GAMMAGROUP

3G-GSM TACTICAL INTERCEPTION & TARGET LOCATION

GAMMAGROUP

INDEX

3G - GSM TACTICAL INTERCEPTION AND TARGET LOCATION

OVERVIEW 3

SECTION 1 - GSM TARGET IDENTIFICATION & LOCATING 4
- BACKGROUND OVERVIEW 5
- ACTIVE OFF-AIR GSM PERMANENT VEHICLE 9
- VEHICULAR SYSTEM 10
- VEHICULAR INSTALLATION SYSTEM 12
- ACTIVE OFF-AIR GSM HIGHLY PORTABLE VERSION 15
- HIGHLY PORTABLE SOLUTIONS 16
- DF EQUIPMENT 18
- HANDHELD DIRECTION FINDER 20
- VEHICLE DIRECTION FINDER 21

SECTION 2 - 3G TARGET IDENTIFICATION & LOCATING 22
- BACKGROUND OVERVIEW 23
- ACTIVE OFF-AIR UMTS OVERVIEW 26
- SPECTRUM SCANNER (SS) 27
- 3G DF EQUIPMENT 28
- HAND - HELD 3G-DF 29

SECTION 3 - GSM VOICE & SMS INTERCEPTION 30
- BACKGROUND OVERVIEW 31
- MASS INTERCEPT-WIDEBAND SOLUTION 34
- MASS INTERCEPT-NARROW BAND SOLUTIONS 36
- TARGETED INTERCEPT - SEMI ACTIVE PASSIVE SYSTEM 38
- TARGETED INTERCEPT - 3G OPTION 39

SECTION 4 - A5.1 DECRYPTORS 41
- BACKGROUND OVERVIEW 42
- NEXT GENERATION A5.1 DECRYPTORS 43

SECTION 5 - ADVANCED MOBILE LOCATION TRACK 46
- ADVANCED MOBILE LOCATION TRACKING 47

OVERVIEW

Cellular networks have created a haven for criminals and terrorists

Over GSM & 3G networks, criminals and terrorist can remain anonymous, able to continue illegal activities on a global scale without fear of action because:

- **No Local Registration is required** – criminals are able to use pre-paid SIM cards or foreign SIM cards without the need to supply any information
- **Post-Paid Subscription Fraud** – criminals are easily able to reprogram phones with a fake identity or use stolen phones and SIM cards

Although powerful Strategic/Countrywide surveillance monitoring tools are at the disposal of Law Enforcement Agencies, the ability to monitor specific criminals/targets critically requires having specific target identity data. In the case of cellular networks the fundamental information is the IMSI (unique identifier or serial number of the SIM) and the IMEI (unique identifier or serial number of the handset).

The IMSI and IMEI is highly prized data, and to protect users it is not normally transmitted within cellular networks. However, if the data is obtained then Law Enforcement Agencies have all they need to monitor Target(s). The challenge is how to overcome the protective security messages within cellular networks protecting their subscribers and covertly elicit specific target user data.

Fortunately, to assist Law Enforcement Agencies we are able to offer solutions which can overcome these challenges. Tactical off-air solutions are available which are able to emulate the cellular network in order to:

1. **Identify & Locate GSM Target(s) Cell-phones**

Determine and locate the identity of a Target(s) GSM cell-phone by pretending to be the real network and tricking the phone to register accordingly. This process allows the unique identity of the phone (IMEI) and the SIM card (IMSI) to be covertly captured, and designated a Target to be precisely located.

2. **Identify & Locate 3G Target(s) cell-phones**

Determine and locate the identity of a Target(s) 3G cell-phone by pretending to be the real network and tricking the phone to register accordingly. This process allows the unique identity of the phone (IMEI) and the SIM card (IMSI) to be covertly captured, and designated Targets to be precisely located.

3. **Intercept the Voice and SMS Communication of Designated Targets**

The communication of Target(s) under surveillance can be captured without their knowledge, including:

- all Voice calls & SMS either made or received by Target(s)
- spoof the identity of Target(s) to falsely send SMS or Voice calls
- divert Calls/SMS so they are not received by the Target(s)
- the ability to edit all SMS before they are received by the Target(s)

GAMMAGROUP

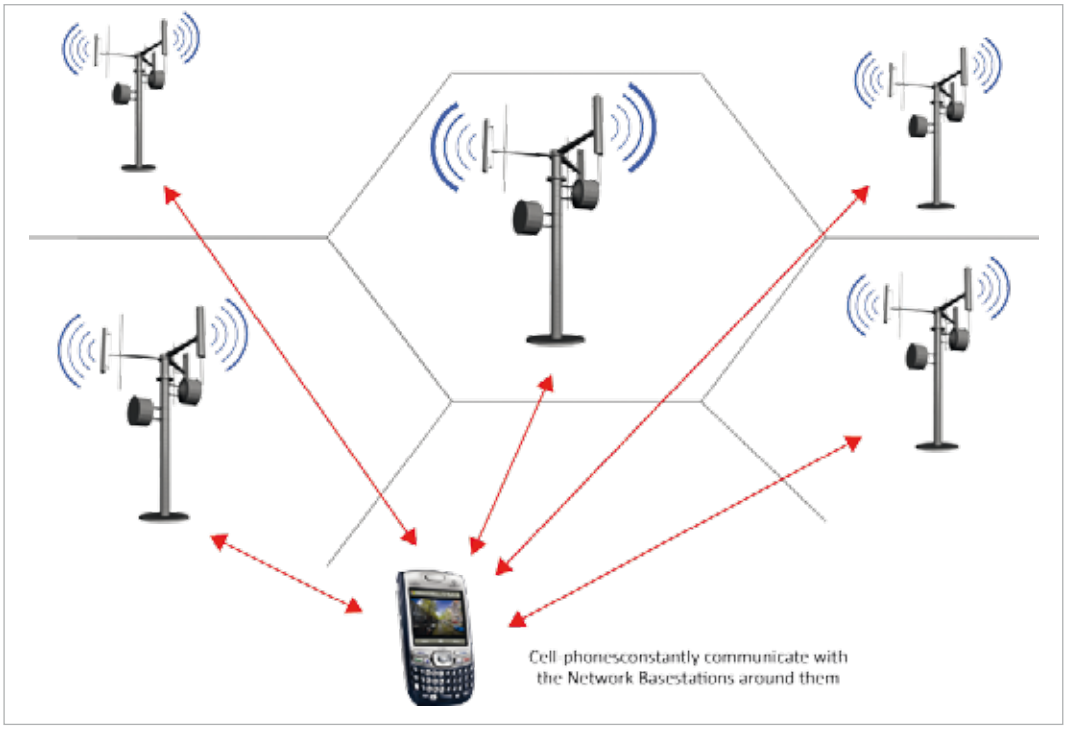
GSM TARGET IDENTIFICATION & LOCATING

GSM/3G NETWORK OVERVIEW	5
GSM IDENTITY CAPTURE	6
GSM TARGET LOCATING	7
TYPICAL OPERATIONAL APPLICATIONS	8
MODEL 4019 PV - ACTIVE OFF-AIR GSM PERMANENT VEHICLE	9
MAPPLICATION EVOLVE4 CONTROL SOFTWARE COMPONENT	10
COVERT VEHICLE ROOF BAR ANTENNA - ANT 8000	11
VEHICLE INSTALLATION OVERVIEW	12
VEHICLE INSTALLATION EXAMPLE	13
ACTIVE OFF-AIR GSM HIGHLY PORTABLE VERSION	15
BODY-WORN IMSI CATCHER	16
RUGGEDISED BRIEFCASE	17
DIRECTION FINDERS	18
HANDHELD DIRECTION FINDER	20
VEHICLE DIRECTION FINDER	21

GSM/3G NETWORK OVERVIEW

GSM is a cellular network, i.e., made up of many cells where each cell contains a Basestation through which subscribers access the Network. The basestation is the fundamental network component which routes all signaling and communications over the air between the cell-phone and Network.

To ensure countrywide connectivity, many thousands of basestations are used. Transmitting on a different frequency to ensure there is no interference, the cell-phone constantly monitors the signal strength of its surrounding basestations. As a subscriber moves, the cell-phone will join the most attractive basestation available to ensure optimum network connectivity. This is an automatic action happening in the background to the ignorance of the user.



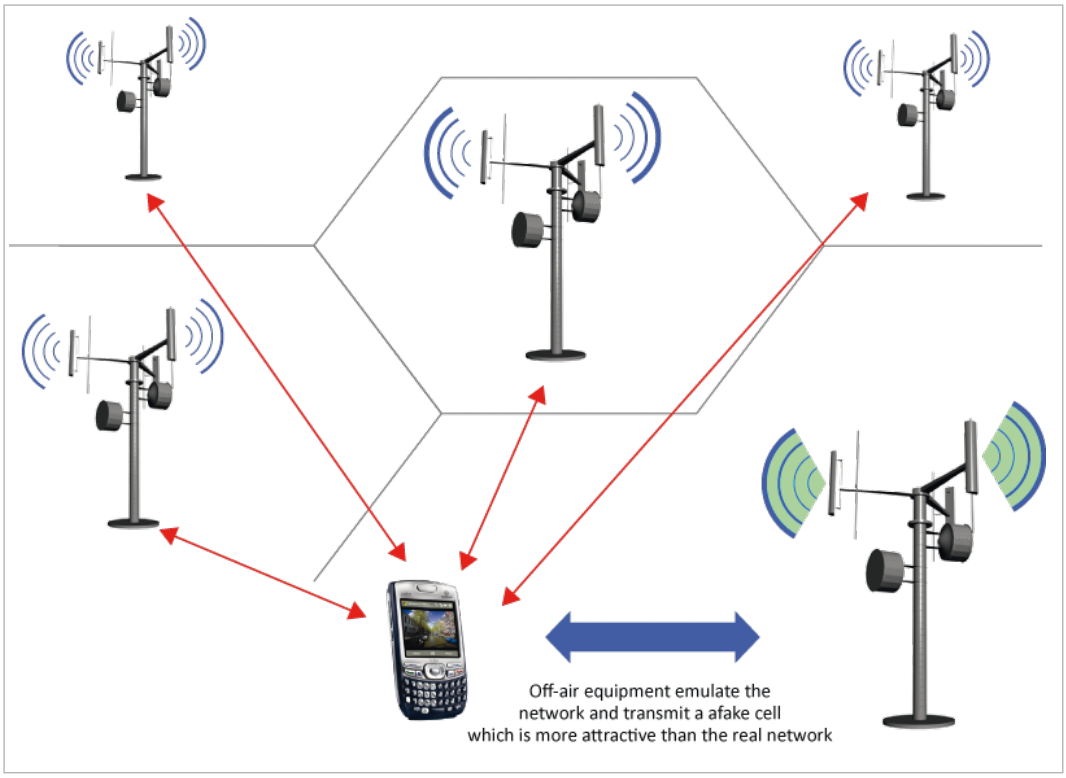
GSM & 3G cellular networks use only 2 unique identifiers: the IMSI (cell-phone identity) and IMEI (SIM card identity). To protect a subscriber's identity the IMSI & IMEI are only transmitted over the air in certain cases: when cellphones are switched on or when crossing special cell boundaries between different LAC (Local Area Code). Networks use instead a 3rd identifiter, the TMSI (Temporary Mobile Subscriber Identity), to communicate with a cell-phone, a temporary identity which is continually changed throughout the day.

GSM IDENTITY CAPTURE

The ability to covertly monitor designated targets is virtually impossible without first knowing the identity of the Target(s) cellphone. The behavior of Targets who are constantly changing phones or SIM cards makes this much harder especially when there may only be limited engagement opportunities.

Working off-air, solutions today take advantage of the requirement for the cell-phone to continually search for the strongest valid network cell. Emulating a valid network cell they will transmit a more attractive signal to attract cell-phones to join. The process of joining results in the cell-phone providing its unique IMSI & IMEI details.

Now Law Enforcement Agencies can target specific cell-phones to covertly obtain their details. It is relatively straightforward within GSM networks to obtain the IMSI & IMEI providing the correct cell is emulated. A cell-phone only actively monitors the 6 strongest neighboring cells. To grab Target(s) requires emulating one of these neighbor cells. Solutions today will aid users in this cell selection process.



BACKGROUND OVERVIEW

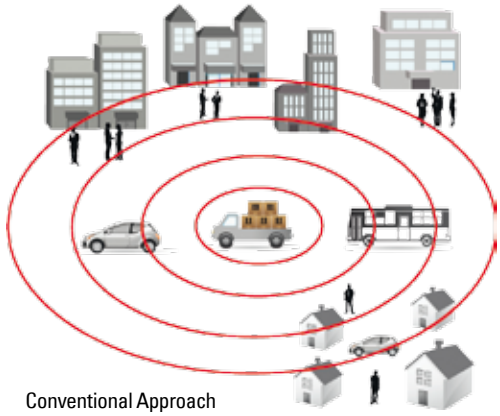
Although acquiring IMSI & IMEI is very fast, the real challenge lies in filtering out the Target(s) identity from unwanted collateral.

For example, operating within busy or crowded areas will result in many thousands of identities being acquired, most of whom will not be of interest or unwanted collateral.

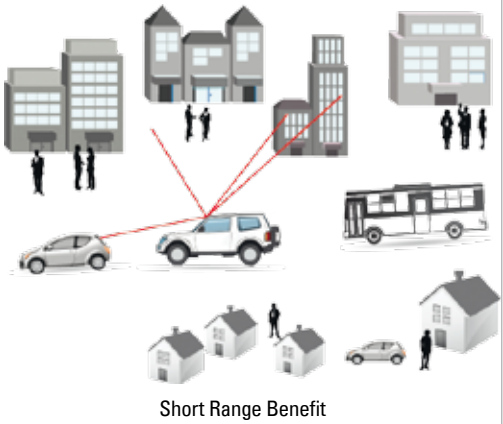
The conventional operating procedure is to physically follow the Target(s), grab identities across multiple locations and look for common IMSI & IMEI.

