An Investigation of a New GSM Systems Jamming Technique without Existing Connections Disruption

Mladen Đ. Mileusnić, Predrag M. Petrović, Branislav R. Pavić, Verica B. Marinković-Nedelicki, Vladimir S. Matić, and Aleksandar V. Lebl

Abstract — This paper presents a new method for jamming of GSM communications. The aim is to decrease voice connection quality, thus disabling users to understand each other, while keeping established connections. The jamming method parameters depend on the algorithm characteristics implemented in SACCH frame. It is proved for three mobile telephony codecs that it is possible to reach unsatisfactory voice connection quality MOS<2 due to jamming of a GSM communications channel. Errors in data transmission during the periods without jamming also cause voice connection quality impairment and this influence is analyzed. The method performances are compared to other solutions.

Keywords — E-model, GSM system jamming, jamming rate, SACCH frame.

I. INTRODUCTION

HOSTILE activities include various types of communications and each type of these communications has its specificity. There is the difference between the jamming of remote controlled improvised explosive devices (RCIED) activation messages and mobile telephony systems jamming (GSM or CDMA). It is also possible that the message for RCIED activation is transmitted by a mobile telephony system [1].

IRITEL centre for radio communications has great, long standing experience and knowledge in the development of radio surveillance and jamming systems and equipment [2-9]. Three generations of GSM mobile phone or cellular jammers have been developed for various outdoor and indoor applications [9]. Figure 1 presents one of IRITEL cellular jammers solutions.

There are various approaches to the implementation of GSM communications jammers like those in references [10-13]. The simplest solutions are the active jammers [10-12], which are always in the operation mode. This type of equipment is called Denial of service in [10] or constant jammers in [13]. The jamming device sends a noise signal only in the frequency range used for GSM signal transmission, thus decreasing a signal to noise ratio [10] or it applies continuous sweep signal jamming [11-12]. There are two possible reactions of GSM system in such a case: 1) it may continue to transmit the signal, which will not be received and 2) the channel will be considered as a busy one and not used for signal transmission [13].

Random jamming may be defined by the alternative periods of active and inactive jamming [13]. As a random jammer has no information about some channel whether it is busy or not, it is possible to jam an inactive channel and to miss a busy one.

There is a possibility that jamming is realized in a more intelligent way, than to continuously send the jamming signal. It means that a jamming device is dominantly in the receive mode with the goal to detect the intention of the mobile station (MS) to communicate with the base station (BTS). The jamming signal is generated only when such a communication exists. In this way the emission power is saved and electromagnetic pollution is decreased [14]. Such a jamming technique is called reactive jamming [13].

Another type of jammers is deceptive jammers [13]. In
this case a jamming device continuously imitates usual GSM traffic using adequately defined frame structure transmissions, causing a GSM system to treat the considered channel as busy.

The spoofing technique (or „Intelligent Beacon Disablers“ technique) is also applied to GSM signal jamming [10], [14]. In this technique the jammer forces the mobile phone to turn off itself. The jamming device behaves as a „beacon“, which orders the MS to disable its ringer or function. Similarly to this technique, „Intelligent Cellular Disablers device“ is capable of detecting the presence of MS and of communicating with the BTS [14]. It sends information to the BTS that the user is in the „quiet“ room, thus telling the BTS not to establish the call.

Intelligent jamming may be used in such a way that a jamming signal is sent only during some periods of GSM frame. These time periods are important for connection setup or for frame error detection or correction [13]. Such a jamming type is based on the precise synchronization with a GSM frame and on the knowledge of GSM frame structure.

There are several differences between GSM communications jamming and RCIED activation message jamming. GSM frame structure, applied signal power and the used bands and frequencies are known in advance. On the contrary, the characteristics of RCIED activation message (frequency range, emission power, modulation type, data rate, message length) are not known a priori. In the case of GSM systems, it is necessary to realize jamming continuously during a longer period of time. For RCIED activation message jamming it is typically required to prevent message appearance including its eventual later repetition. That’s why GSM communications jamming is usually realized in an easier way, but applied jamming techniques could be similar in both cases.

