IJARIIT

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 3)

Available online at: www.ijariit.com

Analysis and detection of SIM box

Vipin Airn
vipin.airn@gmail.com
Kurukshetra University, Kurukshetra, Haryana

ABSTRACT

Over a past two decades, Telecom industry is growing and mode of communication is changing and advanced day by day for catering individual and corporate needs. With the growth and advancement of technologies, telecom frauds are a major concern for research area and delivering the cent percent revenue in the system. Telecommunications fraud is a problem that affects operators all around the globe and one of the most known frauds is illegal to bypass fraud which is used in International voice traffic, in order to avoid carrier charges and this causes opportunity loss of international interconnect usage charge (IUC) to operators and this is major concern for research scope and impacting the revenue at operator level. As a result, cellular operators around the globe lose billions annually. Moreover, SIM box compromises the cellular network infrastructure by overloading local base stations serving these devices. This paper analyses the fraudulent termination of international traffic so suggest statistical, conventional, modern approach for detection of sim box and processes hundreds of millions of anonymized voice call detail records (CDRs). Their outputs of these models are optimally fused to increase the detection rate of sim box. The operator's fraud department confirmed that the algorithm succeeds in detecting new fraudulent SIM box.

Keywords: *IUC (Interconnect Usage charges), CDR (Call detail records), Artificial Intelligence, Bypass Fraud, SIM (subscriber identity module), MO (Mobile Originator), MT (Mobile Terminator), VOIP (Voice over internet protocol).*

1. INTRODUCTION

Imagine you get a call from Unknown local MSISDN and when you pick up the phone and it's from a friend or a family who is living abroad, it does feel strange that you would receive an international call from a local number; this is basically the bypass fraud, or in a case of SIM box method. In this case, the international calls are routed through illegal bypass and feed into box that generally referred as Sim Box which contains multiple sim with low tariffs packs activated to route call. Below graph shows the most prevalent fraud's occurring at network level.

2. IMPACT OF FRAUD ON TELECOM INDUSTRY

Telecommunications, which have become a necessity worldwide and advanced day by day that is reducing communication barriers around the globe, became a motive for fraudsters who are making a lot of money out of illegally accessing communication Set up and using it to make huge profits, by selling services at much lower prices than their original prices. According to a survey by the Communication Fraud Control Association (CFCA) [1], the mobile telecom industry lost $ 29.2 Billion (USD) in 2015 alone due to telecom fraud. Besides those big losses, telecom fraud causes other indirect losses to mobile operators, like: decrease in quality of service, denial of service and network congestion, Customer Churn, Customer dissatisfaction are major challenges that arise due to telecom fraud. Bypass fraud costs telecom companies 6 billion annually and ranked the 2nd most costly fraud worldwide. Fig. 1 shows the top 3 fraud types with their annual losses. The numbers are huge, since major mobile operators in could degrade the country's GDP. Sim box is also one of major retail fraud that globally shares 10-15% of total losses determined by all frauds in telecommunication industry.

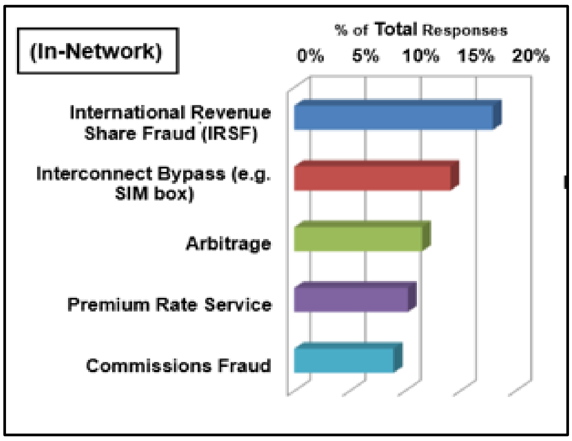

Fig 1. Fraud Responses as per CFCA Report

Unfortunately, more than 80 percent of mobile operators have already experienced SIM box fraud. Africa seems to be the hub for mobile network fraud, with mobile operators there getting hit hard when SIM boxes are used fraudulently. SIM box fraud is leading telecom providers around the world to secure and protect their networks from the phenomenon.