This can be time consuming and often not practical given the careful behavior of organized criminals & terrorists.

It is much more efficient to operate as close as possible to the Target(s) at minimal transmission power. This will reduce the system footprint/area of coverage and hence unwanted collateral.



Conventional Approach



Short Range Benefit

GSM TARGET LOCATING

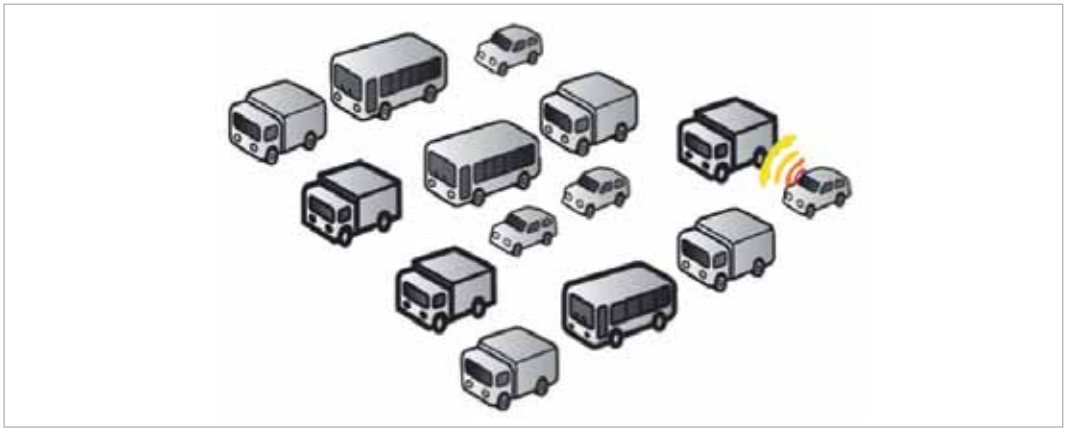
Once the IMSI & IMEI of a Target is known, a cell-phone can be grabbed and forced to transmit. Commonly known as a `Blind` or `Silent` call, the cell-phone transmits without the knowledge of its target.

This RF transmission, normally set to a quiet RF channel where there are no other transmissions, can then be precisely located to within a few metres using vehicular or body worn/handheld direction finding systems.

TYPICAL OPERATIONAL APPLICATIONS

There are a number of wider applications for which IMSI/IMEI systems can be used:

- Large area coverage, for example, borders or particular areas of interest
- At immigration/customs points of entry, whether ports or airports log all visitors as they enter a country
- Scanning of cargo from packages to large containers to identify the presence of GSM devices, whether cell phones or IED triggers
- Detecting the illegal use of mobile phones within Prisons
- Building protection 'known phone' policy enforcement systems for secure buildings, military bases and embassies
- TSCM applications to detect GSM enabled listening devices



Example 1: covert scanning of vehicles or containers

Example 2: automatic point of entry detection system

GAMMAGROUP

MODEL 4019 PV

ACTIVE OFF-AIR GSM PERMANENT VEHICLE

ACTIVE OFF-AIR GSM PERMANENT VEHICLE

GENERAL OVERVIEW

The family of active interception solutions provides a tactical tool for Law Enforcement, Government and Military Agencies.
Utilizing commercial base-station technology and operating independently of the GSM network providers, the family of vehicle and portable products provide the capability to clone and simultaneously transmit multiple fake GSM networks to interact with GSM cell phones.

MAIN FEATURES

- Covertly identifies the unique identity (IMSI/ IMEI) of GSM cell phones
- Locates known targets using their GSM mobiles in conjunction with the direction finding equipment
- Takes control of target phones for the purpose of denying GSM services
- Creates a bubble or exclusion zone to deny GSM network coverage without alerting cell phones
- Intercepts outgoing calls and SMS messages sent by a target
- Rugged form factor for in-vehicle use
- Multiple BTS systems allowing up to 4 BCCH on 1 network or 4 BCCH on 4 different networks
- HighTransmit of output power – up to 50 Watts per Band
- Blind/Silent Call up to 7 target cell phones per BTS
- Simultaneous intercept of up to 4 outgoing voice calls
- Simple to use Graphical User Interface (GUI)

4019 PV

KEY SPECIFICATIONS

Channels
4 Channels
2x900 + 2x1800 or 2x850 + 2x1900 or
1x850 + 1x900 + 1x1800 + 1x1900 (Quad)

Channel Range
Euro: E-GSM, GSM, DCS
US: 850, PCS
Quad: 850, E-GSM, GSM, DCS, PCS

Output Power
1mW to 50W (max) per band

Operating Temperature
-5°C to + 45°C (23°F to 113°F)

Power Consumption (Max.)
600W

Power Supply
24 VDC

Size
W 500mm x H 200mm x D 580mm 28kg

Interface Connections
Antennas:
Directional: 2x Low Band, 2 x High Band
Omni: 2 x Combined
Data/ Audio: Interface via secure Ethernet

Configurations:
- 4019 2I (2-channel IMSI catcher)
- 4019 4I (4-channel IMSI catcher)

Options:
- Blind call, Voice interception, SMS interception, private networking, Service denial
- Option for 2-channel: 2x BTS Upgrade

GAMMAGROUP

MAPPING SOFTWARE

VEHICULAR SYSTEM

MAPPLICATION EVOLVE4 CONTROL SOFTWARE COMPONENT

MAPPING OPTION

Operating in unfamiliar areas can be challenging, especially when under time pressure.
The new Mapplication software component introduces a mapping interface which can help operators to tackle this problem and run faster, more effective missions.

Network structures can be difficult to analyze; Mapplication assists by plotting cell coverage graphically in the mapping interface.
DF operations can be improved by using Mapplication to highlight the boundary of the target cell, reducing the search area.

Transmit power requirements may be hard to judge at the first attempt. Using Mapplication's TX range feature gives the operator a graphical estimate of unit coverage area, allowing better adjustment of unit TX power.

MAPPLICATION OPTION INCLUDES:

- Free software upgrade to Evolve4 Control Software
- GPS with SiRFstar III chipset
- Vector street mapping to cover country of customer's choice
- Network Scanner and accessories can be supplied as a separate option, if required
- Mapplication may require an XPZ or 3GN hardware upgrade, dependent on unit version

MAIN FEATURES

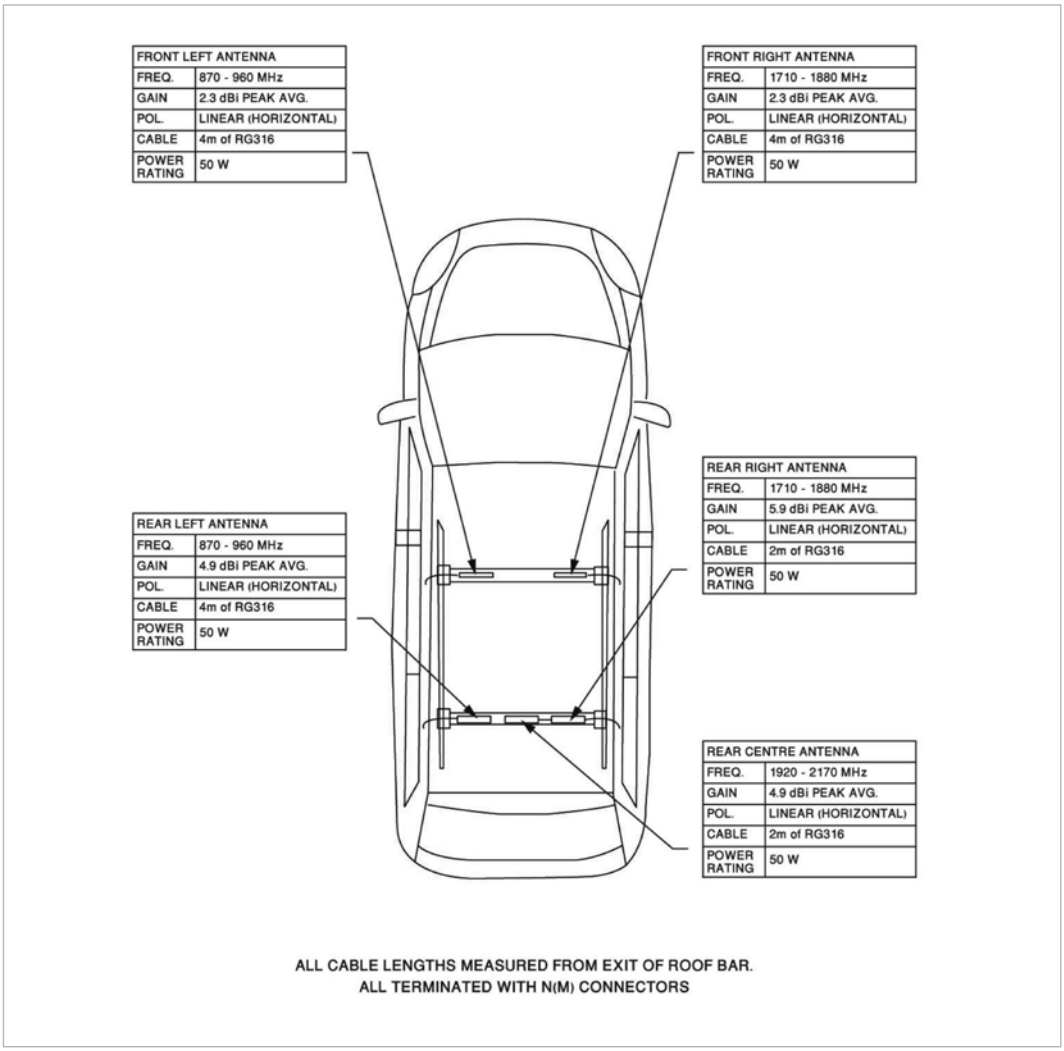
- Introduces a mapping interface to the new Evolve4 Control Software
- Provides graphical display of GSM and WCDMA cell coverage
- Improves DF operations by defining the boundary of the target cell, allowing the operator to reduce the size of the search area with confidence
- Plots unit position on the map in real-time
- TX trail feature shows the route the unit has taken whilst transmitting
- Displays estimated unit TX range via RF propagation modeling
- Geo-tags entries in database with unit position at time of phone acquisition
- Delivered with Navteq street map data for chosen country
- Interoperates with our new Network Scanner which supplies GSM/WCDMA cell data

COVERT VEHICLE ROOF BAR ANTENNA - ANT 8000

VEHICLE INSTALLATION

This document provides information regarding the process of making a permanent installation of the Unit PV variant in a vehicle.
It presumes a basic familiarity with GSM networking and the Unit system.
Key features of the proposed solution include:

- Integrated 2G and 3G solution
- Optional antenna strategies
- Choice of recommended vehicle installations



VEHICLE INSTALLATION OVERVIEW

INTRODUCTION

This document provides information regarding the process of making a permanent installation of the Unit PV variant in a vehicle.

It presumes a basic familiarity with GSM networking and the Unit system.

Key features of the proposed solution include:

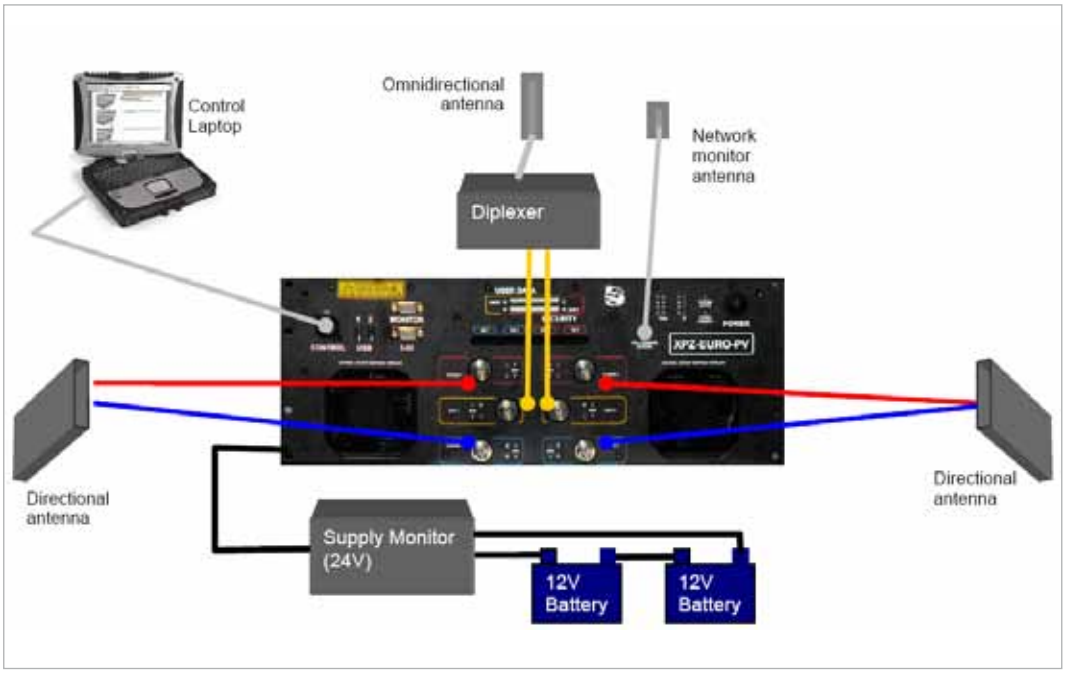
- Integrated 2G and 3G solution
- Optional antenna strategies
- Choice of recommended vehicle installations

INSTALLATION DESIGN PHILOSOPHY

There are two broad design philosophies that may influence decisions taken during the vehicle installation process:

- Covert, where it is of the utmost importance that a vehicle retains the outward appearance of a stock factory model
- Optimum performance, where the main priority is to achieve maximal performance from the unit

The requirements dictated by these design philosophies often run counter to one another, so it is important that consideration be undertaken ahead of the installation about where priorities lie.