The method presented in this paper is not complicated for realization and it is the nearest one to constant and random jamming. Constant jammers have the highest, constantly transmitted emission power, such that they are exposed to easier detection of their presence. Random jammers have a lower emission power, but, as already stated, jamming is not quite reliable because of jamming randomness. All variants of intelligent jamming are complicated for realization, although emission power is significantly lower. The primary goal in the majority of jamming methods is to force the termination of the established connection. On the contrary, a novelty of the method presented in this paper is that it tries to keep the established connections, while decreasing voice connection quality.

Section II presents the main elements of the GSM signal frame structure. Section III is a brief overview of E-model as the voice connection quality estimation method used in this paper. Section IV describes the new jamming method. Section V gives the calculated expected jamming results. Influence of errors when a signal is transmitted without the jamming action is analyzed in Section VI. The simulation program is briefly presented in Section VII. Concluding comments are included in Section VIII.
SACCH frame. There is the procedure when the value of the counter is incremented by 1 each time an error is detected in SACCH frame and the value of this counter is decreased by 2 when there is no error in SACCH frame [17-18]. The maximum value of this RADIO_LINK_TIMEOUT counter [17] and also its starting value at the moment of the connection beginning are usually limited to the value 20-48 [19]. It means that the percent of error SACCH frames may reach JR=66% (where jamming ratio JR presents the part of time when a jamming signal is transmitted), but that no actions are initiated to force the connection termination. This algorithm behaviour is exploited in our analysis.

The implemented modulation technique in GSM systems is Gaussian Minimum Shift Keying (GMSK). Its important characteristic is that each symbol presents one bit. This fact has to be considered in our analysis.

III. VOICE CONNECTION QUALITY ESTIMATION

E-model is the computational model for the estimation of voice connection quality. It joins the influence of various factors into one unique quality measure – a rating factor R [20]. The value of R is connected with Mean Opinion Score (MOS), which is between 1 and 5. The values of MOS and R are connected by a formula and corresponding Fig. B.2 from [20]. The value MOS≤2 may be, in any case, considered as unsatisfactory, i.e. the value when voice is not understandable. The corresponding value of rating factor is R≤39.

The main purpose of E-model is to express voice connection quality in Internet (VoIP) connections. But, according to [21], MOS is used as the measure of voice quality in mobile telephone connections. Taking into account that MOS and R are mutually dependent variables, we implemented E-model to estimate the quality of mobile telephony connection.

According to E-model, a connection rating factor is [20]:

\[ R = 94 - I_{\text{eff}} \]  

where effective equipment impairment factor \( I_{\text{eff}} \) includes impairments caused by the implementation of low-bit codec and influence of random signal loss.

The value of \( I_{\text{eff}} \) is calculated from the equation [20]:

\[ I_{\text{eff}} = I_s + (95 - I_s) \cdot \frac{P_{\text{pl}}}{\text{BurstR}} + B_{\text{pl}} \]  

where:
- \( I_s \) - equipment impairment factor when there is no signal loss;
- \( P_{\text{pl}} \) - transmitted signal loss probability (in %);
- \( \text{BurstR} \) - burst ratio: the quotient of the average lengths of the lost signal parts in real transmitted signal and when signal parts are randomly lost;
- \( B_{\text{pl}} \) - robustness factor, which is specific for each coder type.

The characteristic of GSM mobile systems is burst loss of transmitted signal. But, when bits of coded signal are forming a voice channel, their order is changed, which means that burst loss of coded signal bits is replaced by random loss. That’s why we use the value BurstR=1in equation (2). We are focused on the codecs which are implemented in GSM systems. These are Full Rate (FR) codec (or GSM 06.10), Half Rate (HR) codec (or GSM 06.20) and Enhanced Full Rate (EFR) codec (or GSM 06.60). The values of \( I_s \) and \( B_{\text{pl}} \) for FR are 26 and 43, respectively [22], 23 and 15 for HR [23], [24] and 5 and 10 for EFR [23].

