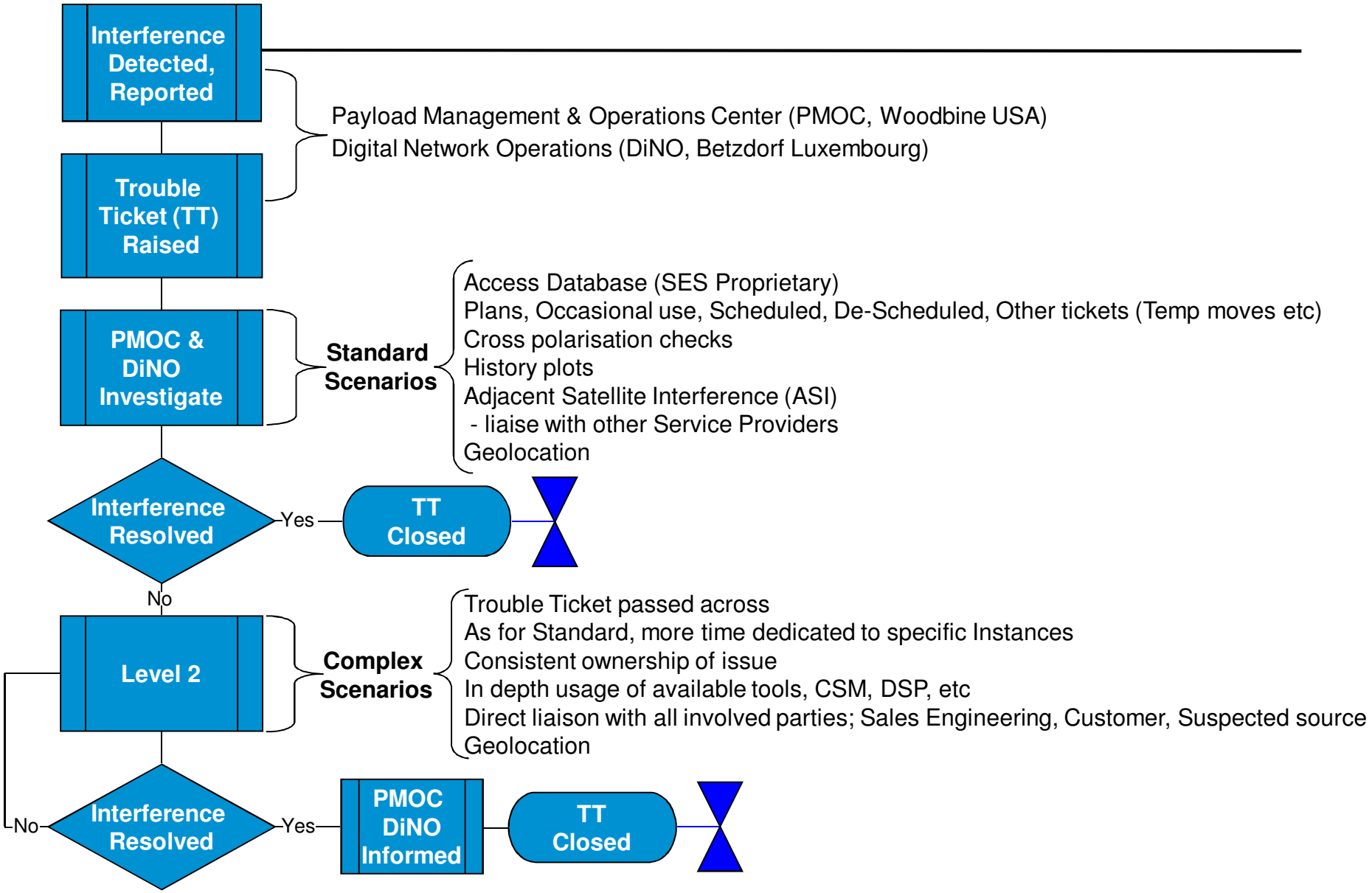
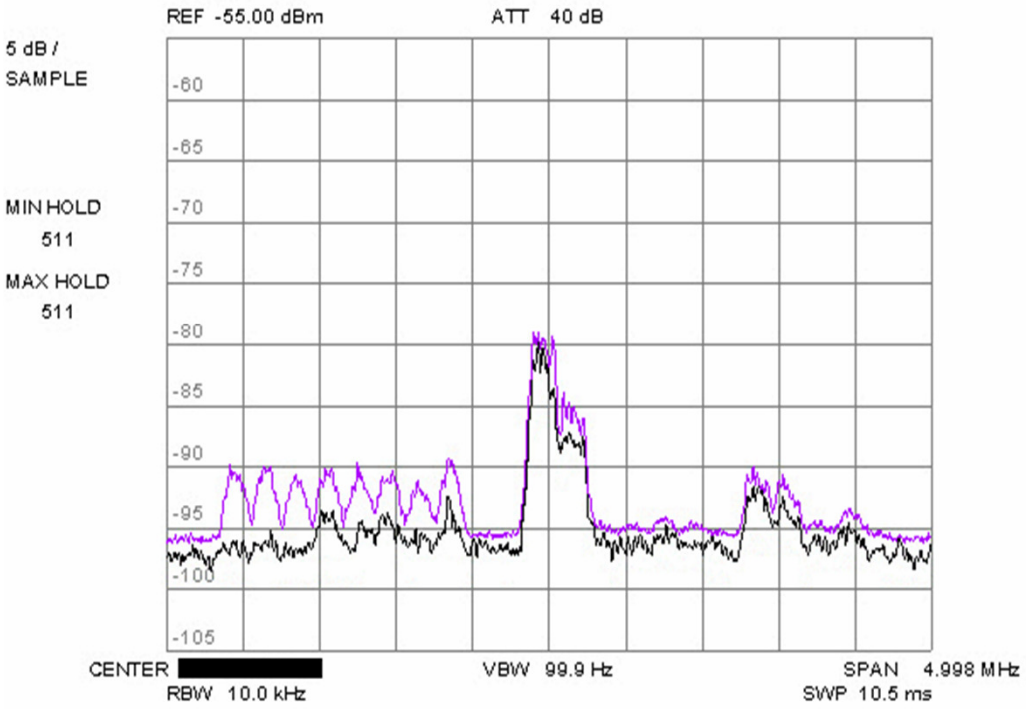

