

PROJETO DE REDES

www.projetoderedes.com.br



Universidade Federal Fluminense

TET – Departamento de Engenharia de Telecomunicações

Professor Orientador: Luiz Claudio Schara Magalhães, PhD.

Projeto Final

Medição de *throughput* nas
redes em malha sem fio

Autor: Leonardo Hideki Ishikiryama

Matrícula: 201.41.051-0

Medição de *throughput* nas redes em malha sem fio

Luiz Cláudio Schara Magalhães

Leonardo Hideki Ishikiriyama

Para
meus pais, irmãs, família, e
minha namorada.
Pelo apoio, conselhos, inspiração e
motivação permanente.

Agradecimentos

A realização deste trabalho contou com a ajuda de diversas pessoas, que estiveram envolvidas direta ou indiretamente com ele.

Agradeço,

primeiramente, ao professor Luiz Claudio Schara Magalhães por ter sido o orientador desta monografia e um grande conselheiro profissional;

ao Douglas Vidal Teixeira e ao Diego Passos , por terem dado um grande suporte na realização das medições presentes neste trabalho;

aos meus pais, irmãs, namorada e demais familiares, pelo apoio incondicional não só para a realização deste trabalho, mas para toda minha formação pessoal e profissional.

Resumo

O presente projeto apresenta um estudo sobre alguns dos conceitos, aplicações e mecanismos de funcionamento mais importantes das redes em malha sem fio, baseadas no padrão IEEE 802.11. Também são apresentados valores medidos de *throughput*, relacionados à questão da justiça nessas redes.

Palavras-chave: redes em malha sem fio, redes *mesh*, *wireless mesh networks*, justiça.

Índice

1. Introdução.....	10
2. Introdução às redes em malha sem fio	12
2.1. Redes sem fio	12
2.2. Redes em malha sem fio.....	14
2.3. Aplicações das WMNs	17
2.3.1. Banda larga residencial	17
2.3.2. Segurança pública	18
2.3.3. <i>Hotspots</i>	19
2.3.4. Sistemas de transporte	20
3. O padrão IEEE 802.11 e sua arquitetura básica	22
3.1. Componentes da arquitetura IEEE 802.11	24
3.1.1. Conjunto básico de serviços independentes (IBSS).....	24
3.1.2. Conjunto básico de serviços (BSS).....	24
3.1.3. Sistema de Distribuição e Rede Estendida.....	25
3.1.4. Portal	26
3.1.5. Serviços dos dispositivos de rede.....	26
3.2. Rede infra-estruturada e não infra-estruturada.....	28
3.3. Subpadrões 802.11{a, b, g}.....	28
3.3.1. 802.11b.....	28
3.3.2. 802.11a	29
3.3.3. 802.11g.....	29
3.3.4. Demais subpadrões da série 802.11	30
3.4. Máximo <i>throughput</i> teórico.....	30
4. Mecanismos de acesso ao meio.....	32
4.1. Componentes básicos do CSMA/CA	33
4.1.1. <i>Carrier Sense</i>	33
4.1.2. <i>Network Allocation Vector</i> – NAV.....	33
4.1.3 <i>Distributed Coordination Function</i> - DCF.....	34
4.1.4. <i>Acknowledgement</i>	35
4.1.5 <i>Point Coordination Function</i> - PCF.....	36
4.1.6. Algoritmo de acesso ao meio	37
4.2. Problema do nó escondido e do nó exposto	38
4.3. RTS/CTS	39
4.4. Fragmentação de quadros no 802.11	39
5. Desafios das WMNs.....	41
5.1 Aumentar o <i>throughput</i> disponível entre os nós da rede.....	41
5.2. Uso de métricas de roteamento que levem em consideração a qualidade do link.....	44
5.2.1. Contagem de Saltos	45
5.2.2. <i>Round Trip Time</i> por salto.....	46
5.2.3. Atraso de um par de pacotes por salto (PktPair)	48
5.2.4. Contador de Transmissão Esperada (ETX).....	49
5.3. Métricas de roteamento para redes multi-rádios	50
5.4. Desenvolvimento de protocolos que assegurem a justiça nas WMNs	51
5.5. Prover segurança e privacidade.....	53
6. Procedimento experimental.....	55
6.1. Aspectos teóricos.....	55
6.2. Topologia da medição	55
6.3. Cenários da medição	57
6.4. Resultados obtidos sem a atuação do OLSR.....	59
6.4.1. TCP.....	60

6.5.2. UDP	64
6.6. Resultados obtidos com a atuação do OLSR	67
6.6.1. TCP.....	68
6.5.2. UDP	72
6.7. Resumo dos resultados obtidos	75
7. Conclusão	78
8. Bibliografia Consultada.....	80

Índice de Figuras

Figura 1 - Influência de um telefone sem fio na comunicação IEEE 802.11b [2]	13
Figura 2 - Topologia em malha [3]	15
Figura 3 - Topologia de redes <i>ad hoc</i>	16
Figura 4 - Exemplo de uma WMN [7]	17
Figura 5 - Banda larga via WMNs [1].....	18
Figura 6 - Rede de segurança pública baseada nas WMNs [8]	19
Figura 7 - Topologia e implementação de um <i>hotspot</i> [8]	20
Figura 8 - Topologia de uma rede de transportes suportada pela WMN [9].....	21
Figura 9 - Conjunto básico de serviços (BSS) [4].....	24
Figura 10 - Sistemas de Distribuição e Pontos de Acesso [4].....	26
Figura 11 - Rede não infra-estruturada e infra-estruturada [10]	28
Figura 12 - Máximo <i>throughput</i> teórico [11]	31
Figura 13 – Variação do <i>throughput</i> com a distância [12].....	31
Figura 14 - Exemplo de uma transmissão sem <i>backoff</i> [13]	34
Figura 15 - Algoritmo de acesso ao meio [13].....	37
Figura 16 - Problema do nó escondido.....	38
Figura 17 - Problema do nó exposto	38
Figura 18 - Topologia de uma WMN.....	41
Figura 19 - Degradação do <i>throughput</i> x Número de saltos	42
Figura 20 - Topologias WMNs: 1, 2 ou 3 rádios [14].....	43
Figura 21 - Resultado comparativo [14]	44
Figura 22 - Métrica de Contagem de Saltos.....	46
Figura 23 - Comparação WCETT, ETT e HOP [16]	51
Figura 24 - Justiça nas WMNs [17]	52
Figura 25 - Topologia dos testes	57
Figura 26 - Cenário – Teste.....	58
Figura 27 - Medição - TCP - Sem OLSR - Enlace 1.....	60
Figura 28 - Medição - TCP - Sem OLSR - Enlace 2.....	61
Figura 29 - Medição - TCP - Sem OLSR - Enlaces 1 e 2	62
Figura 30 - Medição - TCP - Sem OLSR - Enlaces 1 e 2, em ordem inversa.....	63
Figura 31 - Medição – UDP – Sem OLSR – Enlace 1	64
Figura 32 - Medição – UDP – Sem OLSR – Enlace 2.....	65
Figura 33 - Medição – UDP – Sem OLSR – Enlace 1 e 2	66
Figura 34 - Medição – UDP – Sem OLSR – Enlaces 1 e 2, em ordem inversa.....	67
Figura 35 - Topologia obtida dinamicamente	68
Figura 36 - Medição – TCP – Com OLSR – Enlace 1	69
Figura 37 - Medição – TCP – Com OLSR – Enlace 2.....	69
Figura 38 - Medição – TCP – Com OLSR – Enlaces 1 e 2.....	70
Figura 39 - Medição – TCP – Com OLSR – Enlaces 1 e 2.....	71
Figura 40 - Medição – UDP – Com OLSR – Enlace 1	72
Figura 41 - Medição – UDP – Com OLSR – Enlace 2	73
Figura 42- Medição – UDP – Com OLSR – Enlaces 1 e 2.....	74
Figura 43 - Medição – UDP – Com OLSR – Enlaces 1 e 2, em ordem inversa.	74
Figura 44 - Comparação dos Resultados Medidos - Teste "a"	76
Figura 45 - Comparação dos Resultados Medidos – Teste “b”	77
Figura 46 - Comparação dos Resultados Medidos - Teste "c".....	77

Índice de Tabelas

Tabela 1- Redes <i>ad hoc</i> x WMNs	17
Tabela 2 - Padrão 802.11.....	23
Tabela 3 - <i>Throughput</i> x Mecanismos de Segurança [18].....	54

1. Introdução

“As pessoas se movem. As redes não.”

(Matthew S. Gast)

A possibilidade de se comunicar através de dispositivos sem fio vem exercendo grande fascínio sobre os homens. A própria dinâmica do mundo moderno, onde as pessoas precisam ter acesso a uma grande quantidade de informações a todo instante, ajuda a aumentar esse interesse.

Faraday, Hertz e Maxwell foram alguns dos grandes estudiosos dos princípios que tornaram possível a comunicação através do meio sem fio. O grande salto foi dado em 1896, quando Marconi demonstrou o funcionamento do telégrafo. Desde então, as tecnologias de comunicação sem fio não pararam de evoluir.

Com o passar do tempo, várias tecnologias ocuparam lugar de destaque como o rádio e o satélite. A comunicação via satélite foi proposta por Arthur C. Clarke, em 1945, a um periódico técnico britânico. Atualmente, a telefonia celular desempenha esse papel de protagonista. Com a diminuição do custo dos equipamentos, sua crescente qualidade e maiores taxas de transmissão, as redes de dados sem fio também começam a ocupar uma posição de destaque. O número de adeptos é cada vez maior. Um exemplo disso é o grande número de equipamentos que já vem com as interfaces sem fio integradas, como *PDA*s e *laptops*.

A primeira rede local de computadores sem fio implementada foi desenvolvida por Norman Abramson, e batizada de rede Aloha, em 1971. Essa rede foi instalada no arquipélago do Havaí. A motivação era interligar os diversos *campi* da Universidade do Havaí, situados em locais remotos do arquipélago. Uma grande contribuição do trabalho de Norman Abramson foi o seu protocolo de

acesso múltiplo. Esse protocolo viabilizou que os nós compartilhassem o meio de transmissão e também serviu de base para o desenvolvimento do Ethernet.

O presente projeto faz um estudo das redes em malha sem fio, uma das muitas aplicações da tecnologia sem fio para comunicação de dados. Ao longo deste trabalho, as principais características das redes em malha sem fio são levantadas, bem como algumas de suas aplicações. O padrão no qual essas redes se baseiam, o IEEE 802.11, também é apresentado. Um enfoque maior é dado na arquitetura e nos componentes que esse padrão estabelece. O mecanismo de controle de acesso ao meio, o CSMA/CA, é abordado em seguida. O uso do meio sem fio acarreta em uma série de problemas que não existem nas redes que utilizam cabos e que são tratados através do algoritmo CSMA/CA.

Apesar das vantagens que as redes em malha sem fio possuem, muita pesquisa ainda precisa ser feita para que elas trabalhem com o máximo de seu potencial. Por isso, algumas das principais limitações das redes em malha sem fio também são apresentadas, bem como algumas possíveis soluções que estão sendo propostas por pesquisadores de todo o mundo. Existem muitos grupos de estudo nesta linha, como por exemplo o *Microsoft Research Group*, o GT-Mesh da Universidade Federal Fluminense, entre outros.

Uma das grandes questões existentes tange a questão da justiça nessas redes. Portanto, para concluir este trabalho, foi realizada uma série de medições de *throughput*, tendo como base um artigo que apresenta um modelo teórico e resultado de simulações deste mesmo assunto.

2. Introdução às redes em malha sem fio

2.1. Redes sem fio

As redes sem fio, em geral, apresentam uma série de características que as tornam muito interessantes, como a flexibilidade, mobilidade e baixo custo de implantação.

- A flexibilidade se dá pela ausência de cabeamento estruturado. Um projeto de cabeamento estruturado bem feito é aquele que não sofre alterações em função das modificações da topologia da rede. Ou seja, ele deve ser feito prevendo todas as possíveis configurações daquela determinada rede, fornecendo assim, uma certa flexibilidade. Esse projeto é, em geral, muito difícil de ser realizado pois mesmo num projeto bem feito, nunca se tem certeza absoluta de que aquele cabeamento estruturado irá atender à demandas futuras. A ausência do cabeamento estruturado das redes sem fio é uma de suas grandes vantagens, por fornecer uma flexibilidade quase plena. E ainda, abre a possibilidade de se prover conectividade em locais de difícil instalação de cabos. No Brasil, essa tecnologia se apresenta como uma grande ferramenta para a inclusão digital. [1]
- A mobilidade permite que os usuários finais de redes sem fio se movam dentro de uma área de cobertura, o que é amplamente desejado em um ambiente de trabalho, por exemplo.
- O baixo custo de implantação está estritamente associado à ausência de cabeamento estruturado. É muito mais barato prover conectividade através de um roteador sem fio do que realizar todo o planejamento e execução de um projeto de cabeamento estruturado. O tempo de implantação da rede também cai consideravelmente.

Apesar dessas vantagens iniciais apresentadas, as redes sem fio ainda apresentam uma série de limitações. Pesquisadores de todo o mundo estão levantando soluções para a otimização do desempenho das redes sem fio, bem como para a viabilização da implementação de serviços específicos nesta rede. Dentre as limitações existentes, pode-se citar: capacidade, implementação de qualidade de serviço, justiça, privacidade e segurança, complexidade dos protocolos de roteamento, entre outros. Algumas dessas limitações serão mais bem exploradas no Capítulo 5.

A questão da interferência que a onda eletromagnética pode sofrer também é crítica nas redes sem fio. A figura 1 mostra como o uso de um telefone sem fio pode interferir no *throughput* disponível da rede.

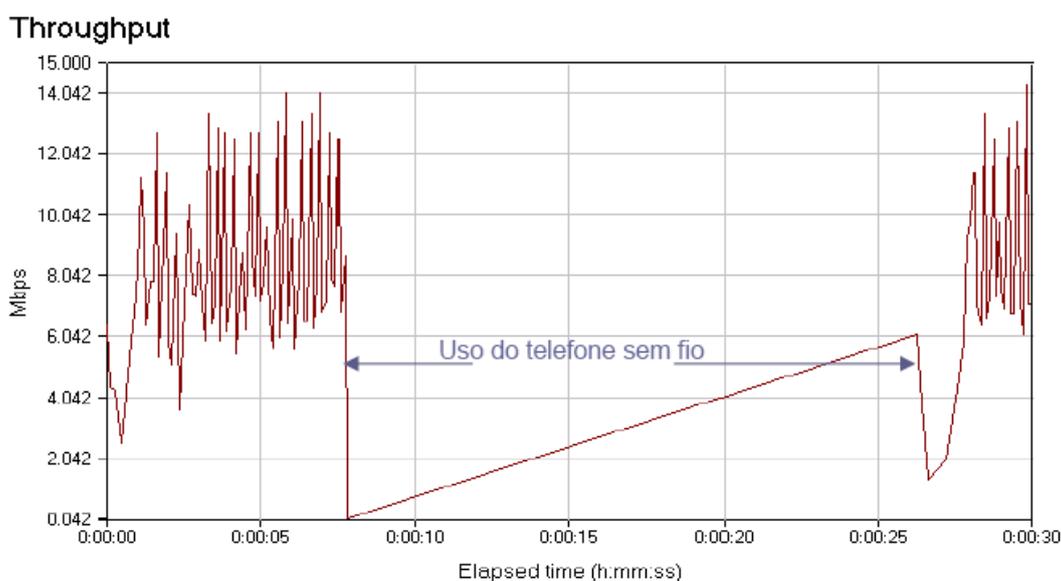


Figura 1 - Influência de um telefone sem fio na comunicação IEEE 802.11b [2]

É importante ressaltar que as redes sem fio não vieram para substituir as redes com fio. Trata-se de uma tecnologia alternativa para algumas aplicações. Por exemplo, se uma empresa já possui todos os seus servidores suportados por uma rede com fio, e se não há qualquer pretensão de se movimentar esses servidores, não há qualquer motivo que justifique a substituição desta rede.

Para um total entendimento das redes sem fio, não basta apenas estudar os princípios da comunicação de dados. Grande parte das limitações reside, basicamente, no fato de se usar o meio sem fio como o meio físico para a transmissão de dados e estar sujeita às leis que determinam como essa transmissão é feita. As ondas eletromagnéticas podem se refletir, refratar e sofrer desvanecimentos, por exemplo. Por motivos óbvios, faz-se necessário, o estudo de mecanismos de propagação da onda eletromagnética. O cálculo da Zona de Fresnel é um importante parâmetro para o projeto dessas redes.

Os principais fatores relacionados à propagação da onda eletromagnética que interferem no desempenho das redes sem fio são a hostilidade do meio sem fio, obstáculos e propagação por multi-percurso.

2.2. Redes em malha sem fio

Por definição, uma rede em malha é aquela que possui todos os seus nós interligados entre si. Em uma rede onde o cabeamento físico se faz necessário, tal topologia se torna muito cara. No entanto, é uma rede altamente confiável devido ao seu alto grau de redundância. Na Figura 2, pode-se observar que cada nó é conectado diretamente a cada um dos demais. Trata-se de uma rede totalmente em malha ou, *full-mesh*. A rede pode ser parcialmente em malha e, neste caso, não será uma rede *full-mesh*.

A melhora do desempenho das redes sem fio em conjunto com a queda considerável de seus custos justificaram a implementação de redes em malha baseadas em tecnologias sem fio. Assim, os altos custos de se implementar uma rede em malha deixaram de existir e o uso desta topologia tornou-se mais viável. As redes em malha sem fio têm como base o padrão IEEE 802.11 e seus sub-padrões,

principalmente o 802.11a, 802.11b, e o 802.11g. Ao longo deste texto, as redes em malha sem fio serão referenciadas simplesmente por WMN (*Wireless Mesh Network*).

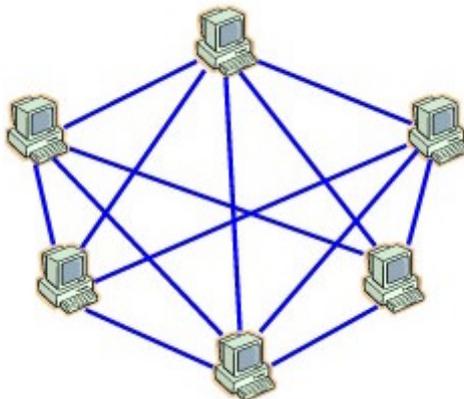


Figura 2 - Topologia em malha [3]

A WMN é uma particularização da rede *ad hoc*. Segundo o padrão IEEE 802.11 [4], uma rede *ad hoc* é “uma rede composta somente de estações móveis que estão dentro do alcance de comunicação umas das outras, via meio sem fio. Uma rede *ad hoc* é, tipicamente, criada de maneira espontânea. (...) Nenhuma habilidade técnica especializada é necessária e pouco (ou nenhum) investimento adicional de tempo ou recursos é necessário, além das estações que irão participar da rede *ad hoc*. O termo *ad hoc* é freqüentemente usado como uma gíria, para se referir a um conjunto de serviços básicos independentes.”

Todos os nós da rede *ad-hoc* podem ser completamente móveis. Assim sendo, há uma interdependência dos nós da rede para que a conexão seja e permaneça estabelecida. Pode-se observar ainda que a topologia muda de forma imprevisível, donde conclui-se que a rede *ad-hoc* deve estar em constante adaptação.

As redes *ad hoc* possuem as mais diversas aplicações. Por exemplo, em reuniões, onde os participantes precisam trocar informações, uma rede deste tipo pode ser estabelecida. Em casos de desastres, com perda dos fios, essas redes podem ser usadas em caráter emergencial e temporário. E

ainda, a rede *ad hoc* pode ser utilizada em campos de guerra, onde aviões, tanques e soldados em movimento precisam trocar informações de maneira rápida e eficaz.

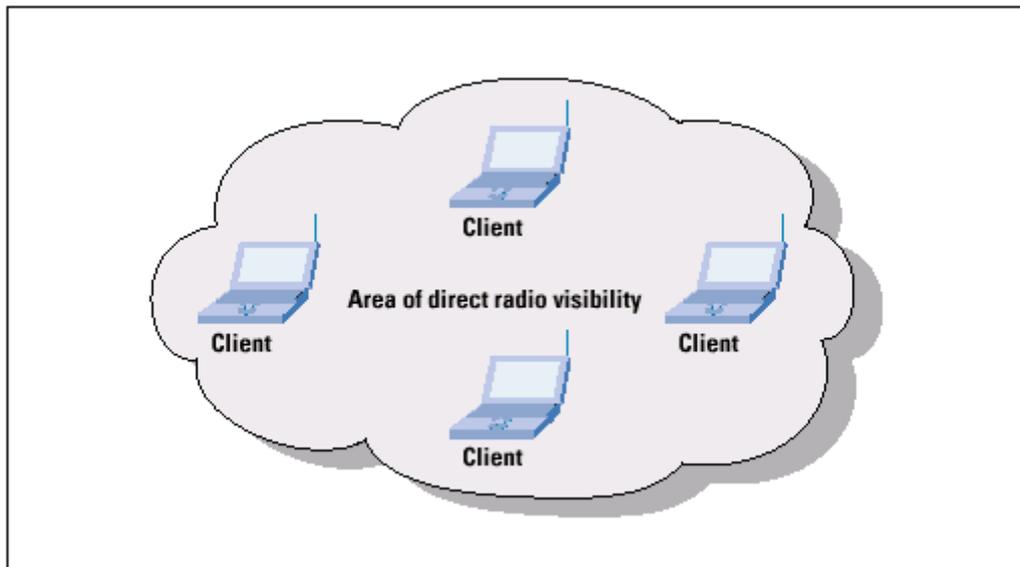


Figura 3 - Topologia de redes *ad hoc*

A grande diferença das WMNs para as redes *ad-hoc* é que os nós possuem posição relativa fixa uns aos outros nós, e possuem acesso à *internet* através de um ou mais *gateways*. O nó pode apresentar mobilidade restrita, ou seja, limitada a uma certa área de cobertura. Assim como nas redes *ad-hoc*, cada nó desempenha, ao mesmo tempo, papel de *host* e roteador.

Pode-se ressaltar ainda, a diferença do padrão de tráfego de dados de uma WMN para uma rede *ad-hoc* [6]: nas WMN, todo o tráfego de dados vem de um *gateway* ou vai para ele. Não há tráfego direto entre os nós da rede. Nas redes *ad-hoc*, tal comportamento não se observa. Nas WMNs, todos os nós, de um modo geral, têm conexão direta com uma fonte de energia. Nessas redes, portanto, a questão da bateria não é tão importante. No entanto, esse é um problema crítico das redes *ad-hoc*.

