Um Modelo Analítico para Avaliação de Desempenho em Redes de Rádio Cognitivo Sob Ataque EUP

Julio Soto, Robson Melo, Aldri Santos, Michele Nogueira

[1]Departamento de Informática - NR2
Universidade Federal do Paraná (UFPR)
Caixa Postal 19081 - Curitiba - PR - Brasil

{jchsoto,rgmelo,aldri,michele}@inf.ufpr.br

Abstract. *The inefficient use of the frequency spectrum has motivated the development of Cognitive Radio Networks. These networks have cognitive abilities and manage the frequency spectrum, resulting in its better use. However, cognitive radio networks are vulnerable to different threats, being Primary User Emulation (PUE) attacks the most distinguishing among them. Such attacks easily destabilize the network, impacting its performance. This paper presents an analytical model designed to assess the performance of cognitive radio networks under PUE attacks. The model is based on queuing theory and was validated by experimentation under different scenarios, using throughput as the main metric. Analyses applying the model show that cognition can improve network throughput, even under PUE attacks.*

Resumo. *A ocupação ineficiente da banda espectral tem motivado os avanços e o desenvolvimento das Redes de Rádio Cognitivo (RRCs). Estas redes possuem a inerente capacidade de gerenciar o espectro de frequência, resultando no seu melhor aproveitamento. Entretanto, as RRCs são vulneráveis a diferentes tipos de ameaças, incluindo os ataques de Emulação de Usuário Primário (EUP). Tais ataques desestabilizam a rede, comprometendo seu desempenho. Este trabalho apresenta um modelo analítico concebido para avaliar o desempenho das RRCs diante de ataques EUP. O modelo tem como base a teoria de filas e foi validado considerando experimentos em diferentes cenários, utilizando a vazão como métrica principal. Os resultados de análises aplicando o modelo mostram que cognição pode melhorar a vazão, mesmo na presença de ataques EUP.*

1. Introdução

Tradicionalmente, o espectro de frequências tem sido alocado por agências regulatórias, como a ANATEL (Agência Nacional de Telecomunicações) no Brasil e a FCC (*Federal Communications Commission*) nos Estados Unidos, de forma estática e ineficiente [Anatel 2009]. Todas as frequências abaixo de 3 Ghz são atribuídas a serviços específicos através de licenças, gerando a escassez do espectro para suportar novos serviços e aplicações. No entanto, análises recentes demostram que o espectro de frequências é subutilizado, podendo ser melhor aproveitado através do uso de mecanismos oportunistas e cognitivos [FCC 2002, FCC 2003, Sousa et al. 2010].

As Redes de Rádio Cognitivo (RRC) surgem como uma possível solução para resolver o problema de escassez e subutilização do espectro [Tang 2010]. A tecnolo-

gia de rádio cognitivo permite que bandas de frequências não utilizadas possam ser reaproveitadas para aumentar a disponibilidade geral dos dados. As RRCs são compostas por dispositivos (nós) capazes de monitorar e identificar as frequências não utilizadas no espectro (também chamadas de espaços vazios). Com base em medições correntes e em conhecimentos adquiridos através de acontecimentos passados, cada dispositivo pode de forma inteligente reconfigurar os parâmetros de transmissão para aproveitar espaços vazios do espectro [Haro and Giupponi 2010, Mitola and Maguire 1999]. A tecnologia de rádio cognitivo prevê funcionalidades para o gerenciamento do espectro, como sensoriamento, decisão, compartilhamento e mobilidade do espectro [Akyildiz et al. 2008, Cabric et al. 2004, Lee and Akyldiz 2011, Tang and Mark 2008].

Dois tipos de usuários compartilham o espectro em uma RRC, sendo chamados de usuários primários e usuários secundários [Akyildiz et al. 2006]. Os usuários primários possuem licenças de uso das bandas e maior prioridade para acessá-las, enquanto os usuários secundários não possuem licenças, mas podem usar as bandas quando elas estiverem ociosas. Entretanto, os usuários secundários não devem causar interferências à comunicação dos usuários primários [Jin et al. 2009a] e, dessa forma, uma RRC deve constantemente monitorar o meio a fim de detectar a presença de um usuário primário. Nos casos em que um usuário primário é detectado, o usuário secundário deve mudar rapidamente para outro canal (ação chamada de *handoff* de frequência).

As RRCs são vulneráveis a diversos tipos de ataques devido às características do meio de comunicação sem fio [Anand et al. 2008]. Os ataques de Emulação de Usuário Primário (EUP) são os mais peculiares nessas redes, podendo ser gerados por usuários secundários – maliciosos ou egoístas – com o objetivo de maximizar o seu uso do espectro [Chen and Park 2006]. No ataque EUP, um usuário secundário manipula o seu rádio para emular o comportamento de um usuário primário com o objetivo de degradar a oportunidade de compartilhamento do espetro e se beneficiar da prioridade de uso do espectro existente para usuários licenciados. Criar soluções para detectar e punir usuários secundários maliciosos ou egoístas é um dos grandes desafios das RRCs [Jin et al. 2009a, Chen et al. 2008], requerendo uma análise prévia do comportamento da rede diante desse tipo de ataque.

Este trabalho apresenta um modelo analítico que tem como base a teoria de filas para avaliar o desempenho de redes com capacidades de cognição diante de ataque EUP. O modelo utiliza a distribuição de *Bernoulli* para representar as trocas de canais e considera um número finito de canais derivados analiticamente. O modelo é validado realizando comparações com resultados alcançados através de experimentações diante de cenários com e sem ataque EUP. A validação utiliza como métrica principal a vazão, que permite medir a taxa de dados enviados em razão do tempo. Esta métrica é facilmente degradada por interferências causadas por ataques EUP [León et al. 2009].