3. SIM BOX

SIM Box basically terminates international traffic into local and at the destination network (at MT Level) local CLI reflects at MT level. At this fraudster pay only local charges or some time usage cheap local tariffs and cards for the termination of traffic. The calling person is paying the international call rates for connecting calls but carriers and destination operator will not able to collect the international call carrier charges and termination charges for the call. Fraudster make money to route calls illegally and earns the benefit of international carriers and termination charges but at the end fraudster have to pay only local termination charges. Sim Box Causes economic loss as well degrade the services of operator, often call quality, congestion network, which results in dissatisfied customer and that cause churn. Detecting sim box over a huge international voice traffic is similar like searching few needles in a huge haystack full of small objects that have same appearance like needles. While operators of the intermediate and destination networks have high financial incentives to understand the problem, they do not have the data to analyze the international calls that are gone because the traffic is terminating MSC is only local traffic only. Also, the absence of publicly available SIM box-related data is a major obstacle for emerging of comprehensive studies on voice bypassing fraud analysis and detection.

Bypass fraud: - To understand how bypass fraud is committed, firstly we describe the legitimate way for international calls. Let's assume that MO (Caller A) and MT (caller B) live in different countries. Caller A makes a call to caller B over the mobile operator. The mobile operator of country A takes the call and send it through his international gateways to carriers (Transit operators). The transit operator then routes the call through legitimate paths and pay a toll to transit operator for landing call to the destination address. When a call is routed through the legitimate path then transit operators and MT operator earns international charges for termination of the call. Basically in Bypass fraud Scenario fraudster basically abuse the international traffic and reroute the traffic illegally by using VOIP (Voice over internet protocol) through sim box. The legitimate route of international call In bypass fraud, the transient operator route the call through a SIM box placed in country B using VoIP, the SIM box then re-route the call through country B mobile operator and pay for just the local tariffs for termination of traffic as presented in given picture of sim box method.

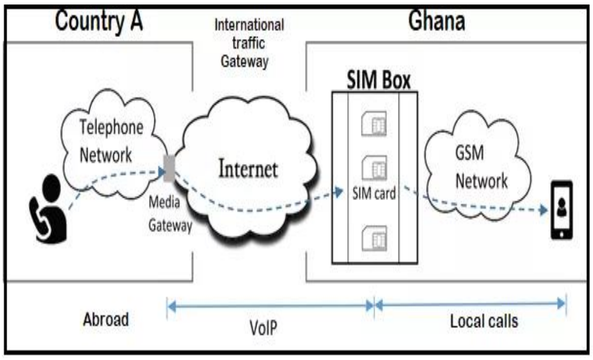

Fig 2. SIM box method for illegal routing

On-net bypass: - In on-net Bypass fraud calls are routed through same operators Sims which are placed in sim box, it this scenario MT operator gets the maximum loss as all calls are local on-net calls so MT Operators gets the opportunity loss of earning international termination charges.

Off-net bypass: - In off-net bypass call are routed and terminated from the different operator so MT operator gets local termination charges instead of international termination charges. In that fraud, MT operator gets the marginal opportunity loss of international carriers but in comparison of international termination and local termination charges have a massive difference so that is also high impact on revenue at the retail level for operators for Off-net Bypass.

4. INTERNATIONAL SIM BOX

To begin international sim box, traffic aggregator carriers sit outside the destination country where the interconnect rate is comparatively high, such as Pakistan, India, Bangladesh, Indonesia, and many others and route the international traffic to pirate carrier (illegal Carrier) and feed traffic to Sim box and then call is terminated to MT (Destination address). In some cases, these traffic aggregators are getting traffic directly from operators too, and their interest is simply to make a profit by terminating traffic at a much lower rate. And they do that by handling over traffic to illegal terminators in the target country. The idea behind international Sim box pass the international traffic over internet cloud, bypass the international gateway exchange. The fraudster usually takes advantage of cheap local tariffs, bundle offers, which earns lower per minute revenue to operators than interconnect rate that can earn from international carriers. For example In Pakistan's case, for example, the operators are losing about half a cent compared to one cent per minute on the interconnect rate. The loss to licensed international carriers is about 5 cents and the government about 2 cents per minute. The winners are the fraudsters, who need a very small investment to steal big money.

