GSMK Overwatch

GSMK Overwatch

GSMK Overwatch enables network operators and authorities to eliminate illegal use of IMSI catchers, network jamming actitivities and GNSS jamming and spoofing atacks, nationwide, 24/7/365

Regain Sovereignty over your Airspace.

Deployment of hostile base stations has become a common threat as costs and procurement hurdles have been continuously falling.

The GSMK Overwatch network security system is the world's first system capable of distributed detection, localization, alarming and neutralization of active attacks on mobile communications via the air interface.

Leveraging GSMK's patented Baseband Firewall technology, powerful stationary sensors can be combined with mobile sensors to permit comprehensive and cost-efficient detection of rogue base stations, including fake cell towers known as "IMSI catchers", as well as individual attacks carried out over the air interface.

The system integrates and synthesizes data from both types of sensors in a national situation report for cellular communications, allowing network operators, government agencies and information critical industries for the first time to detect and combat rogue base stations used for eavesdropping and fraudulent activities in real time.

Without dedicated detection and protection, the existing cellular infrastructure can no longer b trusted:

- **IMSI Catchers**
  IMSI catchers are being widely used by state and non-state actors as size, cost and procurement hurdles are continuously falling.
- **Hostile Takeover of Baseband Processors**
  The air interface(s) of present-day smartphones, tablet computers and M2M devices can be exploited for grave attacks. Baseband processors are highly vulnerable and often not under contr even of manufacturers.
  Depending on the device architecture the baseband controller can be memory master and springboard attacks on the application processor are possible and actively used. Further,

baseband processors often control the audio path directly (room bugs) or would allow DoS attack (phone not reachable).

- **Cellular Jamming**
  Jamming of mobile frequencies (DoS) is either used to disable mobile connectivity or selectively forcing airband communication down to the less secure 2G network.
- **GNSS Jamming and Spoofing**
  Jamming and spoofing is used to manipulate or disable global satellite based navigation systems to compromise location based services (Aviation, tracking, precison timing).

System Key Features

- Comprehensive air interface data analysis and geo referencing (2G, 3G, 4G)
- Scalable system architecture
- Modular system architecture (fixed and mobile)
- Centralized management and data storage
- Graphical GUI - intuitive system handling
- Patented technology
- Unconspicious and ruggedized hardware
- Carrier grade SLA, CARE, incidents
- Compatible with operator redundancy requirements
- Seamless integration into other GSMK Network Security solutions (e.g. GSMK Oversight® SS7/Diameter detection and protection system)

Risk Assessment

Hostile network scenarios have so far rarely been considered in risk modelling although they are an essentia backbone for mission critical audio communications
as well as for messaging and a growing number of M2M applications deployed in critical infrastructures.

The Solution

As a renowned industry leader in the field of secure communication systems and network security, GSMK developed the GSMK Overwatch system allowing the
generation of a continuously updated national situation report by means of distributed detection and localization of rogue base stations, cellular jamming activities and GPS jamming and spoofing attacks.

System Design

The Overwatch mobile network security system, building on a modular and scalable approach, consists of th Overwatch Manager, which constitutes the centralized backend providing data processing, data visualizatior data storage and the map server for geo referencing as well as Overwatch Sensors for encrypted data collection. A high-performance industrial appliance allows easy integration in MNO infrastructure and existing maintenance agreements.

Overwatch Sensors

Two types of sensors are available for modular state and nationwide deployments:
The latest generation Overwatch Sensor (2G, 3G, 4G) is based on a dedicated heavy-duty radio hardware, waterproof (IP67), ruggedized enclosure for out- and
indoor installations and continuous surveillance tasks.

Its design perfectly meets the requirements for fixed (rooftop, attic) installations even under harsh environmental conditions.

Mobile sensor arrays (GSMK Overwatch Tactical Sensor, Generation 2) for mobile on-demand monitoring of temporary hotspots in- or outdoor. The mobile sensors allow monitoring of 3 carriers in parallel and send measurements via 3G, LTE or LAN to the Overwatch backend.

Remote SIM
All GSMK Overwatch sensors work together with the GSMK Remote SIM Appliance that enables up to 1152 SIM cards per system to be remotely and dynamically allocated to individual measurement tasks.
Both sensor types are protected against over the air attacks, using GSMK's cutting edge technology.
Real-time reports are protected by strong encryption on their way from the sensors to the central analysis unit.

Analysis and Visualization
As the sensors continuously provide raw data from the network down to a very low layer (up to 150 criteria), the system heuristics allow a comprehensive view on the air interface's consistency over time and with full geo referencing.

