LTE Privado para Defesa e Segurança Pública no Brasil

Jorge Seki, Juliano Bazzo, Sérgio Barros, Ricardo Takaki, Dick Carrillo

***Resumo*— A tecnologia móvel celular LTE (*Long Term Evolution*) tem sido amplamente utilizada no segmento de Operadoras de Telecomunicações para prover serviços de dados banda larga e de voz. Graças aos avanços tecnológicos em microeletrônica, processamento de sinais e ao contínuo esforço de estudo e padronização de novas funcionalidades realizas pelo 3GPP (*3rd Generation Partnership Project*) e colaboradores, as redes LTE, quando comparadas com redes móveis celulares precedentes, alcançaram ganhos significativos em diversos fatores, como flexibilidade e eficiência no uso do espectro, taxas de transmissão elevadas, simplificação da arquitetura de rede com a convergência para rede "*all*-IP (*Internet Protocol*)" com QoS (*Quality of Service*). Além da flexibilidade e dos ganhos tecnológicos e de capacidade, a disponibilidade e barateamento dos terminais permitiram o surgimento de demandas para aplicação do LTE nos setores de Defesa e Segurança Pública. Apesar de todos os benefícios, contudo, existem restrições de segurança para o uso da tecnologia LTE nestes setores devido às vulnerabilidades da interface aérea do LTE à ataques propositais do tipo *jamming*. Este artigo descreve brevemente a regulamentação da Anatel para o setor de Defesa para, em seguida, abordar a vulnerabilidade da tecnologia LTE aos ataques de *jamming*. Finalmente, são apresentadas propostas de mitigação e respectivos resultados de simulação para uma classe de ataques de *jamming* sem requisitar alterações no padrão especificado pelo 3GPP para a camada física do LTE.**

***Palavras-Chave*— LTE, 3GPP, Defesa, Segurança Pública, *Jamming*, Faixa 698 MHz, Faixa 806 MHz**

I. Introdução

Muitos países já utilizam sistemas LTE para a prestação de serviços considerados de missão crítica [1], tais como em situações de calamidade pública e combate a desastres naturais, ou em situações de colapso da infraestrutura de comunicação básica e em eventos com concentração elevada de pessoas. Para tal, utilizam infraestruturas de Operadoras de Telecomunicações. Contudo, há cenários de missão crítica em que o uso de Operadoras como solução principal de fornecimento de comunicação não é adequada, pois não há garantia de disponibilidade de serviço, nem de robustez contra ataques propositais em ambiente hostil. No Brasil, o setor de Defesa reconhece a necessidade de avanços tecnológicos na comunicação banda larga Militar e busca evolução em direção à tecnologia LTE [2]. Em outros países, sistemas LTE específicos para uso Militar têm sido desenvolvidos e implantados. Porém, o desenvolvimento nessa direção perde uma das vantagens de sistemas LTE que é a disponibilidade de terminais baratos padronizados. Nesse sentido, uma das preocupações para a expansão do uso do sistema LTE para o setor Militar é a questão regulatória relativa ao uso e compartilhamento do espectro de frequência com o uso comercial [3]. Outra preocupação está relacionada com a segurança e a disponibilidade de serviço. Embora o sistema LTE possua mecanismos de segurança, tais como autenticação de usuário, criptografia e de integridade das informações, há vulnerabilidades na interface aérea que, devido à sua natureza compartilhada, é suscetível à interferências, intencionais ou não. Deste modo, em um cenário de aplicação militar, a interface aérea pode ser alvo de ataques de negação de serviço (*denial of service* - DoS) com implementação simples por meio de técnicas de ataque por *jamming* [3].

Jorge Seki, Juliano Bazzo, Sérgio Barros, Ricardo Takaki e Dick Carrillo, CPqD - Centro de Pesquisa e Desenvolvimento em Telecomunicações, Campinas/SP, Brasil, E-mails: jseki, jbazzo, sbarros, rtakaki, dickm@cpqd.com.br.
Este trabalho foi financiado pelo FUNTTEL.

