

Battling illegal call operations with Fraud Management Systems

Nokia Siemens
Networks



Executive summary

Contents

- 02 **Executive summary**
- 03 **Compare: ratio of incoming to outgoing calls**
- 03 **Examine: ratio of on-network to off-network calls**
- 04 **Look: no or low mobility**
- 05 **Scrutinize: many subscribers on one cell and track suspicious activity in close proximity**
- 05 **Ring, ring: high number of calls to distinct numbers**
- 06 **Goodnight calls: unusual number of night calls to distinctive numbers**
- 06 **Your friendly operator speaking: voice-only service usage**
- 07 **Gotcha!: avoiding false positives**
- 08 **Attention: best practices**
- 10 **Regulatory issues with GSM gateways**
- 11 **Conclusion**

Telecommunication operators worldwide have lost a significant amount of revenue from interconnection bypass, mainly due to increased usage of GSM VoIP Gateways - often called SIM Boxes - and technology advances in GSM gateways and VoIP technologies. GSM VoIP Gateways are telecommunication devices that enable calls from fixed, mobile or Internet telephones to be routed through VoIP directly into a relevant GSM network. The most advanced GSM gateway installations can utilize hundreds of mobile SIM cards, provide SIM rotation functionality, allow remote pre-paid recharging, feature antenna splitters and can even store SIM cards off-site.

GSM gateways are often installed in an office's private automatic branch exchange (PABX) in a bid to save costs on office to mobile calls - this is legal in most countries. However, offering commercial telecommunication services such as providing international call termination via GSM gateways without a GSM operator's approval is usually illegal.

Fraud management systems (FMSs) are growing in popularity and this has impacted illegal international call termination gateway operators. For the first time, GSM operators have been utilizing FMSs to carry out sophisticated analysis of CDRs (Call Detail Records) to search for unusual usage behaviour patterns to effectively detect illegal international call termination and block mobile SIM cards engaged in such illegal activities. Although technological advances have allowed GSM operators to better detect such fraud and blocking fraudulent subscribers, the problem still remains unresolved. This is because fraudsters are constantly adapting to new security measures and learning how to counter detection techniques that prevent detection based on analysis of mobile subscribers' usage patterns.

This white paper aims to explain the most common service usage characteristics that allow detection of GSM gateways. It will also describe some of the advanced methods of avoiding detection that are often used by illegal GSM gateway operators.

Compare: ratio of incoming to outgoing calls

It is unusual behaviour for a regular mobile network user to only initiate voice calls, but never receive calls. It is just the opposite with GSM gateways, which frequently initiate outgoing calls to GSM network, but never receive incoming GSM calls. This is because there is rarely any purpose in accepting any calls on GSM gateways, and surely none if a GSM gateway is used to illegally terminate international calls. FMSs are, therefore, able to detect GSM gateways based on this distinctive characteristic of having an unusual ratio of successful incoming to outgoing voice calls. It is not surprising then that this is also one of the first characteristics that fraudsters try to hide to avoid detection.

Novice operators of illegal GSM gateways often divert all calls to mailboxes, or typically never pick up calls. This allows for easy detection by FMSs, enabling operators to block the SIM cards used in illegal call termination. To counter this, more advanced fraudsters try to avoid such distinctive usage patterns. They do this by simply configuring GSM gateways to accept any voice calls, resulting in accepting calls of subscribers who attempt to call back the local VoIP number from the list of missed calls on their mobile phones. This means that when such calls are received on the GSM gateway, incoming calls will be produced, thereby adding incoming calls to CDRs, and making the usage pattern less distinctive. Often, there is more than one call produced for each missed call as subscribers usually will call multiple times upon hearing silence during the first call, attributing it to a network problem.

This new detection avoidance technique was noticed by some telecommunication operators and additional usage profiling was implemented in FMSs.

In addition to just comparing the number of incoming and outgoing calls, operators now also compare the duration of calls, as subscribers calling SIM Boxes will unlikely stay on the call for more than few seconds. Yet, in the constant battle between fraudsters and telecommunication operators, new techniques to prevent detection have also started to emerge.