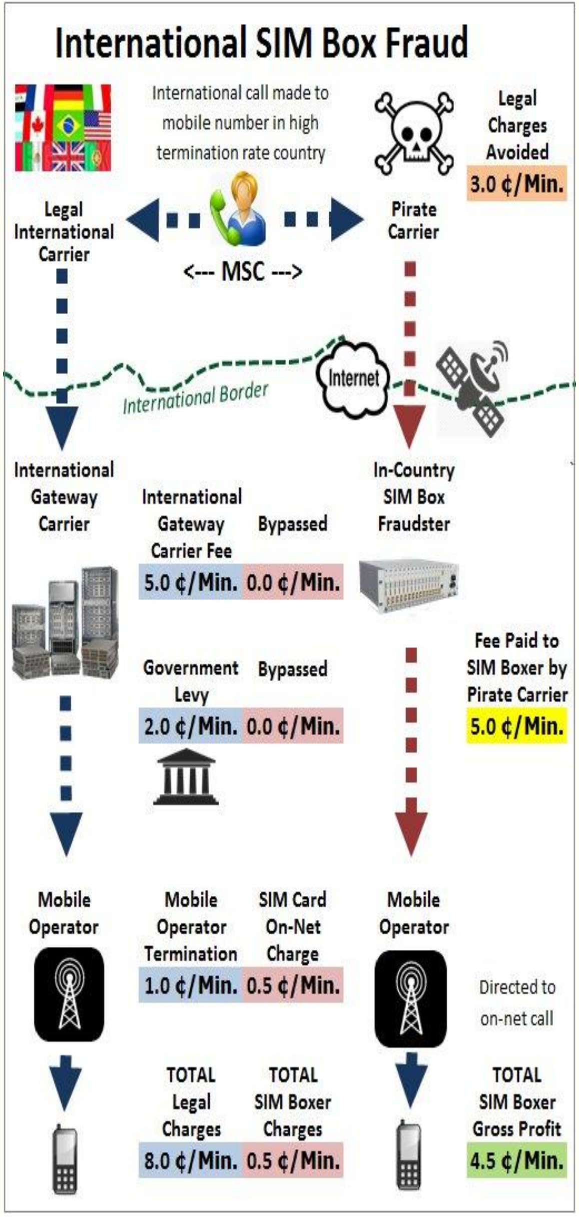

Fig 3. International SIM box

In the above picture if international traffic is routed through a legitimate path which is shown in blue dotted line then total 8.0 ¢/minute will flow from transit operator and destination operator for termination of the call. If call is routed through illegal carrier (Pirate carrier means carrier which is used to bypass the international call to Sim box for getting marginal benefits where the termination cost is high comparatively) the fraudster have to pay 5.0 ¢/minute to intermediate carrier and rest 4.5 ¢/minute (Pirate Carrier provide 5 ¢/minute to sim box so that sim box have to pay only 0.5 ¢/minute for landing local traffic so total profit earned by sim box is 5 ¢/minute – 0.5 ¢/minute = 4.5 ¢/minute.

5. ROAMING SIM BOX

In Roaming Sim box fraud the sim which is inserted in sim box belongs to those countries where either roaming charges or IUC charges are less or may be both. Let us consider an example if the call is received at MT level and Tanzania CLI reflects at receiver level but calling party is calling from Uganda so that is a case of roaming fraud. Basically in roaming fraud is hard to detect as the customer is Uganda customer is roaming in Tanzania so there will be a delay in CDR or TAPIN data processing from roaming or latching operator so the fraudster will enjoy the benefits from sim boxing and Roam Fraud in that scenario in that case. Roaming fraud comes is picture basically in African Countries where the international IUC charges are less.

6. FRAUD DETECTION METHOD

1) A statistical method for Fraud detection:-

B Party Diversity: - By checking the B party Diversity (Calling Number diversity) we can trace the Sim Box. In Ideal case scenarios, B Party diversity is between 95-98%. By checking B party diversity can estimate the sim box but in that method marketing, sales and corporate calling are excluded.

Around the Clock calling: - If the customer is making call 24 X 7 that means it is suspicious usage pattern because it resembles machine calling pattern or Algorithm based calling pattern.

Geographical Location: - Geographical location should be less than 03. For Ideal, Sim Box Scenarios Geographical location is 01 so by taking the traces of geographical location we can detect the sim box pattern like why the customer is making calls from one location or without movement so it is also an important parameter to detect sim box.

Outgoing V/s Incoming calls: - Incoming calls should be less than outgoing calls. Basically, in Sim box Scenarios ratio outgoing calls are 90% or more as compared to incoming calls.