VEHICLE INSTALLATION EXAMPLE

VEHICLE INSTALLATION

An example vehicle installation is described where the Unit and 3G systems were installed into a VW Touareg SUV.

ANTENNA CONFIGURATION

For this installation, directional antennas were mounted on both sides of the vehicle under the large trim panel that forms the back bumper and part of the rear wings.

The antennas were angled slightly upwards to optimize use of the beam pattern. Cables were fed back through access points in the vehicle paneling so that when the rear trim panel was replaced, the antennas and cabling were completely concealed.

An omnidirectional antenna was integrated into the vehicle's factoryfitted "shark's fin" antenna on the roof. With the antenna cover replaced, a completely stock look was achieved.

GAMMAGROUP

MODEL 4019 HP

ACTIVE OFF-AIR GSM HIGHLY PORTABLE VERSION

ACTIVE OFF-AIR GSM HIGHLY PORTABLE VERSION

GENERAL OVERVIEW

The family of active interception solutions provides a tactical tool for Law Enforcement, Government and Military Agencies.
Utilizing commercial base-station technology and operating independently of the GSM network providers, the family of vehicle and portable products provide the capability to clone and simultaneously transmit multiple fake GSM networks to interact with GSM cell phones.

MAIN FEATURES

- Covertly identifies the unique identity (IMSI/IMEI/TMSI) of GSM cell phones
- Locates known targets using their GSM mobiles in conjunction with direction finding equipment
- Takes control of target phones for the purpose of denying GSM service
- Creates a bubble or exclusion zone to deny GSM network coverage without alerting cell phones
- Intercepts SMS messages sent by a target
- Small rugged highly portable design
- Multiple BTS systems allowing up to 2 BCCH on 1 network or 2 BCCH on 2 different networks
- Transmits output power - up to 500mW
- Blind/Silent Call up to 7 target cell phones per BTS
- Built-in WiFi or wired Ethernet connectivity to mini PC (supplied as standard)
- Simple to use Graphical User Interface (GUI)

KEY SPECIFICATIONS

Channels
2 Channels
1 x 900 + 1 x 1800
1 x 850 + 1 x 1900

Channel Range
Euro: E-GSM, GSM, DCS
US: 850, PCS

Channel Frequency
200 KHz

Output Power
1mW to 25W (max) per channel

Operating Temperature
-5°C to + 45°C (23°F to 113°F)

Storage Temperature
-10°C to + 70°C (14°F to 158°F)

Power Consumption (Max.)
60W

Power Supply
12 VDC

Size
W 280mm x H 70mm x D 290mm, 4.43kg

Interface Connections
Antenna Ports:
1 x Combined Tx, 1 x Combined Rx, 1 x WiFi
Data: Interface via secure Ethernet or WiFi

GAMMAGROUP

MODEL 4062

HIGHLY PORTABLE SOLUTIONS

BODY-WORN IMSI CATCHER

GENERAL OVERVIEW

The new generation of GSM & 3G IMSI & IMEI acquisition technology, is designed for rapid Target(s) identity acquisition.
Utilizing our exclusive PAF (Patent Applied For) technology the system is able to acquire identities without any set-up or network analysis required, regardless of the number of networks operating whether GSM or 3G.

The unit is optimized for short range covert operation, designed to allow users to get close to Target(s) to maximize the chances of only catching the Target(s) identities and minimal unwanted collateral. The solution can be used as a standalone device or integrated into wider data-gathering and geo-tracking systems.

FEATURES

- System start-up time of >20 seconds, no network analysis required
- Rapid capture of IMSI/IMEI. Speed of 1-90 seconds from start to capture (average capture time of 45 seconds)
- Works on any GSM based network, in any country
- Does not alter network selection if target device is roaming
- Fully operational in a non-static environment (e.g. moving vehicle)
- Self-contained, battery powered system for field flexibility
- 60 degree directional antennas for precise targeting
- Covert operation using wireless smart-phone or net-book based control system
- Rugged, field-ready construction throughout
- Simplified GUI of ease of operation and minimized training time

SPECIFICATIONS

- Function: Rapid capture of IMSI / IMEI
- Target device network range: 850, 900, 1800, 1850, 3G, 3.5G, UMTS, HSPDA, LTE
- Operating range: 0 – 10 M
- Capture time 1 – 90 seconds
- Power: Internal battery or external 90-264VAC
- Charging: External AC powers unit and charges internal battery (typical 2.5hrs to fully charge)
- Battery operational time: Typical 2.2hrs fully charged
- Temperature range for normal operation: 0-30 deg C
- Dimensions: 40.6 x 33 x 18 cm (Peli 1450)
- Weight: 6.5 kg

GAMMAGROUP

MODEL 4061

HIGHLY PORTABLE SOLUTIONS

RUGGEDIZED BRIEFCASE IMSI CATCHER

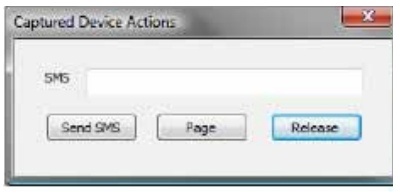
GENERAL OVERVIEW

The new generation of GSM & 3G IMSI & IMEI acquisition technology, is designed for rapid Target(s) identity acquisition. Utilizing our exclusive PAF (Patent Applied For) technology the system is able to acquire identities without any set-up or network analysis required, regardless of the number of networks operating whether GSM or 3G.

The unit is optimized for short range covert operation, designed to allow users to get close to Target(s) to maximize the chances of only catching the Target(s) identities and minimal unwanted collateral. The solution can be used as a standalone device or integrated into wider data-gathering and geo-tracking systems.

FEATURES

- System start-up time of >20 seconds, no network analysis required
- Rapid capture of IMSI/IMEI. Speed of 1-90 seconds from start to capture (average capture time of 45 seconds)
- Works on any GSM based network, in any country
- Does not alter network selection if target device is roaming
- Fully operational in a non-static environment (e.g. moving vehicle)
- Self-contained, battery powered system for field flexibility
- 60 degree directional antennas for precise targeting
- Covert operation using wireless smart-phone or net-book based control system
- Rugged, field-ready construction throughout
- Simplified GUI of ease of operation and minimized training time



SPECIFICATIONS

- Function: Rapid capture of IMSI / IMEI
- Target device network range: 850, 900, 1800, 1850, 3G, 3.5G, UMTS, HSPDA, LTE
- Operating range: 0 – 10 M
- Capture time 1 – 90 seconds
- Power: Internal battery or external 90-264VAC
- Charging: External AC powers unit and charges internal battery (typical 2.5hrs to fully charge)
- Battery operational time: Typical 2.2hrs fully charged
- Temperature range for normal operation: 0-30 deg C
- Dimensions: 40.6 x 33 x 18 cm (Peli 1450)
- Weight: 6.5 kg

DIRECTION FINDERS

PURPOSE

The direction finder (DF) is intended for searching and localizing handsets operating in GSM bands 900, 1800 and 1900MHz. It is the additional equipment for A5.1 stationary or portable active system. The main idea of the target's direction finding procedure is to register the required mobile phone in the internal BTS and switch ON its transmitter. The direction finder must be tuned to the same ARFCN channel as the BTS. From this moment the DF user will hear the detected sound signals of TDMA sequence which is natural for GSM telephony.

MODEL GSM-DFB

While operating the DF, it is necessary to connect it to the antenna connector of the corresponding range. Rotating the antenna right or left allows achieving the maximum in signal level reading on the control unit LED or the maximum volume level in the headphones. Depending on direction and distance from the object, the volume level in headphones will change. The maximum volume of the sound signal is correlated with the target's location. While the operator is approaching the object being searched, it may be necessary to change sensitivity of the device by switching on 3-stepped attenuator 10, 20, 30 dB. Attenuation value is determined by experiment.

Control unit

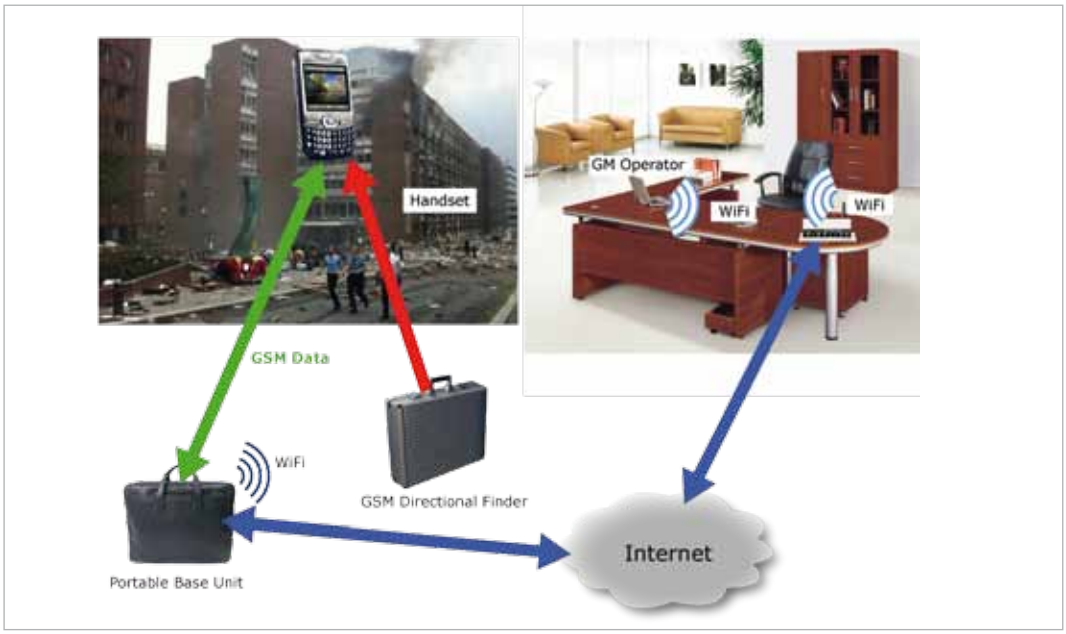
Headphones

Case variant antenna

Body keeping antenna

FEATURES

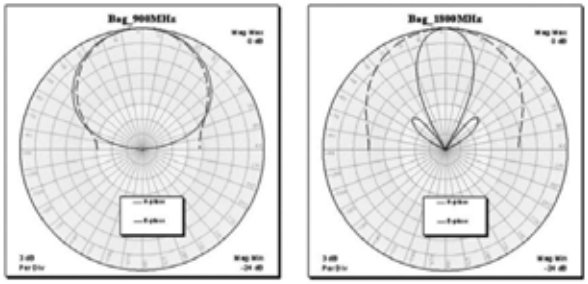
- Compact dimensions
- Case and body variants
- Thin radiation pattern
- Included attenuator
- Sound indication



TECHNICAL SPECIFICATIONS:

Operation band	GSM/DCS, PCS
Attenuator	10, 20, 30 dB 3-stepped
Operation distance	10 - 500 m
Distance correlation parameter	SoundTDMA sequence

RADIATION PATTERN FOR BASIC ANTENNAS



Case variant

Body keeping

GAMMAGROUP

MODEL 4019 HDF

HANDHELD DIRECTION FINDER

HANDHELD DIRECTION FINDER

GENERAL OVERVIEW

Model 4019 HDF is a lightweight, portable and state-of-the-art handheld direction finder (HDF) for tracking and geo-locating cell phones.

The 4019 HDF is designed to work with any Active GSM manipulation system on the market today.
The convenient size of the 4019 HDF, allows it to be deployed in many covert applications normally considered unsuitable for GSM cell phone geo-locating.

The 4019 HDF is field proven and is in current use by many of the leading Law Enforcement Agencies and Special Forces around the world.

MAIN FEATURES

- DF on any ARFCN
- DF in Azimuth (or Elevation using Yagi antenna)
- LCD display showing selected Band and ARFCN
- LED indication showing received signal strength
- Audio indication of received signal strength
- Squelch control for sensitivity adjustment
- Covert mounting possibilities
- Capability for wireless loop attachment to enable highly covert operation
- DF targets to within a few meters
- Lightweight and small in size
- Requires standard 'AA' size batteries
- Various antennas available

KEY SPECIFICATIONS

Function
Provides RF signal strength indication on a selectable RF channel

Frequency Range
Euro: 900MHz Uplink (880-915 MHz)
1800MHz Uplink (1710-1785MHz)
US: 850MHz Uplink (824-849MHz)
1900MHz Uplink (1850-1910MHz)

Rx Sensitivity
Typically ≥ 97 dβm

HHDF Receiver
W 65mm x H 90mm x D 28mm

Weight
0.14kg

Power
3Vdc, 2 x AA Batteries

Battery Life
≥ 10 hours (typical usage)

Antenna
Directional Dual Band Patch Antenna (SMA Connector)

Operating Temperature
-5°C to +50°C (32° F to 122° F)

Storage Temperature
-10°C to +75°C (14° F to 167° F)

Interfaces
On/Off, volume control
Mode/Channel selection
RF Sensitivity adjustment

GAMMAGROUP

MODEL 4019 VDF

VEHICLE DIRECTION FINDER

VEHICLE DIRECTION FINDER

GENERAL OVERVIEW

The VDF is a lightweight, portable and state of the art digital direction finder for tracking and geo-locating GSM cell phones. It features the latest Super Resolution DF processing algorithms. The VDF is designed to be deployed quickly in any vehicle allowing maximum flexibility in vehicle choice, thus maintaining a covert deployment model.
The VDF is a standalone system designed to work with any GSM manipulating system on the market today.

