Análise da Eficácia de um Bloqueador de RF por Varredura: Estudo de Caso para o Sistema GSM

Alex Alvarez da Silva[1], Maurício Henrique Costa Dias[2] e José Carlos Araujo dos Santos[2]
[1]Instituto de Pesquisa da Marinha – IPqM, Rua Ipirú, nº 2, Jardim Guanabara, Ilha do Governador, Rio de Janeiro – RJ
[2]Instituto Militar de Engenharia – IME, Praça General Tibúrcio, nº 80, Praia Vermelha, Rio de Janeiro – RJ

***Resumo* — Este trabalho apresenta um estudo de caso para a condição de bloqueio sobre o sistema de telefonia móvel GSM. É elaborada uma simulação, através do programa MatLab® (Simulink), envolvendo um modelo do canal de tráfego do GSM e uma réplica de um dispositivo bloqueador. Um dispositivo bloqueador foi implementado, sendo usado nos testes da eficácia do bloqueio sobre um terminal GSM comercial. Os resultados obtidos indicam que o bloqueador é eficaz para uma relação interferência-sinal superior aos 20 dB previstos teoricamente, com atuação exclusiva sobre a banda de operação do canal direto, de 1805 a 1880 MHz.**

***Palavras-chaves* — Bloqueio de radiofrequência, bloqueador de telefonia celular, sistema de telefonia móvel GSM.**

I. INTRODUÇÃO

Dentre as tecnologias que utilizam o espaço livre como meio de transmissão para as comunicações, uma das que mais se desenvolveu nos últimos anos foi a de redes de telefonia móvel, que permite a comunicação entre pontos distintos no planeta com mobilidade e qualidade. No panorama atual, existem diversas empresas ligadas a esta tecnologia, entre fabricantes de equipamentos e operadoras de sistemas. Uma quantidade considerável de sistemas e serviços de comunicação é disponibilizada à população.

Em situações onde é necessário inviabilizar o estabelecimento do enlace de comunicação, bloqueadores de RF são frequentemente utilizados. Tais dispositivos têm como função inserir um sinal interferente no espectro eletromagnético para degradar a qualidade do sinal no receptor do sistema, de forma a inviabilizar a recepção do sinal de informação desejado [1][2].

Os dispositivos bloqueadores são amplamente utilizados em aplicações militares de Guerra Eletrônica e, mais modernamente, em situações onde é necessária a efetivação da Garantia da Lei e da Ordem (GLO). Os bloqueadores devem possuir, de forma geral, característica multibanda e capacidade de reconfiguração em frequência e potência, de forma a aumentar sua eficácia sobre os sistemas receptores modernos.

Em sistemas militares, esses dispositivos são fabricados para controle das comunicações táticas, impossibilitando a interceptação das mensagens.

Os primeiros dispositivos de bloqueio foram desenvolvidos para uso militar, onde os chefes táticos usavam comunicações de RF para controlar as suas forças e inviabilizar possíveis interceptações do inimigo nessas comunicações [3]. A Marinha do Brasil utiliza estes equipamentos em operações de Contra Medidas Eletrônicas - CME.

Este trabalho apresenta um estudo de caso para a condição de bloqueio sobre o sistema de telefonia móvel GSM [3]. Foi elaborada uma simulação, através do programa MatLab® (Simulink), envolvendo um modelo do canal de tráfego do GSM e uma réplica de um dispositivo bloqueador. Os resultados obtidos durante os eventos de simulação são apresentados e comentados. Ainda, um protótipo de dispositivo bloqueador foi implementado, permitindo a realização de testes práticos de geração de interferência sobre o canal direto do sistema GSM. Os resultados desses testes são apresentados e comentados.

A seção II apresenta uma abordagem teórica e uma avaliação computacional sobre as condições para bloqueio no sistema GSM. A seção III mostra os resultados dos testes práticos realizados com o sistema comercial GSM. As considerações finais sobre a eficácia do bloqueio no sistema são apresentadas na seção IV.

II. SIMULAÇÃO DO BLOQUEIO EM SISTEMAS GSM

A. Avaliação teórica

O sistema GSM [3][4] utiliza espalhamento espectral FHSS e, sendo assim, existe a condição de ganho de processamento, o qual é função direta do número de canais de salto da informação transmitida. O ganho de processamento no sistema GSM é dado por [5]:

$$G_P = \frac{WN}{R_b} = N \tag{1}$$

onde W é a largura de banda utilizada para o envio dos bits de informação através de um único canal, R_b é a taxa de informação da fonte em bits por segundo (b/s), e N é o número de canais de frequências disponíveis para o salto. Cada canal tem a mesma largura.