The browser-based visualization interface translates the findings into different levels of detail: general netwo status and warnings, suspicious trends/events/correlations up to real-time cell data and historic data for further variance analysis, as well as threat level based alarming (Email, SNMP or custom interfaces).

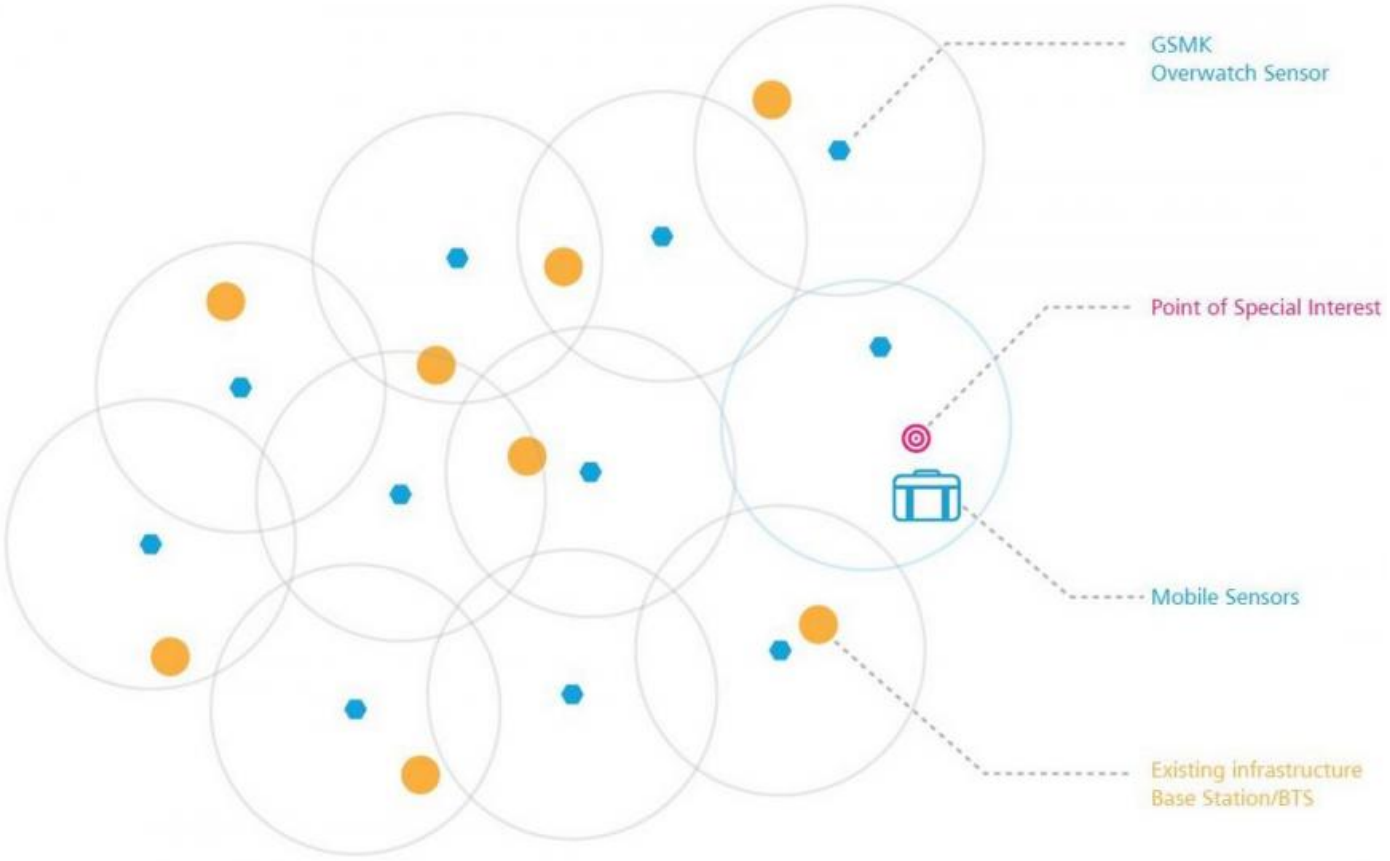
Report Generation and Localization
In order to generate offical documents, the system allows an adaptable report generation including localization of threatening devices for further government action and initiation of other countermeasures.

Deployment
GSMK supports its customers before, during and after deployment with an advanced requirement analysis, full deployment support, training, system swing-in calibration and tailor-made SLAs.

