GreenLeaf®

COMINT

SEMI ACTIVE GSM MONITORING SYSTEM

Surveillance, Interception, Monitoring & Logging System

PASSIVE GSM MONITORING SYSTEM

“ GL-H14 has designed various integrated systems for its Defence and Global intelligence Gathering Customers to meet their COMINT Requirement . The systems have been field - tested and can be customized for each specific requirement to meet your organization related needs ”

Dynamic Solutions for
Evolving Situations

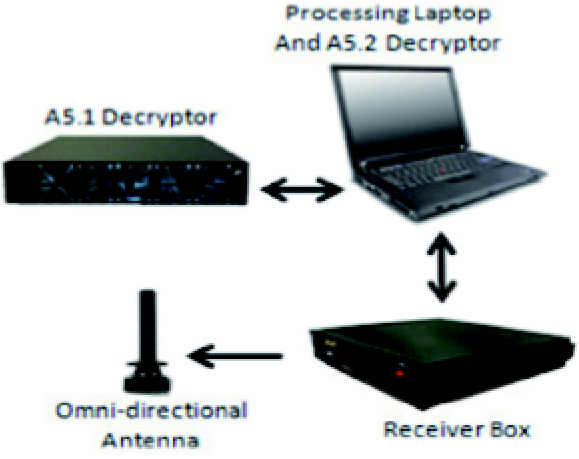
Technology Introduction:

GSM networks are most popular and widespread wireless communication media across the world, having a wide customer base in Europe and Asia-Pacific and command more than 50 percent of mobile customers. The advancement of GSM networks increases rapid growth of its users and services. Being an advance technology it becomes favorites for the criminals. These things created worldwide market for the analysis and monitoring of GSM network.

The advancement of GSM technology, enhanced technological features and increased complexity, presents competitive environment for Shoghi Communications to design and develop solutions to provide total passive OFF -THE- AIR Communication Surveillance system to its various Government and Int ering customers.

GSM operates on standards frequency 850 MHz, 1900MHz, 900MHz and 1800MHz bands and offer services such as SMS, MMS, email, advanced video features, dictionaries.

Due to the widespread availability of GSM networks, a GSM mobile has the potential to seamlessly roam nationally and internationally.



GSM supports data services where users can send and receive data, at rates up to 9600bps.

System Approach:

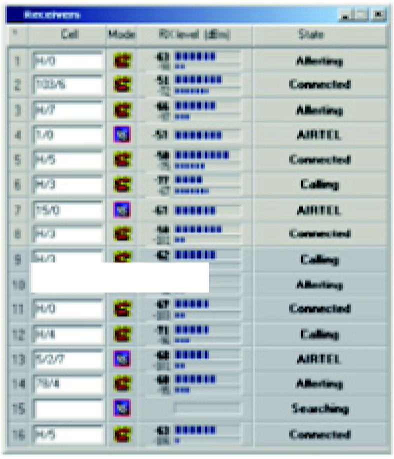
The system designed and developed as a Passive OF-THE-AIR GSM Monitoring System. The Surveillance of UM interface (b/w BTS and Mobile Handset) provides total traffic monitoring of the target. System uses state of art technology to on-line deciphering of A5.1, A5.2 and A5.0 cipher algorithms.

The system comes in a camouflaged case along with Control Laptop and Accessories.

System Solution:

The STN SUR GSMP is a multi-channel tunable GSM Monitoring system. Each receiver is independently tunable to any BTS of the GSM Network. STN SUR GSMP is intended to ensure interception and deciphering of voice conversation from standards GSM-850/900/1800/1900 Cellular network in stationary or in mobile environment. System also intercepts registration and service channel information from the cellular network.

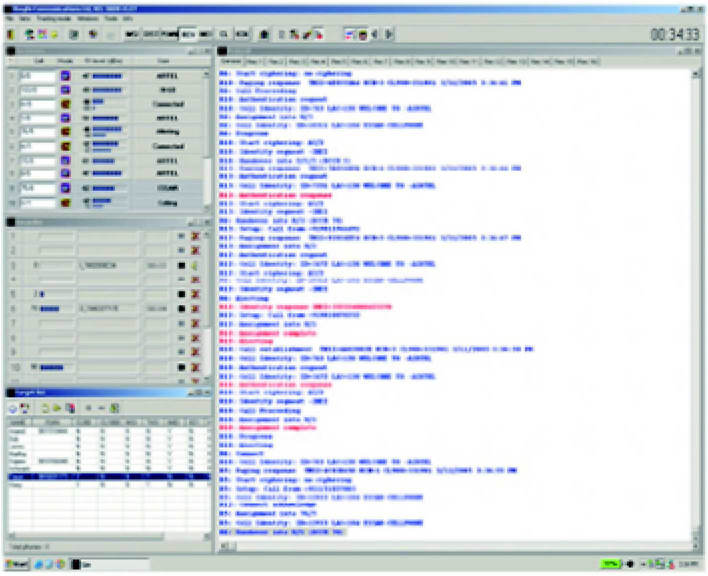
Receiver Window:



#	Cell	Mode	RX level (dBm)	State
1	H/0		-63	Alerting
2	103/6		-51	Connected
3	H/7		-66	Alerting
4	1/0		-51	AIRTEL
5	H/5		-58	Connected
6	H/3		-77	Calling
7	15/0		-61	AIRTEL
8	H/3		-58	Connected
9	H/3		-62	Calling
10				Alerting
11	H/0		-67	Connected
12	H/4		-71	Calling
13	5/2/7		-68	AIRTEL
14	78/4		-68	Alerting
15				Searching
16	H/5		-63	Connected

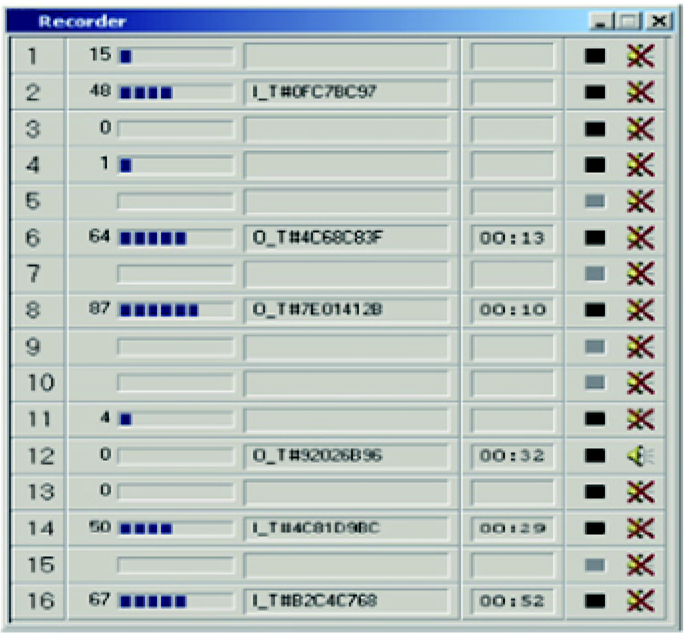
STN SUR GSMP is capable of doing various tasks while conducting monitoring. System compresses and stores intercepted voice calls, SMS's and protocol information on the control PC hard drive. It has the friendly user interfaces, which allows the user to adjust system on the various kinds of tasks, to provide the control of system during its operation.

Main Window



System online deciphers A5/0, A5/1 and A5/2 ciphering algorithms used in the GSM network to cipher the user's communication. To prevent detection of the system's operation and avoid interference to the operation of cellular network the System works as a passive equipment intercepting data directly from the air. The number of channels, being received and recorded by the system, can be upto 32 for one control computer.

