IoT, International Roaming and DDoS

A Risk and a Methodology

#RECONNECT

Why IoT and International Roaming?

01

Have you traveled to a foreign country? IoT Devices also: Connected vehicles, Fleet management, cargo trackers, telecare…

02

Companies are interested in centralize all their SIM logistcal process in a single SIM provider

What happens when hundreds of thousands of devices appear in your network?

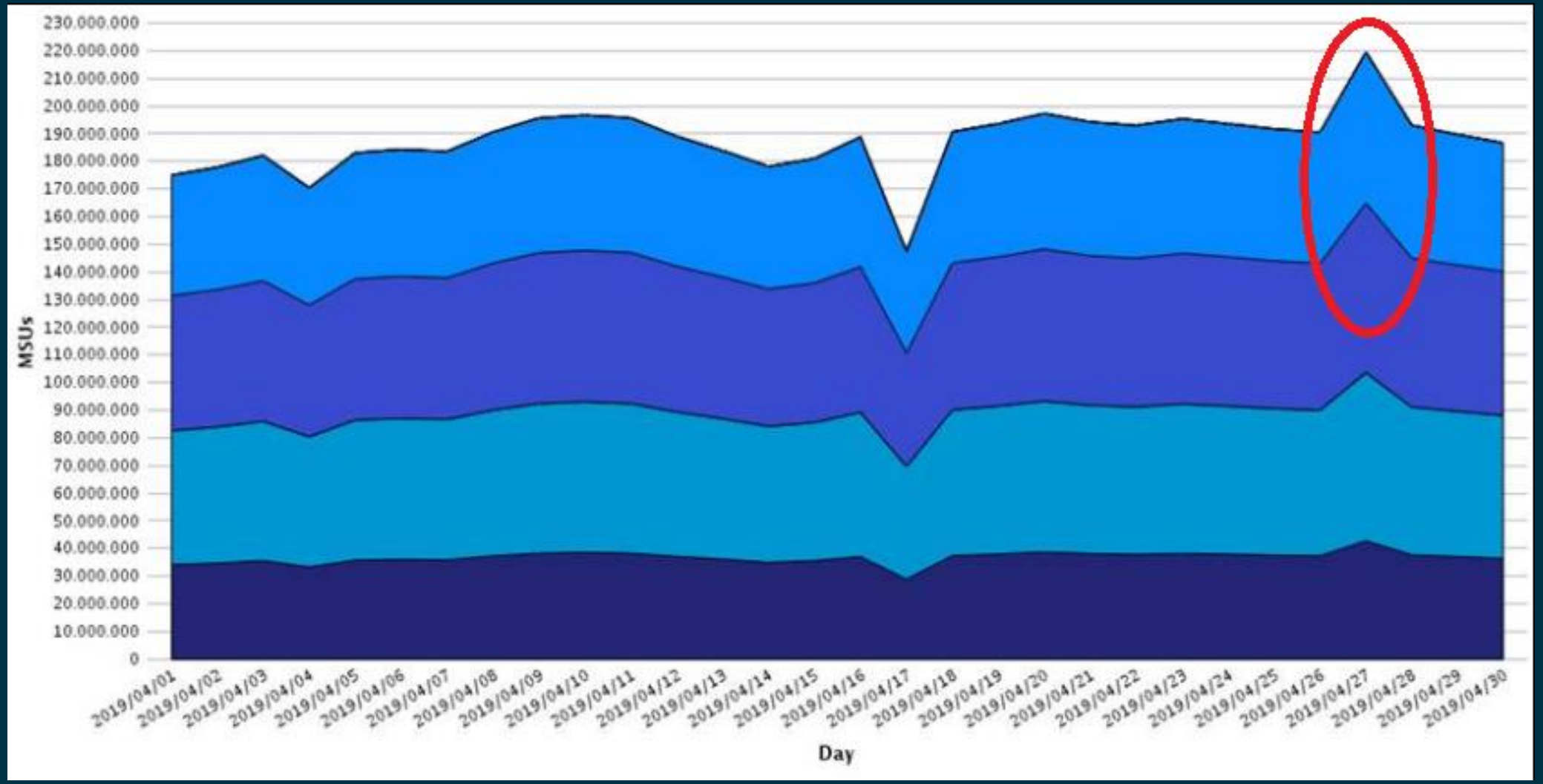
Simultaneous reset

- Because some necessity of the service, a low performance detection or other situations all the SIMs can reset and launch a registering process
- This can be also performed by malicious attacks