Um sistema GSM 1800 possui no mínimo 317 canais de salto, totalizando um ganho de processamento superior a 25dB.

Quando o sistema utiliza técnicas de espalhamento espectral, é utilizado o conceito de margem de bloqueio para ter uma estimativa da relação bloqueio-sinal (J/S) na entrada do receptor. A Margem de Bloqueio, definida por M_J, é o nível de interferência que o sistema é capaz de aceitar, mantendo um nível de performance mínimo especificado. Portanto, quando existir a condição de ganho de processamento, a relação mínima entre os sinais de bloqueio e do sistema deve ser definida pelo parâmetro Margem de Bloqueio, dada por [6]:

$$M_J = G_P(dB) - \left(E_b / N_0\right)_{(REQ)}(dB) - L(dB) \tag{2}$$

onde G_P é o ganho de processamento do sistema, $(E_b/N_0)_{(REQ)}$ é a relação entre a energia de bit e a densidade espectral de potência de ruído requerida pelo demodulador do sistema para um determinado valor de BER típico, e L é a perda de implementação do próprio sistema.

Segundo Stahlberg [6], o bloqueador requer uma taxa de M_J = -5 dB para bloquear o canal GSM com sucesso, sem considerar o ganho de processamento. Assumindo-se um ganho de processamento de 25 dB, a relação M_J passa a ser de 20 dB. Este resultado corresponde ao valor teórico da relação bloqueio-sinal na entrada de um receptor GSM para efetivação do bloqueio sobre seu canal de comunicação.

Em operações de bloqueio, muitas vezes um bloqueador por varredura é empregado. Em tais situações, o canal GSM não está permanentemente sob atuação do ruído. Nos itens seguintes, é mostrado que de fato a eficácia do bloqueio sobre o sistema GSM é dependente da frequência de varredura de tais bloqueadores, e que a relação bloqueio-sinal é bem superior à prevista teoricamente, podendo este limite ser determinado através de simulações do sistema em questão.

B. Sistema GSM

Com o propósito de verificar a condição de geração de interferência sobre o sistema de telefonia móvel GSM através de uma ferramenta computacional, foi laborada em MatLab® uma simulação envolvendo de um modelo do canal de tráfego TCH do sistema GSM [7]-[12], mostrada na FIG. 1.

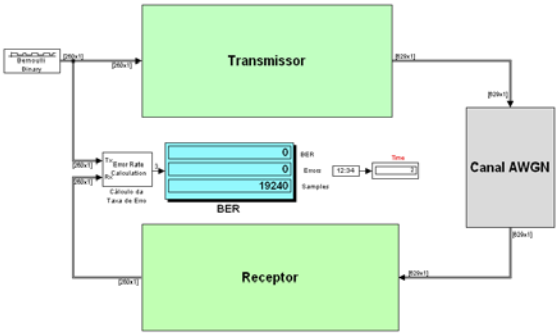

FIG. 1 – Canal de trafego do sistema GSM.

No sistema GSM, as unidades móveis em chamada usam um canal de tráfego TCH (Traffic Channel). O TCH é um canal bidirecional usado para a troca de informações de conversação entre a unidade móvel e a estação base [8]. As informações são divididas em canal reverso e canal direto, dependendo da direção do fluxo (FIG. 2).

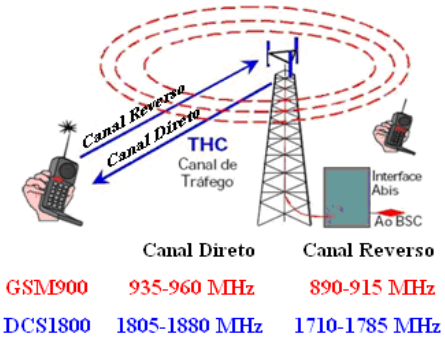

FIG. 2 – Canal de Tráfego no GSM.

O canal de tráfego TCH é responsável pelo envio de voz e dados codificados tanto no canal direto quanto no canal reverso. Para transmissão de voz, o canal TCH pode ser utilizado de duas maneiras distintas: TCH/F (taxa de 13 kbps), e TCH/H (taxa de 6,5 kbps). O presente trabalho utiliza um canal de tráfego TCH/F, que fornece 260 bits por bloco de conversação de 20 ms [9], resultando na taxa de 13 kbps.