II. Cenário Regulatório no Brasil

A contextualização desse artigo baseou-se na resolução 625 da Anatel que foi publicada em 2013 [4]. O documento trata da destinação e regulamentação sobre as condições de uso da faixa de 698 MHz a 806 MHz como apresentado na Figura 1. O Bloco 1, 703 MHz a 708 MHz e 758 MHz a 763 MHz, foi destinado para o Serviço Limitado Privado (SLP), em aplicações de Segurança Pública, Defesa Nacional e infraestrutura, em caráter primário. Iniciativas do Exército Brasileiro, como o Projeto SISNACC (Sistema Nacional de Comunicações Críticas) [6][7], já contam com a utilização desse segmento do espectro.

O Projeto SISNACC tem como objetivo a implantação de uma rede de comunicação móvel de abrangência nacional para as forças armadas e instituições de Segurança Pública, contando com o compartilhamento, por diversas entidades governamentais, de uma infraestrutura de Rede LTE operando na faixa de 700 MHz. Esta é uma iniciativa de grande relevância estratégica para os setores de Defesa e Segurança Pública do país.

Quanto aos demais blocos, estes foram designados pela ANATEL para o Serviço Móvel Pessoal (SMP), tendo sido objeto de licitação da ANATEL de 2014 [5]. São dois segmentos de 40 MHz para canalização FDD, sendo alocados canais de 10 MHz para cada operadora.

III. Cenário Militar e Segurança no LTE

Existem muitas técnicas de ataque por *jamming* visando a interrupção da comunicação em redes sem fio com variados graus de complexidade de implementação [3], [9]. Foram reportadas na literatura, por exemplo, classes de *ataques proativos*, em que o agressor, após detectar o alvo, ataca-o de forma espontânea e constante, o que permite fácil detecção

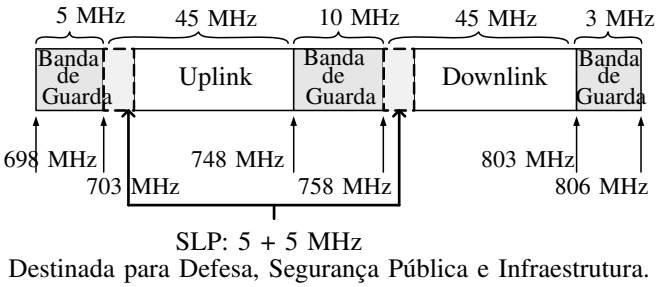

Fig. 1. Canalização conforme Anatel 625/2013 e 3GPP Banda 28.

do ataque. Há também classes de *ataques reativos*, em que o agressor efetua ataque somente quando percebe o sistema alvo ativo, tornando sua detecção mais difícil. Há, ainda, classes sofisticadas de ataque que varrem rapidamente, de forma aleatória e cíclica, os canais de controle do LTE com o intuito de bloqueá-los completamente [3], [10], [11] e, consequentemente, impedir a comunicação dos demais canais por incapacidade de agendamento de recursos de *uplink*. Outras classes são capazes de modificar seu padrão de varredura, dificultando ainda mais sua detecção e a adoção de contramedidas.

Para este trabalho, foram consideradas classes de ataques de *jamming* flexíveis o suficiente para atacar os canais de controle do *uplink* do LTE de maneira constante ou intermitentemente, com ou sem prévia detecção de atividade nesses canais.

IV. Descrição do Experimento

Visando mitigar efeitos danosos decorrentes de ataques por *jamming* em cenários de missões táticas Militares, e simultaneamente, minimizando alterações na padronização do 3GPP referente à tecnologia LTE, são propostas neste artigo duas abordagens baseadas em mudança de canais de transmissão do *Uplink*. Em virtude do cenário e do objetivo, priorizou-se a robustez e disponibilidade em detrimento de eficiência no uso do espectro. Embora dispendiosa, a penalidade em termos de eficiência de espectro foi considerada secundária neste cenário de implantação *greenfield* Militar.