O modelo analítico e experimentos são utilizados para analisar o desempenho das RRCs diante de ataques EUP. Os resultados obtidos mostram que mecanismos de cognição aplicados no compartilhamento do espectro podem aumentar a vazão da rede em aproximadamente 7,45%, mesmo diante de um cenário com ataques EUP. Tal fato tem como justificativa a redução de interferências causadas pelos ataques. Os resultados também comprovam que cenários cognitivos fazem melhor aproveitamento das faixas de frequências ociosas.

Este trabalho está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados. A Seção 3 explica o funcionamento dos ataques de emulação de usuário primário. A Seção 4 detalha o modelo analítico proposto para verificar o desempenho da rede sob a influência de um ataque. A Seção 5 descreve os cenários de experimentação. A Seção 6 apresenta os resultados e análises realizadas. A Seção 7 conclui o artigo e apresenta as direções futuras.

2. Trabalhos Relacionados

Alguns estudos demonstraram que as RRCs são vulneráveis a interferências e aos ataques EUP [Anand et al. 2008]. Tais vulnerabilidades vêm sendo cada vez mais investigadas devido a sua relevância diante dos processos de sensoriamento, decisão, compartilhamento e mobilidade no espectro [Akyildiz et al. 2008]. Essas vulnerabilidades podem impedir que o maior objetivo das RRCs seja alcançado. Dessa forma, pesquisadores têm feito esforços para desenvolver modelos que facilitem a investigação do impacto dessas vulnerabilidades no comportamento da rede e nas operações de compartilhamento do espectro de frequências. Entretanto, observou-se na literatura que a grande maioria dos modelos voltados às RRCs tratam das interferências nos canais, sem avaliar os efeitos dos ataques EUP ou outros ataques no desempenho da rede.

Hong et al. propõem um modelo analítico para interferências em RRCs [Hong et al. 2008]. No modelo, o autor assume que um usuário secundário é capaz de encerrar sua transmissão se estiver dentro de uma distância R do usuário primário. Assim, verifica-se por meio da função densidade de probabilidade *(PDF)* o impacto que o valor de R tem sobre a interferência no espectro [Hong et al. 2008]. O modelo proposto por Chen et al. também utiliza uma *PDF* para construção de um modelo de interferência [Chen et al. 2010]. A modelagem considera dois casos. O primeiro caso aplica um esquema de controle de potência. O segundo caso utiliza um controle de acesso ao meio, empregando *CSMA/CA* para coordenar a operação de pedidos de transmissão por nós que utilizam a tecnologia de rádio cognitivo. Em ambos os estudos a interferência gerada no espectro não é concebida por um ataque de Emulação de Usuário Primário [Chen et al. 2010].

Entre os trabalhos que modelam ataques em RRCs, Jin et al. apresentam um modelo analítico para ataques *DoS* utilizando a aproximação de *Fenton* e Teste de Rádio Seqüencial de Probabilidade Wald *(WSPRT)* [Jin et al. 2009a]. Os autores também propõem um mecanismo prático para detectá-los. O trabalho de Chen et al. apresenta um modelo de defesa contra ataque EUP [Chen et al. 2008]. Nessa investigação é mostrado que um ataque pode interferir severamente no processo de sensoriamento do espectro e reduzir significativamente a quantidade de canais disponíveis para um usuário secundário legítimo. Nesse trabalho é proposto um esquema de verificação do transmissor, chamado *LocDef*. O esquema proposto analisa se um dado sinal é realmente do transmissor estimando sua localização pelas características de seu sinal [Chen et al. 2008].

O trabalho de Chen et al. apresenta uma modelagem analítica para ataques EUP que adaptam a potência de transmissão a fim de não serem detectados [Chen et al. 2009]. Apesar disso, o foco principal do modelo é mostrar as vantagens da solução proposta. O trabalho realiza uma modelagem da solução tendo como base a variância do sinal como método de detecção. O modelo da solução leva em consideração as características do

canal e não a potência do sinal, que pode ser facilmente emulada pelo atacante. Ao comparar com outros trabalhos [Chen et al. 2008, Jin et al. 2009b, Chen and Park 2006], a solução proposta por Chen et al. apresenta melhores resultados. Porém, as análises não examinam o desempenho da RRC diante desses ataques.

Apesar dos estudos relacionados às redes de rádio cognitivo, trabalhos que propõem uma modelagem analítica visando a avaliação de desempenho das RRCs sob ataques EUP são raros. Os estudos realizados não consideram a teoria de filas como uma possível técnica para modelagem analítica e nem a vazão como métrica relevante para avaliação do desempenho da rede. Apesar dos trabalhos correlatos poderem ser utilizados para examinar o impacto de ataques nas RRC, esses trabalhos não tinham este objetivo como foco principal. Uma outra desvantagem dos modelos existentes é a forma de validação aplicada comparando resultados dos modelos apenas com resultados de simulação.

3. Ataque de Emulação de Usuário Primário

Um ataque de emulação de Usuário Primário (EUP) foi inicialmente apresentado por Chen [Chen and Park 2006]. Este ataque é realizado por *usuários secundários* que manipulam seus rádios forçando suas transmissões a terem comportamentos e características similares às transmissões de usuários primários [Jin et al. 2009a, Chen et al. 2008]. Como os usuários primários possuem licenças para transmissão em determinadas faixas de freqüência espectral, a personificação desses usuários possibilita aos usuários secundários uma transmissão dedicada e sem interferência no canal.

