Análise da eficácia de um bloqueador de RF: estudo de caso para terminais IS-95

Ricardo de Souza Toscano, Maurício Henrique Costa Dias, José Carlos Araujo dos Santos[1]

***Resumo* — Este trabalho apresenta um estudo de caso para a condição de bloqueio sobre o sistema de telefonia móvel CDMA (IS-95). É elaborada uma simulação, através do programa MatLab® (Simulink), envolvendo um modelo do canal de tráfego do CDMA (IS-95) e uma réplica de um dispositivo bloqueador. Um dispositivo bloqueador é implementado, sendo usado nos testes da eficácia do bloqueio sobre um terminal CDMA comercial. Os resultados obtidos indicam que o bloqueador é eficaz para uma relação interferência-sinal de cerca de 18 dB, com atuação exclusiva na portadora primária do sistema.**

***Palavras-Chaves* — Bloqueio de RF, bloqueador de telefonia celular, sistema CDMA IS-95.**

***Abstract* — This paper presents a case study of jamming over a CDMA (IS-95) terminal. The system is simulated with MatLab® (Simulink) with a replica of the CDMA channel and an RF jammer. Practical results showed that jamming is effective for an interference-to-signal ratio around 18 dB, just at the primary carrier of the system.**

***Index Terms* — RF blocking, cell phone jammers, CDMA IS-95 system.**

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, e uma quantidade considerável de sistemas de comunicação é disponibilizada à população.

Existem algumas situações em que esta facilidade de se comunicar com mobilidade é mal utilizada. Exemplos freqüentes ocorrem em presídios, locais de realização de concursos, entre outros. Nessas situações é necessário justamente inviabilizar o estabelecimento do enlace de comunicação. Para esta finalidade, utiliza-se um dispositivo denominado *bloqueador* (ou *interferidor*) *de RF* que genericamente tem como função inserir um sinal interferente no espectro eletromagnético para degradação da qualidade do sinal no receptor do sistema, de tal forma a inviabilizar a recepção do sinal de telefonia.

Os dispositivos bloqueadores são amplamente utilizados em aplicações militares (Guerra Eletrônica) e, mais modernamente, em situações onde é necessária a efetivação da Garantia da Lei e da Ordem (GLO). Os interferidores devem possuir, de forma geral, característica multibanda e capacidade de reconfiguração em freqüência e potência, de forma a aumentar sua eficácia sobre os sistemas receptores modernos. O desenvolvimento de dispositivos interferidores com estas funcionalidades é de interesse do Exército Brasileiro, contido em seu Plano Básico de Ciência e Tecnologia.

Este trabalho apresenta um estudo de caso para a condição de bloqueio sobre o sistema de telefonia móvel CDMA (IS-95). Foi elaborada uma simulação, através do programa MatLab® (Simulink), envolvendo um modelo do canal de tráfego do CDMA (IS-95) 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 de aquisição/sinalização (canal 283) do sistema CDMA. 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 CDMA IS-95. A seção seguinte mostra os resultados dos testes realizados com um sistema comercial. As considerações finais sobre a eficácia do bloqueio no sistema são apresentadas na seção IV.

II. SIMULAÇÃO DO BLOQUEIO DE TERMINAIS IS-95

A. Avaliação teórica

Em sistemas de bloqueio, a relação sinal-ruído do sistema é substituída pela relação interferência-sinal, representada por *J/S* [1]. Em sistemas CDMA, a qualidade do sinal é medida através da relação entre a energia de bit e a densidade espectral de potência dos sinais de ruído inerentes ao meio de transmissão (E_b/N_o) [2].

Para os receptores dos terminais móveis tipicamente utilizados em sistemas CDMA comerciais, a faixa de E_b/N_o suficiente para garantir a qualidade do sistema varia de 3 a 9 dB. Estes valores são indicados para a manutenção da taxa de erro de bits em 0,001 (igual a 10^{-3}).

