PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

CEATEC

FACULDADE DE ENGENHARIA ELÉTRICA

CLAUREM PAULUS CEOLIN MARQUES

IDENTIFICAÇÃO DE OFENSORES VIA ANÁLISE DA SENSIBILIDADE DE ESTAÇÕES NA VAZÃO DE REDES IEEE 802.11

PUC-CAMPINAS

2013

CLAUREM PAULUS CEOLIN MARQUES

IDENTIFICAÇÃO DE OFENSORES VIA ANÁLISE DA SENSIBILIDADE DE ESTAÇÕES NA VAZÃO DE REDES IEEE 802.11

Dissertação apresentada como exigência para obtenção do Título de Mestre em Engenharia Elétrica, ao Programa de Pós Graduação Stricto Sensu em Engenharia Elétrica, Pontifícia Universidade Católica de Campinas.

Orientadora: Prof[a]. Dr[a]. Lia Toledo Moreira Mota

PUC-CAMPINAS

2013

Ficha Catalográfica
Elaborada pelo Sistema de Bibliotecas e
Informação - SBI - PUC-Campinas

t621.3845
M357i

Marques, Claurem Paulus Ceolin.
Identificação de ofensores via análise da sensibilidade de estações na vazão de Redes IEEE 802.11 / Claurem Paulus Ceolin Marques. - Campinas: PUC-Campinas, 2013.
94p.

Orientadora: Lia Toledo Moreira Mota.
Dissertação (mestrado) – Pontifícia Universidade Católica de Campinas, Centro de Ciências Exatas, Ambientais e de Tecnologias, Pós-Graduação em Engenharia Elétrica.
Inclui bibliografia.

1. Sistemas de comunicação sem fio. 2. Sistemas de telecomunicação. 3. IEEE 802.11 (Normas). I. Mota, Lia Toledo Moreira. II. Pontifícia Universidade Católica de Campinas. Centro de Ciências Exatas, Ambientais e de Tecnologias. Pós-Graduação em Engenharia Elétrica. III. Titulo.

22.ed. CDD – t621.3845

CLAUREM PAULUS CEOLIN MARQUES

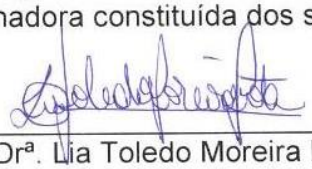
IDENTIFICAÇÃO DE OFENSORES VIA ANÁLISE DA SENSIBILIDADE DE ESTAÇÕES NA VAZÃO DE REDES IEEE 802.11

Dissertação apresentada ao Curso de Mestrado Profissional em Gestão de Redes de Telecomunicações do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas como requisito parcial para obtenção do título de Mestre Profissional em Gestão de Redes de Telecomunicações.

Área de concentração: Gestão de Redes e Serviços

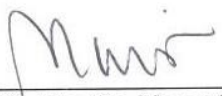
Orientadora: Profª. Drª. Lia Toledo Moreira Mota

Dissertação defendida e aprovada em 16 de dezembro de 2013 pela Comissão Examinadora constituída dos seguintes professores:



Profª. Drª. Lia Toledo Moreira Mota
Orientadora da Dissertação e Presidente da Comissão Examinadora
Pontifícia Universidade Católica de Campinas

Prof. Dr. Alexandre de Assis Mota
Pontifícia Universidade Católica de Campinas



Profª. Drª. Marília Macorin de Azevedo
CEETEPS/FATEC SP

Dedico esse trabalho à minha esposa Eliana

e à minha filha Evelin

meus amores.

AGRADECIMENTOS

Agradeço pela compreensão e incentivo de meus entes queridos em especial à minha esposa Eliana e minha filha Evelin. Simplesmente maravilhosas.

Aos meus pais Antonio e Vanda, e aos meus irmãos Celso e Clauber pelo amor e pelos ensinamentos relativos a valores pessoais indispensáveis para uma vida honesta e digna.

À minha Orientadora Professora Dr^{a}. Lia Mota, pela orientação, esclarecimento e incentivo.

Ao líder do grupo de pesquisa institucional em Eficiência Energética Professor Dr. Alexandre Mota, pelos ensinamentos, atenção e direcionamento.

A todos os professores do programa.

Aos meus amigos pela atenção, cuidado e dicas pessoais durante todo o processo de desenvolvimento desse trabalho.

Aos amigos da turma pelo companheirismo e solidariedade mútuos com que convivemos durante esses dois anos.

Agradeço especialmente ao meu grande amigo Deivis Pirani pela assistência em questões pessoais e técnicas que contribuíram imensamente para o desenvolvimento deste trabalho.

Agradeço imensamente à Ana Raquel pelo companheirismo e apoio durante o projeto de pesquisa, principalmente nos momentos de interação imprescindíveis para o desenvolvimento deste trabalho.

Aos meus amigos Almir Silva, Paulo Barreto e Luiz Barreto. Tenho orgulho de tê-los conhecido e interagido nos trabalhos em grupo durante o curso das disciplinas do programa.

A um grande amigo de longa data Eder Ignatowicz por ter plantado a idéia e me incentivado a conquistar esse importante título acadêmico.

Ao Bi-Campeão Mundial de Clubes da FIFA Sport Club Corinthians Paulista, pelas alegrias proporcionadas ao longo desses dois anos de curso (2012 – 2013).

À PUC Campinas pela bolsa de estudos.

(...) toda nossa ciência, comparada com a realidade, é primitiva e infantil
ainda assim é a coisa mais preciosa que nós temos.

Albert Einstein

RESUMO

Este trabalho apresenta uma análise do comportamento das redes sem fio diante da presença de ofensores – dispositivos causadores do fenômeno conhecido como Anomalia da MAC – em redes IEEE 802.11. Essa análise permite um melhor entendimento do comportamento da rede e isso é necessário para que se possa observar padrões que caracterize o causador da anomalia, tornando possível a identificação do ofensor da rede para que se possa partir para a próxima etapa que é a de mitigar o problema. Por meio de um arranjo de componentes de hardware e software, especificou-se uma bancada de testes que permite a coleta das informações necessárias a partir do ponto de acesso, tais como, a potência recebida e a taxa de transferência efetiva das estações conectadas à rede sem fio. Utilizando uma síntese dessas informações coletadas, na presença de ofensores, pôde-se observar padrões no comportamento da rede que deixaram evidente uma diferença na sensibilidade da estação ofensora em relação à vazão total da rede, o que a caracteriza como ofensora.

Palavras-Chave — Anomalia da MAC, IEEE 802.11, Bancada de Testes, Índice de Sensibilidade.

ABSTRACT

This paper presents an analysis of the behavior of wireless networks on the presence of offenders – devices that cause the phenomenon known as the MAC-Anomaly in IEEE 802.11 networks. This analysis allows a better understanding of network behavior and it is necessary to observe patterns that characterize the cause the anomaly; making possible the identification of the offender from the network so that you can go to the next step which is to mitigate the problem. Through an arrangement of hardware and software components, specify a test bench that allows for the collection of the necessary information from the access point, such as, the received power and the effective throughput of the stations connected to the wireless network. Using a synthesis of this information collected, in the presence of offenders, could observe patterns in the behavior of the network that made clear a difference in sensitivity of the offending station in relation to the total flow of the network characterized as offending.

Key Words — MAC Anomaly, IEEE 802.11, Test Bench, Sensitivity Index.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AP	= “Access Point”
CPU	= “Central Processing Unit”
CSV	= “Comma Separated Values”
DCF	= “Distributed Coordination Function”
DHCP	= “Dynamic Host Configuration Protocol”
GB	= “Gigabyte”
Gb/s	= “Gigabits per second”
HCF	= “Hybrid Coordination Function”
HD	= “Hard Disk”
IEEE	= “Institute of Electrical and Electronics Engineers”
IEEE-SA	= “IEEE Standards Association”
IP	= “Internet Protocol”
Kb/s	= “Kilobits per second”
LAN	= Local Access Network
MAC	= “Media Access Control”
Mb/s	= “Megabits per second”
OSI	= “Open Systems Interconnection”
PCF	= “Point Coordination Function”
PDA	= “Personal Digital Assistant”
QoS	= “Quality of Service”
RAM	= “Random Access Memory”
RAS	= “Remote Access Server”
RF	= Rádio Frequência
RFC	= “Request For Comment”
RSSI	= “Received Signal Strength Indication”
SCP	= “Secure CoPy”

SFTP = “SSH File Transfer Protocol”

SSH = “Secure Shell”

UDP = “User Datagram Protocol”

VoIP = “Voice over IP”

WAN = “Wide Area Network”

WLAN = “Wireless LAN”

SUMÁRIO

1. INTRODUÇÃO

Atualmente, as redes sem fio que utilizam o padrão IEEE 802.11 proporcionam ampla conectividade e mobilidade a uma vasta quantidade de dispositivos de uso cotidiano, tais como: *smartphones*, *tablets*, televisores, *video games*, *laptops*, *palmtops* e estações de trabalho convencionais. Para o mundo corporativo, também se constata que existem novos equipamentos que operam com tecnologia sem fio, tais como: impressoras, câmeras de segurança, leitores de código de barras, entre outros.

1.1 Contextualização do Problema

A demanda crescente de acesso à Internet por parte das pessoas, seja por questões pessoais ou profissionais, de um modo geral, é suportada pela rede sem fio (WLAN – *Wireless Local Area Network*), pois, esta oferece uma característica imprescindível para uma maior disponibilidade de acesso: a mobilidade. Essa necessidade de acesso vem fazendo crescer o surgimento das redes sem fio públicas (PWLAN – *Public* WLAN) por meio dos projetos de cidades digitais e/ou redes metropolitanas de acesso aberto (MENDES, 2009), de forma que o acesso à Internet seja algo cada vez mais trivial.

Até meados da década de 2000, projetos de redes locais, corporativas ou domésticas, apenas por acesso por meio de cabos, eram totalmente aceitáveis. Nos dias de hoje, a maioria dos projetos de redes locais incluem pontos de acesso sem fio como parte da infraestrutura. Isso se dá porque o perfil dos usuários também vem sofrendo mudanças e a exigência ao acesso à rede sem fio é estratégica. Afinal, cada vez mais são oferecidas grandes quantidades de serviços, recursos multimídia e várias outras formas de interatividade com o usuário da rede que é visto, muitas vezes, como consumidor. Por isso, as redes precisam ser mais robustas e confiáveis para suportar esse novo perfil de usuário que faz uso de seus serviços sensíveis a atraso, tais como, Voz sobre IP (VoIP) e Video Conferência, ao

mesmo tempo que faz *download* de músicas ou filmes que não são sensíveis a atraso, mas fazem uso extensivo dos recursos da rede.

1.2 Justificativa para o Desenvolvimento do Trabalho

Da perspectiva da rede sem fio, o aumento do número de dispositivos causa um aumento da competição pelo acesso ao meio; essa disputa para se utilizar o meio físico acaba por afetar negativamente o desempenho da rede. Essa característica é inerente à rede sem fio. Entretanto, é na competição pelo acesso que o maior problema que afeta severamente a rede sem fio pode acontecer. Esse problema é conhecido como anomalia da MAC (HEUSSE, 2003).

O padrão IEEE 802.11 (*Standard* IEEE, 2012) prevê condições de igualdade de acesso a todas as estações conectadas à rede, ou seja, o método de acesso ao meio usado pela tecnologia foi originalmente concebido para fazer com que a vazão total da rede sem fio seja compartilhada igualmente por todas as estações. No entanto, as condições físicas foram completamente desconsideradas, pois uma estação que se encontra em condições desfavoráveis de propagação do sinal, ao transmitir informações pela rede, ocupa o canal por mais tempo. Isso faz com que as outras estações, em condições normais de propagação do sinal, sejam penalizadas, já que se desejarem fazer uso do meio físico, terão de esperar até o canal ficar livre, enquanto seus dados ficam represados.

Como resultado da subutilização dos recursos proveniente dessa condição que a rede possa vir a experimentar, o desempenho é o fator mais importante da rede que pode ser afetado negativamente. Uma análise mais aprofundada acerca do desempenho da rede nessas condições pode resultar na inviabilidade de um projeto.

1.3 Objetivo do Trabalho

No momento em que a anomalia está presente na rede, as condições de tráfego na rede ficam parecidas, ocultando, assim, o dispositivo causador da anomalia. Por isso, o principal objetivo deste trabalho é especificar uma bancada de testes capaz de coletar as informações a partir do ponto de acesso para que as mesmas possam ser analisadas e estudadas, visando identificar condições de anomalia e ofensores da rede.

Os estudos realizados com o auxílio da bancada de testes pode resultar na observação de padrões comportamentais da rede e, com isso, pode-se buscar distinção entre esses padrões de forma a identificar o padrão seguido pelo dispositivo causador da anomalia da MAC (ofensor). Essa identificação é indispensável já que qualquer medida para mitigação da anomalia da MAC só pode ser tomada a partir do momento em que se conhece o dispositivo ofensor.

1.4 Resultados Esperados

Espera-se que a bancada seja capaz de fazer a coleta dos dados necessários para a identificação do dispositivo ofensor da rede, tais como: taxa efetiva, taxa nominal, potência recebida, data e hora da medição e a relação sinal-ruído (SNR – *Signal-to-Noise Ratio*). A bancada também deve ser capaz de emular a anomalia da MAC para que se possa observar seus efeitos.

Além disso, a bancada tem que ser robusta para suportar vários cenários: cenários em que a taxa de transferência pode ir do valor mais alto até o valor mais baixo, passando pelos valores intermediários suportados pela tecnologia escolhida para os experimentos. O número de estações também pode ser diferente. O ideal é que suporte fazer a coleta dos dados de pelo menos uma, duas ou três estações.

A forma como os dados serão armazenados também é uma preocupação, porque, para que seja um processo ágil, é importante que os dados estejam armazenados em um formato bem conhecido e que facilite a importação e

manipulação dos mesmos por meio de outros programas, tais como, o Microsoft Excel e o Scilab. Para isso, a bancada deve armazenar os dados no formato CSV (*Comma Separated Values* – Valores Separados por Vírgula).

Por fim, ao analisar os dados coletados pela bancada, espera-se detectar algum padrão que diferencie os dispositivos causadores da anomalia da MAC.

1.5 Delimitação da Pesquisa

Neste trabalho, os componentes de *hardware* e *software* são reais, por isso a escolha de alguns desses componentes foi fundamental para que os dados necessários para a pesquisa de fato pudessem ser coletados pela bancada de testes. No entanto, isso limitou a quantidade de experimentos ao tempo que se tinha disponível para ocupar o laboratório. Por isso, apenas experimentos com o padrão IEEE 802.11b puderam ser feitos para este projeto de pesquisa.

Como parte do objetivo deste trabalho é observar o comportamento da rede de forma a identificar padrões que caracterizem o ofensor da rede, a mitigação da anomalia da MAC não foi realizada, pois entende-se que esta se trata de uma atividade totalmente diferente e é considerada como uma etapa posterior à etapa da identificação do dispositivo causador da anomalia.

1.6 Organização da Dissertação

O Capítulo 1 apresenta a INTRODUÇÃO, onde se apresenta uma visão geral do problema que será objeto de estudo deste projeto de pesquisa. Neste capítulo, são apresentados os itens Contextualização do Problema, Justificativa para o Desenvolvimento do Trabalho, Objetivo do Trabalho, Resultados Esperados e como está organizada a dissertação.

O Capítulo 2 é denominado ANOMALIA e tem o objetivo de fornecer o embasamento necessário para a compreensão do trabalho. Esse capítulo é

composto pelos itens Rede Sem Fio, Padrão IEEE 802.11, Anomalia da MAC, Priorização da Anomalia e Mitigação da Anomalia.

No Capítulo 3, denominado OFENSORES, tem-se a Definição como o primeiro subitem e na sequência tem-se Vazão da Rede na Presença de Ofensores, Estimativa da Máxima Vazão da Rede, Identificação do Ofensor e Análise de Sensibilidade.

O Capítulo 4 é chamado de MATERIAIS E MÉTODOS. Aqui tem-se a especificação dos componentes de *Hardware* e *Software* da bancada de testes em no item Plataforma de Testes. A seguir, são apresentados os itens desse capítulo: Método de Descoberta e Gerência da Rede, Estimação da Vazão Máxima da Rede e Índices de Sensibilidade.

O Capítulo 5 é o de RESULTADOS e contém os itens Operação da Plataforma de Testes, Testes de Vazão da Rede, Testes de Instalação da Anomalia e Testes de Sensibilidade. Os resultados são expostos, majoritariamente, por meio de gráficos.

Por fim, o Capítulo 6 traz as CONCLUSÕES do trabalho. Apresenta-se um sumário dos resultados obtidos com as perspectivas de aplicação, bem como com as perspectivas de continuidade para o trabalho.

2. ANOMALIA DA MAC EM REDES IEEE 802.11

É considerada uma anomalia tudo aquilo que se desvia de forma acentuada de um padrão de normalidade (DICIONÁRIO MICHAELIS – UOL, 2013). No contexto das redes sem fio, em condições específicas, uma anomalia causa a subutilização dos recursos da rede, sendo esta uma razão pela qual seu estudo possui relevância tecnológica e científica. Características intrínsecas ao protocolo IEEE 802.11 permitem que uma anomalia se instale na rede, provocando uma situação indesejada que afeta, principalmente, o desempenho da rede. Essa situação é chamada de anomalia da MAC (HEUSSE, 2003).

Neste capítulo, são apresentadas as principais características das redes sem fio e o padrão IEEE 802.11. Também são apresentadas a anomalia da MAC, a priorização da anomalia e a mitigação da anomalia como partes da fundamentação teórica deste trabalho.

2.1 Rede Sem Fio

Uma rede sem fio é aquela que permite dispositivos trocarem informações entre si sem que haja a necessidade de conexões por qualquer tipo de cabo. A rede sem fio é um dos meios de acesso à rede mais difundidos e populares, devido à grande quantidade de dispositivos que possuem tal capacidade de comunicação. Os *smartphones* e *tablets* tomaram conta do mercado de aparelhos eletrônicos. Só em 2012, foram vendidos 821 milhões desses aparelhos inteligentes em todo o mundo; em 2013, as vendas devem chegar a 1,2 bilhão e, até 2016, as vendas devem triplicar (GARTNER, 2013). Essa considerável quantidade de dispositivos que suportam a tecnologia sem fio se deve ao fato de a mesma ser bem conhecida, de custo acessível e padronizada pelo IEEE (IEEE STD 802.11, 1999).

Há vários tipos de tecnologias que são capazes de realizar a comunicação sem fio. Entre as tecnologias mais conhecidas que operam sem fio estão (RNP, 2013): *Infravermelho*, *Bluetooth*, IEEE 802.11 (ex: *Wi-Fi*), IEEE 802.15.4 (ex:

ZigBee), IEEE 802.16 (ex: WiMax). Uma rede sem fio pode ser classificada quanto à sua abrangência da mesma forma que as redes cabeadas são como, por exemplo, WPAN (*Wireless Personal Area Network*), WLAN (*Wireless Local Area Network*), WMAN (*Wireless Metropolitan Area Network*) e WWAN (*Wireless Wide Area Network*).

O uso de comunicações sem fio vai além das redes de computadores. Antes de serem empregadas na transferência de dados entre computadores, elas eram utilizadas na comunicação via satélite para diversos fins, como por exemplo, no transporte de sinais de televisão, de rádio e de telecomunicações. A informação é modulada e transmitida por meio de ondas eletromagnéticas. As ondas eletromagnéticas se propagam naturalmente pelo espaço a distâncias variáveis dependendo das condições do ambiente (TANEMBAUM, 2003).

A comunicação sem fio é dependente da frequência utilizada para a transmissão do sinal. Se o sinal é transferido em baixa frequência, as ondas de rádio passam através de obstáculos, mas a potência cai com a distância em relação à fonte do sinal. Já para os sinais que usam alta frequência, as ondas de rádio tendem a viajarem linhas retas, mas são afetadas por condições climáticas, tais como chuva e neblina. Além disso, todas as ondas de rádio estão sujeitas à interferência de motor se outros equipamentos elétricos (TANEMBAUM, 2003).

2.2 Padrão IEEE 802.11

O padrão IEEE 802.11 teve o início de seu desenvolvimento em 1991, após instauração de um comitê para definição de um padrão para conectividade sem fio, tendo sido finalmente lançado em 1997 (IEEE-SA, 2012). Seu propósito consiste em definir um método de acesso ao meio físico e várias especificações físicas para conectividade de rede sem fio dentro de uma WLAN (STANDARD IEEE, 2012).

O objetivo dessa especificação é definir padrões associados à camada 2 do modelo OSI, ou seja, a camada de Enlace de Dados, conforme ilustra a figura 1. A camada de enlace de dados é composta por duas subcamadas, MAC (*Media*

Access Control) e LLC (*Logical Link Control*). A subcamada MAC será discutida mais detalhadamente nas próximas seções deste trabalho.

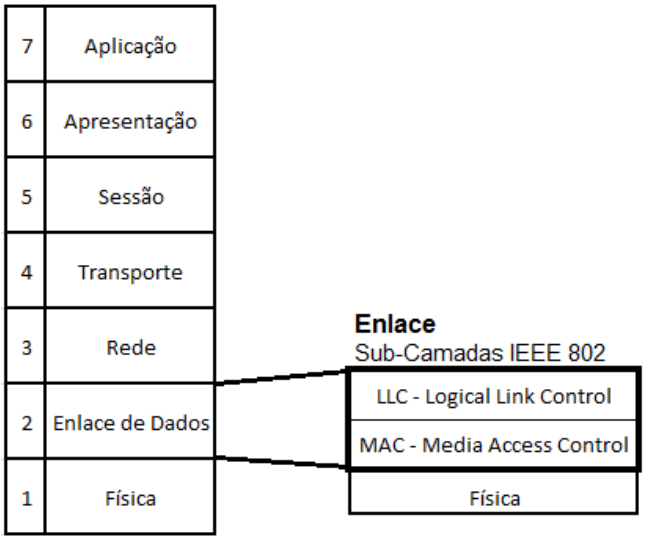


Figura 1: Subcamadas MAC e LLC da Camada de Enlace

A tabela 1 apresenta os padrões mais amplamente difundidos para rede sem fio: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g e IEEE 802.11n. Esses padrões suportam taxas de transferências máximas que vão de 11 a 450 Mb/s e operam nas faixas de frequência de 2,4 e/ou 5 GHz (Wi-Fi, 2013).

Tabela 1: Gerações Wi-Fi

Tecnologia Wi-Fi	Banda de Frequência	Taxa de Dados Máxima
802.11a	**5 GHz**	**54 Mb/s**
802.11b	**2.4 GHz**	**11 Mb/s**
802.11g	**2.4 GHz**	**54 Mb/s**
802.11n	**2.4 GHz, 5 GHz, 2.4 ou 5 GHz (selecionável), ou 2.4 e 5 GHz (concorrente).**	**450 Mb/s**

2.3 Anomalia da MAC

Por meio do método DCF (*Distributed Coordination Function*) que usa o algoritmo CSMA/CA, a camada MAC do padrão IEEE 802.11 prevê condições de igualdade de acesso ao meio a todos os dispositivos presentes na rede. Isso faz com que todas as estações tenham a mesma probabilidade de acessar o meio, não

importando a diferença entre suas condições de conectividade da camada física, nem de taxa de transferência. Como mencionado, a taxa de transferência é determinada mediante negociação entre o ponto de acesso sem fio e o dispositivo admitido na rede e se baseia nas condições de propagação do sinal, ou seja, principalmente na relação sinal/ruído (*Signal-to-Noise Ratio*, SNR). Portanto, a determinação das condições da camada física é fundamental para a identificação dos dispositivos que estão submetidos a condições desfavoráveis de propagação do sinal, possibilitando a tomada de alguma ação do ponto de vista de gerência da rede, antes que esses dispositivos causem a anomalia da MAC (BRANQUINHO, 2006) (HEUSSE, 2003)(GUIRARDELLO, 2008).

A anomalia da MAC foi demonstrada, pela primeira vez, em (HEUSSE, 2003), quando se observou um desempenho consideravelmente degradado de algumas estações em relação a outras da rede. Essa anomalia faz com que uma estação em más condições provoque uma redução na taxa de transferência das demais estações, ao estabelecer comunicação efetiva com o ponto de acesso (GUIRARDELLO, 2008). Para ilustrar este efeito, a figura 2 mostra a taxa de transmissão de duas estações (STA1 e STA2) conectadas a um mesmo ponto de acesso (AP). Pode-se observar a significativa degradação que a transmissão da estação STA1, em boas condições de acesso, sofre a partir de 30 s, quando a estação STA2 (em condições desfavoráveis de transmissão) passa a acessar a rede.