A Figura 1 ilustra o uso do espectro de frequências diante de um ataque de emulação de usuário primário. Na figura, PU representa um usuário primário, SU ilustra um usuário secundário e AT um usuário secundário emulando o comportamento de um usuário primário. Como um usuário primário tem prioridades no uso das frequências licenciadas, um usuário secundário legitimo necessita trocar de frequência caso sua transmissão interfira na transmissão de um usuário primário. A figura ilustra esse comportamento no tempo igual a t_3 e posteriormente no tempo igual a t_6, sendo que neste ultimo a mudança de frequência é provocada pelo ataque.

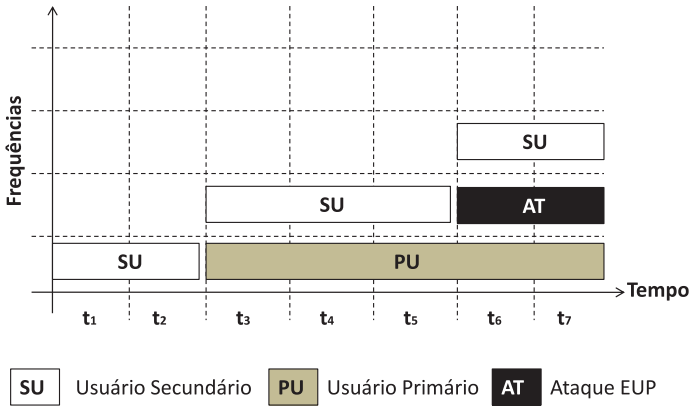

Figura 1. Compartilhamento do espectro de frequência diante de ataque de EUP

Um ataque pode ser gerado por dois tipos de usuários secundários mal comportados: (i) usuário malicioso, que emula o comportamento de um usuário primário com o objetivo de comprometer o funcionamento da rede, e (ii) usuário egoísta, que emula o comportamento de um usuário primário com o objetivo de se beneficiar dos privilégios que este possui e estabelecer uma comunicação exclusiva com outro usuário [Chen and Park 2006]. A ação desses dois tipos de usuários interfere diretamente no processo de compartilhamento do espectro e reduz significativamente os recursos disponíveis para os verdadeiros usuários secundários [Chen et al. 2008].

Os usuários secundários mal comportados podem usar diferentes técnicas para emular o comportamento de um usuário primário. A técnica mais comum para emular um usuário primário considera que os atacantes realizam o sensoriamento do espectro para observar as características de uma transmissão do usuário primário. Através deste sensoriamento, os atacantes conseguem caracterizar a potência e a frequência usadas pelos usuários primários. Em seguida, eles emulam essa potência e frequência a fim de terem privilégios de aceso às frequências licenciadas.

Como contramedidas aos ataques EUP, algumas iniciativas encontradas na literatura buscam detectar e mitigar a existência desses ataques nas RRCs. Dentre estas iniciativas estão os trabalhos de Chen et al. e Jin et al. [Chen et al. 2008, Jin et al. 2009b, Chen et al. 2009]. Sistemas de detecção de intrusão também já foram propostos com o objetivo de detectar a origem do ataque. Esses sistemas em RRC monitoram os dispositivos que possuem mau comportamento detectando os nós suspeitos ou maliciosos. Entretanto, para todos os casos é essencial um bom conhecimento do comportamento dos atacantes e dos efeitos que estes podem ocasionar nas RRCs para propor soluções eficientes. Conhecer bem os efeitos desses ataques auxilia no desenvolvimento de soluções que possam lidar com a degradação dos canais ocasionada pelo bloqueio e redução de uso do espectro pelos usuários secundários legítimos.

4. Modelo Analítico

Esta seção desenvolve um modelo analítico com base na teoria de filas objetivando avaliar o desempenho das RRCs sob um ataque EUP. Consideramos que um primeiro passo para propor soluções de detecção ou prevenção contra ataques EUP seja uma boa análise e conhecimento do impacto desses ataques. Desta forma, este modelo contribui nesta direção. O modelo analisa o desempenho em termos de vazão, haja visto que a vazão é facilmente degradada pelas interferências causadas por ataques EUP.

4.1. Fundamento matemático

Seja E um evento com apenas dois resultados possíveis, sucesso ou fracasso. E pode ser descrito por uma variável aleatória X identicamente e independentemente distribuída (i.i.d.) seguindo a distribuição de *Bernoulli* [Jain 1991]. Para uma variável aleatória X que assume apenas os valores 0 (fracasso) ou 1 (sucesso), p representa a probabilidade de sucesso de E e q representa a probabilidade de fracasso de E com $p + q = 1$. A função de probabilidade de X segue como definida pela Equação 1.

$$P(X = x) = p^x \cdot q^{(1-x)} \tag{1}$$

Desta forma, a Equação 2 define a função de probabilidade para um processo de *Bernoulli* onde uma variável aleatória X é observada n vezes (X_1, X_2, X_3, ..., X_n), com uma quantidade k de sucessos.

$$P(X = k) = \frac{n!}{k!(n-k)!} p^k (1-p)^{n-k} \tag{2}$$

4.2. Hipóteses do modelo

Para o desenvolvimento do modelo analítico, as seguintes premissas foram adotadas:

- O trabalho considera cenários na presença de usuários secundários e de ataques EUP. Os usuários primários não são modelados pois nosso escopo não é avaliar o desempenho do usuário primário, mas sim avaliar a RRC diante dos ataques EUP.
- Os usuários secundários maliciosos possuem um mecanismo para emular o comportamento de um usuário primário.
- Cada nó da RRC é dotado de vários canais, apesar de escolher apenas um canal para transmissão dos dados.
- Quando um usuário secundário malicioso emula um usuário primário, os demais usuários secundários sofrem com interferências medidas através da vazão, forçando-os a realizar uma troca de canal, também chamada de *handoff* de frequência.
- Os nós da rede são dotados de um mecanismo de cognição capaz de verificar o nível de interferência no canal.
- Os nós da RRC implementam um mecanismo de escolha do canal utilizado no momento do *handoff*.
- A presença de um ataque de emulação de usuário primário no canal força trocas de canais pelos nós da RRC.
- O modelo não considera a duração do *handoff*.
- Nos cenários avaliados, um nó chamado de ponto de acesso (*Access Point* – AP) gerencia a troca de canais usados pelos outros nós da rede.
- A quantidade de canais no enlace partindo de um nó para o AP pode ser diferente da quantidade de canais partindo do AP para um nó.
- A troca de canal é modelada através de uma variável aleatória B, onde a probabilidade de trocar ou não de canal é definida pela distribuição de *Bernoulli*. A distribuição considera a vazão do canal quando está acontecendo ou não um ataque, como referência para definir a probabilidade p de ocorrer uma troca.

Dado que em um instante de tempo y cada nó da RRC pode escolher um único canal dentre os disponíveis para transmitir seus dados, a probabilidade de trocas de canal é definida pela Equação 2, onde n é igual ao número de canais disponíveis, k é número de trocas, p representa a probabilidade de trocas e $1 - p$ representa a probabilidade de não ocorrer uma troca. Cada canal disponível é modelado por uma variável aleatória X. Dessa forma, n variáveis aleatórias ($X_1, X_2, X_3, \ldots, X_n$) são observadas em um instante de tempo y, sendo o total de tempo observado igual a T.

A probabilidade p é estimada a partir da presença de um ataque EUP na rede. Se o ataque acontece no canal que está sendo utilizado para transmissão de dados, ele obriga que o usuário secundário mude de canal, então a probabilidade é p. Se o canal

de transmissão não apresenta um ataque ele tem uma probabilidade $1 - p$ na qual não acontece a mudança.

4.3. Modelo de um único canal e de rede

O modelo da rede descrito posteriormente tem como base o modelo de um único canal. O modelo do canal representa um canal utilizado para transferência de dados entre dois nós vizinhos. Um nó é vizinho de um outro quando este encontra-se dentro do raio de alcance do sinal de comunicação de outro nó e quando os dois nós estão utilizando a mesma frequência. Este sinal de alcance é definido pela potência do sinal utilizada pela antena de transmissão/recepção do nó.

O canal utilizado para transferência de dados entre dois nós vizinhos é modelado por uma fila do tipo *M/M/1*. A fila *M/M/1* considera uma chegada de pacotes (em bytes) para transmissão obedecendo um distribuição exponencial representada pelo símbolo λ. Neste modelo, cada pacote é servido pelo canal com uma taxa de serviço μ que também segue uma distribuição exponencial. O modelo tem um único servidor, ou seja, considera apenas um canal, com buffer de tamanho infinito, população de pacotes de chegada de tamanho infinito e cada pacote é servido pelo canal através de uma política do tipo Primeira que Chega, Primeiro que Sai ou *FIFO (First In, First Out)*.

A partir do modelo do canal, o cálculo da vazão é derivado matematicamente por meio da teoria de filas. A vazão é calculada por **enlace**. Entretanto, apenas um canal é escolhido para transmissão de dados em um instante de tempo y. Dessa forma, a carga de pacotes (em bytes) por unidade de tempo indica a taxa de chegada λ no canal, enquanto a taxa de transferência de pacotes (em bytes) por unidade de tempo denota a taxa de serviço μ do canal escolhido para transmissão. A vazão Th é calculada por $Th = \frac{Qd}{T}$, sendo Qd a quantidade total de bytes transferidos de um nó para outro e T o tempo total gasto para completar a transferência. Considerando que j pacotes são transferidos em um intervalo de tempo, a vazão do enlace em bytes é definida pela Equação 3.

$$Th = \frac{Qd}{T} \equiv \frac{\sum_{m=1}^{j} Qd_m}{\sum_{m=1}^{j} T_m} \tag{3}$$

A quantidade total Qd (em bytes) transmitida pelo enlace é dada por $\sum_{m=1}^{j} Qd_m$. Onde a quantidade de bytes em cada pacote é representada por Qd_m. O tempo total T gasto pela transmissão no enlace é dada por $\sum_{m=1}^{j} T_m$. Onde o tempo gasto para transmitir cada pacote é representado por T_m. A transmissão é definida como um conjunto de pacotes (em bytes) referentes a um arquivo. Aplicando o modelo é possível calcular valores generalizados da vazão para cada enlace.

O modelo de rede considera uma situação de troca de dados entre nós gerenciados por um terceiro elemento chamado de *Access Point (AP)* da RRC. O *AP* é o dispositivo que possui técnicas de rádio cognição capazes de controlar a troca de canais e as transmissões na rede. Cada enlace entre o *AP* e um nó, ou entre um nó e o AP, é denotado por E. Sendo que cada enlace possui uma quantidade n de canais.

