SIMBox bypass frauds in cellular networks: a survey

Anne Josiane Kouam, Aline Carneiro Viana, Alain Tchana

SIMBox bypass frauds in cellular networks: a survey

Anne Josiane Kouam D.
Inria, Ecole Polytechnique - IPP
Palaiseau, France
anne.josiane-kouam.djuigne@inria.fr

Aline Carneiro Viana
Inria
Palaiseau, France
aline.viana@inria.fr

Alain Tchana
Inria, ENS Lyon
Lyon, France
alain.tchana@ens-lyon.fr

***Abstract*—Due to their complexity and opaqueness, cellular networks have been subject to numerous attacks over the past few decades. These attacks are a real problem to telecom operators and cost them about USD 28.3 Billion annually, as reported by the *Communications Fraud Control Association*. *SIMBox* fraud, which is one of the most prevalent of these telephone frauds, is the main focus of this paper. *SIMBox* fraud consists of diverting international calls on the VoIP network and terminating them as local calls using an off-the-shelf device, referred to as *SIMBox*. This paper surveys both the existing literature and the major *SIMBox* manufacturers to provide comprehensive and analytical knowledge on *SIMBox* fraud, fraud strategies, fraud evolution, and fraud detection methods. We provide the necessary background on the telephone ecosystem while extensively exploring the *SIMBox* architecture required to understand fraud strategies. Our goal is to provide a complete introductory guide for research on *SIMBox* fraud and stimulate interest for *SIMBox* fraud detection, which remains little investigated. In this vein, we conclude the paper by presenting insights into tomorrow's *SIMBox* fraud detection challenges.**

***Index Terms*—Telephony networks, *SIMBox* fraud survey, *SIMBox*, fraud detection.**

I. Introduction

Telephone fraud presents a considerable problem for Mobile Network Operators (MNO) around the world. According to the CFCA, the global fraud loss is estimated to USD 28.3 Billion in 2019 [1]. In this context, illegal bypass termination [2] also known as *SIMBox* fraud is by far one of the most prevalent fraud affecting the telecommunication market [3]. In many countries, the international termination rate (ITR) is considerably higher than the local (retail) termination rate (LTR) within the country (e.g., up to $2.8 - 28$ times of difference in Cameroon [4]). This makes it profitable for fraudsters to bypass the regular interconnect operator when terminating calls in the country as they can pay the lower local rate instead of the ITR. *SIMBox* fraud is a major problem in developing countries (e.g. about 78% of African countries and 60% of Middle Eastern countries are fraud destinations [5]). Besides, in some these countries, as much as 70% of incoming international call traffic is terminated fraudulently [6]. This could result in losses of up to USD 39.9 Million as in Cameroon in 2015 [7]. This practice is thus illegal in most countries and mainly, in developing countries.

The simplest way of committing bypass fraud involves setting up a *SIMBox* (VoIP GSM gateway). This is a standard device that can be easily acquired via the internet and equipped with a bundle of SIM cards. The calls are typically routed via an internet flow (VoIP) to the *SIMBox* residing in the terminating country. The *SIMBox* then converts the VoIP call into a local mobile call to the receiving party on the local cellular network.

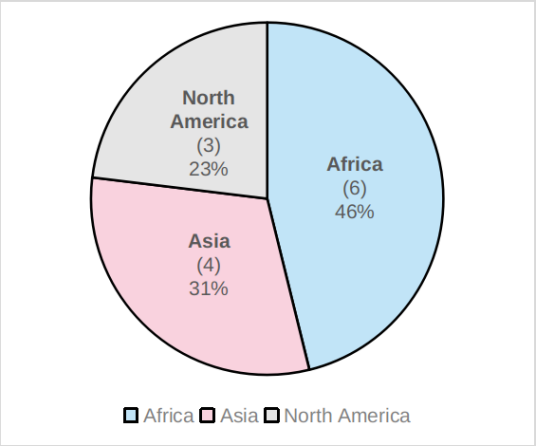

Fig. 1. Distribution of *SIMBox* fraud investigation work by continent.

