BulTrans - 2014
Proceedings
17-19 September 2014
Sozopol

GSM COMMUNICATIONS JAMMING - AN INTELLIGENT METHOD

VESELIN RADKOV
Department of Aeronautics, Techmical University, Sofia, Bulgaria
vradkov@aero.tu-sofia.bg

Abstract:

The GSM communications jamming is used in many cases in the reason of national security measures and for government and political leader's personal security and for prevention of terrorist attacks by distance managed bombs. As usual the special radio-transmitters (Radio-Jammers) are used and these ones as general used brutal RF power force jamming by covering the all GSM spectrum by jamming signal (barrage jamming). This one method requires high-transmitted power on wide RF diapason and in this reason the protected area is less than 100m in general. A new jamming method is offered, based on changes of thin GSM signal structure in this paper. This one method allows more energy effective Jammers to build and wider areas to be covered.

Keywords: *jammer, intelligent, method, jamming, GSM, BCCH.*

I. Introduction

Improvised explosive devices (IED) have been used as long as explosive weapons have existed. The principle of using explosives in a manner other than they were originally developed for has been used for sabotage, terrorism, insurgency and ad hoc military uses is both well established and simple to understand. The Radio Controlled IED (RCIED) are using an RF module to initiate a device. RCIEDs have advantage of flexibility; there is no physical link between commander (terrorist people) and device. In the reason GSM networks are worldwide presented, in many cases as a RF controlled devise is used a simple mobile telephone.

I. Radio jamming

Communication jamming devices were first developed and used by military. Jamming is performed by transmitting a signal to the receiver at the same frequency band or sub-band as the communications transmitter transmits. Jamming is successful when the jamming signal denies the usability of the IED (receiver).

The transmitter used to trigger the RCIED must also be within range of the receiver. This will depend on a number of factors, as explained below. The key radio-parameters are:

- Frequency of operation;
- Transmitted power;
- Transmit and receive antenna heights;
- Antenna gain/loss;
- Noice floor at the receiver;
- Sensitivity of receiver device.

Because of the topology of the scenario, it is likely that the transmitter and device receiver will be within a few hundred meters of each other. The exception to this can be where existing networks are used, such as GSM mobile phone systems. In this case, the BTS used to relay the trigger command may be many kilometers away.

It is possible to identify the critical factors that will affect performance of the RCIED's communication link

- Terrain effects will not normally vary significantly within the operational range, although of course there are exceptions to this;
- Atmospheric variations will in general be negligible;
- Local clutter such as buildings or dense vegetation may be dominant attenuation factor;

- Ground conductivity may be an important factor within this regime, since the antennas will typically be so low above local ground (as general the RCIED's antenna will be on the ground or even under-ground);
- Local fading will be an important factor within the nominal coverage range.

In terms of radio prediction and simulation it is usually not possible to determine where precisely an attack may occur and therefore from a device suppression (i. e. jamming) point of view, a site-general model approach is necessary. US forces adopted a simple model with a correction for ground conductivity [1]. This is used to represent both target and jammer links. This one model assumes that the jammer is for VHF communications links only, that the effective Jammer to Signal Ratio (JSR) is approximately 8:1 (linear terms) and that the links have no or minimal intervening terrain [1].

The model provides two formulae, the first one to determine the necessary jamming power:

$$P_j = P_t K \left(\frac{H_t}{H_j} \right)^z . \left(\frac{D_j}{D_t} \right)^n . \quad (1)$$

And the second, which determines the maximum effective range of a jammer:

$$D_j = D_t^n . \sqrt{\frac{P_j}{P_t K \left(\frac{P_t}{H_j} \right)^2}} , \quad (2)$$

where:
P_j – minimum jamming power required;
P_t – effective power output by the enemy transmitter;
H_j - elevation of jammer above sea level;
H_t – elevation of enemy transmitter above sea level;
D_j – jammer-to receiver link distance, km;
D_t – enemy transmitter-to-receiver link distance, km.
K – jammer tuning accuracy:
=2 – for FM receivers in VHF range;
n – terrain and ground conductivity factor:
=5 – very rough terrain; poor conductivity.
=4 – moderately rough terrain; fair to good conductivity;
=3 – rolling hills; good conductivity;
=2 – level terrain; good conductivity.