MAIN FEATURES

- Geo-locate targets to within a few meters
- DF on any ARFCN
- DF on a specific Timeslot in 'Slotted' mode for increased accuracy when using the Unit
- DF simultaneously in Azimuth and Elevation
- Robust, low profile lightweight antenna unit
- Antenna unit designed for covert internal or external mounting
- Bearing Direction given in relation to North and vehicle heading
- A dual band digital receiver featuring 8 self-calibrating phase synchronous digital receiver branches
- 8 element spatially diverse omni-directional antenna arrays for highly accurate target resolution
- Integrated GPS and Electronic compass for non-moving Line of Bearing (LOB) resolution
- Recording & Playback of LOBs and mission data
- Highly stable Rubidium reference for long-term tracking of time slotted GSM signals
- User-friendly Graphical User Interface (GUI)
- Integrated GIS Mapping engine

KEY SPECIFICATIONS

Function
Provides RF signal strength indication on a selectable RF channel

Channel Range
GSM 900/1800 ARFCN 975-1023, 0-124, 512-885

Direction Finding Axis
Simultaneous in Azimuth and Elevation

Resolution Better than 5°

Accuracy Better than 5°

Sensitivity
Typically $\geq$ -120dβm

DF Algorithms
Super Resolution DF with self-calibration

VDF Receiver
W 448mm x H 135mm x D 348mm 7.2kg

VDF Antenna
W 270mm x H 60mm 1.3kg

GPS Datum WGS-84

Magnetic Compass
2 Axis tilt compensated digital compass

Power Supply
12Vdc, 7.5A, 90W (Rubidium reference cold)
12Vdc, 4.5A, 54W (Rubidium reference warm)

Antenna (rooftop) Azimuth: 360° Elevation: 80°

Antenna (in-vehicle)
Azimuth: 360°, Elevation: (as per vehicle aperture)

Mapping Formats MxD files supported

GAMMAGROUP

3G TARGET IDENTIFICATION & LOCATING

3G NETWORK OVERVIEW	23
KEY CHALLENGES	24
OPERATIONAL PROCEDURE AND IMPLICATIONS	25
ACTIVE OFF-AIR UMTS OVERVIEW	26
SPECTRUM SCANNER	27
3G DF EQUIPMENT	28
HANDHELD 3G-DF	29

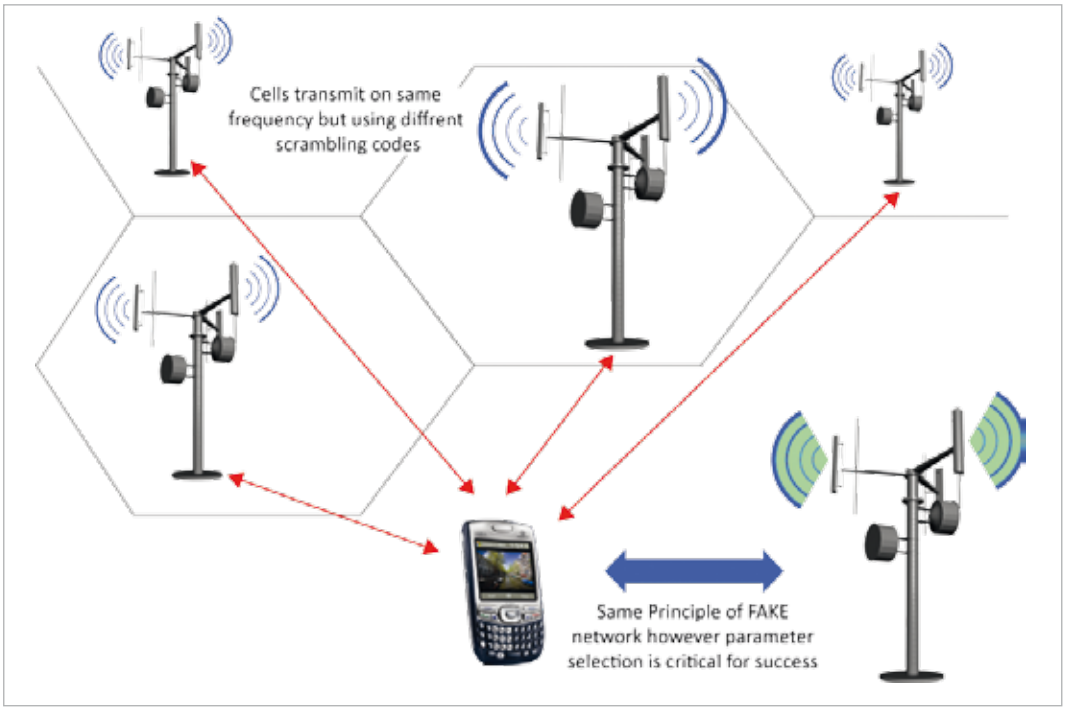
3G NETWORK OVERVIEW

The demand for high speed communications and faster data throughput has excceded the capability of GSM, a second generation communications network. The next or 3rd generation network is an evolution of GSM and uses CDMA (Code Division Multiple Access) instead of TDMA (Time Division Multiple Access) technology to achieve much greater performance. Also known as UMTS these networks are spreading rapidly with most of Europe, Middle East and Asia already covered.

Current IMSI catching equipment, developed for GSM, will not work on 3G networks. 3G differs from GSM by using Scrambling Codes rather than frequencies to separate communications. A popular analogy to show the difference is in a room full of people; in 3G they all speak at the same time whereas in GSM they take turns. The reason why they can communicate when talking at the same time is because they are speaking different languages.

Each cell still contains a Basestation, now called Node B through which subscribers access the Network. Although the Node Bs transmit on the same frequency they use different scrambling codes to ensure there is no interference. Each scrambling code is unique and will not interact with another code. They appear 'noise like' yet can be recovered and transmission is easily reconstructed due to these properties.

As per GSM, a cell-phone will monitor the Node Bs around its location and, if a stronger or more attractive signal is seen, will jump to this Node B. The approach of emulating a real cell and transmitting a Fake cell to attract a cell-phone is still valid, and as before, results in the cell-phone providing its IMSI & IMEI.



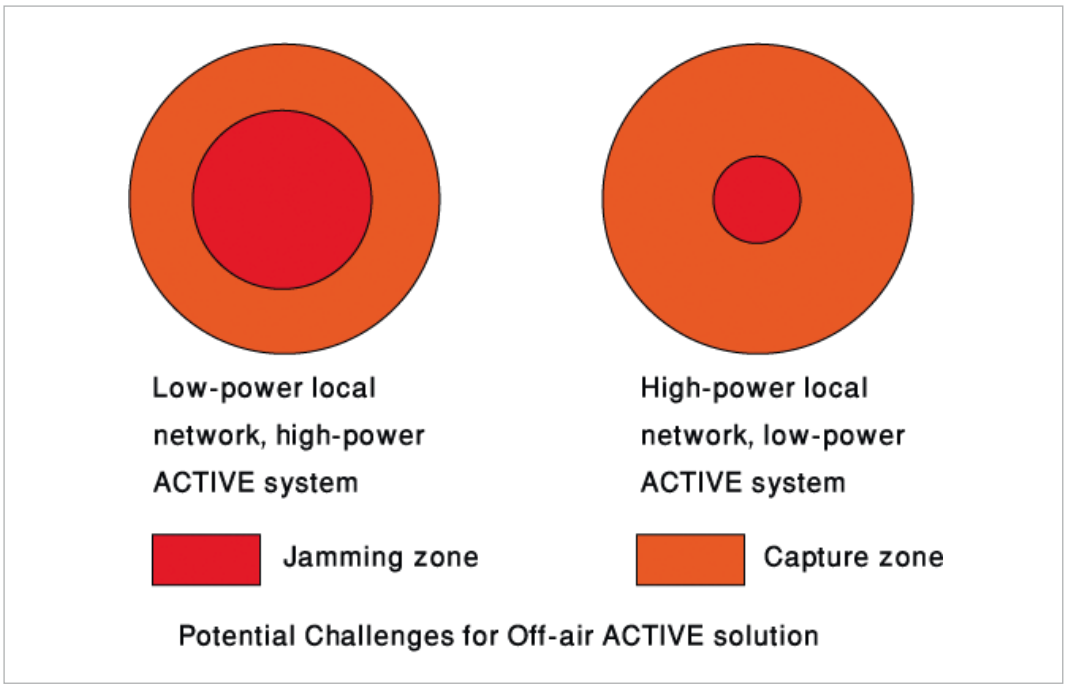
KEY CHALLENGES

Although 3G networks are much more efficient they require very careful power control management to minimize the impact of interference. Although a cell transmits on a different Scrambling Code, essentially a noise-like signal, it is still transmitting on the same frequency as its neighboring cells. The net effect of each cell transmission is to introduce more noise into the 3G network.

Management of the transmission power of each cell is absolutely critical to limit their ability to increase the noise. As noise levels increase within the network, the size of the cell will reduce, with the worst case cell-phones losing network connectivity. To handle this eventuality the 3G network use a back-up frequency to which they switch subscribers.

A 3G ACTIVE system will emulate a real cell to attract cell-phones. It has to transmit on the same frequency as the real network albeit using a different Scrambling Code. This raises the possibility for the ACTIVE system to 'Jam' the network as it is putting essentially more noise into the network. The process of covert identity acquisition requires rejecting cellphones back to the real network. If now, the ACTIVE system also affects the quality of the real network, cell-phones will be reluctant to rejoin a poorer 3G network and will either:

- take longer to rejoin the 3G network, they will wait until the real network cell quality is acceptable.
- connect if they are allowed to the GSM network as cell quality has dropped to an unacceptable level.

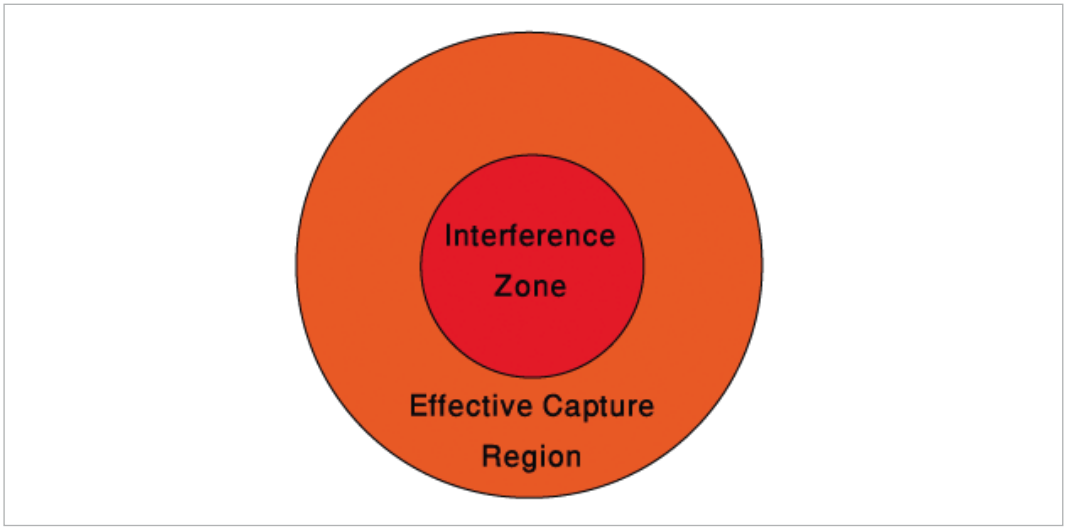


Potential Challenges for Off-air ACTIVE solution

OPERATIONAL PROCEDURE AND IMPLICATIONS

Unlike GSM, it is critical to choose optimum transmission parameters for the ACTIVE system. This requires a deep understanding of the real network and following the recommended protocol to ensure consistent success:

- Gather network information from target area using suitable network monitoring tools whether Test Phones or MMI Spectrum Scanner. Key information requires capturing SIB11 messages to identify optimum emulation cell.
- Choose IMSI Catching Cell configuration including Scrambling code and frequency. Systems will recommend the best cell to emulate in the neighbor list of the network cells. Note, if not done correctly then phones will not be caught, instead they will be pushed off the 3G network by the interference generated by the ACTIVE system.
- Choose IMSI Catching cell transmit power, taking network cell power levels into consideration. Note, the desired capture distance is also very important: the larger the fake cell created the greater the disruption. Note, cell-phones closest to the system will be jammed.



CONCLUSIONS

In comparison to GSM IMSI & IMEI acquisition, the brief summary above shows IMSI Catching in 3G/UMTS is a much more complicated process. Users require a detailed understanding of how 3G networks function and the key parameters used by the network.

The complexity of 3G makes it very easy to incorrectly use ACTIVE systems. The consequences are potentially disastrous, and in the worst case scenario can jam all 3G phones in the deployment area. It is crucial for users to:

- Only use adequate technical solutions, including 3G network training
- Acquire key cell parameters, such as Cell Power and Scrambling Codes
- Transmit at minimum power levels

GAMMAGROUP

MODEL 4019 3G

ACTIVE OFF-AIR UMTS OVERVIEW

ACTIVE OFF-AIR UMTS OVERVIEW

GENERAL OVERVIEW

The 3G is a state-of-the-art multi-channel UMTS (WCDMA) tactical active interception solution. The 3G is currently used in conjunction with the system range. Control is streamlined to a single interface where users can simultaneously acquire the identities of GSM and 3G/UMTS phones.

For geo-locating and tracking purposes the 3G/ UMTS target phone is 'pushed' onto the system cell and then placed into blind call mode.

