in 2021 [2]. More critically, *SIMBox* fraud allows attackers to act as national subscribers, which international terrorists could use for covert operations. *SIMBox* appliances also allow eavesdropping on international phone conversations [3], impeding user privacy and giving the possibility of international espionage, *striking impact attesting SIMBox fraud deserves much more attention.*

Yet, the *SIMBox* fraud mitigation remains little tackled by researchers: only 15 literature approaches since 2011. This paper tackles the two main challenges inherent to fraud mitigation.

Scarcity of fraudulent ground-truth. *SIMBox* fraud investigation relies on network-related datasets (i.e., CDRs) to distinguish between legitimate users and *SIMBox* fraudulent communication behavior. Unfortunately, CDRs suffer a deficiency of ground-truth on known fraudulent traffic, resulting from limited operators' detection capability: operators are generally aware of no or a low percentage of fraudulent users compared to the total amount of users in CDRs. The remaining large portion of users is considered legitimate. Hence, *detection built from such partial fraudulent knowledge likely cause many false negatives*.

Constant fraud evolution. Aiming to be indistinguishable from legitimate users, *SIMBox* fraudsters constantly create and refine their appliance functionalities to mimic human traffic and mobility behavior. Unfortunately, such fraud evolution is not followed by detection: *Current CDR-based detection methods are mostly validated in very particular contexts with no guarantee of generalized efficiency for evolved fraud behaviors*.

This paper introduces *FraudZen* as the first-of-the-literature framework to ease research on the fraud detection. As explained next, *FraudZen* rationale is to break through a *lagging-behind detection*, by providing *updated information* on the fraud behavior that can only *come from the fraudsters*.

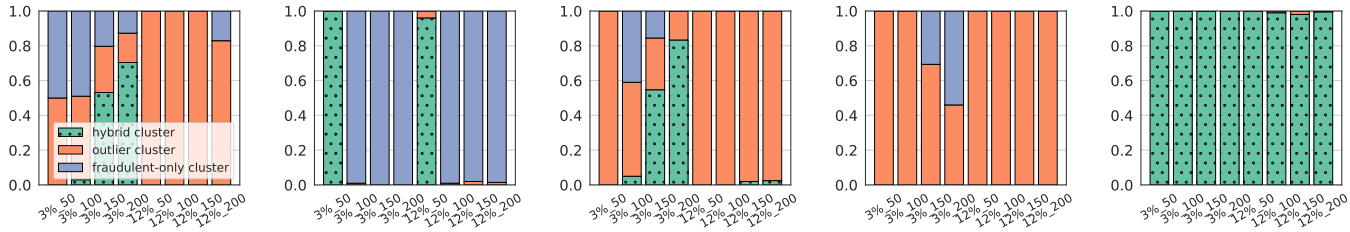
II. How we tackle the problem

FraudZen unleashes the current barriers to fraud investigation in *(c1) providing CDRs with realistic fraudulent ground truth while (c2) associating them with an explicit and measured knowledge of fraud behavior, thus filling the gap for detection leveraging*. Accordingly, researchers and mobile operators can use this tool to (i) inject fraudulent traffic (generated from existing fraud methods or prospected ones) in their CDRs or (ii) investigate the validity of current and future detection methods, in a exhaustive and controlled way. This result is achieved through the following thorough methodology.

a) ***SIMBox market study****:* First, we identify that *SIMBox*'s fraudulent traffic is highly linked to the *SIMBox* appliances generating the fraud. Thus, the *SIMBox fraud's imprint in CDRs results from handling functionalities offered by SIMBox manufacturers with known intent.* With that in mind, we perform a comprehensive *SIMBox* market study to assess the current fraud capabilities [1]. We review the functionalities of all 94 *SIMBox* appliances from the major *SIMBox* manufacturers in the international market. Our study encompasses appliances used by over 2000 fraudsters in more than 31 countries for ten years [4]. It uncovers and categorizes existing *SIMBox* functionalities from their purpose in detection evasion.

b) ***SIMBox fraud modeling****:* Second, we propose the first-of-the-literature *SIMBox* fraud modeling. From the above survey of in-market *SIMBox* functionalities alternatives, we extract information to *"think like a fraudster"*. Our modeling thus provides a framework to define meaningful *SIMBox* frauds. Precisely, through the analysis of 1212 guiding articles and 66 video tutorials [5] from *SIMBox* fraud assisting services (i.e., GoAntiFraud and Antrax), we extract intuitive and easy-to-interpret traits covering the fraud action areas, i.e., traffic, mobility, and social communication behaviors.

c) ***FraudZen framework****:* We then embed our *SIMBox* fraud modeling in the design of *FraudZen*: *an environment for the scalable simulation of SIMBox frauds*. *FraudZen* implements a realistic cellular network architecture involving multiple operators' topology, legitimate users, and *SIMBox* architectures



