Glauber Lustosa Dourado Villa

Controle de banda global em sítios distribuídos com portabilidade de contrato em redes Wi-Fi comunitárias

Vitória, ES

10-08-2021

Glauber Lustosa Dourado Villa

Controle de banda global em sítios distribuídos com portabilidade de contrato em redes Wi-Fi comunitárias

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática da Universidade Federal do Espírito Santo, como requisito parcial para obtenção do Grau de Mestre em Informática.

Universidade Federal do Espírito Santo – UFES

Centro Tecnológico

Programa de Pós-Graduação em Informática

Orientador: Prof. Dr. Magnos Martinello

Coorientador: Prof. Dr. Rodolfo da Silva Villaça

Vitória, ES

10-08-2021

Ficha catalográfica disponibilizada pelo Sistema Integrado de Bibliotecas - SIBI/UFES e elaborada pelo autor

---

Villa, Glauber, 1977-
V712c Controle de banda global em sítios distribuídos com portabilidade de contrato em redes Wi-Fi comunitárias / Glauber Villa. - 2021.
80 f. : il.

Orientador: Magnos Martinello.
Coorientador: Rodolfo Villaça.
Dissertação (Mestrado em Informática) - Universidade Federal do Espírito Santo, Centro Tecnológico.

1. Redes locais sem fio. 2. Empresas - Redes de computadores. I. Martinello, Magnos. II. Villaça, Rodolfo. III. Universidade Federal do Espírito Santo. Centro Tecnológico. IV. Título.

CDU: 004

Universidade Federal do Espírito Santo
Centro Tecnológico
Programa de Pós-Graduação em Informática
Credenciamento/CFE/parecer n. 132/99, de 02/02/99.

REGISTRO DE JULGAMENTO DA DISSERTAÇÃO DO CANDIDATO AO GRAU DE MESTRE PELO PPGI/CT/UFES

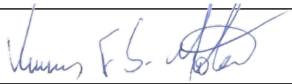
Nº de Matrícula: 2018230868

A Comissão Examinadora da Dissertação de Mestrado intitulada: **"**CONTROLE DE BANDA GLOBAL EM SÍTIOS DISTRIBUÍDOS PARA PORTABILIDADE DE ACESSO À REDES WI-FI COMUNITÁRIAS**"**, elaborada pelo candidato ***Glauber Lustosa Dourado Villa*** ao Grau de MESTRE EM INFORMÁTICA, com área de concentração em Redes de Computadores e Sistemas Distribuídos, recomendou após apresentação da Dissertação realizada no dia Vitória-ES, 20 de agosto de 2021, que a mesma seja (assinale um dos itens abaixo):

(X) Aprovada

( ) Reprovada

Os Membros da Comissão deverão indicar a natureza de sua decisão através de sua assinatura na coluna apropriada que segue:

Aprovado		Reprovado
Prof. Dr. Magnos Martinello		
Prof. Dr. Alextian Bartolomeu Liberato		
Prof. Dr. Vinicius F. S. Motta		

Universidade Federal do Espírito Santo
Centro Tecnológico
Programa de Pós-Graduação em Informática
Credenciamento/CFE/parecer n. 132/99, de 02/02/99.

PARECER ÚNICO DA COMISSÃO EXAMINADORA

O candidato ***Glauber Lustosa Dourado Villa*** apresentou o trabalho intitulado: **"**CONTROLE DE BANDA GLOBAL EM SÍTIOS DISTRIBUÍDOS PARA PORTABILIDADE DE ACESSO À REDES WI-FI COMUNITÁRIAS**"**, como Dissertação de Mestrado no Programa de Pós-Graduação em Informática, Área de Concentração:Redes de Computadores e Sistemas Distribuídos.

Levando em consideração a apresentação escrita do trabalho e a exposição oral do candidato em sessão pública realizada nesta data, esta Comissão Examinadora caracteriza a Dissertação como:

(X) Aprovada

( ) Reprovada

Vitória-ES, 20 de agosto de 2021.

Prof. Dr. Magnos Martinello
Orientador(a)

Prof. Dr. Vinicius Fernandes Soares Mota
Membro Interno

Prof. Dr. Alextian Bartolomeu Liberato
Membro Externo

Universidade Federal do Espírito Santo
Centro Tecnológico
Programa de Pós-Graduação em Informática
Credenciamento/CFE/parecer n. 132/99, de 02/02/99.

