Rogue BTS (IMSI Catcher) Detection System

1. TSCM Deployment

IMSI Catchers, Handheld Directions Finders and related products are typically used for tactical geo-location and intelligence gathering missions, however they are also used for TSCM and secure facility applications.

Core capabilities that make these products suitable for this are:

- Ability to detect and (Locate) Rogue BTS (IMSI Catchers) operating in the vicinity
- Service denial of unauthorised phones in secure facilities
- Geo-location of unauthorised phones
- Registering of IMSI/IMEIs entering a secure facility

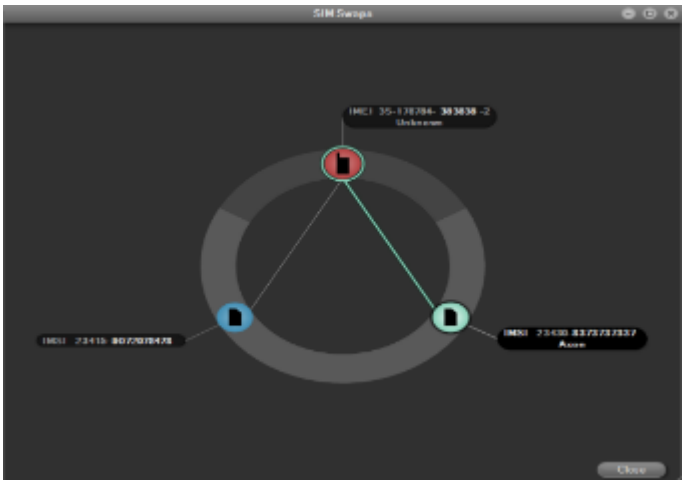
These capabilities are all inclusive in one software defined hardware solution the Pegasus MOTE, which can be set-up on infrastructure or in mobile assets such as vehicles or backpacks (e.g. for VIP Convoys).

Some of the core features that enable this are:

1.1. IMSI/IMEI Registration

The ability to capture handsets as they enter the target area (8W on Pegasus MOTE) building up a database of information that can be managed accordingly vs a whitelist/blacklist. The correlation is advanced ensuring that the system can track multiple handsets/sim cards being used in the event of 'Sim-swaps'.

These handsets can then be geo-located using direction finders or GPS extraction from the handset itself.

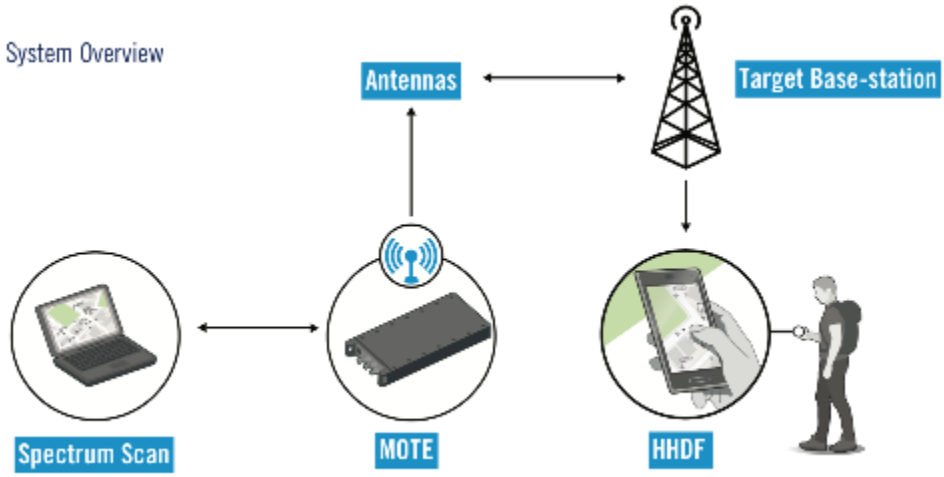


1.2. Rogue BTS Detection

Each 'channel' deployed can act as a Rogue BTS detector, by scanning the surrounding environment and assigning suspicion levels to identified base stations dependant on a variety of factors/cell parameters using our vast experience in cell emulation.