O cenário de simulação está ilustrado na Figura 2, em que uma estação rádio base (eNodeB - *evolved Node B*) equipada com antena omni-direcional é montada sobre um veículo para servir uma tropa composta de 15 soldados, cada qual equipado com um terminal LTE e câmera de vídeo para possibilitar a transmissão de *streaming* de vídeo para uma *Central de Comando*. O sistema LTE veicular foi escolhido para operar na banda 28 FDD (*Frequency Division Duplex*) e possui 9 canais de 5 MHz disponíveis para transmitir o *Uplink*. Um canal de 5 MHz é fixado para *Downlink*. O raio de cobertura da eNodeB veicular foi planejado para cobrir 3 km, e o sistema LTE instalado no veículo é capaz de detectar ataques de *jamming* utilizando sistema WIDS (*Wireless Intrusion Detection System*) utilizadas em outras redes como WiFi [12]. Essa funcionalidade foi considerada embarcada em um sistema de gerenciamento e configuração automática SON (*Self Organizing Networks*).

O inimigo, oculto na vizinhança da eNodeB, possui uma antena direcional e potência suficiente para bloquear plenamente a recepção da eNodeB se este concentrar sua potência na faixa de 5 MHz do *Uplink* da eNodeB. Por isso, adotou a estratégia de atacar os canais de controle no *Uplink* da estação de rádio base pois constitui um só alvo, mais fácil de monitorar e atacar com potência concentrada.

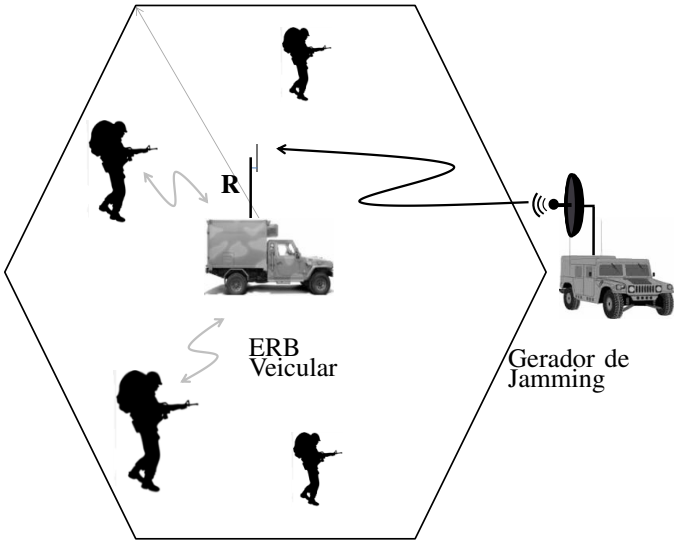

Fig. 2. Cenário de Simulação.

A. Descrição da Proposta de mitigação

Para mitigar os efeitos de ataques por *jamming* no referido cenário, e com os canais disponíveis, duas estratégias são sugeridas neste artigo. A primeira abordagem sugerida, denominada de *Estratégia de Reconfiguração da Frequência de Célula*, é a mudança de faixa de *Uplink* da eNodeB para outra faixa de frequência assim que o ataque tenha sido detectado. A segunda abordagem sugerida, denominada de *Estratégia de Salto em Frequência*, disponibiliza diferentes canais ou subportadoras de operação para o sistema de RF (*Radio Frequency*) da eNodeB e um mecanismo de salto com padrão pseudo-aleatório entre subportadoras para comutar o uso desses canais, ou seja, uma espécie de salto de frequência em subportadoras.

1) Estratégia 1: Reconfiguração da Frequência de Célula: Esta abordagem adota a estratégia de reconfigurar a célula para uma outra faixa de frequência sempre que a eNodeB concluir que está sofrendo ataque por *jamming*. Em virtude da necessária reinicialização da célula, o terminal precisa repetir os procedimentos de busca da célula e de conexão com a eNodeB (procedimento de *attach*), impossibilitando os UEs (*User Equipments*) de se comunicarem por um tempo considerável que pode resultar na interrupção de sessões de aplicação.

