TAF

Journal of Applied and Physical Sciences

JAPS

2016, **2**(3): 77-81

PRIMARY RESEARCH

Dynamic detection system design of fraud simbox to improve quality service of international incoming call

Edi Sukamto [1*], Dadang Gunawan [2]

[1, 2] Department of Electrical Engineering, University of Indonesia, Depok, Indonesia

Index Terms
SIMBOX
Fraud detection
Design

Received: 26 July 2016
Accepted: 26 August 2016
Published: 25 October 2016

***Abstract*—** International Direct Dialing (IDD) is one of the services based on the Telecommunications Operator clear channel access and Voice over IP (VoIP). In running this business, Operators face Grey Operators who do illegal practices by passing traffic of international incoming call without going through the official international service providers called Fraud Subscriber Identity Module Box (SIMBOX). The impacts of this practice are not only the revenue decline, but SIMBOX also provides less good image for the operator because of the low quality service. Some operators have made efforts to implement the mitigation of traffic SIMBOX fraud detection system. This study aims to improve the detection of fraud traffic and maintain the quality of service. This study redesigns the existing SIMBOX fraud detection system to become a dynamic detection system by adding a dynamic control algorithm and is simulated using MATLAB simulation approach. A dynamic system is indispensable as there are various fraud traffic flow profiles that always change and could not be predicted. The results of this study indicate that fraud detection SIMBOX could be improved up to 5,000% and could increase potential revenue to $ 2 billion per month. Thus the fraud detection SIMBOX dynamic system will provide greater detection results than the previous system.

I. INTRODUCTION

Fraud traffic is a challenge that must be faced in the telecommunications business [1-5]. One is fraud on voice traffic termination that is often called SIMBOX fraud as illegal activity on the network (mobile). As a result, mobile operators around the world lose billions (approximately 3% of revenues) each year [1]. One scenario calls fraud committed are hijacking international call termination and transferring them via the Internet to mobile devices as shown in Figure 1. [1].

Official calls from Country A (Alice) and Country B (Bob) in Figure 1.1 should pass through the green line with international interconnection tariffs in accordance with the agreed global operator. But in reality, the route of operator A network is dircected through the Internet (VoIP) at very low rates. In Country B, call is injected back into the operator's network using SIMBOX device with the same SIM card that is used to call on the operator B and resulting in On Net local call (same operator) or off net that is running the specific business scheme with a cheaper price. In this way, SIMBOX operator gains profit from high prices of international termination by just paying a cheap price of domestic calls through the operator B.

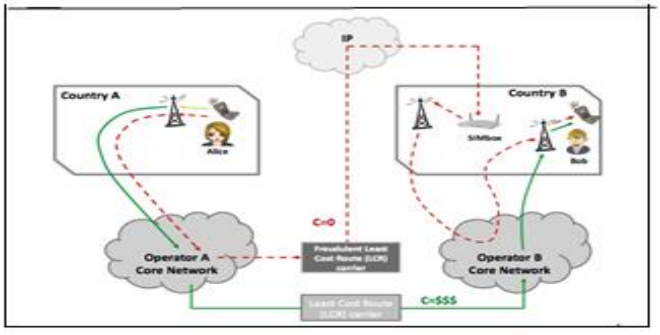

Fig. 1 . International fraud incoming call scenario

*Corresponding author:Edi Sukamto
†Email: edi.sukamto@ui.ac.id

The detailed losses suffered by Operator include:
• Revenue Loss for both operators of IDD service providers and operators as termination (end operator).
• Capital Expenditure (CAPEX) is not according to plan, because this SIMBOX Fraudster can be mobilized easily so it will burden certain BTS and then burden the other BTS.
• The decline in Quality of Services and Image of Operator as network operators experience congestion resulting in customer complaints due to the difficulty in making a call.

One drop in revenue as a result of this fraud can be seen from the decline in the production of one of the incoming international Global Partners X as shown in Figure 2.