O sistema CDMA utiliza espalhamento espectral do tipo seqüência direta e, sendo assim, a relação *J*/*S* necessária para

[1] Instituto Militar de Engenharia - IME, Seção de Engenharia Elétrica, Praça General Tibúrcio, 80, Rio de Janeiro, Brasil. E-mails: ricardo.toscano@yahoo.com.br, mhcdias@ime.eb.br, araujo@ime.eb.br.

efetuação do bloqueio não pode ser definida diretamente pela relação sinal-ruído (RSR) mínima de operação do sistema. Neste caso, deve-se considerar o ganho de processamento do sistema [3], dado por

$$G_P = \frac{W}{R} \quad (ch/b) \tag{1}$$

onde W é a taxa de chaveamento da portadora digital em *chips* por segundo (*ch/s*) e R é a taxa de informação da fonte em *bits* por segundo (*b/s*) do sistema CDMA. O valor do ganho de processamento G_P é de 21 dB, para W = 1.228.800 ch/s e R = 9.600 b/s.

Quando existe a condição de ganho de processamento, a relação mínima entre os sinais de bloqueio (J) e do sistema (S) é definida pelo parâmetro *Margem de Bloqueio* (M_J), que incorpora a melhoria imposta por G_P exclusivamente ao sinal do sistema. A margem de bloqueio, dada por [4]

$$M_J = \frac{G_P}{\left[\left(E_b/N_o\right)_{REQ} \times L\right]} \tag{2}$$

é de 18 dB, considerando o sistema sem perdas de implementação (L = 0 dB). Assim, o valor teórico mínimo da relação J/S é de 18 dB (ou 63,09 de relação entre potências). Espera-se que com valores de J/S acima de 18 dB seja possível efetuar o bloqueio no sistema CDMA. Ressalta-se que o bloqueio é realizado exclusivamente sobre o canal de sinalização (canal 283) do sistema CDMA (que eventualmente também pode ser o canal de comunicação), com o objetivo de impedir a aquisição do sistema pelo terminal móvel. Isto significa que uma ligação já estabelecida pode ser mantida mesmo que o terminal móvel entre na região de bloqueio. Ele será bloqueado (impedido de funcionar) quando tentar fazer nova aquisição do sistema.

B. Simulação do bloqueio no sistema CDMA IS-95

Com o propósito de verificar a condição de geração de interferência sobre o sistema de telefonia móvel CDMA através de uma ferramenta computacional, foi elaborada em MatLab® uma simulação envolvendo a composição aproximada de um dispositivo bloqueador e de um modelo do canal de tráfego do sistema CDMA IS-95.

O sistema CDMA foi escolhido por ser um dos mais complexos em relação à geração e à recepção do sinal e por possuir (teoricamente) mais imunidade ao ruído que outros sistemas. A Fig. 1 mostra o diagrama em blocos do bloqueador implementado, do tipo pontual com varredura [5].

A Fig. 2 apresenta o diagrama em blocos do canal direto de tráfego do CDMA, modelo ponto-a-ponto, de acordo com a norma IS-95A [2]. Este diagrama é um dos exemplos disponíveis do *toolbox* Simulink do Matlab® (versão 6.5). O modelo inclui os circuitos que compõem a geração do sinal, o meio de transmissão e os circuitos de recepção do sinal.

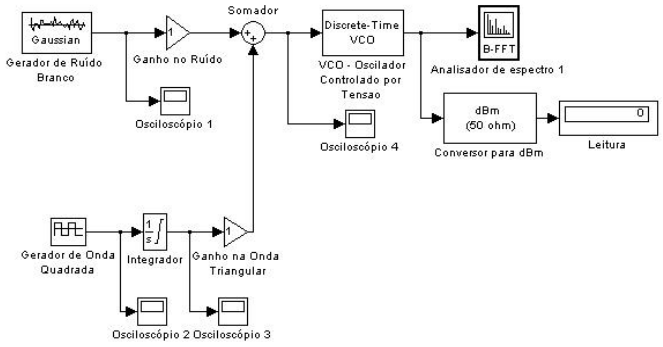

Fig. 1. Esquema do bloqueador implementado para simulação.

A geração do sinal é composta pelos blocos: *Data Source* (Fonte de Dados); IS-95A CRC *Generator* (Gerador do Código de Redundância Cíclica); IS-95A *Fwd Ch Convolutional Encoder* (Codificador Convolucional do Canal Direto); IS-95A *Fwc Ch Repeater* (Repetidor do Canal Direto); IS-95A *Fwd Ch Interleaver* (Entrelaçador do Canal Direto); IS-95A *Fwd Ch Scrambler* (Embaralhador do Canal Direto); *Combine with Sync e Paging, SS Modulate* (Combinação com o Sincronismo e *Paging* - Modulação Seqüência Direta); e *Transmit Filter* (Filtro de Transmissão). Na geração do sinal são incluídos dois Analisadores de Espectro: *Signal before spreading* (Sinal antes do espalhamento); *e Spread spectrum signal* (Sinal com espalhamento espectral).