471ª ATA DE SESSÃO PÚBLICA DE DEFESA DE DISSERTAÇÃO DE MESTRADO

Às 14:00 horas do dia 20 de agosto de 2021, via internet, reuniu-se a Banca Examinadora composta pelos professores: Prof. Dr. Magnos Martinello (PPGI-Orientador(a)), Prof. Dr. Vinicius Fernandes Soares Mota (PPGI - Membro Interno), Prof. Dr. Alextian Bartolomeu Liberato (IFES – Membro externo), para a sessão pública de Defesa de Dissertação do mestrando ***Glauber Lustosa Dourado Villa***, com o tema: "**CONTROLE DE BANDA GLOBAL EM SÍTIOS DISTRIBUÍDOS PARA PORTABILIDADE DE ACESSO À REDES WI-FI COMUNITÁRIAS***"*. Presente os membros da banca e o examinando, o(a) presidente deu início à sessão, passando a palavra ao aluno; após exposição de _ 40____ minutos por parte do examinando, os membros da banca formularam as suas arguições, as quais foram respondidas pelo examinando. Em seguida, o(a) presidente da sessão solicitou que os presentes deixassem a sala para que a banca pudesse deliberar; ao final das deliberações, o(a) presidente da sessão convocou o mestrando e os interessados para ingressarem na sala e, com a palavra, leu a decisão da banca que resultou na:

[X] **APROVAÇÃO** do examinando. Por fim, o presidente da sessão alertou que o aprovado somente terá direito ao título de Mestre após entrega da versão final de sua dissertação com as correções sugeridas pela banca, à Secretaria do Programa, e com anuência de seu/sua orientador(a).

[ ] **REPROVAÇÃO** do examinando. Por fim, o presidente da sessão alertou que o aluno deverá verificar no Regimento do PPGI/UFES quais os efeitos desta decisão, devendo eventuais requerimentos serem dirigidos por escrito à coordenação do PPGI/UFES.

Nada mais havendo, foi encerrada a sessão da qual se lavra a presente ata, que vai assinada pelos membros da banca examinadora e pelo mestrando**.**

Prof. Dr. Magnos Martinello
Orientador(a)

Prof. Dr. Alextian Bartolomeu Liberato
Membro Externo

Prof. Dr. Vinicius Fernandes Soares Mota
Membro Interno

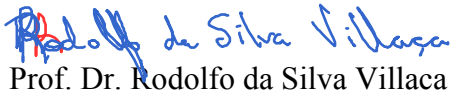
CONTROLE DE BANDA GLOBAL EM SÍTIOS DISTRIBUÍDOS PARA PORTABILIDADE DE ACESSO À REDES WI-FI COMUNITÁRIAS

Glauber Lustosa Dourado Villa

Dissertação submetida ao Programa de Pós-Graduação em Informática da Universidade Federal do Espírito Santo como requisito parcial para a obtenção do grau de Mestre em Informática.

Aprovada em 20 de agosto de 2021:

Prof. Dr. Magnos Martinello
Orientador(a)



Prof. Dr. Rodolfo da Silva Villaca
Coorientador

Prof. Dr. Vinicius Fernandes Soares Mota
Membro Interno

Prof. Dr. Alextian Bartolomeu Liberato
Membro Externo

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

Vitória-ES, 20 de agosto de 2021.

Emitido em 23/08/2021

ATA Nº 1/2021 - COL-CCTI (11.02.21.01.08.02.08)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 23/08/2021 17:36)
ALEXTIAN BARTHOLOMEU LIBERATO
PROFESSOR DO ENSINO BASICO TECNICO E TECNOLOGICO
COL-CCTI (11.02.21.01.08.02.08)
Matrícula: 2630839

Para verificar a autenticidade deste documento entre em https://sipac.ifes.edu.br/documentos/ informando seu número: **1**, ano: **2021**, tipo: **ATA**, data de emissão: **23/08/2021** e o código de verificação: **3a3f73293d**

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

PROTOCOLO DE ASSINATURA

O documento acima foi assinado digitalmente com senha eletrônica através do Protocolo Web, conforme Portaria UFES nº 1.269 de 30/08/2018, por
VINICIUS FERNANDES SOARES MOTA - SIAPE 1331743
Departamento de Informática - DI/CT
Em 23/08/2021 às 19:04

Para verificar as assinaturas e visualizar o documento original acesse o link:
https://api.lepisma.ufes.br/arquivos-assinados/254910?tipoArquivo=O

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

PROTOCOLO DE ASSINATURA

O documento acima foi assinado digitalmente com senha eletrônica através do Protocolo Web, conforme Portaria UFES nº 1.269 de 30/08/2018, por
RODOLFO DA SILVA VILLACA - SIAPE 2650719
Departamento de Informática - DI/CT
Em 24/08/2021 às 15:57

Para verificar as assinaturas e visualizar o documento original acesse o link:
https://api.lepisma.ufes.br/arquivos-assinados/255544?tipoArquivo=O