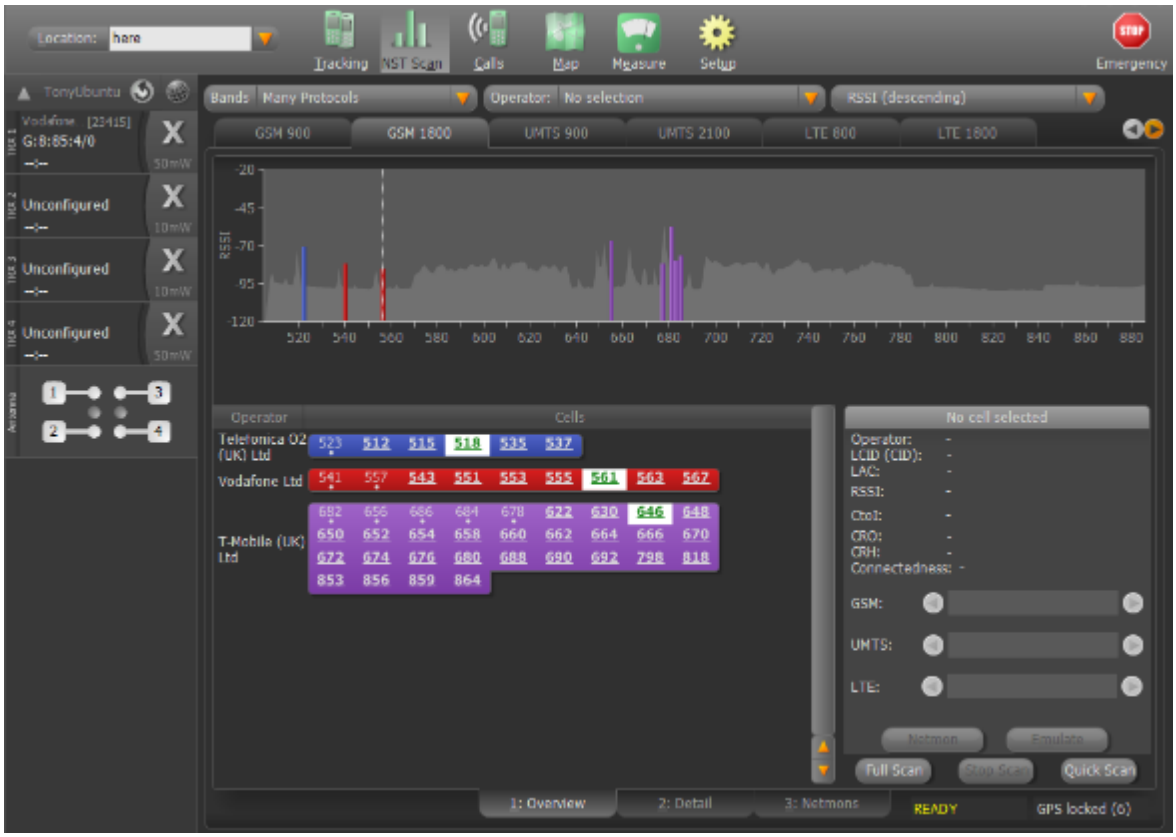
The solution can achieve this on 2G, 3G, 4G and CDMA, and by scanning using multiple channels in conjunction can cover of all key frequencies/protocols.

Unlike handset applications the solution is unbanded, ensuring that any frequency being utilised is detected (Within the frequency range) and specific bands are not missed due to limitations of hardware. This also enables the identification of jamming devices in the vicinity to be detected.



Once more, when a suspicious BTS is detected the user can utilise PEGASUS DF equipment to locate the whereabouts of the system.