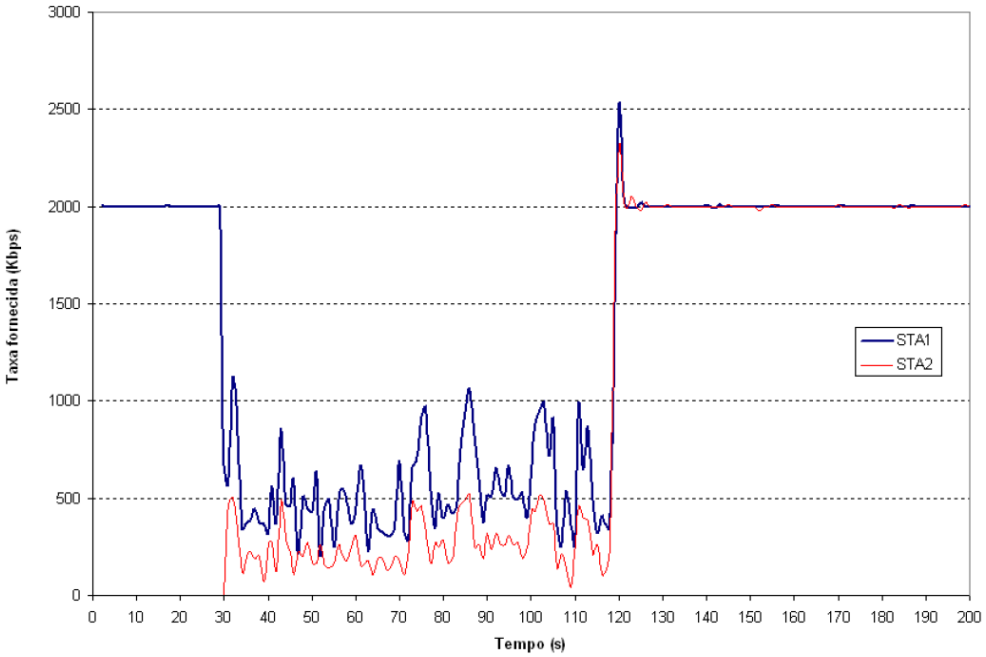


Figura 2: Anomalia da MAC

A anomalia resulta da forma como o controle de acesso ao meio é feito nas redes IEEE 802.11. Conforme citado anteriormente, a técnica de controle de acesso ao meio físico implementada pelo padrão IEEE 802.11 é a DCF (*Distributed Coordination Function*). Essa técnica faz com que todas as estações, conectadas ao ponto de acesso sem fio, tenham condições de igualdade ao acessar o meio físico, pois essa técnica usa o método de múltiplo acesso CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Existem outras técnicas de controle de acesso ao meio físico, tais como, a PCF (*Point Coordination Function*), a HCF (*Hybrid Coordination Function*) e a MCF (*Mesh Coordination Function*), mas, por ser a técnica primária de controle de acesso do IEEE 802.11, a técnica DCF é usada neste trabalho. A figura 3 ilustra a técnica DCF(FERREIRA, 2007).

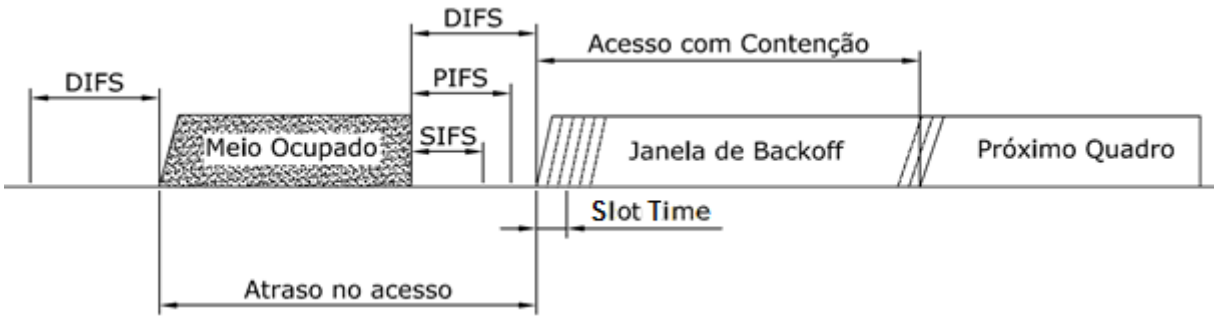


Figura 3: *Distributed Coordination Function*

A temporização praticada (*Standard* IEEE, 2012) pelo padrão IEEE 802.11b é:

- DIFS = 50 µs;
- SIFS = 10 µs;
- PIFS = 30 µs;
- *Slot Time* = 20 µs;
- Janela de *Backoff* = 31 *slots*;

O fato de todas as estações possuírem a mesma chance de acessarem o meio físico é algo que funcionaria bem num cenário em que todas as estações se encontram com as mesmas condições físicas de propagação do sinal RF (Radio Frequência) pela rede. Entretanto, a disposição física, normalmente dispersas, dos dispositivos conectados à rede faz com que as estações tenham condições favoráveis ou desfavoráveis de propagação do sinal pela rede. A taxa de transferência é determinada pela negociação entre uma estação e o ponto de acesso sem fio ao qual ela está conectada. Essa negociação leva em consideração a relação sinal-ruído que está diretamente relacionada com as condições de propagação do sinal RF.

A anomalia da MAC acontece quando se tem dispositivos com diferentes taxas de transferência conectadas à mesma rede sem fio. Isso se dá porque, como mencionado anteriormente, o controle de acesso ao meio usado pelo padrão IEEE 802.11 prevê condições de igualdade no acesso à rede a todos os dispositivos, desconsiderando completamente as condições da camada física. Então, se um dispositivo com uma taxa de transferência baixa começar a transmitir dados pela rede, ele levará mais tempo para terminar a transmissão e, portanto, utilizará o meio físico por mais tempo em comparação com outros dispositivos com taxas de transferência mais altas, para transmitir a mesma quantidade de informação. No momento em que uma estação está transmitindo dados em uma rede sem fio, somente ela poderá fazer uso do meio físico. Enquanto isso, as outras estações esperam para transmitir suas informações no momento em que conseguirem ter acesso ao meio físico, ou seja, essas estações ficam com seus dados represados. Portanto, se um dispositivo estiver transmitindo informações pela rede ao mesmo tempo em que está em condições desfavoráveis de propagação do sinal, os outros

dispositivos terão que esperar um longo tempo para transmitirem seus próprios dados. Por isso, uma condição de subutilização dos recursos se instala, correspondendo ao momento em que a anomalia da MAC está afetando a rede. Na figura 4, observam-se as condições que favorecem o aparecimento da anomalia da MAC descrita acima.

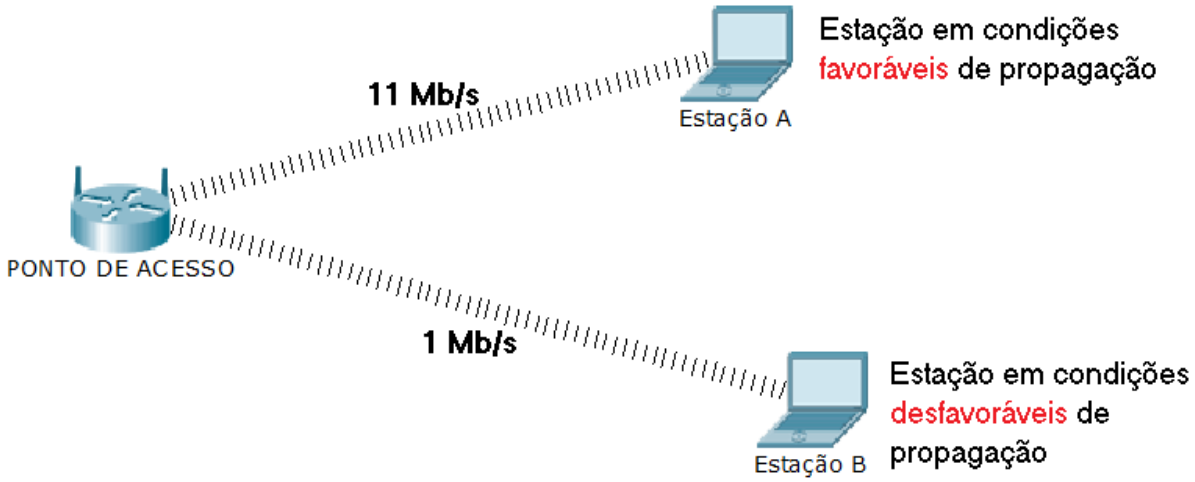


Figura 4: Taxa de Transmissão das Estações

2.4 Priorização da Anomalia

A priorização da anomalia acontece no padrão IEEE 802.11e (IEEE STD 802.11e, 2005). Esse padrão apresenta, como novidade, a implementação de QoS (*Quality of Service*), que basicamente consiste em priorizar determinados tipos de tráfego de dados em relação a outros. Em qualquer rede, o movimento de pacotes de dados de um ponto a outro é chamado de tráfego de dados, mas o tráfego de dados pode pertencer a serviços de redes diferentes. Esses serviços apresentam sensibilidades diferentes em relação a diferentes parâmetros de QoS da rede. Por exemplo, os serviços de voz e vídeo são sensíveis a atraso ou latência na rede e, por isso, recebem uma prioridade maior do que tipos de tráfego de dados como web e *e-mail* na hora de serem encaminhados pelos dispositivos de redes.

Seguindo essa linha de raciocínio, se uma estação que está conectada a uma rede cujo padrão em operação seja o IEEE 802.11e, significa que nessa rede

será implementada qualidade de serviço e priorização de determinados tipos de serviço. Se essa estação, em um determinado momento, se encontrar em uma situação, conforme descrito na seção anterior, em que apresenta condições desfavoráveis de propagação do sinal, ela poderá fazer com que a anomalia da MAC se instale na rede. Sendo este o caso, se a estação estiver transmitindo dados prioritários tais como, voz e vídeo, além de gerar anomalia na rede, esse tráfego será priorizado de acordo com o que o padrão foi desenvolvido para operar, conforme demonstrado em (GUIRARDELLO, 2008), proporcionando, então, uma priorização da anomalia da MAC.

2.5 Mitigação da Anomalia

A anomalia da MAC faz com que a rede, de um modo geral, seja sub-utilizada. Portanto, sua mitigação é fundamental para o bom desempenho da rede. Pela própria natureza da anomalia da MAC, qualquer que seja a solução para mitigá-la, as condições físicas do enlace de dados devem ser levadas em consideração. As condições do meio físico são determinadas por meio da relação sinal-ruído. A relação sinal-ruído é uma medida que compara o nível de sinal desejado e o nível de ruído de fundo. Nas redes IEEE 802.11, a relação sinal-ruído; afeta diretamente a taxa de transferência e, conforme mencionado na seção 2.3 deste trabalho, diferentes taxas de transferência aumentam a probabilidade de que a anomalia se instale na rede. Vários fatores alteram a relação sinal-ruído, entre eles estão a distância entre uma estação e o ponto de acesso, obstáculos físicos presentes no ambiente e condições de propagação do sinal. A ação desses vários fatores sobre um sinal causa o desvanecimento do mesmo ao longo do tempo (RAPPAPORT, 1996).

Em (BRANQUINHO, 2006) a anomalia da MAC foi mitigada, com sucesso, por meio do uso da SRN para controlar a janela de contenção (CW – *Contention Window*) *backoff*. Em outras palavras, ao aumentar ou diminuir o tamanho da janela de contenção, aumenta-se ou diminui-se as chances de uma estação acessar a portadora do sinal sem fio. Portanto, quando uma estação ofensora é conhecida por

meio de uma alta relação sinal-ruído, aumenta-se o tamanho da janela de contenção de forma que esta espere mais tempo para acessar o meio físico em relação a outras estações conectadas à mesma rede, mas com um valor de relação sinal-ruído menor.

Os serviços prioritários de QoS também já foram usados nas redes sem fio para mitigação da anomalia da MAC (KIM, 2005). No entanto, essa solução não levou em consideração as condições da camada física. O QoS leva em consideração o serviço que é usado numa comunicação pela rede e as informações de serviço são encontradas na camada de transporte. Se uma estação tem seu tráfego priorizado pelo QoS e, ao mesmo tempo, ela tem uma baixa taxa de transferência devido a uma também baixa relação sinal-ruído, essa estação possivelmente será uma ofensora, ou seja, uma estação que causará sérios problemas de performance e subutilização dos recursos na rede; e ainda terá prioridade ao enviar seus dados conforme discutido no item 2.4.

Além da mitigação da anomalia por meio de modificações no *hardware/firmware* do ponto de acesso e por meio da implementação do *QoS* na rede, a anomalia também pode ser mitigada usando ao técnica de *Traffic-Shaping* (PERIS, 2012). O *Traffic-Shaping*, nesse contexto, nada mais é do que controlar a taxa de transferência do dispositivo ofensor da rede, de forma a limitar o acesso desse dispositivo ao meio físico da rede. Quanto menos um dispositivo ofensor da rede ocupa o canal, menos ele prejudica a rede. Portanto, à medida que a taxa de transferência de um ofensor é reduzida ou simplesmente limitada, a vazão total disponível da rede aumenta para os dispositivos que estão em condições de propagação favoráveis.

Em suma, é possível encontrar vários trabalhos propondo diferentes técnicas para mitigação da anomalia (KIM, 2005), (BRANQUINHO, 2006), (PERIS, 2012). Entretanto, a identificação do ofensor não é mencionada na maioria desses trabalhos, apesar de tal identificação poder ser considerada uma etapa prévia da mitigação da anomalia da MAC em redes IEEE 802.11. Portanto, explorar o comportamento da rede de forma a poder caracterizar de alguma forma um dispositivo que, eventualmente, possa estar causando a anomalia na rede é de extrema importância, pois ainda não se tem mecanismos para a realização dessa

tarefa. Por isso, uma bancada de testes capaz de emular um ambiente de rede sem fio na presença de ofensores, em taxas de transferências diferentes, possibilita a criação de cenários em que o comportamento da rede possa ser observado para que algum padrão possa ser detectado e explorado.

3. OFENSORES

Num cenário, em uma rede wireless, onde um dispositivo de rede em condições desfavoráveis de propagação ocupa o canal por mais tempo do que um segundo dispositivo, sendo que os dois têm a mesma quantidade de dados para transmitir, o primeiro poderia ser considerado como sendo o ofensor e, o segundo, poderia ser considerado como sendo o ofendido.

3.1 Definição

Neste trabalho, define-se como ofensor todo e qualquer dispositivo que faça com que a operação da rede se desvie de forma acentuada de seu padrão de normalidade. Portanto, entende-se, aqui, que o ofensor é aquele que prejudica os demais dispositivos de rede em condições favoráveis de propagação, por meio da diminuição da capacidade de transmissão e recepção total da rede ou a vazão total da rede.

Outro aspecto que deve ser levado em consideração é que na presença de ofensor, a eficiência energética da rede, de um modo geral também é prejudicada, pois as condições sob as quais um dispositivo se torna ofensor da rede, fazem com que a comunicação não seja eficiente. A queda de eficiência da rede, nesse caso, está diretamente ligada à retransmissão constante de dados em virtude de erros na transmissão; portanto, esse retrabalho da rede gera um maior consumo de energia.

Ao se projetar uma rede, espera-se dessa infraestrutura um determinado desempenho associado a certo consumo energético. Dado o consumo energético que se espera de uma rede mais o desempenho que os dispositivos dessa rede são capazes de proporcionar, se o desempenho é, por alguma razão, afetado negativamente e o consumo energético se mantém então isso vai contra o conceito de eficiência energética. Pois, para aumentar a eficiência energética em um sistema, ou aumenta-se a produtividade do sistema com a energia que ele usa no momento ou mantém-se a produtividade e diminui-se o consumo energético.

3.2 Vazão da Rede na Presença de Ofensores

O ideal é que os recursos da rede sejam distribuídos de forma justa a todos dispositivos conectados à rede sem fio. Na operação normal da rede, o tempo de utilização dos recursos não é compartilhado igualmente, pois um dispositivo pode acabar alocando o canal por mais tempo do que os outros da rede. Vários fatores influenciam nesse compartilhamento dos recursos, tais como, nível de processamento local de um dispositivo, quantidade de dados a serem transmitidos pela rede, qualidade do sistema operacional e do *hardware* em relação aos outros dispositivos da rede, entre outros. No entanto, a presença de um ou mais ofensores, causa um grande impacto negativo no que se refere à vazão máxima da rede e isso faz com que toda sua capacidade de vazão, a ser distribuída pelos dispositivos componentes da rede, seja diminuída consideravelmente.

3.3 Estimativa da Máxima Vazão da Rede

É possível estimar a máxima vazão da rede ao se tentar transmitir uma quantidade de dados superior àquela suportada pela tecnologia implementada na rede. Em outras palavras, ao “estressar” a rede, e medir o *throughput* da mesma no momento do estresse, tem-se, aproximadamente, o valor da máxima vazão.

Numa rede IEEE 802.11b, a taxa nominal de transmissão máxima, de acordo com o padrão, é de 11 Mb/s. Caso haja tentativas sucessivas de acesso à rede sem sucesso devido a erros, a tecnologia faz com que um dispositivo tente se conectar a taxas inferiores, também previstas pelo padrão, sendo que essas taxas são de 5.5 Mb/s, 2 Mb/s e 1 Mb/s. Independentemente das taxas inferiores suportadas pelo padrão, neste trabalho, será considerada a taxa máxima de 11 Mb/s da tecnologia em questão.

Pode-se usar um *software* para a geração artificial de um tráfego equivalente de rede algumas vezes superior a 11 Mb/s, de forma a forçar o uso de toda a capacidade de vazão da rede. O lugar mais apropriado para se fazer a coleta da

taxa de transferência é no ponto de acesso, com apenas uma estação ativa, para eliminar a possibilidade do aparecimento da anomalia da MAC.

3.4 Identificação do Ofensor

No item 2.5, foram apresentadas algumas técnicas para mitigação da anomalia da MAC 802.11, tanto por *hardware* quanto por *software*; porém, ao se utilizar tais técnicas, supõe-se que a identidade de uma estação ofensora seja conhecida. Assim, a identificação do ofensor pode ser considerada como uma etapa prévia da mitigação da anomalia da MAC em redes IEEE 802.11.

A identificação do dispositivo responsável por causar a anomalia da MAC em uma rede é de difícil solução, pois todas as estações ficam reduzidas a condições de tráfego degradadas e próximas. Para identificar o ofensor da rede, vários aspectos devem ser levados em consideração. Métricas indicadoras dessa condição, passíveis de serem utilizadas são, por exemplo: taxa de bits nominal, taxa de bits efetiva, potência do sinal recebido pelo ponto de acesso e a obsolescência/robustez dos dispositivos conectados à rede sem fio.

No momento da associação entre uma estação e um ponto de acesso, existe uma etapa de negociação da taxa de bits nominal, dependendo das condições de propagação do sinal, distância entre estação e ponto de acesso, entre outras coisas. Pode ficar estabelecido que a estação somente poderá enviar seus dados a uma taxa menor que a utilizada pela maioria dos dispositivos conectados à rede. Por isso, a informação da taxa nominal é importante para se determinar o potencial ofensivo de um dispositivo.

A taxa efetiva é a taxa que o dispositivo está de fato transmitindo seus dados pela rede. Qualquer variação da taxa efetiva pode ser entendida como utilização do canal. Se um dispositivo estiver em condições desfavoráveis de propagação e estiver fazendo uso extensivo da rede, pode significar que esse dispositivo tenha um alto potencial ofensivo em relação aos demais dispositivos da rede.

A potência do sinal recebido também é um indicador que deve ser considerado, porque se a potência é baixa, pode significar que o dispositivo está em condições desfavoráveis de propagação do sinal; sendo assim, muitos erros de transmissão poderão ocorrer ao longo de uma transferência de dados e isso pode fazer com que o dispositivo ocupe o canal por mais tempo que o necessário, além de transferir dados a taxas mais baixas.

3.5 Análise de Sensibilidade

Por si só, a análise de sensibilidade pode ser uma estratégia de identificação do ofensor, mas, também, pode ser agregada a um método matemático ou heurístico como uma forma de validação da identificação da ofensividade de um dispositivo.

Essa estratégia consiste, basicamente, em reduzir a taxa de transferência de uma estação suspeita de ser ofensora e monitorar o que acontece com a vazão total da rede. Uma vez que, no padrão IEEE 802.11, todas as estações conectadas à rede compartilham a capacidade de vazão total, se a taxa de dados diminui para uma estação em relação à sua taxa original, significa que essa diferença ficará disponível para outras estações da rede. Se a vazão total da rede aumentar, significa que está ocorrendo a mitigação da anomalia da MAC via *traffic-shaping*, ou seja, a estação em questão tem grande potencial de ser uma estação ofensora.

Dessa forma, quando existe uma relação direta e de mesma proporção entre o que foi reduzido de uma suposta estação ofensora e o aumento da vazão total da rede, então, a estação que teve sua taxa reduzida não é ofensora. Por outro lado, se a vazão total da rede aumentar de uma quantidade superior à que foi reduzida de uma determinada estação, então, essa estação pode ser a ofensora da rede.

4. MATERIAIS E MÉTODOS

Os materiais e métodos usados para o desenvolvimento deste trabalho foram os mecanismos por meio dos quais a coleta de dados foi feita tornando possível a análise desses dados, a instalação e observação da anomalia da MAC. É basicamente, um arranjo de tecnologias de hardware e software que possibilita o estudo das redes sem fio IEEE 802.11.

4.1 Plataforma de Testes

A bancada desenvolvida para os testes é composta, basicamente, por um dispositivo sem fio que atua como ponto de acesso e estações configuradas em computadores portáteis, devidamente equipados com placas que permitem o acesso à rede sem fio. A mobilidade das estações é importante para que seja possível a criação de diferentes condições de camada física. A topologia da rede básica com duas estações (Estações A e B) está ilustrada na figura 5.

Figura 5: Topologia da Rede com Duas Estações

4.1.1 Hardware

Ao longo deste trabalho, vários experimentos foram realizados com uma, duas e/ou três estações, além do próprio ponto de acesso. Com exceção do ponto de acesso sem fio, as outras estações usadas pelos experimentos são dispositivos portáteis (*notebooks*). Esses *notebooks* são dispositivos seminovos e relativamente diferentes entre si. O dispositivo mais robusto, chamado aqui de Estação A, tem uma placa de rede sem fio Intel com capacidade de conexão nos padrões IEEE 802.11 a, b, g e n. Possui um processador Intel I5, 4 GB de memória RAM e um disco rígido de 250 GB. O dispositivo mais modesto é o chamado aqui de Estação B e tem uma placa de rede sem fio IEEE 802.11 a, b, g e n. Possui um processador Intel Core I3, 4 GB de memória RAM e disco rígido de 500 GB. O dispositivo intermediário foi utilizado apenas nos experimentos com três estações e suas características físicas incluem uma placa de rede sem fio IEEE 802.11 a, b, g e n, um processador Intel Core I4 quad, 4 GB de memória RAM e disco rígido de 500 GB.

Todas as estações foram inicializadas e configuradas para fazer o carregamento do sistema operacional Linux Ubuntu a partir de um dispositivo de armazenamento em massa USB (*Universal Serial Bus*) que foi configurado previamente para ser a origem do carregamento do sistema operacional.

Mais detalhes sobre essa atividade serão descrita no item 4.1.2.

O Ponto de Acesso Sem Fio possui uma placa de rede sem fio do fabricante Mikrotik Router Board RB14. Essa é uma placa PCI e está acoplada à placa-mãe de um computador Pentium 4 com processador de 1.5 GHz, 2 GB de memória RAM e 40 GB de disco rígido.

4.1.2 Software

4.1.2.1 Sistema Operacional

Os dispositivos da bancada (ponto de acesso e estações) usam o mesmo sistema operacional, o Linux Ubuntu, escolhido por ser um *software* livre e por possuir robustez e flexibilidade necessárias para atender as necessidades dessa proposta. A instalação padrão do sistema operacional somente foi feita no ponto de acesso sem fio, pois, nas estações, ao invés de uma instalação tradicional do sistema operacional no disco rígido, optou-se pelo carregamento do sistema por meio de dispositivos de armazenamento em massa também conhecido como *pen drive*. Um *pen drive* é constituído por memória *Flash* que é um chip EEPROM (*Electrically Erasable Programmable Read Only Memory* - Memória Apenas de Leitura Programável e Apagável Eletricamente) e pode ser acoplado a um dispositivo por meio da porta USB (*Universal Serial Bus*) (INFORMÁTICA UOL, 2013).

Para carregar o sistema operacional a partir de um *pen drive*, é necessário que se instale um sistema operacional no mesmo. Esse procedimento foi executado em três *Pen Drives* e é ilustrado nos dois passos mostrados a seguir:

1 – Fazer o *download* do Sistema Operacional Linux Ubuntu a partir do *website* oficial (UBUNTU, 2013). O arquivo tem o formato “.iso” e o nome do mesmo é *ubuntu-12.04.3-desktop-i386*.

2 – Fazer *download* do programa *Universal USB Installer* a partir do site (PENDRIVELINUX, 2013) e executar o programa como ilustrado pelas figuras 6 e 7.