International Calls V/s Local Calls: - International calls should be less than Local calls. Basically, in Sim box Scenarios ratio, Local calls are 90% or more as compared to international calls. In sim box, international traffic is fed so that it converts international traffic to local calls so mostly calls will be local calls in sim box scenario. If sim box traffic is programmed like it is reflecting international calls so all calls will be derived from random series or **'+'** so that we can analyze one parameter of sim box.

Less or No GPRS Usage: - For ideal sim box scenarios no GPRS usage found or very less GPRS usage found in Sim Box Cases**.**

Less or No SMS Usage: - For ideal sim box scenarios no SMS usage found or very less SMS usage found in Sim Box Cases.

At Receiver Level: - For Sim box Scenarios at receiver end's Local CLI, Reflects of that country code will reflect so if we come across that scenario while taking the international call so same will be immediately reported to the operator for blocking those Sim box series.

Call quality Analysis: - It might be a factor of sim box while in case of sim box scenarios the call quality drops so at operator level if the customer is the same location is making a complaint about call quality so that can be a case of Sim box.

2) Blacklisted IMEI:- By using Blacklisted IMEI in FMS (Fraud Management system) we can maintain that list which is already blacklisted in any fraud and again some traffic is generated on those numbers so we get alert for the same so we can trace the sim boxing and others fraud in minimal span of fraud run time.

3) Deduping Method: - By inspecting single MSISDN we can trace all the MSISDN that is used or activated by Single IMEI and after that we can do further traffic analysis and can trace all the series of sim box numbers and further we can trace all the IMEI in those these sim are placed after that we can figure out all the Sim that are activated or used by IMEI that data can be extensively analyzed for getting Sim Box MSISDN's.

4) TCG (Test Call Generator): - Test Call Detection is One of the effective methods to detect SIMs used in SIM box traffic which is routed through local path for termination. The incoming call will appear from Local CLI while receiving an international call; that means that international calling path is routed by illegally sim box technology so same data or number.

7. REFERENCES

[1] http://www.cfca.org/fraudlosssurvey Communication Fraud Control Association, 2015 Global Fraud Loss Survey [Internet]. 2015 [cited 2016 Dec 3].
[2] M. Yelland, "Fraud in mobile networks," Comput. Fraud Secur., vol. 2013, no. 3, pp. 5–9, 2013.
[3] R. S. A. H. Elmi, S. Ibrahim, "Detecting SIM Box Fraud Using Neural Network," IT Converg. Secur. 2012, vol. 215, pp. 575–582, 2013.
[4] R. Sallehuddin, S. Ibrahim, A. Mohd Zain, and A. Hussein Elmi, "Classification of SIM Box Fraud Detection Using Support Vector Machine and Artificial Neural Network," Int. J. Innov. Comput., vol. 4, no. 2, pp. 19–27, 2014.
[5] B. Reaves, E. Shernan, A. Bates, H. Carter, and P. Traynor, "Boxed Out : Blocking Cellular Interconnect Bypass Fraud at the Network Edge," USENIX Secur. Symp. 2015, pp. 833–848, 2015.
[6] I. Murynets, M. Zabarankin, R. P. Jover, and A. Panagia, "Analysis and detection of SIMbox fraud in mobility networks," Proc. - IEEE INFOCOM, pp. 1519–1526, 2014.
[7] http://www.cfca.org/fraudlosssurvey Communication Fraud Control Association, 2015 Global Fraud Loss Survey [Internet]. 2015 [cited 2016 Dec 3].
[8]https://www.google.co.in/search?q=simbox+pictures&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjax93y7ejaAhUOPrwKHQi6C_YQ_AUICigB&biw=1366&bih=662#imgrc=YuUNfNLbyuN2oM:

[9]https://www.google.co.in/search?q=simbox+pictures&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjax93y7ejaAhUOPrwKHQi6C_YQ_AUICigB&biw=1366&bih=662#imgrc=YuUNfNLbyuN2oM:

AUTHOR PROFILE

Mr. Vipin Airn is currently working in Telecommunication Field. He is completed M.Tech. From Kurukshetra University, Kurukshetra and B.Tech. (Hons.) From M.D.U. Rohtak, India. He has 03 years of professional experience in Telecom domain with Operator like Vodafone, Airtel, and Idea. Mr. Vipin Airn has authored 1 research papers and areas of interest include Communication Systems, Wireless and Mobile Communication, Digital Signal Processing and Telecom Engineering and communication.