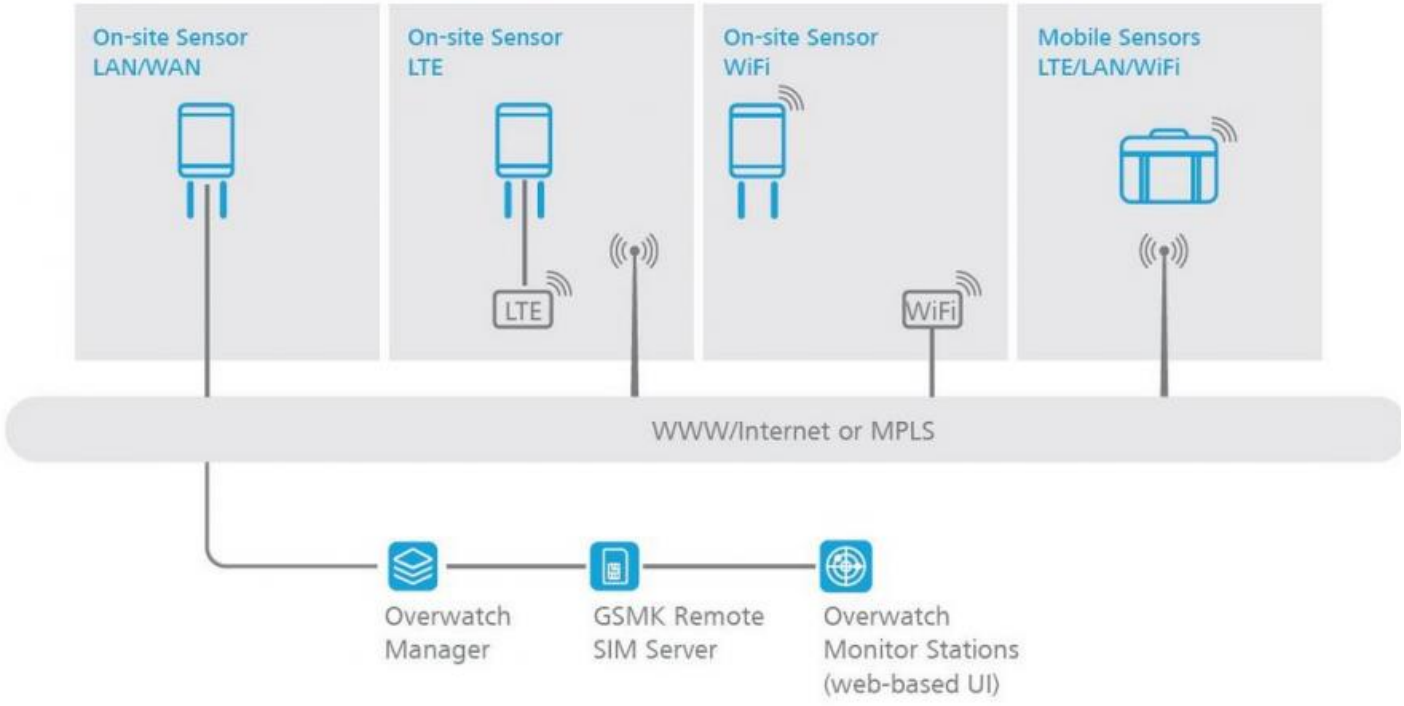
Lab Version
Lab versions are available for testing and maintenance purposes.

System Architecture

The Overwatch "cellular network security system"



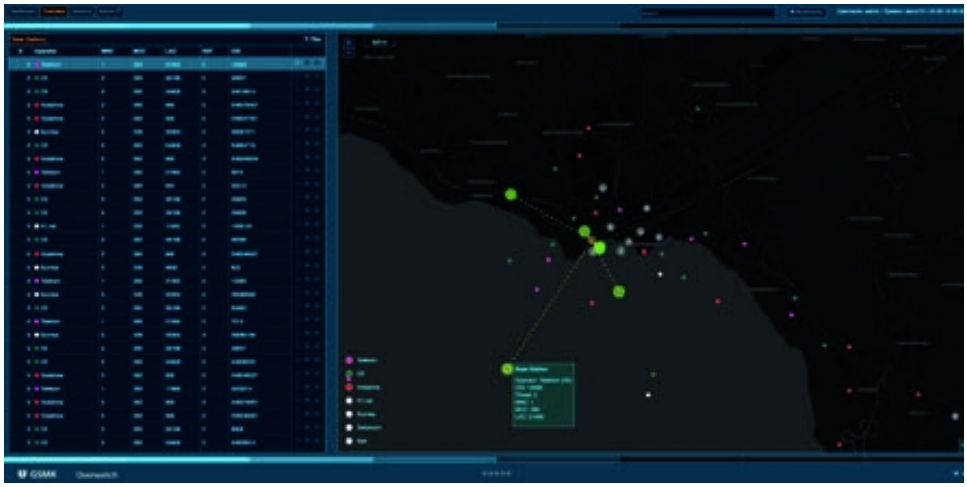
Flexible integration into existing infrastructure
Ethernet, LTE, WiFi