One of the latest techniques employed by fraudsters is to simply play different versions of pre-recorded messages such as "Please wait. You'll be connected in just a minute", or dial tones normally heard when waiting for users to pick up calls. This is done to increase the duration of incoming calls. If such advanced fraud is detected, operators are able to increase the threshold of ratio of duration of incoming to outgoing calls during profiling. Additionally, when checking if particular numbers are used in GSM gateways, operators should also attempt to talk to subscribers, and not disconnect just after hearing voice, as it could be just a recorded voice message.

Yet, in the constant battle between fraudsters and telecommunication operators, new techniques to prevent detection have also started to emerge. One of the latest techniques employed by fraudsters is to simply play different versions of pre-recorded messages such as "Please wait. You'll be connected in just a minute", or dial tones normally heard when waiting for users to pick up calls.

This is done to increase the duration of incoming calls. If such advanced fraud is detected, operators are able to increase the threshold of ratio of duration of incoming to outgoing calls during profiling.

Additionally, when checking if particular numbers are used in GSM gateways, operators should also attempt to talk to subscribers, and not disconnect just after hearing voice, as it could be just a recorded voice message.

Examine: ratio of on-network to off-network calls

The highest ROI from interconnection bypass fraud can be gained if international calls are routed as local on-net calls. This allows fraudsters to benefit financially from discounted rates for on-net calls and often, additional discounts such as free late night calls. Consequently, the proportion of on-net calls to off-net calls becomes an important characteristic of interconnection fraud. In practice, interconnection fraud can be suspected if 90%-100% of all calls are on-net calls, which on most networks, is a rather unusual usage pattern for regular subscribers.

Unfortunately, soon after this usage characteristic started to be commonly used in FMSs, advanced fraudsters deduced this pattern was being utilized in detection, prompting other counter techniques. Nowadays, off-network calls on SIMs used in illegal international call termination frequently reach 35%, or even become equal to a regular usage pattern - depending on the country and operators' fraud management practice.

It is important to mention that the difference between the cost of international and local calls (off-net or on-net) is still large enough to generate significant profit; thus, the need to route some calls as local off-net calls is not a major impact to operators of illegal GSM gateways.

Look: no or low mobility

VoIP to GSM gateways are typically installed in data centres with broadband Internet connectivity; therefore, the typical characteristic of SIMs used in illegal call termination will be very low mobility or no mobility at all.

This characteristic usage in detection of GSM gateways depends on the size of GSM cells, but usually SIMs used in interconnection fraud will appear only in a few neighbour cells, or will disappear and reappear in a distant cell without any cell-to-cell handovers between - indicating that the GSM gateway was moved to another data centre.

This interconnection fraud characteristic is particularly troublesome for fraudsters to avoid as anti-detection techniques require a lot of effort and can be costly. The simplest method employed by fraudsters to avoid this fraud pattern is to "take SIMs for a ride".

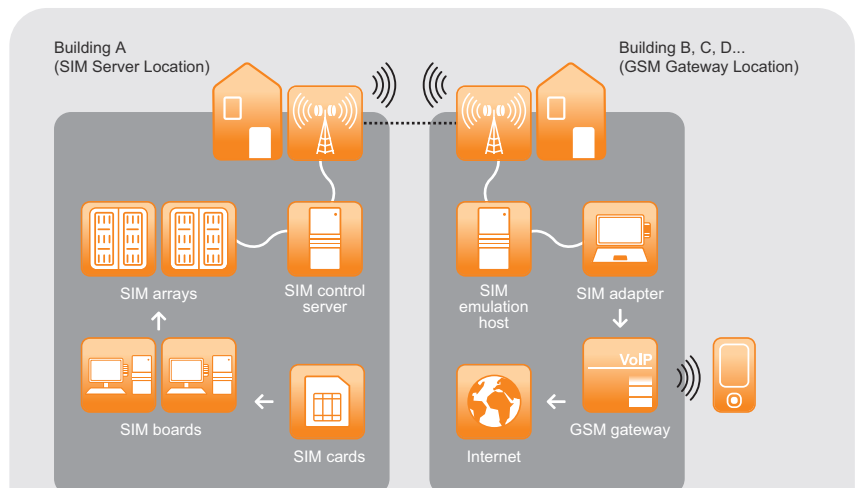
On a daily basis, some SIM card modules are taken out and placed in VoIP Gateway installed on a car, and driven around different GSM cells. This puts the SIM cards in multiple locations and will likely prevent basic detection of stationary SIMs by FMSs.