SES
your satellite company
Satellite IRG Conference 2011
Identifying Rebroadcast (GSM)
October 2011 - Compiled By Andy Williamson (PMOCL2 Manassas)
Presented By Russ Hogan (Betzdorf)

It’s A Team Effort

SES Interference Management



Initial Problem As Reported



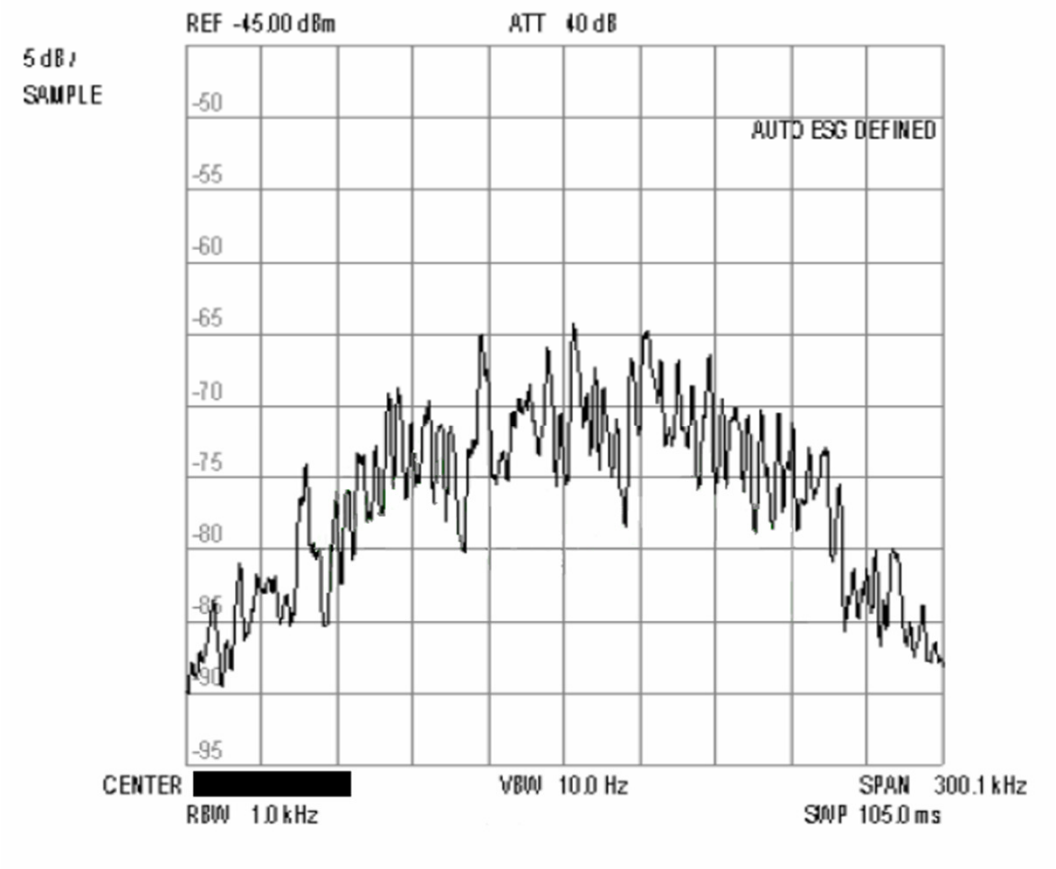
▲ Everything in the picture opposite is interference and should not be there!

▲ Initial problem presented as multiple TDMA-like interferences with 200kHz spacing.

▲ Interferences ranged from 1-2dB right up to 15dB C/N.

▲ Later examples have been seen with >25dB C/N!