The performance of the power prediction model is illustrated in Figure 1 for different categories of ground conductivity [1]. The figure shows the power required to jam a transmission link (enemy) of given distances. The (enemy) communication link distance is shown on the bottom axis. The jamming link distance is a constant 10 km.

Notice that (1) and (2) are independent of frequency and also of minimum receive sensitivity of the enemy receiver. Also notice that for short ranges, the jamming power is very high and probably unreliasable. This is not unreasonable because if the enemy communication devices are closer together, the link is far more difficult to jam.

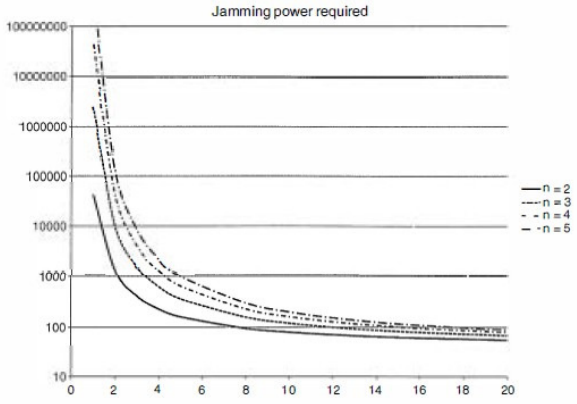

Fig.1 US jamming model for different ground conditions.

It must be noted that there are several caveats to the use of this model [1]:

- Firstly, it assumes no significant obstructions between transmitter and receiver;
- Clutter is not accounted for this model;
- The value produced is a nominal figure to which fading characteristics must be applied;
- The model is fairly coarse.

The model is coarse because of describing and analyzing a unique set of circumstances using actual terrain and clutter values will result in a site-specific model that can't be generalized to different scenarios.

If the jammer does not have the output power to jam a wide band continuously, it can increase its instantaneous jamming level by pulsed jamming. In pulsed jamming, the jammer sweeps the wide band jamming each narrow sub-band for a short period of time. Usually a successful attack requires that the jammer's power is roughly equal to signal's power at the receiver's place.

Classic jamming transmission is simply band-limited noise (barrage jamming, denial jamming, etc.). The objective is to inject an interference signal into the communications frequency so that the actual signal is completely submerged by interference.

In general the GSM jammer is a device that transmit signal on the same frequency at which the GSM system operates, the jamming success when the mobile phones in the area where the jammer is located are disabled.

The non-intelligent jammer is used to form a restricted (protected) area (illustrated in Figure 2) [2], and it is designed to block all mobile phones operate in a certain frequency bands.

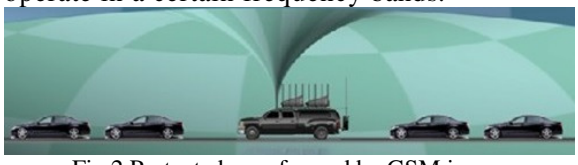

Fig.2 Protected area formed by GSM jammer.

As usual, the non-intelligent system jams the whole downlink frequency band (barrage jamming) even though the mobile phone uses only a small portion of the band.

Following (2), it is easy to note the distance has a strong influence on the signal loss. If the D_j is doubled, the jammer has to quadruple its output in order for the jamming to have the same effect. So, the non-intelligent barrage signal jammers have high energy consumption and low effectiveness, and capable to form as usual about 400 - 600m^2 protected area.

II. Intelligent GSM jamming

II.1. GSM Air Interface.

If an active connection exist between the MS and BTS the mobile terminal is said to be in dedicated mode. If the MS is switched on but remains passive to the network the terminal is said to be in idle mode.

In the GSM network, the Base Transceiver Station (BTS) is the actual RF transceiver using U_m air interface. In U_m interface the physical channels consist of all the available time-slots (TS) of a BTS, i. e. each TS forms one physical channel. The total number of TS is 8 (from #0 to #7).