However, this technique will not be a major obstacle for the operator's fraud management team. If such an anti-detection technique is used, GSM operators can configure FMSs to perform analysis not based on reported locations of mobile SIM cards when activated, but on the locations of SIMs when voice calls were made. Although this method is very effective in detecting GSM gateways, it is unlikely to stop the most committed fraudsters, who constantly try to find new ways to avoid detection.

For instance, in one country, fraudsters started to place GSM gateways in mini-vans and operate from several locations during the day, using long range WiFi for connectivity. Although it is not a very advanced way of escaping detection, it is nevertheless an interesting method. The most significant advancement in avoiding detection of GSM gateways based on low or no mobility came with the use of the SIM Server technology.

SIM Server is a solution that allows

central storage, remote access and remote management on any number of SIM cards, which can be remotely used in GSM gateways or other GSM equipment through Local Area Network (LAN)-connected SIM emulation adapters. In practice, SIM cards used in illegal international call termination, SIM arrays and SIM control server can be located in one building, while GSM gateways, SIM emulation hosts and SIM adapters can be placed in different buildings, with all buildings connected using a wireless network.



Call Termination using SIM Server and GSM Gateway

This solution provides numerous benefits to fraudsters, such as:

- the ability to make SIM cards appear mobile by virtually switching SIM cards using the SIM Management Server to assign SIM stored in SIM Server to different GSM gateways
- intelligent SIM card usage, e.g., night calls handled by selected SIM cards
- easy management of SIM cards (SIMs easily accessible in one location on SIM arrays using hot swappable SIM slots)
- lack of evidence in police raids, as no SIM cards nor SIM management PCs are found on the location where GSM gateways are located (GSM positioning techniques are often used to identify the location of data centres used in interconnection fraud)

The development of such advanced technology definitely proves that call termination via GSM gateways is a highly profitable business.

Scrutinize: many subscribers on one cell and track suspicious activity in close proximity

Major GSM gateway operators commonly use hundreds of SIM cards installed in large VoIP gateways that can be simultaneously activated and used. The characteristic of constantly having a high number of SIM cards used on one cell could indicate the usage of a GSM gateway. However, the location and consistency in the load must also be considered. For instance, in case of bigger than usual usage, we can expect to have elevated usage from a high number of SIM cards at a given location. On the contrary, constantly having many network users in a data centre located outside the city is a very unusual pattern, indicating possible fraudulent use. Furthermore, SIM cards used in illegal call termination will often appear on the same cell or neighbour cells; thus, when positively detecting several cases of illegal call termination on one cell, other less suspicious SIMs on the same cell can automatically be classified as fraudulent based on fewer fraud characteristics.

In order to prevent such significant unusual increase of SIMs on one cell, fraudsters are trying to find large cells to place GSM gateways where it is easy to hide any number of SIM cards.

Due to the requirement of using several SIMs in one location, it is rather difficult to find large free cells that can handle big volumes of calls, making this a major obstacle for GSM gateway operators. Optionally, fraudsters can also disable SIM cards when not in use and activate it whenever there are no more active SIM cards that can handle the call.

In general, fraudulent usage in close proximity is very difficult for fraudsters to avoid, even more than the lack of mobility, which makes this characteristic particularly useful in finding GSM gateways when sophisticated anti-detection methods are used.