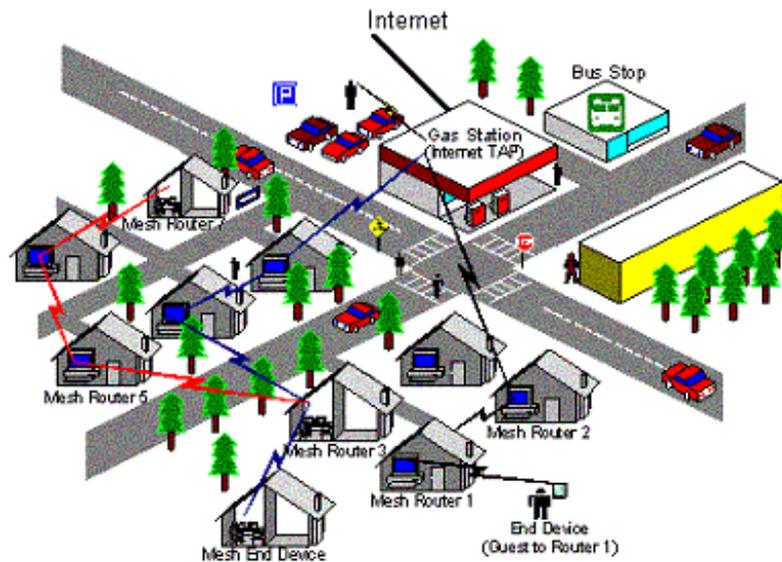


Figura 4 - Exemplo de uma WMN [7]

Características	Redes <i>ad hoc</i>	WMNs
Mobilidade dos nós	Totalmente móveis	Pouca e/ou nenhuma mobilidade
Padrão de tráfego	Aleatório	Tráfego vem de um <i>gateway</i> ou vai para um
Bateria	Ponto crítico	Ponto não-crítico

Tabela 1- Redes *ad hoc* x WMNs

2.3. Aplicações das WMNs

Esta seção tem como objetivo expor algumas das aplicações das WMNs. Pode-se perceber que as possibilidades de implementação das WMNs são infinitas. Mesmo sem operarem com o máximo do seu potencial, o desempenho das WMNs já está num patamar aceitável e já está implementada em diversos lugares do mundo. Com o avanço das pesquisas, a tendência é que o número de aplicações para as WMNs, bem como o número de usuários cresçam cada vez mais.

2.3.1. Banda larga residencial

As WMNs podem ser usadas para prover acesso à *internet* em banda larga para usuários de uma certa região. Para o funcionamento desta aplicação, é necessário pelo menos um *gateway*, que é a

interface entre a WMN e a *internet*. O *backbone* da rede é formado por roteadores sem fio. A distribuição interna aos prédios é feita, geralmente, através de cabos. A UFF provê acesso à *internet* a uma série de prédios vizinhos, através das WMNs [1]. A figura 5 ilustra essa aplicação.



Figura 5 - Banda larga via WMNs [1]

2.3.2. Segurança pública

Algumas cidades dos Estados Unidos já estão utilizando sistemas de segurança pública, suportadas pelas WMNs. Os sistemas de câmeras sem fio para monitoramento de áreas estratégicas da cidade são mais robustos do que os tradicionais. Não há fios que conectam as câmeras ao servidor central, o que torna essa aplicação menos sensível à ação de vândalos. Há, ainda, a possibilidade de se realizar um armazenamento das imagens remotamente, o que aumenta ainda mais a confiabilidade desses sistemas.

A cidade de Beijing, na China, está instalando uma rede de segurança pública e criando uma série de *hotzones* (áreas cobertas pelo sistema de segurança). Esse projeto está sendo executado, tendo em vista as Olimpíadas de Pequim, em 2008.

Além da questão da câmeras de monitoramento, existem muitas outras aplicações. Por exemplo, ao abordar uma pessoa, o policial pode ter acesso à sua ficha criminal, a fim de confirmar a sua suspeita; os bombeiros podem ter acesso às plantas das construções para elaborar o melhor plano de evacuação do local e acabar com o incêndio; paramédicos em uma ambulância podem enviar os sinais vitais de um paciente ao hospital, a fim de obter o suporte de médicos mais experientes.



Figura 6 - Rede de segurança pública baseada nas WMNs [8]

2.3.3. Hotspots

Um *hotspot* nada mais é do que um local onde se provê o acesso à *internet* sem fio. São facilmente encontrados nos Estados Unidos, em locais estratégicos, como aeroportos, cassinos, hotéis e restaurantes. Por exemplo, todas as lanchonetes da rede *Starbucks* fornecem esse tipo de acesso, em parceria com a operadora *T-Mobile*.

Com o crescente número de usuários de *laptops* e *PDA*s que são compatíveis com as redes sem fio, a criação de *hotspots* é uma grande estratégia para se fidelizar clientes. A figura 6 ilustra uma topologia de um *resort* que provê *hotspots* aos seus hóspedes, bem como uma possibilidade de implementação de um *hotspot* em um prédio.

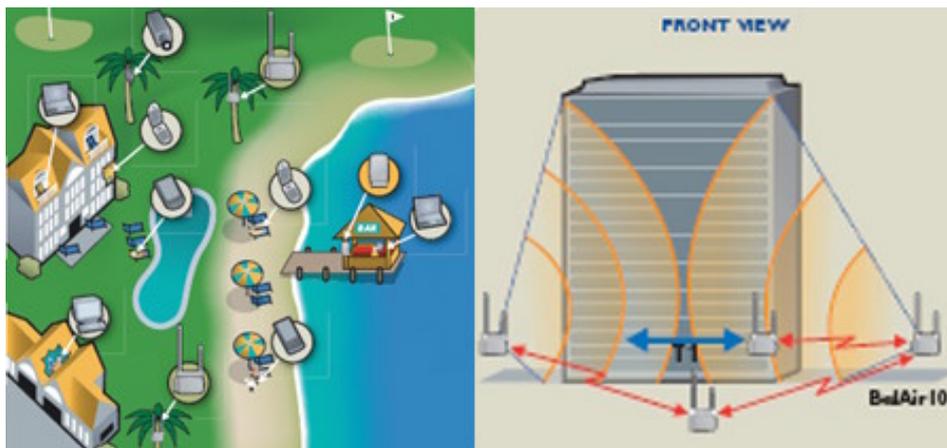


Figura 7 - Topologia e implementação de um *hotspot* [8]

2.3.4. Sistemas de transporte

Através da implementação das WMNs em pontos estratégicos da rede de transportes, pode-se oferecer serviços como: sistema inteligente de semáforos, temporizados de acordo com o fluxo de veículos que trafegam em cada direção e sentido; prover informações aos usuários de transporte público a situação do veículo que esperam.

Por exemplo, se uma pessoa está aguardando o ônibus A, ele sabe em que ponto da rota este ônibus se encontra, se ainda há lugares vazios e também o tempo estimado para que esse ônibus chegue até ela. Esse ponto pode ser estendido à questão de segurança nos ônibus, uma vez que é possível detectar qualquer mudança de rota.

Através desta aplicação, o sistema de multas passa a ser *real-time*. Se um radar acusar excesso de velocidade de um veículo, por exemplo, ele pode fotografar o infrator e enviar essa foto e a ocorrência para o sistema, instantaneamente. A figura 8 ilustra a topologia de uma rede de transportes baseada nas WMNs.

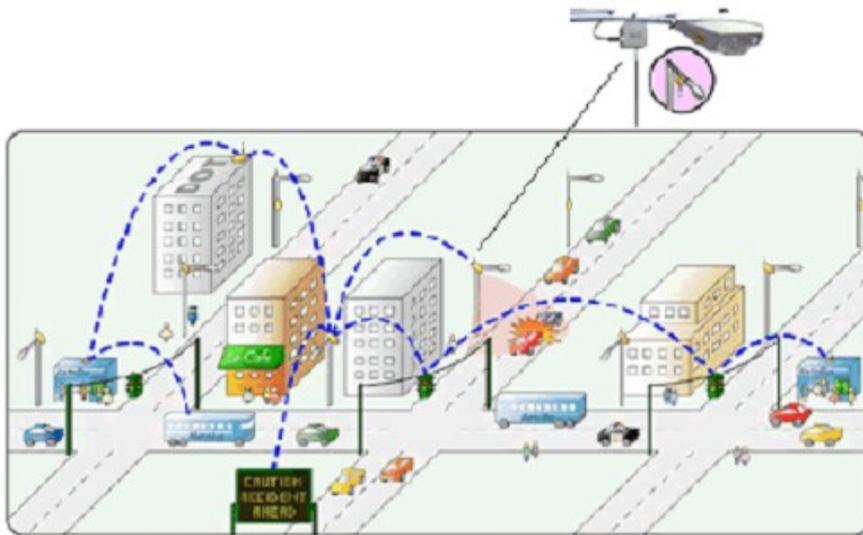


Figura 8 - Topologia de uma rede de transportes suportada pela WMN [9]

3. O padrão IEEE 802.11 e sua arquitetura básica

Uma vez apresentada a WMN e algumas de suas aplicações, é necessário entender o padrão no qual elas se baseiam e quais são as entidades que a compõem. O padrão atual 802.11 [4] foi apresentado pelo IEEE em 1999, como uma atualização do padrão original apresentado em 1997. Ele foi introduzido como sendo uma tecnologia capaz de sustentar uma rede local sem fio (WLAN – *Wireless LAN*).

Trata-se do primeiro padrão que se propôs a descrever o funcionamento de uma LAN sem fio. Ele contempla tecnologias de transmissão como o *Direct Sequence Spread Spectrum* (DSSS), o *Frequency Hopping Spread Spectrum* (FHSS) e o infravermelho. Este último acabou não ganhando aplicações comerciais.

O espalhamento de espectro, utilizado tanto pelo DSSS como pelo FHSS, é uma tecnologia de guerra. Através deste espalhamento, as informações ficam espalhadas dentro do espectro de frequências, o que aumenta a sua banda de transmissão. Em contrapartida, a sua relação sinal ruído fica mais baixa, o que torna este sinal quase imperceptível a certos receptores, característica muito valorizada nos campos de batalha.

O padrão 802.11 descreve a operação de sistemas DSSS que operam a 1 Mbps e 2 Mbps, e também os sistemas FHSS, nessas mesmas taxas. A faixa de frequências atendida por este padrão vai de 2,4 a 2,4835 GHz. Esse padrão descreve apenas as duas primeiras camadas do modelo OSI: física (PHY) e controle de acesso ao meio (MAC).

O grande objetivo deste padrão é suportar a mobilidade das estações, inerente aos sistemas sem fio, de modo que essa mobilidade seja transparente às camadas superiores. Ou seja, a aplicação não

precisa se preocupar se está sendo usado um meio sem fio ou um cabo coaxial. Essa questão é restrita às camadas 1 e 2 do modelo OSI.

802.2			Data Link Layer
802.11 MAC			
FH	DS	IR	PHY Layer

Tabela 2 - Padrão 802.11

Os desafios de se implementar uma rede de dados sem fio são inúmeros. O padrão 802.11 [4] enumera uma série desses desafios, dentre os quais, pode-se destacar:

- As fronteiras do meio não são bem definidas num determinado instante. Não se pode medir, com precisão, o limite do alcance um rádio. Obviamente, fora dessas fronteiras, as estações não conseguem receber nem enviar dados.
- São vulneráveis a sinais externos, estando sujeitas a interferências.
- Comunicam-se através de um meio menos confiável que os usuais cabos de cobre ou fibras ópticas, por exemplo. As ondas eletromagnéticas estão sempre sujeitas a ações de agentes externos, o que pode comprometer o desempenho e, principalmente, a segurança das redes sem fio;
- Possuem topologia dinâmica, o que aumenta a sua complexidade.
- Não possuem conectividade plena. Além disso, a premissa de que cada estação pode ouvir todas as demais pode ser falsa. Por exemplo, uma estação pode estar escondida das outras, e mesmo assim pode estar disputando o acesso ao meio, como acontece no problema do nó escondido.

3.1. Componentes da arquitetura IEEE 802.11

Uma rede baseada no padrão 802.11 [4] possui diversos componentes que interagem entre si. O padrão define todos esses possíveis componentes da rede.

3.1.1. Conjunto básico de serviços independentes (IBSS)

O componente mais básico da arquitetura 802.11 é o conjunto básico de serviços independente (IBSS). É também a rede local sem fio mais básica que se pode ter. Deve possuir, pelo menos, dois dispositivos. Como esse conjunto independente é geralmente formado sem qualquer planejamento, para fins específicos e por um curto período de tempo, ele também é conhecido como rede *ad-hoc* ou BSS *ad-hoc*. Os dispositivos que pertencem a um IBSS comunicam-se diretamente uns com os outros, sem a necessidade de um dispositivo centralizando toda a conexão.

3.1.2. Conjunto básico de serviços (BSS)

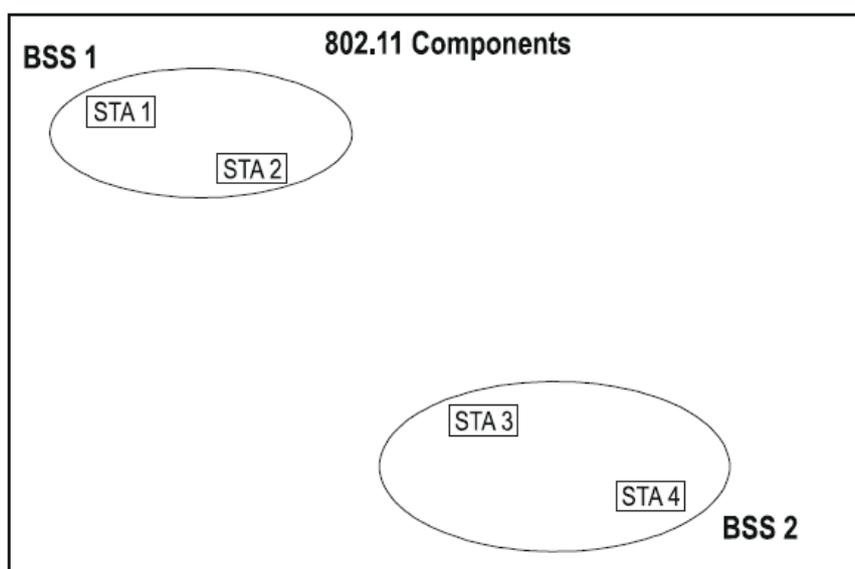


Figura 9 - Conjunto básico de serviços (BSS) [4]

O conjunto básico de serviços (BSS), é um agrupamento lógico de dispositivos, controlado por uma única função lógica de coordenação (um *access point*, por exemplo). Esta função lógica de coordenação centraliza todo o tráfego da BSS. Neste caso, uma estação não pode se comunicar diretamente com a outra. Os dados, necessariamente, devem passar pelo ponto central. Para prover toda a mobilidade e dinâmica requeridas pelas redes sem fio, tem-se que a associação entre uma estação e uma BSS deve ser dinâmica.

3.1.3. Sistema de Distribuição e Rede Estendida

O meio físico, assim como para as redes cabeadas, impõe uma série de limitações. Ele limita a distância máxima suportada entre duas estações para que elas se comuniquem, por exemplo. Para lidar com essa limitação física, o padrão 802.11 define ainda, na seção de arquitetura, o conceito de área. Os limites das áreas de cobertura não são bem definidos. Como qualquer sistema baseado em rádio, estão sujeitas às condições de propagação da onda eletromagnética.

Por isso, em alguns casos, é necessário uma extensão de cobertura. Para resolver este problema, as BSSs podem ser projetadas de forma interdependente, formando assim uma rede estendida. Essa rede é composta por múltiplas BSSs, interconectadas pelo sistema de distribuição (DS). Esse sistema suporta as estações móveis provendo serviços lógicos necessários para lidar com mapeamento de endereço de destino e a integração de múltiplos BSSs. Um AP pode ser usado para formar um DS. Muitas vezes, o sistema de distribuição também é chamado de *backbone* da rede.

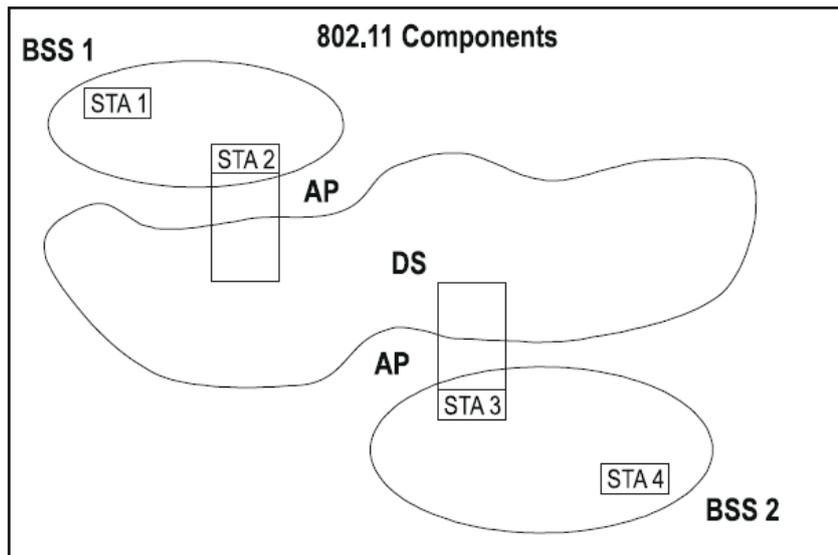


Figura 10 - Sistemas de Distribuição e Pontos de Acesso [4]

3.1.4. Portal

Finalmente, para a integração da rede sem fio com a tradicional LAN cabeada, o padrão apresenta o portal. O portal é um ponto lógico onde os dados oriundos de uma rede não 802.11 entram no DS da rede 802.11. O portal pode ser um AP, por exemplo.

3.1.5. Serviços dos dispositivos de rede

Para garantir o funcionamento e a interoperabilidade dos dispositivos baseados no 802.11, há uma série de serviços especificados no padrão que os dispositivos devem ser capazes de prover. Há uma rotina a ser cumprida pelos terminais para que possam utilizar os serviços de rede, e essa rotina depende dos serviços dos dispositivos de rede.

- 1) O terminal deve ser capaz de encontrar a rede sem fio. Para isso, ele ouve o meio para tentar detectar alguma rede sem fio disponível. Em inglês, essa etapa é conhecida por *scanning*. O *scanning* pode ser passivo ou ativo. No caso de um *scanning* passivo, o terminal simplesmente escuta os pacotes do meio sem fio e identificam a rede. No caso ativo, o

terminal envia quadros sonda, contendo a identificação da rede na qual ele deseja se conectar ou uma identificação *broadcast*.

- 2) Uma vez encontrada a rede, o terminal deve ser configurado para conversar com a SSID correta. A SSID é o identificador do conjunto de serviços, e é enviado em *beacons*, que são pequenos quadros de gerenciamento, e em outros pacotes.
- 3) De posse da SSID do dispositivo no qual pretende se conectar, o terminal deve passar pela fase de autenticação. Nesta etapa, o dispositivo da rede verifica a identidade do terminal. Há uma verificação se o terminal é, de fato, quem ele diz ser. A autenticação pode ser aberta, onde nenhuma senha é requerida, ou fechada, através do protocolo WEP (*Wired Equivalent Privacy*).
- 4) Se o terminal conseguir a sua autenticação, ele precisará se associar à rede. A associação à uma rede nada mais é do que uma permissão para enviar e receber pacotes.

Além dos serviços presentes neste processo inicial, os dispositivos também devem prover:

- De-autenticação – relacionado à estação: é o encerramento de uma autenticação previamente estabelecida;
- Dissociação – relacionado ao sistema de distribuição: é o encerramento de uma associação previamente estabelecida;
- Distribuição – relacionado ao sistema de distribuição: é através deste serviço que as estações enviam os quadros pela rede;
- Integração – relacionado ao sistema de distribuição: permite a transmissão e a recepção de quadros entre dispositivos 802.11 e não 802.11;
- Re-associação – relacionado ao sistema de distribuição: ocorre quando um dispositivo move para outro lugar da rede. Assim, ele precisa se re-associar à um novo *access point*, para que este

negocie a transferência dos quadros que estavam no *buffer* do *access point* antigo. Além disso, esse serviço anuncia ao sistema de distribuição que o terminal se movimentou;

3.2. Rede infra-estruturada e não infra-estruturada

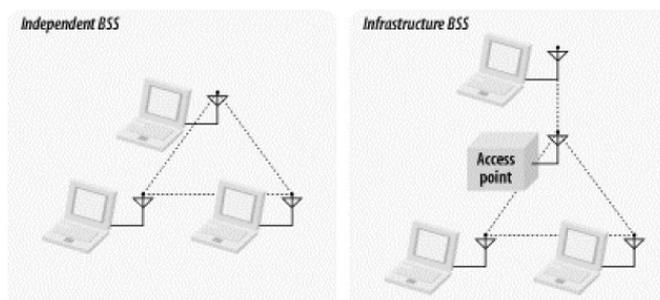


Figura 11 - Rede não infra-estruturada e infra-estruturada [10]

As redes em fio podem ser infra-estruturada e não infra-estruturada. Na primeira, existe a presença de um *access point*, que centraliza todo o acesso. Por exemplo, se um nó quiser falar com outro, necessariamente ele terá de passar pelo AP, o que não ocorre na rede não infra-estruturada, onde todos os nós podem falar uns com os outros, desde que estejam dentro da área de alcance.

3.3. Subpadrões 802.11{a, b, g}

3.3.1. 802.11b

Como ocorre em muitos casos, o avanço tecnológico das redes sem fio baseadas no padrão 802.11 acabou sendo mais rápido do que a própria padronização. Os fabricantes de equipamentos, impulsionados pela grande aceitação e popularização da tecnologia entre os usuários finais, desenvolveram por conta própria, meios de se alcançar transmissões mais velozes do que as padronizadas, beirando os 11 Mbps.

O grande problema é que os dispositivos que estavam sendo vendidos, e operavam à essa taxa, não eram padronizados, o que acarretou num grande problema para esses dispositivos interoperarem. Como resposta a esse cenário, veio o subpadrão 802.11b. Ele especifica sistemas DSSS que operam a 1, 2, 5,5 e 11 Mbps, dependendo do esquema de modulação adotado. Essa grande melhora nas taxas de transmissão se deve ao uso de diferentes esquemas de codificação e modulação. Este padrão não trata de sistemas FHSS.