O meio de transmissão é composto pelo bloco *Rayleigh Multipath and AWGN Channel* (Canal AWGN - ruído branco gaussiano aditivo, e sujeito a multipercursos, com distribuição Rayleigh); e por um Analisador de Espectro *Filtered spread spectrum signal* (Sinal com espalhamento espectral filtrado).

A recepção do sinal é composta por: *Receive Filter* (Filtro de Recepção); IS-95A *Fwd Ch Detector* (Detector do Canal Direto) e os seus circuitos de apoio para recuperação do sinal; IS-95A *Fwd Ch Deinterleaver* (Desentrelaçador do Canal Direto); IS-95A *Fwd Ch Derepeater*, (Módulo que retira a repetição do Canal Direto); IS-95A *Fwd Ch Viterbi Decoder* (Decodificador de Viterbi do Canal Direto); IS-95A *Fwd Ch Frame Quality Detector* (Detector de Qualidade do Quadro do Canal Direto) e os módulos de medição da taxa de erro de bits (BER – *Bit Error Rate*) e de quadros (FER – *Frame Error Rate*) com seus respectivos mostradores.

O objetivo da simulação é inserir o sinal gerado pelo dispositivo bloqueador dentro do meio de transmissão do canal de tráfego do CDMA e verificar o resultado da interferência nos módulos de medição de taxa de erro de bits e de quadros.

Com o intuito de verificar a eficiência do bloqueio sobre o sistema CDMA, sem nenhuma fonte de perturbação a não ser a gerada pelo dispositivo bloqueador, o bloco Canal AWGN – ruído branco gaussiano aditivo, e sujeito a multipercursos, com distribuição Rayleigh foi retirado da simulação. Foi inserido no canal um somador para a junção do sinal interferente ao sinal do sistema CDMA. A Fig. 3 apresenta o diagrama em blocos da simulação.