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

PROTOCOLO DE ASSINATURA

O documento acima foi assinado digitalmente com senha eletrônica através do Protocolo Web, conforme Portaria UFES nº 1.269 de 30/08/2018, por
MAGNOS MARTINELLO - SIAPE 1669875
Departamento de Informática - DI/CT
Em 29/08/2021 às 09:25

Para verificar as assinaturas e visualizar o documento original acesse o link:
https://api.lepisma.ufes.br/arquivos-assinados/258048?tipoArquivo=O

Não há exemplo maior de dedicação do que o da nossa família. À minha querida família, que tanto admiro, dedico o resultado do esforço realizado ao longo deste percurso.

Agradecimentos

Agradeço primeiro a Deus por ter me mantido na trilha certa durante este projeto com saúde e forças para chegar até o final. Deixo um agradecimento especial ao meu orientador Magnos Martinello e ao coorientador Rodolfo Villaça pelo incentivo e pela dedicação dos seus escassos tempos ao meu projeto de pesquisa. Ao Labnerds, com intermédio do professor Moisés Ribeiro, por ter me "adotado"durante este percurso contribuindo amplamente neste processo. À minha esposa Francielle pela compreensão e paciência demonstrada durante o período do projeto. Também agradeço ao meu irmão Daniel que sempre me ajudou com sua vasta experiência desde o início deste projeto de pesquisa.

"Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes."

(Marthin Luther King)

Resumo

O Wi-Fi comunitário ainda se mostra como inovadora opção, oferecendo conectividade abrangente e abrindo portas para novos modelos de negócios em provedores de serviços de Internet. Este trabalho propõe um sistema limitador de banda distribuído capaz de aprimorar o uso do recurso de banda para o Wi-Fi Comunitário usando tecnologias de redes definidas por software e protocolos padrões existentes no mercado. Este sistema como instância especializada do padrão SDN, adiciona um mecanismo limitador de banda denominado (*meters*) e uma aplicação que atua em distribuídos limitadores de banda controlando de forma centralizada bandas agregadas globais e um método de validação experimental que compara limitações de banda globais em distribuídos sítios com limitações de banda locais em um único sítio. Um protótipo foi implementado utilizando o protocolo Openflow, controlador Ryu e uma aplicação em Python com suporte a comunicação via API REST. Demonstramos neste protótipo uma rede distribuída que adiciona ao estado da arte um novo tipo de portabilidade, e adicionalmente, uma aplicação que controla banda de fluxos de forma distribuída, prevenindo excessos de tráfego agregado comuns nas opções atuais de mercado para Wi-Fi Comunitário.

Palavras-chaves: SDN, openflow, controle distribuído, wi-fi comunitário.

Abstract

Community Wi-Fi still proves to be an innovative option, offering comprehensive connectivity and opening the door to new business models at Internet service providers. This work proposes a distributed bandwidth limiting system capable of improving the use of the bandwidth resource for Community Wi-Fi using network technologies defined by software and standard protocols existing in the market. This system, as a specialized instance of the SDN standard, adds a bandwidth limiting mechanism called (*meters*) and an application that acts on distributed bandwidth limiters centrally controlling global aggregated bandwidths and an experimental validation method that compares limitations of global bandwidth on distributed sites with local bandwidth limitations on a single site. A prototype was implemented using the Openflow protocol, Ryu controller and a Python application that supports communication via REST API. In this prototype, we demonstrate a distributed network that adds a new type of portability to the state of the art, and additionally, an application that controls bandwidth in a distributed manner, preventing excess aggregate traffic common in current market options for Community Wi-Fi.

Keywords: SDN, openflow, distributed rate limiting, community wi-fi.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

AP	Access Point
API	Application Programming Interface
DHCP	Dynamic Host Configuration Protocol
FTTH	Fiber-to-the-home
GNS3	Graphical Network Simulator-3
HTTPS	Hyper Text Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IOT	Internet of Things
IP	Internet Protocol
iPoE	Internet Protocol over Ethernet
JSON	JavaScript Object Notation
LAN	Local Area Network
M2M	Machine to Machine
SDN	Software Defined Networking
SI	Southbound Interface
SSID	Service Set Identifiers
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VNF	Virtualized Network Function
WAG	Wireless Access Gateway
WLAN	Wireless Lan
WPA2	Wi-Fi Protected Access v2
XML	Extensible Markup Language

Sumário

1 Introdução

1.1 Cenário Geral - Motivação

Com as tecnologias sem fio se tornando cada vez mais predominantes, os provedores de serviços de internet precisam projetar suas redes da melhor forma possível se desejam acompanhar o crescimento das novas demandas. A não uniformidade no gerenciamento de recursos usados nas soluções existentes e a falta de programabilidade tornam essa tarefa ainda mais desafiadora.