O bloco transmissor é divido em duas partes, codificação e modulação, como na FIG. 3.

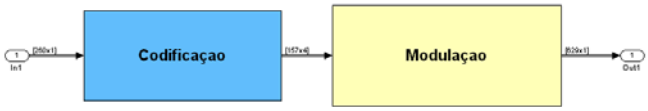

FIG. 3 – Bloco transmissor do GSM

A natureza da interface aérea GSM resulta na introdução de alguns erros de bit. Os bits são manipulados de forma que haja uma maior probabilidade de que os erros ocorram onde prejudiquem menos. A qualidade do som é mais afetada pelos bits de coeficientes mais significativos do que pelos bits menos significativos. Os bits de menor importância, ou bits de tipo II, não têm correção ou detecção de erros. Os bits mais importantes, de tipo Ia, têm detecção de erro, com a inclusão de bits de CRC. No tipo Ia e no tipo de importância média Ib, há a inclusão de bits de correção de erro convolucional.

O processo de codificação do GSM consiste em: adição de 3 bits de paridade aos 50 bits da classe Ia, código de blocos, adição de 4 bits ‘0’ aos 132 bits da classe Ib mais a saída do código de blocos, resultando em 189 bits. O código convolucional recebe os 189 bits e gera 378 bits codificados. A saída do codificador é somada com os 78 bits não protegidos da classe II, totalizando 456 bits codificados.

Os 456 bits de dados de conversação são divididos em 8 blocos de 57 bits codificadores (*interleaving*). Cada rajada (*burst*) do TCH transporta dois blocos de 57 bits codificadores de dados provenientes de dois segmentos diferentes de 20 ms de conversação com 456 bits. A FIG. 4 mostra o sistema em questão.

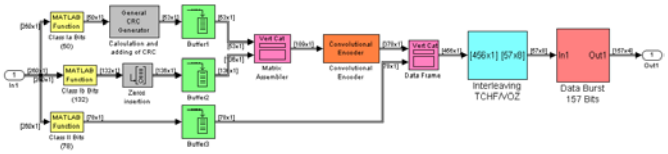

FIG. 4 – Diagrama do processo de codificação do GSM utilizado nas simulações.

Segundo a norma GSM 05.02 [8] a rajada de RF é divida em [13]:

- Bits finais (*tail bits*) – grupos de três bits nulos colocados no início e no fim do fragmento de rajada útil;
- 57 bits codificadores – informação a ser enviada;
- 1 bit sinalizador de roubo (*stealing flag*) – indica ao receptor que tipo de dados é transportado pela rajada. Quando há necessidade de envio de informações urgentes ao usuário, os bits sinalizadores possibilitam "roubar" a rajada de tráfego para que sejam enviadas mensagens de controle;
- 26 bits de treinamento (*bits training*) – utilizados para sincronizar o receptor com a informação de chegada;
- 1 bit sinalizador de roubo (*stealing flag*);
- 57 bits codificadores;
- 3 bits finais (*tail bits*);
- Tempo de guarda (*guard time*) – tem comprimento de 8.25 bits e é utilizado para evitar a colisão de duas estações móveis.

A FIG. 5 ilustra a rajada de dados do sistema GSM.

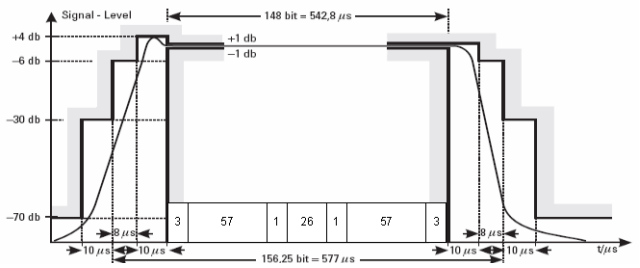

FIG. 5 – Rajada do sistema GSM.

Após montar a rajada, o sistema GSM transmite o sinal utilizando o formato de modulação digital 0,3GMSK, FIG. 6. O "0,3G" descreve a banda do filtro gaussiano de pré-modulação utilizado para reduzir o espectro do sinal modulado e o "MSK" é a transição dos bits 1 e 0, que são representados por deslocamento de frequência da portadora de RF.