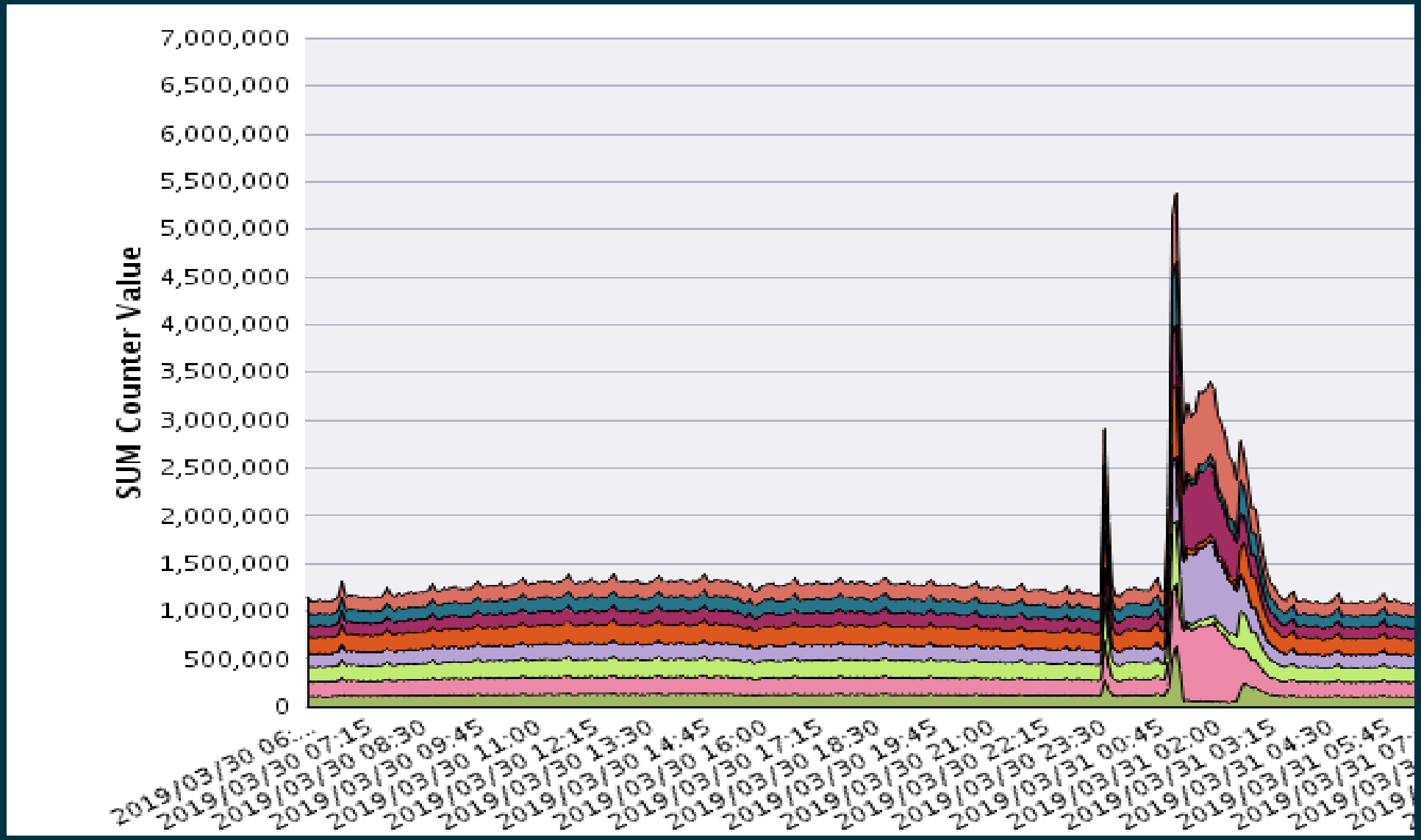
Simultaneous reattaching

- If a hundreds of devices try to register in the network at the same time a collapse can happen. If a collapse in the network happens the device can continue trying to register more and more…
- In 3GPP signaling this is known as Signallig Storm.