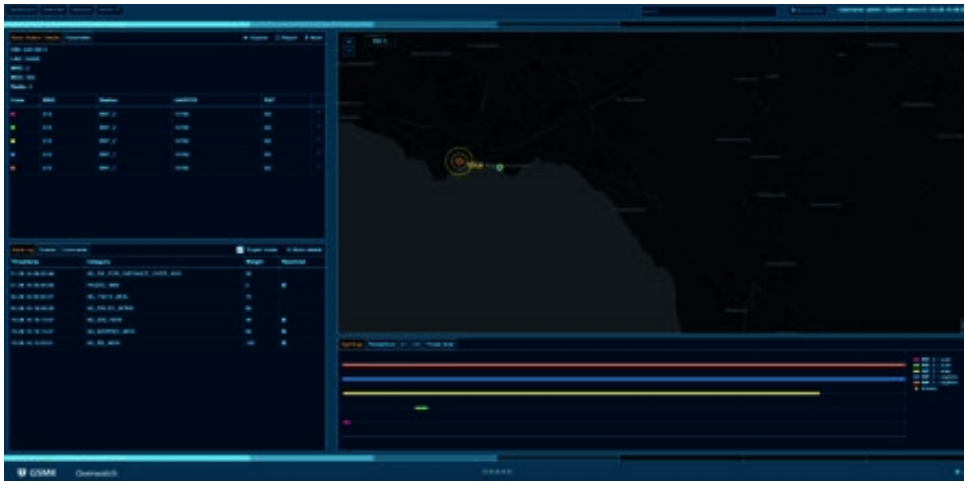
Overwatch Manager User Interface

Information Visualization and System Management

Overwatch Manager
Full geographic referencing of live data.



Overwatch Manager
Continuous measurement of cellular parameters and flexible threat level configuration



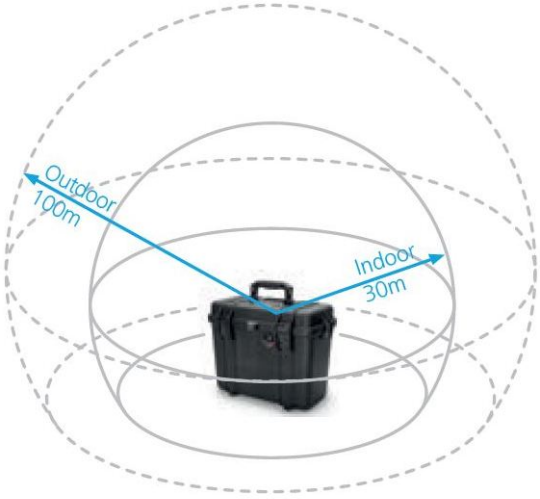
Overwatch Manager
Detailed and self-learning alerting with flexible interfaces to existing NOC applications

Overwatch Hardware

Sensors and Management Platform

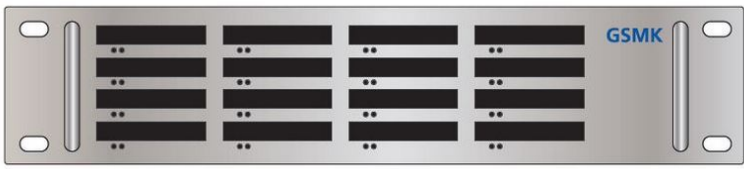
Overwatch Stationary Sensor
Military-grade waterproof sensor platform for comprehensive and continuous detection in fixed or mobile installations.

Overwatch Mobile Sensor
Military-grade tactical sensor system for on-demand monitoring of temporary hotspots.
Plug-and-play deployment for continuous monitoring of 3 MNOs.
Built-in high-precision GPS and LTE modem for encrypted data transmission to the Overwatch backend.



Overwatch Manager
Backend system
High-grade applicance, HP ProLiant, Gen10

Overwatch Remote SIM Server
Flexible SIM to device allocation with the scalable GSMK Remote SIM system
The carrier-grade rack mountable server allows up to 1152 SIM cards to be remotely allocated to sensor systems deployed in the field.



GSMK Overwatch - 360° Mobile Network Protection