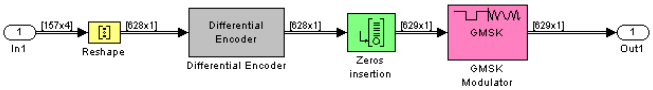

FIG. 6 – Diagrama do processo de modulação do GSM utilizado nas simulações.

O bloco receptor é o caminho inverso do sinal, o qual passa por um bloco de demodulação e um bloco de decodificação, como mostrado na FIG. 7.

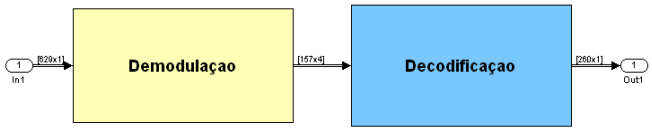

FIG. 7 – Bloco receptor do GSM.

C. *Bloqueio Eletrônico*

De forma genérica, o bloqueio eletrônico caracteriza-se pela irradiação ou reflexão intencional de energia eletromagnética com o objetivo de degradar a qualidade do sinal a ser recebido pelo receptor de um sistema de comunicação.

Há diferentes técnicas para impedir que os sistemas de comunicações funcionem. Segundo Poisel [1][2], as estratégias mais comuns de CME de bloqueio sobre um sistema são: Bloqueio por ruído (*Noise Jamming*), Bloqueio por tom (*Tone Jamming*), Bloqueio por varredura (*Swept Jamming*), Bloqueio por pulso (*Pulse Jamming*), Bloqueio seguidor (*Follower Jamming*) e Bloqueio inteligente (*Smart Jamming*).

Para verificar a condição de geração de interferência sobre o sistema de telefonia móvel GSM, foi elaborada em MatLab® uma simulação de um dispositivo bloqueador por varredura, configurado para inserir o sinal de bloqueio no canal direto do sistema GSM, de 1805 a 1880 MHz. A FIG. 8 mostra o diagrama em blocos do bloqueador implementado, do tipo pontual com varredura[3].

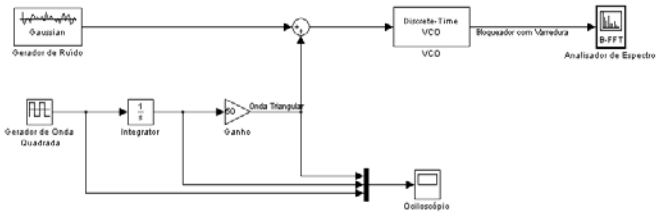

FIG. 8 – Dispositivo bloqueador pontual por varredura.

D. *Simulação do bloqueio no sistema GSM*

Com o intuito de verificar a eficiência do bloqueio sobre o sistema GSM, sem nenhuma fonte de perturbação a não ser a gerada pelo dispositivo bloqueador, o bloco Canal AWGN foi retirado da simulação. Foi inserido no canal um somador para a junção do sinal interferente ao sinal do sistema CDMA. A FIG. 9 apresenta o diagrama em blocos da simulação.

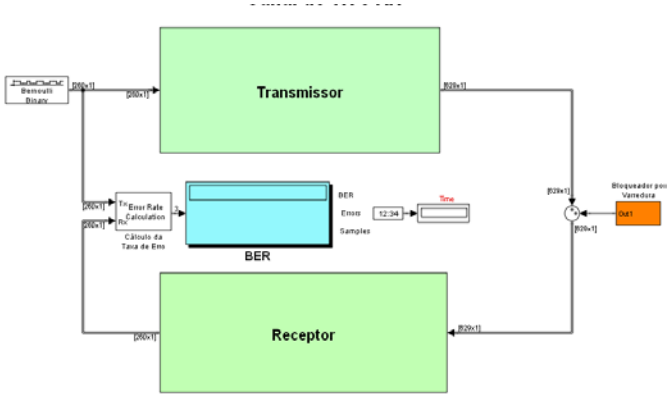

FIG. 9 – Canal de trafego do sistema GSM na presença de um dispositivo bloqueador pontual por varredura.

A qualidade do sinal em um sistema GSM é definida pelo parâmetro RxQUAL, que é a média da taxa de erro (BER) medida na recepção. O sistema GSM mantém a qualidade do sinal para RxQUAL de até 3,2% [14] [15] .