On the other hand the GSM channels consist a set of logical channels which each perform a special task. There are twelve different types of logical channels in GSM (Table 1), separated into 3 groups:

Table 1

Channel name	Logical Channel name	Direction
BCH (Broadcast Control Channels)	**FCCH** (Frequency Correction Channel)	BTS→MS
	SCH (Synchronization Channel)	BTS→MS
	BCCH (Broadcast Control Channel)	BTS→MS
CCCH (Common Control Channels)	**PCH** (Paging Control Channel)	BTS→MS
	RACH (Random Access Channel)	BTS←MS
	AGCH (Access Grant Channel)	BTS→MS
	CBCH (Cell Broadcast Channel)	BTS→MS
Dedicated Control Channels	**SDCCH** (Stand-Alone Dedicated Control Channel)	BTS↔MS
	SACCH (Slow Associated Control Channel)	BTS↔MS
	FACCH (Fast Association Control Channel)	BTS↔MS
TCH (Traffic Channels)	**TCH** (Traffic channel for voice/data)	BTS↔MS

In the GSM technology standard each TS exists either 51 times in a multi-frame 51 or 26 times in a multi-frame 26.

There are lots of different ways of mapping logical channels on a physical one. The physical TS#0 is reserved for the common channels and therefore this one is the most important.

The traffic channels are used for voice and data load transportation so these ones are never mapped on TS#0 of the beacon (BCCH) frequency.

The following logical channels are used in idle mode:

FCCH - in search of a new beacon frequency;
SCH - in search of a new beacon frequency;
BCCH - while monitoring the system (GSM network) information;
PCH - while monitoring whether there is call;
AGCH - waiting for the immediate assignment of a channel;
RACH - sending a channel request to the GSM network.

Asses to these channels is possible following the burst sequence shown in Figure 3.

Fig. 3. A burst sequence at the Beacon frequency TS#0.

Most channels transmit their data on a normal burst. In TS#0 at first a Frequency correction burst is emitted, followed by Synchronization bursts. The following 4 bursts set up a message from the BCCH. The next 4 bursts set up a message from the paging channel, and so on.

II.2. Air interface Logical channels

II.2.1. Frequency Correction Channel

The FCCH is only required for the operation of the radio subsystem and its only task is to carry information for frequency correction of the MS. It has no supplementary information about the BTS or the network. The FCCH hence provides only information about the existence of a cell using the concerned frequency which enables the MS to measure the signal strength. The so called Frequency Burst is directly mapped on the TS#0, there is no coding or the like, since there is no bit-information to be broadcasted.

II.2.2. Synchronization Channel

The SCH aims to help the mobile to synchronize to a BTS. It provides a long training sequence for synchronization and the Frame Synchronization Element.

The Synchronization Information Element consists hence of 25 Bits. These Bits are correction

coded and resulting in a 77 bit message which is split up into two 39-bit sections emitted in a synchronization burst.

II.2.3. Broadcast Control Channel

When a mobile terminal is switched on, it changes from status “MS - power off” to the initial status “MS- power on” (idle), MS starts a "cell selection procedure", as usual this is a BCCH. There is a beacon frequency on this channel, i. e. a distinguishing frequency in a cell.

In idle mode the mobile listens to the BCCH, which is intended to broadcast regularly all necessary information to the MS which it needs to register in the system. The network will provide the following information:

- identification of the network, location area and cell;
- information for candidate cell measurement;
- description of the control channel structure;
- utilization of the RACH;
- different supported options;
- length of the message part belonging to phase1 protocol;
- BCCH scheduling (optional).

This data will be delivered in System Information Messages.

Every System Information Message is wrapped into a 23-byte-word. After these 23 bytes are (correction) coded and interleaved. The word, now extended to 456 bits plus 4*2 flag bits, is sent on the four bursts of every multi-frame reserved for the BCCH. This means there is one System Information Message transmitted every 235,38ms.

II.2.4. Paging Channel

If a mobile is called, this call will be announced to the network by sending a paging message (Paging Request) on paging channel of the CCCH. The mobile will subsequently send a Channel Request on the RACH indicating in the establishment cause field of this message that it has received a paging message. This causes the network to allocate a dedicated channel for this MS, which will then send a paging response on the DCCH to the network. After the usual authentication process any data transmitted on this channel will be ciphered. In a sequence step the actual call establishment will be initiated by the network.

II.2.5. Random Access Channel

RACH message has 4 octets length as this is shown in Figure 4 and this one message contains information about access permission to the network.