Para elucidar a operação da eNodeB nesta estratégia, suponha que o inimigo monitore o espectro, detecte e ataque o *Uplink* da eNodeB veicular. Diante do consequente aumento das medidas de erro de transmissão no canal de controle e da incapacidade de decodificar esses canais, o Controlador SON declara que a eNodeB está sob ataque de *jamming* e efetua o procedimento de reconfiguração das faixas de frequências de *Uplink* e *Downlink* da eNodeB, através das seguintes ações:

1) Pelo PDSCH (*Physical Downlink Shared Channel*) a eNodeB envia um comando para desconexão dos terminais

e parâmetros para a escolha das novas frequências de transmissão e recepção.
2) A eNodeB seleciona as configurações de enlace com as quais ela irá subir após a reinicialização.
3) A eNodeB reinicializa.
4) A eNodeB opera com a nova configuração de enlace e a célula é ligada.
5) Os terminais começam o processo de busca da célula e conexão na eNodeB.

O tempo decorrido entre as ações 4 e 5 pode se estender por muitos segundos, período em que os terminais ficam incapazes de estabelecer comunicação com a *Central de Controle* e que pode resultar em interrupção da sessão de aplicação.

2) Estratégia 2: Salto em Frequência: Nesta abordagem, a eNodeB conta com uma série de subportadoras de RF para modulação do *Uplink* (nas simulações, foram consideradas de 2 a 9 subportadoras) e pode saltar entre essas subportadoras segundo um padrão pseudo-aleatório combinado com os terminais e, assim, evitar o ataque. Esta abordagem não requer reinicialização da célula mas, somente circuitos comutadores de RF, ou comandos de reconfiguração, tanto na Estação de Rádio Base quanto nos terminais. Desta forma, esta abordagem elimina a penalidade de interrupção de serviço para busca e conexão a cada ataque detectado.

Um intervalo mínimo para decidir o salto poderia ser fixado para ser a cada TTI (*Transmission Time Interval*), embora períodos mais longos, da ordem de dezenas ou centenas de TTI, possam ser escolhidos. Contudo, quanto menor for o intervalo para a decisão de salto, menos tempo o inimigo terá para efetuar o *jamming* de forma contínua. Por outro lado, o LTE possui mecanismos de retransmissão automática HARQ (*Hybrid Automatic Repeat Request*) que podem impedir ou minimizar a perda de comunicação dentro de um quadro inteiro, isto é, caso o ataque ocorra de forma contínua dentro de um período menor que a duração de um quadro LTE. Assim, a escolha de um intervalo mínimo de 10 milissegundos (ou 1 quadro LTE) pareceu razoável.

Um fator importante nesta estratégia de saltos de frequência é a sincronização do padrão de saltos entre a estação de rádio base e seus terminais conectados. A sequência que determina o padrão de saltos pode ser preestabelecida ou ser atualizada, através do PDSCH, no início da missão tática Militar. O mecanismo de detecção de ataque presente no controlador SON permite a eNodeB descartar canais que tenham sidos identificados como estando sob ataque e, dessa forma, prover novas configurações de padrões de salto excluindo os canais sob ataque. Esta abordagem não contém a penalidade temporal relacionada com reinicialização, busca e conexão para o terminal, nem a penalidade implícita de interrupção de serviço decorrente da reinicialização.

A Figura 3 representa uma operação segundo a abordagem de salto em frequência, ilustrando saltos entre três subportadoras: f_{c_1}, f_{c_2}, e f_{c_3} que são, respectivamente, subpordadoras centrais dos canais C_1, C_2 e C_3. A sequência de saltos ilustrada começa na subportadora f_{c_2} e, no período de um quadro LTE, salta para a subportadora f_{c_3} para, após o período de outro quadro LTE, saltar para subportadora f_{c_1}, onde sofre ataque por *jamming*. Ela permanece sob ataque na f_{c_1} pelo período de um quadro LTE onde saltará para uma outra portadora prevista em sua sequência pseudo-aleatória de saltos.