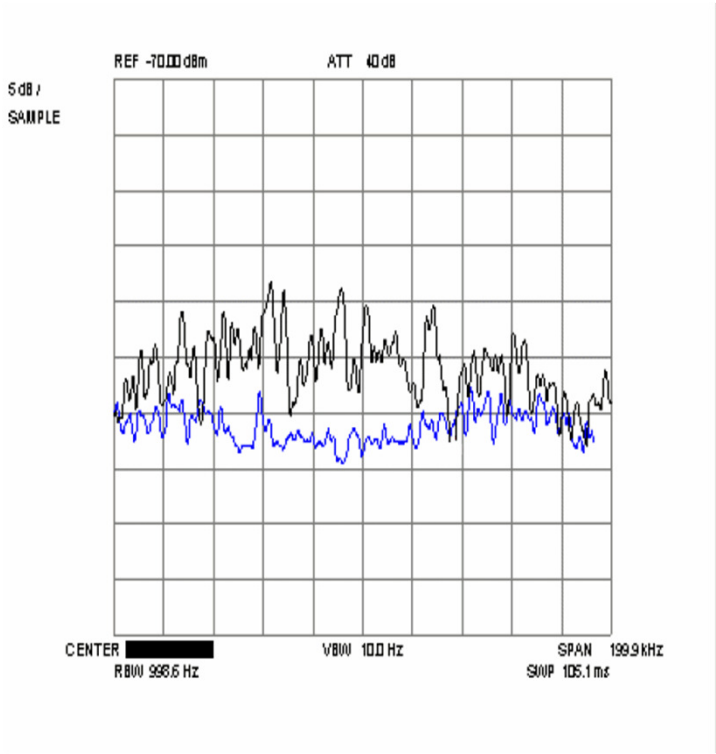
Close-Up Spectral Plot

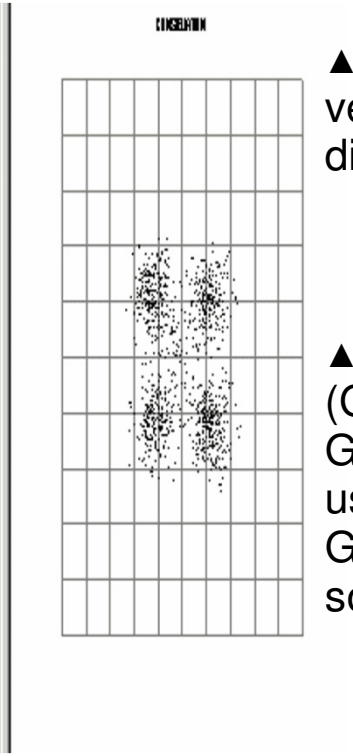


▲ Close-up spectral plot shows a 'rounded' shape unlike most 'flat-top' digital carriers transmitted over satellite.

▲ Initially, it was thought this could be a digital carrier with the scrambler/energy dispersal disabled.

Modulation Analysis





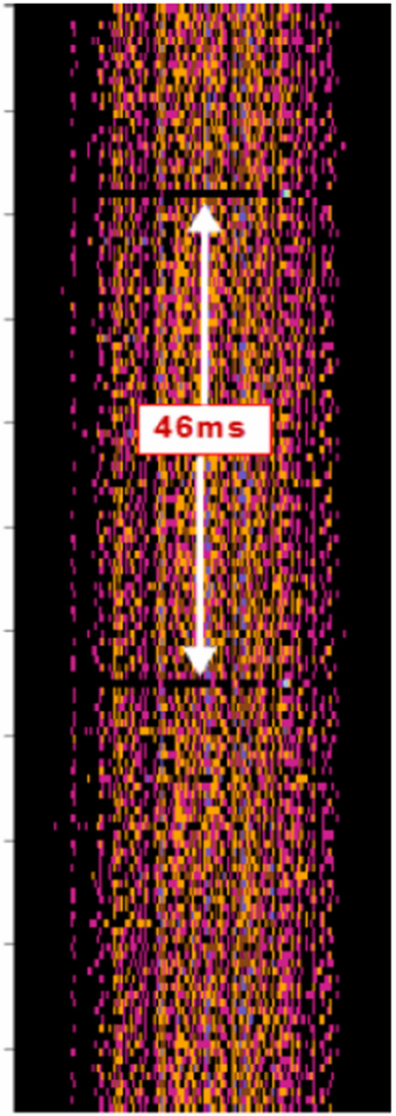
▲ Modulation analysis showed a very noisy and broken constellation display.

- ▲ Not unlike that seen when viewing typical TDMA signals.

▲ The combination of a rounded (Gaussian) spectral shape due to GMSK modulation and the apparent use of TDMA led us to start looking at GSM cell towers as being a possible source.

- ▲ GSM signals use GMSK modulation, some DSP units will misidentify this as O-QPSK with a symbol rate of about 134ks/s (neither are correct as it's really GMSK with a symbol rate of 270.833ks/s).

Spectrogram Analysis



▲ The proof that we were indeed looking at a GSM rebroadcast was the spectrogram analysis which clearly showed the timing correction bursts.

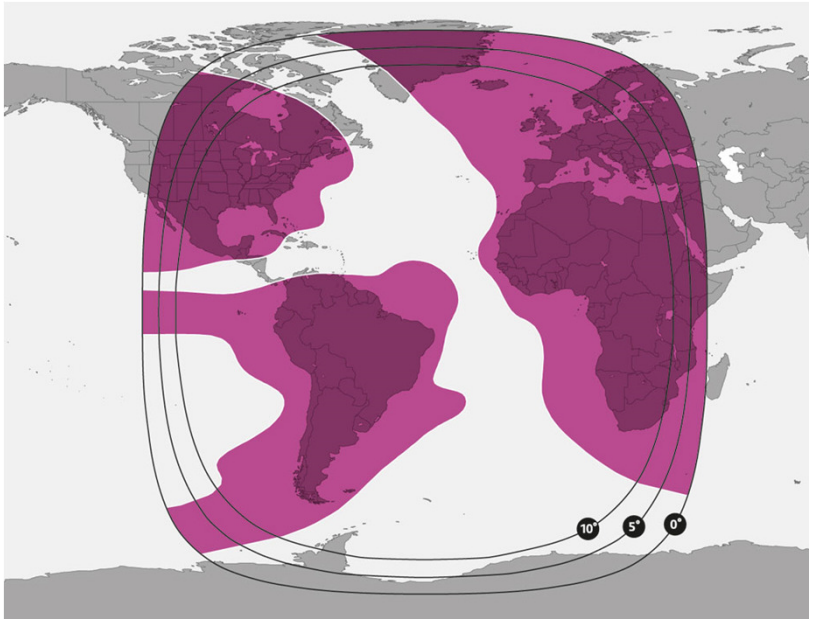
▲ In GSM, a timing burst is sent after every tenth frame.