O sistema foi simulado com o bloqueador configurado com frequência de varredura de 70 Hz, 200 Hz, 700 Hz e 10 kHz, cujos resultados são mostrados na FIG. 10. A linha tracejada na figura representa o limite de BER aceitável, correspondente ao valor de RxQUAL de 3,2%.

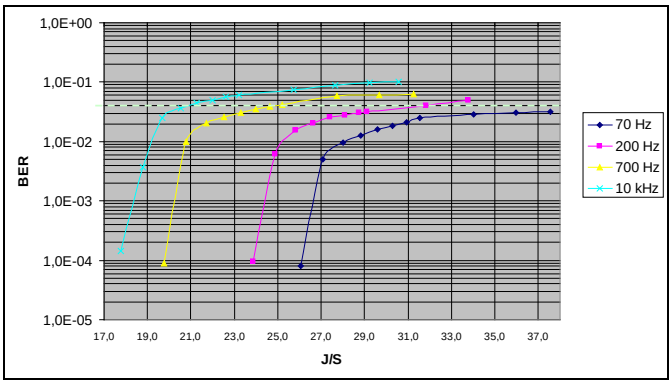

FIG. 10 – Relação entre a BER e a razão J/S no receptor de um canal de tráfego do sistema GSM com bloqueador por varredura.

Para a varredura do bloqueador configurada com 70 Hz o sistema indicou pouca ocorrência de bits e quadros com erro, e a BER ficou dentro do limite esperado para o sistema GSM. Com essa frequência de varredura o bloqueador não foi eficaz.

Aumentado a varredura para 200 Hz, o sistema indicou mais ocorrência de bits e quadros com erro. Para valores de J/S menores que 31,82 dB a BER ficou dentro do limite esperado. A partir do valor de 31,82 dB, a BER aumentou e o sistema ficou na condição de bloqueio em todas as simulações, caracterizando a degradação na qualidade do sinal imposta pela presença do bloqueador. Com o aumento do sinal de varredura, o sistema apresentou uma degradação maior, quando comparado aos parâmetros do sinal de varredura gerado com 70 Hz.

Aumentado a varredura para 700 Hz, para valores de J/S menores que 24,62 dB a BER ficou dentro do limite esperado para o sistema GSM. A partir do valor de 24,62 dB, a BER aumentou e ficou na região de bloqueio em todas as simulações.

Com o bloqueador configurado com varredura de 10 kHz, a razão J/S de bloqueio passou a ser de 20,53 dB.

III. TESTES EXPERIMENTAIS DO PROTÓTIPO

A. *Descrição do protótipo*

A FIG. 11 apresenta o digrama em blocos do dispositivo bloqueador implementado, para inserção de ruído em uma única banda de frequências do GSM, canal direto.

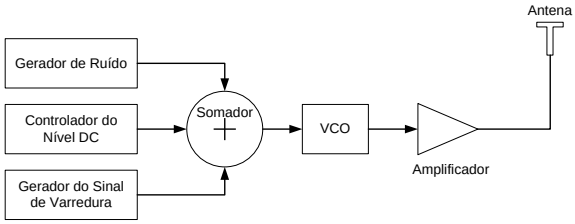

FIG. 11 – Diagrama em blocos do dispositivo bloqueador implementado.

B. *Testes realizados*

O bloqueio sobre o sistema de telefonia móvel celular GSM foi testado com um telefone celular comercial, marca NOKIA, modelo 2100, da operadora Claro (Rio de Janeiro). Para fins de validação da eficácia do bloqueador, foi feita a inserção do sinal de bloqueio, com uma largura de banda de 75 MHz, cobrindo toda faixa do canal direto, de 1805 a 1880 MHz.

Como não foi possível obter os parâmetros de cobertura de RF do sinal do sistema GSM, foi feita a medição dos níveis de potência de recepção do sinal *S* nas proximidades do local de realização dos testes. Essas medições foram feitas através de um aparelho celular Motorola, modelo V555, que possui essa facilidade.

A FIG. 12 apresenta a relação J/S medida para uma distância entre o bloqueador e a estação móvel de 10 m e os resultados da ação do bloqueador.