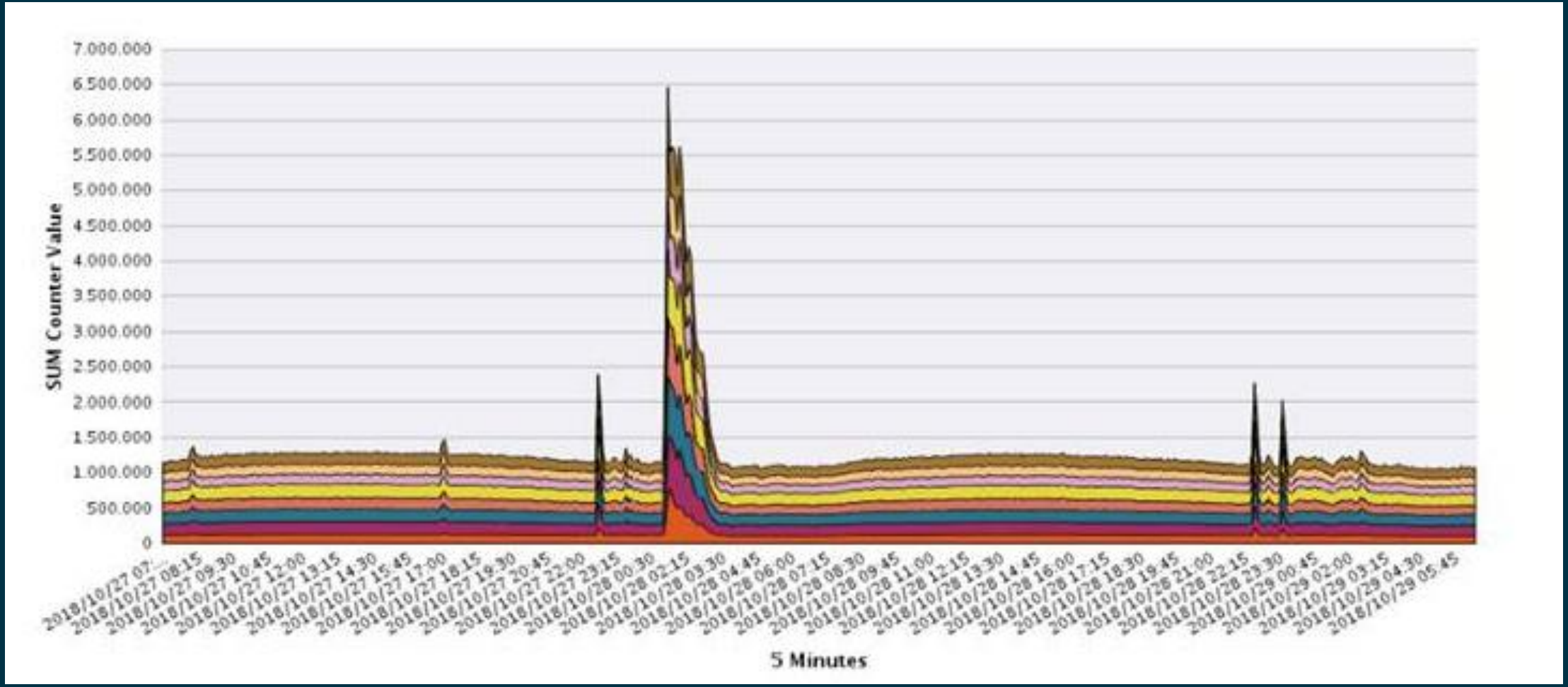
Traffic increament because a Cancel Location Peak