Os dispositivos compatíveis com o 802.11b são, necessariamente, compatíveis com o 802.11. A grande aceitação desse padrão pode ser atribuída aos baixos custos e às altas taxas de transmissão. Opera na mesma frequência do 802.11, 2,4 GHz. E, como o 802.11, está vulnerável aos mais diversos tipo de interferência, como telefones sem fio, fornos de microondas, entre outros.

3.3.2. 802.11a

Esse subpadrão opera a 5 GHz, o que o torna incompatível com os dois padrões anteriores. Alcança-se taxas bem superiores, como por exemplo, 54 Mbps. Como a atenuação de um sinal é função da frequência do mesmo (a atenuação possui um valor da ordem da raiz quadrada da frequência de operação), os dispositivos que se baseiam neste subpadrão estão sujeitos a uma atenuação maior.

3.3.3. 802.11g

Opera na mesma frequência do 802.11 e 802.11b, sendo portanto, compatível com eles. O seu grande diferencial é a taxa de transmissão que consegue prover: assim como o 802.11a, alcança-se taxas de 54 Mbps. Utiliza a técnica de modulação conhecida por OFDM (*Orthogonal Frequency Division Multiplexing*). Este padrão reúne as principais características dos subpadrões 802.11a (alta taxa de transissão) e do 802.11b (menor atenuação).

3.3.4. Demais subpadrões da série 802.11

O IEEE possui ainda outros subpadrões da série 802.11. O 802.11d trata de uma especificação para operação em domínios regulatórios adicionais. O 802.11e trata de melhorias na implementação de qualidade de serviço. O 802.11F recomenda uma prática para interoperabilidade de *access points* de diversos fabricantes, através do *Inter-Access Point Protocol* em sistemas de distribuição, suportando operações IEEE 802.11.

O subpadrão 802.11h traz um adendo de gerenciamento de extensão de espectro e potência transmitida na banda de 5GHz na Europa. O 802.11i trata da segurança e o 802.11j traz um adendo para a operação entre 4,9 e 5 Ghz no Japão. Tem-se ainda o subpadrão 802.11k, que trata da implementação da qualidade de serviço em nível físico e o 802.11n, que é uma tentativa de se alcançar taxas de transmissão ainda mais elevadas, de aproximadamente 100 Mbps.

3.4. Máximo *throughput* teórico

Segundo pesquisadores da North Carolina State University [11], apesar de se explicitar as taxas de transferência citadas acima, é impossível obtê-las na prática. Para o 802.11b, por exemplo, tem-se um *throughput* de 11 Mbps. Essa taxa só se refere à taxa de dados de rádio, e ainda, a só uma parte dos pacotes. Por exemplo, sem erros e para pacotes de 1460 bytes, a taxa que se obtém é de 6,1 Mbps. A eficiência é significativamente menor para pacotes menores.

O máximo *throughput* que se obtém no 802.11 pode ser definido como a quantidade de unidades de dados de serviço da camada MAC (SDUs), que podem ser transmitidas por unidade de tempo. A figura 12 apresenta um dos resultados expostos no referido artigo, em função do tamanho das

mensagens, no esquema de espalhamento de espectro (*Frequency Hopping* ou *Direct Sequence*) e a taxa de transmissão, utilizando o RTS/CTS.

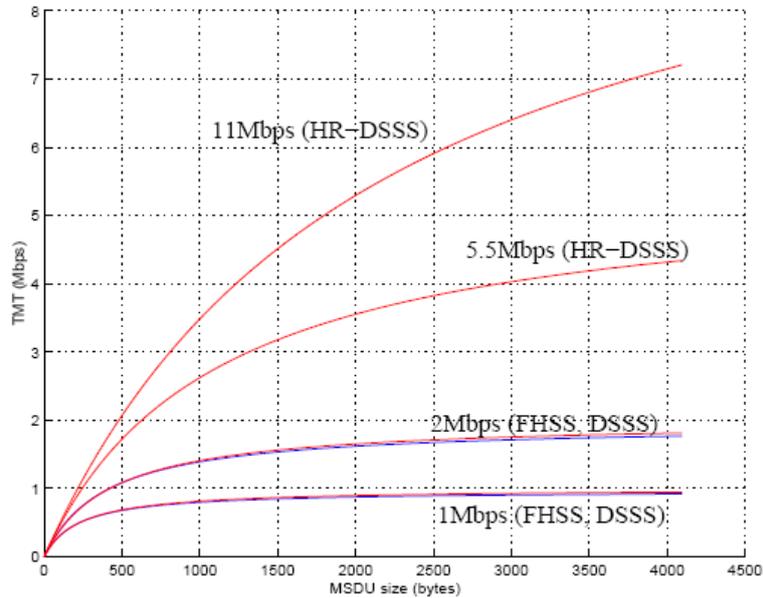


Figura 12 - Máximo *throughput* teórico [11]

O *throughput* depende ainda, da distância que separa a origem do destino. Pode se dizer que o *throughput* é inversamente proporcional à distância. Isso pode ser justificado pela maior atenuação que a onda eletromagnética irá sofrer, em função da maior distância. A rede se adequa a esta distância através DRS (*Dynamic Rate Shifting*), e ocorre na medida em que essa distância aumenta. Essa informação é de suma importância para um projeto ser bem sucedido.

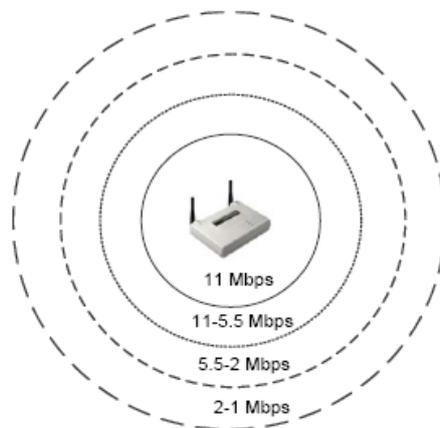


Figura 13 – Variação do *throughput* com a distância [12]

4. Mecanismos de acesso ao meio

Uma vez conhecido o padrão e a sua arquitetura básica, apresenta-se um dos pontos chave do funcionamento das redes sem fio. O uso da interface aérea como meio de transmissão de dados acarreta em uma série de problemas que não existiam nas redes cabeadas. Por isso, os mecanismos de acesso ao meio devem ser muito mais robustos do que os das redes cabeadas.

Deve-se prover o múltiplo acesso ao meio, mas a detecção da colisão, como é feita nas redes Ethernet não é mais suficiente. O algoritmo utilizado é o CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*). Ao invés disso, a colisão deve ser evitada, através do algoritmo de CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Esse algoritmo também é do tipo LBT (*Listen before talk*). A estação transmissora deve primeiro ouvir o meio e aguardar até que o canal da portadora esteja disponível antes de transmitir.

Enquanto o CSMA/CD consegue detectar colisão no meio, o CSMA/CA deve direcionar os seus esforços para se evitar as colisões. Os autores Pejman Roshan e Jonathan Leary , no livro “802.11 Wireless LAN Fundamentals” [13], fazem uma analogia do CSMA/CA a uma conferência telefônica:

- 1) Antes do participante falar efetivamente, ele deve indicar qual é a duração estimada de sua fala. Esse valor indica aos demais participantes, quanto tempo eles deverão esperar antes de ter a oportunidade de falar.
- 2) Os demais participantes não podem nem cogitar em falar enquanto a duração indicada pelo participante que está com a palavra não se encerrar.
- 3) Os participantes só sabem se sua voz foi ouvida se eles receberem uma confirmação dos demais, quando terminam de falar.

- 4) Se eles não receberem a confirmação de que os outros participantes ouviram a sua fala, significa que ela foi perdida. Eles devem esperar uma fatia de tempo aleatória. Só após a expiração desta fatia de tempo é que eles podem tentar falar novamente.
- 5) Se dois participantes começarem a falar ao mesmo tempo, eles continuam falando um sobre o outro.

4.1. Componentes básicos do CSMA/CA

Baseando-se no algoritmo exemplificado acima, os autores ainda definem os componentes básicos do algoritmo CSMA/CA podem ser definidos. São esses componentes básicos que irão fornecer os meios adequados de se sustentar este algoritmo

4.1.1. *Carrier Sense*

É o detector de portadora. Se um nó da rede quiser transmitir dados, o primeiro passo é escutar o meio, assim como ocorre no CSMA/CD, para se certificar de que ele não está sendo usado por outro nó. Existem dois métodos para se verificar o uso do meio:

- 1) verificação direto na camada física para saber se a portadora está presente.
- 2) utilização da função de detecção de portadora virtual, também conhecido por vetor de alocação de rede. Em inglês, *network allocation vector*.

4.1.2. *Network Allocation Vector – NAV*

Através do NAV, é possível “reservar” o uso do meio. Ele nada mais é do que um *timer* que vai sendo atualizado de acordo com os quadros transmitidos através do meio. Suponha que uma estação

A esteja enviando dados para uma outra estação B. Por se tratar de um meio compartilhado, uma eventual estação C também escutaria essa transmissão. O quadro 802.11 contém um campo de duração, cujo valor deve ser tal, que seja suficiente para que a transmissão de A para B seja realizada com sucesso, incluindo o tempo de confirmação que a estação B deve enviar para A, confirmando o recebimento do quadro. A estação C, tendo acesso a essa informação, atualiza o seu valor de NAV para que ela não tente transmitir enquanto a transmissão de A para B durar. Ao fim da transmissão da estação A para a estação B, o valor do NAV da estação C deve chegar a zero. Finalmente, a estação C pode tentar retransmitir.

4.1.3 Distributed Coordination Function - DCF

Assim que o meio se torna disponível para a transmissão, a estação deve esperar uma certa fatia de tempo antes de transmitir. Essa fatia de tempo é denominada DIFS. Tão logo o DIFS expira, o meio se torna disponível para a transmissão. A figura 14 ilustra uma transmissão de dados com o DIFS.

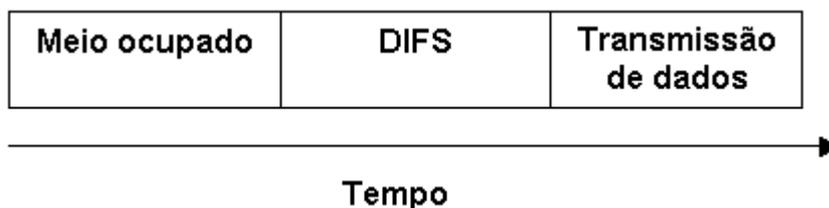


Figura 14 - Exemplo de uma transmissão sem *backoff* [13]

Por que a estação não pode transmitir assim que o seu NAV é decrementado a zero? Suponha o cenário onde estação A esteja transmitindo dados para B. Suponha também que C e D estejam no aguardo do fim dessa transmissão para poder utilizar o meio. Como as estações C e D conseguem escutar o que A está transmitindo para B, as duas estações terão o mesmo valor para o NAV. Assim que a transmissão de A para B se encerra, C e D escutarão o meio e tentarão transmitir seus dados. Nesta situação, fica caracterizada uma grande probabilidade de ocorrência de colisão.

Para fazer com que as colisões não ocorram em situações como essa, o DCF usa um recuo ou *backoff*. Assim, um algoritmo de *backoff* aleatório escolhe um valor de 0 até o valor de contenção da janela. O valor de *backoff* é a quantidade de tempo, além do DIFS, que uma estação terá de esperar, após ter detectado a disponibilidade do meio, para poder transmitir.

Para ilustrar o exemplo da utilização do *backoff*, suponha que as estações B e C possuem o mesmo valor de NAV estão aguardando o término da transmissão de A para poder transmitir. Embora B e C possuam os mesmos valores de NAV, em função do algoritmo de *backoff*, um dos dois irá transmitir primeiro. A estação que for preterida, deverá escutar o meio, atualizar o valor do NAV, e retomar o processo.

4.1.4. *Acknowledgement*

Até o momento, não há nenhuma garantia de que o receptor recebeu o quadro enviado com sucesso. Como o transmissor pode se certificar de que sua informação foi efetivamente recebida? O 802.11 especifica que, ao receber um quadro com sucesso, o receptor envie um quadro de confirmação (*ack*).

O não recebimento do quadro *ack* pode caracterizar uma perda de pacote, causada até mesmo por uma colisão. O transmissor incrementa o seu contador de retransmissões, dobra o valor da janela de contenção, e reinicia o processo de acesso ao meio.

Se a estação receptora tivesse que passar pelo mesmo mecanismo de acesso ao meio para transmitir o quadro *ack*, provavelmente o tempo de espera pelo *ack* do transmissor expiraria. Por isso, a transmissão do quadro *ack* é considerado um caso especial. Ele não precisa implementar o

algoritmo de *backoff* aleatório. E ainda, o quadro *ack* não precisa esperar o DIFS antes de ser transmitido. Ele só precisa aguardar um intervalo de tempo SIFS, que é menor que o DIFS em dois intervalos de tempo. Isso garante uma certa prioridade para que a estação receptora envie a confirmação a tempo.

Caso a estação transmissora não receba o *ack*, a janela de contenção é dobrada e o processo de acesso ao meio é repetido. Para cada falha de transmissão, incrementa-se o contador de retransmissões e dobra-se a janela de contenção, até um valor máximo, determinado pelo administrador da rede.

4.1.5 Point Coordination Function - PCF

É um mecanismo opcional de acesso ao meio, usado em conjunto com o DCF. O PCF é um mecanismo de acesso ao meio que provê entrega de quadros sem contenção de e para o AP. A maior parte dos fabricantes não inclui suporte ao PCF porque ele aumenta o *overhead* da BSS. Quando se utiliza esse mecanismo, existe um ponto central, geralmente o AP, que coordena o acesso ao meio, através de *pooling*. De tempos em tempos, esse ponto central pergunta a cada estação se elas têm algo a transmitir. O grande viés deste mecanismo é a sua não aplicabilidade em redes de grande porte.

Estações especiais, os pontos coordenadores, são utilizadas para assegurar que o meio não ofereça qualquer contenção. Como este ponto está vinculado ao AP, pode-se assumir que o PCF só pode ser implementado em redes infra-estruturadas. Através do PCF, consegue-se suportar aplicações quase em tempo real. O PCF fornece um acesso justo ao meio, através de *tokens*. Esse serviço, no entanto, não é suportado o tempo todo.

Como o PCF não é muito implementado, foge ao escopo deste projeto entrar em maiores detalhes relacionados ao seu mecanismo de funcionamento.

4.1.6. Algoritmo de acesso ao meio

Todo o mecanismo de acesso ao meio pode ser resumido, de uma maneira geral, na figura 15. A estação que está pronta para transmitir deve ouvir o meio para saber se ele está disponível. Se o meio estiver ocupado, a estação deverá continuar a fazer essa verificação até que o meio fique livre.

Como já foi visto anteriormente, uma estação só poderá tentar transmitir se o seu valor de NAV for nulo. Em seguida, gera-se um número de *backoff* aleatório, para se evitar possíveis colisões. Faz-se uma verificação para saber se nenhuma outra estação está transmitindo. Caso não esteja, e o valor do *backoff* aleatório for nulo, finalmente o quadro poderá ser enviado.

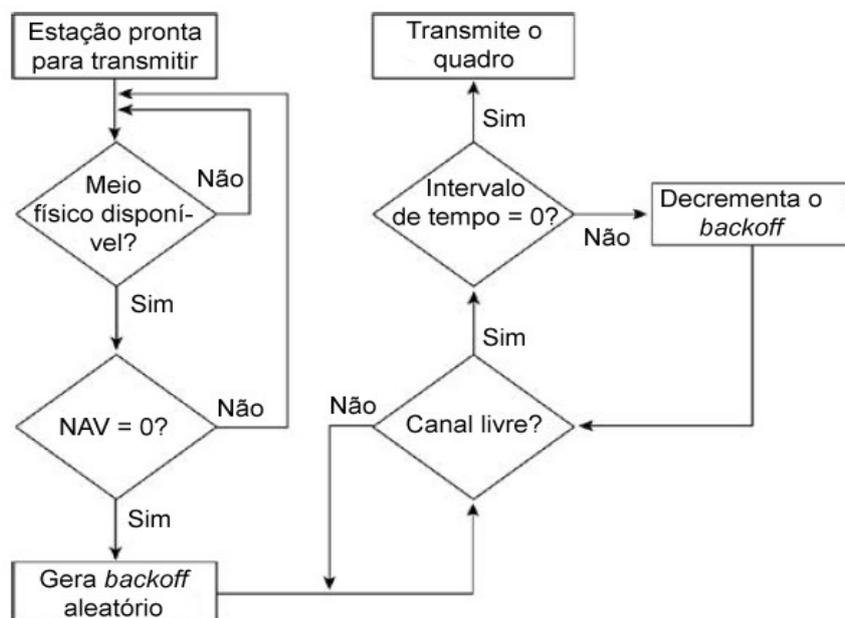


Figura 15 - Algoritmo de acesso ao meio [13]

4.2. Problema do nó escondido e do nó exposto

Uma estação A pode ter problemas em acessar ao meio, em virtude de uma estação B, que está dentro dos limites de alcance de uma estação C, por exemplo, mas fora do seu próprio alcance. Essa situação é conhecida como “problema do nó escondido”. Como a estação B está dentro da região de alcance da estação C, ele acaba competindo o acesso ao meio com as outras estações. Como a estação B não consegue ouvir que a estação A está transmitindo dados para a estação C, ela pode tentar a transmissão com C e causar uma colisão.

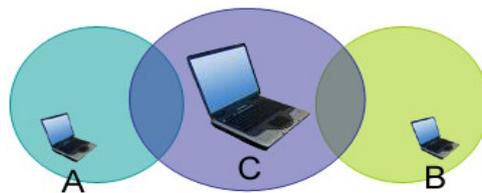


Figura 16 - Problema do nó escondido

O problema do nó exposto é caracterizado por uma estação não poder transmitir seus dados, em função da existência da transmissão de uma estação vizinha. Na figura 10, suponha que C está transmitindo dados para B. Se D quiser transmitir dados para A, ficará impossibilitado, uma vez que, em virtude da transmissão já existente, ele teria um valor de NAV não nulo.

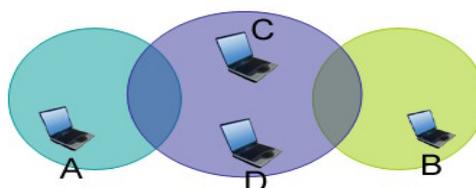


Figura 17 - Problema do nó exposto

4.3. RTS/CTS

O primeiro quadro que uma estação transmite para reservar o meio é o RTS (*request to send*). Esse quadro é enviado ao destino e a todos as estações que conseguem escutá-lo. Ele contém o tempo estimado que se deseja ocupar o meio: é a soma do tempo de transmissão e o tempo de chegada do *ack*. Se o destino aceitar a transmissão, ele responde o quadro RTS com um CTS (*clear to send*), com um campo que contém a duração da transmissão, que deve ser suficiente para atender o tempo estimado no RTS.

Qualquer outro nó que receber o CTS não deverá transmitir pelo período de tempo determinado neste quadro, o que resolve o problema do nó escondido. Assume-se que, se o nó está recebendo o CTS, é porque ele está dentro da área de alcance do destino. Sendo assim, qualquer tentativa de transmissão por parte deste nó poderá causar alguma interferência na transmissão existente.

E ainda, qualquer nó que receba somente o RTS e não o CTS, pode transmitir para o seus nós vizinhos, o que poderia resolver o problema do nó exposto.

4.4. Fragmentação de quadros no 802.11

Ao invés de se transmitir quadros de tamanho muito grande, a camada MAC do 802.11 fragmenta esses quadros. O principal objetivo disso é aumentar a confiabilidade da transmissão através do meio sem fio. Em se tratando de um meio hostil, a probabilidade de se conseguir transmitir fragmentos menores com sucesso é maior do que com quadros muito grandes. Cada fragmento deve ser confirmado individualmente. Caso haja alguma falha de transmissão, como colisão ou perda de quadro, somente este fragmento menor precisará ser retransmitido, o que aumenta o *throughput* do

meio. O 802.11, no entanto, só fragmenta quadros unicast. Os quadros broadcast e multicast são transmitidos inteiros.

A grande desvantagem é que a fragmentação aumenta o *overhead* da camada 2, devendo, portanto, haver um equilíbrio entre confiabilidade e aumento do *throughput* com o *overhead*.

5. Desafios das WMNs

Por se tratar de um assunto relativamente novo, desafios a serem superados pelas WMNs estão surgindo a cada momento. Abaixo, alguns destes desafios estão relacionados, bem como para onde estão sendo direcionados os esforços dos pesquisadores para a superação dos mesmos.

- Aumentar o *throughput* disponível entre os nós da rede;
- Uso de métricas de roteamento que levem em consideração a qualidade do link;
- Métricas de roteamento para redes multi-rádios;
- Desenvolvimento de mecanismos que assegurem a justiça nas WMNs;
- Prover segurança e privacidade;

5.1 Aumentar o *throughput* disponível entre os nós da rede

A interface aérea é, intrinsecamente, um meio compartilhado e hostil. Grande parte das WMNs implementadas trabalha com um único rádio e em um único canal. Além disso, nas WMNs, cada nó é *host* e roteador ao mesmo tempo. Tudo isso, de certa maneira, contribuí para que o *throughput* disponível para cada nó caia consideravelmente.

Como um nó não pode transmitir e receber pacotes simultaneamente, tem-se que o *throughput* decresce à metade.

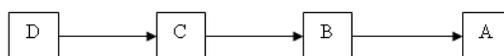


Figura 18 - Topologia de uma WMN

Na figura 18, o nó C não pode receber pacotes de D e enviar seus pacotes a B ao mesmo tempo. Fato que não ocorre numa rede cabeada, onde existe um par de fios responsável exclusivamente por enviar pacotes, e outro para receber.