▲ As each GSM frame is 4.615ms, the timing burst is seen every 46.15ms.

NSS-10
322.5°E (37.5°W)

SES

Delivering high-powered capacity to Africa, Europe and the Americas



NSS-10 C-band Coverage

Launch Date:	Feb 2005
Payload (36 MHz equiv):	C-band: 49 transponders
Coverage	Africa, Europe, South America, North America
Services:	Supports services for telecom and VSAT operators

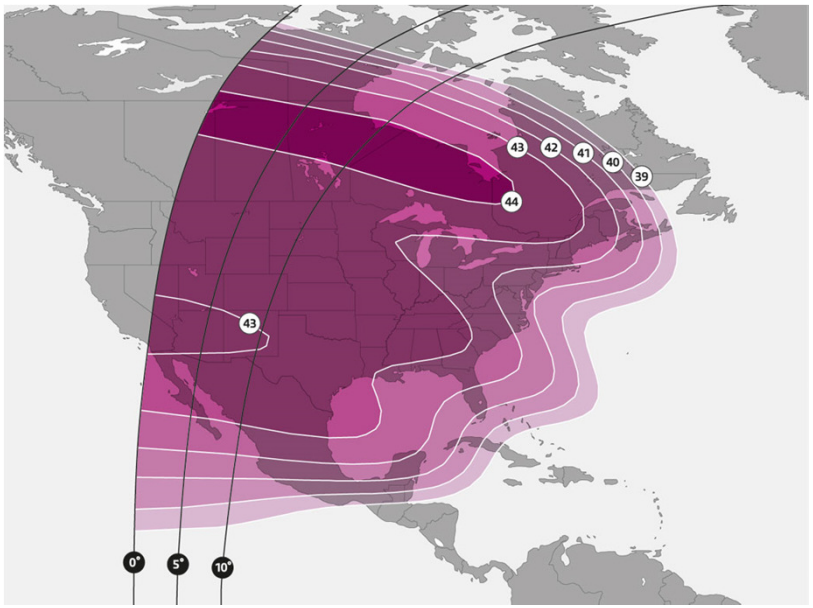
- Individual transponder switching capacity and unique simultaneous downlink functionality; high throughput ideal for supporting GSM backhaul services
- Serves the critical and high demand in Africa while offering connectivity for hub services based in Europe and North America
- Cross connectivity between all beams
- Linear polarisation

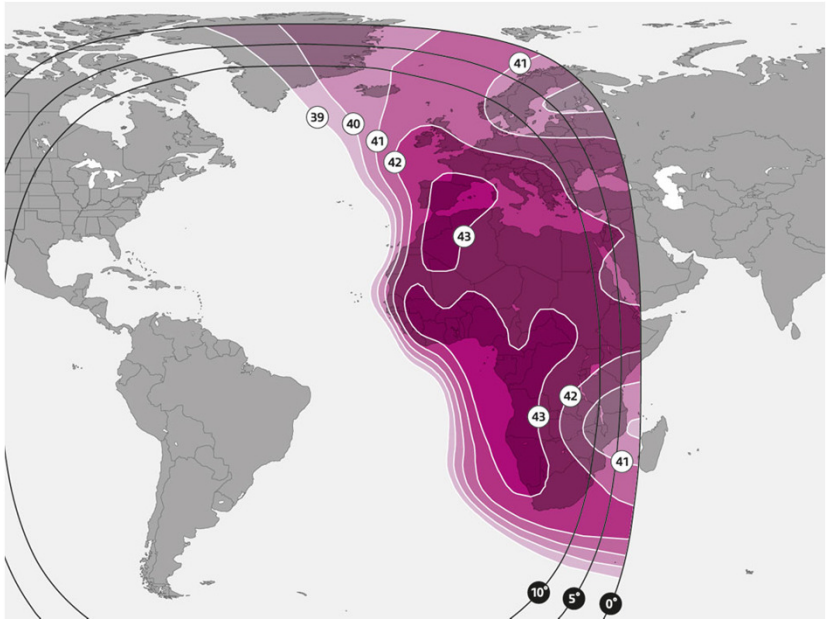
NSS-10

322.5°E (37.5°W)