IV. THE METHOD OF JAMMING

The applied jamming strategy may be explained on the base of Fig. 3. A jamming signal is transmitted during the periods, designated by \( T_{\text{jam}} \) (Fig. 3a) and not transmitted during \( T_s \). The jamming rate is, then:

\[ JR = \frac{T_{\text{jam}}}{T_{\text{jam}} + T_s} \]  

Besides the value of JR, which must be JR≤0.66, it is important that \( T_{\text{jam}} \) is not too long in order that the counter RADIO_LINK_TIMEOUT does not reach the value smaller than 0. We have chosen the value \( T_{\text{jam}}\leq2\cdot T_s=9.2\text{ms} \). In this way it is possible that the value of counter is decreased only for two units consecutively as the result of jamming.

Jamming is realized as a frequency sweep (Fig. 3b). It means that signal frequency is linearly changed during \( T_{\text{jam}} \) from its minimum value (\( f_{\text{min}} \)), corresponded to the lower limit of GSM band to its maximum value (\( f_{\text{max}} \)). The signal frequency at the moment of starting the next \( T_{\text{jam}} \) period is equal to the frequency at the moment of the previous \( T_{\text{jam}} \) period end.

The upper and lower bound frequency of one TDMA signal are designated as \( f_{\text{sw}} \) and \( f_{\text{ol}} \) respectively (Fig. 3b). It is \( f_{\text{sw}}-f_{\text{ol}}=200\text{kHz} \). During the time while a jamming signal is changed between \( f_{\text{sw}} \) and \( f_{\text{ol}} \) it is possible that bits of GSM signal are incorrectly received (bits B03 and B04 and other hatched bits of GSM signal in Fig. 3c). Even in the case that jamming frequency is between \( f_{\text{sw}} \) and \( f_{\text{ol}} \) during the whole bit duration, it is possible that this bit is correctly received. The probability of false bit reception while a sweep signal frequency is in the range of considered TDMA signal frequency will be designated as \( P_{\text{sw}} \).

Let us designate the time of one sweep cycle as \( T_{\text{sw}} \) and the duration of one bit (and, also, one symbol) in GSM signal as \( T_b \) (Fig. 3c). The reciprocal values of these time intervals are sweep signal frequency (\( f_{\text{sw}} \)) and the bit rate of GSM signal (\( f_{b} \)). Then the jamming probability of the considered bit (i.e. that jamming frequency is in the range of the corresponding TDMA signal) is equal to

\[ P_{\text{j}} = \frac{T_{\text{sw}}}{T_{\text{sw}} + f_{\text{sw}}} \]  

The necessary condition is that \( T_{\text{sw}}\leq T_{\text{sw}} \). The optimum jamming strategy is to adjust \( f_{\text{sw}} \) in such a way that it is \( T_{\text{sw}}=T_{\text{sw}} \). In this case the time interval while jamming frequency coincides with the GSM channel frequency is maximum and equal for each channel. If the jamming frequency is further increased, i.e. if it is \( f_{\text{sw}}\leq f_{\text{sw}}\leq2\cdot f_{b} \), the time of frequencies coincidence is for some channels increased, but for others decreased compared to the optimum case. This time of coincidence depends on the fact whether the considered bit is jammed once or two times during its lifetime.
The necessary condition is that $T_b \leq T_{sw}$. The optimum jamming strategy is to adjust $f_{sw}$ in such a way that it is $T_b = T_{sw}$. In this case the time interval while jamming frequency coincides with the GSM channel frequency is maximum and equal for each channel. If the jamming frequency is further increased, i.e. if it is $f_b < f_{sw} < 2f_b$, the time of frequencies coincidence is for some channels increased, but for others decreased compared to the optimum case. This time of coincidence depends on the fact whether the considered bit is jammed once or two times during its lifetime.