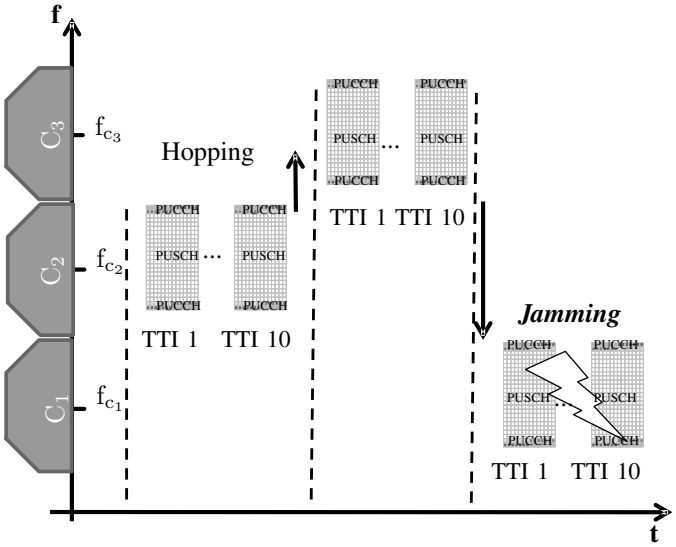

Fig. 3. Comunicação no *Uplink* utilizando salto em frequência.

B. Simulação do LTE e Jamming

Para simular o ataque foi utilizada uma ferramenta de código fonte aberto NS-3 [13]. Esta ferramenta é utilizada pela comunidade acadêmica e por desenvolvedores para realização de testes e simulações de redes de diferentes tecnologias. Em particular, para o sistema LTE, os seus elementos foram baseados no módulo LENA NS-3 que foi desenvolvido para simular redes LTE e possui representação em código C++ dos principais elementos que compõem uma rede LTE, tais como a eNodeB, o núcleo da rede de pacotes (EPC - *Evolved Packet Core*), e os terminais. Adicionalmente, este pacote contém modelos 3GPP de simulação de canais, mobilidade, controle de potência, canais de dados e de controle, e outros aspectos relevantes para uma simulação razoável de uma rede LTE.

O cenário de simulação é baseada na Figura 2 utilizando as configurações mostradas na Tabela I, que resume parâmetros específicos de cada estratégia. O pelotão é servido por uma eNodeB (montada em veículo) responsável por irradiar o sinal LTE para todas as direções. O inimigo tem uma antena direcional com um feixe focado na tentativa de bloquear totalmente a recepção do canal de controle do *Uplink* da eNodeB, após τ_1 milisegundos. Este período é baseado no número máximo de retransmissões HARQ. Após este tempo, a eNodeB remove o terminal e o processo de reconexão é iniciado. O protocolo LTE é desenvolvido para manter a conexão estabelecida para este período mesmo com a presença de forte interferência. Para a *Estratégia 2*, o mesmo valor τ_1 foi utilizado para período de salto em frequência. O ataque de *jamming* adota a estratégia de focar um único canal por um longo período pois a probabilidade de obstruir tal canal ou subportadora é maior do que se tentasse acompanhar os saltos da eNodeB, em virtude de a sequência de salto adotada na *Estratégia 2* ser pseudo-aleatória e do fato da eNodeB não monitorar se um canal já se encontra sob ataque, de modo a evitá-lo.

O inimigo escaneia os canais LTE de *uplink* para tentar encontrar a nova frequência de operação da eNodeB. O período de escaneamento é proporcional ao número de canais disponíveis para a *Estrategia 1*, o qual pode ser descrito pela variável aleatória uniforme τ_2. É assumido na *Estratégia 2* que o inimigo não pode rastrear o sinal LTE em um período abaixo de 10 milissegundos, que foi considerado como o tempo necessário para ele varrer o espectro para identificar um sinal LTE, focar os canais de controle do *uplink* e então atacar. A simulação da rede LTE utiliza a variável aleatória τ_3 para representar o período de mudança da eNodeB para um novo canal. Na *Estratégia 1* esse tempo é muito grande devido à célula LTE ser desligada e religada para que o processo de reconexão do terminal inicie de novo. Na *Estratégia 2*, a célula LTE não é desligada nem religada e, portanto, o salto do canal ou da portadora é imediato pois esta troca de célula é baseada em um comando de comutação de RF.

Na simulação os terminais transmitem *streaming* de vídeo para a eNodeB utilizando a banda máxima possível, virtualmente, no limite da capacidade da célula. O vídeo é paralisado quando ocorre o ataque de *jamming* mas a sessão de transporte lógica não é interrompida, de modo que o ataque não adiciona qualquer atraso significante ao sistema. A vazão de *Uplink* da célula é medida no final das simulações de cada estratégia, sendo os resultados obtidos e comparados. Cada simulação é composta por 10 repetições de 5 minutos cada. A banda FDD 28, do 3GPP, (APT 700 MHz) utilizada nas simulações é composta por nove canais de 5 MHz de banda cada, que podem ser utilizados para prover comunicação para áreas remotas tais como fronteiras ou também para propósito Militar.