(a) *fd_naive* (b) *fd_traffic* (c) *fd_mobility* (d) *fd_social* (e) *fd_all*

Fig. 1: In-crowd-blending metric per fraud model: distribution of fraudulent users in OC/HC/FC clusters.

of varying sizes and configurable locations. Such simulation scenarios are calibrated by the configuration of 122 real-world parameters. Hence, from input legitimate (i.e., traffic and mobility models) and fraudulent (*SIMBox* fraud model) users' parameters, *FraudZen* generates CDRs traces of both legitimate and fraudulent users.

d) ***In-crowd-blending capability****:* At last, we define a metric capturing *a fraud model's efficiency* from *FraudZen* generated traces. The *in-crowd-blending capability* of a *SIMBox* fraud model refers to its ability to make fraudulent users blend into the crowd of legitimate ones. It comes from the intuitive idea that the more a fraud model yields 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 *from CDR-based literature works* (e.g., number of calls per day; number of unique cell Ids).

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.

Hence, 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* as: $ICB(fm) = \frac{|HC|}{|HC|+|FC|+|OC|}$.

III. Validation and Key observations

This section validates *FraudZen* ability for efficient *SIMBox* fraud generation, under realistic cellular network scenarios, by characterizing the ICB of five generated fraud models (fm).

We perform experimental setup with 21K legitimate users from a fully anonymized real-world traffic CDRs. This dataset is enriched with our realistically-emulated trajectories using the *Enhanced-Working Day Mobility Model* (En-WDM) [6].

Regarding fraudulent users' behavior, we design an advanced *SIMBox* fraud model (i.e., *fd_all*) following insights from a GSM termination tutorial [7]. [7] indicates the *fd_all*'s *SIMBox* configurations in terms of traffic, mobility, and social (i.e., calling interactions) behavior to provide as input to the *FraudZen* framework. Then we distinguish four fraud models obtained by reproducing such advanced configurations for no (i.e., *fd_naive*) or a unique behavioral feature (i.e., *fd_traffic*, *fd_mobility*, or *fd_social*) allowing to assess their significance at the fraud efficiency. Multiple simulation scenarios are obtained by combining values of (i) percentages of incoming international traffic (i.e., 3% and 12%) and (ii) numbers of SIM cards in the fraudulent architecture (i.e., 50, 100, 150 and 200).

Fig. 1 reports the *in-crowd-blending capability* per fraud model and under the different considered scenarios: The *fd_all* fraud model (Fig. 1e) yields all fraudulent users in hybrid clusters regardless of the scenario. *This attests FraudZen capability to leverage the current in-market SIMBox functionalities at the generation of frauds very close to human behavior, thus highly efficient.* This provides evidence of the need to enhance current CDR-based *SIMBox* fraud detection of the literature.

Further analysis indicates (i) *fd_traffic* fraud model is counter-intuitively worse than *fd_naive* due to its naive mobility behavior shared by all fraudulent users. (ii) *fd_mobility* fraud model follows the same trend as *fd_naive* while being more efficient. This suggests improving mobility rather than traffic has a better impact on the effectiveness of fraud strategies. (iii) At last, *fd_social* fraud model's results show the social component does not greatly impact the fraud effectiveness.

IV. What we plan next

FraudZen will be released to ease and promote research on SIMBox fraud mitigation. We believe such a tool is indispensable for research in this field where data is intrinsically private. In future works, we plan to implement literature *SIMBox* fraud detection approaches and assess their performance and limitations against the above fraud models through a comprehensive evaluation given by multiple parameters. We will then have hints to build a more resilient detection approach.

References

[1] A. J. Kouam, A. C. Viana, and A. Tchana, "Simbox bypass frauds in cellular networks: Strategies, evolution, detection, and future directions", *IEEE Communications Surveys & Tutorials*, 2021.
[2] C. F. C. Association, "Fraud loss survey", tech. rep., 2021.
[3] GoAntiFraud, "Call recording". https://goantifraud.com/en/ejointech-skyline-gsm-termination-solution#call-recording, March 3 accessed 2023.
[4] GoAntiFraud, "Top 5 popular gsm gateway manufacturers".
[5] GoAntiFraud, "Goantifraud blog". https://goantifraud.com/en/blog, n.d.
[6] A. J. Kouam, A. Carneiro Viana, A. Garivier, and A. Tchana, "Génération de traces cellulaires réalistes", in *CORES*, 2022.
[7] A. FlamesGroup, "Answers of voip communications expert olga saiko". https://www.youtube.com/watch?v=YodIXMqw6Ek, August 2011.