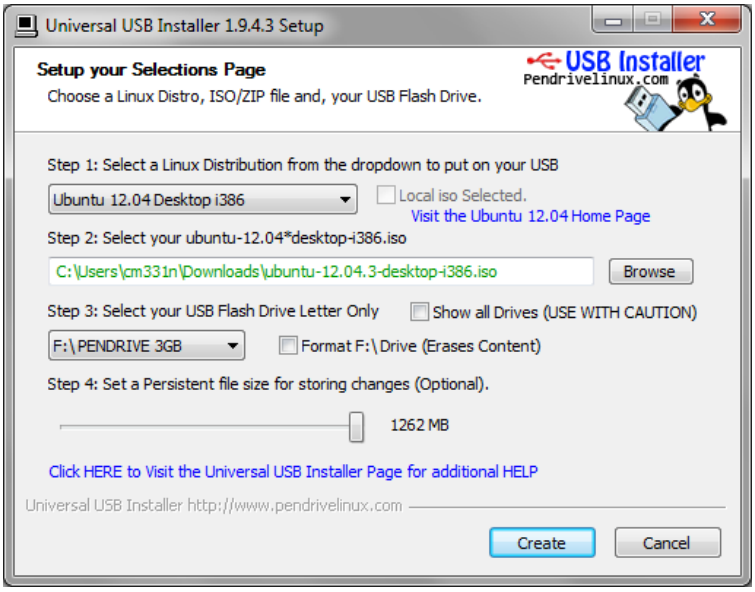


Figura 6: Tela Inicial de Instalação do Sistema Operacional no *Pen Drive*

Como pode-se observar, na primeira tela do programa para a confecção do *pen drive* de inicialização do sistema operacional, deve-se apontar a distribuição Linux que pretende-se instalar no dispositivo USB (*pen drive*). Após a indicação da distribuição, aponta-se o caminho em que foi armazenado previamente (Passo 1) o sistema operacional no computador. E por último, seleciona-se o dispositivo USB onde se deseja fazer a instalação do sistema operacional. Há ainda uma etapa opcional em que se determina um espaço que será usado pelo sistema para armazenamento permanente dos dados do usuário.

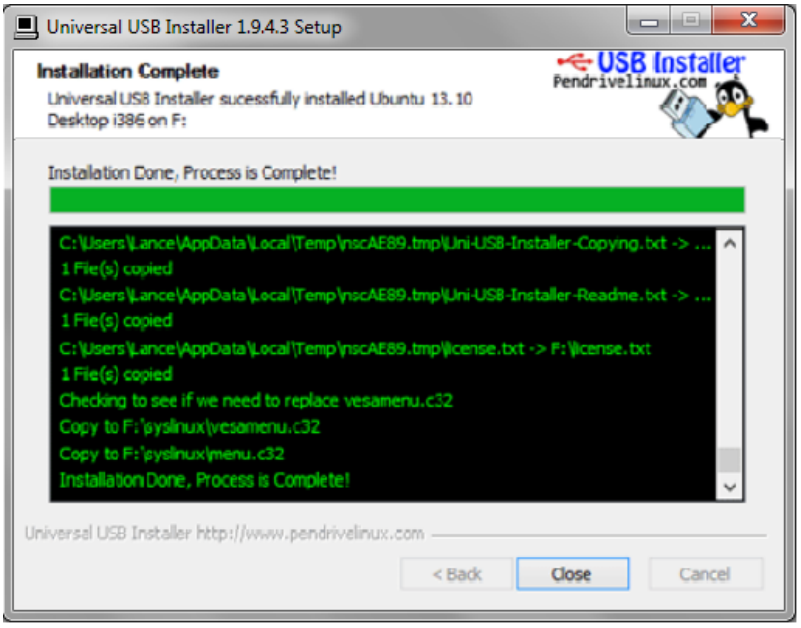


Figura 7: Tela Final de Instalação do Sistema Operacional no *Pen Drive*

Observa-se, nessa tela, que a instalação chegou ao fim e que o *pen drive* tem a capacidade de carregar um sistema operacional na inicialização do sistema.

4.1.2.2 Gerador de tráfego

Para estabelecimento dos fluxos de dados, o software de geração de tráfego de dados conhecido como *Iperf* (IPERF, 2013) foi ajustado para ser cliente nas estações e servidor no ponto de acesso. O objetivo no uso desse gerador de tráfego é criar tráfego de rede de forma a reproduzir um ambiente o mais próximo possível do real. A anomalia da MAC somente pode ser observada e/ou instalada na rede, se algum dispositivo cujas características operacionais sejam desfavoráveis fizer uso da rede.

A praticidade em se gerar tráfego com o auxílio de um gerador de tráfego como o *Iperf*, é que não há a necessidade de configuração de equipamentos adicionais para se transferir arquivos pela rede para reproduzir um ambiente real.

4.1.2.3 Linguagem de *Script*

A linguagem *Bash Script* foi utilizada para se desenvolver os *scripts* para a coleta das informações necessárias para este trabalho. *Bash* é um *shell* do *Unix* ou interpretador de linguagem de comando e por meio dessa linguagem de linha de comando interage-se com o sistema operacional.

Essa linguagem foi escolhida porque é a uma linguagem padrão no terminal do sistema operacional Linux Ubuntu. O terminal é uma interface de linhas de comandos (CLI – *Command Line Interface*) por meio da qual quaisquer comandos podem ser emitidos para que se possa tomar ciência da operação do sistema de um modo geral. O sistema interpreta os comandos digitados nessa CLI e exibe na tela a saída apropriada para o comando que foi emitido. Essa saída que geralmente é exibida na tela pode ser manipulada por meio de filtros que coletam e/ou armazenam somente as informações necessárias para o usuário. Os *scripts* usados para a coleta dos dados estão no Apêndice I.

O sistema Linux Ubuntu também conta com recursos como uma interface gráfica para interação do usuário com o sistema. No entanto, optou-se pela operação da plataforma a partir da interface de linhas de comando, já que para este trabalho, precisam-se emitir comandos para inicio e encerramento da coleta de dados que de outro modo, seria mais difícil e tornaria a operação da plataforma mais dispendiosa. Afinal, apenas dois comandos são utilizados, um para inicio da coleta e outro para encerramento.

4.2 Método de Descoberta e Gerência da Rede

O método de descoberta da rede consiste em atender as solicitações de associação dos clientes. Essa descoberta é dinâmica no sentido em que o monitoramento das solicitações de associação é constante e ocorre concomitantemente ao gerenciamento das estações em diferentes condições de tráfego.

O gerenciamento das estações consiste em usar filtros para separar e armazenar as informações consideradas necessárias a partir do sistema operacional em execução no ponto de acesso sem fio. Como mencionado na seção anterior, o sistema operacional usado pelo ponto de acesso é o Linux Ubuntu. Seu console permite uma flexibilidade muito grande, pois é diretamente em seu console que são escritos e executados scripts na linguagem *Bash Script*. As informações necessárias são capturadas por meio desses *scripts,* que filtram as saídas dos comandos, exibindo somente o que se precisa para se determinar os dispositivos da rede, bem como os parâmetros importantes para avaliação da ofensividade.

Como um exemplo do que foi descrito acima, pode-se usar o comando:

"*iw dev wlan1 station dump*"

a partir do console do *Linux Ubuntu*, cuja saída fornece várias informações operacionais usadas para se determinar a vazão total da rede. A taxa de bits nominal na qual a interface aérea WLAN 1 está operando e a sua taxa de bits efetiva, também podem ser determinadas. A figura 8 ilustra a saída do comando.

```
$ iw dev wlan1 station dump
Station 12:34:56:78:9a:bc (on wlan0)
        inactive time:  304 ms
        rx bytes:       18816
        rx packets:     75
        tx bytes:       5386
        tx packets:     21
        signal:         -29 dBm
        tx bitrate:     54.0 MBit/s
```

Figura 8: Saída do Comando "*iw"*

Com a linguagem descrita no item 4.1.2, pode-se coletar cada um dos valores exibidos pelo comando "*iw dev wlan1 station dump*" e armazená-los em variáveis de forma que os dados possam ser processados adequadamente e posteriormente armazenados. Os *scripts* desenvolvidos neste trabalho se encontram nos Apêndices 3 e 4.

4.3 Estimação da Vazão Máxima da Rede

Sob condições normais, a vazão máxima da rede pode ser estimada por meio de uma tentativa de transferência de dados por parte de uma estação conectada à rede, através de um *software* especifico para emular o fluxo de dados (*Iperf*) ajustado para operar em uma taxa superior à taxa nominal da rede. Ou seja, o estresse causado à rede por meio da tentativa de transferência forçada a uma taxa acima à taxa nominal da rede, faz com que o *throughput* máximo seja atingido.

Essa tentativa de estressar a rede também é válida com múltiplas estações fazendo um extensivo uso da rede. Na teoria, a divisão da vazão máxima suportada pela rede pelo número de estações conectadas deveria resultar em uma taxa igual para todas as estações, mas, na prática, o que se observa é diferente. Algumas estações transmitem dados pela rede a taxas superiores do que outras; no entanto, a soma das taxas de transferência de todas as estações equivale à vazão total da rede (considerando aqui que não há o aparecimento da anomalia da MAC).

A importância em se estimar a vazão máxima da rede é saber quando uma rede está sofrendo com a presença de um ofensor, pois, a principal consequência da anomalia da MAC IEEE 802.11 é o impacto negativo na vazão máxima da rede. Se várias estações se conectarem à rede, mas a vazão total da rede se mantiver, então, a anomalia da MAC não está instalada na rede.

4.4 Índices de Sensibilidade

Conforme abordado no item 3.5, a análise de sensibilidade é feita com o uso de um índice de sensibilidade. Esse índice de sensibilidade é um valor que representa um decremento ou incremento na taxa de transferência de um dispositivo da rede, com o objetivo de verificar qual foi o resultado dessa ação na vazão total. Por exemplo: momentos após o decremento do valor determinado como índice de sensibilidade espera-se uma resposta positiva na vazão total da rede; caso a vazão da rede apresente um aumento consideravelmente acima do que foi decrementado, conclui-se que o dispositivo que teve sua taxa de transferência

decrementada era o ofensor da rede; senão, o dispositivo não era o ofensor da rede. O contrário também é verdadeiro, ou seja, por consequência de um eventual incremento na taxa de um dispositivo ofensor, uma diminuição considerável na vazão total da rede seria observada.

Neste trabalho, observou-se o comportamento da sensibilidade da rede após a coleta dos dados. O cálculo do índice de sensibilidade para as estações em relação à própria vazão total da rede é dado pela equação 1:

$$S_i = \frac{\Delta TE_i}{\Delta VT} \quad (1)$$

Onde:

- $\boldsymbol{S_i}$ é o índice de Sensibilidade da estação i;
- $\Delta\boldsymbol{TE_i}$ é a variação da Taxa de Transferência da Estação i, no intervalo de tempo considerado para o cálculo do índice de sensibilidade;
- $\Delta\boldsymbol{VT}$ é a variação da Taxa da Vazão Total da rede, no intervalo de tempo considerado para o cálculo do índice de sensibilidade.

5. RESULTADOS

Os componentes da plataforma de testes foram descritos de forma individual no item 4.1 e a forma como esses componentes interagem possibilita a análise da rede por meio da coleta de dados, tornando possível a observação do efeito que é objeto de estudo deste trabalho. Portanto, a validação da plataforma de testes é uma etapa fundamental para a realização dos experimentos necessários para identificação da anomalia da MAC. A figura 9 ilustra fisicamente a bancada de testes e seus principais componentes.

Figura 9: Equipamentos da Bancada de Testes

5.1 Operação da Plataforma de Testes

Quando se iniciam as operações dos equipamentos que compõem o experimento, por meio do sistema de inicialização descrito no item 4.1.2, as estações identificam, automaticamente, as redes sem fio disponíveis. Cabe ao operador da plataforma escolher em cada estação a rede apropriada à qual está

associado o ponto de acesso. Feita essa identificação, as estações se associam no ponto de acesso e recebem um endereço IP automaticamente.

Nessas condições, a rede básica está montada, mas, não está operacional. O próximo passo consiste em inicializar o gerador de tráfego (*Iperf*) no ponto de acesso (no modo *server*), que fica em modo de espera, na “escuta” do canal, aguardando as estações. O tráfego entre cada estação e o ponto de acesso, é estabelecido por meio da inicialização do gerador de tráfego (no modo *client*) em cada estação individualmente. Assim, as relações de tráfego na rede são controladas por meio do estado do gerador de tráfego nas estações e não no ponto de acesso. No entanto, a presença de tráfego não implica necessariamente em coleta de dados. Somente após a emissão de comandos apropriados no ponto de acesso, a coleta dos dados pode ser iniciada e/ou finalizada.

5.1.1 Comando para Início do Processo de Coleta dos Dados

O comando para início do processo de coleta dos dados consiste em digitar os seguintes termos (sem aspas) no console do ponto de acesso, após acessá-lo local ou remotamente: “*./sta_monitor start N”*. Esse comando tem o objetivo de disparar o *script* chamado sta_monitor, o qual contém as instruções para a coleta dos dados propriamente dita. O número “N” representa o número de medidas a partir das quais a média é calculada para que seja armazenada apenas uma coleta ao invés de todas, ou seja, o dispositivo armazena a média de “N” medições como taxa efetiva, taxa nominal e potência do sinal recebido. Cada medida leva um segundo para ser feita e também são armazenadas sem que nenhum cálculo seja feito; portanto, as medidas “cruas” também são armazenadas pelo sistema. A figura 10 ilustra o fluxograma que mostra como o comando para início do processo de coleta de dados funciona:

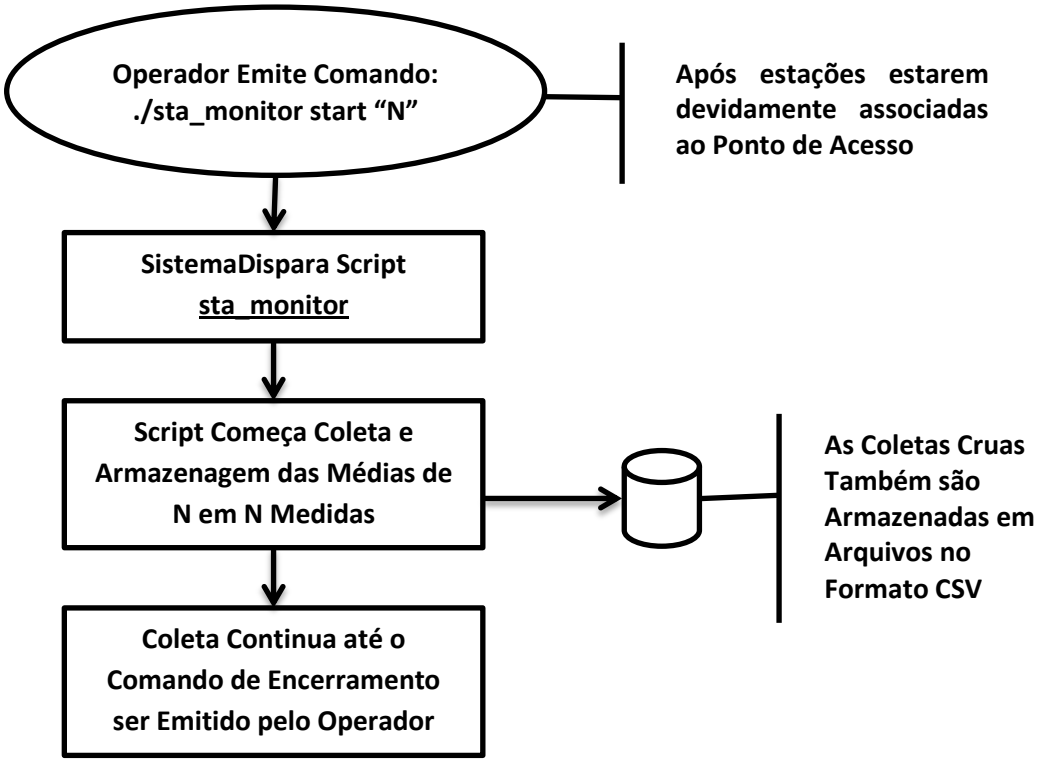


Figura 10: Fluxograma do Início de Coleta de Dados

5.1.2 Comando para Encerramento do Processo de Coleta dos Dados

Da mesma forma que o operador emitiu o comando para dar início à coleta de dados, o comando de encerramento de dados precisa ser emitido a partir do console do ponto de acesso e sua sintaxe é como se segue (sem aspas) "*./sta_monitor stop"*. A figura 11 ilustra o fluxograma que mostra como o comando de encerramento funciona.

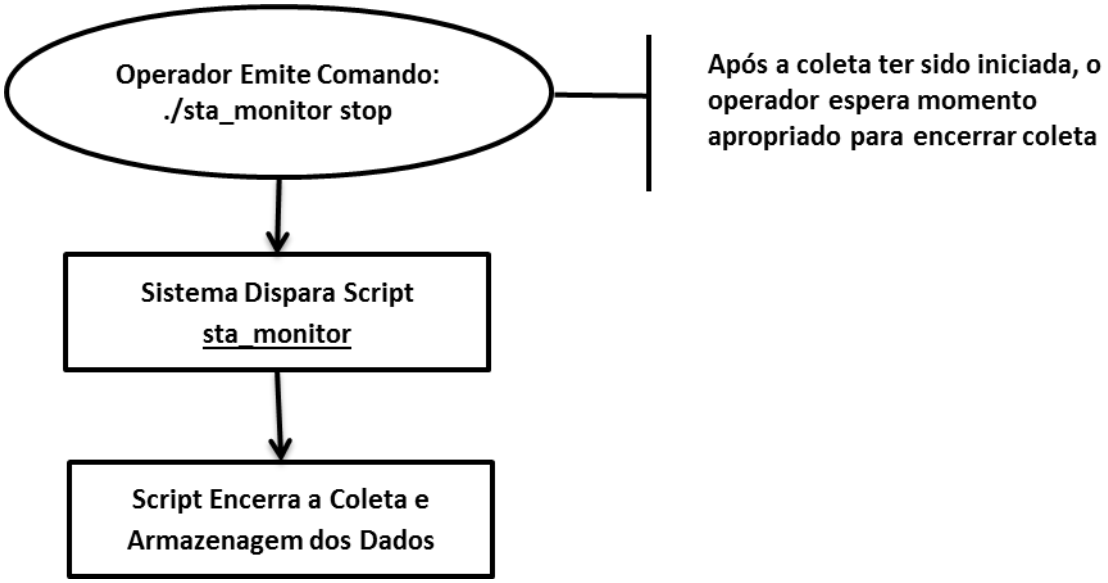


Figura 11: Fluxograma de Encerramento de Coleta de Dados

5.1.3 Estrutura de Arquivos de Dados

Na tabela 2, podem ser observadas as medições na ordem em que elas foram coletadas pelo *script* no ponto de acesso e dispostas no arquivo CSV.

Tabela 2: Estrutura dos Arquivos de Dados no Formato CSV

Data e Hora	Potência do Sinal Recebido (dBm)	Ruído (dBm)	SNR (dB)	Taxa Nominal (Mb/s)	Taxa Efetiva (bits/s)
5/16/2013 18:56	-40	-80	40	11	7063824
5/16/2013 18:56	-41	-80	39	11	7248480
5/16/2013 18:56	-41	-80	39	11	6940752
5/16/2013 18:56	-44	-80	36	11	6928512
5/16/2013 18:56	-43	-80	37	11	6977472

Com o resultado da coleta em mãos, torna-se possível a realização de análises sobre a anomalia da MAC se instalando na rede, a vazão das estações individualmente (caso não haja a presença da anomalia) ou apenas a vazão da rede (*throughput*).

5.2 Testes de Vazão da Rede

Nestes testes, foram utilizados dois cenários para se determinar a vazão total disponibilizada pelo ponto de acesso da rede. No primeiro, apenas uma estação foi usada (denominada Estação A). Esta estação foi forçada a alocar toda capacidade da rede por meio do ajuste do *software* para a geração artificial de tráfego. Em outras palavras, com o objetivo de levar a rede ao seu limite, configura-se o gerador de tráfego para usar uma taxa de dados algumas vezes maior que a taxa efetiva da rede de 11 Mb/s, conforme ilustrado na figura 12.

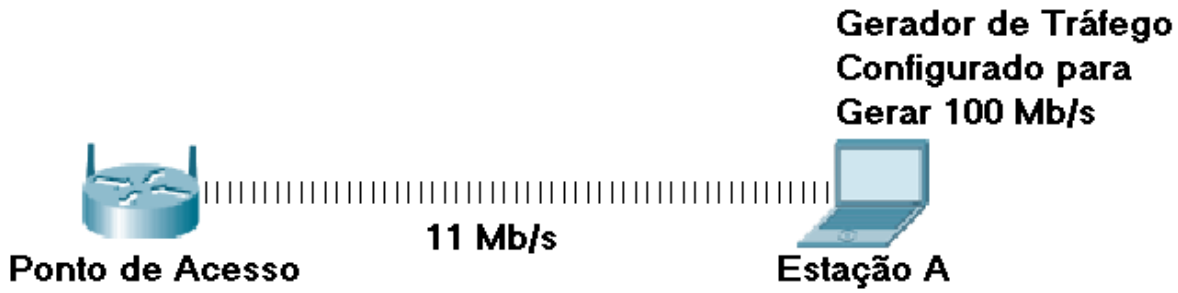


Figura 12: Topologia do Primeiro Cenário do Teste de Vazão da Rede

Nessas condições, a gerência da rede resultou em uma coleta de dados que se aproxima da vazão total efetivamente monitorada na placa de rede do ponto de acesso, conforme ilustrado pela figura 13:

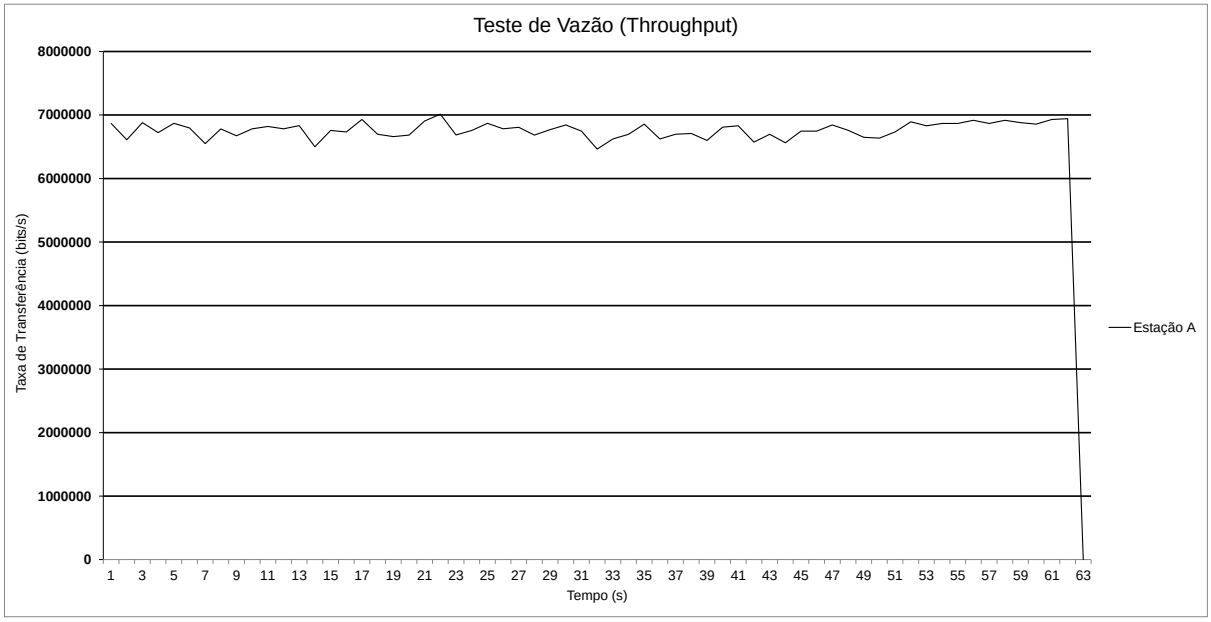


Figura 13: Teste de Vazão da Rede com uma Estação

Neste caso, verifica-se que a capacidade limite de vazão do ponto de acesso é da ordem de 6764945 bits/s ou, aproximadamente, 6,76 Mb/s.

Já no segundo cenário testado para se determinar a vazão da rede, duas estações foram deixadas livres para negociar suas taxas com o ponto de acesso, conforme ilustrado na figura 14.