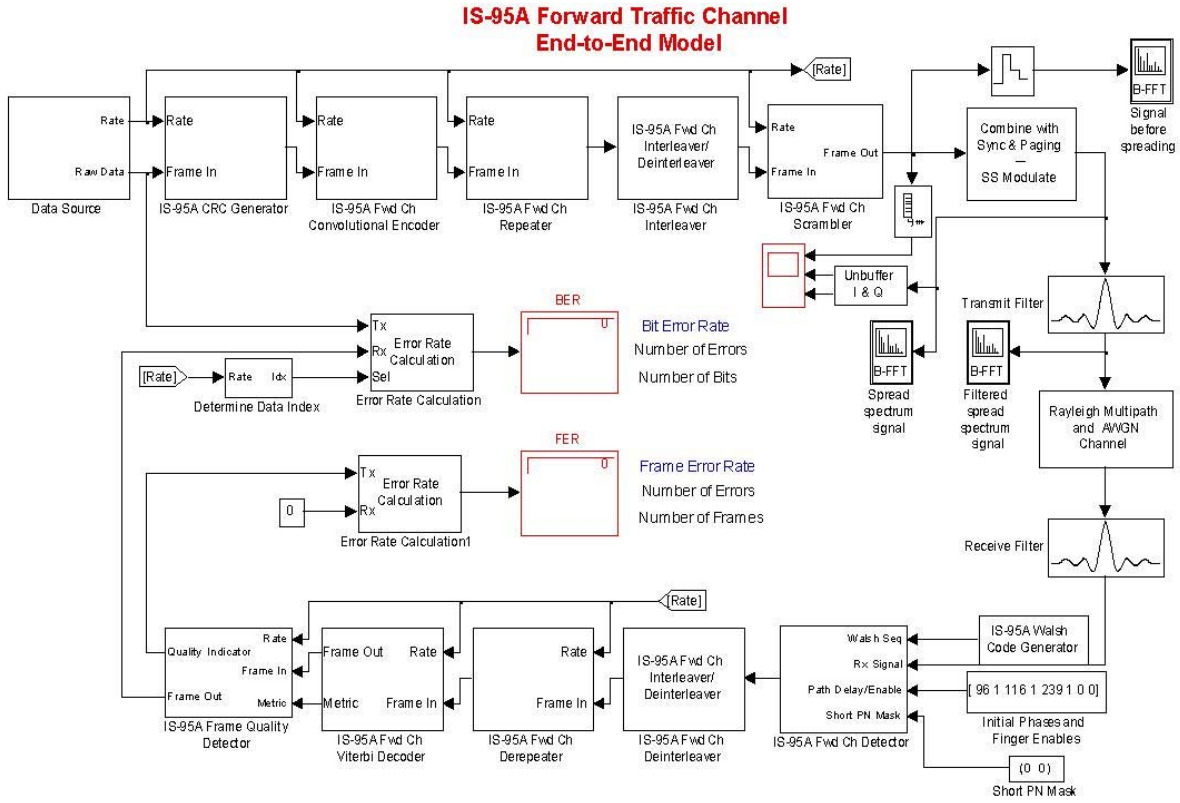

Fig. 2. Modelo ponto-a-ponto do sistema CDMA IS-95A disponível em MatLab® (Simulink).