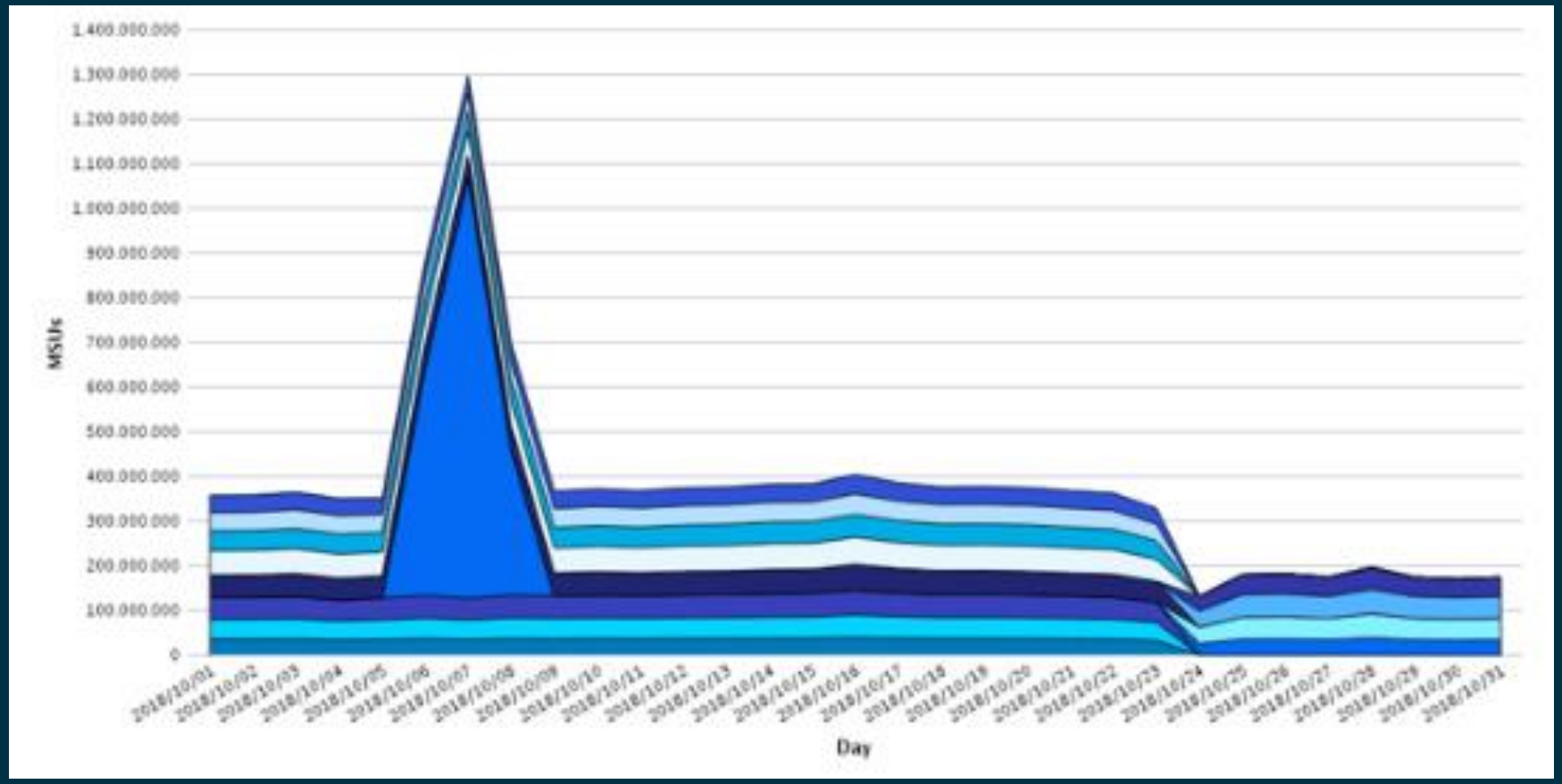
Traffic increament because a Cancel Location Peak