C. Resultado e análise das simulações

A Figura 4 mostra a taxa de *Uplink* da célula com variação de 2 a 9 canais/bandas disponíveis, normalizada com o cenário livre de *jamming*. A vazão da célula é obtida como a soma de todas as vazões individuais de cada terminal. Verifica-se que o desempenho da *Estratégia 1* é bem inferior ao da *Estratégia 2*, especialmente devido ao atraso das mudanças de frequências que penaliza a transmissão por vários segundos. A *Estratégia 2* tem um desempenho 50% melhor do que a primeira estratégia. Este desempenho diminui a medida que o número de canais disponíveis diminui. Por outro lado, o cenário com 9 canais perde apenas 1 de 9 quadros, obtendo-se a vazão simulada no valor de 80% em comparação com o cenário livre de *jamming*.

As Figuras 5 e 6 apresentam os *bytes* recebidos sobre o tempo de amostragem para uma quantidade de canais/bandas de 2 e 9 respectivamente. A *Estratégia 1* trabalha como uma chave liga/desliga e no período desligado todos os *bytes* são perdidos com o *jamming*, existindo uma transição entre os estados devido ao processo de *attach* dos terminas e, como esperado, existem muito mais transições com o decréscimo das bandas disponíveis. Para a *Estratégia 2*, os saltos ocorrem de forma pseudo-aleatória tendo-se uma amostra de 150 *frames* LTE os quais nunca são bloqueados totalmente pelo *jamming* na recepção da eNodeB. Assim, não sendo percebida as mesmas transições da *Estratégia 1*, e como esperado, os *bytes* recebidos diminuem conforme ocorre o decréscimo dos canais disponíveis.

TABELA I
PARÂMETROS DO CENÁRIO DE SIMULAÇÃO

#	Parâmetro	Valor
1	Banda 3-GPP	28
2	Frequência	703 – 748 (*Uplink*) 758 – 803 (*Downlink*)
3	Largura de banda	5 MHz
4	Número de canais de 5 MHz na faixa 28	9
5	Número de células	1
6	Distância máxima do pelotão para eNodeB (raio da célula)	R=3 km
7	Tamanho do pelotão (Número de terminais)	15
8	Tipo de antena da estação veicular	OMNI OMNI
9	Período de *jamming* para derrubar a célula	$\tau_1 = 150$ ms
10	Período de varredura para *jamming* em c canais	$\tau_2 = U(3, 7c/2)$ s
11	Período de Mudança de frequência da Rede LTE	Cenário 1: $\tau_3 = U(10 - 20)$ s Cenário 2: 0 ms (instantâneo)

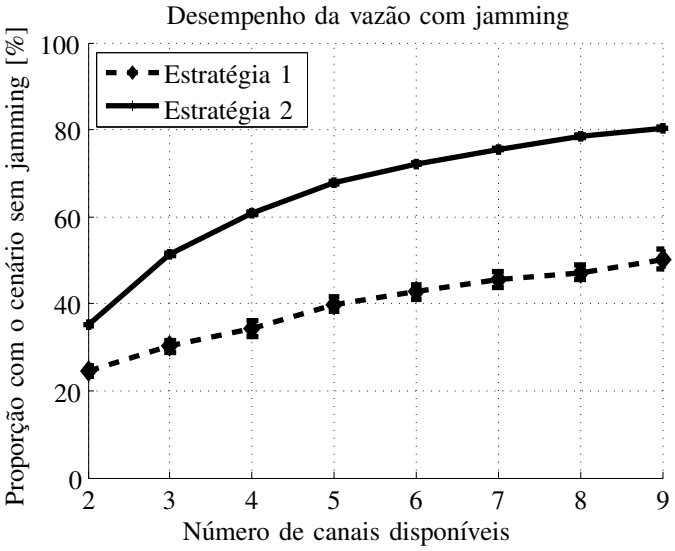

Fig. 4. Bytes recebidos no período de simulação na camada PDCP *Packet Data Convergence Protocol* e com 2 canais/bandas disponíveis.