Ring, ring: high number of calls to distinct numbers

Interconnection bypass usage pattern is also characterized by a high number of voice calls to distinct phone numbers as VoIP gateways tend to service a large number of users calling different numbers. However, the application of this characteristic is error-prone, as GSM boxes legally used in PABXes of recruitment companies often are wrongly classified as used in interconnection fraud. The next characteristic could be useful in preventing such false positives.



Goodnight calls: unusual number of night calls to distinctive numbers



It is highly unusual for a regular office subscriber to frequently call distinctive numbers during late night hours. Thus, the presence of frequent late night calls to distinctive numbers is another unusual pattern that can indicate SIM Boxing. When paired with the characteristic of high number of distinct destinations of voice calls, it can yield very good detection results.

This characteristic is also difficult for fraudsters to avoid. International VoIP services cater to a large number of users, most calling different phone numbers. It is, therefore, highly unusual for a regular user to constantly call different mobile numbers, making this characteristic useful in detecting SIM Boxes. The common method to counter detection by FMSs is to implement automatic SIM mapping depending on time of the day, and route night calls through separate SIM cards. Such SIM routing features are commonly provided with SIM server solutions and are sometimes supported by more advanced GSM gateway products.

Your friendly operator speaking: voice-only service usage

The vast majority of mobile network users will frequently use both SMS and voice services; hence, not sending SMS is also a characteristic of SIM Boxing.

In theory, it is possible for fraudsters to send random SMSes, i.e., informing callers about the duration of the call, or optionally service international SMSes via GSM gateways or distribute spam via SMS. Yet, this has rarely been observed on real networks. Therefore, usage of only voice services by subscribers remains a very valuable tool in detecting interconnection fraud.

Gotcha!

avoiding false positives

Good FMSs will allow implementation of all the above rules to detect gateway interconnection fraud. In order to lower the risk of false positives, it is necessary to consider multiple fraud characteristics in analysis. If only one characteristic is used to detect interconnection fraud, such as subscriber-only using voice services, the analysis would certainly be invalid, as all subscribers who simply do not like to use SMS would be considered as potential GSM gateways.

However, by adding one more factor such as the ratio of incoming to outgoing calls, the analysis becomes more valuable as subscribers who do not use SMS, make many calls but never receive calls are very rare. It is important to note that even by using two-factor analysis, it is still possible to get false positives.

Consider this scenario: in one case where a FMS identified several subscribers with the following usage pattern:

- High number of outgoing calls with no incoming calls
- Unusual ratio of on-network to off-network calls
- No mobility
- High number of distinct destination of calls

Additional characteristics that could also increase the likelihood of mobile SIM cards being used in fraud are:

- Suspected number is prepaid
- Recently activated SIM cards
- False information provided by subscriber (i.e., invalid contact information given during registration)

In general, articulation of multiple detection techniques lowers the risk of false detection of SIM cards used in illegal call termination. Mobile operators should be aware, however, that fraudsters could change usage patterns to avoid detection with the use of sophisticated methods. This white paper covered some of the most common methods. However, to prevent usage by illegal GSM gateway operators, this document will not discuss other successful anti-detection techniques.