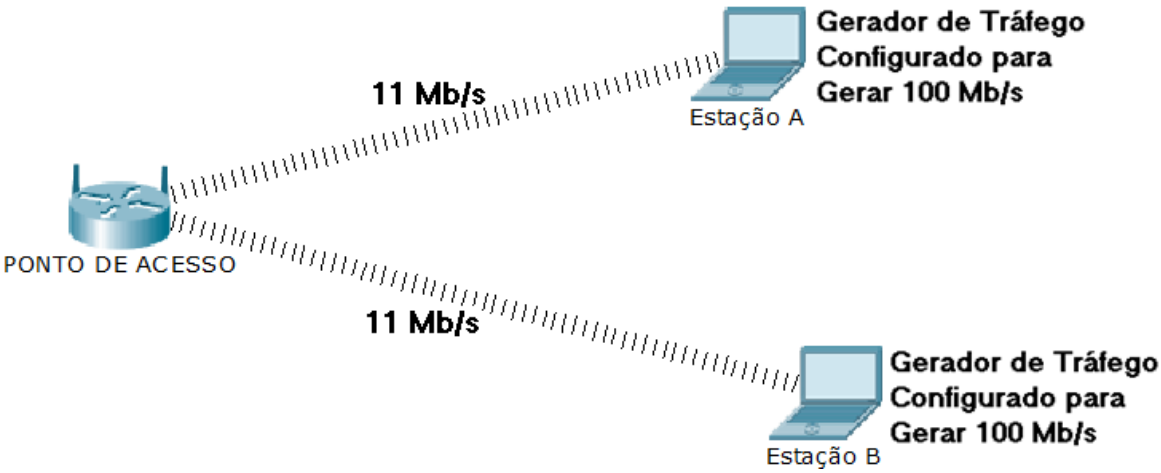


Figura 14: Topologia do Segundo Cenário do Teste de Vazão da Rede

Nesse cenário, a estação A inicia tráfego com o ponto de acesso aos 11 segundos de monitoramento, enquanto a estação B inicia tráfego com o ponto de acesso aos 74 segundos e encerra esse tráfego aos 135 segundos. A estação A

encerra seu tráfego aos 138 segundos. A Figura15 ilustra a evolução das taxas de transmissão praticadas pelas duas estações com o passar do tempo.

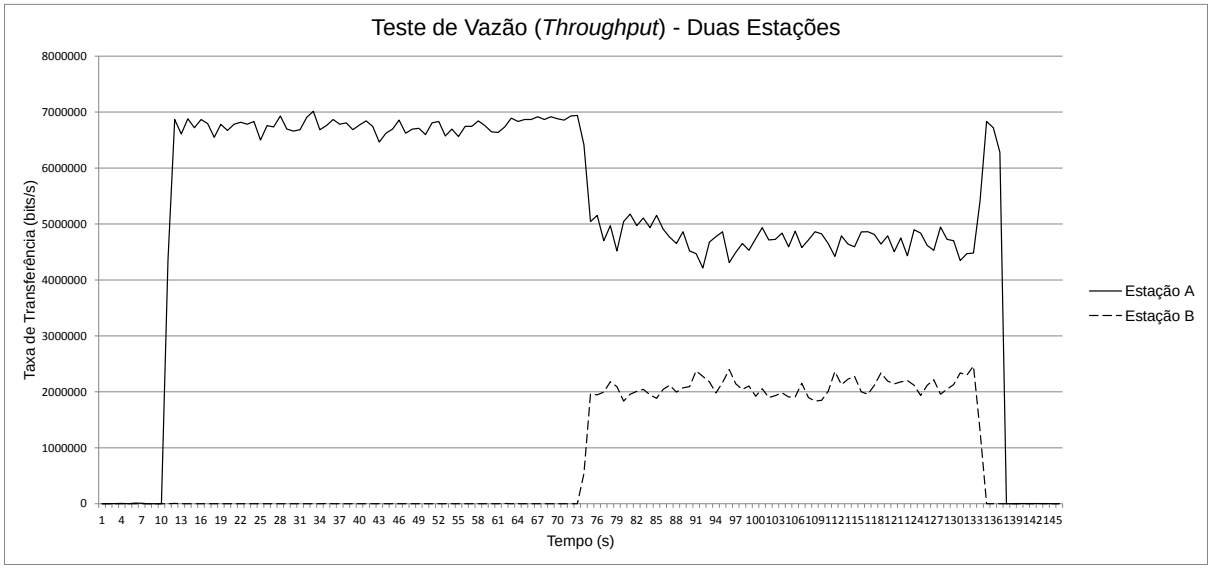


Figura 15: Teste de Vazão da Rede com Duas Estações

Nesse caso, a estação A ocupa praticamente toda a capacidade do canal no início do experimento. Posteriormente, observa-se um compartilhamento da capacidade do canal quando a estação B passa a fazer uso da rede. No entanto, não houve caracterização da anomalia, pois a capacidade total de vazão total (*throughput)* da rede, igual à soma das vazões de ambas as estações, é mantida, conforme ilustrado na figura 16.

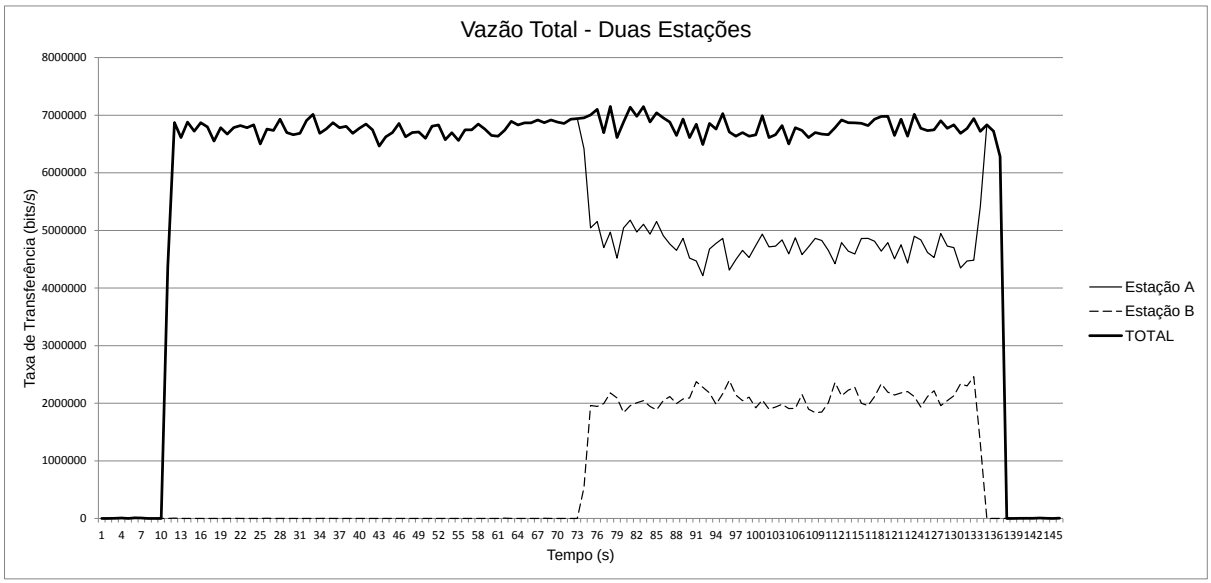


Figura 16: Teste de Vazão Total da Rede com Duas Estações

Repetindo-se o experimento para três estações, conforme ilustrado na figura 17, o mesmo comportamento sobre o compartilhamento da capacidade do canal pode ser observado.

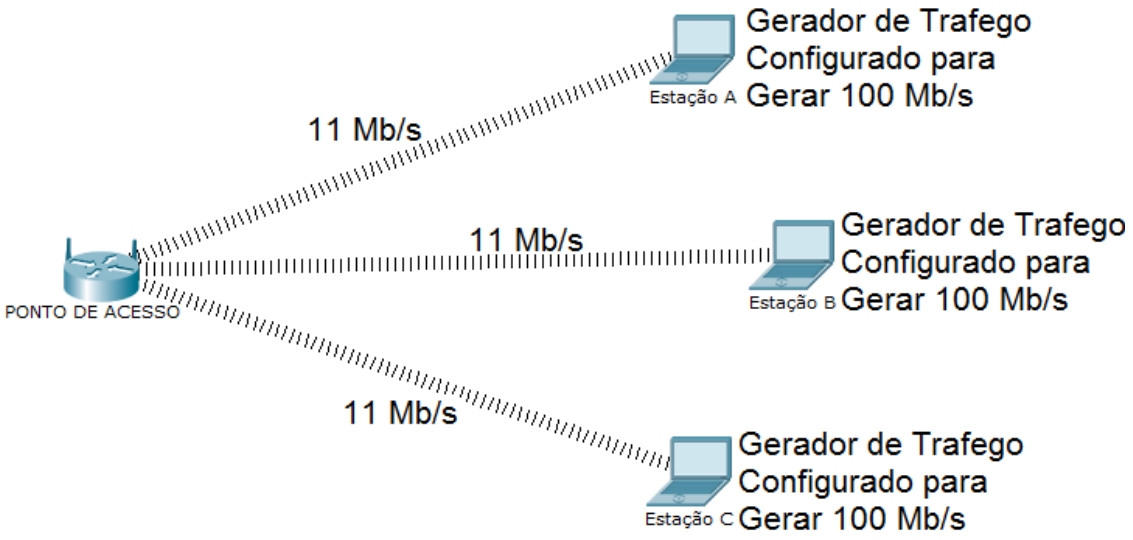


Figura 17: Topologia do Terceiro Cenário do Teste de Vazão da Rede

Neste experimento, todas as estações já estavam gerando tráfego de dados e começaram a ser monitoradas. O valor médio da soma das coletas da taxa de transferência efetiva (vazão) é de 6999890 bits/s ou aproximadamente 6,99 Mb/s conforme observado na figura 18.

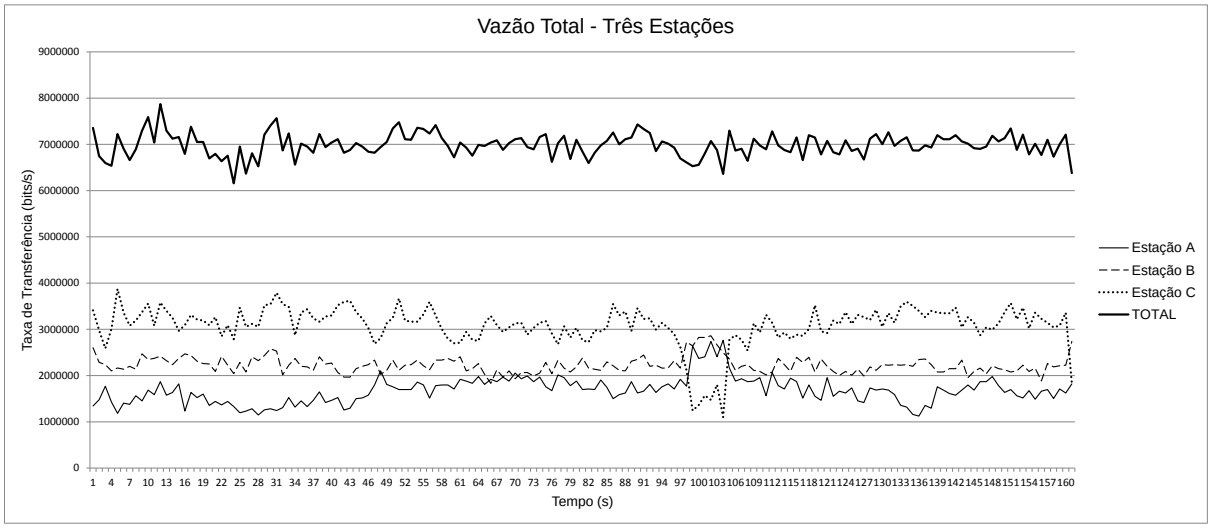


Figura 18: Teste de Vazão Total da Rede com Três Estações

O teste de vazão é importante porque é possível detectar se a anomalia está instalada na rede por meio da análise da soma das vazões. Se a soma das vazões

resulta em um valor inferior ao valor da vazão típica de uma rede sem anomalia, então, a rede está diante da presença da anomalia da MAC.

5.3 Testes de Instalação da Anomalia

A plataforma de testes especificada neste trabalho permite a instalação da anomalia da MAC, ou seja, com o auxílio da bancada, pode-se reproduzir as condições sob as quais a anomalia se instala na rede. Por meio da coleta e armazenamento dos dados, a etapa seguinte é realizar a análise dos mesmos. Portanto, a instalação da anomalia é fundamental para o estudo e entendimento do problema, para que se desenvolva um método de identificação do dispositivo causador da anomalia (ofensor).

Vários cenários foram desenvolvidos, no decorrer do trabalho, para se entender mais sobre o comportamento da anomalia. Em alguns cenários, a anomalia foi criada de forma artificial por meio de configurações específicas feitas nas estações usadas nos experimentos e isso consiste, basicamente, em forçar uma estação a operar em taxas de dados específicas que normalmente diferem das taxas de outras estações. Outra forma de observar a anomalia é pela degradação da potência do sinal recebido, que consiste em aumentar a distância entre a estação e o ponto de acesso ou fazer uso de obstáculos com o mesmo propósito. Há ainda um experimento, em um ambiente real, em que a anomalia se instalou com sucesso na rede e a plataforma de testes foi capaz de coletar e armazenar corretamente os dados.

Nos cenários em que a taxa de transferência foi alterada e/ou forçada a operar abaixo dos os outros dispositivos da rede, pode-se observar a anomalia se instalando instantaneamente, conforme mostrado na figura 19, em que a estação foi forçada a operar a 1 Mb/s.

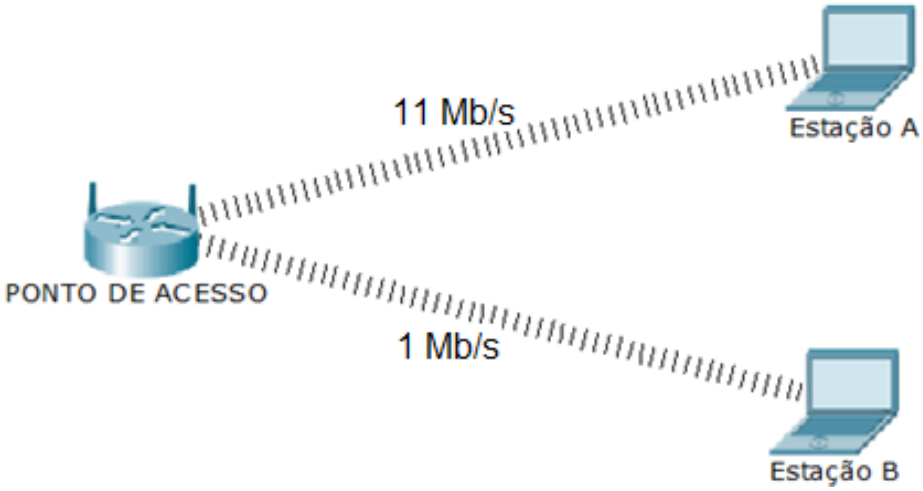


Figura 19: Topologia da Rede – Estação Operando a 1 Mb/s

A gerência da rede resultou em uma coleta de dados que reflete os efeitos das medições monitoradas na placa de rede do ponto de acesso. Desde o início do experimento, a Estação A está transmitindo dados a uma taxa média de 6966251 bits/s, ou aproximadamente 6,96 Mb/s, quando a Estação B entra transmitindo a 1 Mb/s aos 65 segundos. Nesse ponto, pode-se ver claramente a anomalia se instalando na rede. Aos 134 segundos a Estação B para de transmitir dados pela rede e a anomalia deixa de ocorrer, conforme ilustrado pela figura 20.

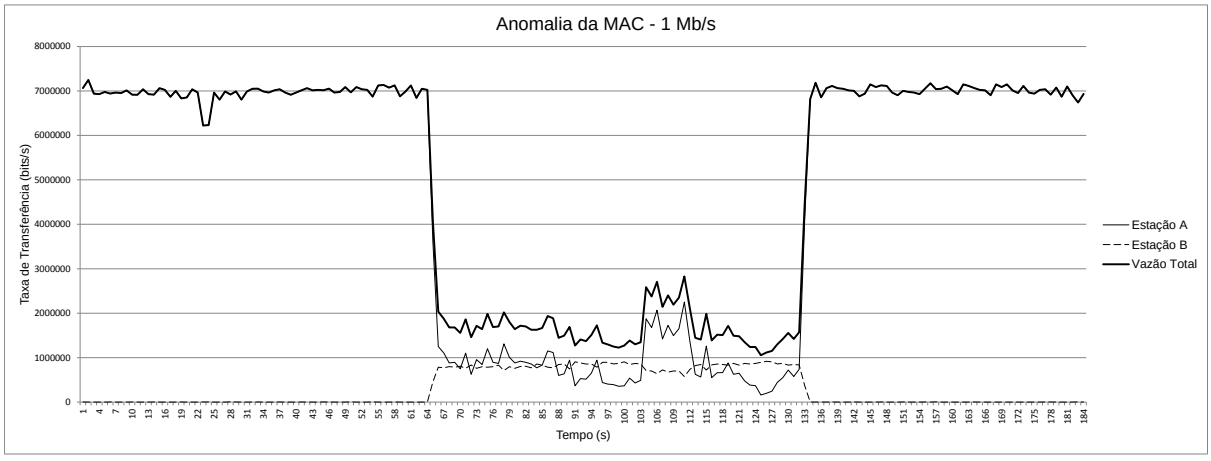


Figura 20: Anomalia da MAC com Taxa de Transferência de 1 Mb/s

Observa-se que, sob os efeitos da anomalia, a vazão total da rede é afetada negativamente e isso faz com que os recursos da rede sejam subutilizados. No momento em que a anomalia está instalada na rede, a vazão total média é de 1654821 bits/s, ou aproximadamente 1,65 Mb/s, contrastando com a vazão inicial de

aproximadamente 6,96 Mb/s, de quando a rede não estava sofrendo os efeitos da anomalia.

Os efeitos da anomalia puderam ser reproduzidos e observados não só com a taxa do ofensor de 1 Mb/s mas, com taxas mais altas também, tais como, 2 Mb/s e 5,5 Mb/s. A figura 21 ilustra o cenário com duas estações sendo uma com taxa de 11 Mb/s e outra com taxa de 2 Mb/s.

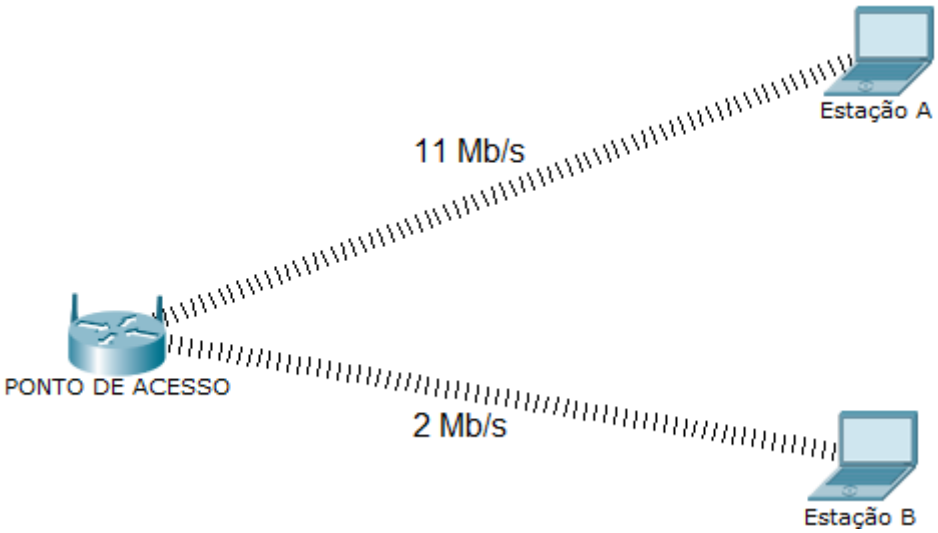


Figura 21: Topologia da Rede – Estação Operando a 2 Mb/s

Os efeitos em taxas mais altas são similares e a principal característica é a vazão total da rede sendo afetada negativamente, conforme ilustrado pela figura 22, a Estação A, num primeiro instante, faz uso de toda a vazão da rede cuja média era de aproximadamente 6,99 Mb/s. Aos 77 segundos a Estação B começa a transferir dados pela rede a uma taxa de 2 Mb/s causando anomalia da MAC na rede. A vazão total ficou reduzida à 3099356 bits/s, aproximadamente, 3 Mb/s. Aos 137 segundos, a Estação B para a transmissão completamente e a vazão total da rede retorna aos valores observados no início do experimento. Dada a vazão total sem anomalia e a vazão total com anomalia, a degradação foi de 3,99 Mb/s.

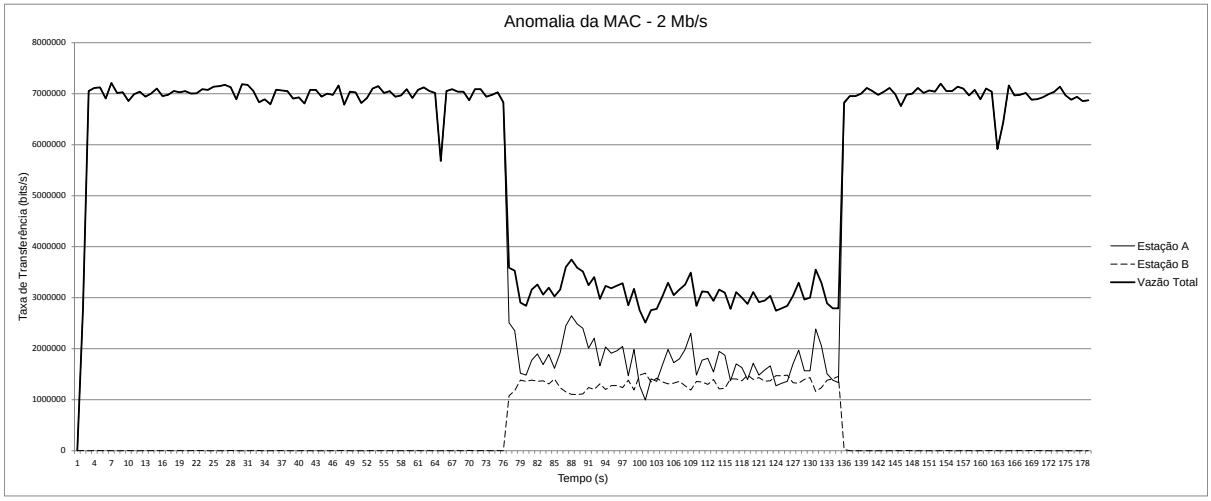


Figura 22: Anomalia da MAC com Taxa de Transferência de 2 Mb/s

No cenário ilustrado pela figura 23, com as taxas das Estações A e B operando em 11 Mb/s e 5,5 Mb/s, respectivamente, pode-se observar que os efeitos da anomalia da MAC são minimizados, mas não deixam de estar presentes.

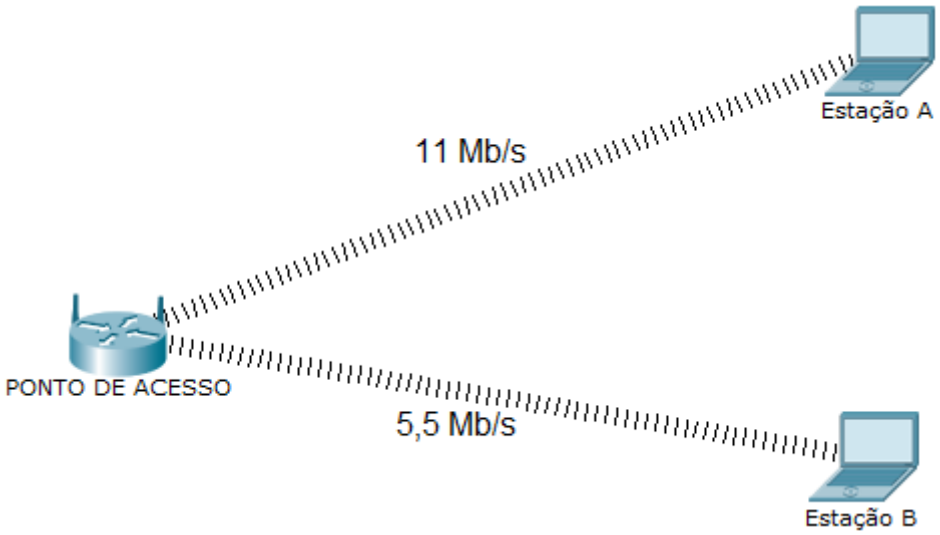


Figura 23: Topologia da Rede – Estação Operando a 5,5 Mb/s

Nos momentos iniciais do experimento, a vazão total da rede é de 6975031 bits/s ou aproximadamente 6,97 Mb/s e a Estação A faz uso de toda essa taxa. Aos 62 segundos a Estação B começa fazer uso da rede a uma taxa de 5,5 Mb/s. Durante o tempo em que a Estação B fica na rede a vazão total média é de 5707264 ou aproximadamente 5,70 Mb/s. A diferença entre a vazão original, apenas com a Estação A, e a vazão com a presença da Estação B é de 1267767 ou aproximadamente 1,26 Mb/s; em outras palavras, a vazão da rede diminuiu em 1,26

Mb/s com a presença da Estação B configurada para operar em 5,5 Mb/s conforme mostrado na figura 24.