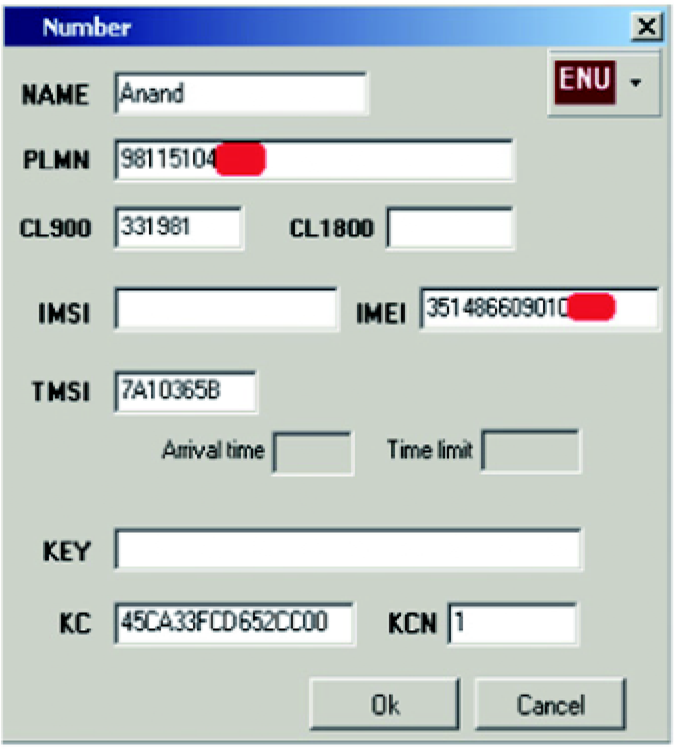
Recorder Window



Recorder

1	15		
2	48	I_T#0FC7BC97	
3	0		
4	1		
5			
6	64	O_T#4C68C83F	00:13
7			
8	87	O_T#7E01412B	00:10
9			
10			
11	4		
12	0	O_T#92026B96	00:32
13	0		
14	50	I_T#4C81D9BC	00:29
15			
16	67	I_T#B2C4C768	00:52

Target Creation Window



Number

NAME Anand

PLMN 98115104[redacted]

CL900 331981 CL1800

IMSI IMEI 35148660901[redacted]

TMSI 7A10365B

Arrival time Time limit

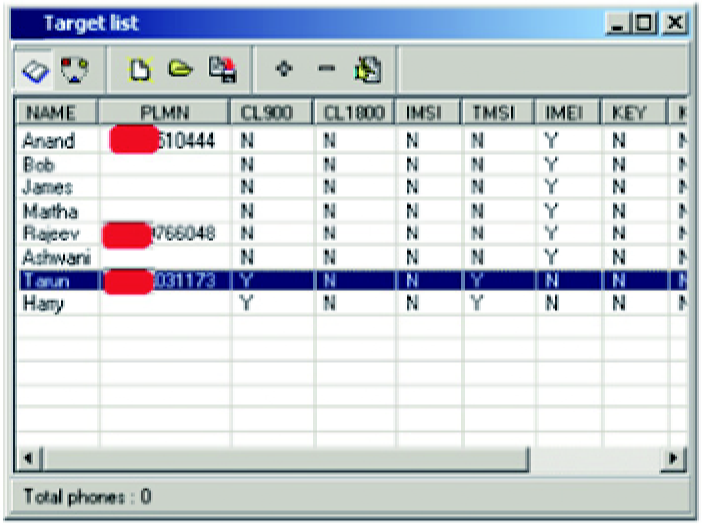
KEY

KC 45CA33FCD652CC00 KCN 1

Features:

- 100% Passive system. Presence of the system cannot be detected by anyone.
- Capable of Intercepting Voice and SMS communications
- Capable of monitoring GSM-850/900/1800/1900 networks
- Real-Time Passive Deciphering of A5/1, A5/2, A5/0 (Real-Time Deciphering of A5/1 algorithm is Optional)
- The system support FR, EFR, HR, AMR voice codec's
- On line monitoring up to 16 duplex channels.
- Interception Monitoring and logging of communication standards in stationary or in mobile environments.
- Automatically detects the ciphering algorithms used on the network in real-time
- All the recorded cell phone conversations, call related information, network information is stored in hard disk of the processing computer.
- Selection of the Targets by different parameters such as IMEI, IMSI, TMSI, Target distance from the base station, Type of target handset, Target's dialed & received number (PLMN).
- Monitoring of both forward and reverse channels (duplex conversation).
- The system automatically handles Frequency Hopping and Handovers
- Subscriber's location finding relative to the base station (LAC, BS, sector, distance with accuracy of 550 m) with possibility of its indication on the digital map (optional)