SES

Delivering high-powered capacity to Africa, Europe and the Americas

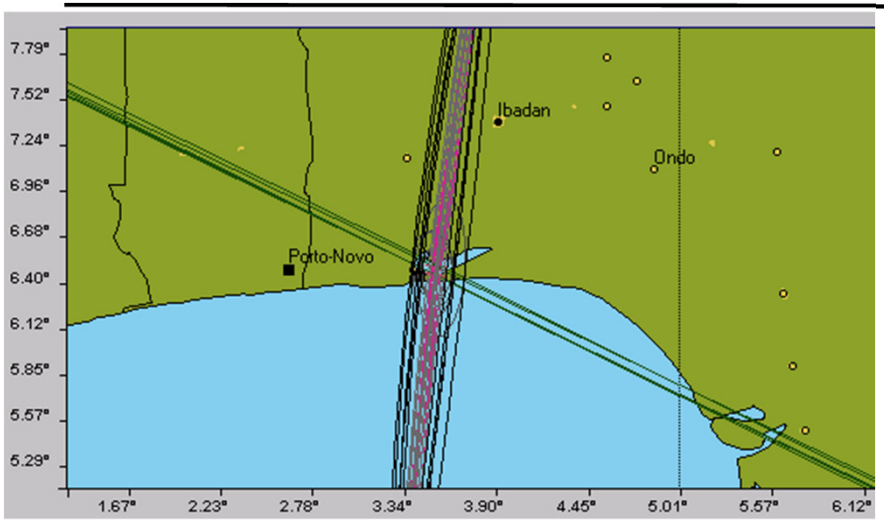


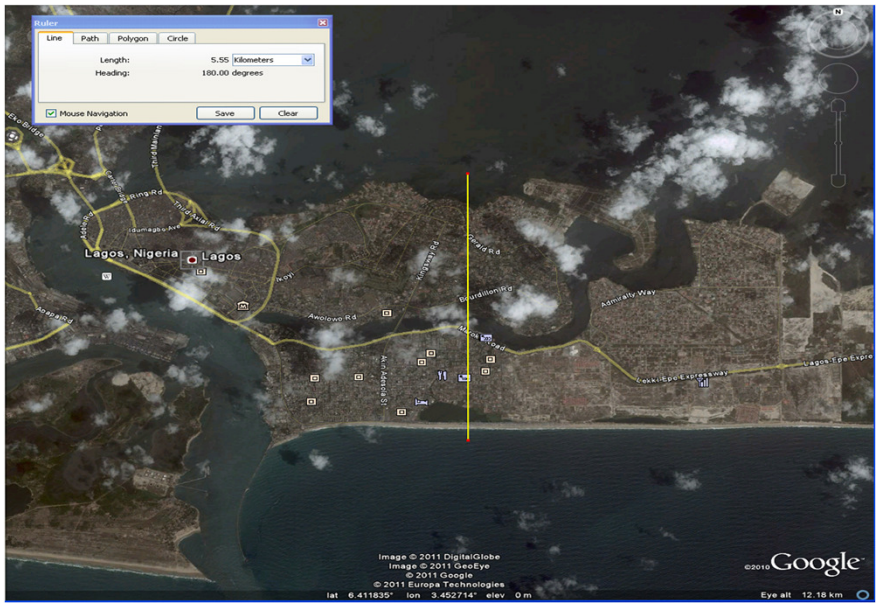


NSS-10 North America C-band beam

- Serves the critical and high demand in Africa while offering connectivity for hub services based in Europe and North America
- Cross connectivity between all beams
- Linear polarisation

Geolocation





▲ Geolocation gave us the an initial area of interest.

▲ However, within a this busy City it is difficult to pinpoint specific Uplinks.

▲ Further Geolocation narrowed it down to the Victoria Island area near Lagos.

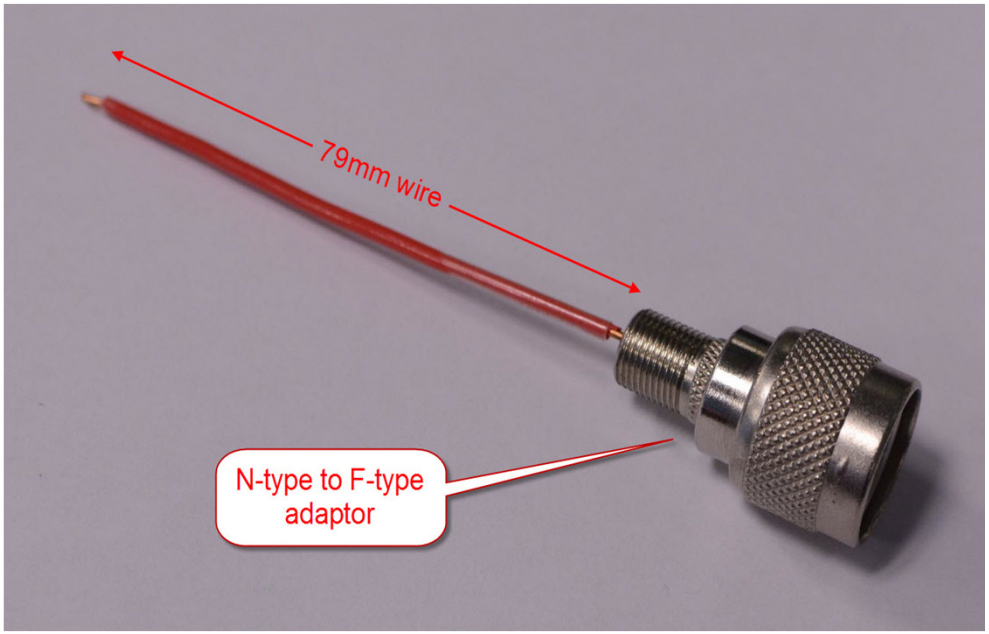
Initial Identification

▲ To try to identify the source of the rebroadcast, we used an LNB to translate the GSM signals back into the 935-960MHz frequency range.

▲ We then made a temporary antenna by pushing 79mm of wire (1/4λ at 947.5MHz) into an N-type to F-type adaptor which we connected to the LNB output in order to re-radiate the signals.