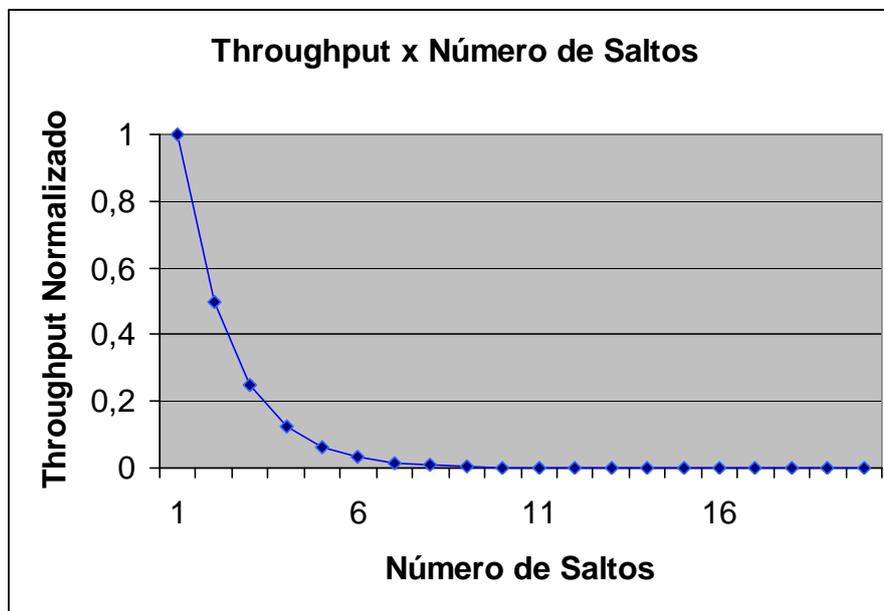


Figura 19 - Degradação do *throughput* x Número de saltos

A degradação do *throughput* em relação ao número de saltos para se alcançar o *gateway* é da ordem da metade do *throughput* por salto. Assim, se um nó está a 4 saltos do *gateway*, o seu *throughput* efetivo será da ordem de $(1/2)^4 = 1/16$ do *throughput* existente.

Existe uma linha de pesquisa que aponta para o uso de mais de um rádio por nó, a fim de aumentar o *throughput* da rede. Os pesquisadores do *Microsoft Research Group* estão indo nesta linha. Com o barateamento do *hardware* e com o comprovado ganho de desempenho, a relação custo-benefício de se implementar redes multirádios está cada vez melhor. A empresa Mesh Dynamics, financiada pela Força Aérea dos Estados Unidos, realizou um estudo comparativo do desempenho das redes com mais de um rádio [14].

O referido estudo aponta a possibilidade de se trabalhar em três topologias diferentes, como pode ser observado na figura 20.

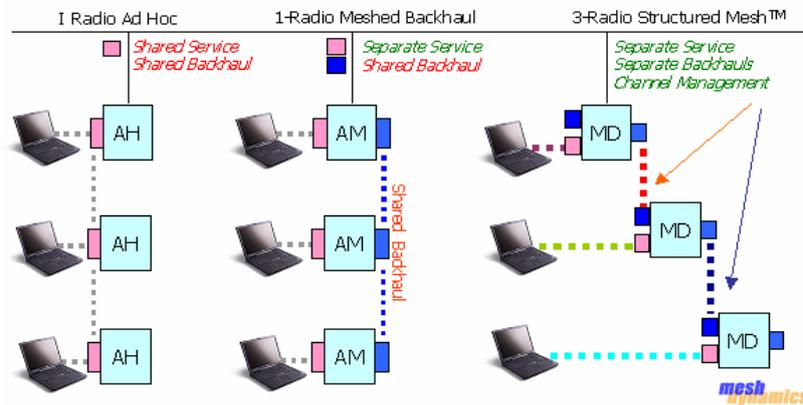


Figura 20 - Topologias WMNs: 1, 2 ou 3 rádios [14]

A primeira, é a tradicional: operação em um rádio e em um canal. No entanto, como os usuários finais também estão usando interfaces sem fio, eles acabam concorrendo o *throughput* com os roteadores, o que degrada ainda mais o desempenho. Na segunda topologia, tem-se os roteadores operando em uma frequência e um canal específico, e os usuários finais utilizando outra frequência. Essa topologia é análoga a uma WMN onde os usuários finais são atendidos por cabos. E, finalmente, a última topologia possui rádios operando em diferentes canais, o que possibilita a transmissão e recepção simultânea em alguns nós. Essa topologia é análoga a uma WMN onde os roteadores possuem mais de um rádio e os usuários finais são atendidos por cabos.

Como já era esperado, o resultado obtido pelo estudo aponta um desempenho muito superior para o equivalente da WMN, onde os roteadores possuem dois rádios e os usuários finais são atendidos por cabo. O referido estudo chama esta topologia de rede *mesh* estruturada.

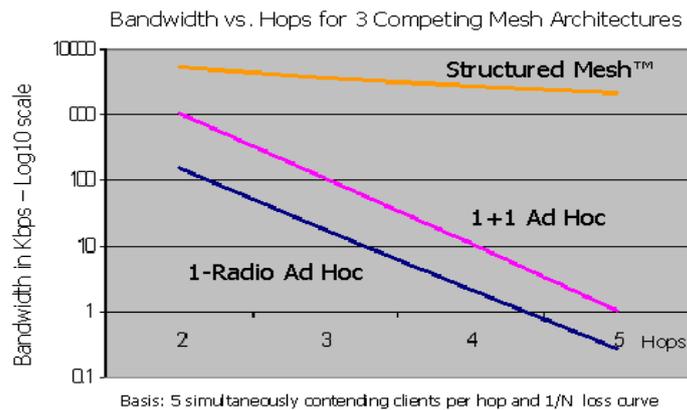


Figura 21 - Resultado comparativo [14]

5.2. Uso de métricas de roteamento que levem em consideração a qualidade do link

A métrica de roteamento traduz o quão boa ou ruim é uma rota. É quantizada, fornece um valor numérico atribuída às mais diversas rotas, para que se possa ter um parâmetro de comparação para a escolha da melhor rota. Em redes que utilizam protocolos de roteamento dinâmicos, os valores das métricas de cada rota são atualizados de tempos em tempos, para que o roteador faça a melhor escolha.

Toda métrica de roteamento é diretamente associada a um custo. Assim sendo, pode-se dizer que a melhor métrica é aquela está associada a um menor custo. As métricas utilizadas em redes sem fio devem levar em consideração não só o número de saltos, como também outros parâmetros como a qualidade dos *links*, por exemplo.

A princípio, a filosofia que adotada era a de se optar por rotas com o menor número de saltos possível. No entanto, não foi difícil perceber que utilizar somente a quantidade de saltos como métrica para o roteamento não era muito eficaz. Essa métrica não leva em consideração propriedades de propagação da onda eletromagnética nem a largura de banda do *link*. Em diversas

situações, uma rota com baixa largura de banda era utilizada por ser constituída de menos saltos que uma rota com uma maior largura de banda disponível.

Assim sendo, outras métricas de roteamento foram desenvolvidas, a fim de se otimizar o desempenho das redes sem fio [15].

5.2.1. Contagem de Saltos

O custo da métrica de roteamento baseada nesta métrica é associado ao número de saltos existentes entre a origem e o destino da transmissão. O custo é diretamente proporcional ao número de saltos, donde conclui-se que, a rota escolhida será aquela que apresentar o menor número de saltos entre o transmissor e o receptor.

A grande vantagem desta métrica é a sua simplicidade e facilidade de implementação. É fácil desenvolver um contador de saltos de uma rota. E ainda, também é fácil comparar o número de saltos existentes entre as mais diversas rotas para se determinar a que possui o menor número de saltos. Além disso, contar número de saltos não requer qualquer medida adicional.

Em contrapartida, a grande desvantagem desta métrica é o fato dela não levar nem consideração a taxa de perdas nem o *throughput* disponível do *link*. Na figura 22, considere que o *link* em azul possui um *throughput* de 20 Mbps, o vermelho de 1 Mbps e o preto de 15 Mbps. Pela métrica da contagem de saltos, se quisermos escolher o melhor caminho para se transmitir de A até C, o caminho a ser escolhido é aquele que está representado pelo *link* em vermelho, uma vez que apenas um salto é necessário. No entanto, este *link* é o que possui o menor *throughput* disponível. Uma melhor opção seria a que escolhesse o *link* em azul, levando-se em consideração que ele possui o maior *throughput* disponível.

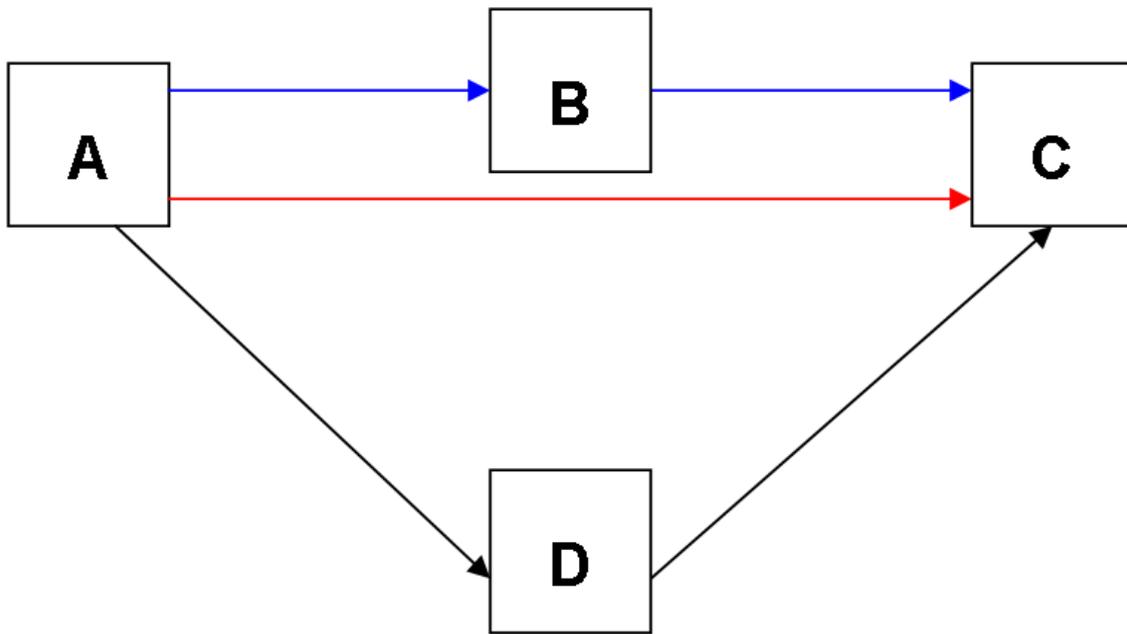


Figura 22 - Métrica de Contagem de Saltos

5.2.2. Round Trip Time por salto

Baseia-se no valor medido de atraso do RTT visto por pacotes sonda *unicast* entre nós vizinhos. O cálculo RTT é feito da seguinte maneira:

1. O nó envia um pacote sonda, contendo a marca de tempo, para cada um dos seus vizinhos, a cada 500ms.
2. Os vizinhos respondem a este pacote sonda imediatamente, através do pacote *ack*. Esse pacote *ack* ecoa a marca de tempo.
3. De posse dos pacotes *ack*, o nó remetente mede o RTT de cada vizinho.

Esta métrica também leva em consideração as amostras passadas das medições realizadas, dando um peso de 10% para o RTT atual, através de uma média exponencial ponderada. O algoritmo também lida com perdas de pacotes sonda, pacotes *ack* ou qualquer outro tipo de pacote que for

detectada. Na ocorrência de qualquer uma dessas perdas, a média exponencial mantida pelo remetente é elevada em 20%.

O custo desta métrica é associado à soma dos RTTs de cada *link*. Assim sendo, a rota que tiver a menor soma de RTTs será a rota escolhida. A qualidade do *link* é medida de diversas maneiras:

1. Nós vizinhos ocupados: pacote sonda e/ou pacote ack sofrerá atraso muito grande, elevando-se o valor do RTT.
2. Outros nós da vizinhança ocupados: pacote sonda e/ou pacote ack sofrerão atraso muito grande, em virtude da ocupação do canal por esses outros nós, elevando-se, novamente, o RTT.
3. *Link* na rota com perdas: 802.11 forçará a retransmissão do pacote sonda e/ou do pacote *ack* até que estes sejam entregues, o que também elevará o RTT.
4. Perdas do pacote *ack* e/ou pacote sonda: o transmissor irá detectar a perda, e aplicará a penalidade de 20% já mencionada anteriormente.

A vantagem desta métrica é que ela evita *links* com altas taxas de perdas e/ou sobrecarregados. No entanto, ela possui algumas desvantagens, como: as eventuais filas que os pacotes sonda estão sujeitos a enfrentar; a dependência com a carga, que pode gerar a chamada instabilidade de rotas; o *overhead* ocasionado pelo uso de pacotes sonda; não leva em consideração a taxa de transmissão de dados com pacotes sonda grandes;

5.2.3. Atraso de um par de pacotes por salto (PktPair)

Baseia-se na medida do atraso de um par de pacotes sonda *back to back* à um nó vizinho. Foi desenvolvida para resolver o problema da distorção da medida do RTT por salto, em virtude dos possíveis atrasos em filas. Essa métrica é obtida da seguinte maneira:

1. Nó transmissor envia um par de pacotes sonda *back to back* a cada vizinho, de 2 em 2 segundos. O primeiro pacote sonda é pequeno e o segundo é grande.
2. Nó receptor é responsável por calcular a diferença de atraso entre a chegada do primeiro e do segundo pacote.
3. Nó transmissor recebe a informação da diferença de atraso dos pacotes sonda que foram enviados ao nó receptor.

Da mesma maneira que ocorre na métrica anterior, o transmissor também leva em consideração os atrasos passados, mantendo uma média exponencial ponderada. Novamente, o custo é associado à soma dos atrasos. E, novamente, essa métrica mede a qualidade do *link* de diversas maneiras:

1. Se o *link* possuir uma alta taxa de perdas, a necessidade de retransmissões irá aumentar o valor da métrica.
2. Se o *link* possuir um baixo *throughput*, o segundo pacote sonda irá sofrer um atraso muito grande, em virtude do seu tamanho, o que também irá ser refletido na métrica.

A grande melhora desta métrica sobre a anterior é a sua menor sensibilidade aos atrasos nas filas, uma vez que os dois pacotes sonda enviados estão sujeitos às mesmas filas. O fato de se utilizar um pacote sonda maior também pode ser considerado uma vantagem, uma vez que torna a métrica mais sensível à largura de banda. A grande desvantagem do uso desta métrica é o *overhead*, que é ainda

maior que o RTT por salto, uma vez que são enviados dois pacotes sonda, sendo que um deles de tamanho maior

5.2.4. Contador de Transmissão Esperada (ETX)

Essa métrica é baseada numa estimativa do número de retransmissões necessárias para se enviar um pacote *unicast*, levando-se em consideração a taxa de perdas de pacotes *broadcast* entre nós vizinhos. Ela é calculada da seguinte maneira:

1. Cada nó envia um pacote probe *broadcast* por segundo. Esse pacote probe contém um contador do número de pacotes probe recebidos pelos nós vizinhos nos últimos 10 segundos.
2. Cada nó calcula a taxa de perdas dos pacotes sonda nos *links* de e para os seus vizinhos.

Essa medida leva em consideração que o 802.11 MAC não retransmite os pacotes *broadcast*. Assim, o nó transmissor é capaz de estimar o número de retransmissões de um pacote *unicast*. Por exemplo, considerando-se dois nós A e B. Se o nó A recebeu 6 pacotes *broadcast* de B nos últimos 10 segundos e B recebeu 9 dos 10 pacotes *broadcast* enviados por A, também nos últimos 10 segundos, pode-se dizer que a taxa de perdas foi de 0,4 para o nó A e 0,1 para o pacote B.

Como já foi visto anteriormente, a transmissão de um pacote só é tida como um sucesso, caso o transmissor receba um pacote *ack* vindo do destino. Para o exemplo acima, temos uma probabilidade de $(1-0,4)*(1-0,1) = 54\%$ para que a transmissão de um pacote seja um sucesso, em uma única tentativa. Assim, temos 46% de que ou o pacote ou o *ack* será perdido. Estatisticamente, se for assumido que as perdas são independentes, o número de retransmissões esperadas é de $1 / 0,54 = 1,851$, que é o valor da métrica ETX para este *link*.

O custo desta métrica é a soma dos ETX de todos os *links* entre o transmissor e o receptor. Assim, a rota que contiver a menor soma de ETX será a rota escolhida. A principal vantagem desta métrica é o menor *overhead*. A sua principal desvantagem é o fato dos pacotes sonda não passarem pela mesma taxa de perda, por se tratarem de pacotes *broadcast*.

5.3. Métricas de roteamento para redes multi-rádios

Além da vantagem de se obter um *throughput* efetivo maior, o uso de mais de um rádio oferece outros pontos fortes adicionais, como uma maior robustez, devido à diversidade em frequências. No entanto, as métricas citadas anteriormente com as quais se costuma trabalhar em redes *mesh* não são as mais adequadas, uma vez que não levam em consideração as interferências entre *links* que utilizam um mesmo canal.

Em [7], há uma proposta de uma métrica de roteamento mais adequada para ser implementada em redes sem fio que utilizam mais de um rádio. É o chamado WCETT. Essa métrica se baseia no ETT, mas leva em consideração, explicitamente, a interferência dos *links* que utilizam um mesmo canal. Essa métrica foi incorporada ao protocolo de roteamento Multi-Radio Link Quality Source Routing (MR-LQSR). Ela assume pouca ou nenhuma mobilidade dos nós, além dos múltiplos rádios de um nó estarem sintonizados em canais não interferentes, o que garante, de fato, uma melhoria em função da existência do rádio extra.

No MQ-LQSR, os nós descobrem *links* para os seus vizinhos e medem a qualidade desses *links*. A informação da qualidade dos *links* é propagada por toda a rede, fazendo com que os nós tenham conhecimento geral da topologia. A escolha das rotas é realizada da seguinte maneira: preferência

por *links* com alto *throughput* e baixas taxas de perda; preferência por caminhos com canais diversos e preferência por caminhos mais curtos.

Através da utilização desta combinação, obteve-se um desempenho 250% melhor que o da contagem de saltos e 80% melhor que o da ETT. Os ganhos foram mais consideráveis em cenários com caminhos mais curtos e com menor carga.

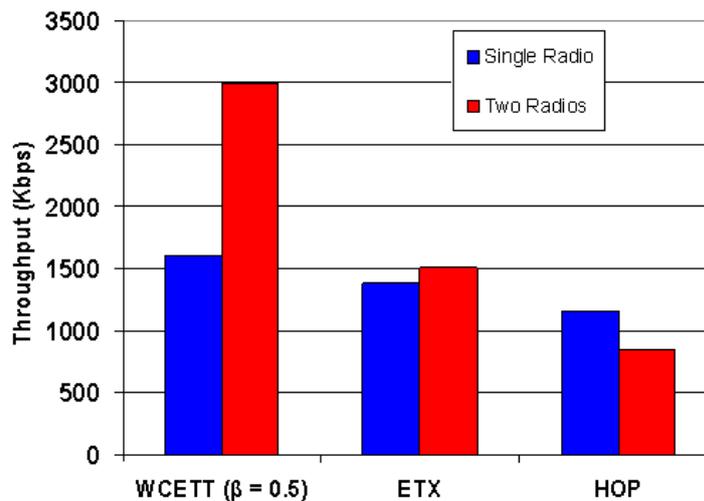


Figura 23 - Comparação WCETT, ETT e HOP [16]

Através da figura 23, pode-se perceber que a eficiência do WCETT é maior, mesmo se só for utilizado um único rádio. No entanto, o seu ganho significativo se dá quando se utiliza dois rádios por nó. Uma curiosidade, é que a métrica de contagem de saltos é pior quando se utiliza dois rádios, ao invés de um só.

5.4. Desenvolvimento de mecanismos que assegurem a justiça nas WMNs

Como já foi abordado anteriormente, nas WMNs, cada nó desempenha, ao mesmo tempo, papel de *host* e roteador. Isso se torna um problema crítico [17]: o nó deverá priorizar o encaminhamento de

pacotes ou deverá priorizar o envio dos pacotes gerados por ele mesmo? Para o funcionamento da rede, como um todo, o que se espera é que haja uma divisão justa de *throughput* disponível entre todos os nós da rede que desejarem utilizá-la num determinado momento.

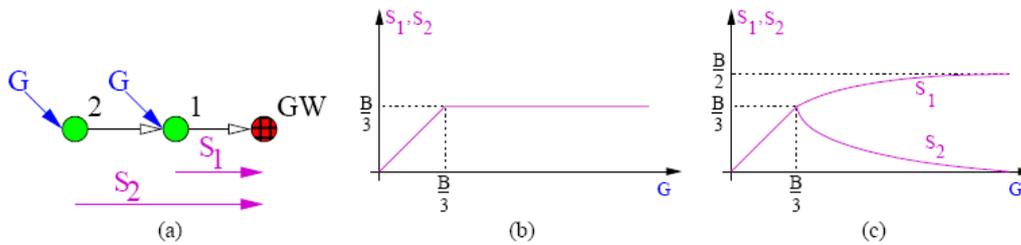


Figura 24 - Justiça nas WMNs [17]

O que se observa em simulações é que os protocolos utilizados nas WMNs são justos, e não absolutamente justos. Na figura 24-a, tem-se uma topologia onde a justiça se faz necessária. Note que o nó mais próximo ao *gateway* está numa situação em que ele está encaminhando pacotes oriundos do nó 2 e, ao mesmo tempo, está transmitindo os seus próprios pacotes para o *gateway*.

No caso ideal, a figura 24-b mostra uma divisão absolutamente justa do *throughput* disponível. O que se concluiu para uma simulação real é que, ao ser submetido a uma crescente demanda por *throughput*, o nó mais próximo ao *gateway* passa a priorizar os seus próprios pacotes e acaba inviabilizando o uso da rede pelo nó 2, como pode ser observado na figura 24-c.

Fica evidente, portanto, a necessidade da criação de protocolos que trabalhem bem a questão da justiça, com diferentes esquemas de filas, por exemplo. Esse tópico será melhor explorado no capítulo 6, aonde serão apresentados os resultados obtidos em medições feitas na própria rede interna da UFF.

5.5. Prover segurança e privacidade.

A segurança nas redes sem fio pode ser considerado um problema crítico. Qualquer pessoa, dentro do alcance da rede, pode ter acesso ao meio, sem qualquer problema., o que já torna essa modalidade de rede menos segura que as redes cabeadas.

Há um ponto ainda mais grave: como as redes sem fio estão, em geral, conectadas à redes internas cabeadas, um possível invasor poderia usar o meio sem fio como porta de entrada para as informações da rede interna de uma empresa, por exemplo.