Deste modo, cada canal segue o modelo descrito anteriormente, e a Figura 2 ilustra um enlace composto de canais entre um nó da RRC e o AP. Dado que cada nó pode

escolher apenas um canal dentre os canais disponíveis em um enlace para transmitir seus dados, a probabilidade de trocas de canal é definida pela Equação 2, sendo k igual a 1.

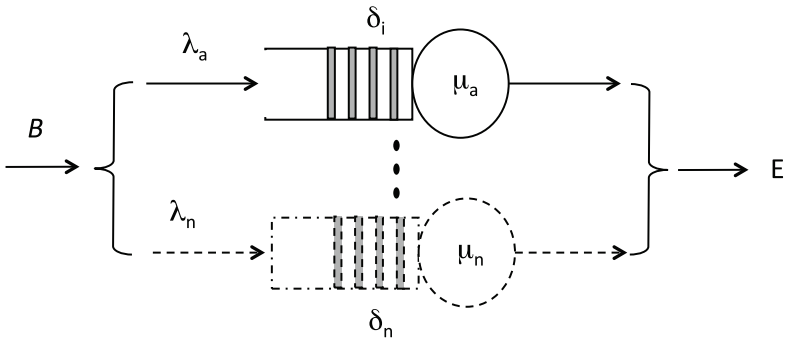

Figura 2. Modelo do enlace

Com base no que foi previamente apresentado, as seguintes definições são derivadas. E_{NAP} é a variável que representa o conjunto de todos os canais que têm origem nos nós em direção ao AP. Esse conjunto é denotado pela união dos canais, ou seja, $E_{NAP} = \bigcup_{i=1}^{n} \delta_i, i = 1, 2, 3, ..., n$. Por outro lado, o conjunto C_{APN} representa todos os canais existentes partindo do AP até um nó, sendo denotado por $C_{APN} = \bigcup_{i=1}^{n} \delta_i, i = 1, 2, 3, ..., n$. Assim, $Q_{CN} = E_{NAP} \bigcup C_{APN}$ representa todos os canais disponíveis entre um nó e outro da rede tendo como mediador o AP. O tamanho, $|Q_{CN}|$, define a quantidade de canais disponíveis entre quaisquer dois nós da rede. Denota-se E como sendo a representação de um enlace sendo este com origem no nó transmissor até o AP ou do AP até o nó receptor. O modelo de rede aplica a Equação 1 sob o conjunto Q_{CN} de canais.

5. Cenários de experimentos

A validação do modelo analítico foi realizada por meio de medição. Os programas AirRadar [Koingo Software 2011] e Finder [Apple 2011] foram utilizados para captura e contabilização dos pacotes enviados e recebidos, além de medir o nível do interferência nos canais do enlace. Os experimentos seguiram os seis cenários descritos a seguir. A Tabela 1 resume os equipamentos utilizados nos experimentos, dispostos de diferentes formas em cada cenário. Esses equipamentos foram escolhidos para representar duas situações. Uma em que a rede possui capacidade de cognição e outra em que a rede não pussui capacidade de cognição.

Equipamento	Descrição
Nó A	MacBook modelo 3.1, Sistema Operacional Mac Os X Leopard
Nó B	MacBook Pro modelo 7.1, Sistema Operacional Mac Os X Snow Leopard
Nó C	HP Pavillon Tx2 touchsmart, Sistema Operacional Windows 7 ultimate
Nó D	Sony Vaio pcg-7d2l, Sistema Operacional Windows XP Service Pack 2
AP - AccessPoint	AirPort Extreme Base Station (802.11n), modelo a1354
Forno Microondas	Samsung modelo SMW 6700W transmitindo sob frequência de 2450 MHz

Tabela 1. Equipamentos utilizados nos experimentos de validação dos modelos

Os nós A e B são usuários secundários e compõem a RRC em conjunto com o AP. Os equipamentos A, B e o AP possuem mecanismos de cognição e troca de canais implementados. Por se tratar de dispositivos que utilizam tecnologias proprietárias, os mesmos

não disponibilizam maior informações sobre os processos cognitivos utilizados. Os nós C e D não possuem mecanismos de cognição ou troca de canais. Estes últimos foram utilizados a fim de comparar o desempenho de um cenário com cognição e um cenário sem cognição. Um forno microondas foi utilizado como um usuário secundário malicioso que emula o comportamento de um usuário primário. Este seguiu um comportamento malicioso controlado pelos autores no momento dos experimentos.

Cenário 1: Os nós A e B conectados diretamente (no mesmo raio de alcance) e dispostos como apresentado na Figura 3. A comunicação entre esses dois nós é feita inicialmente pelo canal 1 a uma frequência de 2.412 GHz. Neste cenário, não se gera interferências de um ataque EUP.

Cenário 2: Neste cenário, os nós C e D também estão conectados diretamente e a comunicação se dá através do canal 1 e frequência 2.412 GHz. Este cenário também não apresenta a ação de ataques EUP e a disposição dos nós também segue a Figura 3. A diferença do cenário 1 para o cenário 2 é a capacidade de cognição dos nós A e B. Os dois cenários são avaliados para posterior comparação em relação aos cenários com presença de ataques EUP.

Cenário 3: Utiliza os mesmos equipamentos e disposição física do cenário 1. Entretanto, a ação de um ataque EUP é gerada através da presença do forno microondas que emula um ataque. O microondas tem prioridade de uso no canal 1 da frequência 2.4 GHz e segue a disposição apresentada na Figura 4.

Cenário 4: Obedece as mesmas características do cenário 3, substituindo os nós A e B, pelos nós C e D.