SIMBox fraud is a significant problem for telecommunication operators and tax authorities of the affected countries, as international traffic taxes cannot be collected. Beyond direct revenue loss, bypass fraud also leads to poor customer experience. Examples of such call quality experience degradation are low voice quality due to latency issues, highly-compressed IP connections, longer call set up time, or still, missing or incorrect Calling Line Identifier (CLI). In particular, this latter results in many call rejections by the called party, while missed calls are not returned. Such degradation impacts the customer experience, which has a direct effect on loyalty, lifetime value, and revenue. All of this results in the *SIMBox* fraud being in the top three types of phone system frauds that cause a significant loss to mobile network operators [8].

Few research works have investigated this issue (a total of 13 publications distributed by continent in Figure 1). We believe this is essentially due to the fact that the fraud mainly affects developing countries, though some papers discussed the issue in USA.

The purpose of this manuscript is to provide all the necessary elements to understand the *SIMBox* fraud problem in its entirety. It is intended to support readers wishing to begin research into *SIMBox* fraud detection and may spark

new interest in research in this area which is currently little explored. To the best of our knowledge, this is the first paper in the literature presenting the current state-of-the-art of *SIMBox* fraud. More specifically, we present a comprehensive review of the literature on this topic while providing a better understanding of such fraud and discussing open research issues in the area of *SIMBox* fraud detection. In short, we define our contributions as follows:

- We provide an overview of the full telephony ecosystem with the involved mobile telephony network equipment and stakeholders, as well as discuss the main telephony functionality concerned by *SIMBox* fraud, i.e., call routing (see Section II).
- We describe the *SIMBox* fraud ecosystem while explaining how *SIMBox* fraud works, its financial benefits for fraudsters, and what facilitates its existence (see Section III).
- We deeply explore the system behind the *SIMBox* by commenting on its components and architecture (see Section IV). This work is based only on extensive research into the specifications of different SIMBox models; indeed, no similar work has been done in the past.
- We then narrow our focus and consider newer models of *SIMBox* having the advanced capability of simulating human communication behaviour, which hardens detection. In this vein, we examine the temporal evolution of *SIMBox* fraud strategies related to human behavioural simulation (see Section V).
- After extensively exploring the *SIMBox* fraud ecosystem, we study the related detection methods in literature. Here, a categorization of *SIMBox* detection methods is introduced and a qualitative comparison is presented (see Section VI).
- Our main finding is that *SIMBox* fraud is a very tricky problem due to the following aspects: it involves major stakeholders in the telephony area which could be fraudulent; it is related to economic factors for internal development which it would be difficult for developing countries to do without; it is accentuated by the increasing popularisation among mobile subscribers of VoIP applications for international telephone calls.
- As in most security problems, fraudsters are evolving at the same rate, if not faster, than the research community. The use of AI advances (for instance to mimic human behaviour in frauds) has attracted considerable attention because it hardens the identification of fraudulent calls. In this perspective, we highlight some incoming challenges concerning the evolution of telecommunication technologies (such as 5G and 6G) and take the risk in prospecting the frauds of tomorrow (see Section VII).

Finally, we draw conclusions of our work in Section VIII.

II. The telephony ecosystem

The telephony ecosystem has enormously evolved from a level where calls were made through primitive and pre-traced channels to a more complex environment in which numerous frauds have spread. This environment involves several telephone networks and specialized equipment able to switch from these networks to others, forming a global architecture which is outlined in Figure 2. This section presents the full telephony ecosystem.