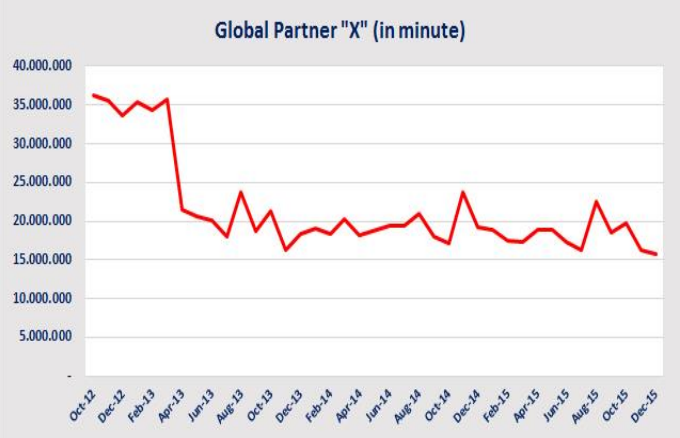

Fig. 2 . The decrease in production due to SIMBOX traffic [7]

II. INTERCONNECTION AND FRAUD DETECTION

Interconnection is the interconnection between telecommunication networks of different telecommunication network operators. Interconnection between telecommunications operators must be implemented in Indonesia to provide assurance to users to access telecommunications services.

A. Point of Interconnection (PoI)

In Telecommunication Networks, Point of Interconnection (PoI) is the meeting point between two (2) Telecommunications Operators that interconnects them. Technically, the junction is in the established network Digital Distribution Frame (DDF) Central Gateway (SG) Telecommunications Operators used to channel all traffic interconnections that occur or occur elsewhere by agreement of the parties. Through the PoI, all contracted traffics are distributed.

B. Cost of Interconnection

Interconnection costs arising from Interconnection Service are based on call-per-call (call by call basis). In addition, the cost of interconnection opens the possibility for adjustment of Interconnection fee on the basis of economic value which is determined based on the committed amount / volume capacity and amount / volume of traffic.

C. Fraud Detection System

When there is communication between the Operator (operator) network with other networks without going through the operator PoI and free of charge interconnection, then there is a fraud as in the case of incoming international services above. In the effort of minimizing the risk, some operators have been implementing a fraud detection system model through dummy call.

The algorithm used to detect fraud traffic is to provide a device Call Traffic Generator and some domestic SIM Card carriers that are used as the originating number (A #). These devices perform a dummy call every day that is fixed with a determined schedule. Call is routed towards Global Partner that acts as Huber Tier-1 and then supplied to Huber Tier-2 or Tier-3. Call traffic is distributed by Huber Tier-2 or Tier-3 to SIMBOX operator via the internet link access with large capacity that is leased from Network Access Provider (NAP) or the Internet Service Provider (ISP). Call traffic from SIMBOX enters the terminating number (B #), and then it is captured by the receiver and monitoring system. The next process is verifying the numbers from call traffic, and if the numbers are not the same as the originating number (A #) that have been generated before, then the numbers are confirmed as the numbers of fraud used by SIMBOX Operator and then those numbers are blocked[6].

D. Fraud Traffic Flow

The amount of fraud traffic has changing patterns. Fraud traffic happens because of cooperation via internet traffic routing between global carriers and domestic carriers in the termination state (destination). Usually traffic fraud scheme is carried out based on certain business scheme within a specified period. This causes traffic routing patterns of fraud vary widely, in order to meet committed volume, global carriers can deliver traffic fraud in large numbers within a certain period.

ISSN: 2414-3103
DOI: 10.20474/japs-2.3.2

III. DYNAMIC SYSTEM'S DESIGN

A dynamic system is designed by adding a dynamic control algorithm. In this algorithm, each dummy call sent within t minutes will change if traffic fraud condition that occurs also changes as shown in Figure 3.

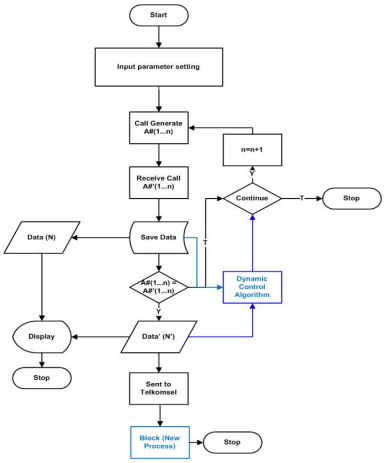

Fig. 3 . Dynamic process system block design

A. Model Simulation

By sampling the dummy call which is sent and is injected as fraud, the number of dummy calls that are sent can then be created for the transfer function (method ARMAX)[8-11]. MATLAB simulation model is shown in Figure.4.