Pode-se perceber a importância do uso e do desenvolvimento de mecanismos que forneçam uma maior segurança para as redes sem fio. Hoje em dia, existem diversos tipos de segurança implementados nas redes sem fio. Dentre os mecanismos utilizados [18], destacam-se o WEP (*Wired Equivalent Privacy*), que foi proposto em conjunto com o 802.11, o uso de *firewalls* e VPNs com o IPSec.

O porém de todos esses mecanismos de segurança é o *overhead* que eles inserem na rede, fazendo-se necessária uma avaliação de segurança x custo. O artigo “Avaliando a Sobrecarga Introduzida nas Redes 802.11 pelos Mecanismos de Segurança WEP e VPN/IPSec” [18] trata justamente deste assunto.

Neste artigo, é feita uma comparação do *throughput* disponível da rede, para o WEP de 128 bits, o VPN sobre o IPSec e o VPN sobre o IPSec + o WEP de 128 bits. Pode-se perceber, claramente, que a utilização destes mecanismos de segurança, aumenta o *overhead* na rede. Para o tráfego TCP, há uma queda de quase 40% pela utilização do WEP, de 60% pela utilização do VPN sobre o IPSec e de 72% pela combinação dos dois anteriores.

Para o tráfego UDP, a queda pela utilização do WEP foi de 25%, de 43% pela utilização do VPN sobre o IPSec e de 82,35% pela combinação dos dois anteriores. Esses resultados estão representados na tabela 3.

Segurança Tráfego	Sem Segurança	WEP 128 bits	VPN/IPSec	WEP 128 bits + VPN/IPSec
TCP	4,4 Mbps	2,7 Mbps	1,8 Mbps	1,2 Mbps
UDP	5,1 Mbps	3,8 Mbps	2,9 Mbps	0,9 Mbps

Tabela 3 - *Throughput* x Mecanismos de Segurança [18]

6. Procedimento experimental

6.1. Aspectos teóricos

O procedimento experimental a seguir baseia-se no artigo de J. Jun e M. L. Sichitiu [19]. Neste artigo, eles propõem um modelo para se medir o *throughput* nominal da camada de enlace de uma rede *mesh* e também introduzem a questão da justiça nas WMNs, que é abordada mais profundamente no artigo “Fairness and QoS in Multihop Wireless Network”, dos mesmos autores [17]. Segundo eles, é fato que a camada MAC já assegura uma justiça relativamente boa, o que, no entanto, não quer dizer que a camada de rede também o faça.

O objetivo deste teste é medir, na prática, como se comportam os nós da WMN com relação à questão da justiça, já abordada na seção 5.4.

No artigo “Measured Analysis of TCP Behavior across Multihop Wireless and Wired Networks”, os autores deixam claro que “algumas conexões TCP capturam o canal sem fio e levam o *throughput* de outras conexões virtualmente a zero”. [20]

6.2. Topologia da medição

O procedimento experimental para análise do modelo proposto anteriormente foi baseado na topologia apresentada na figura 25 e foi realizado na rede sem fio interna da UFF. Os roteadores sem fio utilizados neste teste são do fabricante *Linksys*, modelo **WRT54G**, que trabalham com apenas com um rádio e com um único canal (no caso destas medições, o **canal 11**). A taxa negociada de transmissão foi fixada em **24 Mbps**.

A ferramenta utilizada para a medição do *throughput* foi o *iperf*. O *iperf* nada mais é do que um medidor máximo de *throughput* disponível entre dois nós da rede, através da geração de tráfego UDP e TCP. Foi desenvolvido por pesquisadores da Universidade de Illinois. O nó para o qual o tráfego será direcionado deverá rodar o modo servidor desta aplicação ao passo que, o nó de origem do tráfego deverá rodar o modo cliente. Neste cenário, o nó mais próximo ao *gateway* rodou o modo servidor do *iperf* e os demais nós executaram o cliente.

O *iperf* imprime na tela os resultados obtidos com as medições, quase que instantaneamente. No caso destas medições, como seria necessário trabalhar em cima das medições para apresentá-las em formato gráfico, o *iperf* imprimiu os resultados dentro de um determinado arquivo. Abaixo, segue um exemplo de como o *iperf* mostra os resultados medidos:

```
-----
Client connecting to 10.151.8.1, TCP port 5001
TCP window size: 16.0 KByte (default)
-----
[ 6] local 10.151.9.1 port 1052 connected with 10.151.8.1 port 5001
[ ID] Interval      Transfer      Bandwidth
[ 6] 0.0- 1.0 sec   1728 KBytes   14156 Kbits/sec
[ 6] 1.0- 2.0 sec   1768 KBytes   14483 Kbits/sec
[ 6] 2.0- 3.0 sec   1752 KBytes   14352 Kbits/sec
[ 6] 3.0- 4.0 sec   1720 KBytes   14090 Kbits/sec
[ 6] 4.0- 5.0 sec   1752 KBytes   14352 Kbits/sec
[ 6] 5.0- 6.0 sec   1768 KBytes   14483 Kbits/sec
[ 6] 6.0- 7.0 sec   1720 KBytes   14090 Kbits/sec
[ 6] 7.0- 8.0 sec   1720 KBytes   14090 Kbits/sec
[ 6] 8.0- 9.0 sec   1776 KBytes   14549 Kbits/sec
[ 6] 9.0-10.0 sec   1768 KBytes   14483 Kbits/sec
[ 6] 10.0-11.0 sec  1728 KBytes   14156 Kbits/sec
[ 6] 11.0-12.0 sec  1768 KBytes   14483 Kbits/sec
[ 6] 12.0-13.0 sec  1720 KBytes   14090 Kbits/sec
[ 6] 13.0-14.0 sec  1752 KBytes   14352 Kbits/sec
[ 6] 14.0-15.0 sec  1744 KBytes   14287 Kbits/sec
[ 6] 15.0-16.0 sec  1736 KBytes   14221 Kbits/sec
[ 6] 16.0-17.0 sec  1776 KBytes   14549 Kbits/sec
[ 6] 17.0-18.0 sec  1752 KBytes   14352 Kbits/sec
[ 6] 18.0-19.0 sec  1744 KBytes   14287 Kbits/sec
[ 6] 19.0-20.0 sec  1648 KBytes   13500 Kbits/sec
[ 6] 20.0-21.0 sec  1728 KBytes   14156 Kbits/sec
[ 6] 21.0-22.0 sec  1768 KBytes   14483 Kbits/sec
[ 6] 22.0-23.0 sec  1752 KBytes   14352 Kbits/sec
[ 6] 23.0-24.0 sec  1720 KBytes   14090 Kbits/sec
[ 6] 24.0-25.0 sec  1752 KBytes   14352 Kbits/sec
[ 6] 25.0-26.0 sec  1768 KBytes   14483 Kbits/sec
[ 6] 26.0-27.0 sec  1720 KBytes   14090 Kbits/sec
[ 6] 27.0-28.0 sec  1720 KBytes   14090 Kbits/sec
[ 6] 28.0-29.0 sec  1776 KBytes   14549 Kbits/sec
```

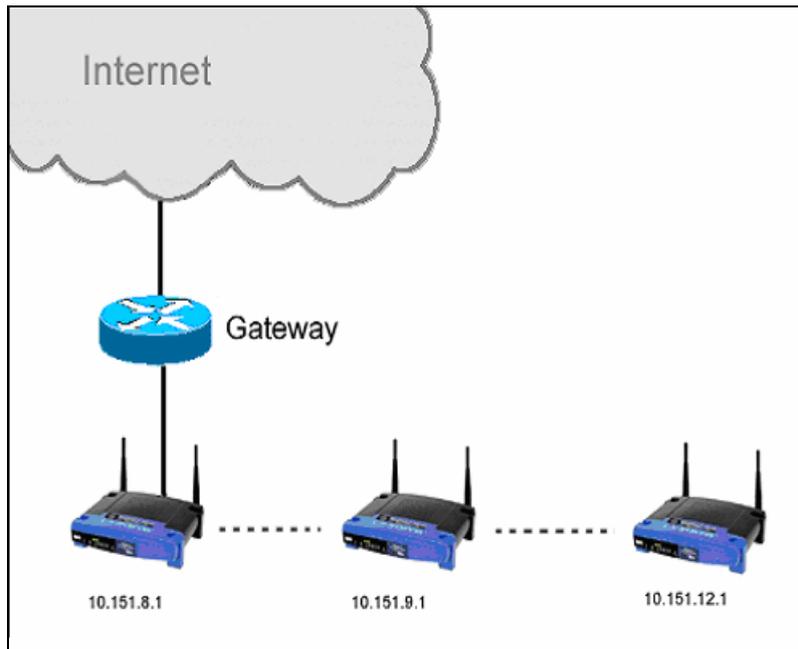


Figura 25 - Topologia dos testes

6.3. Cenários da medição

A rede interna da UFF utiliza o protocolo de roteamento dinâmico, OLSR, baseado na métrica ETX. Como já foi visto anteriormente, nesta métrica, cada nó transmite um pacote *broadcast* por segundo, o que acaba aumentando o *overhead*, e conseqüentemente, diminuindo o *throughput*.

Por isso, num primeiro momento, o protocolo de roteamento dinâmico, OLSR, foi desativado e substituído por rotas estáticas. O objetivo principal foi eliminar ao máximo o *overhead* associado à métrica ETX. Ainda nesse cenário, todos os testes se repetiram tanto para TCP, quanto para UDP. Assim, foi criado um parâmetro de comparação para se verificar como os mecanismos de controle de fluxo do TCP interferem no desempenho da rede.

Num segundo momento, o protocolo de roteamento dinâmico foi ativado. Assim, as rotas estáticas foram substituídas por rotas dinâmicas. Neste novo cenário, pretendeu-se avaliar a influência do

protocolo de roteamento no desempenho da rede. Também para este cenário, todos os testes se repetiram tanto para TCP, quanto para UDP, pelos mesmos motivos apresentados acima.

Para esses dois cenários distintos, foi realizada a seguinte rotina de testes:

- Medição do *throughput* dos enlace 1, 2 e 3, separadamente;
- Medição do *throughput* simultâneo dos enlaces 1 e 2;
- Medição do *throughput* simultâneo dos enlaces 1 e 2, em ordem inversa;

A idéia de se medir o *throughput* simultâneo dos enlaces 1 e 2 de duas maneiras diferentes, ora começando o gerador de tráfego, TCP ou UDP, do enlace 1, ora do enlace 2, é verificar se o primeiro enlace estabelecido tem alguma prioridade sobre o segundo, ou vice-versa.

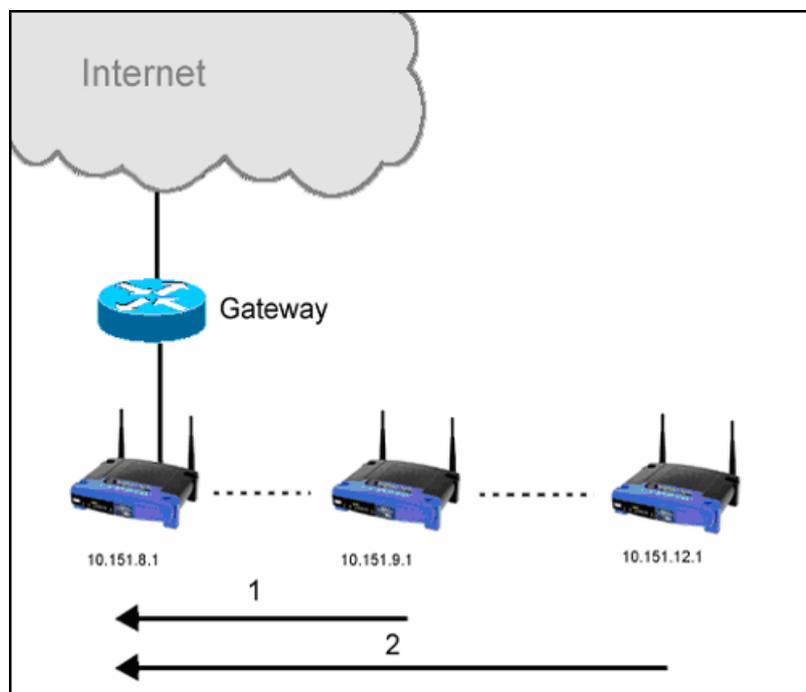


Figura 26 - Cenário – Teste

6.4. Resultados obtidos sem a atuação do OLSR

Para a realização desta etapa das medições, o protocolo de roteamento dinâmico foi desativado. Em seguida, as seguintes rotas estáticas foram colocadas em cada um dos nós:

- Nó 10.151.8.1 (o mais próximo ao *gateway*):

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
10.151.12.1	10.151.9.1	255.255.255.255	UGH	2	0	0	eth1
10.151.2.1	10.151.9.1	255.255.255.255	UGH	3	0	0	eth1
10.151.9.1	*	255.255.255.255	UH	1	0	0	eth1
10.152.0.224	*	255.255.255.224	U	0	0	0	vlan0
200.20.15.0	*	255.255.255.0	U	0	0	0	vlan1
10.151.0.0	*	255.255.0.0	U	0	0	0	eth1
default	rt.ic.uff.br	0.0.0.0	UG	0	0	0	vlan1

- Nó 10.151.9.1:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
10.151.12.1	*	255.255.255.255	UH	1	0	0	eth1
10.151.8.1	*	255.255.255.255	UH	1	0	0	eth1
10.151.2.1	10.151.12.1	255.255.255.255	UGH	2	0	0	eth1
10.152.1.0	*	255.255.255.224	U	0	0	0	vlan0
10.151.0.0	*	255.255.0.0	U	0	0	0	eth1

- Nó 10.151.12.1

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
10.151.8.1	10.151.9.1	255.255.255.255	UGH	2	0	0	eth1
10.151.2.1	*	255.255.255.255	UH	1	0	0	eth1
10.151.9.1	*	255.255.255.255	UH	1	0	0	eth1
10.152.1.96	*	255.255.255.224	U	0	0	0	vlan0
10.151.0.0	*	255.255.0.0	U	0	0	0	eth1

6.4.1. TCP

a) Medição do *throughput* dos enlaces 1 e 2, separadamente.

1. 14258 kbps
2. 2479 kbps

Os gráficos das figuras 27 e 28 mostram a variação dos *throughputs* ao longo do tempo. Como foi apontado anteriormente, o *throughput* deve cair à metade quando se aumenta um salto (figura 18). Esse fato se explica por um nó não poder enviar e receber dados ao mesmo tempo. Ao se analisar o *throughput* médio, percebe-se que a degradação do *throughput* em função do número de saltos é de uma ordem superior à metade.

Ou seja, na prática, o desempenho é ainda pior do que o esperado pela teoria. É possível que este fato seja causado pela queda do *throughput* com o aumento da distância (figura 12) ou até mesmo por interferências que podem exercer influência no caminho entre os nós.

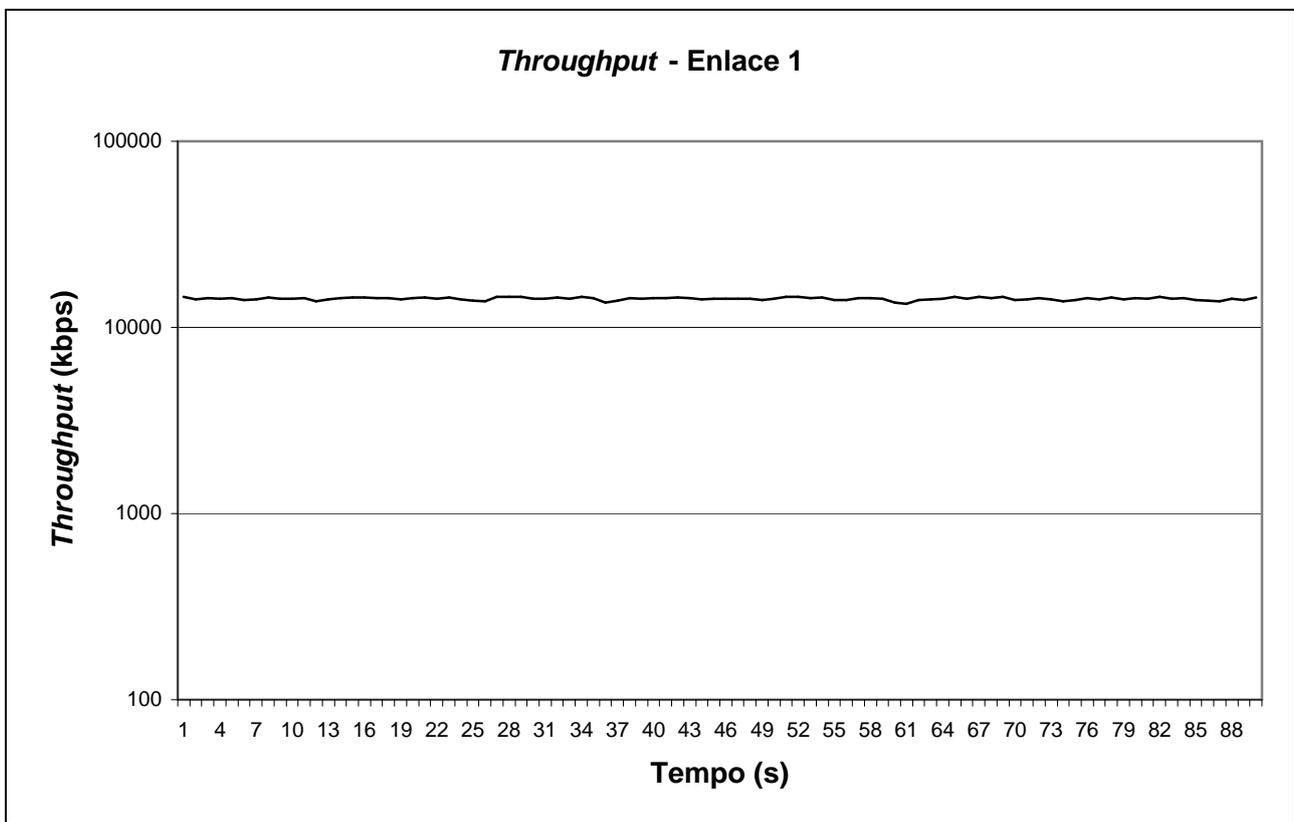


Figura 27 - Medição - TCP - Sem OLSR - Enlace 1

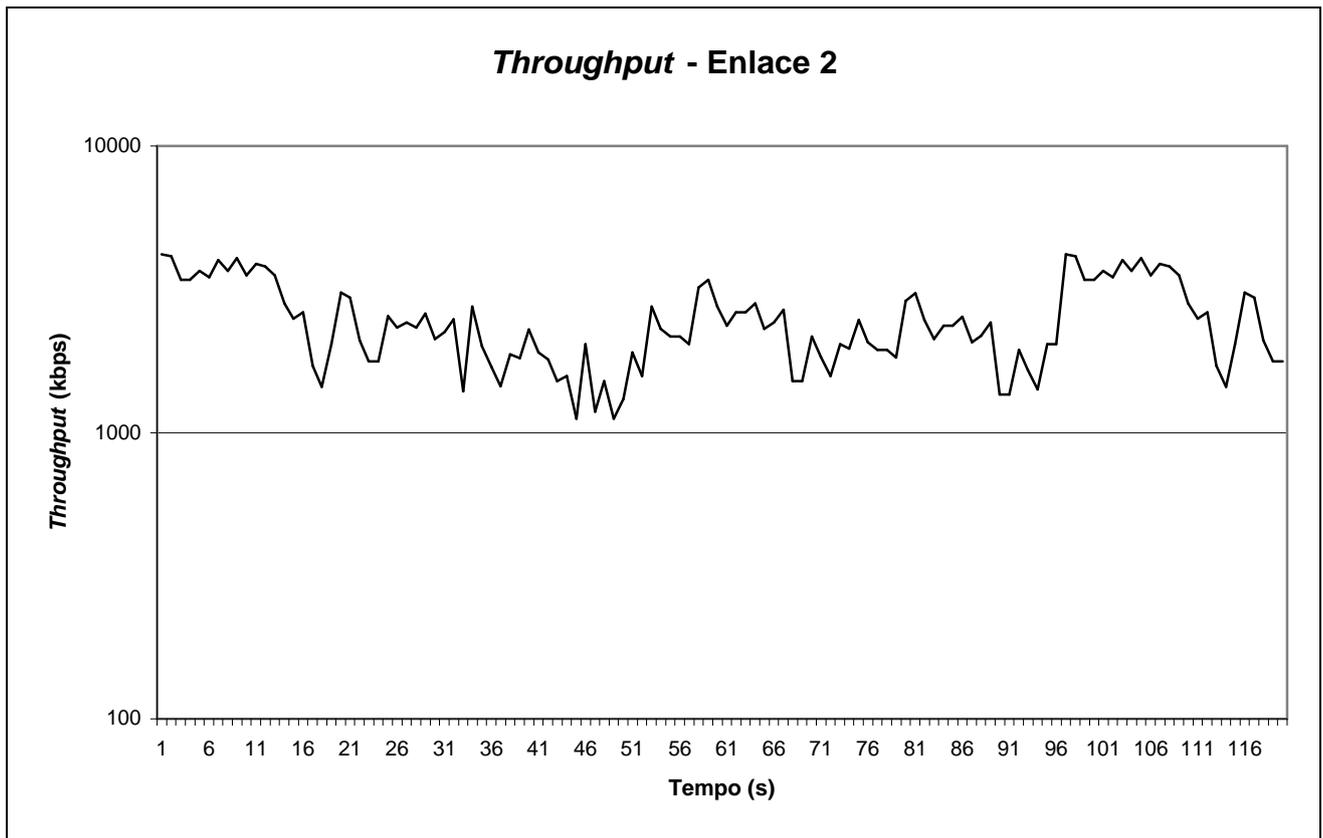


Figura 28 - Medição - TCP - Sem OLSR - Enlace 2

b) Medição do *throughput* simultâneo dos enlaces 1 e 2

Para a realização desta medição, inicialmente, foi acionado o *iperf* apenas do enlace 1. Aproximadamente 30 segundos após o início da medição, o *iperf* do enlace dois foi executado.

Analisando-se o resultado desta medição, pode-se perceber que o enlace 1, que está mais próximo ao *gateway*, nem percebe a presença do enlace 2. Ele simplesmente pára de encaminhar os pacotes vindos do enlace 2 e prioriza os seus próprios pacotes. O enlace 1 continua com o seu *throughput* médio, enquanto que o enlace 2 fica impossibilitado de utilizar a rede. Através desta medição, pode-se perceber que a justiça não está sendo implementada.