MAIN FEATURES

- 3G Identify grabbing using protocol message exchanges rather than 'Jamming'
- Advanced Node B configuration for emulation of any UMTS network
- Fast UMTS cell configuration using optional 3G Spectrum Scanner
- Integrated 2G/3G system operation when connected to a GSM-XPZ system
- Single combined database for 2G & 3G operation
- Identification whether mobile phone is caught on 2G or 3G
- UMTS Band 1 (2100MHz) operation
- Transmits 2x3GPP configured UMTS cells simultaneously to a maximum of 5W each
- Adjustable Node B transmission power, ranging from 1mW to a maximum of 20W on a single Node B
- Integrated Antenna Switch for up to 3 antennas
- User friendly Graphical User Interface (GUI)
- Powerful database search facility for quick target identification

KEY SPECIFICATIONS:

Function
Simultaneously acquires the identity parameters (IMSI, IMEI & TMSI) of UMTS cell phones off-air from two different UMTS networks
'Push' target cell phones to GSM in a controlled manner for geo-locating

Correctly interacts with non-target cell phones to preserve 3G network service in the operational zone

Channels
2 Channels

Channel Range
UMTS Band 1 (2110-2170MHz)

RF Output Power
2 x 5W max or 1 x 20W max

RF Output Connector
3 x N Type

Size
W 324mm x H 180mm x D 398mm

Weight
16.5kg (20kg including carry case)

Operating Temperature
-5°C to + 45°C (23°F to 113°F)

Storage Temperature
-10°C to + 70°C (14°F to 158°F)

Power Supply
12 VDC – 24 VDC

Power Consumption (Max.)
16A, 400W maximum

GAMMAGROUP

MODEL 4024 SPECTRUM SCANNER (SS)

SPECTRUM SCANNER

GENERAL OVERVIEW

The Spectrum Scanner (SS) is a lightweight, portable and state-of-the-art 3G or UMTS spectrum Scanning Tool. Featuring the latest bespoke receiver technology, the unit is a standalone system designed to work with any UMTS manipulation system on the market today.
Using optimized scanning technology, the SS will fully decode all 3G or UMTS information required for the configuration of a 3G or UMTS IMSI grabber.
The Spectrum Scanner provides the information in a simple, easy to understand format.

MAIN FEATURES

- Simple Graphical User Interface (GUI) reducing training time for new operators
- Capability to scan all channels in a single frequency band
- Fast scanning time, typically less than 120 seconds
- SIM card free operation
- Detailed analysis of nominated channels/ UARFCNs
- Display of total Received Signal Strength Indication (RSSI) per UARFSN
- Display of Received Signal Code Power (RSCP) per scrambling code
- Read MIB and all broadcast SIBs transmitted on the P-CCPCH, for each detected cell

SYSTEM MODES

Spectrum Overview
Scans all channels within frequency band for UMTS channels in use

Detailed Analysis
Displays detailed network structure information of selected network operator/UARFCN

Recommend Cell Emulation
Takes the output of the scan and recommends in order the best cell to emulate

Network Monitor
Takes the input of the scan and provides decoded neighbor list information for the requested cell

KEY SPECIFICATIONS:

Function
Scans all channels in specified frequency band for active UMTS

Channel Range
UMTS Band 1 (2100MHz)

Sensitivity
3 GPPTS25.101 compliant

Supply Voltage
12Vdc or 24Vdc

Power Consumption
<60W

Antenna Connector
SMA female

Receiver Unit
W 323mm x H178mm xD288mm 4.81kg

Operating Temperature
- 5°C to + 45°C (23°F to 113°F)

Display Device
Panasonic Toughbook CF 19

Interfaces
RJ45 Ethernet
USB

3G DF EQUIPMENT

GENERAL OVERVIEW

3G Blind Call is a new software feature for the 3GN UMTS system. It allows 3G phones to be locked to the 3GN and placed in a UMTS blind/ silent call for tracking purposes.
This is the only way to establish blind calls to phones that are set in "3G only" mode, and it removes the reliance on passing the 3G phone to a GSM system for tracking – the target phone stays on 3G frequencies at all times.
The 3G-DF can detect and track the signal from a 3G phone in a blind call, allowing the DF operator to locate it.

3G-DF FEATURES

- Provides indication of target RSCP (Received Signal Code Power) to enable operator to judge distance and bearing to target
- Features graphical and audio feedback of current target RSCP level for ease of use in challenging operational scenarios
- Quick and simple to use with minimal configuration required

BLIND CALL FEATURES

- New Acquisition mode for the 3G and DF target status for 3G phones makes operation simple
- Multiple 3G blind calls can be supported by each 3GN Node B
- Automatic 3G power control ensures that Node B and phone TX power are continually adjusted to optimal levels to maintain the blind call
- The 3GN can continue to take registration from other 3G phones whilst maintaining a blind call to the target phone

3GDF Unit and laptop showing sample GUI

GAMMAGROUP

MODEL 4019-3G-HDF

HANDHELD 3G-DF

HANDHELD 3G-DF

GENERAL OVERVIEW

The 3G Handheld Direction Finder (3G-HHDF) is a lightweight, portable, state-of-the-art device for tracking and geo-locating cell phones.
The 3G-HHDF works with the 3GN's 3G Blind Call feature to allow tracking of W-CDMA devices. It is also backwards compatible with GSM.
The 3G-HHDF is controlled by a smart phone connected to the unit over a Bluetooth link. This makes the unit easy to configure and use without attracting attention.
The 3G-HHDF features multiple feedback mechanisms to cater for a variety of mission scenarios. Choose from visual, audio or vibration feedback depending on the operational needs. requirement.

KEY SPECIFICATIONS

Function:
Provides RF signal strength indication on a selectable UARFCN/ARFCN

Frequency Range (MHz)
GSM: 850 band, 900 band (inc. E-GSM), 1800 band, 1900 band
W-CDMA: 50 band, 900 band, 1700 band, 1800 band, 1900 band, 2100 band

Size (mm)
DFU: 120(l) x 65(w) x 28(d)

High band antenna:
78(l) x 78(w) x 18(d)

Low band antenna:
120(l) x 120(w) x 17(d)

Weight (grams)
DFU: 140

High band antenna:
230/460 (element/array)

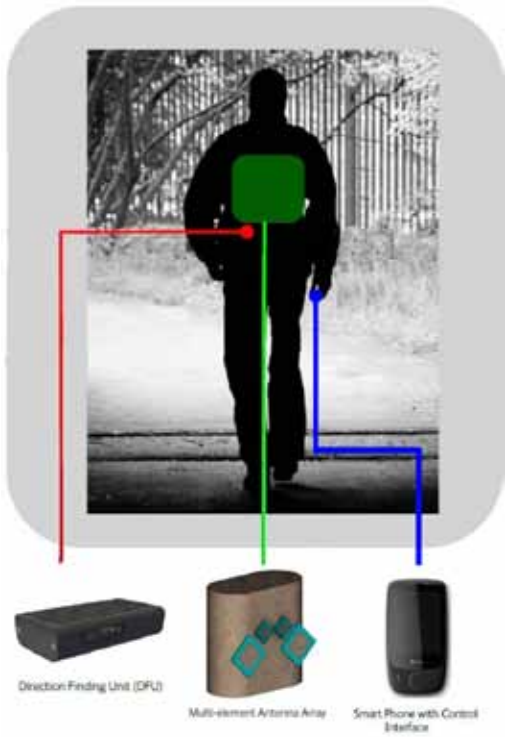
Low band antenna:
550/1100 (element/array)

Power
2 x AA batteries

Battery Life (DFU)
Circa 4 hours (typical usage)

MAIN FEATURES

- Allows direction finding of W-CDMA and GSM devices
- Resolves target location to within a few metres
- Direction Finding Unit (DFU) is controlled by smart phone over Bluetooth (wireless) or USB (wired) link
- Choice of multiple feedback mechanisms
- Can DF on BTSs and Node Bs, in addition to target mobile devices.
- Covert body-worn antenna pack included
- Compatible with multiple antennas for different scenarios
- Audio and vibration feedback modes allow for highly covert operation
- DFU protocol and frequency configuration is software adjustable to user requirements



Antenna:
4 x patch antennas in configurable array

Interfaces:
On/Off, Status LED, Smart phone interface

GAMMAGROUP

GSM VOICE & SMS INTERCEPTION

OVERVIEW	31
OPERATIONAL APPLICATION	32
TARGETED INTERCEPT	33
WIDEBAND PASSIVE INTERCEPTION	34
GSM MONITORING FULLY PASSIVE SYSTEM WITH A5.1 REALTIME DECIPHER	36
SEMI ACTIVE PASSIVE SYSTEM	38
3G OPTION	40

OVERVIEW

The cellular structure of GSM means all traffic is communicated from the Network through a Basestation to subscribers. This last step involves transmitting over the air, the weakness, and, hence, attack point for interception solutions.
To secure a Network, an Operator implements encryption on the Traffic communication. A5.1 encryption is used to encrypt the Voice and SMS communications within Europe, and for export outside of Europe, A5.2 was developed.

A5.1 DECRYPTION CHALLENGES

GSM uses the principle of a private and public key to encrypt communications where the private key is known only to the subscriber and Network. At the start of each call, the subscriber will undergo an Authentication process with the Network. Once passed, each communication session will be encrypted using a newly generated session key called the Kc.

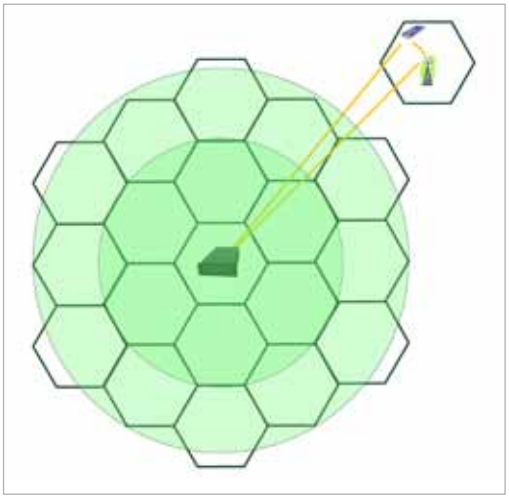
All A5.1 decryption solutions must derive the Kc to decrypt the communication session. Although attacks are openly published and well understood, the challenge is to be able to do this in real-time where real-time is defined as the time from when the call-set-up process first starts, to when the call is encrypted. This generally takes no more than 2 seconds and the call must be decoded by this point. The call will start frequency hopping, which means the signal will jump to different pre-arranged ARFCN (Absolute RF channel number) making it impossible to follow the call if the hop sequence is not known.

Outside Europe, there remains a security weakness utilizing the availability of A5.2. Solutions were able to trick Target phones into dropping to the weaker A5.2 standard to encrypt the session, making it much easier to intercept. This loophole is now closed, easily demonstrated by trying to intercept the latest mobiles which no longer are supplied with A5.2 support. The complexity of A5.1 means large amounts of processing power is required to explore all the possible solutions to derive the Kc. To further reduce the possibility of intercept, Network Operators are now strengthening their Network security. Called Randomization and already being deployed in Europe, the available data required by any solution is significantly reduced which means most solutions will be seriously impacted.

OFF-AIR CAPABILITY

There are two fundamental approaches for the interception of GSM communications:

- **PASSIVE** - completely covert, these solutions do not transmit or interfere with the real network. They monitor the cellular activity, receiving and decoding the signalization and communications over the air. This approach captures all communications and is suited for MASS Intercept, i.e. all calls within an area.
- **MAN-IN-THE-MIDDLE** - based on the ACTIVE solutions already described, these solutions transmit a fake network to take control of designated Target(s). Cloning their identity, any communication either made or received is decoded and monitored. This approach captures only Targeted communication and is suited for TARGETED Intercept, i.e. specific calls in an area.



OPERATIONAL APPLICATION

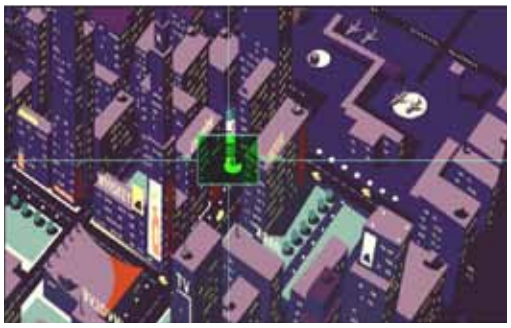
The different Operational scenarios or methods of possible deployment are: catch all communications within an area (MASS Intercept) and catch only specific communications or (TARGETED Intercept).

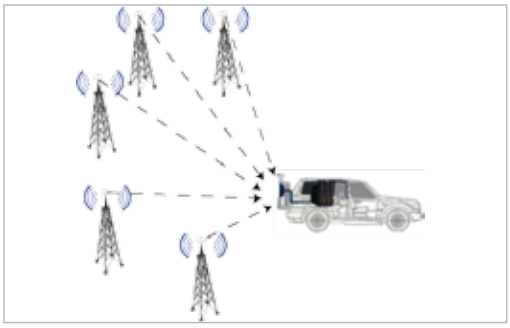
MASS INTERCEPT

These solutions are optimized to capture all communications within an area. They comprise of a Receiver Front End and a Decryptor also known as a Black Box. The Receiver captures communications off-air, the Decryptor derives the Kc to allow the communication to be deciphered. To handle large traffic volumes ultra-high speed Decryptors are required where typical decryption speeds will exceed 4 Kc/s.