V. CONCLUSÕES

Este artigo apresenta um estudo do uso do sistema LTE em setores de Defesa e Segurança Pública e estuda as vulnerabilidades do sistema LTE a ataques de *jamming*, com apresentação de duas estratégias para mitigar os efeitos de degradação de desempenho de sistemas LTE devido à este tipo ataque. A primeira estratégia com uso de reconfiguração de frequência da célula e, a segunda estratégia com o uso de salto em frequência. As simulações destas duas estratégias mostraram que as propostas são efetivas para mitigar os ataques de *jamming* e são capazes de manter ativa a comunicação. Nas simulações, a *Estratégia 1* apresentou degradação na capacidade de vazão de dados maior do que a *Estratégia 2* devido às penalidades subjacentes em termos de tempo de procedimento de busca da célula, acesso aleatório e reconexão dos terminais, pois na *Estratégia 1*, o ataque por *jamming* força a reconfiguração da célula em outra faixa de frequência

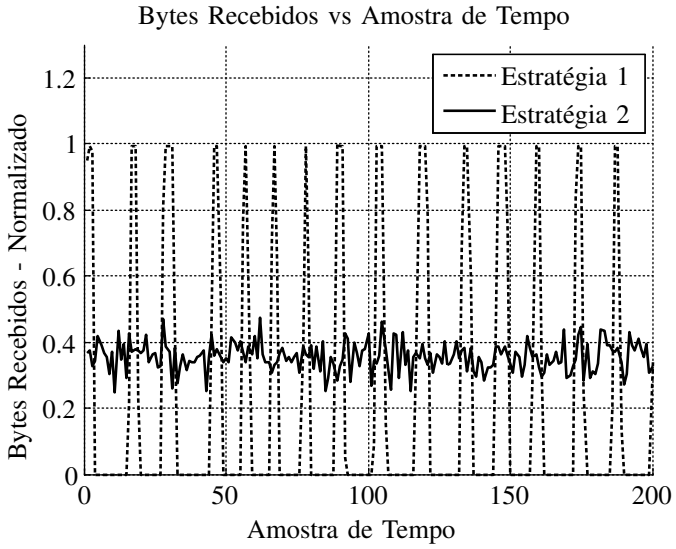

Fig. 5. Bytes recebidos no período de simulação na camada PDCP e com 2 canais/bandas disponíveis.

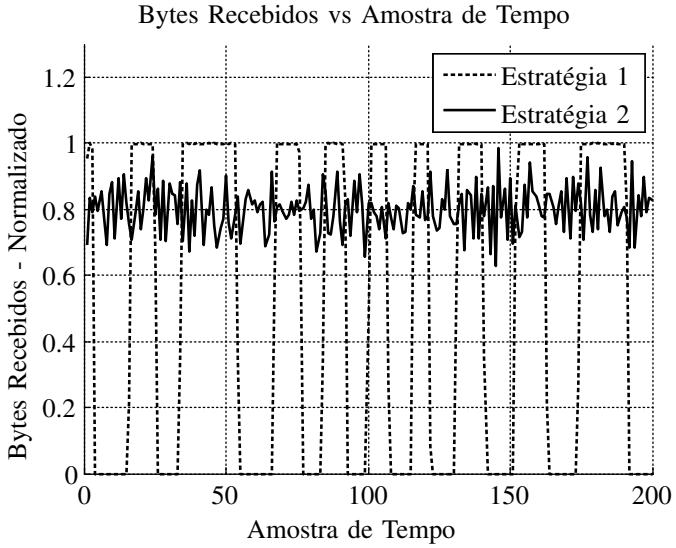

Fig. 6. Bytes recebidos no período de simulação na camada PDCP e com 9 canais/bandas disponíveis.

disponível o que leva a um operação de liga/desliga da eNodeB ao longo do tempo. Já a *Estratégia 2*, ao utilizar saltos em frequência, torna a eNodeB imune às penalidades temporais associadas à *Estratégia 1*. À medida que aumenta o número de canais disponíveis para salto, os efeitos de retransmissão decorrentes de ataques de *jamming* são reduzidos.