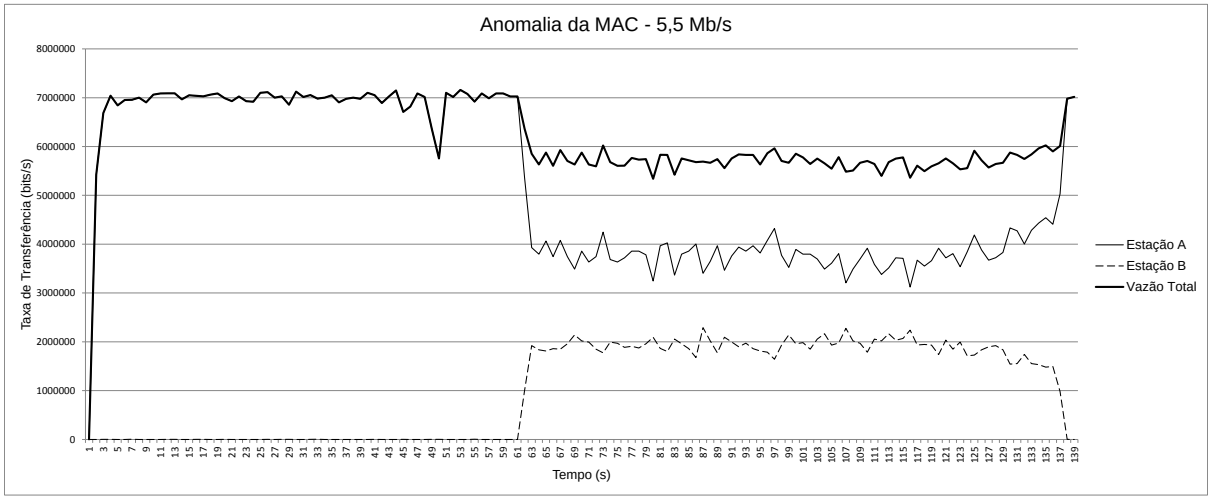


Figura 24: Anomalia da MAC com Taxa de Transferência de 5,5 Mb/s

Com o objetivo de explorar a instalação da anomalia em condições desfavoráveis de propagação do sinal, a estação B foi progressivamente afastada do ponto de acesso enquanto demandava tráfego da rede, sendo, portanto, colocada em uma condição de redução da relação sinal-ruído. Com isso, se tornou a ofensora da rede em alguns momentos, como observado na figura 25.

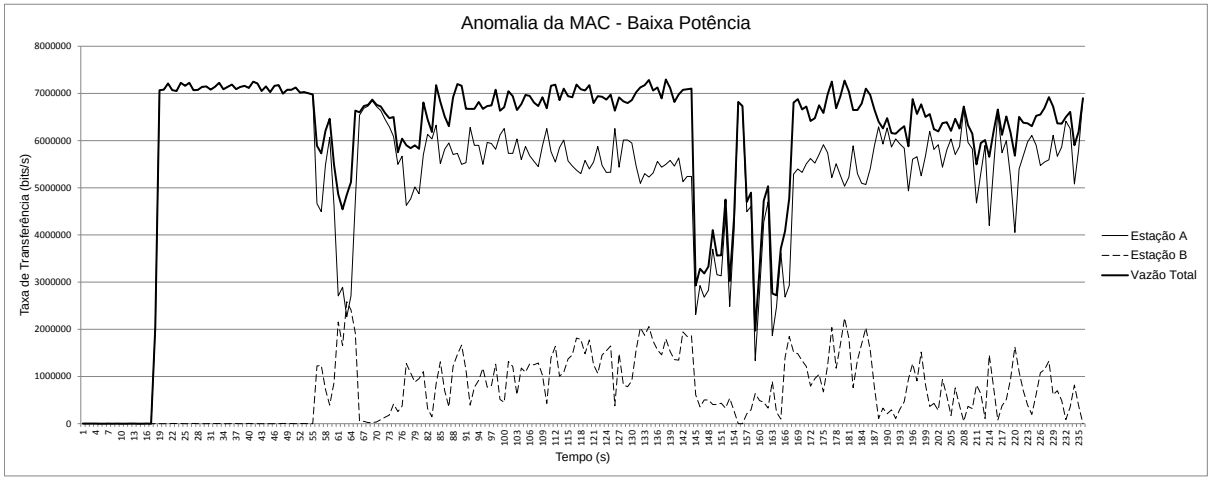


Figura 25: Anomalia da MAC em Condições Desfavoráveis de Propagação do Sinal

Os experimentos com duas estações foram repetidos para cenários com três estações. No cenário com três estações, pôde-se observar todas as características do experimento com duas estações, tais como, o compartilhamento da vazão total

da rede pelas estações nos momentos em que não há a presença de um dispositivo ofensor na rede e no momento em que há a presença de ofensor, a rede tem seus recursos subutilizados. A figura 26 ilustra a anomalia da MAC com taxa de transferência de 1 Mb/s num cenário com três estações.

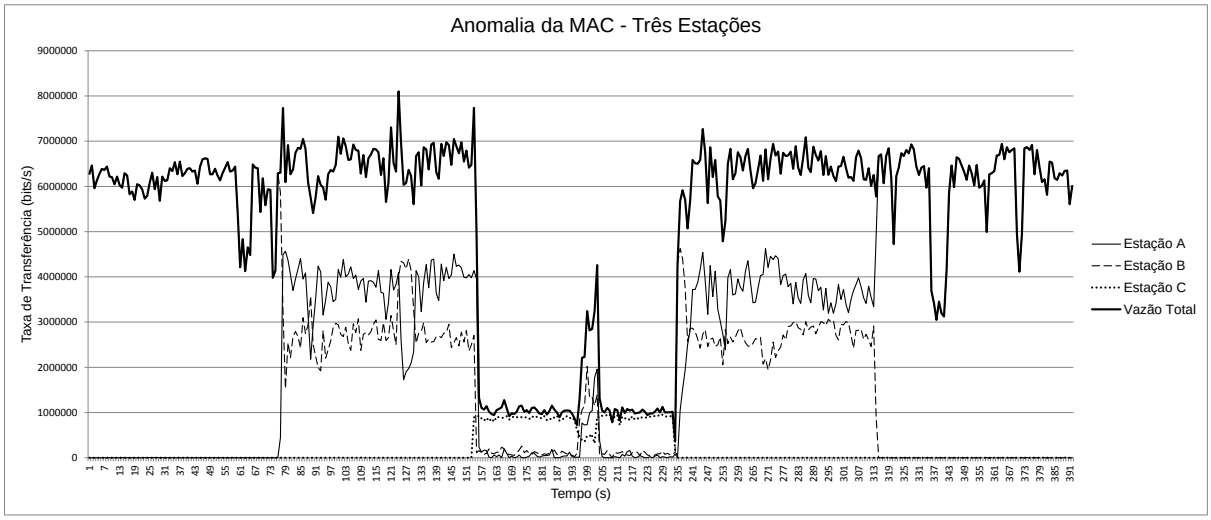


Figura 26: Anomalia com Taxa de Transferência de 1 Mb/s - Três Estações

Em outro experimento com três estações, foi explorada a possibilidade de uma estação, num determinado momento ser ofensora e, num segundo momento, tornar-se não-ofensora. Na Figura 27, aos 143 segundos de medição, a Estação B começa fazer uso da rede a uma taxa de 1 Mb/s. Ela permanece na rede sendo ofensora até os 216 segundos e, então, foi deixada livre para negociar sua taxa de transferência com o ponto de acesso. A partir da negociação, a estação começa a transmitir dados pela rede a uma taxa nominal de 11 Mb/s. Neste ponto, a estação deixa, portanto, de ser a ofensora da rede, pois se encontra nas mesmas condições da demais estações da rede. Após o período de negociação a rede fica estável novamente e as três estações passam a compartilhar a vazão total da rede conforme esperado em uma rede sem a presença da anomalia. A figura 26 ilustra as etapas da estação que deixa de ser ofensora da rede após um breve período em que era a causadora da anomalia da MAC.

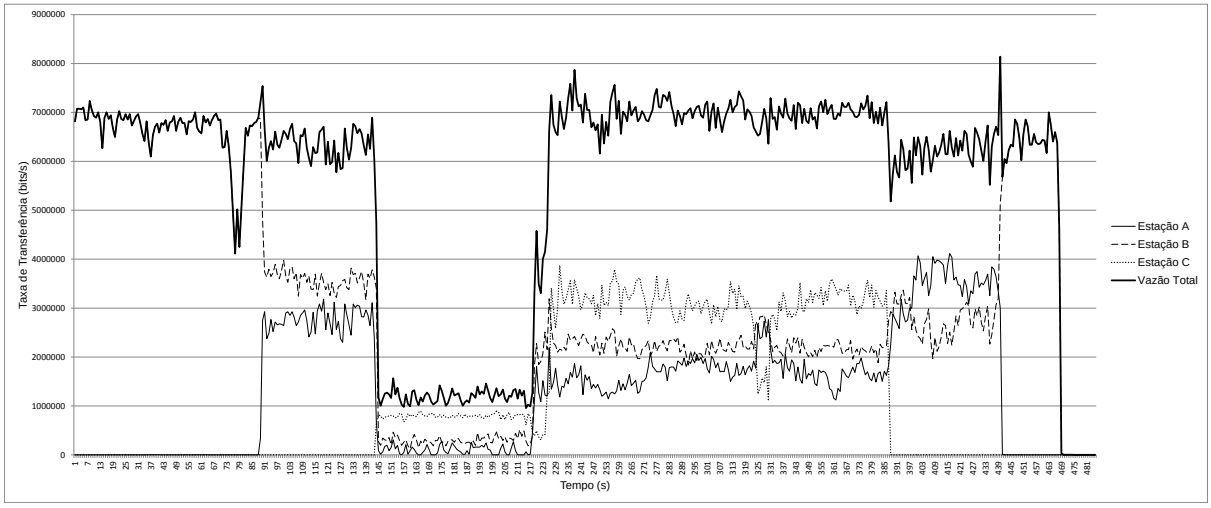


Figura 27: Máquina Ofensora Torna-se Não-Ofensora - Três Estações

5.4 Testes de Sensibilidade

O teste de sensibilidade é fundamental para determinação do ofensor da rede. Em termos gerais, o comportamento dos dados no momento em que ocorre a anomalia mostra que a mínima queda na taxa de transferência da estação ofensora representa um aumento significativo na vazão total da rede, por isso, observa-se que a sensibilidade da estação ofensora tende a ficar com valores menores e negativos. O valor de ΔT nos experimentos executados neste trabalho é de 10 segundos. A figura 28 ilustra os efeitos da sensibilidade numa rede com duas estações. Nesta figura vê-se claramente que a Estação B, representada por “SensB” é a ofensora da rede.

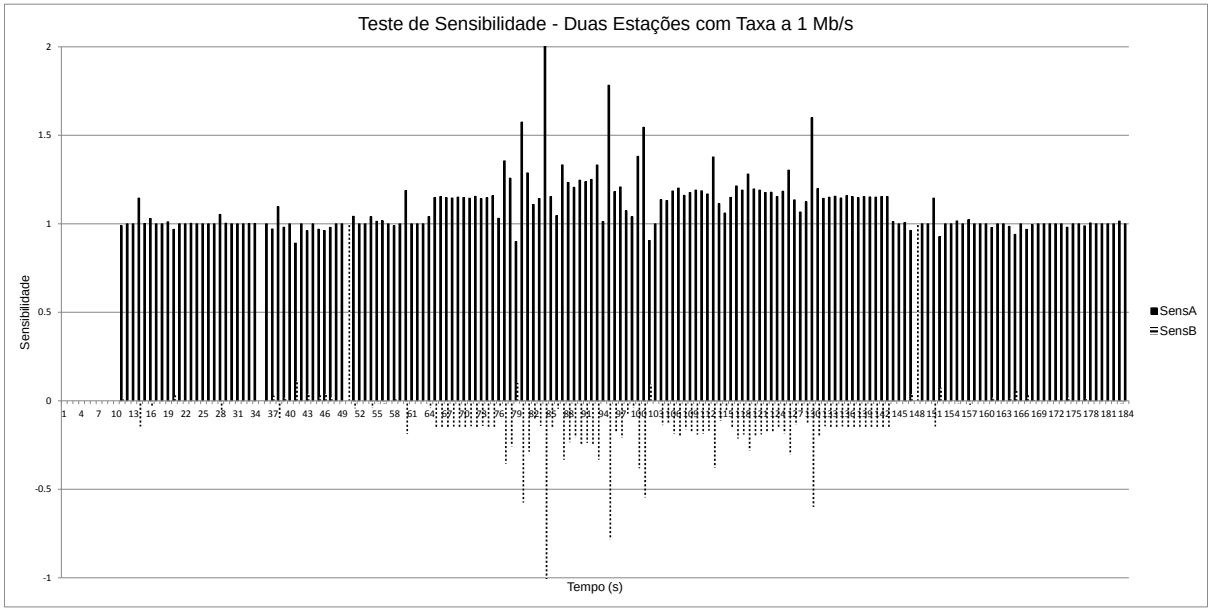


Figura 28: Teste de Sensibilidade - Duas Estações com Taxa de 1 Mb/s

Resultado similar foi observado no cenário com duas estações operando a 2 Mb/s representado pela figura 29. A sensibilidade da estação B se manteve negativa na maior parte do tempo em que a estação permaneceu na rede.

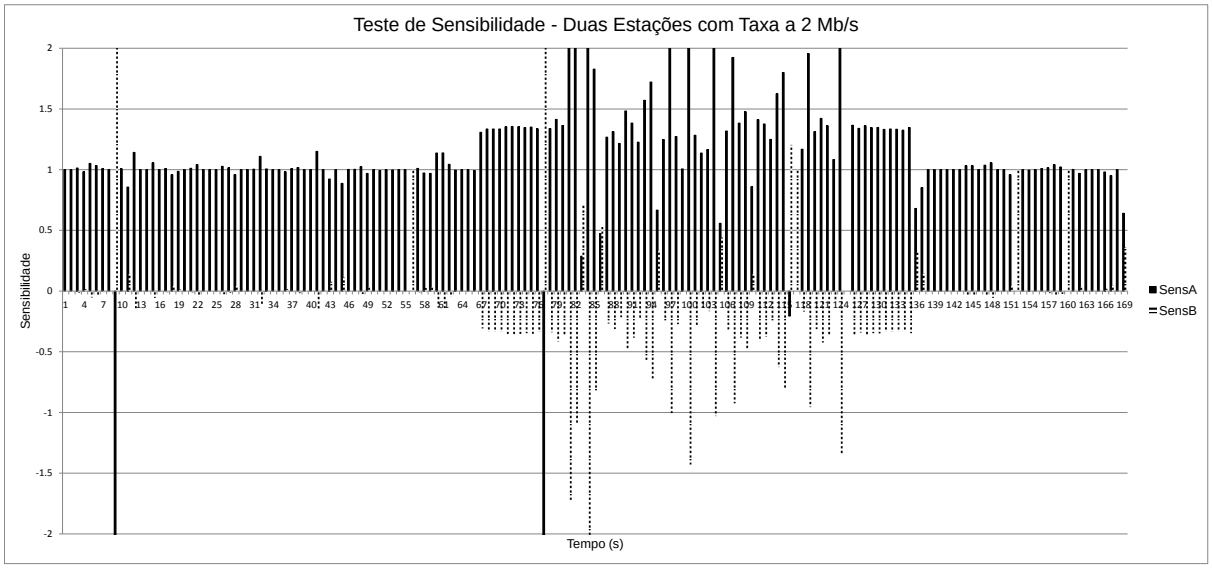


Figura 29: Teste de Sensibilidade - Duas Estações com Taxa de 2 Mb/s

Bem como nos resultados prévios com duas estações e taxas de 1 Mb/s e 2 Mb/s, o resultado do teste de sensibilidade com duas estações com taxa de transferência de 5,5 Mb/s também é conclusivo e a estação ofensora, no caso a

estação B, apresenta a sensibilidade com valores negativos conforme ilustrado pela figura 30.

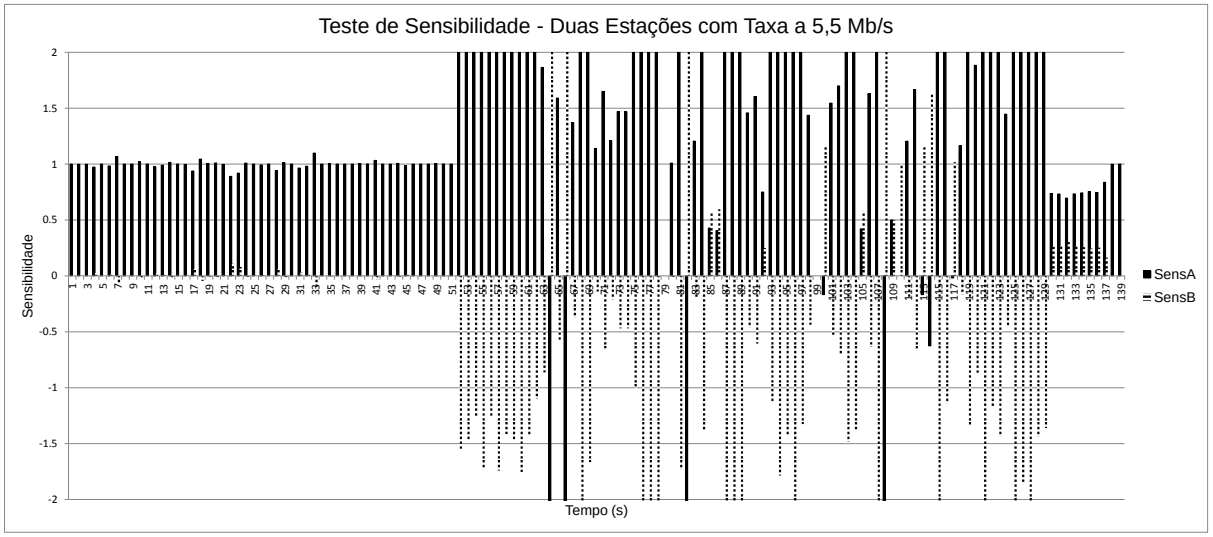


Figura 30: Teste de Sensibilidade - Duas Estações com Taxa de 5,5 Mb/s

Quando o cenário muda e passa a ter três estações ao invés de duas, os resultados obtidos são mais complexos, mas ainda apresentam um comportamento notável que segue o mesmo padrão descrito anteriormente, conforme ilustrado pela Figura 31.

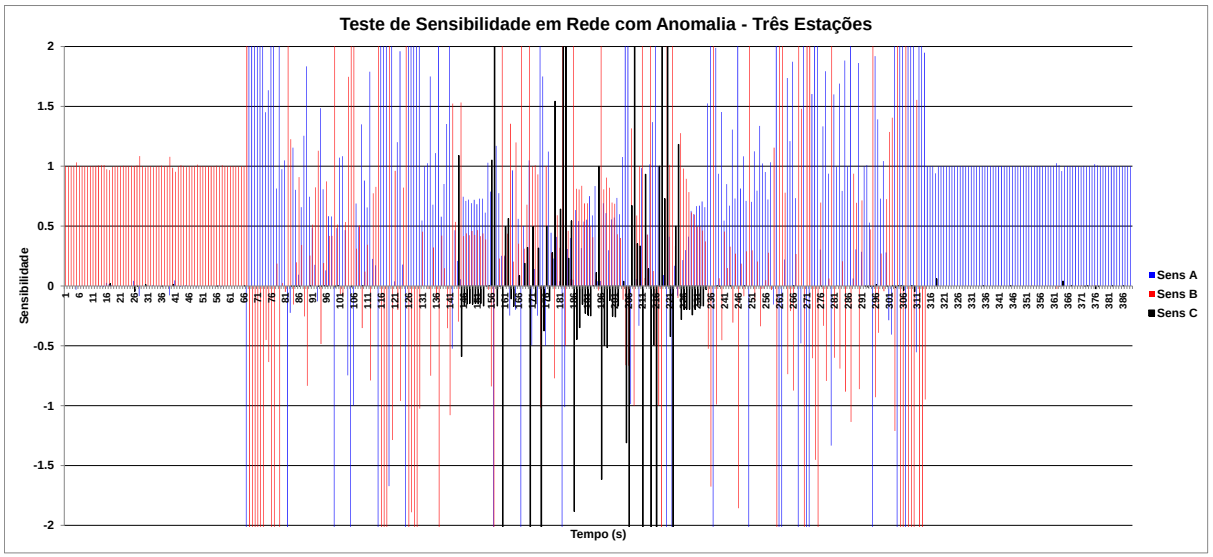


Figura 31: Teste de Sensibilidade - Três Estações com Taxa de 1 Mb/s

Para ser mais bem compreendida, a figura 31 foi segmentada em 3 partes em que a rede apresenta comportamentos diferentes (Parte A, Parte B e Parte C).

Como pode se observar na Parte A, ainda na figura 32, até os 66 segundos de coletas de dados, somente a estação B estava transmitindo dados pela rede fazendo uso de toda vazão.

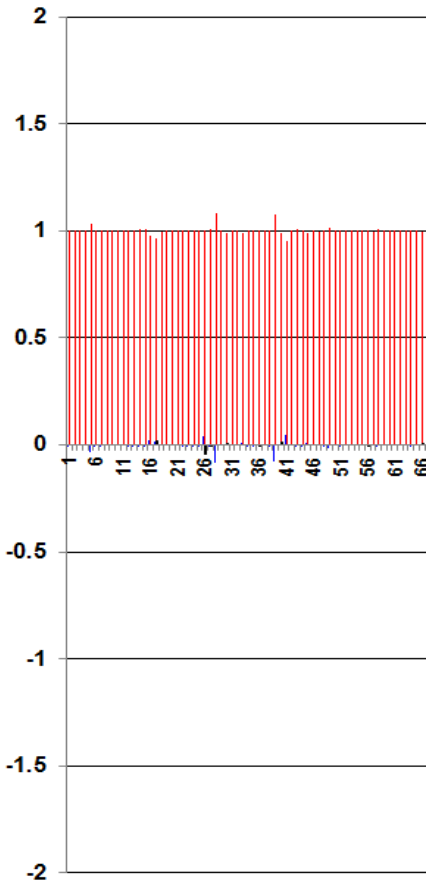


Figura 32: Teste de Sensibilidade – Três Estações – Parte A

Na Parte B representada pela figura 33, aos 67 segundos, a estação A começou a fazer uso da rede, então, a vazão total passou a ser compartilhada, mas ainda não há a presença de anomalia uma vez que o padrão observado nos experimentos anteriores ainda não foi observado até os 143 segundos.

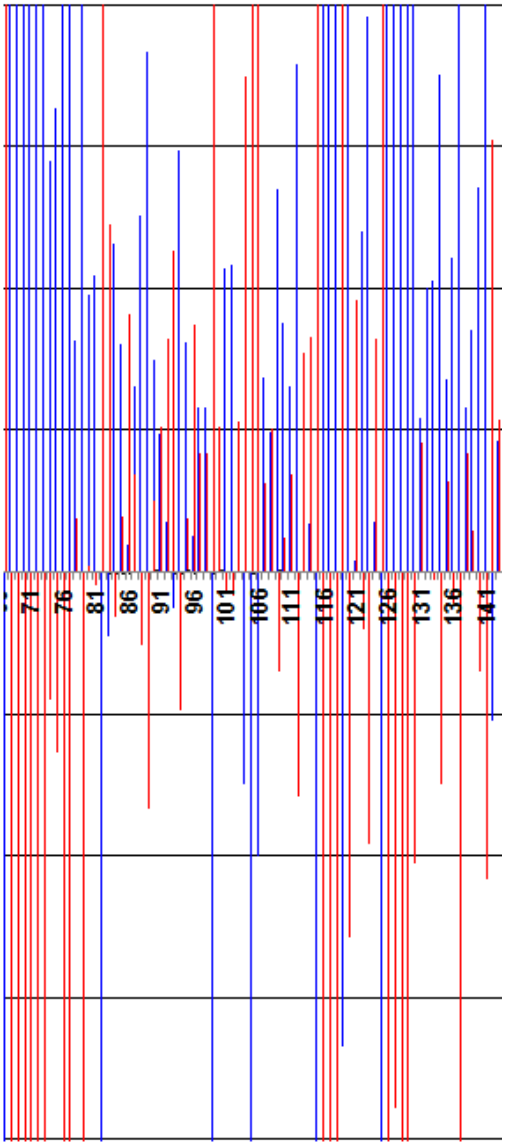


Figura 33: Teste de Sensibilidade - Três Estações – Parte B

A Parte C, ilustrada pela figura 34, mostra que aos 144 segundos, a estação C entra na rede com a taxa de transferência forçada a operar em 1 Mb/s. Nesse momento, pode-se observar o padrão que caracteriza a anomalia da MAC, pois, os valores das medições da estação C tendem a ser baixos e negativos nos momentos em que há variação em sua taxa de transferência. Observa-se o fato da sensibilidade da estação ofensora ser menor do que a sensibilidade das demais estações da rede, pois, uma vez que a estação ofensora tem sua taxa alterada para mais ou para menos, o reflexo disso na rede é oposto e consideravelmente maior do que a alteração propriamente dita nas outras estações.