A. Mobile telephony networks

1) Cellular networks: Cellular devices are widely used for more than just entertainment and phone calls, and their scale is becoming greater and more significant. The cellular network is an open public network to which end subscribers have direct access through distributed over land areas, named *cells*, each served by at least one fixed-location transceiver, known as *base station*. For a customer, the *Mobile Equipment* is the entry point to the 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. From a more technical perspective, the SIM card is uniquely identified on the network by its *International Mobile Subscriber Identity* (IMSI); it contains a cryptography key assigned by the operator to encrypt communication. The IMSI is used by the mobile equipment (i) to detect the provider's network amongst surrounding emitted beacon frames, and (ii) to get attached to that network through the base station. Each generation of mobile communication uses encryption over the wireless channel and specific equipment to handle communications and customer identification. Yet, at the level of a provider, mobile devices can use different generations of mobile communication to access the network.

Call and SMS routing are services provided by cellular networks and involve several connected types of equipment. Base stations are connected to a *Mobile Switching Center* (MSC) of the core network through the base station controller. The MSC is responsible for keeping and updating subscriber information in the *Home Location Register*, registration and authentication of subscribers with the help of the *Authentication Center*, and call/SMS routing. Some MSCs provide an access gateway to the PSTN network or to an external IP network like the Internet. They are called *Gateway MSCs* (GMSC) and do not manage base station controllers.

Last but not least, operators keep track of all services transiting on their networks and resource use. This is done through network switches, where *Charging Data Records* (CDR[1]) are generated. CDRs are collected and processed through *Charging Gateway Functions* [10] in a central location. There, they can be used for billing purposes or by fraud management units (referred to as *Revenue Assurance and Fraud Management* [11]) for telecommunication fraud prevention or detection.

2) VoIP networks: Voice over IP (VoIP) is a technique that makes it possible to transmit voice over wired (cable/ADSL/optical fiber) or wireless (satellite, Wi-Fi, UMTS

[1]Once referred to *Call Detail Records* and later to *Charging Data Records* in the 3GPP specification [9]