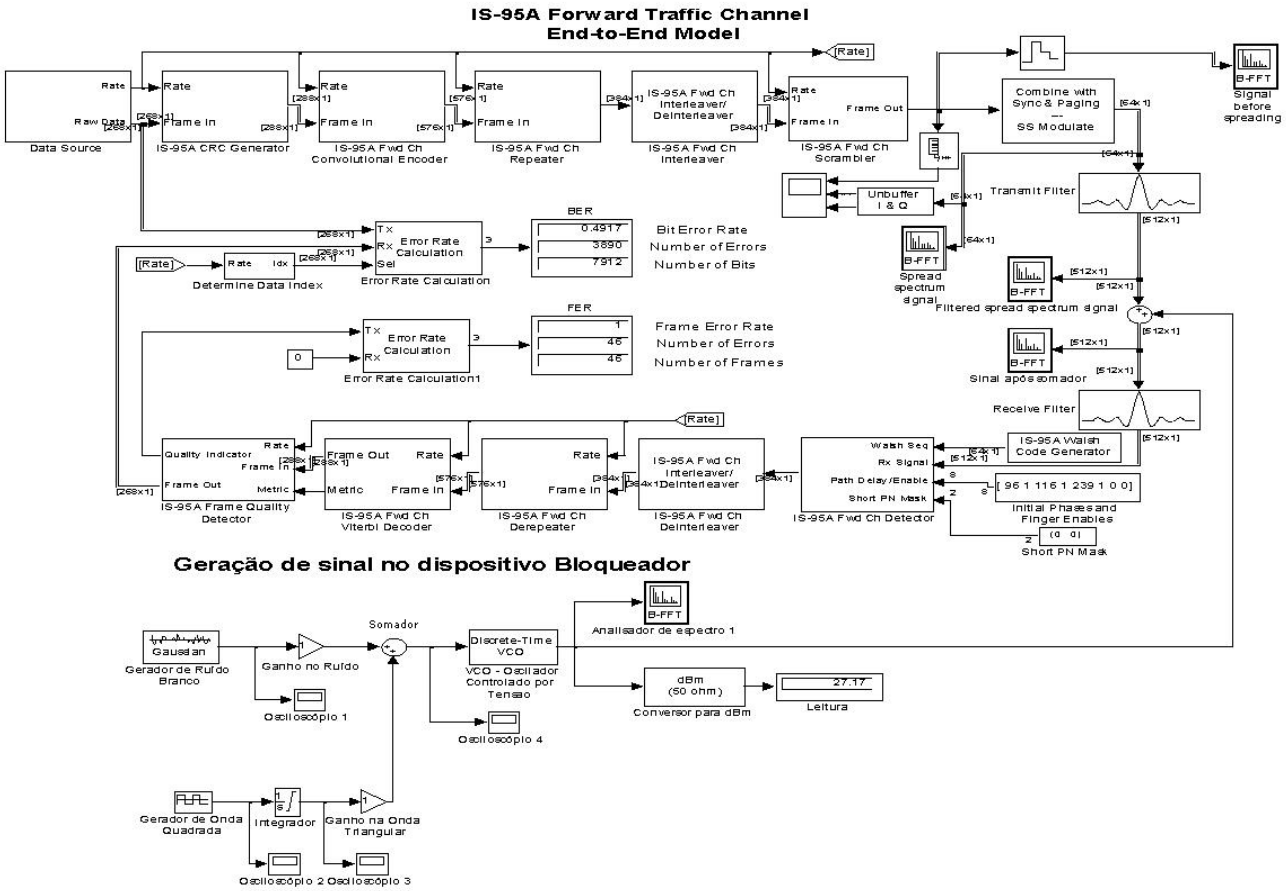

Fig. 3. Diagrama em blocos do circuito simulado.

A Tabela I apresenta os resultados de uma rodada de simulação para diversos valores de *J*, mantendo-se *S* constante. Para valores de *J/S* menores que 18,39 dB, o sistema não indicou a ocorrência de bits e quadros com erro. A partir desse patamar, começaram a surgir valores não nulos de BER e FER nos medidores, caracterizando assim uma degradação na qualidade do sinal imposta pela presença do bloqueador. O aumento da quantidade de bits e quadros errados acompanhou diretamente o aumento da relação *J/S*. Uma observação interessante é que para valores muito maiores de *J/S* (por exemplo, *J/S* = 32 dB), o valor da BER se aproximou de 0,5, ou seja, os bits 0 e 1 eram igualmente prováveis (probabilidade de 0,5).

TABELA I
RESULTADOS OBTIDOS NA SIMULAÇÃO

Teste	J (dBm)	S (dBm)	J/S (dB)	BER	FER
1	7	-7	14	0	0
2	8,57	-7	15,57	0	0
3	9,26	-7	16,26	0	0
4	9,53	-7	16,53	0	0
5	9,78	-7	16,78	0	0
6	10,27	-7	17,27	0	0
7	11,39	-7	18,39	0,00083	0,03571
8	11,49	-7	18,49	0,00083	0,03571
9	11,59	-7	18,59	0,00083	0,03571
10	11,70	-7	18,70	0,00083	0,03571
11	11,80	-7	18,80	0,00726	0,07143
12	11,89	-7	18,89	0,00726	0,07143
13	12,37	-7	19,37	0,01391	0,1786
14	13,26	-7	20,26	0,03447	0,3214
15	14,07	-7	21,07	0,1136	0,5714
16	14,80	-7	21,80	0,2245	0,7500
17	15,48	-7	22,48	0,2747	0,8214
18	16,11	-7	23,11	0,3167	0,8929
19	16,70	-7	23,70	0,3617	0,9286
20	17,25	-7	24,25	0,4007	0,9286
21	17,77	-7	24,77	0,4286	0,9643
22	18,25	-7	25,25	0,4387	0,9643
23	18,72	-7	25,72	0,4458	0,9643
24	19,16	-7	26,16	0,4523	0,9643

Vale mencionar que os resultados da Tabela I não podem ser considerados como absolutos, pois o circuito no Simulink incorpora o comportamento estatístico esperado para o problema durante a realização das simulações. Com isso, uma pequena diferença pôde ser observada nos resultados em função da variação do tempo de duração das simulações (contador do próprio sistema). Para possibilitar uma maior homogeneidade nos resultados apresentados, o tempo de duração de cada evento de simulação foi o mesmo (T = 0,620). O total de bits e quadros correspondentes a essa duração foi de 4816 e 28, respectivamente. No geral, diferentes rodadas de simulações apresentaram valores compatíveis com os da rodada correspondente à Tabela I.

III. TESTES EXPERIMENTAIS DO PROTÓTIPO

A. Descrição do protótipo

A Fig. 4 apresenta a topologia do dispositivo bloqueador implementado, para inserção de ruído em uma única banda de freqüências. Os nomes dos módulos do circuito correspondem às suas funções no bloqueador [5].

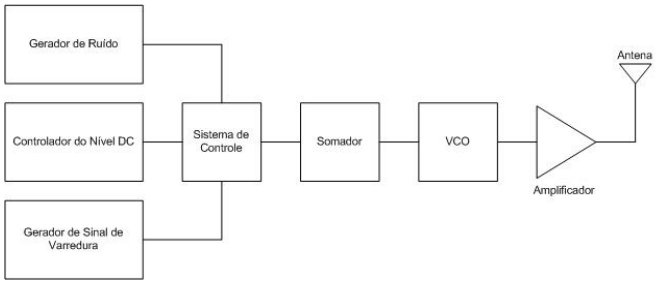

Fig. 4. Diagrama em blocos do dispositivo bloqueador implementado.