Target List Window



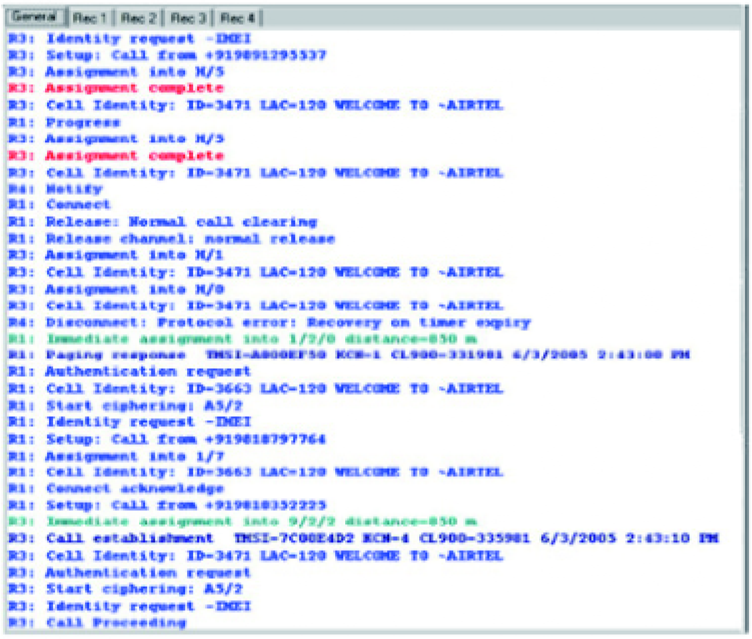
Target list

NAME	PLMN	CL900	CL1800	IMSI	TMSI	IMEI	KEY	K
Anand	[redacted]	N	N	N	N	Y	N	N
Bob		N	N	N	N	Y	N	N
James		N	N	N	N	Y	N	N
Martha		N	N	N	N	Y	N	N
Rajeev	[redacted]	N	N	N	N	Y	N	N
Ashwani		N	N	N	N	Y	N	N
Tarun	[redacted]	Y	N	N	Y	N	N	N
Harry		Y	N	N	Y	N	N	N

Total phones : 0

- Possibility of finding TMSI/IMSI/IMEI of a known MSISDN
- Switching ON/OFF the recording of conversations, network information and other parameters.
- Display current status of receivers (recording/ scanning) and target numbers.
- Several STN SUR GSMP systems can be configured in a LAN environment to provide a near-exact physical location of the target and to form a Central Monitoring Station.
- Scanning of GSM network parameters in the controlled area (Service Provider, Broadcast Channel No., LAC, Cell IDs, and Signal Levels).
- On-Line listing of the Cell phone calls.
- Possibility of round-the-clock operation in an auto mode without the operator involvement.
- Simplicity of maintenance, which does not require a deep knowledge, either in the field of computers, or in the field of cellular communication systems.

Protocol Window



```
R3: Identity request -IMEI
R3: Setup: Call from +919891295537
R3: Assignment into H/5
R3: Assignment complete
R3: Cell Identity: ID=3471 LAC=120 WELCOME TO -AIRTEL
R1: Progress
R3: Assignment into H/5
R3: Assignment complete
R3: Cell Identity: ID=3471 LAC=120 WELCOME TO -AIRTEL
R4: Notify
R1: Connect
R1: Release: Normal call clearing
R1: Release channel: normal release
R3: Assignment into H/1
R3: Cell Identity: ID=3471 LAC=120 WELCOME TO -AIRTEL
R3: Assignment into H/0
R3: Cell Identity: ID=3471 LAC=120 WELCOME TO -AIRTEL
R4: Disconnect: Protocol error: Recovery on timer expiry
R1: Immediate assignment into 1/2/0 distance=850 m
R1: Paging response  TMSI-A800EF50 KCN-1 CL900-331981 6/3/2005 2:43:00 PM
R1: Authentication request
R1: Cell Identity: ID=3663 LAC=120 WELCOME TO -AIRTEL
R1: Start ciphering: A5/2
R1: Identity request -IMEI
R1: Setup: Call from +919818797764
R1: Assignment into 1/7
R1: Cell Identity: ID=3663 LAC=120 WELCOME TO -AIRTEL
R1: Connect acknowledge
R1: Setup: Call from +919818352225
R3: Immediate assignment into 9/2/2 distance=850 m
R3: Call establishment  TMSI-7C00E4D2 KCN-4 CL900-335981 6/3/2005 2:43:10 PM
R3: Cell Identity: ID=3471 LAC=120 WELCOME TO -AIRTEL
R3: Authentication request
R3: Start ciphering: A5/2
R3: Identity request -IMEI
R3: Call Proceeding
```

A5.1 Decryptor

The system is a multi-processor circuit board housed inside ruggedized case along with cooling system. It is powered from compact external power supply.

It is controlled by the processing laptop, which is responsible for communication between decryptor and A5/1 encrypted bit stream

GSM Interception System sends to A5/1 encrypted bit stream – usually one Encrypted burst derived from forward (down link) channel. A5/1 decipher calculates ciphering key Kc and sends it back to the GSM interception system. The GSM interception system implements Kc and decrypts communication which is almost immediate process.