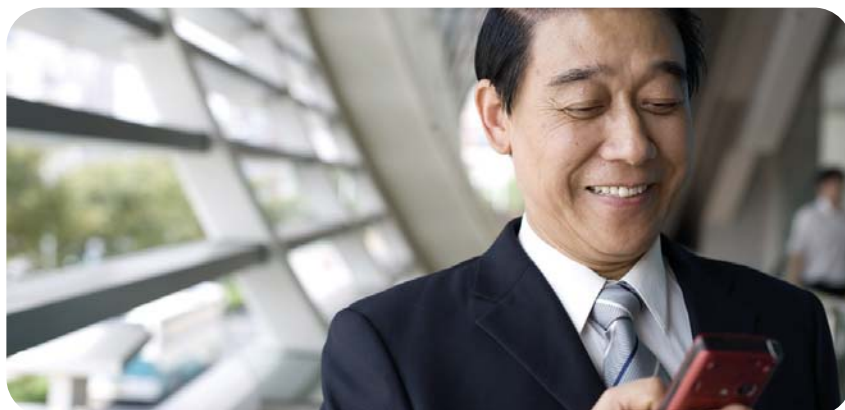


Attention: best practices

As previously explained, analysis of usage patterns in FMSs is highly effective in fighting illegal GSM gateways, but can sometimes result in falsely identifying legitimate mobile SIM cards as being used in interconnection fraud. It is also possible for fraudsters to employ sophisticated techniques to avoid detection through analysis of certain known fraud patterns. Thus, for the most effective and least-error prone method of detecting GSM gateways used in interconnection fraud, the best approach lies in a combination of utilizing FMSs and test calls.

The main advantage of adding test-calls to the process is error-free discovery of SIM cards used in illegal call termination. Operators can simply call on-net numbers by using VoIP service and based on the CDRs, identify on-net MSISDNs that handled the calls. If the VoIP calls were found to be unauthorized by the operator, it will unveil SIM cards that are used in illegal call termination. The advantage of error-free discovery is not limited to immediately terminating SIM cards used in fraudulent activities without affecting legitimate users; it can also be used to gather intelligence on detection-avoidance techniques used by illegal GSM gateway operators.

Operators can simply extract CDRs, analyse usage patterns based on the SIMs used in illegal call termination. This will reveal all the detection avoidance techniques used by fraudsters and allow operators to optimize FMSs to detect more sophisticated interconnection fraud.



Furthermore, based on test-call results, operators have another advantage - that is the ability to know the cell-id in which SIM cards are used in illegal call termination. As previously explained, fraudulent usage in close proximity is very difficult for fraudsters to avoid, which makes this characteristic particularly useful in detecting GSM gateways even if sophisticated anti-detection methods are used.

By knowing the location of SIM cards used in illegal call termination, GSM operators can simply search for other suspicious SIM cards on the same cell. If the GSM cell size is relatively small, operators can take the risk of blocking all SIMs on suspect cells without taking any significant risk of blocking legitimate subscribers.

This leads to the question, "If test-calls are so successful in detecting illegal use of GSM gateways, why don't we simply use it instead of FMSs?"

Unfortunately, test-calls without FMS is not an effective solution as GSM operators are not able to run test calls from every single VoIP service in the world, resulting in potentially missing some VoIP GSM gateway operators.

Furthermore, in order to identify every single SIM card used in a GSM gateway, operators would have to run hundreds of test-calls - one for each SIM - making it a costly operation. Another factor to consider is that test-call activities financially benefit operators of illegal GSM gateways.

There are simple and practical methods of fraud analyzing. For example, fraud management teams could use a scoring methodology when deciding to block particular SIMs, or even block International Mobile Equipment Identity (IMEI). However, it is important to be very careful with blocking IMEIs as this has been effectively targeted by fraudsters and could affect regular users.

A sample scoring methodology used to identify SIM cards used on illegal GSM gateways follows:

Usage characteristic scoring

| Usage characteristic | Uniqueness | Difficulty to avoid detection | Fraud Score |
|---|------------|-------------------------------|-------------|
| No mobility or low mobility | High | Very high | +7 |
| Use of only voice service | Medium | Very high | +6 |
| Ratio of incoming to outgoing calls | High | Medium | +5 |
| High number of calls to distinct numbers | Medium | High | +5 |
| Very high usage of voice service | Low | Medium | +3 |
| Significant number of subscribers on one cell | Low | Medium | +3 |
| Unusual number of night calls | Medium | Low | +3 |
| Ratio of on-network to off-network calls | Low | Low | +2 |

Scoring points: Low = 1, Medium = 2, High = 3, Very High = 4

Note: If advanced GSM gateway fraud is not observed on the network, scoring can be based on the uniqueness without considering the 'difficulty to avoid detection' factor.