Now the value $P_{pl}$ in (2) may be calculated as:

$$P_{pl} = 100 \cdot JR \cdot P_{err} \cdot P_j = 100 \cdot JR \cdot BER.$$  

(5)

V. RESULTS

The values of $R$, obtained on the base of equations (1)-(5), are presented in Fig. 4 and Fig. 5. The results are presented for FR, HR and EFR codec as the function of $BER=P_{err} \cdot P_j$. The parameter for these figures is $JR$.

![Fig. 4. Connection rating factor $R$ as a function of bit error rate ($BER$) for three GSM codecs when jamming rate is $JR=0.5$.](image)

![Fig. 5. Connection rating factor $R$ as a function of $BER$ for three GSM codecs when jamming rate is $JR=0.63$.](image)

For the practical analysis it is necessary that the value $P_{err}$ is known. In that case the values of $JR$ and $P_j$ are chosen according to Fig. 4 and Fig. 5 to achieve the value $R \leq 39$.

The voice connection will still exist, because the value of counter RADIO_LINK_TIMEOUT does not fall below 0, but the voice connection quality is very bad (MOS≤2), where users do not understand each other.

![Fig. 6. Connection rating factor $R$ as a function of jamming rate $JR$ for three GSM codecs when $BER$ is 0.5.](image)

### TABLE I – THE NECESSARY JR TO ACHIEVE R=39 FOR VARIOUS GSM CODECS WHEN BER IS 0.5.

<table>
<thead>
<tr>
<th></th>
<th>FR (GSM 06.10)</th>
<th>HR (GSM 06.20)</th>
<th>EFR (GSM 06.60)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.623</td>
<td>0.24</td>
<td>0.25</td>
<td></td>
</tr>
</tbody>
</table>

**Example:** FR codec is implemented in a GSM system. Let us suppose that $P_{err}=0.5$ is the probability of false bit reception when sweep signal jamming frequency is in the range of considered channel. Choose the value of $JR$ and $T_{sw}$ to achieve connection quality MOS≤2.

**Solution:** it is $R>39$ (MOS>2) for $BER=0.5$ if $JR=0.5$ when FR codec is applied (Fig. 4). That’s why it is
necessary to choose \( JR = 0.63 \) (Fig. 5). As \( R \) is now a bit less than 39 \( (R=38.8) \) for \( BER = 0.5 \), we must choose the maximum value \( P_p = 1 \), i.e. \( T_{sw} = T_q = 3.69\mu s \), or \( f_{sw} = 271 \) kHz.

There is a possibility that environmental conditions cause also a signal loss until it is \( BER \leq 0.66 \) and to still have a connection, because it is \( RADIO\_LINK\_TIMEOUT > 0 \).

**Remark 1:** the value \( BER = 0.5 \) is the typically achieved value when the jamming signal level is significantly greater than the level of the signal which has to be blocked. This is proved in [25] for MPSK modulated signals, where \( M \) may be 2, 4, 8 or 16. The value \( M=8 \) is used for Enhanced Data GSM Evolution (EDGE) systems. When considering graphs from [26] for GMSK modulated signals, it may be concluded that the \( BER \) values are between 0.2 and 0.4 depending on the measurement (calculation) conditions for the signal to noise level ratio \( S/N = 0 \) dB. The approximate \( BER \) formula for GMSK signals may be found in [27] and it shows that \( BER \) value tends to 0.5 when the ratio \( S/N \) is increased. The detailed analysis of \( BER \) for GMSK modulated signals for \( S/N < 0 \) dB could be the subject of our future analysis.

**Remark 2:** under normal traffic conditions FR coding is applied to communications realization until some threshold of the number of instantaneously busy traffic channels [28]. HR codec is applied to connections only in the case of high traffic load when more than threshold number of channels is busy. That’s why it is important to design jammer role also according to the requirements for HR codec.

**VI. INFLUENCE OF SIGNAL TRANSMISSION ERRORS**

Until now we have supposed in this paper that jamming is realized under the conditions where there are no other error sources. This means that it has been \( P_{p} = 0 \) in the time intervals between two jamming signal bursts.