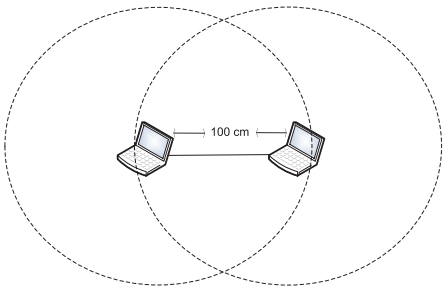

Figura 3. Cenários 1 e 2: disposição dos nós

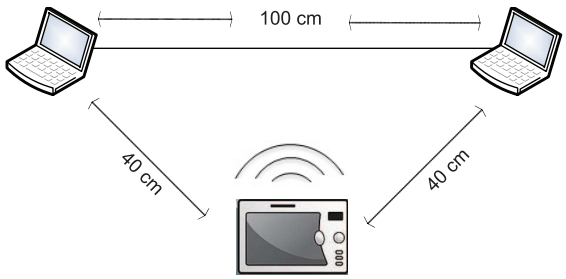

Figura 4. Cenários 3 e 4: disposição dos nós

Cenário 5: Os nós A e B estão conectados por uma rede sem fio gerenciada por um terceiro elemento, o Access Point (AP). O AP cria uma rede para comunicação com 2 canais, o canal 1 na frequência de 2.412 GHz e o canal 36 na frequência 5.18 GHz. Sua disposição segue a ilustração da Figura 5. Neste cenário ações do ataques EUP não são geradas.

Cenário 6: Segue a mesma configuração do cenário 5. Entretanto, a ação de um ataque EUP é inserida através do forno microondas que tem prioridade de usar o canal 1 da frequência 2.4. A disposição física do cenário 6 é representada na Figura 6.

Estes cenários utilizados nos experimentos buscam reproduzir em menor escala um ambiente de rede cognitiva. Deste modo, os nós A, B, C e D representam os usuários

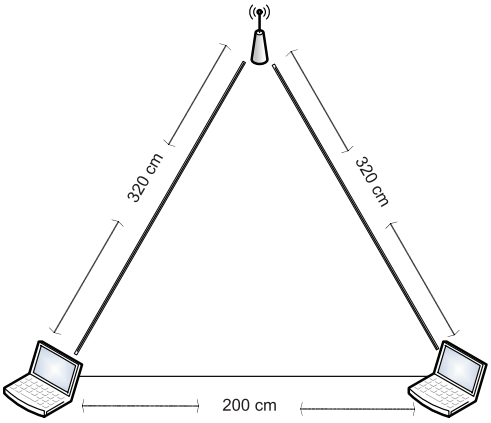

Figura 5. Cenário 5: disposição dos nós

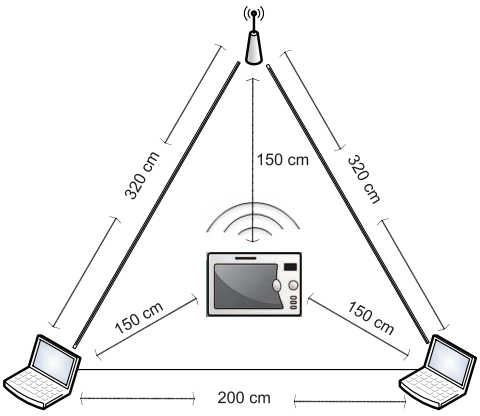

Figura 6. Cenário 6: disposição dos nós

secundários, que aproveitam espaços vazios do espectro, e a ação do forno microondas representa um ataque de emulação de um usuário primário. Quando os usuários secundários estiverem transmitindo dados e o forno microondas for ligado, a transmissão dos usuários secundários deve ter seu funcionamento interrompido, forçando os usuários secundários a mudarem para um canal de frequência diferente para poderem continuar sua transmissão.

A fim de gerar carga para os experimentos, a transmissão de um arquivo de 955 MBytes foi realizada em cada cenário. Nos cenários 1 e 3, o nó A transmite o arquivo para o nó B. Nos cenários 2 e 4, o nó C transmite o arquivo para o nó D. Enquanto nos cenários 5 e 6, o nó A transmite o arquivo para o nó B, passando pelo AP. Os experimentos foram realizados no Departamento de Informática da UFPR, em uma rede isolada para não sofrer interferências de outras redes.

6. Validação dos Modelos e Análise de Desempenho

A Figura 7 apresenta uma comparação entre os resultados alcançados através do modelo analítico e de experimentos para os cenários 1, 2, 3 e 4. Em todos os quatro cenários os resultados obtidos através dos experimentos ficaram bem próximos dos resultados alcançados através do modelo analítico. As comparações tomam como referência a métrica vazão.

A partir dos experimentos verificou-se também que no cenário 1, o nó A levou 7 minutos e 15 segundos para transmissão do arquivo de carga da rede. Durante este tempo o canal de transmissão apresentou baixas taxas de ruído e se manteve constante com uma *vazão* de 2,2 Mbits/seg. Um valor aproximado para a vazão também foi alcançado através do modelo analítico. Particularmente para o cenário 1, o modelo de canal foi utilizado, uma vez que os nós A e B possuem uma comunicação direta.

Através dos experimentos, observou-se que no cenário 2 o tempo gasto para a transmissão do arquivo entre as máquinas C e D teve um aumento de três vezes e meio com relação ao tempo gasto no cenário 1. A vazão no cenário 2 diminuiu em 71.37% em relação ao cenário 1. Este comportamento em relação à vazão também foi observado através dos resultados provenientes do modelo analítico. No cenário 2, também utilizou-se apenas o modelo de canal.