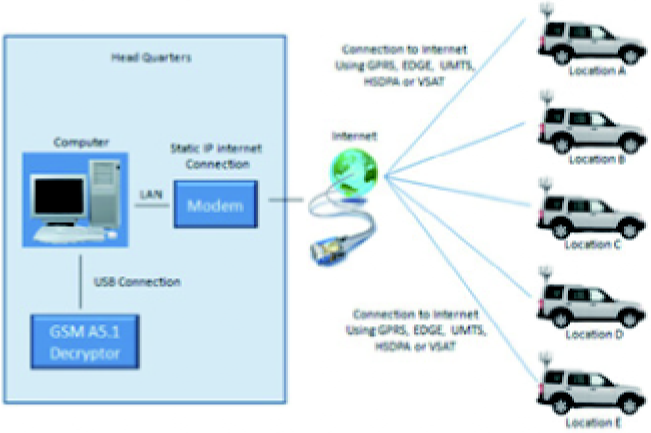
The decryptor is available in various configurations depending upon the user's choice. The configuration depends on the deciphering time. The various available options are 0.75 seconds, 3 seconds and 150 seconds

GSM Interceptor and A5/1 Decipher can be connected either directly by USB cable or wirelessly using any available communication means (GPRS, UMTS, satellite link, etc.). A5/1 decipher can serve more than one GSM Interception Systems (maximum up to 5 GSM interceptors).

Technical Specifications of A5.1 Decryptor

- Average deciphering time: 0.75 sec, 3sec, 150sec
- Probability of deciphering: 100% with BER=0
- Connection with GM system LAN, Internet via VPN
- Operating Temperature Range: + 5° C to +25° C
- Storage Temperature Range: -20° C to +60° C
- Humidity: +40° C at 95%
- Power Consumption: 1000W
- Weight: 16.5 kg
- Dimensions: 500x310x180 mm
- Power Supply: 110-230 V AC + 10%

Multiple System using One Decryptor


Head Quarters
Computer
Static IP internet Connection
LAN
Modem
USB Connection
GSM A5.1 Decryptor
Internet
Connection to Internet Using GPRS, EDGE, UMTS, HSDPA or VSAT
Connection to Internet Using GPRS, EDGE, UMTS, HSDPA or VSAT
Location A
Location B
Location C
Location D
Location E

Operational Modes:

The system works 100% passively and is fully invisible to the GSM provider or target irrespective of the operational mode because no radio signals are radiated by the system. All incoming GSM signals are received only by RX Omni-directional antenna (forward and reverse channels) and are decoded with the help of special software.

Scanning Mode

In this mode it is possible to receive GSM information from all networks, located within the area of coverage by the system. This is the first step before tuning the system to required ARFCNs. It is also possible to set up the system in such a way that some of the predefined receivers can collect this information continuously to support mobile operation (car, train, etc)

Interception Mode

Ensuring interception of traffic from mobile stations located within the coverage range of the system.

There are two modes of control:

- Random (all mobile stations);
- Target Mode (only targets or possible targets)

Random Mode: This mode is used when there is no previous information about target. The system must be started without any selection limitations (Filters). The operator must investigate each intercepted GSM session and make a decision about target presence in this area. This type of operation is named "Random mode".

This mode is also useful in situations in which you are monitoring an area where you suspect the presence of the target. The target has to be identified based on his voice or identities of his handset or called number. When the target is identified the operator can mark as call "target" in the system software. The system will automatically add the targets identities in a target list, which can be activated later in the Target Mode for precisely monitoring only the target's calls. The Random Mode is generally used for reconnaissance.

Target Mode: This mode is intended for selection of target of interest based on target identities. These identities can be collected either in the Random Mode as explained earlier or by other intelligence methods. The target identities include IMSI, IMEI, TMSI, ClassMark, KCn. The target identities along with a target name can be stored in a target list. Once this mode is activated the system will only intercept calls of targets that are present in the target list. It is not necessary that all the target identities have to be obtained in order to intercept the calls, but the more identities you have the chances of identifying the target will be more.

TMSI detector

A system can automatically discover each TMSI reallocation command in the target's session. If that was not the case the target may disappear from the system whenever there is a TMSI change. For calculating the TMSI the system establishes a silent call to the targets mobile, the system will automatically break the call before alerting signal on the target's side. So, in this case the system becomes not fully passive.
The method is useful when operator know MSISDN number of the target's handset in order to arrange a call.