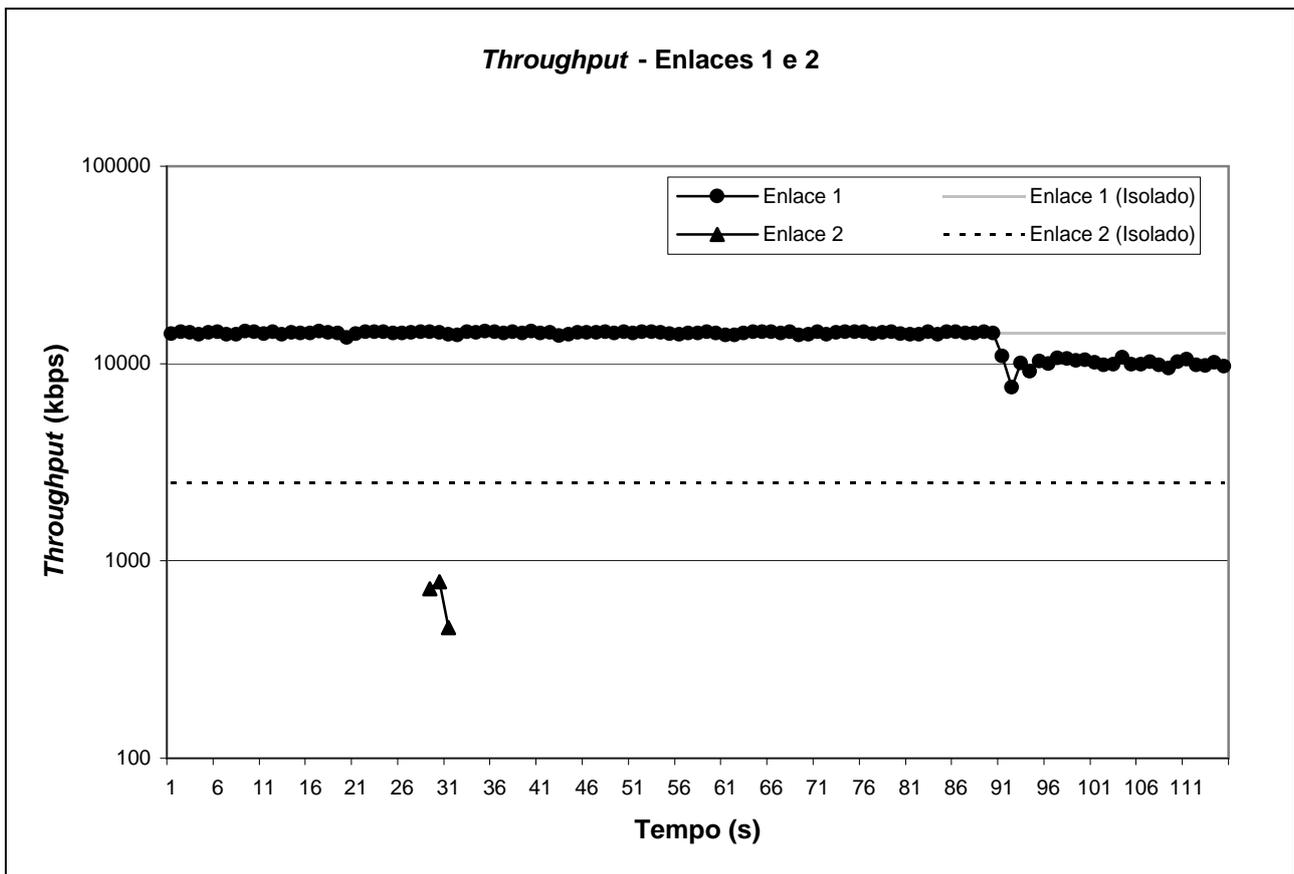


Figura 29 - Medição - TCP - Sem OLSR - Enlaces 1 e 2

O *throughput* médio disponível para o enlace 1 foi de 14283 kbps, ou seja, aproximadamente o mesmo *throughput* medido de quando não havia concorrência. Já para o enlace 2, foi de aproximadamente zero. Configura-se um cenário completamente desfavorável para o enlace 2.

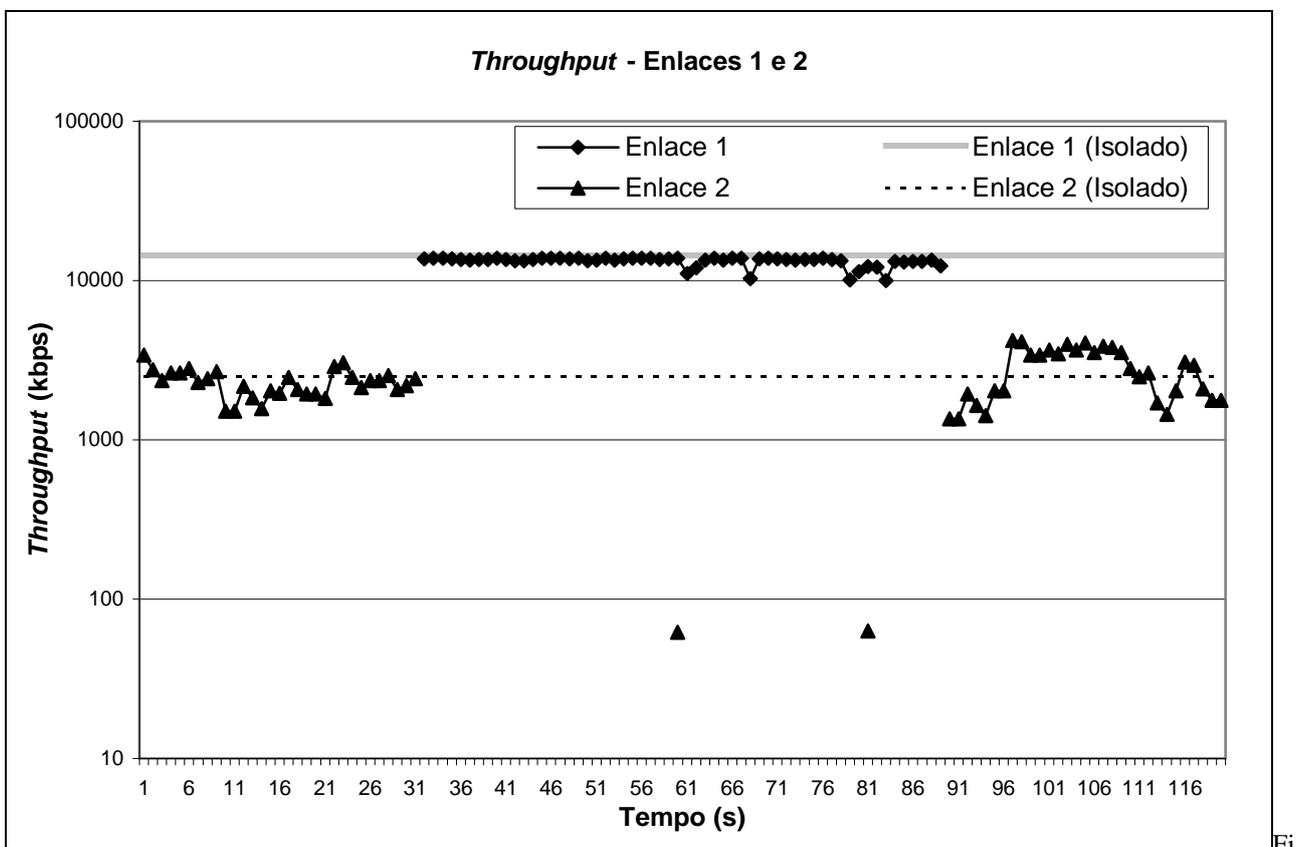
c) Medição do *throughput* simultâneo dos enlaces 1 e 2, em ordem inversa.

Trata-se da mesma medição realizada anteriormente, mas neste caso, o primeiro gerador de tráfego TCP a ser acionado é o do enlace 2.

Para este teste, a mesma situação ocorreu. O enlace 1, por estar mais perto do *gateway*, pára de encaminhar os pacotes vindos de outros nós da rede e passa a priorizar somente os seus próprios. Ao ter o seu gerador de fluxo TCP acionado, o enlace 1 simplesmente derruba o enlace 2, que passa a não ter mais acesso à rede. Ao ser interrompido, o enlace 2 passa a poder utilizar a rede

novamente. Novamente, a justiça não pôde ser observada nesta medição. O que espera-se, para os demais testes, é que este cenário se repita, somente com uma diferença do *throughput* disponível, uma vez que o TCP possui o controle de fluxo e o OLSR aumenta o *overhead* na rede.

A idéia de se inverter a ordem de acionamento do *iperf* é garantir que o nó com a conexão já estabelecida não tenha nenhuma prioridade sobre os demais que querem utilizar a rede. O que se observa é que, apesar do enlace 2 ter sido estabelecido primeiro, ao se executar o gerador de tráfego TCP do enlace 1, este, por estar mais próximo ao *gateway*, passa a utilizar a rede em benefício próprio e, como ocorreu anteriormente, pára de encaminhar os pacotes vindo dos outros nós. O *throughput* medido para o enlace 1 durante a concorrência ao meio foi de 13213 kbps e, para o enlace 2, ele novamente tendeu a zero.



gura 30 - Medição - TCP - Sem OLSR - Enlaces 1 e 2, em ordem inversa

6.5.2. UDP

Uma vez que o UDP **não** possui controle de fluxo, espera-se que os resultados das medições de *throughput* sejam superiores aos obtidos na medição realizada com o TCP.

a) Medição do *throughput* dos enlaces 1 e 2, separadamente.

1. 17949 kbps
2. 3774 kbps

Como já era esperado, os resultados medidos para o UDP foram consideravelmente maiores, uma vez que este protocolo não apresenta o controle de fluxo do TCP. O aumento para o enlace 1 foi de 26% e para o enlace 2 foi de 52%. O ganho de *throughput* foi mais significativo para o enlace que envolve o nó que está mais distante do *gateway*.

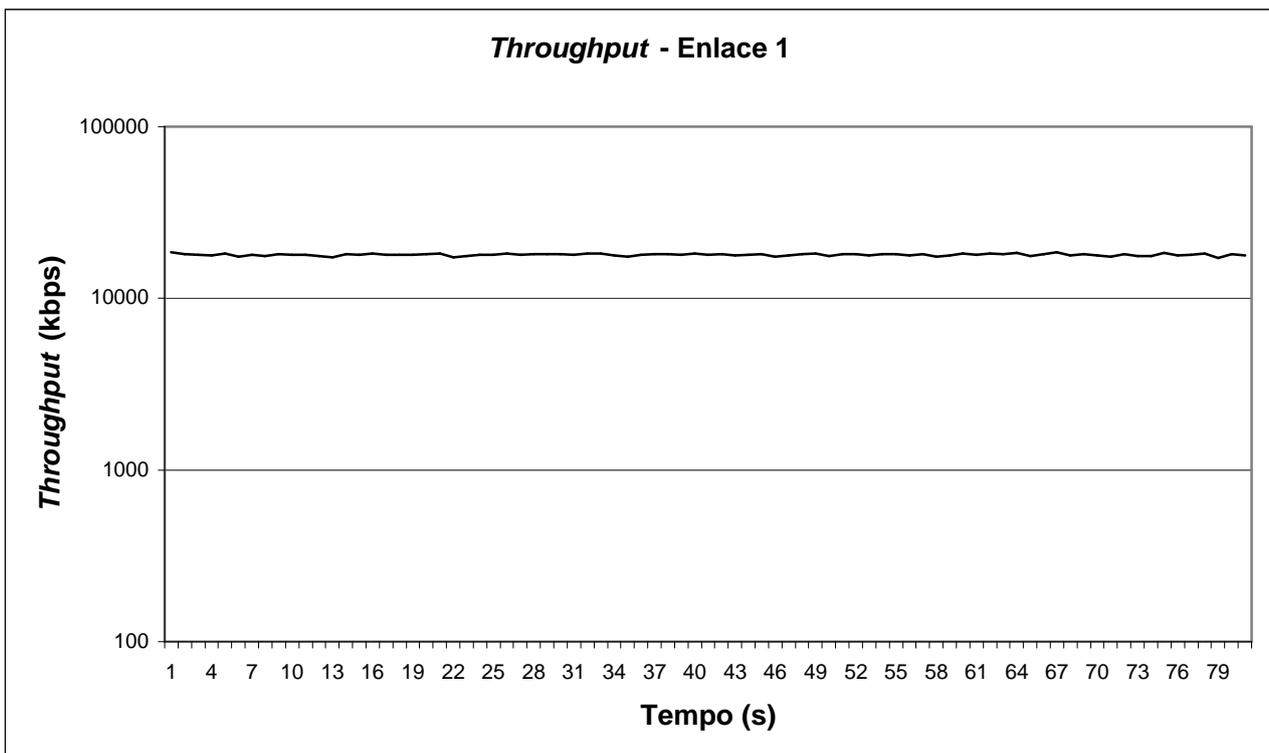


Figura 31 - Medição – UDP – Sem OLSR – Enlace 1

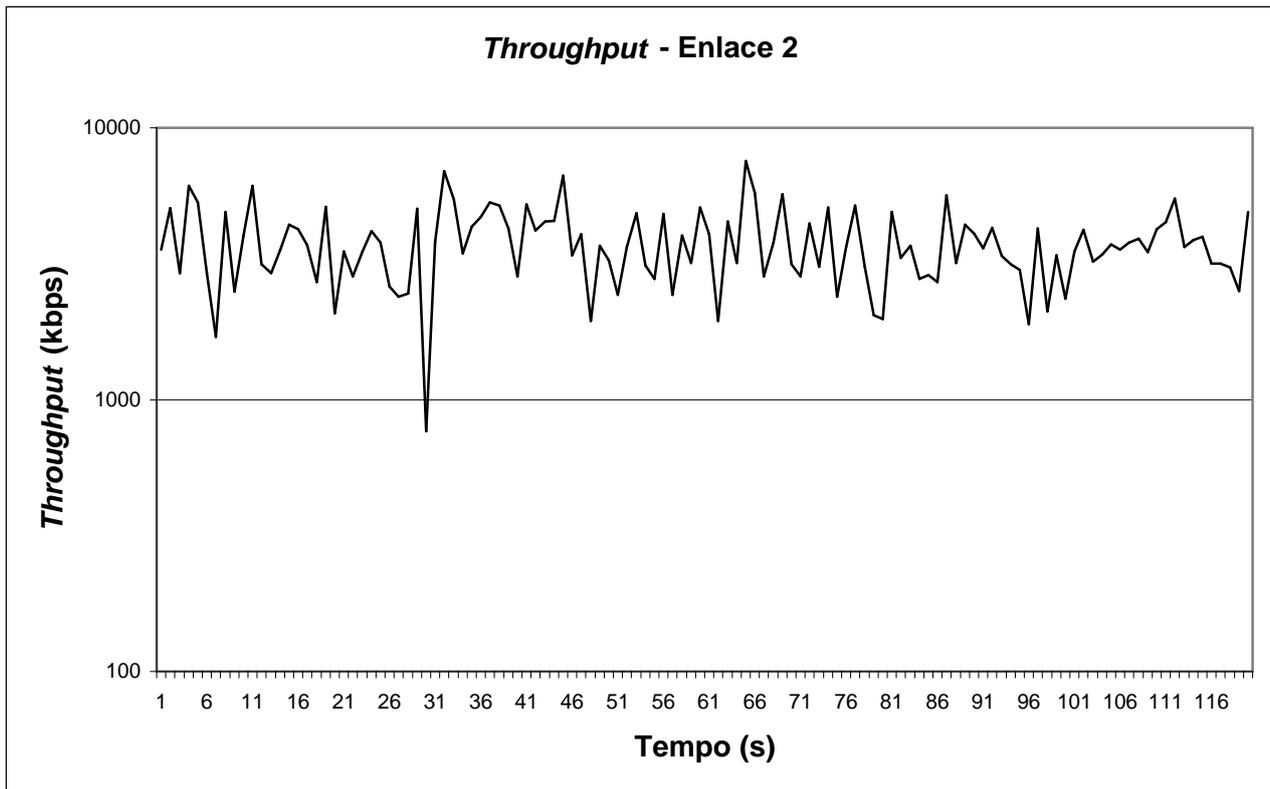


Figura 32 - Medição – UDP – Sem OLSR – Enlace 2

b) Medição do *throughput* simultâneo dos enlaces 1 e 2

Para a realização desta medição, inicialmente, foi acionado o *iperf* apenas do enlace 1. Aproximadamente 30 segundos após o início da medição, o *iperf* do enlace dois foi executado.

Nesta medida, pode-se perceber que ainda sobra algum *throughput* para o enlace 2. Uma situação bem melhor do que a que ocorreu para o TCP. No entanto, a justiça está longe de ocorrer nesta situação, uma vez que a queda do *throughput* disponível para este enlace é muito grande. Também vale observar que, para o enlace 1, o *throughput* permaneceu praticamente o mesmo.

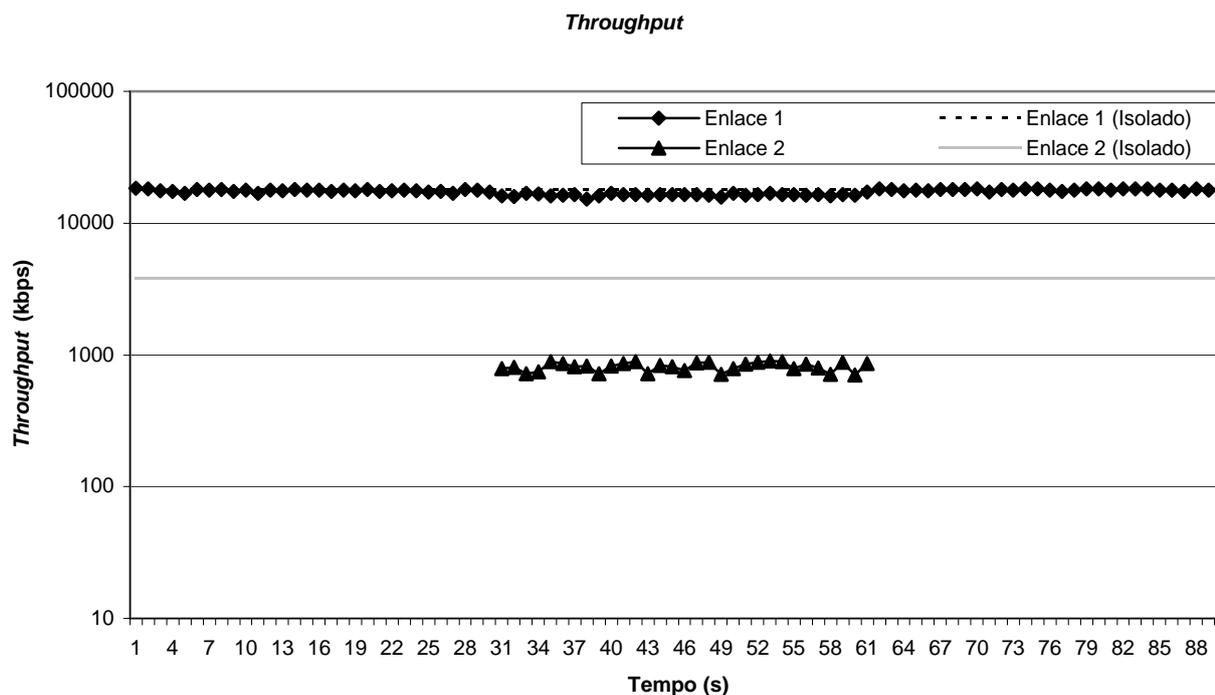


Figura 33 - Medição – UDP – Sem OLSR – Enlace 1 e 2

O *throughput* medido para o enlace 1 foi de 16384 kbps e, para o enlace 2, foi de 814,06. Isso representa uma queda de 9% para o enlace 1 e de quase 80% para o enlace 2.

c) Medição do *throughput* simultâneo dos enlaces 1 e 2, em ordem inversa

Trata-se da mesma medição realizada anteriormente, mas neste caso, o primeiro gerador de tráfego TCP a ser acionado é o do enlace 2. As mesmas observações feitas para o item anterior valem para esta medição.

Para o enlace 1, tem-se um *throughput* medido de 15147 kbps e, para o enlace 2, um de 794 kbps. Ou seja, a situação anterior se repete aqui, donde pode-se concluir que não há qualquer tipo de privilégio para o enlace que é estabelecido primeiro.

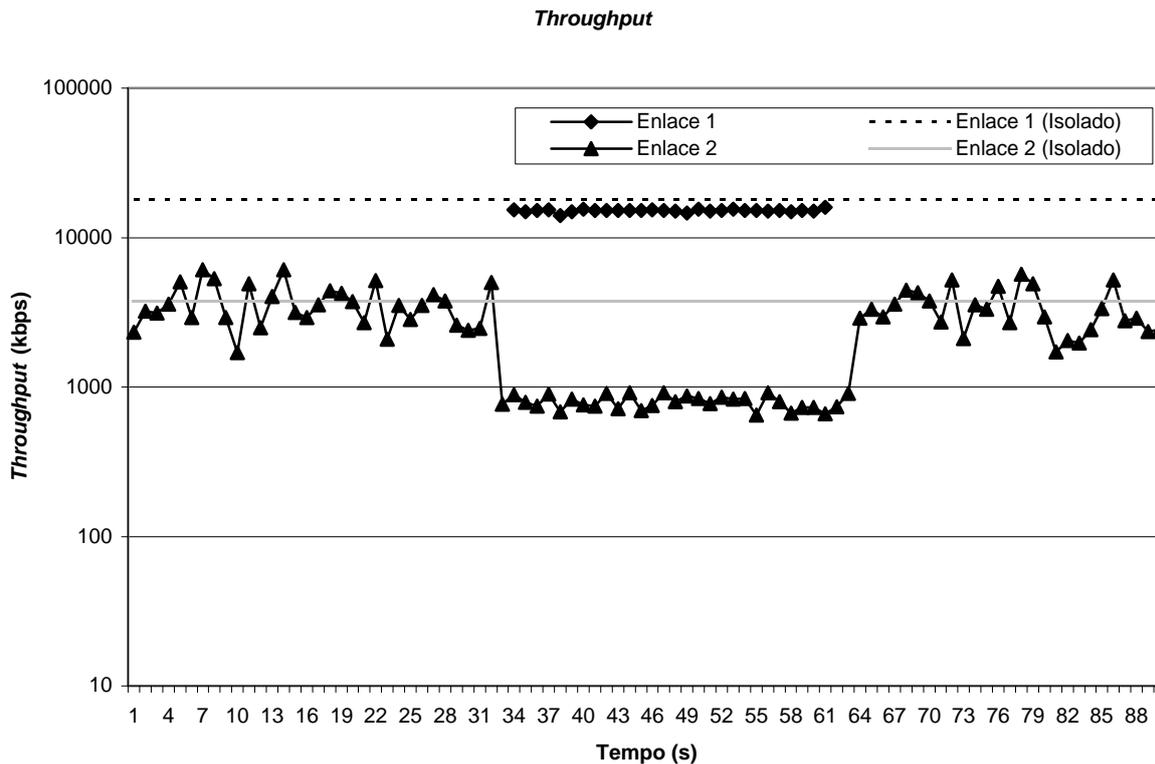


Figura 34 - Medição – UDP – Sem OLSR – Enlaces 1 e 2, em ordem inversa

6.6. Resultados obtidos com a atuação do OLSR

Para a realização desse teste, o OLSR foi habilitado. A topologia obtida dinamicamente foi a mostrada na figura 35. Esta topologia é disponibilizada no sítio do GT-Mesh (<http://mesh.ic.uff.br>), e é atualizada dinamicamente, quando o OLSR está habilitado.