A *Estratégia 2* simulada não excluiu o canal atacado dentro das opções de salto, de modo que em sua sequência de saltos os terminais ainda consideram o salto para o canal atacado. Assim, o desempenho da *Estratégia 2* poderia ser melhorado nas simulações se o canal atacado fosse eliminado da sequência pseudo-aleatória de saltos a ser atualizada para os terminais através do PDSCH. Deste modo, a *Estratégia 2* tornaria-se imune à ataques em canais fixos. Logicamente, os canais eliminados precisariam ser monitorados pela eNodeB para serem incluídos na sequência de saltos novamente caso o ataque a esses canais seja interrompido. Embora o desempenho em termos de robustez ao ataque por *jamming* tenha sido satisfatório, uma restrição relacionada com a *Estratégia 2* é o uso dispendioso do espectro. Uma proposta para melhorar o uso do espectro de frequência seria distribuir os blocos de recursos dos terminais entre todos os canais ou subportadoras disponíveis e prover sequências pseudo-aleatórias de saltos diferentes para diferentes terminais. Contudo, esta abordagem aumentaria a complexidade do escalonador da eNodeB ou da escolha dos padrões de salto para impedir as colisões de recursos de transmissão dos terminais durantes seus saltos.

AGRADECIMENTOS

Este trabalho contou com o suporte financeiro do Ministério Brasileiro de Comunicações através do FUNTTEL/FINEP 01.12.0481.00.

REFERÊNCIAS

[1] S. Forge, R. Horvitz and C. Blackman, “Is Commercial Cellular Suitable for Mission Critical Broadband?”, A study prepared for the European Commission DG Communications Networks, Content and Technology by: SCF Associates LTD. European Union, 2014.

[2] J. Andrusenko, J. L. Burbank, and F. Ouyang, “Future Trends in Commercial Wireless Communications and Why They Matter to the Military”, Johns Hopkins APL Technical Digest, Volume 33, Number 1 (2015).

[3] T. C. Clancy, M. Norton, M. Lichtman, “Security challenges with LTE-advanced systems and military spectrum”, Military Communications Conference, MILCOM 2013-2013 IEEE, 375-381, 2013.

[4] Agência Nacional de Telecomunicações, “Resolução nº 625, de 11 de novembro de 2013” http://www.anatel.gov.br/legislacao/resolucoes/2013/644-resolucao-625

[5] Edital Licitação Nº 2/2014 ”Radiofrequências na Faixa de 700 MHz”, ANATEL, Set-2014.

[6] Sitio defesanet, “SISNACC integrará sistema de comunicações críticas”, 16-Abr-2015, http://goo.gl/Pw8mCK

[7] Sitio Progeto, “Progeto participa da implantação de sistema estratégico para a segurança nacional“, Jan-2015, http://www.progeto.com.br/2015/01/

[8] ”LTE Networks for Public Safety Services”, http://goo.gl/UB6VSQ.

[9] K. Grover, A. Lim, Q. Yang, “Jamming and Anti-jamming Techniques in Wireless Networks: A Survey”, International Journal of Ad Hoc and Ubiquitous Computing archive Volume 17 Issue 4, December 2014, Pages 197-215.

[10] J Kakar, K McDermott, V Garg, M Lichtman, V Marojevic, JH Reed, “Analysis and Mitigation of Interference to the LTE Physical Control Format Indicator Channel”, Military Communications Conference (MILCOM), 2014 IEEE, 228-234, 2014.

[11] M Lichtman, T Czauski, S Ha, P David, J H Reed, “Detection and Mitigation of Uplink Control Channel Jamming in LTE”, Military Communications Conference (MILCOM), 2014 IEEE, 6-8 Oct. 2014, 1187-1194.

[12] K Hutchison, “Wireless Intrusion Detection Systems”, GIAC Security Essentials Certification (GSEC) Practical Assignment Version 1.4c, SANS Institute 2005.

[13] N. Baldo, “The ns-3 LTE module by the LENA project”. [Online]. Available: https://www.nsnam.org/ tutorials/consortium13/lte-tutorial.pdf