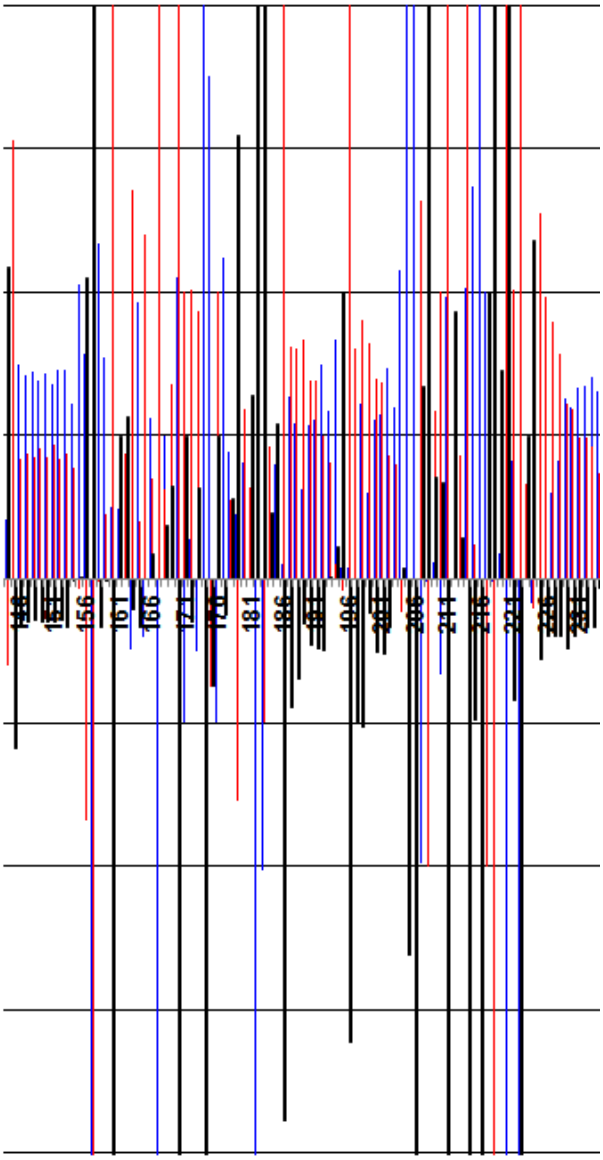


Figura 34: Teste de Sensibilidade - Três Estações – Parte C

Ao sair da rede, aos 233 segundos, a estação C deixa de causar a anomalia na rede e as estações A e B passam a compartilhar toda vazão total da rede conforme visto na figura 30. Finalmente, aos 314 segundos, a estação B sai da rede e a estação A fica com toda vazão da rede.

No próximo experimento, um cenário com três estações também foi usado para demonstrar os efeitos de uma estação que é ofensora ao entrar na rede, mas, num segundo momento, ela se torna uma estação normal, ou seja, ela para de causar a anomalia da MAC. Este experimento está ilustrado na figura 35.

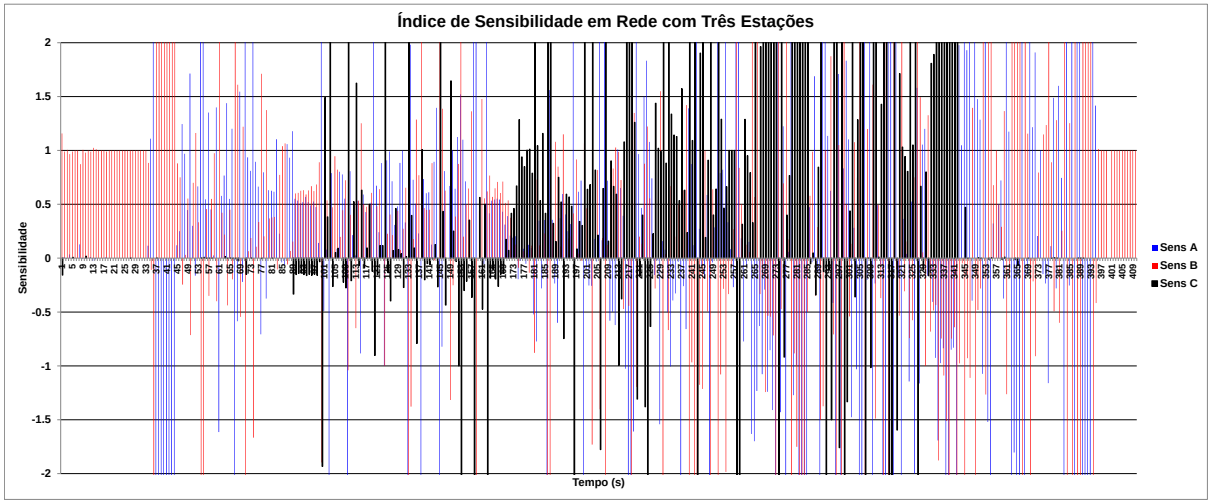


Figura 35: Teste de Sensibilidade - Três Estações com Taxa de 1 Mb/s

Inicialmente, uma única estação na rede ocupa toda a vazão total, isso equivale a dizer que qualquer sensibilidade observada depende de quanto a estação está usando a rede já que a vazão total da rede e a taxa da estação em questão são as mesmas.

Na figura 36, logo que se inicia uma transferência de dados pela rede aos 89 segundos do experimento, observa-se que a estação C instala a anomalia da MAC na rede.

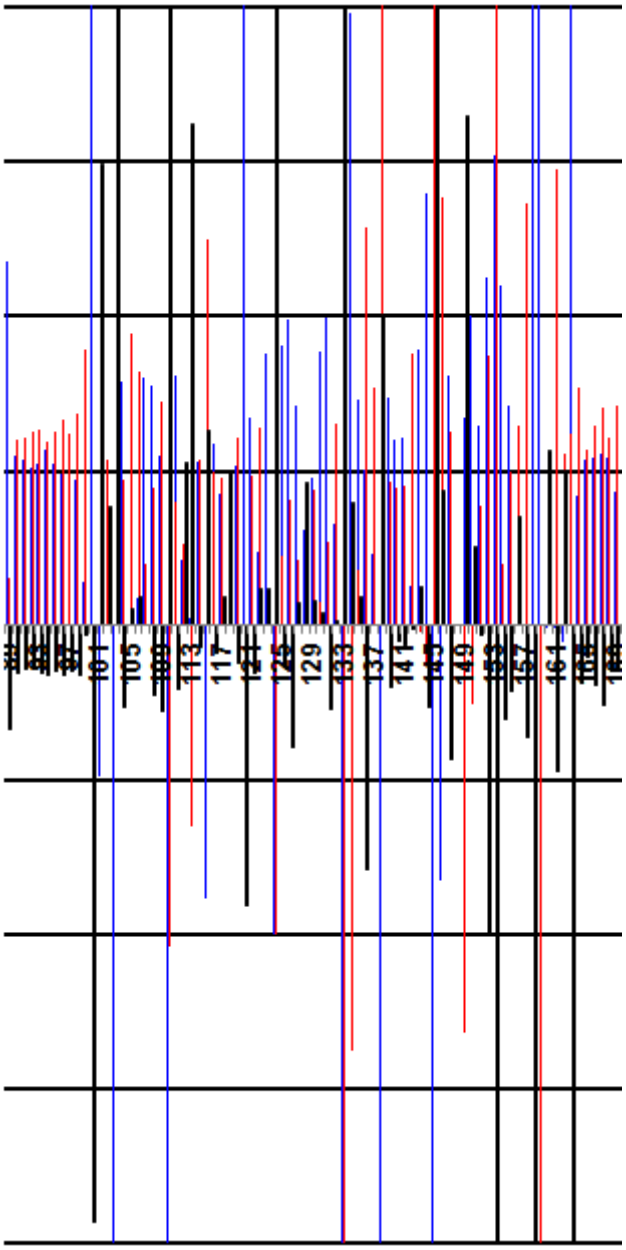


Figura 36: Teste de Sensibilidade - Três Estações - Taxa de 1 Mb/s – Parte A

Aos 169 segundos, a estação C deixa de ser a causadora da anomalia e o que se observa é que ela passa a compartilhar a vazão total da rede normalmente com as outras duas estações até os 345 segundos, como ilustrado pela figura 37.

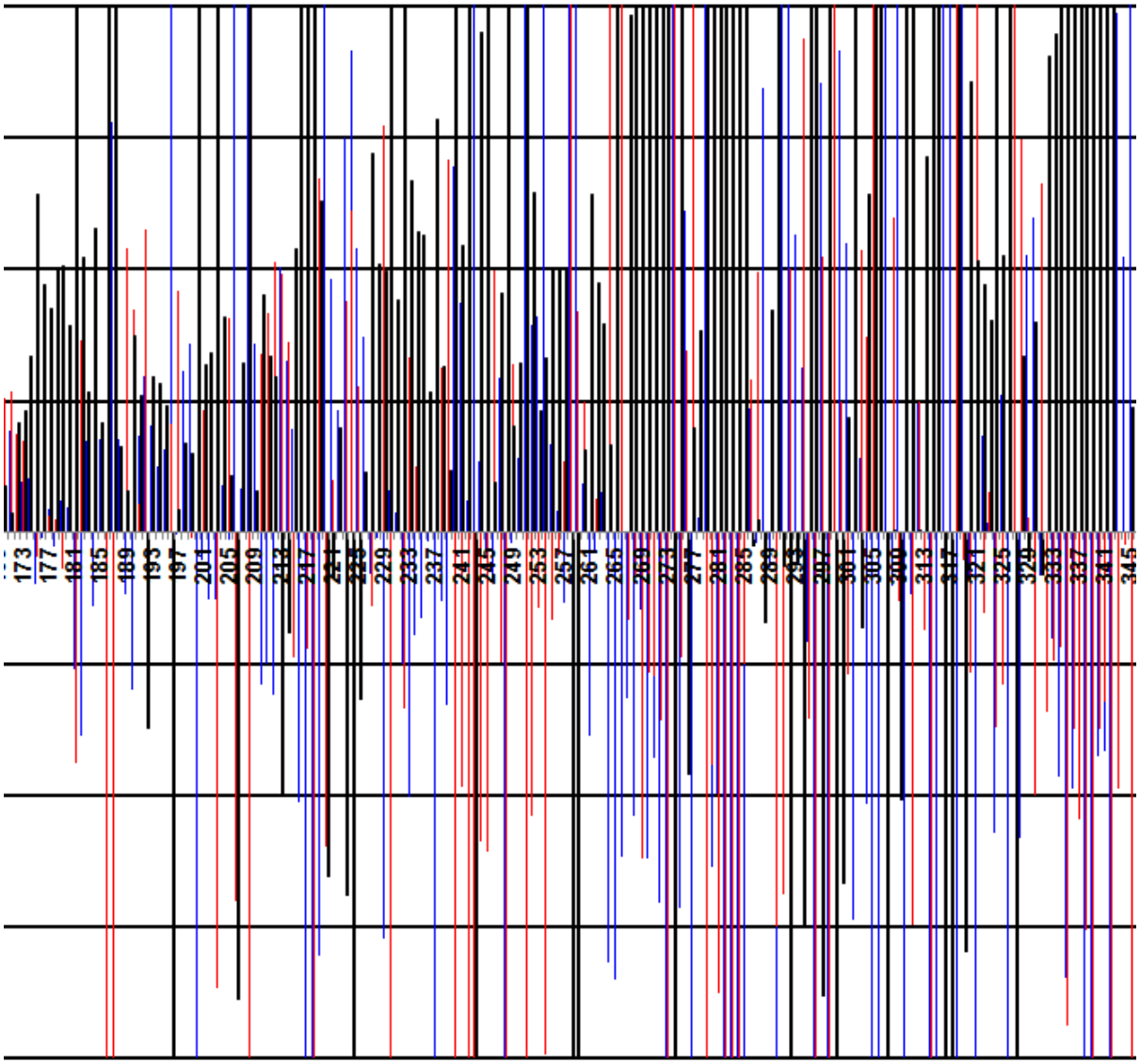


Figura 37: Teste de Sensibilidade - Três Estações - Taxa de 1 Mb/s – Parte B

Os experimentos mostraram que o comportamento da rede, a partir da perspectiva da sensibilidade, é diferente nos momentos em que a anomalia está instalada na rede e nos momentos em que as estações compartilham livremente a vazão total da rede sem a presença de ofensores. Os testes de sensibilidade foram reproduzidos com diferentes quantidades de estações (uma, duas e três estações), com diferentes taxas de transferências (1 Mb/s, 2 Mb/s, 5.5 Mb/s e 11 Mb/s) e com dois cenários combinados no mesmo experimento em que uma estação fez o papel de ofensora da rede e depois deixou de ser a causadora da anomalia da MAC.

6. CONCLUSÕES

Neste trabalho, foi investigado um fenômeno das redes sem fio IEEE 802.11 conhecido como Anomalia da MAC. A partir dos procedimentos adotados por este trabalho, a investigação acerca da anomalia na verdade foi uma busca por padrões que caracterizem o comportamento da rede no momento em que está ocorrendo a anomalia.

Neste sentido, verificou-se que a estação ofensora afeta negativamente a vazão total (*throughput*) da rede, o que caracteriza a presença de anomalia. Sob os efeitos da anomalia, as vazões das estações da rede ficaram semelhantes ocultando, porém, o dispositivo causador da anomalia da MAC.

Para comprovação dessas características, foi implementada uma bancada de testes que possibilita a reprodução de condições reais de anomalia em uma rede. A bancada é capaz de coletar informações da rede, bem como, instalar a anomalia por meio de uma estação ofensora com limitação de vazão ou potência de recepção. Basicamente, a bancada é composta por um ponto de acesso sem fio, estações e ferramenta de geração artificial de tráfego de dados.

A partir da experimentação nessa bancada, com redes com duas e três estações, verificou-se que em condições de anomalia, a variação da vazão da estação ofensora é, em geral inversa à variação da rede. Mais ainda, pequenas alterações na vazão da estação causadora da anomalia, provocam uma resposta significativamente maior na resposta. Essas características não foram observadas como comportamento geral das estações não ofensoras.

Desta maneira, tornou-se possível diferenciar a estação ofensora das demais a partir da observação do seu comportamento na rede. Esse comportamento pode ser caracterizado por um índice de sensibilidade, através do qual as estações que apresentam esse índice negativo e de dimensão reduzida são as prováveis ofensoras.

Futuros desenvolvimentos deste trabalho incluem:

- A repetição dos experimentos para outras tecnologias de rede sem fio, tais como: IEEE 802.11a, IEEE 802.11g e IEEE 802.11n.
- Utilizar um número maior de estações na rede para observar seu comportamento.
- Observar o comportamento da rede sob o efeito da anomalia criada por múltiplos ofensores.
- Considerar a possibilidade de incluir a capacidade de mitigação da anomalia da MAC na bancada de testes.

REFERÊNCIAS

BRANQUINHO, O. C.; REGGIANI, N.; FERREIRA, D. M.. Mitigating 802.11 Mac Anomaly Using SNR to Control Backoff Contention Window. In: IEEE Computer Society, v. 4, p. 55-61, 2006.

FERREIRA, D. M. Minimização do efeito da anomalia em redes IEEE 802.11 usando SNR para controlar o CW. Dissertação para obtenção do grau de mestre na UNICAMP, Campinas, 2007.

GARTNER. Acesso em 11/10/13, disponível em: http://www.gartner.com/newsroom/id/2227215.

GUIRARDELLO, M. Política de QoS com Priorização de Acesso ao Meio para Redes IEEE 802.11. 2008. 104f. Dissertação para obtenção do grau de mestre na Pontifícia Universidade Católica de Campinas, Campinas, 2008.

HEUSSE, M and ROUSSEAU, F; BERGER-SABBATEL, G; DUDA, A. Performance Anomaly of 802.11b, IEEE INFOCOM 2003.

IEEE STD 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (Phy) Specifications. ANSI/IEEE STD 802.11, Information Technology, 1999 Edition.

IEEE - SA (IEEE - *Standards Association*). Acesso em 15/10/2013, disponível em: http://www.ieee802.org/11/Reports/802.11_Timelines.htm.

INFORMÁTICA UOL. Acesso em 22/10/2013, disponível em: http://informatica.hsw.uol.com.br/memoria-flash.htm.

KIM, Hyogon, YUN, Sangki, KANG, Inheye, BAHK, Saewoong. Resolving 802.11 Performance Anomalies trough QoS Differentiation. IEEE Communications Letters, vol. 9, No. 7, July 2005.

MENDES, L.S.; BOTTOLI, M.L.; BREDA, G.D.; (2009). "Digital cities and open MANs: A new communications paradigm," Communications, 2009. LATI (COM '09. IEEE Latin-American Conference on, vol., no., pp.1-8.

PENDRIVELINUX (*Universal* USB *Installer*). Acesso em 03/04/2013, disponível em: www.pendrivelinux.com

RNP (Rede Nacional de Ensino e Pesquisa). Acesso em 11/10/2013, disponível em: http://www.rnp.br/newsgen/9805/wireless.html.

STD - IEEE (Standards - IEEE). Acesso em 15/10/2013, disponível em: http://standards.ieee.org/getieee802/download/802.11-2012.pdf.

UBUNTU. Acesso em 22/09/2013, disponível em: www.ubuntu.com/download/desktop

WI-FI Alliance (Wireless Fidelity Alliance). Acesso em 16/10/2013, disponível em: http://www.wi-fi.org/discover-and-learn

APÊNDICE

Apêndice 1: Artigo submetido e aprovado para exposição nas sessões técnicas orais do VII Workshop de Pós-Graduação e Pesquisa do Centro Paula Souza em São Paulo, no período de 17 a 18 de outubro de 2012.

Bancada de Testes para Controle de Vazão em Redes Wi-Fi

BANCADA DE TESTES PARA CONTROLE DE VAZÃO EM REDES WI-FI

ARTURO JOSÉ FENILE PERIS
Pontifícia Universidade Católica de Campinas – São Paulo – Brasil
aperis@gmail.com
CLAUREM PAULUS CEOLIN MARQUES
Pontifícia Universidade Católica de Campinas – São Paulo – Brasil
clauremmarques@yahoo.com.br
ALEXANDRE DE ASSIS MOTA
Pontifícia Universidade Católica de Campinas – São Paulo – Brasil
amota@puc-campinas.edu.br
LIA TOLEDO MOREIRA MOTA
Pontifícia Universidade Católica de Campinas – São Paulo – Brasil
lia.mota@puc-campinas.edu.br

Resumo – O presente trabalho descreve uma bancada de testes que mostra como é possível controlar a vazão em redes Wi-Fi para mitigar os efeitos de um problema conhecido como “Anomalia da MAC”, controlando a taxa de transferência dos dispositivos que têm más condições de propagação do sinal. Esse problema, basicamente, consiste em usuários com boas condições de transmissão que podem ser prejudicados por outros que estão transmitindo em alta potência devido às más condições em que se encontram do ponto de vista do enlace de dados até o AP (Access Point).

Abstract – The present work describes a workbench test that shows how it is possible to control IEEE802.11 networks throughput in order to mitigate the effects of a problem in Wi-Fi network known as “MAC Anomaly” by controlling the devices transfer rate which has bad signal propagation conditions. This problem, basically, consists in users with good transmission conditions to be affected by other users that are transmitting

with a high potency due to bad conditions from the data link perspective to the AP (Access Point).
Palavras-chave: IEEE 802.11, Wi-Fi, Bandwidth Management.

Introdução

A popularidade das redes Wi-Fi faz com que elas sejam encontradas muito facilmente nos mais diversos ambientes, como por exemplo: restaurantes, hotéis, aeroportos, empresas, escolas e universidades. Esse cenário difuso que as rede Wi-Fi se encontram hoje, tornam o controle dos usuários uma tarefa muito difícil.

Analisando os usuários dessas redes, pode-se perceber que eles apresentam os mais diferentes perfis de navegação. A rede é acessada para leitura de e-mails, pesquisas, acesso à redes sociais, mensagens instantâneas, downloads, videos, entre outros. A cada dia aumenta o número de dispositivos com capacidades para se comunicar através das redes Wi-Fi, entre esses dispositivos estão os numerosos celulares e os tablets.

Esse trabalho propõe uma bancada de testes que permite o controle de vazão nessas redes, para que os efeitos da anomalia da MAC sejam estudados para que possam ser combatidos.

Metodologia

Para realizar o controle de vazão propriamente dito, foi construída uma bancada de testes fundamentada naquela proposta em (PERIS et al., 2010); na presente proposta, porém, os papeis de NAS e “Captive Portal” passaram a ser executados pelo software CoovaChilli. Esta bancada foi construída tendo em vista a utilização de equipamentos e soluções disponíveis comercialmente ou sem restrição de acesso. os equipamentos e configurações utilizados são mostrados na Figura 1.

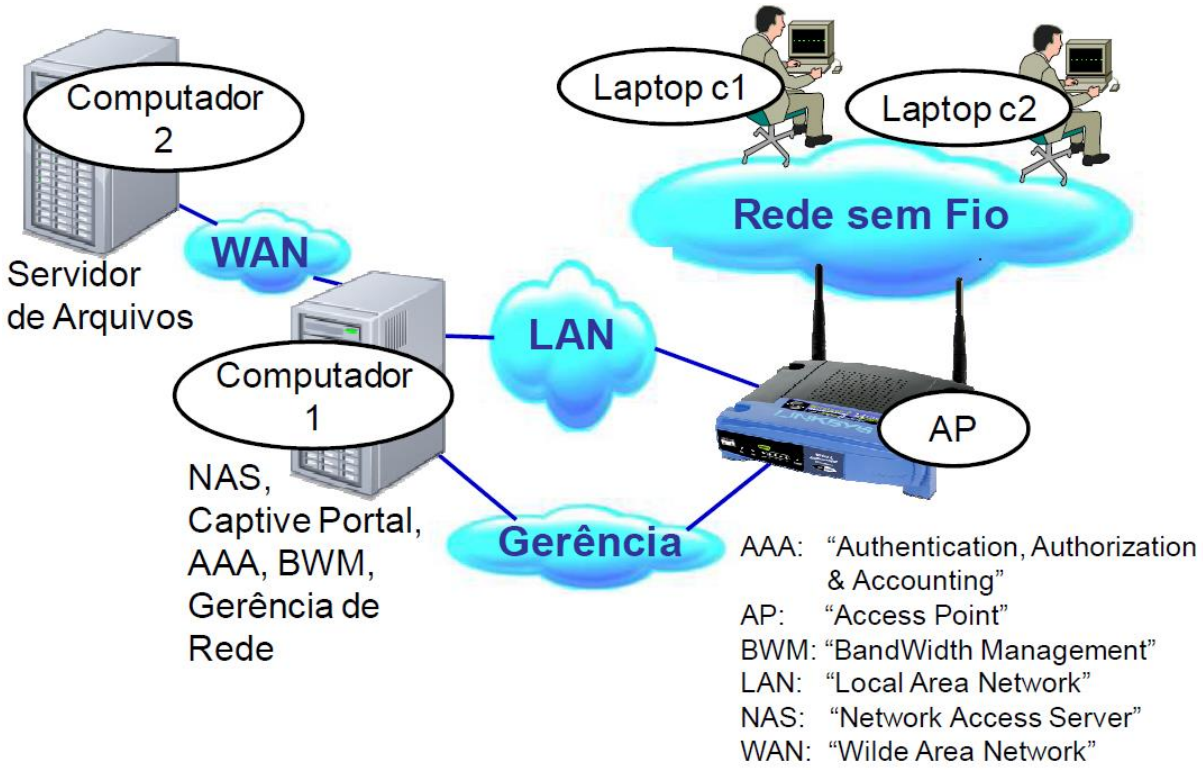


Figura 1 - Componentes da Bancada de Testes

Um único equipamento (computador 1), que concentrou as funções do núcleo NAS, "Captive Portal", AAA, BWM e Gerência de Rede.

Configuração do Computador 1:

- Computador Virtual suportado pelo software VMWare Player versão 3.1.5 (VMware, 2011) instalado num computador AMD Athlon XP, 1,5 GB RAM, HD 160GB (Sistema operacional Windows XP SP3).
  - o Linux Ubuntu-Server 11.11 (Ubuntu, 2011);
  - o 8950AAA (8950AAA, 2011);
  - oCoovaChilli (CoovaChilli, 2011);
  - oGrase (Grase, 2011).

Com isto, este computador desempenha as seguintes funções da arquitetura dos experimentos:

- NAS,
- Captive Portal,
- AAA,

- BWM,
- Gerência de Rede

Configuração do Computador 2:

- AMD Athlon XP, 1.0 GB RAM, HD 160GB.
  - o Windows XP SP3.
  - oOpenSSH (Incluindo SFTP e SCP)

Este computador desempenha as seguintes funções da arquitetura dos experimentos:

- Servidor de arquivos.

Os arquivos utilizados foram de tamanhos diversos, variando de 50 Kbytes a 2 Gbytes.

Configuração do Laptop c1:

A configuração do Laptop c1 é:

- Lenovo ThinkPad T60
  - o Windows XP
  - o Software WinSCP (WinSCP, 2012)
  - o Cópia de arquivos em rede suportada pelo WinSCP.

Configuração do Laptop c2:

A configuração do Laptop c2 é:

- Asus EeeePc AMD Vision 51
  - o Windows 7 SE
  - o Software WinSCP (WinSCP, 2012)
  - o Cópia de arquivos em rede suportada pelo WinSCP.

Configuração do AP:

- Linksys wrt54G com o firmware DD-WRT (DD-WRT, 2011).
- Modo bridge: Todas as funções típicas de roteador desempenhadas por esse tipo de equipamento foram eliminadas.
- Conexão via Telnet habilitada: Este tipo de conexão foi utilizado para a coleta de informações de RSSI das conexões ativas.