Let us now consider the situation when there is an error in the GSM signal when there is no jamming. The probability of such an error \( (P_{p}) \) is very small in the case of Internet connections (transmission over optical cables), but may be significantly greater for mobile communications.

The value of \( P_{p} \) in (2) is now expressed by

\[
P_{p} = 100 \cdot (JR \cdot BER + (1 - JR) \cdot P_{b})
\]

![Fig. 7. Connection rating factor \( R \) as a function of bit transmission error \( P_{b} \) for two GSM codec when \( BER \) is 0.5 and when \( P_{p} \) is not negligible.](image)

Fig. 7 presents a connection rating factor \( R \) as a function of bit transmission error \( P_{b} \) for two values of jamming rate: \( JR = 0.1 \) and \( JR = 0.2 \). During periods with a jamming signal GSM signal error probability is \( BER = 0.5 \) and when there is no jamming signal, GSM signal error probability is \( P_{b} \). The results are presented for the values of \( P_{b} \) between 0% and 4%. It is interesting to notice that the value of \( R \) may fall to 39 or even less both for EFR and HR codec when \( JR = 0.2 \) and \( P_{b} = 3 \). When the value \( JR \) is increased (in Fig. 7 when it is increased from 0.1 to 0.2), the influence of \( P_{b} \) on the degradation of connection quality is decreased.

**VII. METHOD VERIFICATION**

The presented jamming method is verified implementing our original simulation program, which is based on a set of random numbers generation. Each result is obtained after at least 100,000 times of executing a program simulation loop. The main purpose of the program has been to analyse the performances of combined sweep and barrage jamming \( (S/N < 0 \) dB), but for an implementation in this program noise level is decreased \( (S/N > 0) \). Two main aims in the simulation have been: 1) to prove the \( P_{p} \) value obtained by (5) and 2) to estimate the maximum expected value of the register \( RADIO\_LINK\_TIMEOUT \), thus confirming that a connection would not be disrupted during jamming. The corresponding signal in the simulation is obtained as the vector sum of RCIED activation signal, jamming sinusoidal signal and Gaussian white noise signal for the period \( T_{jam} \), while the signal consists of RCIED activation signal and noise signal during \( T_q \) [8]. The jamming signal phase as also noise signal phase in relation to the RCIED activation signal directly follow from the uniformly distributed random number. Amplitudes of noise signals are calculated starting from the uniformly distributed random numbers, which are modified using the Box-Müller method [29]. The simulation is performed for the variable values according to the example from Section V, including \( JR = 0.63 \). According to simulation, \( P_{p} = 0.312 \), which satisfactorily agrees with the value \( P_{p} = 0.315 \) on the base of (5). The maximum values of the register \( RADIO\_LINK\_TIMEOUT \) as a function of the ratio \( S/N \) during simulation are presented in Table II.

<table>
<thead>
<tr>
<th>( S/N ) (dB)</th>
<th>( RADIO_LINK_TIMEOUT )</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>&lt; 4</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>6</td>
<td>&gt; 20</td>
</tr>
</tbody>
</table>

**VIII. CONCLUSIONS**

A new method for jamming of GSM systems is presented in this paper. Compared to most other solutions, the aim is not to force the termination of the jammed communication, but to decrease the connection quality to the level where users cannot understand each other. In this way the probability to think about the jammer presence is decreased in comparison to the solutions when connection is terminated. This method is based on the behaviour of SACCH frame, fire code and the implemented criteria in it. The analysis is performed for the three most widely used GSM codec types. With respect to constant jamming, necessary emission power as well as radiation level are decreased. Jamming emission power depends on the value of \( JR \), meaning that it is less than 66% of the jamming power in the case of constant jamming.
method is similar to random jamming (there are periods of jamming activity and inactivity), but more reliable, because there is no danger of avoiding jamming of an active channel. The jamming emission power is higher than in the case of intelligent jamming. However, the jamming method is simpler, because there is no need to synchronize jamming signal transmission with GSM signal frame or to detect MS and communicate with BTS like in various methods of intelligent jamming.

REFERENCES