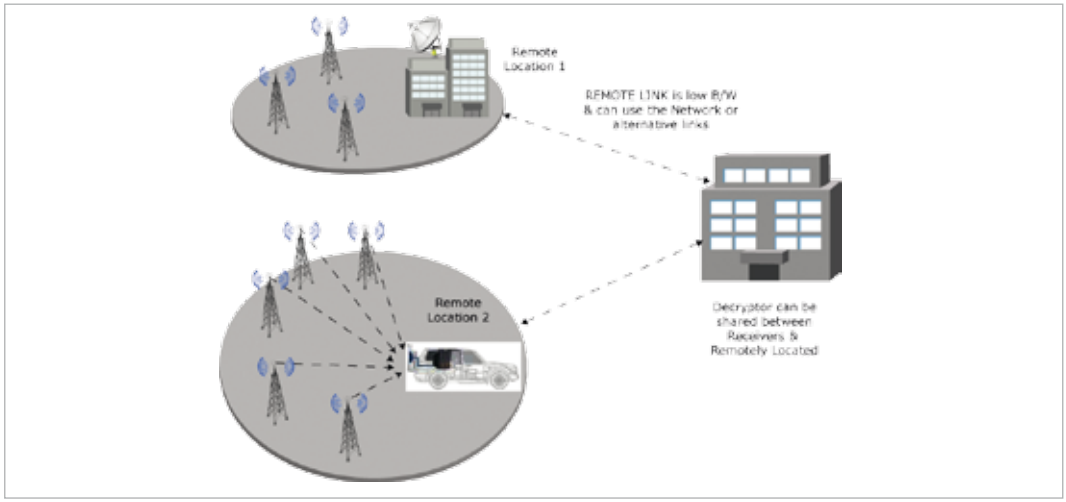
In busy or city/urban environments many cells will be used. Potentially to cover the 900 & 1800 GSM Band, the receiver will need to handle a total of 512 RF channels. This means using Wideband Receiver technology, they have the capability to cover the complete RF band and are much more effective in capturing communications.

Wideband Passive solutions are suitable for highly tactical deployment; they can be covertly used from vehicles or buildings very easily. If clients are operating under financial constraints then Narrowband Receiver, solutions which have reduced channel coverage, are potential alternatives although cell coverage will be reduced.





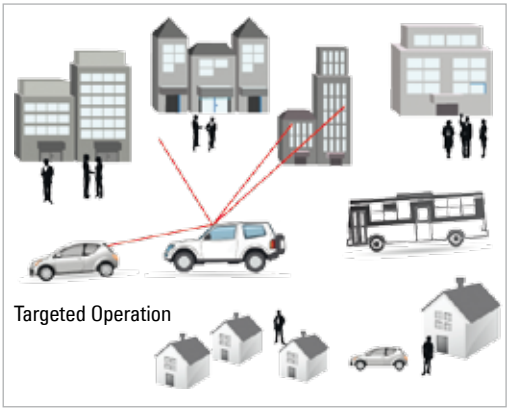
The Decryptor unit can be shared or used by multiple Receivers.This allows for cost effective deployment, for example a Decryptor could be stored in a secure area/control centre with a low bandwidth link to the Receiver(s).



TARGETED INTERCEPT

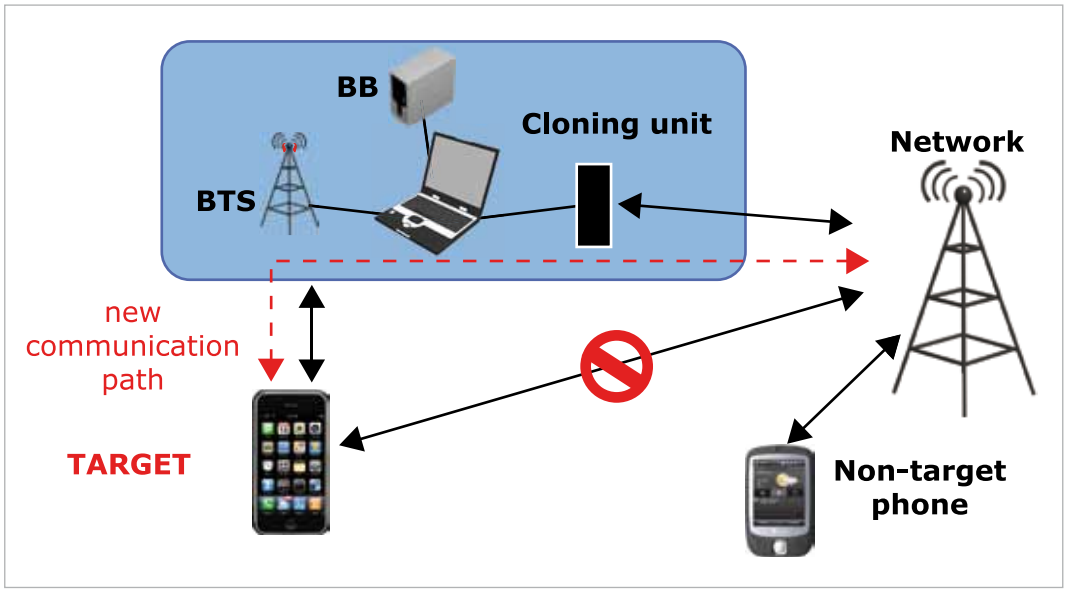
These solutions are optimized to capture communications from specific or designated Target(s). They emulate the network and transmit a FAKE cell to lock the Target(s) taking designated subscribers off the real network and simultaneously cloning the Target(s) identity.

Solutions are highly portable and can be covertly deployed from a vehicle or building.


Targeted Operation

The key elements are an ACTIVE Front End and a Decryptor unit. The method of operation is similar to ACTIVE IMSI catcher solutions where awareness of the Network and correct cell selection is paramount. Cell-phones in the vicinity will be captured, however, only designated Target(s) are locked, the rest or 'unwanted collateral' are rejected back to the real Network.

During the process of locking Target(s) to the FAKE network, the Target(s) are cloned with only the cloned copy rejoining the real Network. The net result is both the Network and Target(s) believe they are still connected to each other, unaware of the man-in-the-middle. All communication routes through the system with the calls and SMS monitored once decrypted. Complete covert interception of all incoming and outgoing communications is possible with Target(s) under the control of the system.



GAMMAGROUP

MODEL 4070 MASS INTERCEPT - WIDEBAND SOLUTION

WIDEBAND PASSIVE INTERCEPTION

Wideband Passive Interception: a passive interceptor based on a specific radio frontend that covers the whole GSM radio spectrum. It automatically decodes and analyzes the signals exchanged off-the-air on the GSM cells.The receiver is wideband, this means it can handle many more cells and simultaneous communications than narrowband receivers.

The solution uses a Wideband receiver to perform Voice and SMS decoding in real-time. To reach this performance it cannot manage the whole band simultaneously, the GSM traffic needs to be intelligently filtered first, normally using Network Operator cells as the criteria.

Compared with Narrowband solutions the key benefits are:

- MASS interception regardless the number of cells
- Real-time performance
- Target priority management
- Exhaustive interception of signalization and SMS
- Portable solution

THE SYSTEM

The product is a passive wideband intercept system and, as described above, is a Tactical solution specifically designed to intercept multiple Voice calls and SMS within an area. Typically used from a vehicle, it can be easily transported to allow use within buildings, or sensitive locations, such as Borders or busy crowded areas.

MODEL 4070 IS DESIGNED TO HANDLE 2 MAIN TYPES OF MISSION:

- Mass interception to listen and record all communications exchanged within the covered area
- Target interception to specifically intercept the communications of a highly valuable target. The target will have been previously identified by: IMSI, IMEI, phone number …

PORTABLE UNIT

The system is available in a number of form factors to give clients flexibility, which include a rack mounted 19" configuration or a suspended 1/2 19" case, which is embedded in a specific case for protection.

2U 19" Rack mount configuration

Suspended chassis configuration

GAMMAGROUP

MODEL 4070 MASS INTERCEPT - WIDEBAND SOLUTION

THE KEY FEATURES OF THE SYSTEM ARE:

- Cannot be detected by the Network Operator or Targets
- Multi-band coverage, covers the full DCS or PCS band
- Captures all GSM signalization. Note, this is interesting to detect target presence in the controlled area even with no communication
- Intercepts and records on the controlled cells, from 1 to 20 simultaneous Voice communications (uplink and downlink)
- Allows user to make free interception of voice and SMS on the monitored cells with an advanced target and priorities management.
- Full Handover management capability, means Targets can be intercepted even if they are mobile
- Intercepts all the exchanged SMS within an area, all latine and non latine characters handled
- The system can be used in two kinds of operations: Infrastructure mode or Tactical mode
- Very easy to set up, simplified GUI to scan GSM cellular environment, choose the desired cells to intercept and monitor the intercepted SMS and voice calls
- Highly portable, can be operated from AC , DC or with batteries

TECHNICAL SPECIFICATIONS

Physical	
Covered Bands	GSM900, EGSM900, DCS1800, PCS 1900 OPTIONAL: GSM850
Bandwidths	35 MHz for 900 MHz 75 MHz for 1800 MHz and 1900 MHz
GSM channels count	100 (100 uplink – 100 downlink)
Weight	27Kg
Size	59 cm x 37 cm x 44 cm
Alimentation	11 – 32 V DC 110 – 220 V AC
Power Consumption	300 W
Temperature Range	0° to 40° C
Functions	
Campaign/mission management	OK
Max No. of GSM channels processed	100 UL/DL in groups of 5
Max No. of call recorded simultaneously	20
Max No. of SMS recorded simultaneously	Unlimited.
Processing of GSM 850 and PCS 1900 band	Optional GSM/PCS down converter
Selection of base stations simultaneously and indifferently in GSM, EGSM, DCS bands	OK
Listening of "on the fly" calls	OK
Follow-upon identifiers : IMSI, IMEI,TMSI, MS-ISDN, Ki	OK
Follow-up of target with TMSI re-allocation	OK
A5/2 buffering	OK
A5/1 "ready" interface	OK
A5/2 "ready" interface	OK

GSM MONITORING FULLY PASSIVE SYSTEM WITH A5.1 REALTIME DECIPHER

Narrowband Passive Interception: A passive interceptor based on narrowband receivers, essentially small radio units. Each radio unit is dedicated to wait for a call departure on specific frequencies (specific operator – cell). When a call (or SMS) starts, one of the radios is dedicated to do the interception of this call. Narrowband interceptors are typically 4, 8, 16 or 32 channel devices where a 16 channel system following 4 cells simultaneously will have 4-channels locked on the cell's main frequency, leaving 12 free channels to be allocated on any call start (or SMS). This means the more channels which are dedicated to specific cells then the less the capability to simultaneously intercept a call or SMS.

PURPOSE

The system is intended for passive real-time GSM monitoring in the following bands:
850, EGSM/DCS, PCS.

The main idea of this system is to create a clone of the target's handset, catch its real radio traffic and discover information from the coded part of the session (coded by A5.2 or A5.1 GSM algorithm).

A5.2 decipher is represented as special software in the operator's PC.

A5.1 decipher is implemented as a separate multi-processor unit.

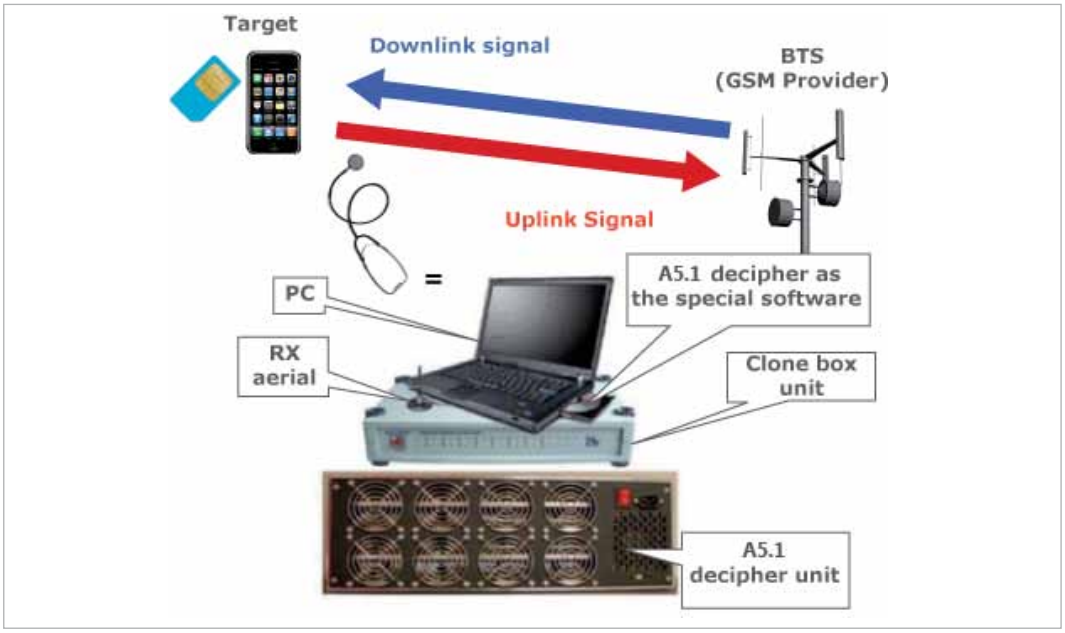
Useful for operation with all GSM providers, who encrypt OTA data by A5.2 and A5.1 ciphering.