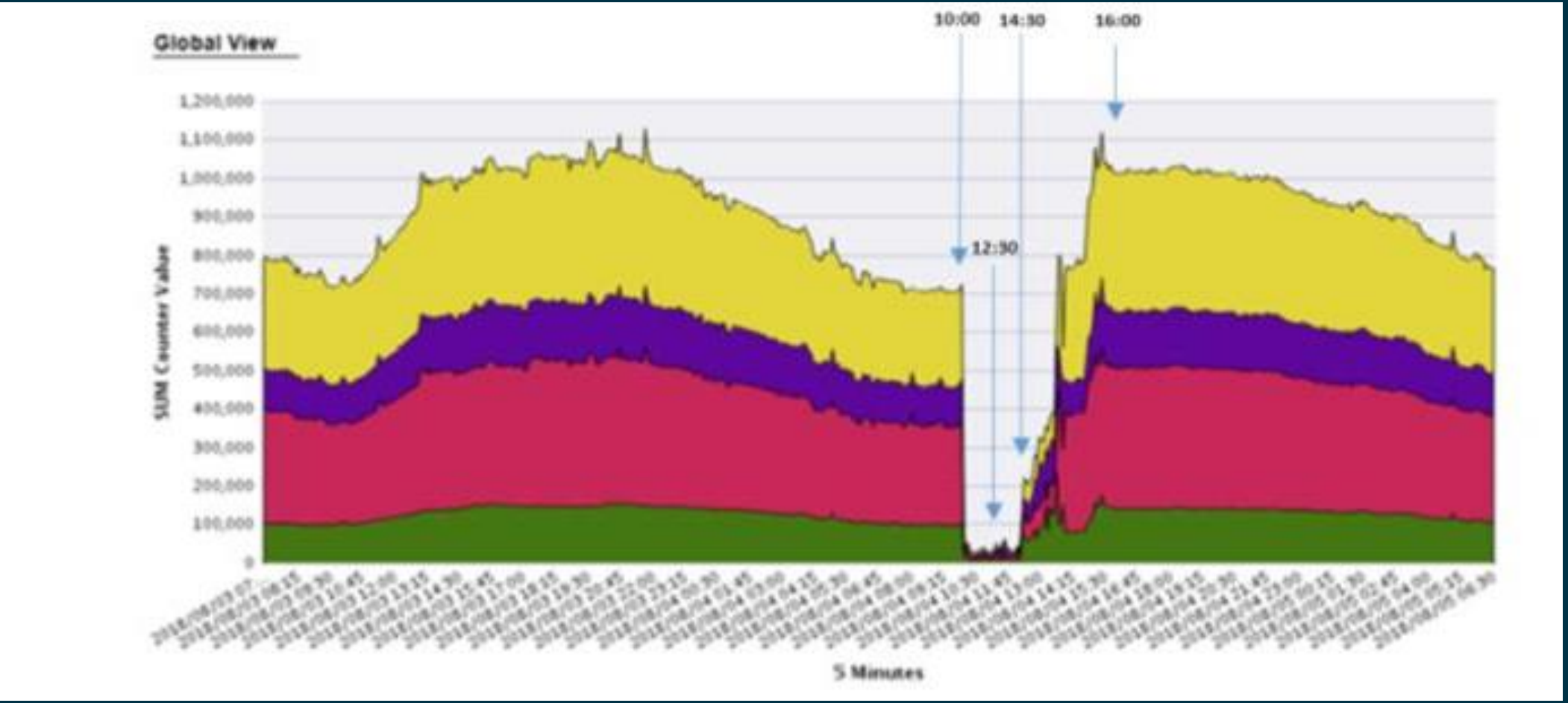
Traffic increament because a Cancel Location Peak



Traffic increament because a Cancel Location Peak



Traffic of users lost because IoT DDoS



Counter Measures

Traffic pattern detection

IoT devices have classic elements and patterns to be detected and clasified. A traffic peak launches a comprobation and check the current traffic pattern with the learnt ones. First step is discard human traffic.

IMSI

Some operators have specific IMSI ranges for their IoT SIMs. This is reported through IR21 documents.

UL

Update Location is the signalling command that usually generates the signalling storm. A lot of this kind of commans or launching in a regular basis can mean IoT devices

IMEI

IMEI in GTP network can also give us detail if problem is at IP level. You can check the frames agains an IMEI database.

GTP traffic

GTP traffic can have patterns that provide information about an automatic behaviour

Counter Measures: how to react

Isolated networks

This is a preventive architecture: IoT traffic should be isolated from the users one, in different networks.

In this way IoT devices attack don’t affect to human communications

Different STP/DRA, different PGW and EPC

Resize through Cloud

Modern APIs of the virtual Infrastructure pemite resize he affected elements if a capacity bottleneck is being created by a signalling storm

More CPU, Memory or bandwith can be assigned in the affected frame.

Block problematic devices

The devices can be blocked once you have located the IMSI. Not only from core elements like HSS, but also in intermediate not critical platforms linked to the Steering through traffic redirection at DRA level.

Counter Measures

Once we have identified an attack: what?