The RACH Control Parameters located consist the cell barring access indicator (bit 2 in octet 2). If this one bit is 0, the cell is not blocked, if bit state is 1, the cell is blocked for access and in this case MS will be informed the cell is not in service nor for incoming nor for originated call. In other words, the all MS served by this channel (i. e. by this BTS) will be out of functionality, nevertheless they are turned on.

bit No.	8	7	6	5	4	3	2	1
octet 1	0	1	1	1	1	0	0	0
	RACH control parameters IEI							
octet 2	Max Retrans			Tx-integer			CELL BARR ACCESS	RE
octet 3	AC C15	AC C14	AC C13	AC C12	AC C11	EC C10	AC C09	AC C08
octet 4	AC C07	AC C06	AC C05	AC C04	AC C03	AC C02	AC C01	AC C00

Fig. 4. RACH control parameters

Parameter’s meaning:

Max Retrains:	maximum number of access attempts;
Tx-integer:	number of time slots to spread access attempts;
Cell Barr Access:	barring options indicator
RE:	call re-establishment
EC:	emergency call
AC Cn:	access control classes (from 0, 1, 2, 3 ……. to 15)

III. Method for intelligent GSM jamming

Following the Logical channels structure used in GSM networks, an intelligent GSM jamming is possible to be implemented by changing the system information messages sent on the BCCH.

The idea is to change the RACH message and especially CELL-BARR-ACCESS bit from 0 to 1. The BCCH has to be emitted in the modified version constantly and with a significantly bigger signal strength than the BCCH version emitted by the BTS. In general this is not serious problem in the reason the distance between the jammer and RCIED will be many times shorted than the distance between BTS and RCIED.

The realization of this method will include following jammer's functions:

- receiving of the BCCH of BTS with the biggest signal strength;
- extraction and decoding of the received BCCH;
- the ability to extract and to modify all BCCH messages;
- the ability to re-emit the modified and re-coded BCCH.

In this method the GSM jammer acts as a "retranslator" between the BTS and all MS located in the protected zone. This means it either acts as the BTS with the biggest signal strength in the protected zone, taking over its "personality" i. e. making the MS "believe" it is the real BTS itself.

The jammer must to have two separate antennas: one for signal reception and one for the emission of the modified signal. This is for two reasons. Firstly, the cell phone jammer has to listen to the downlink signal from BTS and to re-emit this one signal after signal processing (i. e. modified signal) at the same time. Secondly, the emitting antenna has to be separated from the receiving one since it otherwise would perturb its receiving signals.

The functionality of the BCCH-method will hence be as follows:

1.It firstly scans the frequency spectrum, looking for the strongest BTS and then synchronizes to this BTS. In the reason the jammer and RCIED will be close each other, the strongest BCCH emission to the jammer will also be the strongest one to any MS in the protected zone.

2.Once synchronized to the BTS the jammer will take one 51-multitrame, extract the BCCH and change the System Information Messages (i. e. RACH control parameters) to the desired "jamming" values. There is one System Information Message emitted every 0,235s (every multi-frame).

3.Change of the original RACH message by the fake message. The BCCH messages that do not contain the RACH will be simply forwarded.

4.Finally, both false/original BCCH will be emitted on air by Transmitter working on separate antenna. The aim is to omit a stronger signal than the served GSM cell (BTS).

Conclusions

1.The presented above method for GSM communications jamming is independent from any special device or network feature and will hence work on any GSM cell phone in any GSM network. It will also be applicable to future devices.

2.The presented method is very useful to build an intelligent jammer device. In fact this one device will be not a typical jammer, but nevertheless the final result will be GSM services stoppage on the wide protected area.

3. It is not necessary high output jamming power in the reason of:

- the intelligent jammer will be very close to the RCIED than served BTS;
- the intelligent jammer will emits power on BCCH frequency only, not on wide GSM diapazon.

4.The disadvantages of this method are:

- the BCCH has to be modified and re-emitted all the time. This disadvantage hence has to be compensated by a good operation status control strategy.
- if there protected area is covered by a few GSM operators, it is must to have jammer for each operator coverage.

Acnowledgements

The author thanks to Sintis Technology Company and to NIIS at the Technical University of Sofia for financial support under Contract N14000.

References

[1] Adrian Graham, Communications, Radar and Electronic Warfare, John Wiley & Sons Ltd., 2011

[2] Corporate broshure, Sintis Technology Ltd., Sofia, 2013.

[3] ETSI: Digital cellular telecommunications system; Call Barring supplementary services - Stage 2 (GSM 03.88), version 5.0, 1996.

[4] ETSI: European digital cellular telecommunications system (Phase 2); Operator determined barring (GSM 02.41), 1994.