Additional scoring for suspected subscribers

| Additional scoring | Fraud Score |
|--------------------------------------|-------------|
| MSISDN detected using test-calls | Maximum |
| SIM Boxing detected on the same cell | +9 |
| Incoming calls diverted to mail-box | +4 |
| Suspected number is prepaid | +1 |
| Number recently activated | +1 |

Using this very basic scoring methodology, any subscriber with a usage characteristic matching a fraud score above 22 can be considered as GSM SIM Boxing suspects. If combined with additional scoring, the final number goes above 32, consider blocking the suspect subscriber. A lower score could require further review before deciding on blockage. Blocking of IMEIs on networks should be considered for subscribers with the MAXIMUM scores, or if particular IMEIs were detected multiple times where illegal SIM Boxing was detected. However, operators should be very careful with blocking IMEI of devices suspected to be used in illegal GSM gateway operations.

Please note that this is just a sample scoring and in real practice, operators will likely need to design comprehensive methodologies and define the process of dealing with GSM gateways.

Regulatory issues with GSM gateways



It is also important to consider legal issues when dealing with GSM gateways. In several countries, operators of GSM gateways filed in lawsuits against telco operators following termination of SIM cards used in GSM gateways.

Legal regulations concerning bypass vary from country to country and, unfortunately, rarely encourage mobile operators to carry out enforcement procedures. Hence, operators usually follow the practice of introducing restrictions into contracts forbidding routing calls from/towards other networks and the reselling of calls.

GSM Europe's (European Interest Group of the GSM Association) recommendation for the European Commission and industry bodies is to encourage Member States to prohibit the use of GSM gateways for the conveyance of third party traffic by carriers.

The option being implemented by most operators is to ensure that commercial terms and conditions exclude the use of GSM gateways for routing third party traffic. Operators should then be free to detect, identify and terminate such subscriptions which are in breach of contract or in breach of any national legislation preventing the use of such devices.

GSM Europe further recommends that the use of GSM gateways by private and corporate users should remain possible but that mobile operators should be free to define reasonable commercial terms and conditions to protect the integrity and quality of their networks.

[Source: GSM Europe paper on "Use of Gateways for Mobile Communications", 2003]

Conclusion

To conclude, a combination of FMSs and test-calls is the optimal tool in fighting illegal call termination using GSM gateways (SIM Boxes). Fraud management teams must also stay abreast of current fraud types and methods, as well as acquiring the knowledge of implementing appropriate detection techniques in various scenarios.



Nokia Siemens Networks Corporation
P.O.Box 1
FI-02022 Nokia Siemens Networks
Finland

Visiting address:
Karaportti 3, ESPOO, Finland

Switchboard +358 71 400 4000 (Finland)
Switchboard +49 89 5159 01 (Germany)

Author
Nokia Siemens Networks is a leading global enabler of communications services. The company provides a complete, well-balanced product portfolio of mobile and fixed network infrastructure solutions and addresses the growing demand for services with 20,000 service professionals worldwide. Nokia Siemens Networks is one of the largest telecommunications infrastructure companies with operations in 150 countries. The company is headquartered in Espoo, Finland.

The contents of this document are copyright © 2008 Nokia Siemens Networks. All rights reserved.

A license is hereby granted to download and print a copy of this document for personal use only. No other license to any other intellectual property rights is granted herein. Unless expressly permitted herein, reproduction, transfer, distribution or storage of part or all of the contents in any form without the prior written permission of Nokia Siemens Networks is prohibited.

The content of this document is provided "AS IS", without warranties of any kind with regards its accuracy or reliability, and specifically excluding all implied warranties, for example of merchantability, fitness for purpose, title and non-infringement. In no event shall Nokia Siemens Networks be liable for any special, indirect or consequential damages, or any damages whatsoever resulting from loss of use, data or profits, arising out of or in connection with the use of the document. Nokia Siemens Networks reserves the right to revise the document or withdraw it at any time without prior notice.

Nokia Siemens Networks and the Wave-logo are registered trademarks of Nokia Siemens Networks. Nokia Siemens Networks product names are either trademarks or registered trademarks of Nokia Siemens Networks. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.