B. Testes realizados

O conceito do bloqueio sobre o sistema de telefonia móvel celular CDMA (IS-95) foi testado com um terminal CDMA (telefone comercial), marca ZTE, modelo C133.

No sistema CDMA, definido na norma IS-95, existe a designação de duas portadoras chamadas de "primária" e "secundária", as quais são utilizadas pelo terminal móvel para acesso inicial ao sistema. Essas portadoras são vitais no processo de aquisição do sistema por parte do móvel. Depois do acesso inicial, caso exista alguma outra portadora disponível na célula, o móvel pode receber a sinalização para trocar de portadora. Por designação da IS-95, as portadoras primária e secundária da banda A correspondem aos canais 283 e 691, respectivamente [2].

Para fins de validação da eficácia do bloqueador, foi feita a inserção do sinal de bloqueio, com uma largura de banda de 1,23 MHz, somente sobre a portadora primária (canal 283, 878,49 MHz). Neste caso, considerando-se a sensibilidade à variação de voltagem de sintonia do VCO utilizado, de 21 a 36 MHz/V, não foi necessária a utilização do efeito da varredura em freqüência durante os testes. Com isso, o dispositivo bloqueador com varredura utilizado nos testes passou a operar segundo o conceito de bloqueio com ruído em banda estreita [1], pois atuou somente num canal específico do sistema, sem o efeito da varredura em freqüência.

Como não foi possível obter os parâmetros de cobertura de RF do sinal do sistema CDMA, foi feita a medição dos níveis de potência de recepção deste sinal *S* nas redondezas da Praça General Tibúrcio (Urca – RJ) e, principalmente, nas proximidades do local de realização dos testes (Laboratório de Microondas do IME). Essas medições foram feitas através de um aparelho celular Nokia, modelo 2280, que possui essa facilidade. A ERB responsável pela cobertura está distante 550 metros do local do teste, existindo diversos obstáculos no trajeto do sinal. A antena utilizada pela operadora é do tipo painel e não está apontada para o local de realização do teste. A Fig. 5 apresenta o mapeamento do valor de potência recebida (em dBm) em função do aumento da distância entre a ERB e o aparelho medidor, nas proximidades do IME.

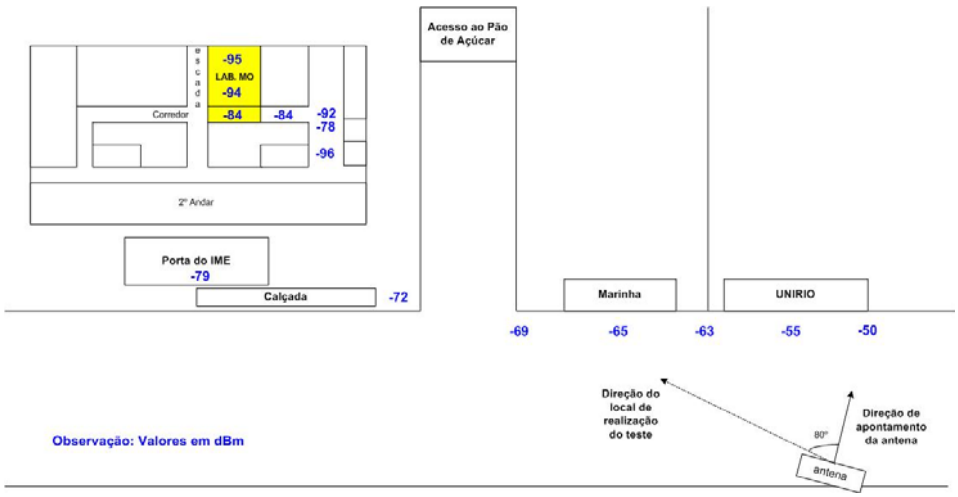

Fig. 5. Mapeamento da potência do sinal da ERB CDMA mais próxima ao IME (valores em dBm).