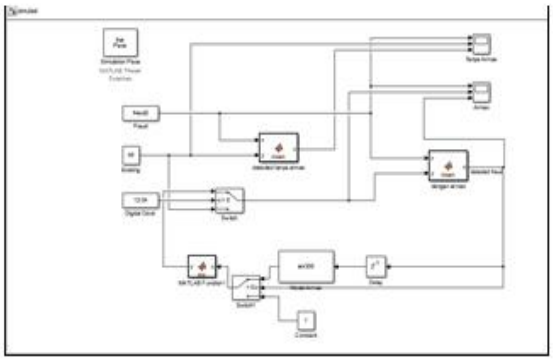

Fig. 4 . System simulation Model with MATLAB 2015

B. Traffic Fraud Flow Profile

Traffic fraud flow profile that was tested in this experiment shows 6 profiles as follows:

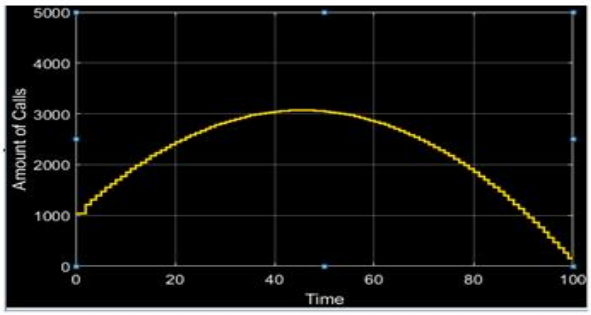

Fig. 5 . Fraud-1 profile

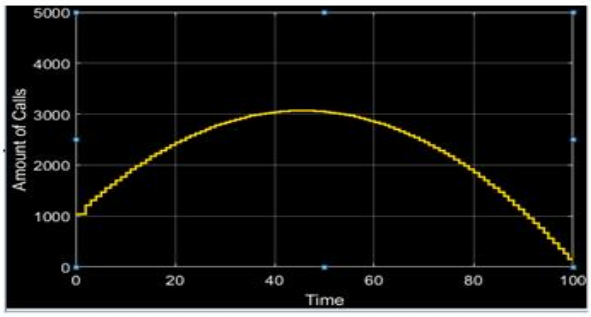

Fig. 6 . Fraud-2 profile

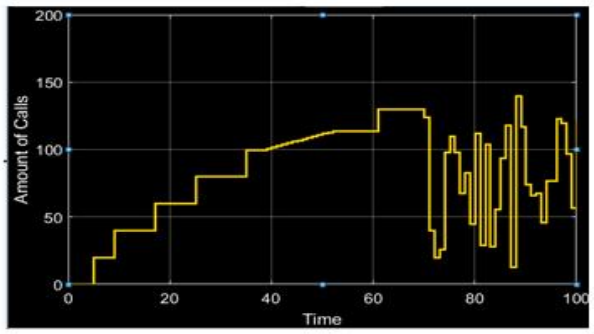

Fig. 7 . Fraud-3 Profile

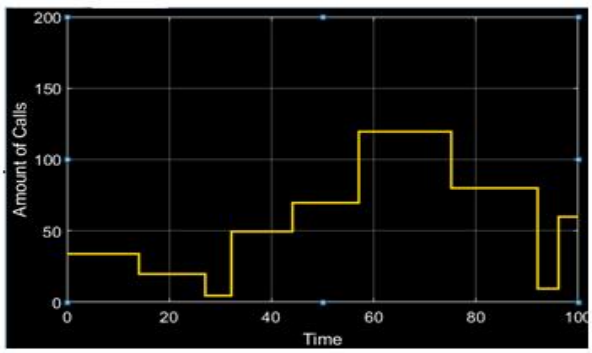

Fig. 8 . Fraud-4 profile

ISSN: 2414-3103
DOI: 10.20474/japs-2.3.2

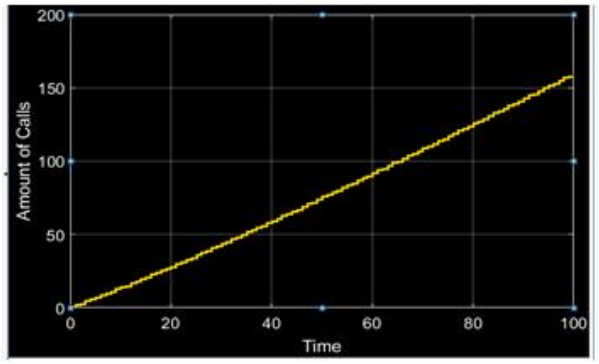

Fig. 9 . Fraud-5 profile

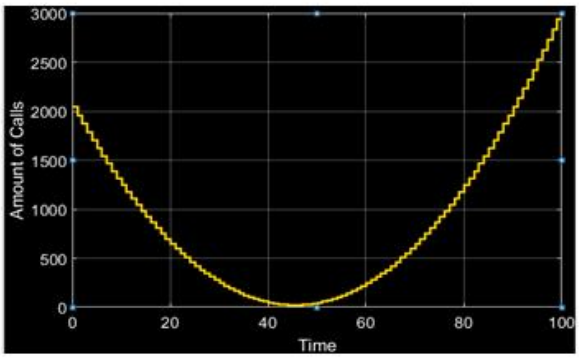

Fig. 10 . Fraud-6 profile

IV. SIMULATION RESULTS AND ANALYSIS

The results of the simulation of dynamic systems against fraud profile-1 can be seen as in Figure 11.

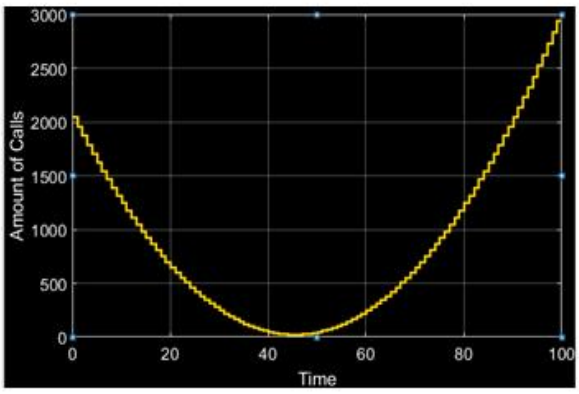

Fig. 11 . Existing system detection result

Figure 11 and Figure 12 show the simulation results of the detection of fraud against fraud-1 flow profile. The blue line represents the number of dummy calls generated from the system, the yellow line represents the detected model of fraud traffic flow and the orange line represents the maximum fraud that is detected (the number of fraud traffic itself). In Figure 12, it is shown that the parameters of dummy call on the existing system are set 40 calls per 3 minutes, so that the maximum chance of traffic fraud that is able to be detected was 4,000 calls (40 calls / t x 100t), according to the number of dummy calls sent (orange lines). With the amount of traffic fraud amounting to 222,121 calls, the loss opportunity for fraud that occurred was 218,121 calls.

With the implementing of the new system as shown in Figure 12, dummy call sent will be continuously improved in line with the amount of fraud detected. It is seen in the picture on the t-13, the number of dummy calls sent is greater than the amount of fraud that occurs so that there is a maximum chance of detecting the entire fraud flow of traffic being streamed. In this condition, the amount of traffic fraud that is able to be detected amounted to 209,970 calls, an increase in the number of detected fraud is 205,970 calls, or there is an increase up to 5,097% so that loss of opportunity that happens could be reduced to 12,151 calls.

