GSM INTERCEPTION

Cellular Network Monitoring System
GSM INTERCEPTION

Destination: is applied for searching, intercepting and signal recording of cellular networks with the purpose of control of talks, SMS and localization of subscribers.

The complex is soft-hardware and consists of:

The hardware:

- The unit of signals’ receiving and processing - up to 8 units on 1 control computer (up to 128 channels).
- Antenna-feeder system.
- The control computer (Notebook).
The software:

• The control program for units of signals’ receiving and processing.
• Applications for processing archives.
• Decoder A5/2 - as an integration option of the control computer.

Technical capabilities:

• Interception and decoding of signals from base stations and mobile telephones GSM frequency band 850/900/1800/1900 MHz in real time.
• The cellular networks' control with hopping application.
• An automatic recording of negotiations and the protocol on a disc or the external carrier.
• Voice codecs FR, EFR, HR.
• SMS the decoder for national alphabets and UNICODE.
• Archives, such as «sound + events» with partitioning on dates and on subscribers.
• The channels restoration system for reduction of probability of the purpose’s skip at the intensive traffic.
• The "pilot" call for detection of the subscriber and his numbers.
• Developed system of events filters of the cellular network.
• Interactive general and channel events protocols with system of filters.
System Components:

• Hardware
• Antennas and feeders set
• Connecting Cable to Be Connected to the PC’s USB-port
• Power Cable
• Car Lighter Connecting Cable
• CD, Containing Software
• CD, Containing Operating Instruction
• Test Mobile Phone with the Open Engineering Program
• “Boomerang” Device for IMSI and TMSI Determination
• IKG Head phones
• Portable Computer
Basic Program of the System
Working Area of the Basic Program is divided into four main parts:

• Top left-hand third is a window of receivers’ current status (Receivers Window);

• Middle left-hand third is a window of voice data recording channels current status (Recorder Window);

• Bottom left-hand third is a window of intercepted numbers list, their selection parameters and their current status (Target List Window);

• Right-hand half is a protocol window that is registering events in received channels (Protocol Window).
Protocol Windows

[Protocol window with text details]

1. Release channel: conditional IE error
2. Paging response DMG=73074002 CL100=301803 11:39:56 21.01.03
3. Authentication request
4. Paging response DMG=73074002 CL100=301803 11:39:57 21.01.03
5. Call Identity: ID=1754, LAC=009
6. Cell Identity: ID=2345, LAC=009
7. Authentication request
8. Start ciphering: no ciphering
9. MSI Allocation: TMSI=01070003
10. Cell Identity: ID=2345, LAC=009
11. Authentication request
12. Compress acknowledge
13. Start ciphering: no ciphering
14. Paging response DMG=23401073903673 CL100=333901 11:40:03 21.01.03
15. Call Identity: ID=2345, LAC=009
16. Allocation: TMSI=01070003
17. Call from 8-902-6345203
18. Assignment into 19/3
19. Call Identity: ID=2340, LAC=009
20. Call establishment TMSI=09074006 CL100=301800 11:40:12 21.01.03
21. Authentication request
22. Start ciphering: no ciphering
23. Compress acknowledge
24. Disconnect Normal call clearing
25. Release complete Normal call clearing
26. Release channel: normal release
27. Call establishment TMSI=73074002 CL100=331801 11:40:26 21.01.03
28. Authentication request
29. Call Identity: ID=2340, LAC=009
30. Start ciphering: no ciphering
Purpose of Protocol Windows

Protocol Windows register all the System’s activity. All the messages, concerning cellular system intercepted events, receivers’ re-assignment, receiver’s assignment to new radio channels, recording channels turning on and off and so on are displayed on the control PC screen. The above is done to provide for System’s operator quick feedback as well as for saving operation protocol in a file for subsequent analysis of the working session.

Protocol Window has several tabs. The one on the left (GENERAL) is a General Protocol Window. It displays the data coming from all of the receivers. Protocol Window is meant for displaying some groups of events both on the screen and in the protocol file as well as for ensuring quick access to the events processing commands.
ARCHIVE OF RECORDS Program

Used for listening to and sorting speech files, stored by the Basic Program.
Purpose of Sound Processing Window:
Sound Processing Window is meant for solving software tasks of voice data recording and processing. Per se, Sound Processing Window is a software supported multichannel sound recorder.

The window supports standard functions of beginning and completion of sound recording, pausing as well as concurrent recording of all available voice channels and listening to one of the channels in real time. Each voice channel is connected to sound receiving unit.
Base Station Parameters Edit Dialog. Base Stations Description Dialog is meant for either entering or editing data, reflecting Base Stations parameters.
SMS Interception.

Text messages (SMS) when intercepted are stored as a text in a protocol file.
For activity of the decoder A5/2 no preliminary identification information (for example, key Ki) is required. All necessary data for decoder’s activity are intercepted during communication session. It allows to hold interception of communication sessions with cryptographic protection A5/2 in real time mode. The probability of successful deciphering of a session depends on quality of the intercepted signal. On reliably received channels it reaches 100 %.
The technical data on receiving channel refers to the receiver input.

<table>
<thead>
<tr>
<th>Parameter’s name</th>
<th>GSM-900</th>
<th>DCS - 1800</th>
<th>PCS-1900</th>
<th>GSM-850</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward Channel Received Frequencies Band, MHz</td>
<td>935-960 MHz</td>
<td>1805-18 80</td>
<td>1930-1990</td>
<td>824-849</td>
</tr>
<tr>
<td>Reverse Channel Received Frequencies Band and Transmission in Active Mode, MHz</td>
<td>890-915 MHz</td>
<td>1710-17 85</td>
<td>1850-1910</td>
<td>869-894</td>
</tr>
<tr>
<td>Frequency Channel Spacing</td>
<td>200 KHz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The number of controlled channels, MHz</td>
<td>124</td>
<td>375</td>
<td>299</td>
<td>124</td>
</tr>
<tr>
<td>Receiver Type</td>
<td>With dual frequency conversion, asynchronous</td>
<td>With triple frequency conversion, asynchronous</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>-----------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receiver sensitivity in Normal Environment</td>
<td>Not worse than -105 dBm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(noise level=20dB)</td>
<td>Level-wise BER=10^{-7}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Output Power</td>
<td>+30dBm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antenna Feed Impedance (within the working</td>
<td>50 Ω</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frequencies Band</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emitted interferences level</td>
<td>-36 dBm up to 1 GHz, (&lt;-30 dBm &gt; 1 GHz)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time of Hopping Step Change</td>
<td>&lt;500µS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Demodulator</td>
<td>GMSK Asynchronous (Agere Systems Inc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Synchronization</td>
<td>Adaptive test</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Air Frames Errors Correction</td>
<td>Viterby Convolution decoder, double strike</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consumed Wattage (per channel)</td>
<td>&lt;1W</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Speech Codecs</td>
<td>FR, EFR, HR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Combined Structure of Channels Organization</td>
<td>TDMA/FDMA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Range of Working Temperatures at not more than 90%</td>
<td>+5°C …+40°C (it is possible to operate the system in the range of -20°C +50°C on condition there is no moisture of condensation, but in that case radio channel parameters can degrade and won”t meet the ones specified in the Table)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>