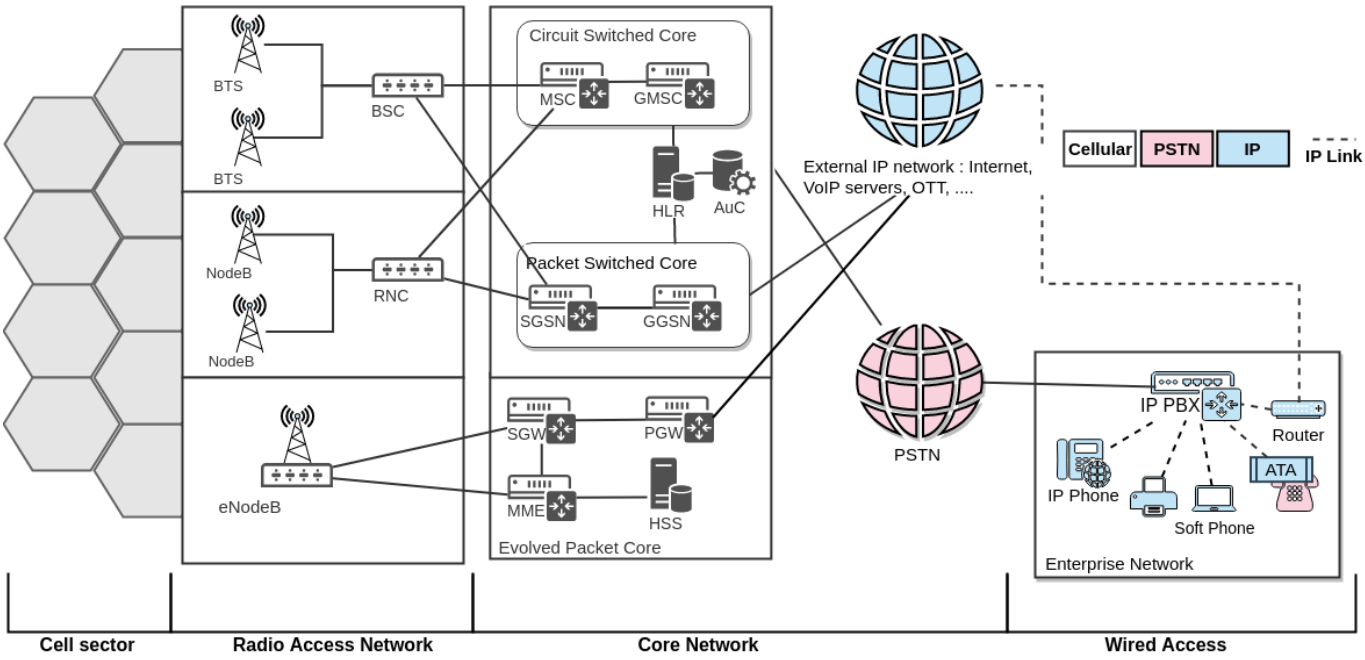

Fig. 2. Telephony networks architecture overview : Cellular network, PSTN network, VoIP network and gateways; from the access to the core.

or LTE, etc) IP networks, whether private networks or the Internet. VoIP network's whole idea is based on *VoIP servers*, *VoIP clients*, and *VoIP gateways* exchanging data and signaling information according to specific protocols. VoIP servers provide authentication, management, accounting, transport, billing, and routing services to VoIP clients in any IP network. VoIP clients are hard phones (also referred to as IP phones), soft-phones (any computing device with specific software to exchange over VoIP), and even analog phones combined with an *Analog Telephone Adapter*. VoIP gateways are specific network types of equipment, allowing VoIP voice calls and fax to reach the PSTN and the cellular network and vice-versa. Through a media and a signaling components, VoIP gateways compress and packetize voice data, deliver output packets to and from an IP network [12]. Some IP-PBXes (IP Private Branch Exchange)[2], for instance, can ensure a VoIP gateway function from the company's internal IP network to the external PSTN network (see Figure 2).

To ensure the compression and the packetization of analog voice signals for transmission over digital line, while keeping a certain acceptable quality for end-users, specific algorithms (called codecs) are designed. Codecs are used to encode voice traffic picked up by the microphone to digital data and encapsulate that data such that its transmission is faster and the call experience is better. There are several codecs, proprietary, and open-source ones, determining the sound quality and bandwidth usage. The more bandwidth a codec requires, the better the voice quality is. The choice of an appropriate codec is, therefore, strictly relative to the network efficiency. [12] summarizes the most well-known voice codecs. Some codecs are provided on the top of signaling protocols, which ensure codec configuration and other key functions in a call establishment. A signaling protocol enables network components to communicate with each other, establishes a multimedia session between two or more participants of the call, maintains it, and tears it down. *Session Initiation Protocol* (SIP) is a well-know application-layer VoIP signaling protocol. As such, it can allow interoperability between VoIP types of equipment from different manufacturers. More details on signaling protocols covering services are described in [12].

VoIP is also available on cellular networks. Some applications called *Over-The-Top* (OTT) apps (e.g., Skype, Discord) have been developed on the top of VoIP networks and provide for instance cheap call services, attracting more users and seen as a threat by mobile operators [14]. Cellular networks provide mobile connectivity through the Packet Switched Core comprising a *Serving Gateway Support Node* and a *Gateway GPRS Support Node* to fulfill packet-switched data transfers.

VoIP is cheaper than other telephony networks because it relies on an existing service and infrastructure, the Internet. No new connections need to be made whether the call is local or international: the Internet network has already done all. On the other hand, the quality of VoIP calls is generally poor due to bandwidth sharing (for services other than VoIP) and IP network latency. As a result, calls are affected by packet losses, delay, and jitter. Missing packets that are due to packet loss or jitter cause gaps in the audio. Such gaps are then filled by default silence audio or generated audio with *Packet Loss Concealment* algorithms.

[2]Enterprise usually use a PBX to manage their internal and external communication needs. A traditional PBX provides extensions, i.e., an internal phone number to reach each user within the enterprise. A traditional PBX uses phone cables for all internal lines which is expensive to deploy and manage. To the contrary, an IP-PBX can connect IP phones or soft phones over IP [13]