A área em destaque na Fig. 5 se refere ao local de realização dos testes. Dentro desta área, com o dispositivo bloqueador operando, foi feita também a medição da potência do sinal de bloqueio *J* em alguns pontos (7 pontos dentro do Laboratório e 2 pontos externos ao mesmo, próximos à porta), com a utilização de um analisador de espectro HP8566B. Uma consideração a ser feita é que as medições de *S* e *J* foram feitas por equipamentos distintos, cada qual com sua antena específica, com uma pequena diferença em seus respectivos ganhos, fato este que não comprometeu os resultados conceituais dos testes.

A Tabela II apresenta os resultados das medições de *S* e *J* nos 9 pontos escolhidos, a relação *J/S* de cada ponto, a localização física dos mesmos (interno ou externo ao laboratório) e os resultados da ação do bloqueio. Os valores de *J* relativamente baixos são devidos ao equipamento utilizado para bloqueio, de baixa potência (8,6 dBm).

TABELA II
RESULTADOS DOS TESTES

Ponto / Localização	*J* (dBm)	*S* (dBm)	*J*/*S* (dB)	Resultado
1 / interno	-44,10	-95	50,9	Bloqueio
2 / interno	-51,20	-94	42,8	Bloqueio
3 / interno	-51,50	-94	42,5	Bloqueio
4 / interno	-56,70	-94	37,3	Bloqueio
5 / interno	-59,20	-94	34,8	Bloqueio
6 / interno	-60	-94	34	Bloqueio
7 / interno	-62	-94	32	Bloqueio
8 / externo	-65,50	-84	18,5	Intermitente
9 / externo	-67,3	-84	16,7	Celular operando

O bloqueio foi obtido com êxito dentro do Laboratório de Microondas, onde a relação *J/S* esteve superior à margem de bloqueio de 18 dB. O telefone móvel CDMA não conseguiu efetuar a aquisição do sistema, demonstrando em seu visor a mensagem "procurando serviço". No ponto de medição 8 (externo ao Laboratório), a condição de bloqueio se apresentou de forma intermitente, visto que a relação *J/S* esteve oscilando em valores próximos a 18 dB. No ponto de medição 9 (também externo ao Laboratório), onde a relação *J/S* esteve menor que 18 dB, o telefone móvel efetuou a aquisição normalmente do sistema e tornou-se disponível na rede.

Enquanto o dispositivo bloqueador permaneceu ligado, a condição de bloqueio esteve presente dentro da respectiva área. Poucos segundos após o desligamento do bloqueador, o telefone CDMA conseguiu fazer a aquisição na rede e entrar em operação.

IV. COMENTÁRIOS FINAIS

O presente trabalho apresentou um estudo de caso sobre o efeito de um bloqueador de RF em terminais IS-95, incluindo: a identificação dos aspectos relevantes ao funcionamento do sistema CDMA, a determinação teórica da margem de bloqueio para este sistema, a simulação de um sistema de bloqueio sobre um modelo do sistema CDMA IS-95 em MatLab®, e a avaliação experimental do bloqueio no sistema.

Os resultados teórico, das simulações e prático mostraram boa concordância, indicando que o uso da técnica de bloqueio em um sistema CDMA IS-95 é eficaz quando a relação interferência-sinal *J/S* é superior a 18 dB. Na prática, usou-se a técnica de bloqueio com ruído banda estreita na portadora primária do sistema.

AGRADECIMENTOS

Este trabalho teve o suporte do Departamento de Ciência e Tecnologia do Exército - DCT/EB.

REFERÊNCIAS

[1] R. A. Poisel, *Modern Communication Jamming Principles and Techniques*, Artech House, Inc., 2004.

[2] CDMA Development Group – Welcome to the World of CDMA, disponível em http://cdg.org/technology/cdma_technology/a_ross/cdmarevolution.asp, em 25/11/2005.

[3] D. J. Goodman, *Wireless Personal Communications Systems*, Addison-Wesley Wireless Communications Series, 1997.

[4] M. A. Sturza, Spread Spectrum Techniques and Technology, disponível em http://www.3csysco.com/publications.htm, adquirido em 01/12/2005.

[5] R. S. Toscano, Bloqueador de Múltiplas Freqüências: Concepção do Sistema e Estudo de Caso para Terminais IS-95. Dissertação de Mestrado, IME, 2006.