Avaliando-se a topologia obtida dinamicamente, pode se concluir que se trata da mesma topologia utilizada nos testes sem roteamento dinâmico. Com isso, pode-se assumir que, na topologia proposta anteriormente, cada nó só consegue se comunicar diretamente com o nó vizinho. Nesta análise, pretende avaliar a influência da existência do protocolo de roteamento dinâmico no desempenho da rede. *A priori*, pode-se esperar resultados inferiores aos obtidos anteriormente, uma vez que a presença do protocolo de roteamento dinâmico, associado à métrica ETX, aumenta o *overhead* na rede.

Rede interna

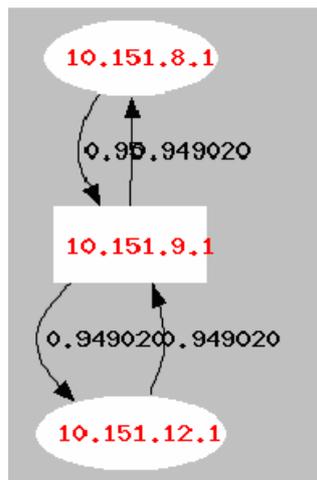


Figura 35 - Topologia obtida dinamicamente

6.6.1. TCP

a) Medição do *throughput* dos enlace 1 e 2, separadamente.

1. 13333 kbps
2. 2283 kbps

Avaliando-se o resultado destas medições, pode-se perceber que eles são inferiores aos resultados obtidos para o TCP, sem a presença do protocolo de roteamento dinâmico. Como foi antecipado, esse resultado já era esperado, uma vez que a presença do protocolo de roteamento dinâmico aumenta o *overhead* na rede.

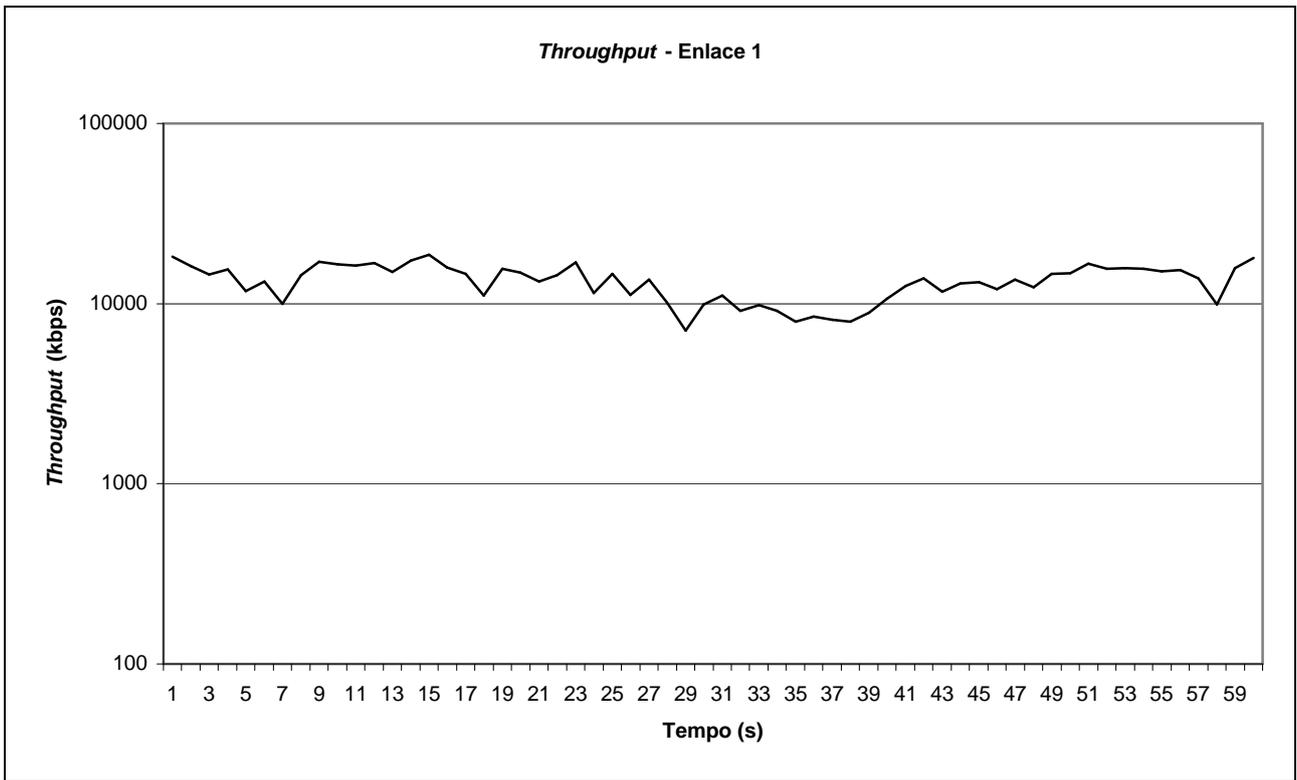


Figura 36 - Medição – TCP – Com OLSR – Enlace 1

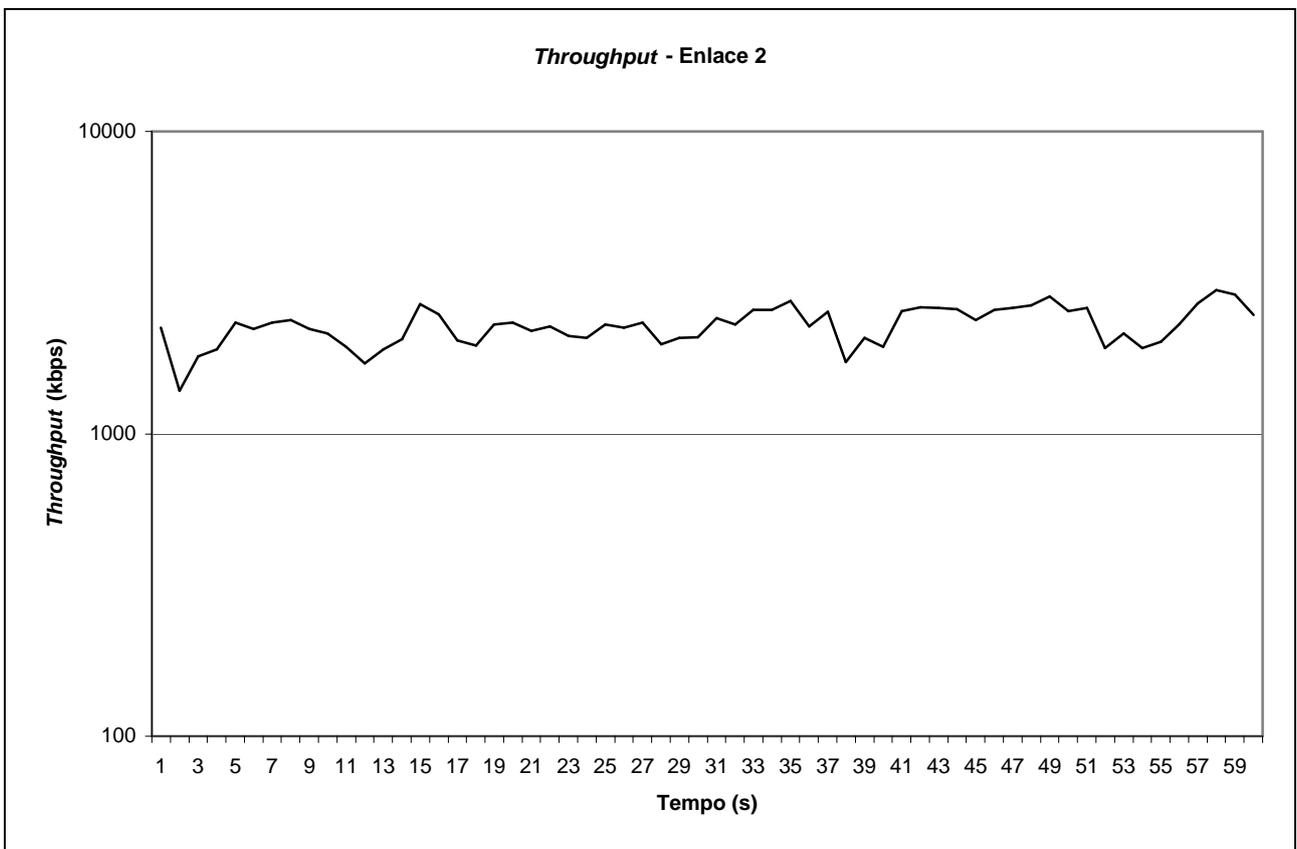


Figura 37 - Medição – TCP – Com OLSR – Enlace 2

b) Medição do *throughput* simultâneo dos enlaces 1 e 2

Para a realização desta medição, inicialmente, foi acionado o medidor de *throughput* apenas do enlace 1. Após alguns instantes, foi acionado o medidor de *throughput* do enlace 2.

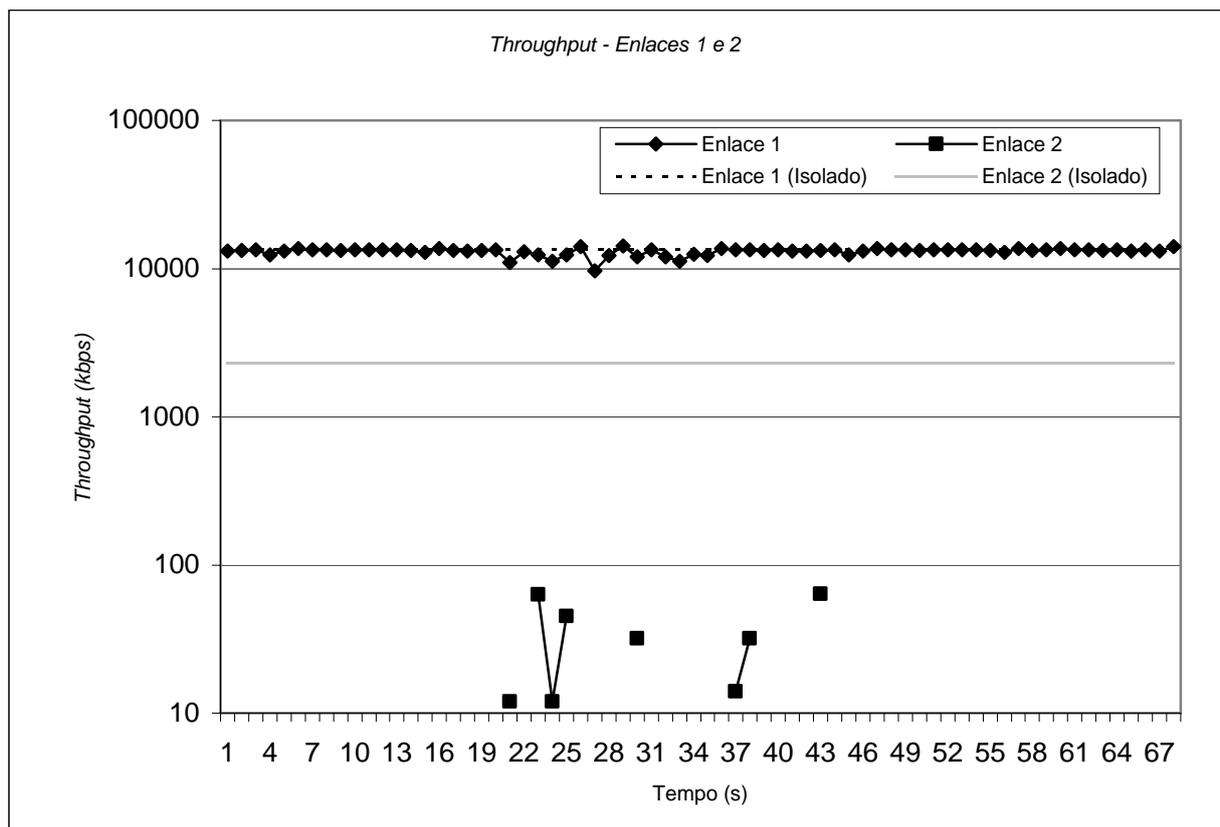


Figura 38 - Medição – TCP – Com OLSR – Enlaces 1 e 2

Para este teste, observa-se o mesmo comportamento da situação em que o protocolo de roteamento dinâmico estava desabilitado. No entanto, os valores medidos são consideravelmente menores, e podem ser atribuídos ao overhead inserido pelo protocolo de roteamento dinâmico.

Para o enlace 1, mediu-se um *throughput* de 12621 kbps e, para o enlace 2, observou-se um *throughput* que tendeu a zero.

c) Medição do *throughput* simultâneo dos enlaces 1 e 2, em ordem inversa.

Para a realização desta medição, inicialmente, foi acionado o medidor de *throughput* apenas do enlace 2. Após alguns instantes, foi acionado o medidor de *throughput* do enlace 1.

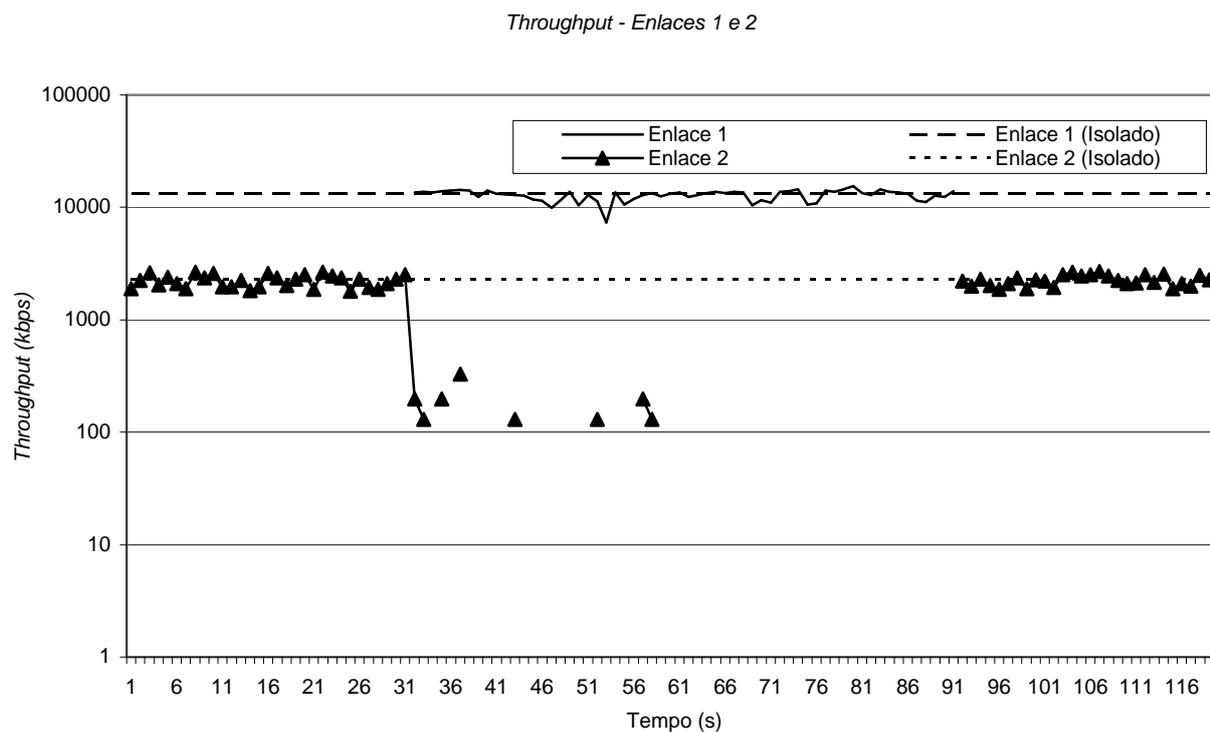


Figura 39 - Medição – TCP – Com OLSR – Enlaces 1 e 2, em ordem inversa

Mais uma vez o comportamento da medição realizada sem a presença do protocolo de roteamento dinâmico se repetiu, com valores de *throughput* menores, como já era esperado. Para o enlace 1, mediu-se um *throughput* de 12796 kbps e, para o enlace 2, novamente mediu-se um *throughput* aproximadamente nulo.

6.5.2. UDP

a) Medição do *throughput* dos enlace 1 e 2, separadamente.

1. 16518 kbps

2. 3211 kbps

Avaliando-se o resultado destas medições, pode-se perceber que eles são inferiores aos resultados obtidos para o UDP, sem a presença do protocolo de roteamento dinâmico. Como foi antecipado, esse resultado já era esperado, uma vez que a presença do protocolo de roteamento dinâmico aumenta o *overhead* na rede.

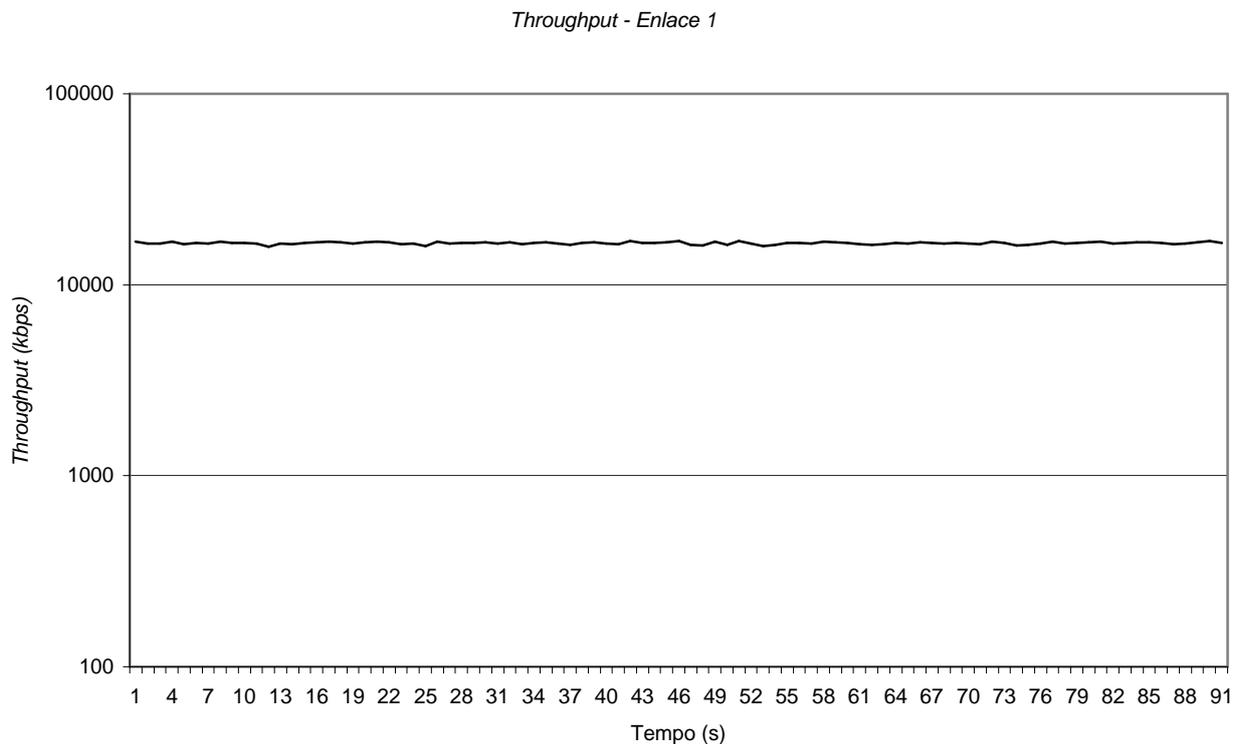


Figura 40 - Medição – UDP – Com OLSR – Enlace 1

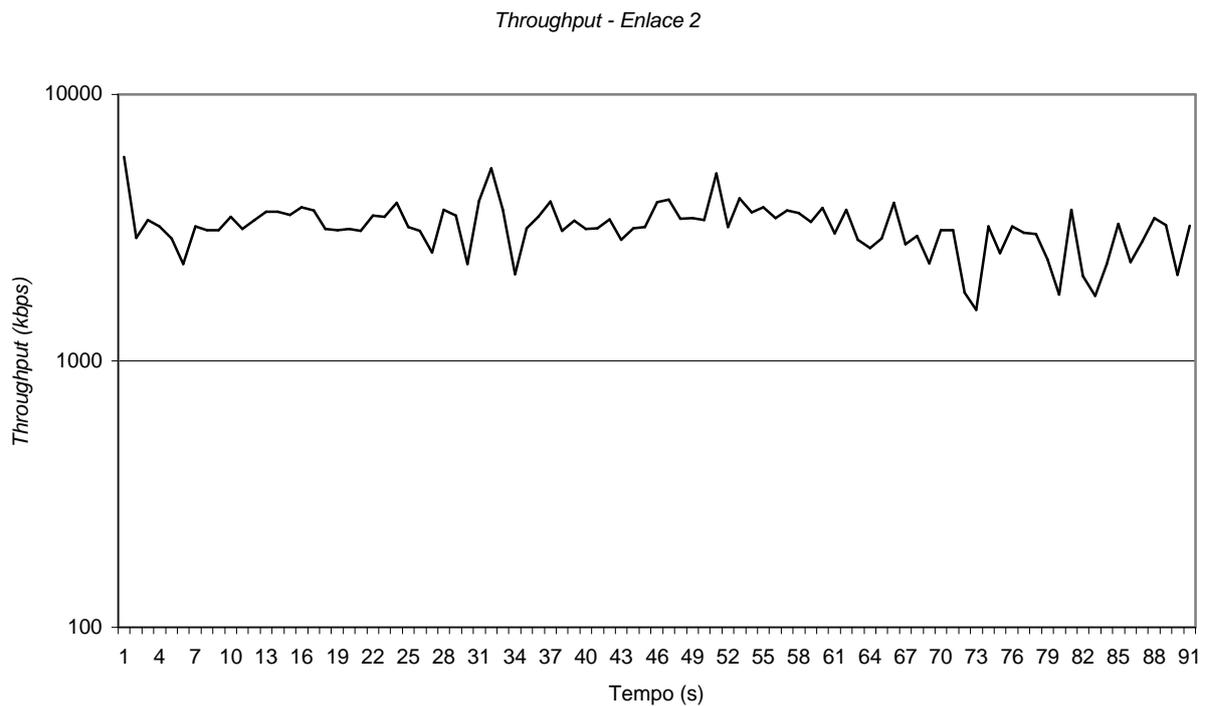


Figura 41 - Medição – UDP – Com OLSR – Enlace 2

b) Medição do *throughput* simultâneo dos enlaces 1 e 2

Para a realização desta medição, inicialmente, foi acionado o medidor de *throughput* apenas do enlace 1. Após alguns instantes, foi acionado o medidor de *throughput* do enlace 2.