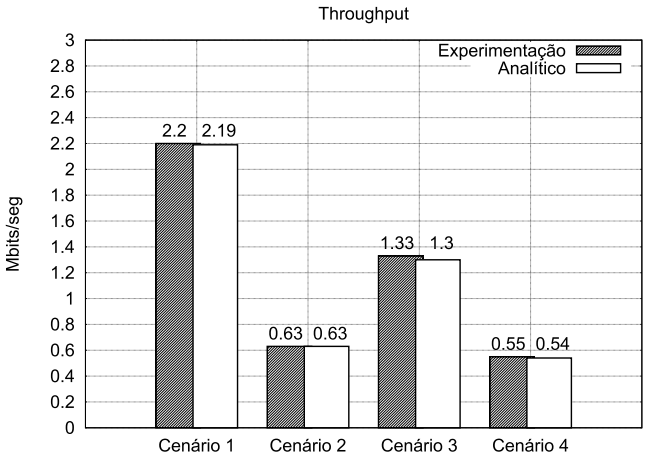

Figura 7. Validação do modelo de canal

No cenário 3, uma configuração idêntica ao cenário 1 é utilizada adicionando a ação do ataque EUP. A partir dos resultados de experimentos, foi possível observar o impacto do ataque EUP na comunicação entre os nós A e B. Quando o atacante inicia sua ação, a taxa de transmissão cai influenciando diretamente no tempo necessário para a transmissão completa do arquivo. O tempo de transmissão teve um aumento de 69,93% no tempo comparado com o cenário 1. Em relação à vazão, uma perda de 39,55% foi observada através dos experimentos. Este comportamento também foi verificado através do modelo analítico do canal. Os valores de vazão alcançados pelo modelo analítico e pelos experimentos ficaram bem próximos.

No cenário 4, uma situação em que a comunicação entre os nós C e D sofre interferência do ataque EUP, o tempo necessário para a transmissão completa dos dados foi o maior em relação a todos os experimentos. O tempo teve um aumento de 15,53% em relação ao cenário 2, que tinha sido o maior tempo de transmissão do arquivo até então. A vazão comparado ao mesmo cenário 2 teve um queda de 12,70% nos experimentos. Um valor aproximado a este também foi alcançado através do modelo analítico.

No cenário 5, com a criação de uma rede com os nós A e B e a comunicação entre eles gerenciada pelo AP sem a interferência de um atacante, foi possível identificar a criação de 2 canais de comunicação pelos nós e AP. Deste modo, através dos experimentos verificou-se que o tempo gasto para a transmissão do arquivo de carga da rede foi de 6 minutos e 59 segundos. Apesar do AP passar a receber os pacotes antes de retransmitilos, a criação de outro canal para transmissão em uma frequência diferente, resultou em um menor gasto de tempo em relação ao cenário 1. A vazão alcançada neste cenário foi de 2,30 Mbits/seg através dos experimentos. O resultado alcançado através do modelo de rede também apresentou um valor de vazão próximo ao valor alcançado pelos experimentos. A Figura 8 apresenta a comparação entre os resultados alcançados por experimentos e pelo modelo analítico.

O cenário 6 sofre o impacto do atacante EUP. Verificou-se através dos experimentos que o tempo gasto para a transmissão do arquivo foi 4,41% menor que o tempo alcançado no cenário 5. Tal comportamento é justificado pela possibilidade de uso dos dois canais disponibilizados pelo AP. A vazão neste cenário teve um aumento de 7,39%

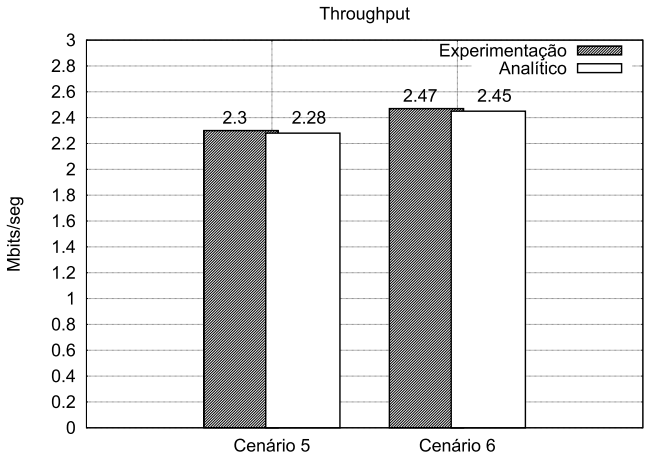

Figura 8. Validação do modelo de rede

quando comparado ao cenário 5. A vazão alcançada através do modelo de rede resultou em um valor aproximado àquele alcançado pelo experimento. Tal resultado é justificado pelo fato do atacante forçar a troca de canal e pelo mecanismo de gerência do espectro implementado no AP.

7. Conclusões

Este artigo apresentou um modelo analítico para avaliação de desempenho de redes de rádio cognitivo (RRC) diante de ataques de emulação de usuário primário (EUP). A tecnologia de rádio cognitivo vem sendo desenvolvida nos últimos anos com o objetivo de ocupar de forma eficiente a banda espectral. Entretanto, apesar das vantagens dessa tecnologia e do uso dela para prover uma comunicação eficiente entre nós de uma rede, usuários maliciosos tentam se beneficiar da prioridade que usuários licenciados têm no uso do espectro. Dessa forma, esses usuários emulam o comportamento de usuários primários a fim de ter acesso ao espectro de forma prioritária.