Conexões físicas entre os componentes:

- Laptops c1 e c2 <--> AP: IEEE 802.11 (Wi-Fi)
- Computador 1 <--> AP: cabo FastEthernet.
- Computador 2 <--> AP: cabo FastEthernet.
- Computador 1 <--> Computador 2: Interface virtual VMWare.

Estas conexões podem ser vistas na Figura 2.

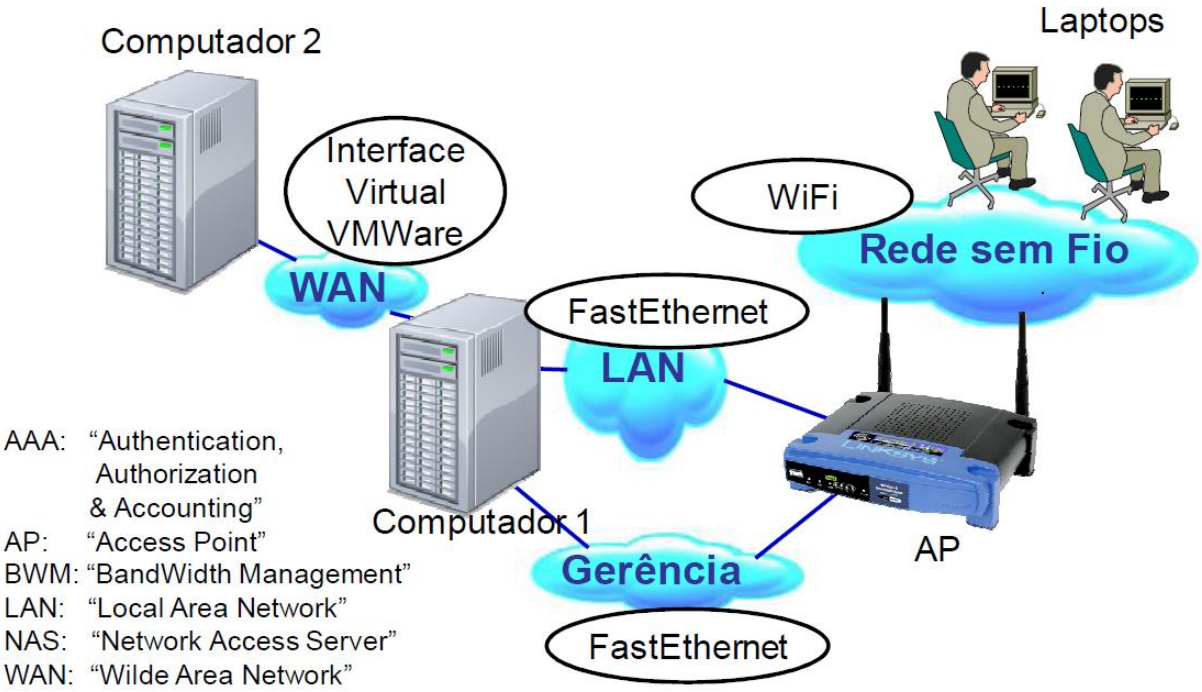


Figura 2 - Conexões físicas entre os componentes

Procedimento de Validação

O procedimento de validação teve como objetivo verificar se a bancada de testes descrita estava em condições normais de operação, se as conexões estavam operacionais e se a coleta de dados ocorria de forma consistente.

Este procedimento consistiu em executar o controle de vazão do Laptop c1, utilizando o seguinte ambiente:

- O BWM faz o controle da largura de banda disponível para o Laptop c1.
- Somente o Laptop c1 gera tráfego
- O Laptop c1 gera tráfego suficiente para ocupar toda a vazão permitida pelo NAS.
- As informações de tráfego do Laptop c1 são coletadas.

O resultado esperado para o procedimento de validação era um arquivo CSV com as informações do tráfego transmitido e recebido pelo Laptop c1.

Resultados Obtidos

Em todo o procedimento, os 2 laptops conectaram-se ao AP via sinal Wi-Fi e conectaram-se ao CoovaChili via Web-Browser. O Laptop c1 sempre utilizou o usuário “teste” e o Laptop c2 sempre utilizou o usuário “teste2”. Além disso, o Laptop c1 sempre ficou próximo ao AP, enquanto o Laptop c2 sempre ficou distante e em locais desfavoráveis para a propagação de sinal RF. A cada 5 minutos, o AAA reduziu a vazão permitida para o Laptop c2 em 10% de seu valor.

A Figura 3 apresenta a tela de login do Grase/CoovaChilli e a Figura 4 mostra a confirmação da conexão do usuário. Os resultados decorrentes do procedimento de validação foram coletados e utilizados para gerar um gráfico, comparando o tráfego de download com o RSSI de uplink. Esse gráfico gerado pode ser visto na Figura 5.

Figura 3 - Tela de login do Grase/CoovaChilli

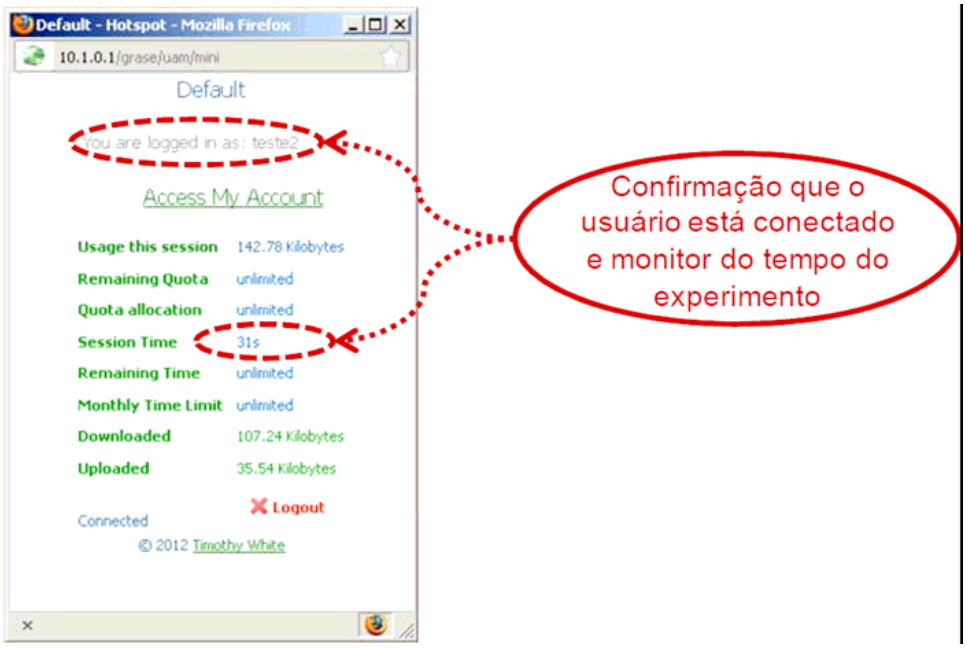


Figura 4 – Confirmação de conexão no Grase/CoovaChilli

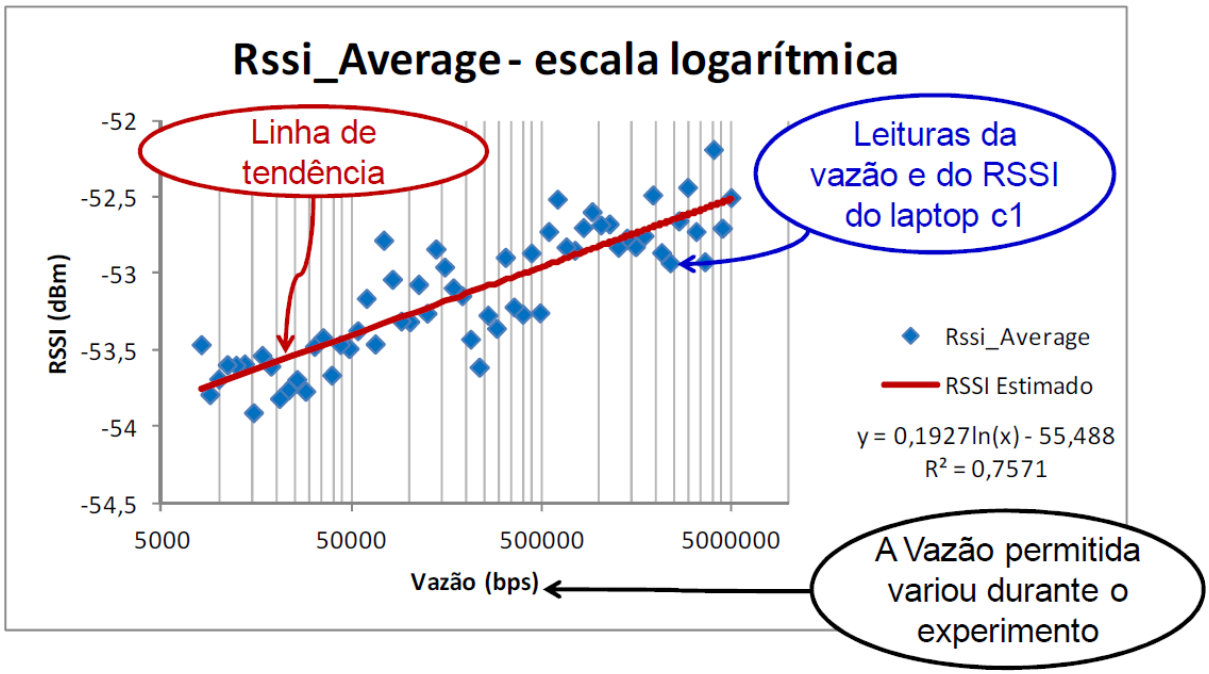


Figura 5 - RSSI x Vazão no procedimento de validação

Esse resultado confirma que a bancada estabelece as conexões dos usuários com a internet e coleta/consolida os dados (do NAS e do AP) corretamente. Além disso, o resultado confirmou que a limitação da vazão dos usuários ocorre como esperado.

Conclusões

O procedimento de validação comprovou que a bancada de testes funcionou dentro do esperado. Isso significa que:

- O tráfego que o Laptop c1 gerou foi corretamente coletado
- O RSSI do uplink foi corretamente medido
- O BWM comandou corretamente a restrição de tráfego do Laptop c1
- O NAS restringiu o tráfego da sessão do usuário de acordo com o comandado pelo BWM
- O “Captive Portal” registrou a sessão do usuário junto ao AAA corretamente. Além disso, as mensagens de “accounting” foram corretamente enviadas para o AAA.

Referências

8950AAA. Documentação On-line do 8950AAA, http://www.8950aaa.com, acessado em 17/6/2011.

COOVACHILLI. CoovaChilli Project, http://coova.org/CoovaChilli acessado em 17/6/2011.

DD-WRT. Documentação On-line do DD-WRT, http://www.dd-wrt.com/wiki, acessado em 17/6/2011.

FREERADIUS. The FreeRADIUS Project, http://freeradius.org/, acesso em 20/4/2012

GRASE. GRASE Hotspot, http://grasehotspot.org/, acessado em 28/07/2011

HEUSSE, M.; ROUSSEAU, F.; BERGER-SABBATEL, G.; DUDA, A..Performance Anomaly of 802.11b.IEEE INFOCOM 2003, 2003.

MOTA, L.; MOTA, A.; FONTOLAN, L. F.. Quality of Sercice Policy for IEEE802.11 networks with service rate selection based on fairness index. 2011. JOURNAL OF COMPUTER SCIENCES, VOL. 7, p600 - 604, 2011

PERIS, A. J. F.; CYRIACO, F. S.; BIAZOTTO, L. H.; BRANQUINHO, O. C.; MOTA, A. A.; MOTA, L. T. M.. Projeto De Bancada De Testes Para Estudos Em Transmissões Wi-Fi. 2010. 40th IGIP - International Symposium on Engineering Education, 2010.

ROSHAN, P.; LEARY, J.. 802.11 Wireless LAN Fundamentals, Cisco Press, ISBN: 1-58705-077-3, 2003.

Contato

Claurem Marques e Arturo Peris são mestrandos na PUC-Campinas, no curso de Gestão de Redes de Telecomunicações.

Alexandre Mota e Lia Mota são docentes permanentes do Programa de Pós-graduação em Engenharia Elétrica da PUC-Campinas.

Apêndice 2: Artigo submetido e aprovado para exposição nas sessões técnicas do XXXI SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES – SBrT2013 - no período de 1 a 4 DE SETEMBRO DE 2013, FORTALEZA, CE.

Identificação de Ofensores em Redes IEEE 802.11 Utilizando Lógica Nebulosa

Identificação de Ofensores em Redes IEEE 802.11 Utilizando Lógica Nebulosa

Claurem P. C. Marques, Ana R. C. Siqueira, Deivis F. Pirani, Thalis Avansi, Marcelo L. F. Abbade, Alexandre A. Mota e Lia T. M. Mota

***Resumo* — Este artigo apresenta um método para identificar ofensores - dispositivos causadores da anomalia da MAC - em redes IEEE 802.11, utilizando lógica nebulosa. Para viabilizar tal identificação, foi especificada uma bancada de testes que permite a coleta das informações necessárias para determinar a potência recebida nas estações e a taxa de transferência efetiva dos dispositivos conectados a uma rede. Utilizando uma síntese dessas informações coletadas, um sistema nebuloso baseado em regras associa um potencial ofensivo para todos dispositivos conectados à rede, permitindo assim identificar o provável ofensor.**

Palavras-Chave* — *Anomalia da MAC, IEEE 802.11, Lógica Nebulosa, Bancada de Testes.

***Abstract* — This paper presents a method to identify devices causing the MAC anomaly in IEEE 802.11 networks using fuzzy logic. To do so, a test bench with specific hardware and software configuration was implemented, that allows gathering of information needed to determine transmission power and throughput of network stations. With these data, a fuzzy system was developed to determine an offensive potential for all network devices, permitting to identify the probable offending device.**

Keywords* — *MAC Anomaly, IEEE 802.11, Fuzzy Logic, test workbench.

I - INTRODUÇÃO

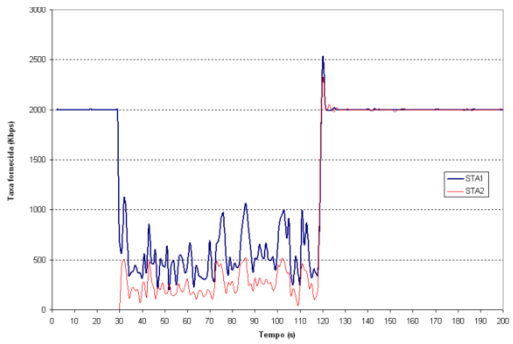
Atualmente, as redes sem fio padrão IEEE 802.11 proporcionam ampla conectividade e mobilidade a uma vasta quantidade de dispositivos de uso cotidiano, tais como: smartphones, tablets, televisores, video games, laptops, palm-tops e estações de trabalho convencionais. Para uma determinada rede sem fio, o crescente aumento do número desses dispositivos causa um aumento da competição pelo acesso ao meio; essa disputa para se utilizar o meio físico acaba por afetar o desempenho da rede.

O padrão para redes locais sem fio IEEE 802.11b foi inicialmente descrito em 1997 [1]. Esse padrão suporta taxas de transferência de 11 Mb/s, 5.5 Mb/s, 2 Mb/s e 1 Mb/s, de acordo com a negociação entre o ponto de acesso e a estação conectada à rede. Desde seu surgimento, o padrão passou por diversas revisões [2] com o intuito de melhorá-lo. O propósito da maioria das revisões era alcançar a melhoria do desempenho, mas algumas tinham o propósito de melhorias para segurança [3] e qualidade de serviço [4].

Por meio do método DCF (Distributed Coordination Function) que usa o algorítmo CSMA/CA, a camada MAC do padrão IEEE 802.11 prevê condições de igualdade de acesso ao meio físico por parte de todos dispositivos presentes na rede. Isso faz com que todas as estações tenham a mesma probabilidade de efetivamente acessar o meio, não importando a diferença entre suas condições da conectividade da camada física, nem de taxa de transferência. Como mencionado, a taxa de transferência é determinada mediante negociação entre o ponto de acesso sem fio e o dispositivo admitido na rede e se basea nas condições de propagação do sinal, ou seja, na relação sinal/ruído (*signal-to-noise ratio*, SNR). Portanto, a determinação das condições da camada física é fundamental para a identificação dos dispositivos que estão submetidos a condições desfavoráveis de propagação do sinal, possibilitando a tomada de alguma ação do ponto de vista de gerência da rede, antes que estes dispositivos causem a anomalia da MAC [5] [6] [7].

A anomalia da MAC em redes com o padrão IEEE 802.11b foi demonstrada pela primeira vez em [6], quando se observou um desempenho consideravelmente degradado de algumas estações em relação a outras da rede. Essa anomalia faz com que uma estação em más condições provoque uma redução na taxa de transferência das demais estações, ao estabelecer comunicação efetiva com o ponto de acesso [7]. Para ilustrar este efeito, a Figura 1 mostra a taxa de transmissãode duas estações (STA1 e STA2) conectadas a um mesmo ponto de acesso (AP). Pode-se observar a significativa degradação que a transmissão da estação STA1, em boas condições de acesso, sofre a partir de 30 s, quando a estação STA2 (em condições desfavoráveis de transmissão) passa a acessar a rede.

Claurem Marques, Deivis Pirani, Ana Siqueira, Thalis Avansi, Marcelo Abbade, Alexandre Mota e Lia Mota¸ CEATEC, Pontifícia Universidade Católica de Campias, Campinas-SP, Brasil.
E-mails: claurem.pcm@puccampinas.edu.br, deivis.fp@puccampinas.edu.br, anarcsiqueira@gmail.com, thalisvz@hotmail.com, abbade@puc-campinas.edu.br, mota.profalexandre@gmail.com, lia.mota@puc-campinas.edu.br



Observação da Anomalia da MAC – Reproduzido em [7]

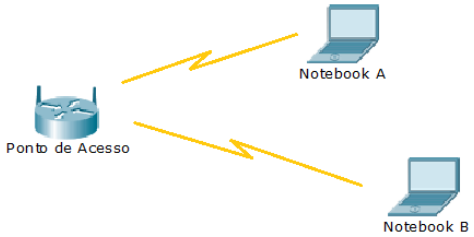
Assim, torna-se interessante controlar e/ou eliminar os efeitos desse fenômeno em redes sem fio. Em [5], foi proposto um modelo para mitigar a anomalia da MAC usando a relação sinal-ruído para controlar a janela de contenção backoff, o que exige implementações tanto em hardware quanto no firmware do ponto de acesso. Já em [8], a anomalia foi mitigada com

Essa identificação depende de diferentes fatores, uma vez que é determinada pelas condições de acesso da estação ofensora. A proposta desse trabalho é a utilização de lógica nebulosa para concatenar o efeito de diferentes variáveis da rede que são diretamente afetadas por essas condições de acesso, gerando assim uma métrica indireta do potencial de uma determinada estação da rede vir a se tornar uma estação ofensora. Em síntese, o sistema de regras nebulosas proposto visa determinar um índice numérico para cara estação conectada a um determinado ponto de acesso, de tal forma que quanto maior esse potencial de ofensividade, maior a chance da estação em questão ser um ofensor da rede. Assim, pode-se identificar o ofensor em qualquer instante, verificando-se aquela estação que tem o maior potencial ofensivo.

Este trabalho está organizado da seguinte forma. Na seção II é detalhada a bancada de testes; a seção III descreve o sistema nebuloso; a seção IV apresenta a discussão dos resultados e, por fim, é apresentada a conclusão do trabalho.

II - BANCADA DE TESTES

A bancada desenvolvida para os testes é composta basicamente por um dispositivo sem fio que atua como ponto de acesso (AP) e estações configuradas em computadores portáteis, devidamente equipados com placas que permitem o acesso à rede sem fio. A mobilidade das estações é importante para que seja possível a criação de diferentes condições de camada física. A topologia da rede básica com duas estações (notebooks A e B) está ilustrada na Fig. 2.



Topologia da rede básica da bancada de testes.

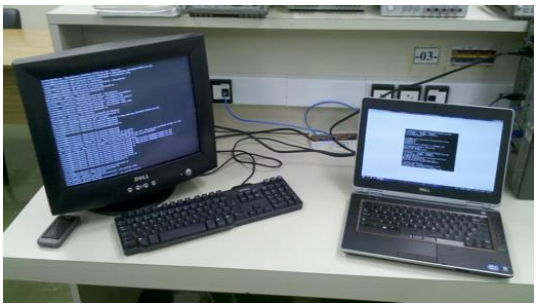
A - Configuração da Rede Básica

Na rede básica, configurada com duas estações, o notebook A tem uma placa de rede sem fio Intel com capacidades de conexão nos padrões IEEE 802.11 a, b, g e n. Possui um processador Intel I5, 4 GB de memória RAM e um disco rígido de 250 GB. O sistema operacional é o Linux Ubuntu Desktop.

O notebook B tem uma placa de rede sem fio IEEE 802.11a, b, g e n. Possui um processador Processador Intel Core I3, 4 GB de memória RAM e disco rígido de 500 GB. O sistema operacional desse notebook é o Linux Ubuntu Desktop.

O Ponto de Acesso Sem Fio possui uma placa de rede sem fio do fabricante Mikrotik Router Board RB14. Essa é uma placa PCI e está acoplada à placa-mãe de um computador Pentium 4 com processador de 1.5 GHz, 2 GB de memória RAM e 40 GB de disco rígido. A Fig. 3 ilustra os componentes da rede básica de testes em bancada.

Os dispositivos da bancada (ponto de acesso e estações) usam o mesmo sistema operacional, o Linux Ubuntu, escolhido por ser um software livre e por possuir robustez e flexibilidade necessárias para atender as necessidades dessa proposta. Para estabelecimento dos fluxos de dados foi utilizado o Jperf, uma versão Java do Iperf, com interface gráfica, ajustado para ser cliente nas estações com o servidor no ponto de acesso.



Equipamentos da Bancada de testes.

B - Emulação da Anomalia

A emulação da anomalia é fundamental para que se possa observar o comportamento da rede sem fio e analisar os efeitos decorrentes. É possível reproduzir a anomalia da MAC utilizando a bancada de testes proposta neste trabalho e observar em tempo real exatamente quando ela se instala. Para isso, as estações podem ser movidas para lugares distantes do ponto de acesso ou posicionadas atrás de obstáculos que atenuam o sinal. Com isso, ocorre alteração do sinal e conseqüente degradação na relação sinal-ruido das estações, o que significa que a qualidade do enlace na camada física se torna desfavorável e que, portanto, passam a acontecer erros com maior freqüência, fazendo com que mais pacotes de dados sejam perdidos. Configura-se assim um cenário apropriado para o surgimento da anomalia da MAC, como descrito em [6].

Na implementação realizada, as estações podem se conectar à rede assim que o ponto de acesso é ligado, pois o sistema fica ativo automaticamente. Nessa condição, os experimentos podem ser adequadamente criados para reproduzir, registrar e analisar a anomalia da MAC, permitindo que a proposta desse trabalho possa ser desenvolvida e validada. Alguns scripts na linguagem Bash Script foram desenvolvidos para automatizar a leitura das informações de camada física das estações da rede. Essas informações são usadas para se determinar a relação sinal-ruído e a taxa de transferência de cada dispositivo conectado à rede sem fio, que são entradas utilizadas no sistema nebuloso para determinar o potencial ofensivo das estações, como descrito a seguir.

III - SISTEMA NEBULOSO

A identificação do dispositivo responsável por causar a anomalia da MAC em uma rede é de difícil determinação, pois todas as estações ficam reduzidas a condições de tráfego degradadas e próximas. Visto que agilidade e precisão na hora de identificar o ofensor da rede são fundamentais para mitigar a anomalia, o sistema nebuloso pode ser agregado ao próprio ponto de acesso de forma que, à medida que as informações sobre a rede são coletadas e o sistema nebuloso começa a ser alimentado, uma lista com o potencial ofensivo dos dispositivos da rede vai sendo gerada em tempo real.

A avaliação do potencial ofensivo de uma estação é inicialmente feita de forma qualitativa, por meio de um processo de inferência, determinado por um conjunto de regras nebulosas. As variáveis nebulosas de entrada necessárias para essa inferência, descritas na Tabela I, também expressam níveis qualitativos das variáveis exatas (ou *crisp*) coletadas da rede pela bancada de testes, através de conjuntos nebulosos. Esses níveis qualitativos de entrada são determinados na etapa de Fuzzificação do sistema nebuloso [9]. Assim, a cada conjunto nebuloso da Tabela I é associado um grau de pertinência μ.