O valor medido para o enlace 1 foi de 13325 kbps e, para o enlace 2, foi de 460 kbps. Comparando-se este mesmo teste com o análogo, só que para TCP, tem-se um aumento significativo do *throughput*, para ambos os enlaces.

Throughput - Enlaces 1 e 2

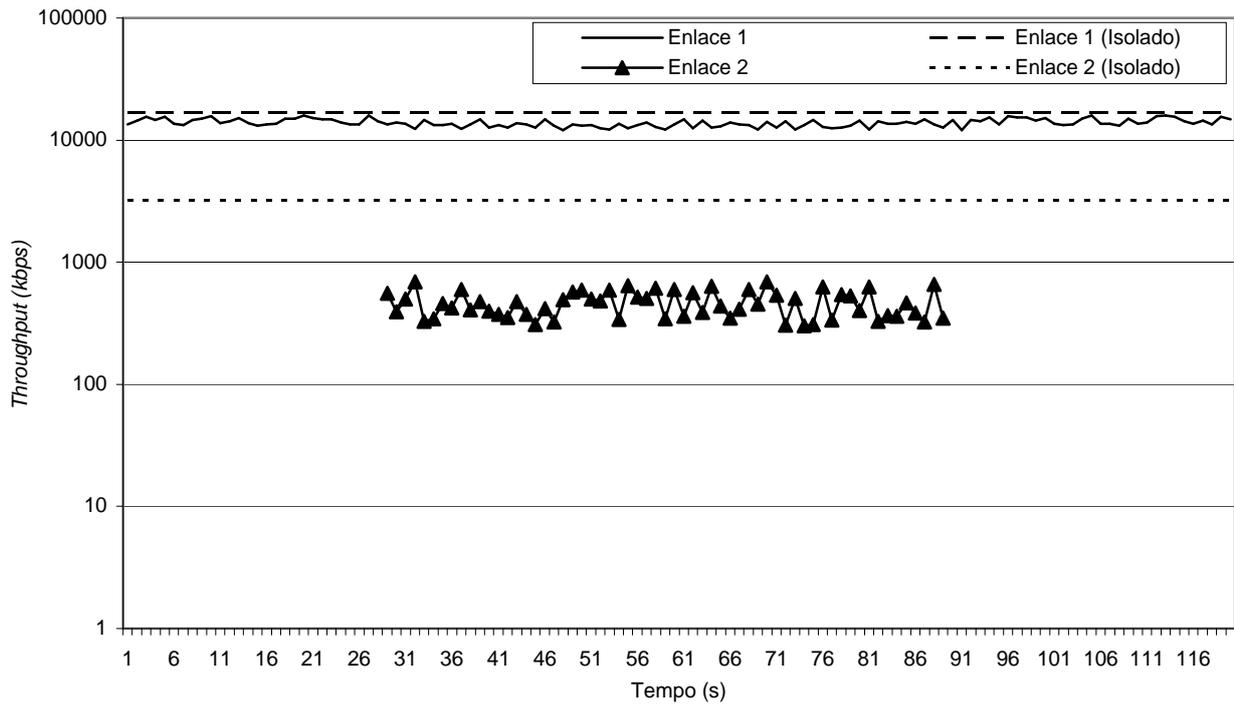


Figura 42- Medição – UDP – Com OLSR – Enlaces 1 e 2

c) Medição do *throughput* simultâneo dos enlaces 1 e 2, em ordem inversa.

Throughput - Enlaces 1 e 2

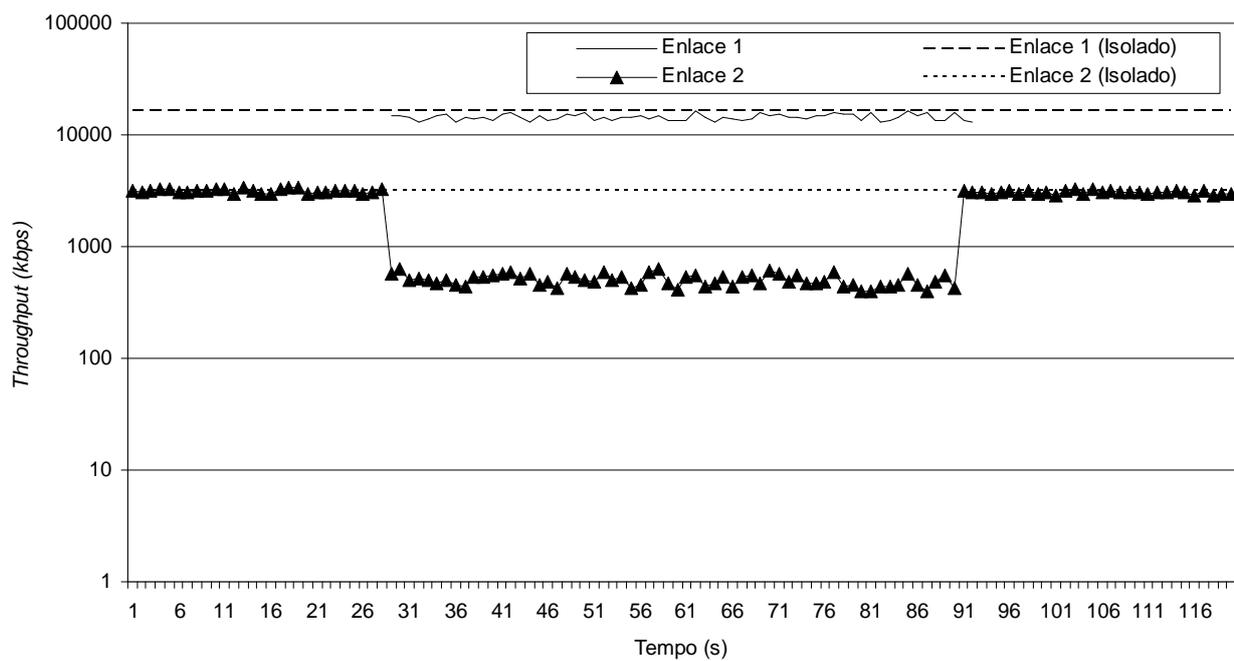


Figura 43 - Medição – UDP – Com OLSR – Enlaces 1 e 2, em ordem inversa.

Os valores medidos para os enlaces 1 e 2, respectivamente, foram de 14434 kbps e 585 kbps. Este resultado é, aproximadamente, o mesmo resultado obtido no teste anterior, o que prova que a ordem do início da geração do tráfego UDP não interfere no resultado da medição.

6.7. Resumo dos resultados obtidos

Nesta seção, apresenta-se o resumo de todos os resultados medidos nos testes. Pode-se observar que o comportamento dos enlaces se repete, tendo mudanças apenas no valor do *throughput* medido. Por exemplo, tem-se que para o TCP, seja para rotas estáticas, seja para o roteamento dinâmico, quando há uma concorrência pelo *throughput*, o nó que está mais distante do *gateway* fica impossibilitado de utilizar a rede.

Já para o UDP, tal fato não ocorre. O que se observa é uma queda considerável de *throughput* do enlace que envolve o nó que está mais distante do *gateway*. Estes resultados ratificam a necessidade de se implementar mecanismos que forneçam justiça para esses tipos de rede.

Uma outra observação a ser feita é que, para uma topologia onde a rede não está em malha, é mais vantajoso se trabalhar com rotas estáticas, uma vez que consegue-se um ganho considerável de *throughput*, como pode ser visto pela tabela 3. Este trabalho pode ser estendido para uma análise comparativa de outros protocolos de roteamento, para se verificar qual deles é o que insere mais *overhead*.

	Rotas estáticas		Roteamento Dinâmico (OLSR)	
	TCP (kbps)	UDP (kbps)	TCP (kbps)	UDP (kbps)
Enlace 1	14258	17949	13333	16518
Enlace 2	2479	3774	2283	3211
Enlace 1	14283	16384	12621	13325
Enlace 2	0	814	0	460
Enlace 1	13213	15147	12796	14434
Enlace 2	0	714	0	585

Tabela 3 - Resumo dos resultados obtidos nos testes

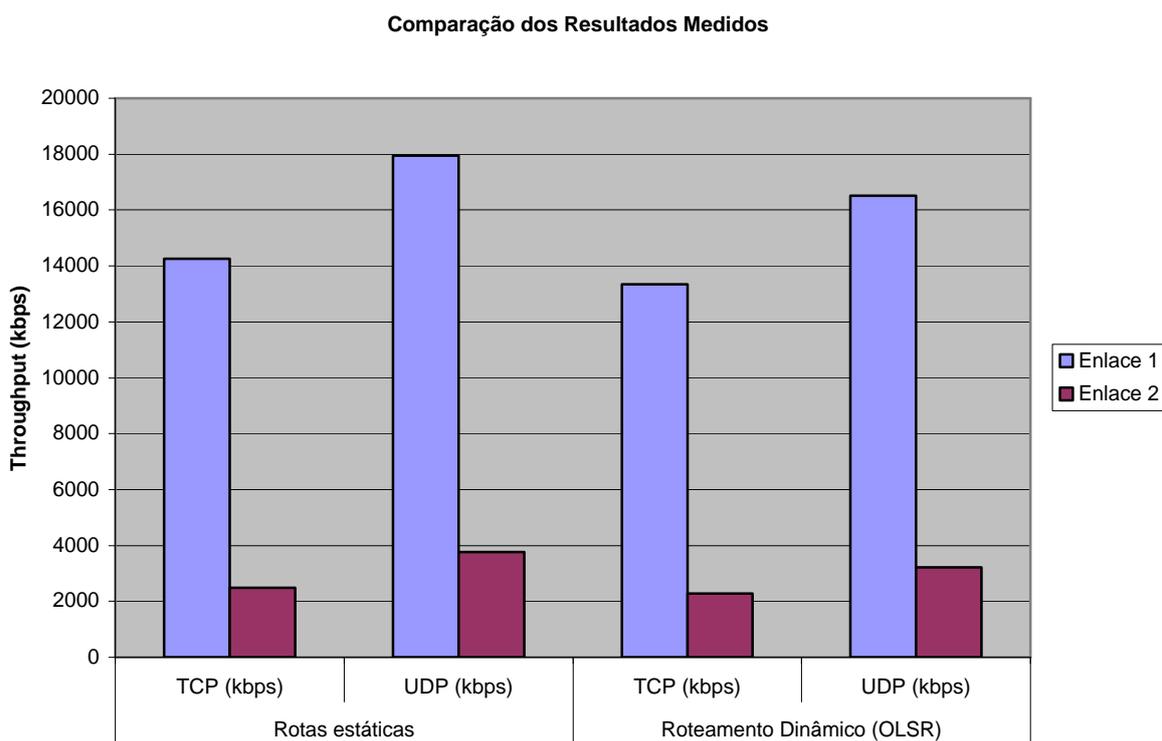


Figura 44 - Comparação dos Resultados Medidos - Teste "a"

Comparação dos Resultados Medidos

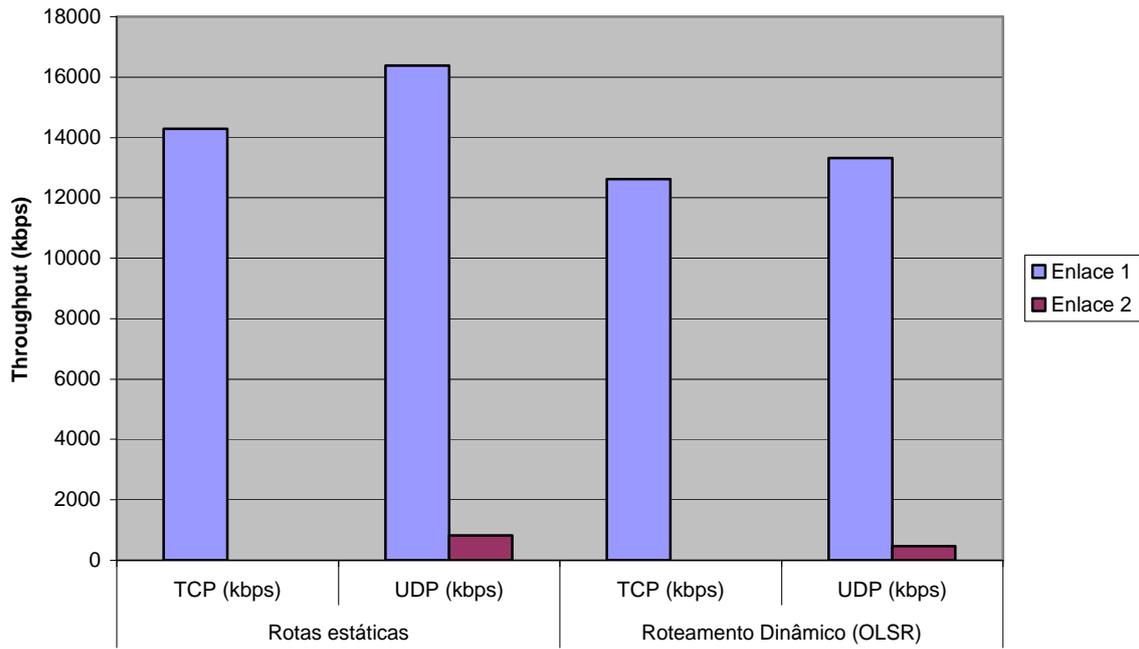


Figura 45 - Comparação dos Resultados Medidos – Teste “b”

Comparação dos Resultados Medidos

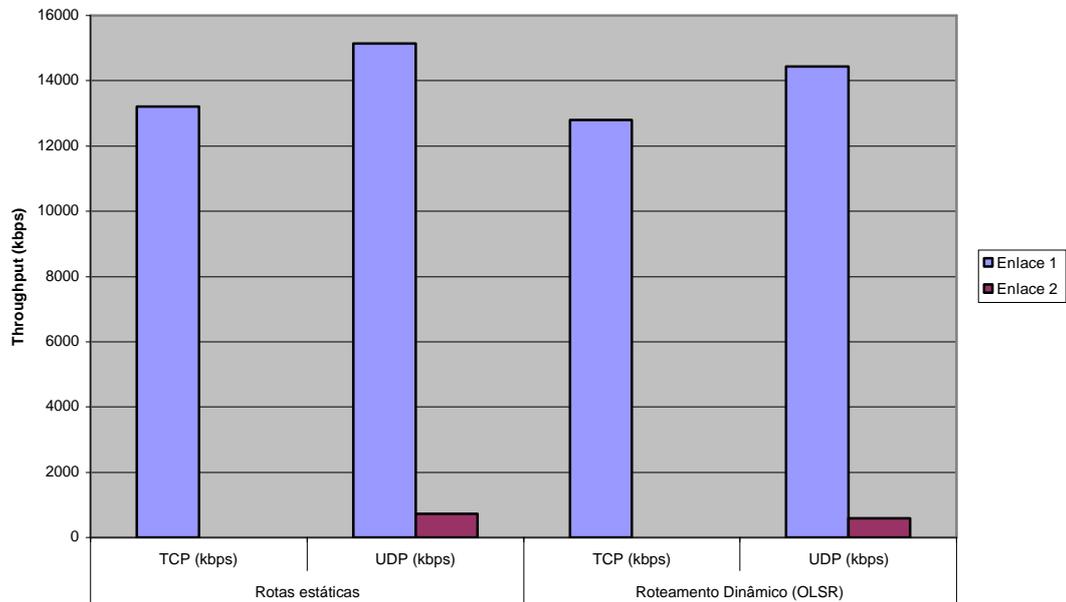


Figura 46 - Comparação dos Resultados Medidos - Teste "c"

7. Conclusão

O presente projeto foi dividido em duas etapas. A primeira etapa corresponde a um grande estudo que foi feito sobre as WMNs. Nesta etapa, os fundamentos das redes sem fio em geral foram apresentados, suas vantagens, desvantagens, mecanismos de funcionamento e limitações. Em seguida, focou-se um pouco mais nas WMNs. Como se trata de um assunto relativamente novo, sobre o qual estão sendo realizados inúmeros estudos ao redor do mundo, muitos assuntos apresentados neste projeto foram baseados em artigos técnicos da comunidade científica. Através destes artigos, pode-se perceber para onde estão sendo direcionados os esforços dos pesquisadores para que as grandes limitações das WMNs sejam superadas da maneira mais eficiente possível.

A segunda etapa deste projeto corresponde a uma atividade prática. Num primeiro momento, o objetivo foi avaliar o ganho em desempenho de se utilizar redes baseadas em mais de um rádio. Para esta análise, eram necessários equipamentos específicos que, infelizmente, não chegaram a tempo para a medição.

Uma outra atividade então foi realizada. Esta atividade teve como base um artigo técnico que tratava da questão da justiça nas WMNs. Uma rede onde a justiça é implementada é aquela que consegue dividir, da melhor maneira possível, o *throughput* disponível entre os enlaces ativos. O que pode ser visto, através deste mesmo artigo e dos valores medidos é que a justiça ainda não é implementada nessas redes, o que pode ocasionar eventuais problemas de uso da rede. Assim sendo, essa questão deve ser analisada e deve ser levada em consideração no projeto de uma WMN. Vale ressaltar que o tráfego TCP/UDP utilizado para realizar estas medições não são tráfegos de aplicações reais. A ferramenta utilizada, o *iperf*, utiliza todo o *throughput* disponível. O padrão de tráfego das aplicações reais é diferente deste apresentado.

Através deste projeto, pode-se perceber a grande potencialidade existente nesta tecnologia. As redes sem fio baseadas no IEEE 802.11 são uma grande alternativa para a última milha / último metro. Apesar das limitações apresentadas neste trabalho, em muitos casos, a relação custo-benefício já justifica o seu uso. E ainda, através deste trabalho, pode-se perceber a importância e necessidade da realização de pesquisas nas WMN em vários aspectos diferentes, como a própria questão da justiça, segurança, entre outros.

8. Bibliografia Consultada

- [1] Magalhães, Luiz Claudio Schara, “Redes em Malha para Inclusão Digital”, Universidade Federal Fluminense.
- [2] Breuel, Cristiano Malanga, “Redes em malha sem fios”, Universidade de São Paulo.
- [3] Learn that, <http://www.learnthat.com>
- [4] ANSI/IEEE Std 802.11, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, 1999.
- [5] Internet Society, <http://www.isoc.org>
- [6] Lee, Ann; Ward, Paul A.S., “A Study of Routing Algorithms in Wireless Mesh Networks”, Technical Report, University of Waterloo.
- [7] Microsoft Research Group, <http://research.microsoft.com/mesh>
- [8] Belair Networks, <http://www.belair.com>.
- [9] Teleco, <http://www.teleco.com.br>
- [10] Gast, Matthew, “802.11 Wireless Networks: The Definitive Guide”, O’ReillyPub.
- [11] Jun, Jangeun; Peddabachagari, Pushkin and Sichitiu, Mihail, “Theoretical Maximum Throughput of IEEE 802.11 and its Applications”, North Carolina State University, NC.
- [12] “Certified Wireless Network Administrator – Official Study Guide”, Planet3 Wireless, 2002.
- [13] Roshan, Pejman; Leary, Jonathan, “802.11 Wireless LAN Fundamentals”, Cisco Press, 2004.
- [14] Mesh Dynamics, <http://www.meshdynamics.com/MDPerformanceAnalysis.html>
- [15] Draves, Ricardo; Padhye, Jitendra; Zill, Brian, “Comparison of Routing Metrics for Static Multi-Hop Wireless Networks”, Microsoft Research Group.
- [16] Draves, Ricardo; Padhye, Jitendra; Zill, Brian; “Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks”, Microsoft Research Group.

- [17] Jun, Jangeun; Sichitiu, Mihail, “Fairness and QoS in Multihop Wireless Networks”, Technical Report, North Carolina State University.
- [18] Maciel, Paulo Ditarso; Nunes, Bruno Astuto Arouche; Campo, Carlos Alberto Vieira; Moraes, Luiz Felipe Magalhães, “Avaliando a Sobrecarga Introduzida nas Redes 802.11 pelos Mecanismos de Segurança WEP e VPN/IPSec”, RAVEL, COPPE/UFRJ
- [19] Jun, Jangeun; Sichitiu, Mihail, “The Nominal Capacity of Wireless Mesh Networks”, Technical Report, North Carolina State University.
- [20] Bae, Sang; Xu, Kaixin; Lee, Sungwook; Gerla, Mario, “Measured Analysis of TCP Behavior across Multihop Wireless and Wired Networks”, University of California, LA.
- [21] Duncan, Isabela Barreto, “Modelagem e Análise do Protocolo IEEE 802.11”, COPPE/UFRJ, 2006.
- [22] Brenner, Pablo, “A technical tutorial on the IEEE 802.11 protocol”, Breezecom – Wireless Communications.
- [23] Muller, Nathan J., “Wireless A to Z”, McGraw-Hill
- [24] Iperf – <http://dast.nlanr.net/Projects/Iperf>
- [25] Kurose, James; Ross, Keith W.; “Computer Network – A top-down approach”, Pearson – Addison Wesley
- [26] Odom, Wendell, “Cisco CCNA – Guia da Certificação 640-11”; Alta Books