FEATURES

- Fully passive control of forward and reverse ARFCN channels
- Real-time GSM A5.1 decryption
- The system operates secretly on long distances
- Random and selective operation modes
- The system supports Frequency Hopping and all types of voice codecs: FR, EFR, HR, AMR
- The system records voice sessions, SMS messages and call related information to HD
- 8 full duplex channels in one clone box unit. Clone box multiplexing possibility
- BRAND-NEW FEATURE: if you use our Passive system together with Active, you can get the public numbers of the wanted IMSI/IMEI
- Automatic speech recognition (voice identification) system
- LAN and USB connection
- High equipment reliability

GAMMAGROUP

MODEL 4071 MASS INTERCEPT - NARROW BAND SOLUTIONS



TECHNICAL SPECIFICATIONS:

Frequency Range	850, EGSM/DCS, PCS
Possible channel quantity configuration (forward/ reverse) in one clone box unit	1..8/1..8
Received level (RX_LEV) indication at -100 dBm	Lower Limit -104 dB Upper Limit - 96 dB
Received level(RX_LEV) indication at -45 dBm	Lower Limit - 49 dB Upper Limit - 41 dB
Channel spacing	200KHz
Modulation	GMSK at BT = 0.3
RF sensitivity	- 110 dBm
Possible operation Range	50-20000 m
Connection with PC	LAN, Internet via VPN, USB
Clone box unit power consumption	≤ 20W (configuration depended)
A5.1 deciphering unit power consumption	1000W
Clone box unit dimensions	330x268x54 mm
A5.1 deciphering unit dimensions	500x310x180 mm
Average deciphering time	0.75 sec, 3sec, 150sec
Power supply - Clone box unit - Personal computer - A5.1 Deciphering unit	 - AC 110-230 / 24V - AC 110-230 / 12-16V - AC 110-230 V

GAMMAGROUP

MODEL 4072

TARGETED INTERCEPT – SEMI ACTIVE PASSIVE SYSTEM

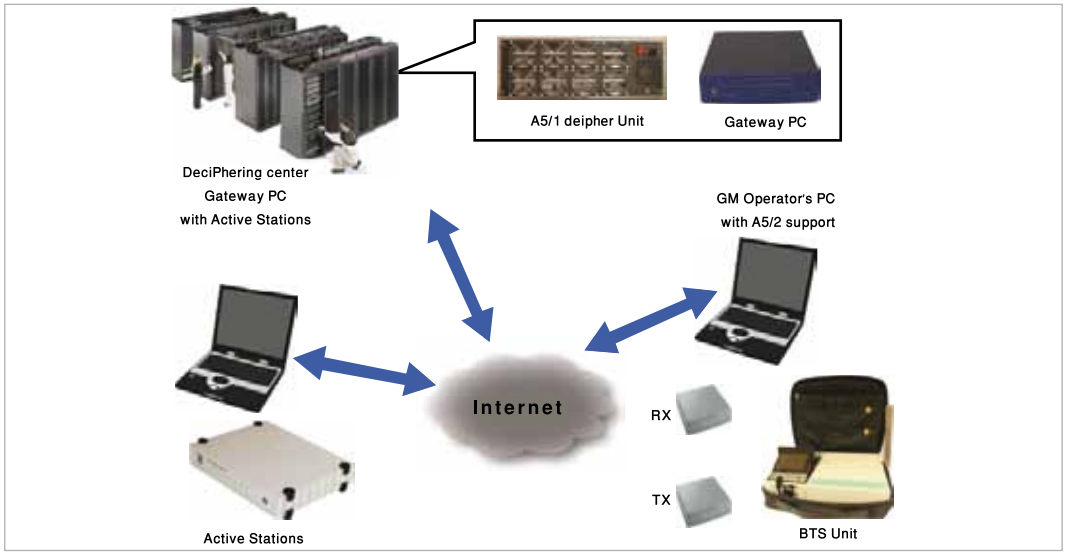
SEMI-ACTIVE PASSIVE SYSTEM

The system is intended for active real-time GSM monitoring in the following bands: 850, GSM/DCS, PCS.

The main idea of this system is to create a fake BTS with the best operation parameters for mobile phones in the working area. Each of them will register in this fake BTS. From this moment on all GSM connections can be monitored by the system. An Active Station unit is intended to provide communication for the fake BTS with the real network. An A5.1 decipher unit is intended for KC evaluation in order to discover the coded part of the air session, closed by A5.1 algorithm. The fake BTS and AS unit may be separated distantly and connected via Internet.

FEATURES

- The system operates secretly in Real-Time with all types of ciphering (A5.1, A5.2, A5.0) in GSM networks
- Detects GSM handsets located within area controlled by the system
- Manipulates state of handsets registered by the system
- Records voice sessions, SMS messages and call related information to HDD
- Calls and SMS censoring with emulation network activity
- Automatic Public Numbers (PN) detection for registered handsets
- Automatic speech recognition (voice identification) system
- The system is able to monitor GPRS traffic
- LAN (ETHERNET) connection
- High equipment reliability



GAMMAGROUP

MODEL 4072

TARGETED INTERCEPT – SEMI-ACTIVE PASSIVE SYSTEM

TECHNICAL SPECIFICATIONS

Frequency Range	850, 900, 1800, 1900 MHz (each BTS is separately packaged)
Output power	0.1 – 4 Watts for case variant
Operation Range	
– from BTS unit to mobile phone	– 50 - 800 m
– from mobile phone to AS	– VPN connection depended
Channel spacing	200KHz
Modulation	GMSK at BT = 0.3
RF sensitivity	- 110 dBm
Quantity of registered targets	Unlimited (recommended 50)
Quantity of parallel encrypted conversations	1-6 for 1 Active Stations unit
Connection with PC and other units	LAN, Internet via VPN
Incoming calls, SMS, etc.	Yes
External battery	capability to autonomous operation up to 10 hours
Dimensions:	
– BTS metal	– 330x268x80 mm
– BTS plastic portable	– 290x260x75 mm
– AS metal	– 330x268x54 mm
Operating Temperature Range	+0° C to +55°
Power supply	
– Active Stations unit	– AC 110-230 / 24V
– Case variant BTS unit	– AC 110-230 / 12-16V
– Personal Computer	– AC 110-230 / 12-16V

GAMMAGROUP

MODEL 4072 3G

TARGETED INTERCEPT 3G OPTION

3G OPTION

To handle 3G networks there is a 3G option add-on system which can be integrated with the GSM system. This device will emulate a 3G network to attract 3G mobiles and, for designated Targets, selectively push them to GSM where they remain unless they are rebooted or pushed back to 3G by the GSM system.

Non-target phones are not affected and remain in 3G-mode.

The key features of this option are:

- Automatically scans and detects parameters of all 3G networks
- Detects all 3G phones and collects all their identities (IMSI, IMEI and TMSI)
- Displays phone model, country of origin and name of network provider
- Measures distance to all 3G phones with accuracy of less than 30 m
- Selectively forces only designated Target(s) to GSM
- Selectively blocks communication of 3G target's phones
- 2100 MHZ capability only

TECHNICAL SPECIFICATIONS

Frequency Range	UMTS band1
	1920-1980MHz
	2110-2170 MHz
Power supply - 3G Base Unit - Personal computer	 - 24V - 12-16V
External battery	capability of autonomous operation up to 10 hours
Output power	0.1 - 5 Watts
Connection via LAN or WLAN	Yes
Operation Range	50 - 1500 m
Portable 3G Unit Dimensions	290 x 260 x 75 mm

GAMMAGROUP

A5.1 DECRYPTORS

INTRODUCTION	43
PASSIVE A5.1 DECRYPTOR	44
ACTIVE A5.1 DECRYPTOR	45

Decryptors are subject to export control and require an export license.

BACKGROUND OVERVIEW

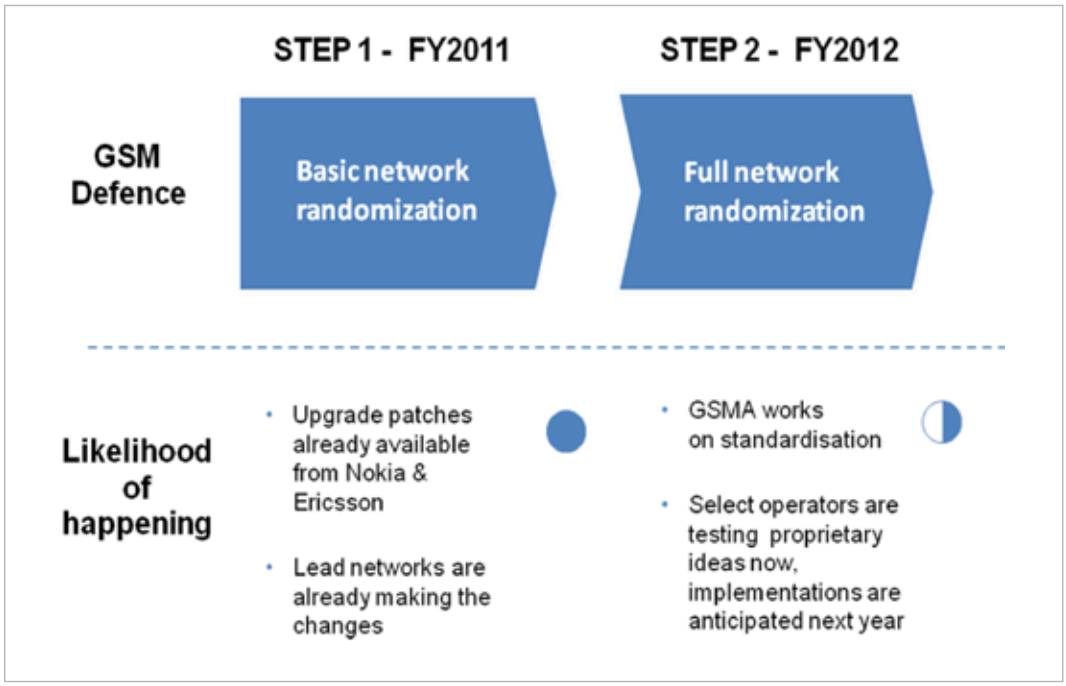
The cellular structure of GSM means all traffic is communicated from the Network through a Basestation to Subscribers. This last step involves transmitting over the air, the weakness and, hence, attack point for interception solutions.

To secure Networks, the Operator implements A5.1 encryption on the Traffic and encrypts each communication session using a newly generated session key called the Kc. The ability to derive the Kc in real-time A5.1 is critical to decode each session, i.e. each Voice and SMS communication.

The most commonly used method by decryptor is based on the 'Brute Force Attack' where:

- method is over 10 years old and a non-intelligent approach to derive Kc
- attack relies on receiving specific signaling messages (Plaintext)
- messages used are taken only from the Downlink
- statistical approach means there is no absolute time it takes to derive Kc
- signal strength or signal errors have a dramatic effect on system performance
- any variation in network implementation means it is not possible to get Kc
- requires lots of processing power making solutions large & power hungry

Although the weaknesses within GSM networks are well known it is only now Network Operators are implementing the required security upgrades. The biggest change will be when Randomization, a software upgrade, which reduces the available predictable plaintext, is introduced at end 2011/early 2012. Any changes in the Plaintext will have a catastrophic effect on the current generation of PASSIVE Decryptors.



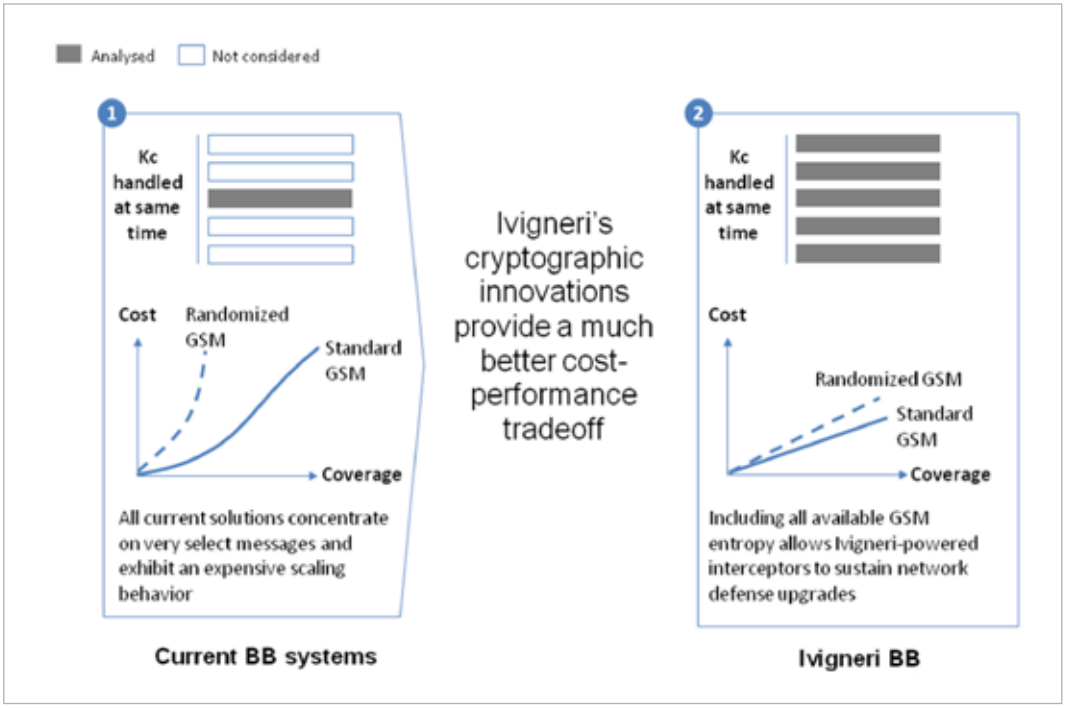
Decryptors are subject to export control and require an export license.

INTRODUCTION

The forthcoming introduction of Randomization as part of a suite of security upgrades by Network Operators in 2011 & 2012 will cause a major performance impact for the current generation decrypt systems and, therefore, off-air passive solutions.