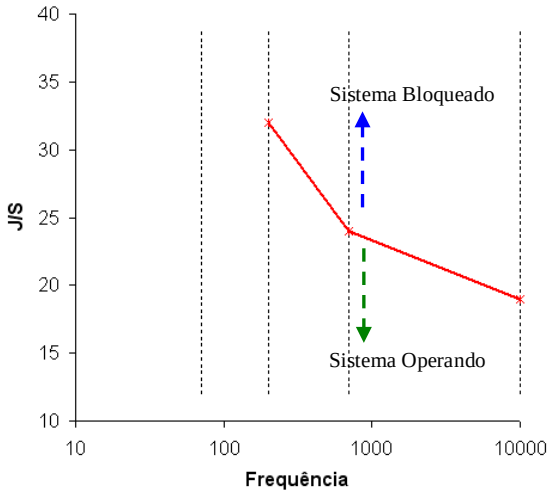

FIG. 12 – Relação J/S medida a 10 m do bloqueador, para diferentes freqüências de varredura.

Para a frequência de varredura de 70 Hz o bloqueio não foi eficiente e o celular operou normalmente para todas as relações de J/S.

Aumentando a frequência de varredura do sinal de bloqueio para 200 Hz o celular operou normalmente até a relação J/S de 32 dB. A partir desse valor o sistema permaneceu sempre bloqueado.

Configurando o sinal de bloqueio com varredura de 700 Hz o celular ficou em operação para relação J/S de 24 dB. A partir desse valor o sistema permaneceu sempre bloqueado.

Por fim, o bloqueador foi configurado com varredura de 10 kHz. Com essa varredura o celular ficou em operação para relação J/S de 19 dB. A partir desse valor o sistema permaneceu sempre bloqueado.

C. *Valores Simulados × Valores Práticos*

Para fins de comparação dos resultados medidos com os teóricos foram considerados três valores de BER. Foi escolhido um valor acima e um valor abaixo do limite de BER de 3,2% estabelecido anteriormente, conforme mostra a Tabela I.

TABELA I VALORES J/S SIMULADOS PARA UMA BER FIXA

BER	Frequência	J/S (dB)	Efeito
2,1%	70 Hz	30,2	Sistema Operando
	200 Hz	26,1	Sistema Operando
	700 Hz	22,3	Sistema Operando
	10 kHz	18,7	Sistema Operando
3,2%	70 Hz	-	Sistema Operando
	200 Hz	29,12	Sistema Inoperante
	700 Hz	23,52	Sistema Inoperante
	10 kHz	20,4	Sistema Inoperante
4,8%	70 Hz	-	Sistema Operando
	200 Hz	33,76	Sistema Inoperante
	700 Hz	26,5	Sistema Inoperante
	10 kHz	21,4	Sistema Inoperante

Os valores de J/S simulados para uma BER fixa, Tabela I, foram plotados juntos com os valores práticos da FIG. 12. Os resultados estão ilustrados na FIG. 13.

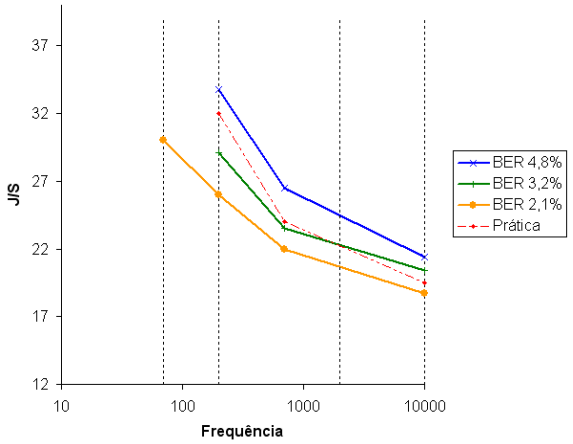

FIG. 13 – Resultados simulados e práticos.

Para uma BER fixa de 2,1% era esperado nas simulações que o sistema permanecesse sempre em operação para todas as frequências de varredura do bloqueador. A linha inferior do gráfico (laranja) corresponde a esta situação. Comparando com as medidas práticas, a linha laranja ficou dentro dos limites de operações para todas as frequências de varredura de bloqueio, comprovando as expectativas.