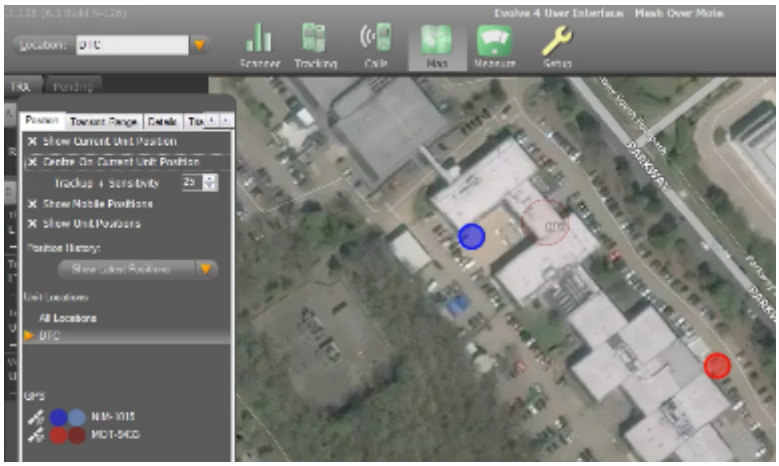
The system is capable of providing a detailed breakdown of the spectrum analysis for technical users:



1.3. Remote Operation

The systems can be deployed as a network, functioning of one GUI and database allowing for a scalable solution.

Pegasus MOTEs/Nimbus are connected utilising 4G, WiFi or our own proprietary IP Mesh products that enable for a secure and robust connection that is independent of 4G jammers that may be in operation in conjunction with the suspected Rogue BTS ensuring the connection does not drop.



The above graphic shows the deployment of two systems.

1.4. Automation

The systems are fully SDR, providing the listed capabilities in one box. Systems can be set to continuously scan mode for a full-time monitoring of the cellular environment and therefore alert of suspicious BTS activity, but they can also be pre-programmed to carry out other activities at event triggers.

Meaning that at set times the systems could be instructed to carry out IMSI registrations e.g. during opening/closing times to track in-flow/out-flow of handsets, as well as function solely as BTS detectors.

2. Specifications

2.1. Pegasus MOTE & PA

Pegasus MOTE is a man-portable low range IMSI Catcher, it is ideal for covert & platform limited applications.

It is a wideband protocol agile single channel unit with some unique key features such as unattended deployment, remote operation as well as the standard IMSI catcher features.

Channels	One (1)
Frequency Range	GSM bands: GSM-850, E-GSM, DCS, PCS UMTS Bands: I, II, III, IV, V, VIII FDD bands: 1-4,5, 7, 8, 9, 10, 12, 13, 17, 20, 25, 26, 28 & 66 LTE TDD bands: 38, 40 & 41
Protocol Support	GSM, UMTS, LTE LTE FDD bands: 1-4,5, 7, 8, 9, 10, 12, 13, 17, 20, 25, 26, 28 & 66 LTE TDD bands: 38, 40 & 41
RF Output Power	MOTE unit 50mW MOTE + PAPSU (optional PA) 4W all UMTS & LTE bands 8W GSM
Power Supply	12-17VDC (14.8VDC nominal) external battery
Power Consumption	20W (unit only) 100W (unit + PAPSU)
Size (inches)	7.60(L) x 3.54(W) x 1.10(H)
Weight	700g (unit only) 4.4kg (unit + PAPSU)
Operating Temperature	0°C to 49°C
Environmental Rating	IP67

External Power Amplifier

Size	225 x 247 x 70 mm
Weight	4 kg
Transmit Power (UMTS/LTE)	4W
Transmit Power (GSM)	8W

2.2. Pegasus HHDF

The Hand-Held Direction Finder is the covert, man-portable offering which provides the user the ability to locate the target handset in close proximity.

Unlike standard Direction Finders, this is not a simple RDF solution resulting in greater range and reduction in interference

The below table outlines the specification for the HHDF unit:

Frequency Range:	GSM: 850 band, 900 band (Inc. E-GSM), 1800 band & 1900 band UMTS: Bands: I, II, III, IV, V & VIII
Power Supply	3 x AA batteries
Power Consumption	Typical battery life 3.5hrs
Size (cm)	HHDF: 12 (L) x 6.5(W) x 2.8(H) High Band Antenna: 78(L) x 78(W) x 18(H) Low Band Antenna: 120(L) x 120(W) x 17(H)
Weight	HHDF: 140 grams High Band Antenna: 230/460 grams (element/array) Low Band Antenna: 550/1100 grams (element/array)
Operating Temperature	0°C to 49°C
Antenna	2 x body worn antennas
Interfaces	On/Off, Status LED, Smart phone interface