O modelo está fundamentado na distribuição de *Bernoulli* para definição da probabilidade de trocas de canal. O modelo foi validado comparando resultados gerados por ele e por experimentos. A validação mostrou que o modelo proposto apresenta um nível de precisão entre 97 a 99% em relação aos experimentos. A partir dos experimentos também observou-se o impacto dos ataques EUP no tempo de transmissão e vazão de um arquivo, considerando cenários com e sem cognição. Comparou-se resultados também de cenários com e sem ataques, sendo possível concluir que abordagens como base em cognição e escolha de canal melhoram a vazão de uma rede com a assistência de um equipamento gerenciador do espectro mesmo na presença de ataques EUP.

Como trabalhos futuros, pretende-se utilizar o modelo a fim de realizar mais análises do desempenho da RRC considerando outras métricas importantes como latência. Além disso, o modelo será estendido a fim de considerar características mais detalhadas das redes de rádio cognitivo, tais como controle de acesso ao meio em cenários com mais de dois nós comunicando-se entre si. Espera-se após as análises propor uma solução contra ataques EUP tratando de aspectos relevantes observados.

Referências

Akyildiz, I., Lee, W.-Y., Vuran, M., and Mohanty, S. (2008). A survey on spectrum management in cognitive radio networks. *IEEE Communications Magazine*, 46(4):40 –48.

Akyildiz, I. F., Lee, W.-Y., Vuran, M. C., and Mohanty, S. (2006). Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey. *Computer Networks*, 50:2127–2159.

Anand, S., Jin, Z., and Subbalakshmi, K. (2008). An analytical model for primary user emulation attacks in cognitive radio networks. In *3rd IEEE Symposium on DySPAN, New Frontiers in Dynamic Spectrum Access Networks*, páginas 1–6.

Anatel (2009). Divisão do espectro no brasil, http://www.anatel.gov.br/portal/exibirportalinternet.do. Data do último acesso: 20/12/2010.

Apple (2011). http://support.apple.com/kb/ht2470. Data do último acesso: 02/05/2011.

Cabric, D., Mishra, S., and Brodersen, R. (2004). Implementation issues in spectrum sensing for cognitive radios. In *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*, volume 1, páginas 772 – 776 Vol.1.

Chen, R. and Park, J.-M. (2006). Ensuring trustworthy spectrum sensing in cognitive radio networks. In *SDR 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, páginas 110 –119.

Chen, R., Park, J.-M., and Reed, J. (2008). Defense against primary user emulation attacks in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 26(1):25–37.

Chen, Z., Cooklev, T., Chen, C., and Pomalaza-Raez, C. (2009). Modeling primary user emulation attacks and defenses in cognitive radio networks. In *IEEE 28th International, Performance Computing and Communications Conference (IPCC)*, páginas 208 –215.

Chen, Z., Wang, C.-X., Hong, X., Thompson, J., Vorobyov, S., and Ge, X. (2010). Interference modeling for cognitive radio networks with power or contention control. In *IEEE Wireless Communications and Networking Conference (WCNC)*, páginas 1–6.

FCC, F. C. C. R. (2002). Spectrum policy task force report, no. 02.2135.

FCC, F. C. C. R. (2003). Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies, no. 03.108.

Haro, C. A. and Giupponi, L. (2010). Radio y redes cognitivas. Technical report, AEI eMOV – Plataforma Tecnológica Española de Comunicaciones Inalambricas.

Hong, X., Wang, C.-X., and Thompson, J. (2008). Interference modeling of cognitive radio networks. In *IEEE Vehicular Technology Conference (VTC) Spring*, páginas 1851 –1855.

Jain, R. (1991). *The Art of Computer Systems Performance Analysis*. John Wiley and Sons, 1st edition.

Jin, Z., Anand, S., and Subbalakshmi, K. P. (2009a). Detecting primary user emulation attacks in dynamic spectrum access networks. In *IEEE International Conference on Communications (ICC)*, páginas 2749–2753.

Jin, Z., Anand, S., and Subbalakshmi, K. P. (2009b). Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis esting. *SIGMOBILE Mobile Computing and Communications Review*, 13:74–85.

Koingo Software (2011). http://www.koingosw.com/. Data do último acesso: 30/04/2011.

Lee, W.-Y. and Akyldiz, I. F. (2011). A spectrum decision framework for cognitive radio networks. *IEEE Transactions on Mobile Computing*, 10(2):161 –174.

León, O., Hernández-Serrano, J., and Soriano, M. (2009). A new cross-layer attack to TCP in cognitive radio networks. In *IEEE Second International Workshop on Cross Layer Design (IWCLD)*, páginas 1 – 5.

Mitola, J. and Maguire, G. Q. (1999). Cognitive radio: making software radios more personal. *IEEE Personal Communications*, 6(4):13–18.

Sousa, M., R.F.Lopoes, and W.T.A. Lopes and, M. A. (2010). Redes cognitivas um novo paradigma para as comunicações sem fio. In *Simpósio Brasileiro de Redes de Computadores e Sitemas Distribuídos (SBRC)*.

Tang, S. (2010). Performance modeling of an opportunistic spectrum sharing wireless network with unreliable sensing. In *International Conference on Networking, Sensing and Control (ICNSC)*, páginas 101 –106.

Tang, S. and Mark, B. (2008). Modeling an opportunistic spectrum sharing system with a correlated arrival process. In *IEEE Wireless Communications and Networking Conference (WCNC)*, páginas 3297–3302.