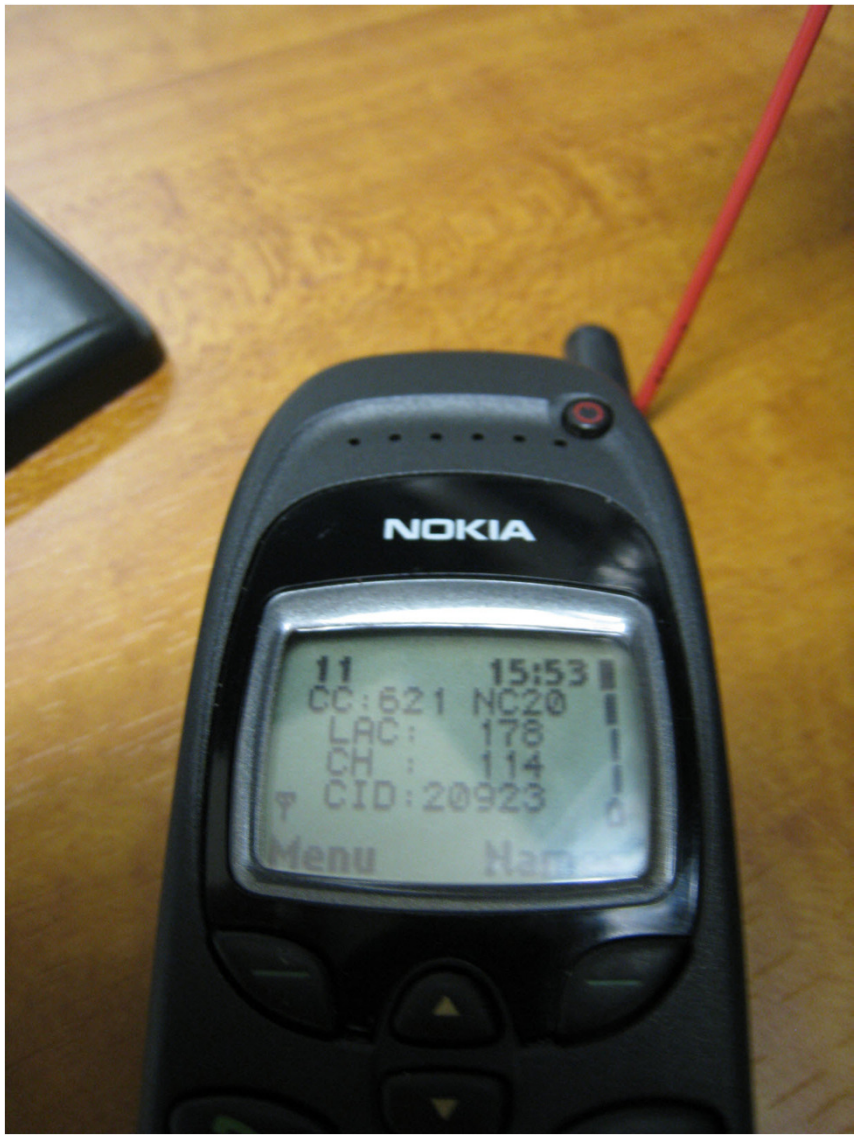
▲ We held this antenna near an old EU spec Nokia cell phone to obtain cell tower information.

Temporary Antenna



▲ Close-up of the temporary antenna showing the 79mm of wire pushed into the N-type to F-type adaptor.

Netmonitor Display

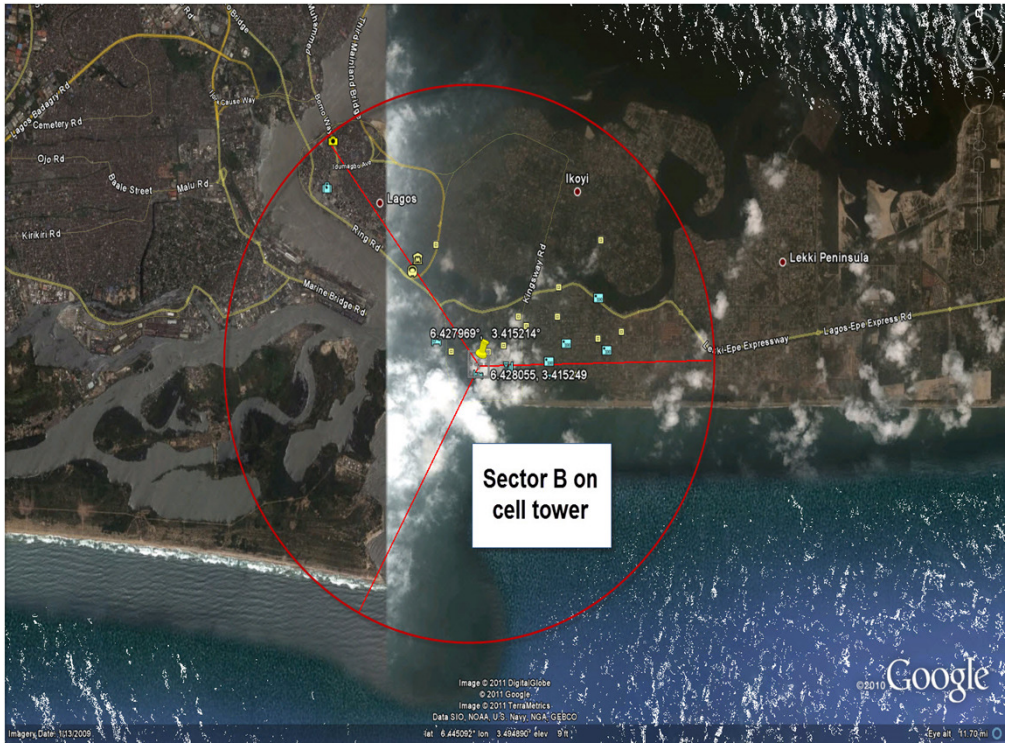


▲ We used the Netmonitor screen in an unlocked Nokia 6150 to get information about the cell tower that was getting rebroadcast onto the satellite.