A. Fuzzificação

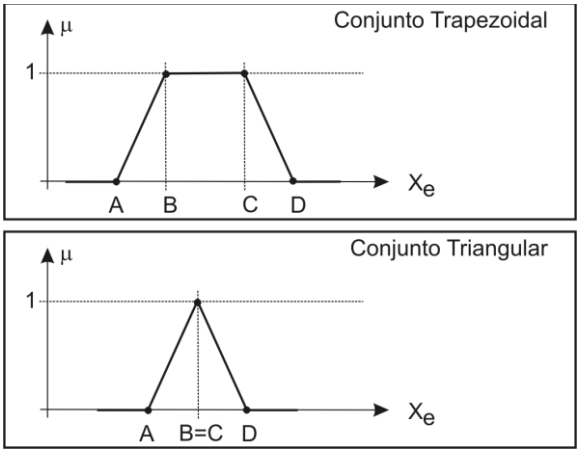
Cada conjunto nebuloso é definido por valores modais [A,B,C,D] conforme a Fig. 4. Considerando essa definição, para um valor medido *xe* de uma entrada *crisp*, o valor de pertinência associado ao seu conjunto nebuloso pode ser calculado como segue:

Se (xe < A) OU (xe >= D), μ=0;

Se (xe > A) E (xe < B), μ=((xe-A)/(B-A));

Se (xe >= B) E (xe <= C), μ=1;

Se (xe > C) & (xe < D), μ=((D-xe)/(D-C));



Tipos de conjuntos nebulosos e seus valores modais

B - Implicação Nebulosa

Com a finalidade de proporcionar processamento rápido do potencial ofensivo, neste trabalho foi empregado o seguinte formato para a construção das regras nebulosas:

SE (x É A) E/OU(y É B) ENTÃO (z É C)

na qual *x*, *y* e *z* são variáveis nebulosas e A, B e C são seus qualificativos, ou seja, seus conjuntos nebulosos associados conforme a Tabela I. A implicação nebulosa consiste em associar um valor de pertinência μ_C ao conjunto de saída C, a partir das pertinências μ_A e μ_B dos conjuntos de entrada A e B previamente determinadas na etapa de Fuzzificação, de forma que:

$$\mu_C = \text{mínimo}\{\mu_A, \mu_B\}$$

Se mais de uma regra nebulosa realiza implicação no conjunto C, o valor de μC deve ser assumido como o máximo entre os possíveis valores que seriam associados a partir de cada uma das regras.

As regras nebulosas identificadas nesse experimento estão no Apêndice I.

C - Defuzzificação

Esta etapa consiste na transformação do raciocínio nebuloso, até então trabalhado com as variáveis e valores lingüísticos, para valores numéricos simples ou crisp. Para tanto, torna-se necessária a unificação ou sobreposição dos conseqüentes implicados na etapa anterior, requerendo-se o uso de uma técnica de defuzzificação [9]. Neste trabalho, para valorizar a robustez e precisão do resultado, foi adotado o método do Centro de Gravidade ou Centróide (COG), que determina o valor exato do potencial ofensivo como o centro de gravidade da figura plana formada pela união de todas as distribuições de regras sobre a variável nebulosa de saída. Maiores detalhes sobre o cálculo do Centro de Gravidade podem ser encontrados em [9].

VARIÁVEIS NEBULOSAS

Variável Nebulosa	Escopo	Conjunto Nebuloso	Valores Modais	Pertinência Associada
Obsolescência da Estação (OE)	0 a 100 [%]	Alta	[50,80,100,100]	μ_{OA}
		Média	[20,50,50,80]	μ_{OM}
		Baixa	[0,0,20,50]	μ_{OB}
Potência do sinal recebido (PR)	0 a -100 [dBm]	Alta	[0,0,10,60]	μ_{PA}
		Média	[10,60,60,75]	μ_{PM}
		Baixa	[60,75,90,100]	μ_{PB}
Taxa Nominal negociada (TN)	0 a 11 [Mb/s]	Alta	[3,5,11,11]	μ_{TNA}
		Média	[1,3,3,5]	μ_{TNM}
		Baixa	[0,0,2,3]	μ_{TNB}
Taxa Efetiva praticada (TE)	0 a 100 [% de TN]	Alta	[50,70,100,100]	μ_{TEA}
		Média	[20,40,40,60]	μ_{TEM}
		Baixa	[0,0,20,30]	μ_{TEB}
Potencial ofensivo (PO)	0 a 100	Muito Alta	[60,70,90,100]	μ_{POMA}
		Alta	[50,60,60,70]	μ_{POA}
		Média	[40,50,50,60]	μ_{POM}
		Baixa	[30,40,40,50]	μ_{POB}
		Muito Baixa	[0,20,30,40]	μ_{POMB}

IV - RESULTADOS

A bancada de testes se traduz em um sistema capaz de fornecer, para cada estação na rede, a medição da potência do sinal recebido, da taxa nominal negociada entre o ponto de acesso e a estação, da taxa efetiva que a estação realmente está utilizando e a data e hora de cada leitura. Esses dados são armazenados em arquivos no formato ".csv". O sistema nebuloso que leva em consideração os dados coletados pela bancada de testes para identificar dispositivos com maior potencial ofensivo foi implementado usando o ambiente Scilab [10]. A rede básica descrita anteriormente, com um ponto de acesso e duas estações, foi utilizada para a coleta dos dados. A eficácia do sistema foi testada em três diferentes cenários, descritos a seguir.

A - Cenário sem presença da Anomalia

No primeiro cenário testado, as estações A e B foram deixadas livres para negociar suas taxas com o ponto de acesso. A Fig. 5 ilustra a evolução das taxas de transmissão praticadas pelas duas estações com o passar do tempo. Observa-se um compartilhamento da capacidade do canal enquanto a estação B está ativa, mas não houve caracterização da anomalia, pois a capacidade total de *throughput* da rede é mantida. A partir dos dados fornecidos para o sistema nebuloso, é possível determinar o potencial ofensivo para cada estação. A Tabela II ilustra as entradas e saída do sistema nebuloso nesse cenário, para as duas estações (A e B).

DADOS PARA O SISTEMA NEBULOSO

Variável	A	B
Obsolescência do equipamento	0.3	0.3
Potência do sinal recebido (dBm)	-41.73	-44.59
Taxa nominal negociada (Mb/s)	11	11
Taxa efetivamente praticada (%)	38,36	6,45
Potencial ofensivo	0.35	0.40

Da Tabela II, observa-se que o maior potencial ofensivo está associado à estação B, embora não esteja caracterizada a anomalia. Isso indica que, em caso de degradação da rede, é mais provável que a estação B se torne a ofensora.

B - Presença da Anomalia por restrição de taxa

No segundo cenário testado, a estação A foi deixada livre para negociar sua taxa com o ponto de acesso, enquanto a estação B foi configurada para ser a ofensora, operando em 1 Mb/s . A Fig.6 ilustra a evolução das taxas de transmissão praticadas pelas duas estações com o passar do tempo. Observa-se a caracterização da anomalia a partir da entrada da estação B na rede, com a degradação radical da transmissão da estação A, reduzindo bastante a capacidade total de *throughput* da rede. A Tabela III mostra as entradas e saída do sistema nebuloso no segundo cenário, para as duas estações (A e B).

DADOS PARA O SISTEMA NEBULOSO

Variável	A	B
Obsolescência do equipamento	0.3	0.3
Potência do sinal recebido (dBm)	-42.42	-43.72
Taxa nominal negociada (Mb/s)	11	11
Taxa efetivamente praticada (%)	42,81	2,66
Potencial ofensivo	0.35	0.37

Da Tabela III, observa-se que o maior potencial ofensivo está associado à estação B, indicando que o sistema nebuloso foi capaz de identificar corretamente o ofensor.

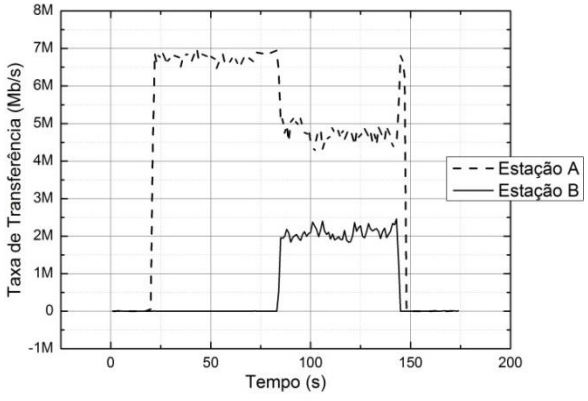
C - Presença da Anomalia por restrição de potência

No terceiro cenário testado, as estações A e B foram deixadas livres para negociar suas taxas com o ponto de acesso. No entanto, a estação B foi configurada para ser a ofensora, sendo posicionada de forma a fazer com que a potência média percebida no ponto de acesso seja de -86dBm. A Fig.7 ilustra a evolução das taxas de transmissão praticadas pelas duas estações com o passar do tempo. Como anteriormente, observa-se a anomalia com a entrada da estação B na rede, pois, embora não caracterizada durante todo o tempo, em alguns pontos há inequívoca degradação radical da transmissão da estação A e do *throughput* total da rede.

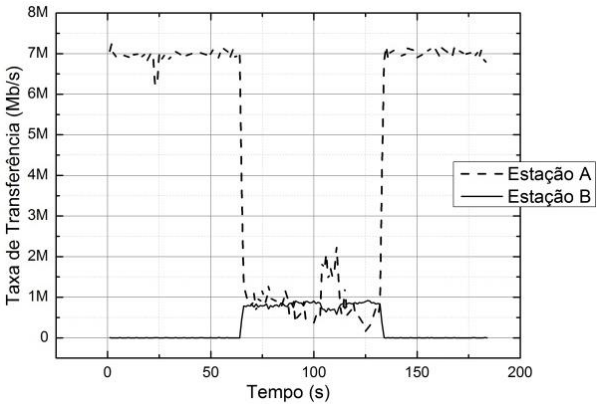
A Tabela IV mostra as entradas e saída do sistema nebuloso no segundo cenário, para as duas estações (A e B). Dessa Tabela, observa-se que o maior potencial ofensivo está associado à estação B, indicando que o sistema nebuloso também foi capaz de identificar corretamente o ofensor para o caso de potência degradada.

DADOS PARA O SISTEMA NEBULOSO

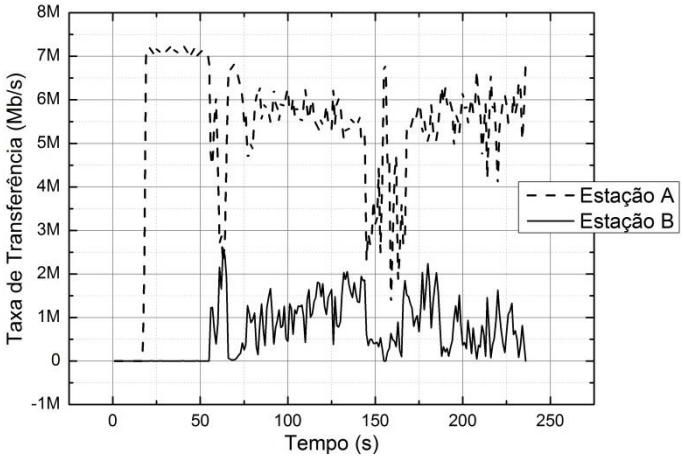
Variável	A	B
Obsolescência do equipamento	0.3	0.3
Potência do sinal recebido (dBm)	-57.72	-86.51
Taxa nominal negociada (Mb/s)	11	11
Taxa efetivamente praticada (%)	47,36	6,36
Potencial ofensivo	0.41	0.65



Taxas no Primeiro cenário - Rede sem anomalia.



Segundo cenário – Ofensor operando com taxa degradada.



Terceiro cenário – Ofensor operando com baixa potência

V - CONCLUSÕES

Com a vasta quantidade de dispositivos tecnológicos com capacidade de comunicação em redes locais sem fio *Wi-Fi* sendo desenvolvidos na atualidade, torna-se importante considerar o problema da anomalia da MAC inerente às redes IEEE 802.11. A caracterização da anomalia faz com que recursos sejam sub-utilizados tornando a tecnologia ineficiente quanto ao desempenho técnico, econômico e energético.

Ao emular a anomalia com a bancada de testes proposta neste trabalho, foi possível coletar e armazenar as informações sobre estações em uma rede sem fio, além de criar e executar cenários com o propósito de validar o sistema nebuloso.

O sistema nebuloso proposto foi capaz de identificar o ofensor em condições de degradação de taxa e de potência da estação ofensora. A escolha de um sistema nebuloso para determinar o potencial ofensivo das estações através de da concatenação das variáveis coletadas na bancada de testes permite que a identificação do ofensor possa ser feita de maneira mais rápida do que se todas as possibilidades e configurações da rede tivessem que ser analisadas para tal identificação. Nesse sentido, favorece-se que ações de controle possam ser tomadas mais rapidamente pela gerência da rede.

Finalmente, o console do sistema operacional Linux Ubuntu também oferece ao ponto de acesso grande flexibilidade e agilidade, pois a partir dele é possível fazer qualquer verificação ou configuração do sistema em tempo real. Isso é importante para minimizar o tempo que a anomalia afeta a rede ou mesmo que ela se instale, e dessa forma também se evita desperdício de recursos da rede e se viabiliza que os usuários tenham taxas de dados que permitam um nível aceitável de qualidade de serviço e experiência.

AGRADECIMENTOS

À PUC-Campinas pelo financiamento da pesquisa e ao CNpQ pelo apoio e bolsas.

REFERÊNCIAS

[1] Institute of Electrical and Electronics Engineering, 1997. 802.11- 1997 IEEE Standard for Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, DOI=http://dx.doi.org/10.1109/IEEESTD.1997.85951

[2] IEEE. http://standards.ieee.org/about/get/802/802.11.html, Acessado em 2013-05-10.

[3] Institute of Electrical and Electronics Engineering, 2004. IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements. IEEE Standards. 2004-07-23.

IEEE Std 802.11e-2005. IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements – Nov, 2005.

Branquinho, O. C.; Reggiani, N.; Ferreira, D. M.. Mitigating 802.11 Mac Anomaly Using SNR to Control Backoff Contention Window. In: IEEE Computer Society, v. 4, p. 55-61, 2006.

Heusse, Martin and Rousseau, Franck; Berger-Sabbatel, Gilles; Duda, Andrzej. Performance Anomaly of 802.11b, IEEE INFOCOM 2003.

Guirardello, M.. Política de QoS com Priorização de Acesso ao Meio para Redes IEEE 802.11. 2008. 104f. Dissertação para obtenção do grau de mestre na Pontifícia Universidade Católica de Campinas, Campinas, 2008.

Peris, A. J. F. Controle de vazão em redes IEEE 802.11 com presença de ofensores. 2012. 126P. Dissertação para obtenção do grau de mestre na Pontifícia Universidade Católica de Campinas, Campinas, 2012.

Shaw Ian S. Simoes Marcelo Godoy. Controle e modelagem Fuzzy. 2005. 2° Edição. Editora Edgard Blücher.

Scilab. Open Software for Numerical Computation. 2013. http://www.scilab.org/, Acessado em 2013-05-10.

APÊNDICE I

Síntese das Regras Nebulosas:

SE ObsolecEqpto É Alta E PotSinalReceb É Alta ENTÃO Ofensividade É Média

SE ObsolecEqpto É Alta E PotSinalReceb É Media ENTÃO Ofensividade É Alta

SE ObsolecEqpto É Alta E PotSinalReceb É Baixa ENTÃO Ofensividade É Muito Alta

SE ObsolecEqpto É Media E PotSinalReceb É Alta ENTÃO Ofensividade É Alta

SE ObsolecEqpto É Media E PotSinalReceb É Media ENTÃO Ofensividade É Média

SE ObsolecEqpto É Media E PotSinalReceb É Baixa ENTÃO Ofensividade É Baixa

SE ObsolecEqpto É Baixa E PotSinalReceb É Alta ENTÃO Ofensividade É Muito Baixa

SE ObsolecEqpto É Baixa E PotSinalReceb É Media ENTÃO Ofensividade É Baixa

SE ObsolecEqpto É Baixa E PotSinalReceb É Baixa ENTÃO Ofensividade É Médio

SE ObsolecEqpto É Alta E TaxaEfetiva É Alta ENTÃO Ofensividade É Muito Alta

SE ObsolecEqpto É Alta E TaxaEfetiva É Media ENTÃO Ofensividade É Alta

SE ObsolecEqpto É Alta E TaxaEfetiva É Baixa ENTÃO Ofensividade É Média

SE ObsolecEqpto É Media E TaxaEfetiva É Alta ENTÃO Ofensividade É Alta

SE ObsolecEqpto É Media E TaxaEfetiva É Media ENTÃO Ofensividade É Alta

SE ObsolecEqpto É Media E TaxaEfetiva É Baixa ENTÃO Ofensividade É Média

SE ObsolecEqpto É Baixa E TaxaEfetiva É Alta ENTÃO Ofensividade É Média

SE ObsolecEqpto É Baixa E TaxaEfetiva É Media ENTÃO Ofensividade É Baixa

SE ObsolecEqpto É Baixa E TaxaEfetiva É Baixa ENTÃO Ofensividade É Muito Baixa

SE PotSinalReceb É Alta E TxNominalNeg É Alta ENTÃO Ofensividade É Baixa

SE PotSinalReceb É Alta E TxNominalNeg É Media ENTÃO Ofensividade É Baixa

SE PotSinalReceb É Alta E TxNominalNeg É Baixa ENTÃO Ofensividade É Média

SE PotSinalReceb É Media E TxNominalNeg É Alta ENTÃO Ofensividade É Baixa

SE PotSinalReceb É Media E TxNominalNeg É Media ENTÃO Ofensividade É Média

SE PotSinalReceb É Media E TxNominalNeg É Baixa ENTÃO Ofensividade É Alta

SE PotSinalReceb É Baixa E TxNominalNeg É Alta ENTÃO Ofensividade É Média

SE PotSinalReceb É Baixa E TxNominalNeg É Media ENTÃO Ofensividade É Alta

SE PotSinalReceb É Baixa E TxNominalNeg É Baixa ENTÃO Ofensividade É Muito Alta

SE PotSinalReceb É Alta E TaxaEfetiva É Alta ENTÃO Ofensividade É Média

SE PotSinalReceb É Alta E TaxaEfetiva É Media ENTÃO Ofensividade É Baixa

SE PotSinalReceb É Alta E TaxaEfetiva É Baixa ENTÃO Ofensividade É Muito Baixa

SE PotSinalReceb É Media E TaxaEfetiva É Alta ENTÃO Ofensividade É Alta

SE PotSinalReceb É Media E TaxaEfetiva É Media ENTÃO Ofensividade É Média

SE PotSinalReceb É Media E TaxaEfetiva É Baixa ENTÃO Ofensividade É Baixa

SE PotSinalReceb É Baixa E TaxaEfetiva É Alta ENTÃO Ofensividade É Muito Alta

SE PotSinalReceb É Baixa E TaxaEfetiva É Media ENTÃO Ofensividade É Alta

SE PotSinalReceb É Baixa E TaxaEfetiva É Baixa ENTÃO Ofensividade É Média

SE PotSinalReceb É Baixa ENTÃO Ofensividade É Alta

Apêndice 3: Script para Descoberta da Rede

Script Sta_Monitor (Monitorar cada Estação da Rede)

```
#!/bin/bash
case "$1" in
start)

# Termina processos da ferramenta em execucao ou presos
killall -s SIGTERM get_sta_info> /dev/null 2>&1

# Intervalo para tirar as medias
mean_interval=$2
if [ -z $mean_interval ]; then
echo "Utilize: ./sta_monitor {start|stop|clear_data} <int_para_tirar_medias>" >&2
exit 1
fi

## Executa rotina para cada estacao conectada ao AP
for station in `iwdev wlan0 station dump |grep Station |cut -d " " -f 2`; do
./get_sta_info $station $mean_interval&
done
;;
stop)
killall -s SIGTERM get_sta_info
;;
clear_data)
timestamp=`date "+%Y%m%d-%H%M%S"`
tarjcvfmedicoes/bkp_medicoes_$timestamp.tar.bz2 medicoes/*.csv> /dev/null 2>&1
tarjcvfmedicoes/raw_data/bkp_raw_data_$timestamp.tar.bz2
medicoes/raw_data/*.csv> /dev/null 2>&1
rm -f medicoes/*.csv> /dev/null 2>&1
rm -f medicoes/raw_data/*.csv> /dev/null 2>&1
;;
erase)
rm -f medicoes/*.csv> /dev/null 2>&1
rm -f medicoes/raw_data/*.csv> /dev/null 2>&1
;;
*)
echo "Utilize: ./sta_monitor {start|stop|clear_data} <int_para_tirar_medias>" >&2
exit 1
;;
esac
```

Apêndice 4: Script para Coleta das Informações da Rede

Script Get_Sta_Info (Coletar Informações das Estações)

```
#!/bin/bash

# MAC da estacao
station=$1

# Intervalo para tirar as medias
mean_interval=$2

# Roda as medicoes infinitamente ateh receber o stop do sta_monitor
while [ true ]; do

# Contador do intervalo de medicoes, passado via parametro
count=$mean_interval
count2=$count
count3=$count

# Declara a matriz de saida
declare -A output

# Arquivo para armazenar as saidas
file_name=`echo $station |tr -d ':'`
file_name=$file_name.csv

while [ $count -gt 0 ]; do

## Armazena nivel de ruido do canal
  # Numero da linha correspondente ao ruido do canal em uso
line_index=`iwdev wlan0 survey dump |awk '$0 ~ str{print NR+1 FS}' str="frequency"`
# Ruido do canal (no formato, por exemplo: -95)
noise=`iwdev wlan0 survey dump |awk "NR==$line_index{print}" |cut -d ':' -f 2 |tr -d ' \t' |cut -d 'd' -f1`

# Armazena as informacoes da primeira coleta na variavelsta_output
sta_output=`iwdev wlan0 station get $station |grep -E 'rx bytes:|rx packets:|tx bytes:|tx packets:|tx retries:|signal:|tx bitrate:' \
  |cut -d ':' -f 2 |tr -d  ' \t'`
sta_output=`echo $sta_output |sed 's/ /,/g'`
rx_bytes=`echo $sta_output| cut -d ',' -f1`

  # Aguarda 1 segundo antes da segunda coleta (para calculo da taxa de transmissao)
sleep 1

  # Armazena as informacoes da segunda coleta na variavelsta_output_now
sta_output_now=`iwdev wlan0 station get $station |grep -E 'rx bytes:|rx packets:|tx bytes:|tx packets:|tx retries:|signal:|tx bitrate:' \
  |cut -d ':' -f 2 |tr -d  ' \t'`
```

```
sta_output_now=`echo $sta_output_now |sed 's/ /,/g'`
rx_bytes_now=`echo $sta_output_now| cut -d ',' -f1`

# Sinal da estacao (no formato, por exemplo: -52)
signal=`echo $sta_output_now |cut -d ',' -f6 |cut -d 'd' -f1`
# Bitrate de transmissao da estacao (no formato, por exemplo: 54.0)
tx_bitrate=`echo $sta_output_now |cut -d ',' -f7 |cut -d 'M' -f1`
# Taxa de transmissao em bits por segundo (no formato, por exemplo: 11040)
tx_rate=$(( ($rx_bytes_now - $rx_bytes)*8 ))
# SNR (no formato, por exemplo: 41)
snr=$(( $signal - ($noise) ))

  # Armazena valores da rodada na matriz
output[${count},1]=$signal
output[${count},2]=$noise
output[${count},3]=$snr
output[${count},4]=$tx_bitrate
output[${count},5]=$tx_rate

  # Armazena dados "crus" de cada medicao
timestamp=`date "+%Y-%m-%d %H:%M:%S"`
  echo
$timestamp,${output[$count,1]},${output[$count,2]},${output[$count,3]},${output[$cou
nt,4]},${output[$count,5]} >>medicoes/raw_data/$file_name

# Decrementa o contador
count=$(( $count-1 ))

done

# Inicializa variaveis para armazenar a soma
sum_sinal=0
sum_txbitrate=0
sum_txrate=0

# Contabilizacao dos valores para armazenar no CSV
while [ $count2 -gt 0 ]; do

  # Soma as grandezas obtidas por cada medicao
sum_sinal=$(( $sum_sinal+(${output[$count2,1]}) ))
sum_txbitrate=`echo "scale=1; $sum_txbitrate+${output[$count2,4]}" |bc -l`
sum_txrate=$(( $sum_txrate+${output[$count2,5]} ))

# Decrementa contador
count2=$(( $count2-1 ))

done

# Calcula as medias e gera arquivo CSV
mean_sinal=`echo "scale=1; $sum_sinal/$count3" |bc -l`
```

```
mean_txbitrate=`echo "scale=1; $sum_txbitrate/$count3" |bc -l`
mean_txrate=`echo "scale=1; $sum_txrate/$count3" |bc -l`

# Calcula a porcentagem da taxa efetiva sobre a taxa nominal
# Converte a taxa efetiva para Mbps
mean_txrate_mbps=`echo "scale=3; $mean_txrate/1000000" |bc -l`
percentage_txrate=`echo "scale=2; $mean_txrate_mbps/$mean_txbitrate" |bc -l`
percentage_txrate=`echo "scale=1; $percentage_txrate*100" |bc -l`

timestamp=`date "+%Y-%m-%d %H:%M:%S"`
echo
$timestamp,$mean_sinal,$mean_txbitrate,$percentage_txrate,$mean_txrate_mbps
>>medicoes/$file_name

done
```