The only hope for Law Enforcement and Government Agencies is the emergence of next generation BB technology from Ivigneri, designed to handle these changes:

- state-of-the-art capability takes a new highly intelligent predictive approach
- implements clever Cryptographic shortcuts which do not rely on receiving specific messages or plaintext
- uses both the U/L and D/L
- we use the whole signalization stream which significantly improves the real world performance especially when signals are of mixed quality
- intelligent approach reduces the need for high power processing
- our solutions derive multiple Kc simultaneously
- solutions are extremely power efficient



Decryptors are subject to export control and require an export license.

GAMMAGROUP

MODEL
IVG 500

NEXT GENERATION A5.1 DECRYPTORS

PASSIVE A5.1 DECRYPTOR

The IVIG-MASS is a state-of-the-art high-performance A5/1 decryption system. Using the latest deep analysis decryption techniques the IVIG-MASS is designed to recover Kc even on networks where Randomization is implemented or where signal quality is poor.
Optimized for integration with PASSIVE GSM interception equipment, IVIG-MASS provides government agencies with real-time A5/1 covert future proofed monitoring capability.

FEATURES

- Real-time deciphering of GSM A5/1 traffic
- Supports all GSM networks that encrypt voice calls and text message
- Deep analysis mode can calculate Kc where Networks have implemented Randomization
- High throughput mode optimized for low to medium noise data and no Randomization
- Optional A5/2 and Thuraya decryption capability
- Modular solution allows system to be easily increased in performance
- Can be remotely operated

SPECIFICATIONS

Cryptographic	
Performance	High Throughput mode: 6Kc/s @ 95% success
	Deep Analysis Mode: 2Kc/s @ 99% success
A5/1	Standard
A5/2	Optional
Thuraya	Optional
Physical	
Weight	17 Kg
Size	3 HE Server
Data interface	TCP over Ethernet or SSG tunnel
Power consumption	peak 350 W
Environmental	
Operating Temperature Range	5 - 30°C
Humidity	< 70%
Shock Proof	No

Decryptors are subject to export control and require an export license.

GAMMAGROUP

MODEL
IVG 501

NEXT GENERATION A5.1 DECRYPTORS

ACTIVE A5.1 DECRYPTOR

The IVIG-TACT is a state-of-the-art ultra-portable high performance A5/1 decryption system. Using the latest decryption techniques the IVIG-TACT has been optimized for integration with ACTIVE GSM interception equipment to provide Government Agencies with real-time A5/1 covert monitoring capability.

FEATURES

- Real-time deciphering of GSM A5/1 traffic
- Supports all GSM networks that encrypt voice calls and text messages
- Optional A5/2 decryption capability
- Runs from a laptop
- Lightweight – less than 4Kg
- Low Power Consumption
- Can be remotely operated

SPECIFICATIONS

Cryptographic	
Speed	Real-Time (1 Kc / 2s)
Success Rate	99%
A5/1	Standard
A5/2	Optional
Physical	
Weight	3.5 kg (incl. analysis laptop)
Size	Standard Laptop
Data interface	TCP or Bluetooth
Power consumption	60 W (2h battery backup included)
Environmental	
Operating Temperature Range	0 - 35°C
Humidity	< 90%
Shock Proof	Yes

Decryptors are subject to export control and require an export license.

GAMMAGROUP

ADVANCED MOBILE LOCATION TRACKING

ADVANCED LOCATIONTRACKING AND MOBILE
INFORMATION & DECEPTION SYSTEM 47

ADVANCED LOCATION TRACKING AND MOBILE INFORMATION & DECEPTION SYSTEM (ALTAMIDES)



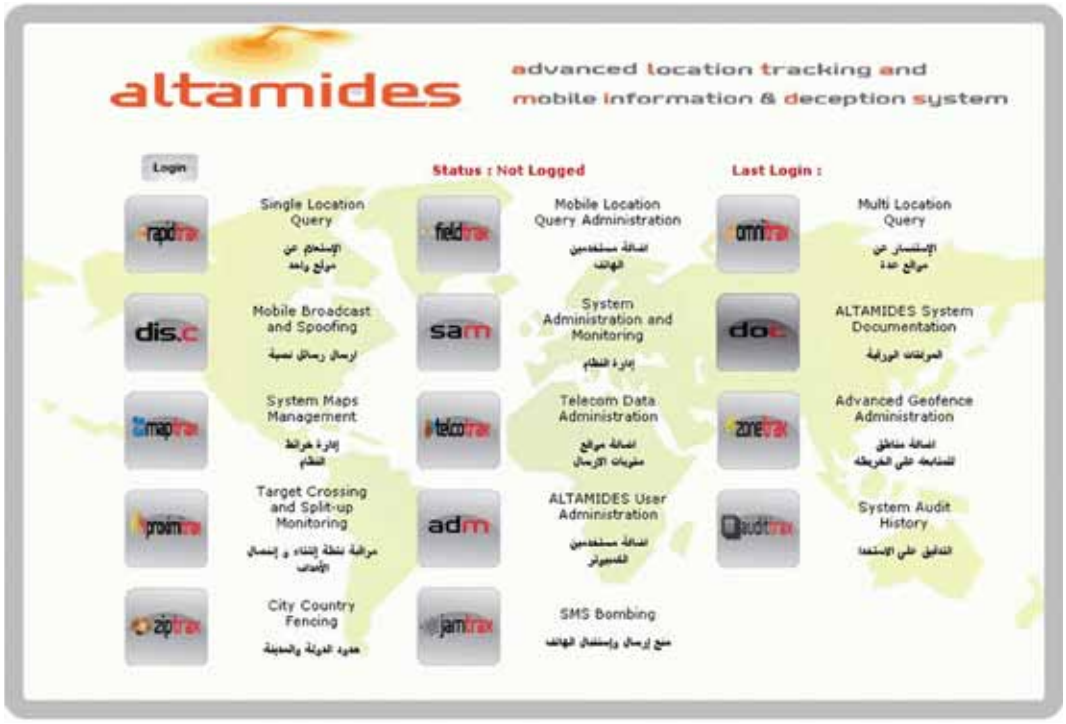

TECHNICAL DESCRIPTION

Scope of the ALTAMIDES

The purpose of this platform is to provide the CLIENT with a facility to locate and report the vicinity location of a GSM device (i.e. mobile phone).

The ALTAMIDES facility enables suitably authorized users to designate "targets," to make queries as to the location, and have the results reported both in text and overlaid on a digital map or photograph.
The following sections summarize, in short, the functionality and capabilities of the standard ALTAMIDES platform.

OVERVIEW OF ALTAMIDES (STANDARD CONFIGURATION)



The platform can be defined as having two distinct primary sub-systems, being:

Location Unit

This component comprises the platform's hardware and supporting software that enables the interface to the Signaling System No. 7 (SS7).

Location Suite

This component comprises the application software and the management tools with multi-language support.
The scope and capabilities of the standard platform are summarized briefly as follows:

A) Location Unit (LU):

- The basic Location Unit includes:
  - Up to 4 x SS7 Signaling links (Time Slots) per unit
  - Up to 20 location queries per second
  - 10/100 Ethernet connectivity
  - Software Interface to Location Suite
  - API Interface for 3rd party applications
  - SS7 interface for location requests and location information provisioning over SS7
  - White-list authorization feature for location queries
  - Basic location request and location status logging
  - Provisioning of raw location data (such as IMSI, MSC, LAC, Cell-ID, Subscriber Status, Location Age)
  - Integrated basic database functionality for information, such as Longitude/Latitude, MSC-/Cell-Name etc

B) Location Suite (LS):

The ALTAMIDES Suite provides a role-based Single Sign-on mechanism, a method of access control that allows users to login once, and gain access to multiple resources of software modules within the full range ALTAMIDES suite, dependent on the access rights (role) assigned by the respective ALTAMIDES Administrator, without the need to enter multiple passwords, therefore, reducing the user administration effort and reducing password fatigue.
Furthermore, the Location Suite is multi-language enabled. CLIENT can implement a default language and each user of the system has the capability to configure their preferred language, if other languages are configured in the system.

RapidTrax

Location front-end Web-interface:

- Graphical and textual display of current location for a single target
- Single point graphical and textual display of historical location information for single target
- Report display/download for historical location information
- Single Target Location Administration for
  - Location Scheduling
  - Target Administration
- Multipoint location area prediction for single target
- White/Black/Red listing of mobile phone numbers
- GSM configuration only
- Worldwide reverse fixed-line phone number lookup capability
- National fixed-line reverse lookup and graphical display capability
- SMS-based location result forwarding to mobile devices

Location back-end Engine:
- Location Scheduling Engine for single targets
- Location Routing Engine
- Location Result Processing Engine
- Location GSM interface
- ALTAMIDES iSMSC Network Failover and Load Balancing (optional)

OmniTrax

Location front-end Web-interface:
- Graphical and textual display of current location for multiple targets
- Graphical and textual display of historical location information of multiple targets
- Multiple-target movement visualization
- Report display/download of historical location information
- GIS Navigation Interface Engine
- Target Location Administration for:
- Location Scheduling
  - Target – User visibility
  - Target Administration
- White/Black/Red listing of mobile phone numbers
- Supports GSM and GPS Tracking

Location back-end Engine:
- Location Scheduling Engine for multiple targets
- Location Routing Engine
- Location Result Processing Engine
- Location GSM and GPS interface
- ALTAMIDES iSMSC Network Failover and Load Balancing (optional)

ZoneTrax (requires OmniTrax)

- GSM and GPS GeoFencing Administration Tool
- Intelligent GSM GeoFencing across Cellular Networks
- GSM GeoFencing Autoupdate (in case of cell data changes)
- Cell Shape and Cell Direction Display
- Multiple target movement visualization
- Customizable GSM Geofencing with Cell Select and Deselect option
- Display Pop-up, SMS and/or Email Alert capability
- White/Black/Red listing of mobile phone numbers

ZipTrax (requires OmniTrax)

- GSM District/City/Country Fencing Administration Tool
- District/City/Country Fencing Autoupdate (in case of cell data changes)
- Multiple target movement visualization
- Orthogonal target functionality with ZoneTrax
- Display Pop-up, SMS and/or Email Alert capability
- White/Black/Red listing of mobile phone numbers

ProximiTrax (requires MapTrax)

- Targets and Alarm Setup forTarget Monitoring (coming together and/or going apart)
- Supports GSM and GPS targets
- GSMTarget Monitoring based on Cell or MSC IDs
- Multiple target movement visualization
- Orthogonal target functionality with ZoneTrax
- Display Pop-up, SMS and/or Email Alert capability
- White/Black/Red listing of mobile phone numbers

FieldTrax (requires RapidTrax)

- SMS MO Engine for Location Requests from the field (i.e. location tracking via mobile phone)
- White/Black/Red listing of mobile phone numbers
- Mapping of Cell ID to textual location
- Google Maps/Microsoft Bing Maps hyperlink target location display transmission to mobile devices
- Field Location History Function
- FieldTrax Administration Module with tracking history database

DIS-C

- SMS Broadcasting and Spoofing Interface:
- SMS Broadcasting Interface
- Spoofing capability (e.g. to impersonate someone via SMS)
- Broadcast Scheduler
- Destination MSISDN Database
- Destination MSISDN Dataset Import Feature
- SMS Delivery Status Reporting
- SMS Receiving Feature
- SMS Reply Reporting

SMS Broadcasting and Spoofing Engine:

- SMS Scheduling Engine
- SMS Routing Engine
- SMS Delivery Status and Reply Engine

JamTrax

Denial of Service Attack on target mobile device in order to disable most or all mobile device radio functions with:

- Scheduling Engine
- Jamming History Function
- White/Black/Red listing of mobile phone numbers

MapTrax

Map Administration and Map Database:

- Map Administration/ImportTool
- Map Database

ADVANCED MOBILE LOCATION TRACKING

TelcoTrax

- Cell/MSC/fixed-line PSTN Database with Graphical Administration:
- Front-end Cell Database Administration Tool to create, edit and upload Cell and MSC Database
- Audit Trail Function for recording, archiving and Cell Data recovery
- Cell Database Time Stamp and Version Capture
- World-wide fixed-line PSTN Database
- Fixed-line PSTN Import Tool

AuditTrax

- Real-Time Recording and Display of all system transactions and activities
- Historical Transaction Records retrievable based on multiple search criteria
- Historical Transaction Record Download in PDF, Excel and CSV format
- Capability to be used as monitoring and control tool for ombudsman-like entities

Target Management System

- Real-Time Relational Database System supporting many millions of target data entries
- Bulk Upload, Management and Analysis of target data sets
- Target Data accessible/importable from various ALTAMIDES modules
- Target Data Report and Download Functionality
- SQL Interface for 3rd party relational and data mining tools

System Administration and Monitoring

- Graphical System and Application Monitoring and Administration Interface
- Multiple Source Logging and Database Storing of system information and commands (e.g. for audit trails)
- System configuration, monitoring and maintenance capability
- Backup and Archiving capability (optional)

Network Features:

- Technical setup for SS7 and iSMSC access. (SS7 links and IP connectivity as defined in "Connectivity with local GSM Service Provider" below)
- Supports connections to multiple iSMSCs with different SS7 connectivity for failover and improved international coverage and roaming target tracking purposes
- Browser-based application for easy control of security and access of remote users (e.g. via HTTPS and VPNs)

Support Services

- Technical Support
- Email and Instant Messenger-based User Help
- 24-hours Operations Hotline Support
- Remote System Maintenance and System Support (on Client request)

Upcoming New Release Features (during 2011):

- Number Range Management for TelcoTrax
- Cell Density Visualization
- FieldTrax Mobile Administration Extension
- Real-time SubCell Tracking
- Mobile Cell Collector
- GIS Interface




GAMMAGROUP

GAMMA GROUP

info@gammagroup.com
www.gammagroup.com