▲ In this example, the information obtained is:

- **CC : 621** = Country Code Nigeria
- **NC20** = Cell Provider Network Code
- **LAC : 17** = Local Area Code for Victoria Island, near Lagos
- **CH : 114** = GSM Channel 114; translates to 957.8MHz
- **CID : 20923** = Antenna 2 (or B) on cell provider tower 0923

Identifying Search Area



▲ We contacted the cell provider and supplied them with the cell information obtained from the Netmonitor screen.

▲ They were extremely helpful and to help us narrow down our search area.

▲ They provided the exact GPS coordinates of the cell tower and the azimuthal direction that the ‘B’ antenna on the tower services

Identifying The Uplink

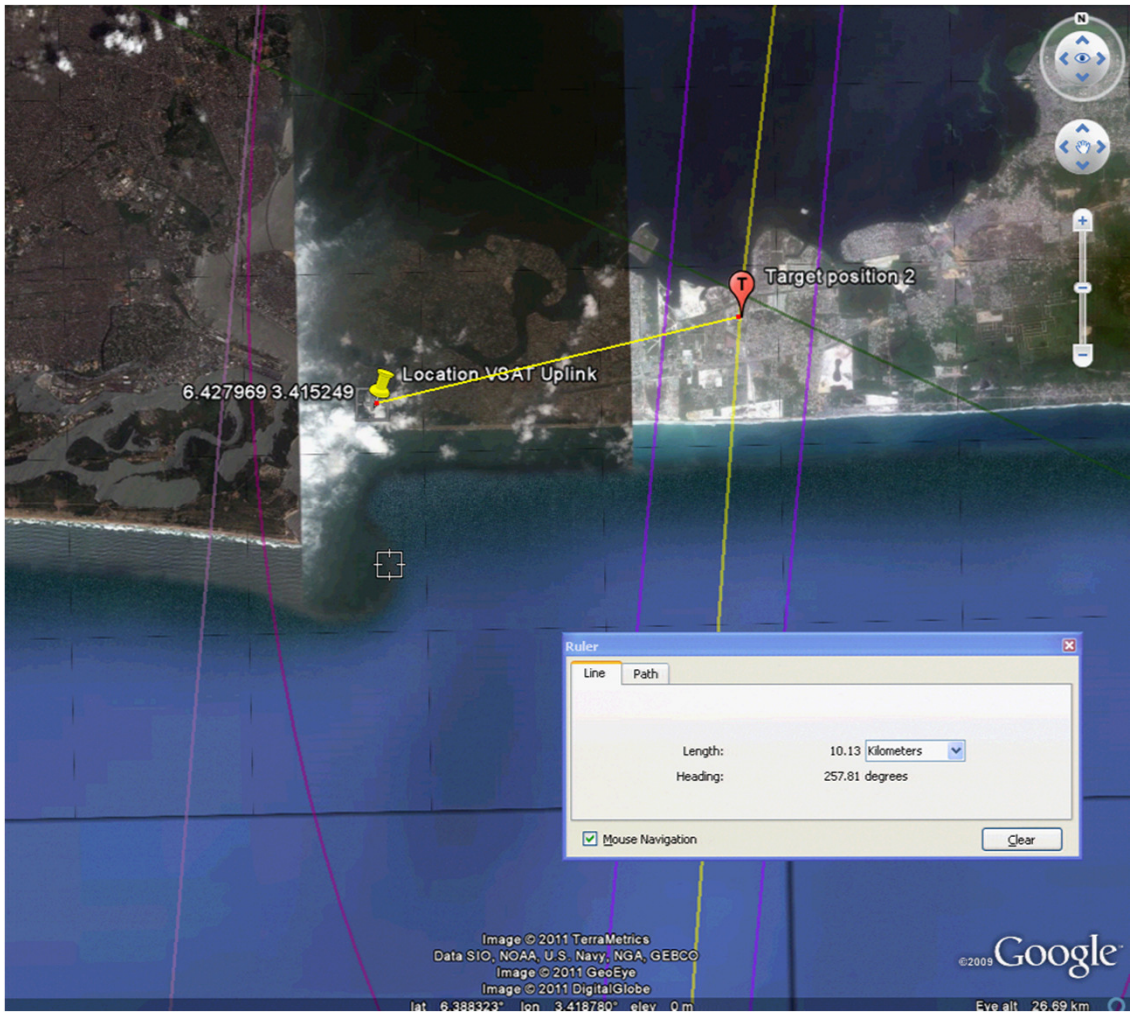
▲ After contacting and muting a number of nearby uplinks, we found the source of the GSM rebroadcast.

▲ It was located about 380m from the cell tower.

▲ It should be noted that the cell tower provider was at no fault whatsoever as the problem was found to be an un-terminated L-band combiner port at the VSAT uplink.