IMSI

Some operators have specific IMSI ranges for their IoT SIMs. This is reported through IR21 documents.

UL

Update Location is the signalling command that usually generates the signalling storm. A lot of this kind of commans or launching in a regular basis can mean IoT devices

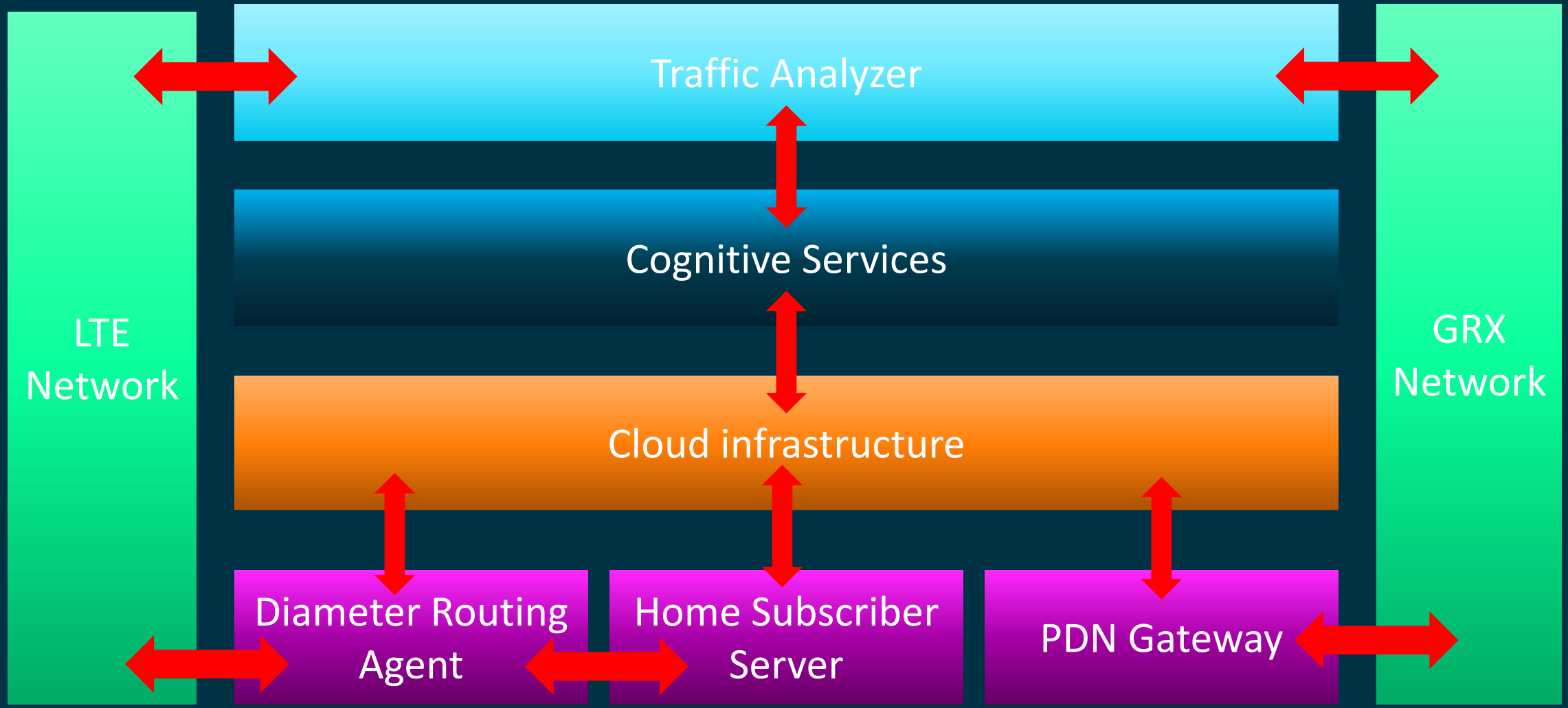
IMEI

IMEI in GTP network can also give us detail if problem is at IP level. You can check the frames agains an IMEI database.

GTP traffic

GTP traffic can have patterns that provide information about an automatic behaviour

Architecture



#RELEVANCE

#REVENUES

#RESPONSIBILITY

#RETURNS

M#TIVATION


Telefónica