Para o limite de BER de 3,2%, foi observado nas simulações que o sistema permanecia sempre em operação para a frequência de varredura de 70 Hz, independentemente da relação *J/S*, e inoperante para outras frequências de varredura como o valor de *J/S* indicado na figura. A linha cheia intermediária do gráfico (verde) representa os valores de J/S simulados correspondentes a uma BER de 3,2%. Comparando com as medidas práticas, os resultados apresentaram comportamentos semelhantes. Para a frequência de varredura de 200 Hz, nas simulações era esperado que o sistema ficasse inoperante para uma relação J/S de 29 dB. Na prática o valor foi de 32 dB. Para as frequências de 700 Hz e 10 kHz, os pontos correspondentes na linha verde do gráfico ilustram que o sistema ficou dentro dos limites de bloqueio. Para a frequência de varredura de 70 Hz o sistema permaneceu em operação nos dois casos, simulados e práticos.

Para BER fixa de 4,8% era esperado nas simulações que o sistema permanecesse em operação para a frequência de varredura de 70 Hz e para as outras frequências de varredura o sistema ficasse inoperante. A linha superior do gráfico (azul) representa os valores de J/S simulados que correspondem aos valores J/S práticos, para BER fixa de 4,8%. Comparando com as medidas práticas, a linha azul ficou dentro dos limites bloqueio para todas as frequência de varreduras de bloqueio esperadas. Para a frequência de varredura de 70 Hz o sistema permaneceu em operação nos dois casos, simulados e práticos.

IV. CONCLUSÃO

O presente trabalho apresentou um estudo de caso sobre o efeito de um bloqueador de RF sobre um sistemas GSM, incluindo a identificação de aspectos relevantes ao funcionamento do sistema GSM, a determinação teórica da margem de bloqueio para este sistema, a simulação de um sistema de bloqueio sobre um modelo de canal de tráfego do GSM em MatLab®, e a avaliação experimental do bloqueio no sistema.

Os resultados simulados e práticos mostraram boa concordância, indicando que o uso da técnica de bloqueio em um sistema GSM é eficaz quando a relação interferência-sinal J/S obedece a FIG. 13 para diferentes freqüências de varredura do bloqueador utilizado. Tais valores, para baixas freqüências de varredura, foram bem superiores aos 20 dB previstos teoricamente. Para uma freqüência de varredura de 70 Hz o bloqueio foi completamente ineficaz.

REFERÊNCIAS

[1] R. A. Poisel, Introduction to Communication Electronic Warfare Systems. Artech House, Inc., 2002.
[2] R. A. Poisel, Modern Communication Jamming Principles and Techniques. Artech House, Inc., 2004.
[3] A. Silva, Simulação e Análise da Eficácia das Técnicas de Bloqueio em Sistemas de Comunicações: Ênfase no Sistema GSM. Dissertação de Mestrado, IME, 2009.
[4] D. Goodman, Wireless Personal Communications Systems. Addison-Wesley Wireless Communications Series, 1997.
[5] W. Lee, Mobile Cellular Telecommunications - Analog and Digital Systems. McGraw-Hill, Inc, 1995.
[6] M. Stahlberg, Radio Jamming Attacks Against Two Popular Mobile. Helsinki University of Technology, 2000.
[7] GSM 05.01, Digital cellular telecommunications system (Phase 2+), Physical layer on the radio path, General description. European Telecommunications Standards Institute, 2000.
[8] GSM 05.02, 3rd Generation Partnership Project, Technical Specification Group GSM/EDGE, Radio Access Network, Multiplexing and multiple access on the radio path. European Telecommunications Standards Institute, 2001.
[9] GSM 05.03, Digital cellular telecommunications system (Phase 2+), Channel coding. European Telecommunications Standards Institute, 2005.
[10] GSM 05.04, Digital cellular telecommunications system (Phase 2+), Modulation. European Telecommunications Standards Institute, 2001.
[11] GSM 05.05, Digital cellular telecommunications System (Phase 2+), Radio Transmission and Reception. European Telecommunications Standards Institute, 2005.
[12] GSM 05.08. Digital cellular telecommunications System (Phase 2+), Radio subsystem link control. European Telecommunications Standards Institute, 2000.
[13] G. Bauch and V. Franz, Iterative Equalization and Decoding for the GSM – System, Munich University of Technology, 1998.
[14] Y. Tseng and W. Hwang, The Influence of Propagation Environment in a Live GSM Network, National Koahsiung University of Applied Sciences, 2001.
[15] J. Wigard, T. Nielsen, P. Michaelsen., S. Skjaerris and P. Magensen, The influence of discontinuous transmission on equal statistics in GSM, in IEEE 49th Vehicular Technology Conference, Houston – EUA, vol. 3, pp. 2505-2509, Jul 1999.