Identifying The Uplink

- Geolocation was 10km away from VSAT uplink.



Expanding The Concept

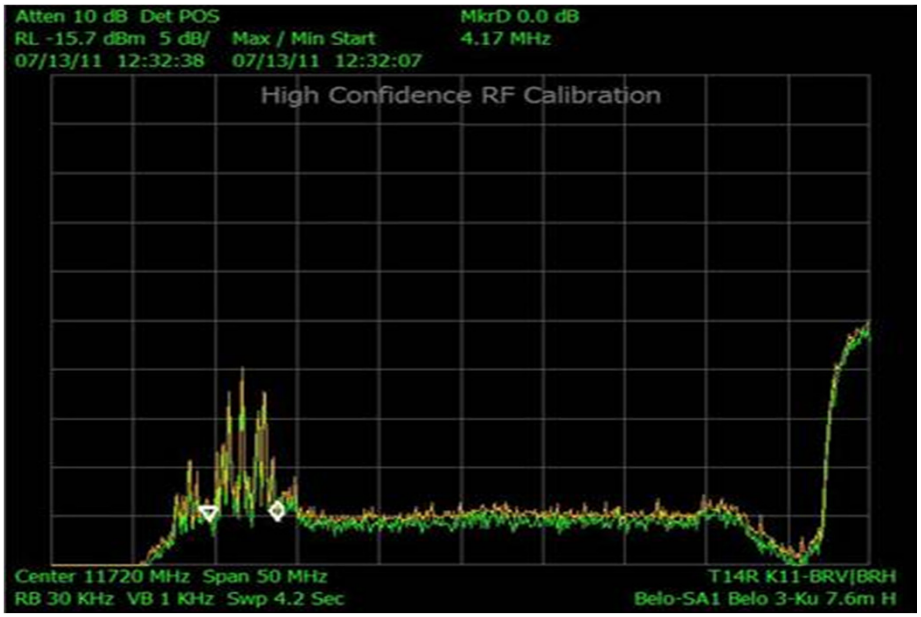
▲ Now that the concept of using an unlocked cell phone to identify a rebroadcast cell tower was proven, we expanded the concept to make it more reliable and less likely to give erroneous results from local cell towers.

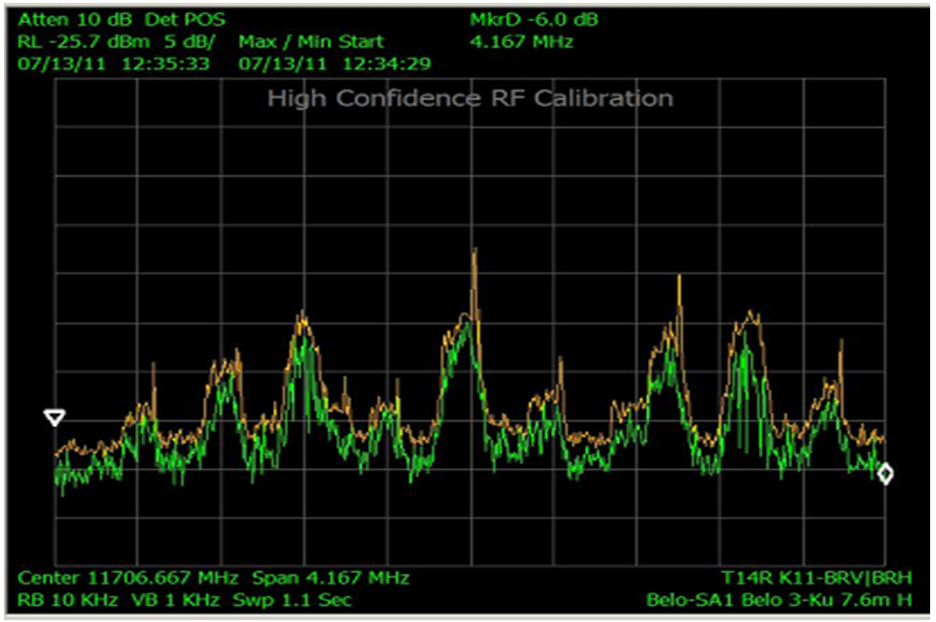
▲ The Nokia 6150 has an external antenna connector that was originally designed to be used with a car kit. When an external antenna is plugged in, it disconnects the built-in antenna. We used this to our advantage to ensure the cell phone only sees signals from the LNB and not anything local.

▲ We modified the phone to have a BNC connector permanently installed in the external antenna jack. Now the LNB output can be connected directly to the phone.

▲ Other Nokia phones that can be used for this are the 2100, 3330, 5110, 6210, 7110, 8210 and 8250 models. However, they need to be non-North America spec phones or they won't cover the correct frequency ranges needed (unless they are tri or quad band phones).

Theory At Work - Telesat





▲ GSM signals are spaced 200kHz apart. All the interferences shown are 400kHz apart so it's possible there are two sectored antennas on the cell using alternate frequencies, or the channels are coordinated between adjacent cells to avoid mutual interference to each other.

▲ The highest uplink frequency seen as interference is at 14010MHz. This works out perfectly for it to be GSM900 if the offending uplink is using a standard 13050MHz LO on their BUC which means the 935-960MHz of the GSM900 system will be seen from 13985-14010MHz. Probably unable to see the lower end as that will fall into the transponder roll-off.

SES
your satellite company

Thank you!

Teamwork Makes It Easier