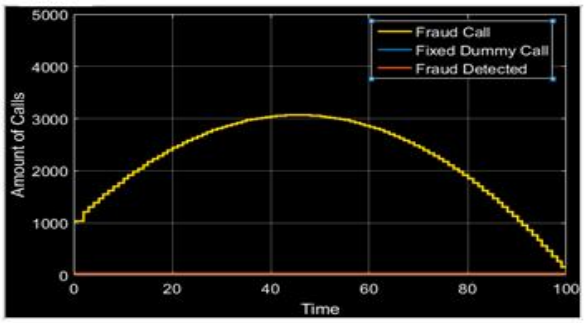

Fig. 12 . Results of dynamic detection system

V. CONCLUSION

From the results of simulation and analysis, we concluded that fraud detection SIMBOX dynamic systems can improve system performance by providing larger fraud detection results. Detection results of the existing system and dynamic profile fraud-1 to 6 can be seen in Table 1

ISSN: 2414-3103
DOI: 10.20474/japs-2.3.2

TABLE 1
COMPARISON RESULTS OF EXISTING (FIXED) SYSTEM DETECTION (BEFORE IMPROVEMENT) AND DYNAMIC (AFTER IMPROVEMENT)

	Before Improvement (Fixed Syatem)				After Imprfovement (Dynamic System)			
Fraud Profile	Total Fraud Call	Dummy Call	Fraud Detection	Max Probability	Dummy Call	Fraud Detection	Max Probability	% of Detected fraud
Profil-1	222.121	4.000 (fixed 40 call per 3 menit)	4.000	2%	286.691(dinamik per 3 menit)	209.970	95% 5	097%
Profil-2	12.734	4.000 (fixed 40 call per 3 menit)	3.730	29%	16.721(dinamik per 3 menit)	12.195	96%	227%
Profil-3	7.995	4.000 (fixed 40 call per 3 menit)	3.636	45%	9.655(dinamik per 3 menit)	7.051	88%	94%
Profil-4	6.131	4.000 (fixed 40 call per 3 menit)	3.401	55%	7.948(dinamik per 3 menit)	5.812	95%	71%
Profil-5	7.786	4.000 (fixed 40 call per 3 menit)	3.461	44%	10.519(dinamik per 3 menit)	7.786	100%	125%
Profil-6	87.910	4.000 (fixed 40 call per 3 menit)	3.963	5%	101.423(dinamik per 3 menit)	74.947	86%	1768%

REFERENCES

[1] I. Murynets, M. Zabarankin, R. P. Jover and A. Panagia, "Analysis and detection of SIMbox fraud in mobility networks," in IEEE INFOCOM IEEE Conference on Computer Communications, 2014, pp. 1519-1526.

[2] A. Aljarray and A. Abouda, "Analysis and detection of fraud in international calls using decision tree," 2015. [Online]. Available: goo.gl/gUg9Kd

[3] P. Hoath, "Fraud overview, TAF regional seminar on costs and tariffs," 2015.

[4] Simon Woodhead, "VoIP fraud analysis," 2015. [Online]. Available: goo.gl/z42ip5

[5] i3 Forum, "International interconnection forum for services over IP (i3 Forum), IP international interconnections for voice and other related services," 2015. [Online]. Available: goo.gl/XyT5em

[6] R. Zaenal, "Analisis pengendalian risiko bisnis layanan wholesale incoming SLI Telkom = Risk control analysis of telkom incoming SLI wholesale," University of Indonesia Liberary, Depok, Indonesia, 2013.

[7] PT. Telekomunikasi Indonesia "Operational Review DWS : Realisasi Monitoring Hasil Deteksi Fraud SIMBOX periode tahun 2015". Jakarta. Indonesia, TELKOM, Divisi Wholesale Service, 2015.

[8] D. S. Stoffer, "Estimation and identification of space-time ARMAX models in the presence of missing data," *Journal of the American Statistical Association,* vol. 81, no. 395, pp. 762-772, 1986. **DOI:** 10.1080/01621459.1986.10478333

[9] R. T. Baillie, "Predictions from ARMAX models," *Journal of Econometrics,* vol. 12, no. 3, pp. 365-374, 1980. **DOI:** 10.1016/0304-4076(80)90062-7

[10] J. Pakanen and S. Karjalainen, "An ARMAX-Model approach for estimating static heat flows in buildings," *Jouko Pakanen & Sami Karjalainen,* vol. 4, no. 5, 2002.

[11] L. He and M. Karny, "Estimation and prediction with ARMMAX model: A mixture of ARMAX models with common ARX part," *International Journal of Adaptive Control and Signal Processing,* vol. 17, no. 4, pp. 265-283, 2003.

— This article does not have any appendix. —

ISSN: 2414-3103
DOI: 10.20474/japs-2.3.2