Para lidar com a crescente complexidade nos projetos de ampliação de rede, os provedores de serviços precisam de ferramentas que permitam gerenciar uniformemente as partes com e sem fio de suas redes, por exemplo, para verificar as configurações de rede, solucionar problemas ou depuração sistêmica. Resumidamente, os provedores precisam prover condições uniformes ou padronizadas, que economizem a utilização de recursos, centralizando e facilitando sua operação(SCHULZ-ZANDER et al., 2014).

O Wi-Fi, sinônimo do padrão IEEE802.11 estabelecido pelo *Institute of Electrical and Electronics Engineers (IEEE)*, implementa redes locais sem fio (WLAN). Este é o padrão frequentemente presente em redes residenciais, corporativas ou áreas públicas, permitindo que usuários com seus laptops, celulares e outros dispositivos se comuniquem uns com os outros ou tenham acesso à internet, via um provedor de acesso à internet (ISP), sem utilização de cabos.

Nas residências, o Wi-Fi privado é, normalmente, entregue aos usuários através de equipamentos como roteadores Wi-Fi domésticos, pontos de acesso (AP) e extensores de alcance. Por outro lado, em áreas públicas, o Wi-Fi público é entregue aos usuários através de equipamentos mais robustos e com maior alcance (*hotspots* comerciais públicos).

Há algum tempo os provedores já utilizam o Wi-Fi Comunitário como um serviço agregado ao serviço de internet, e este é considerado uma peça chave para novas estratégias de retenção e crescimento da base de clientes. Este serviço oferece conectividade abrangente e mobilidade aos usuários, utilizando as infraestruturas pré-existentes constituídas de roteadores Wi-Fi. Junto à introdução do Wi-Fi em 5 gigahertz, o Wi-Fi comunitário ganhou ainda mais força, principalmente em ambientes urbanos, onde existe a alta densidade de roteadores Wi-Fi domésticos como células de baixo alcance e alto desempenho (INTEL, 2018).

Neste contexto, um contrato entre clientes e provedores é gerado, contendo (i) a banda contratada máxima, em Mb/s, para uso compartilhado dos dispositivos de usuários subordinados à este cliente, (ii) a quantidade de dispositivos, (iii) a identificação do

contrato, e (iv) a identificação dos dispositivos dos usuários. Firmado este contrato, o cliente passa a ter usuários que podem ser classificados como usuários privados – que utilizam sua rede privada em sua residência (ou sítio) – , ou usuários em trânsito – que utilizam as redes nas residências ou sítios de outro cliente.

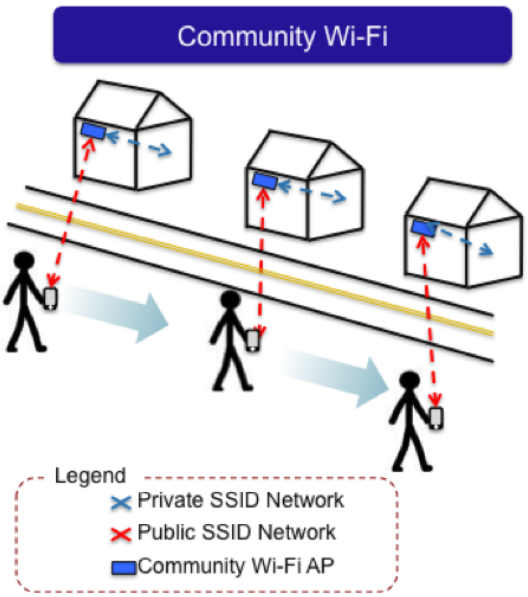


Figura 1 – Wi-Fi Comunitário (GANTI, 2014)

No Wi-Fi comunitário, o roteador Wi-Fi passa a ser chamado de *homespot*. Os *homespots* são disponibilizados aos clientes com uma configuração padrão estática e descentralizada. Ou seja, para ser alterada, esta configuração depende de um acesso remoto com aplicativos de terminal ou similares, executando comandos em lotes em todos os equipamentos.

A banda entregue aos dispositivos conectados na rede privada, abstraindo o *backbone* do provedor e a própria internet, é composta pela concatenação de duas conexões em série. A primeira conexão se dá entre o *homespot* e o equipamento concentrador no site do provedor, normalmente utilizando tecnologias como *pppoe* (CARREL et al., 1999), iPOE, e técnicas de enfileiramento que limitam a largura de banda de acordo com o contrato estabelecido. Já a outra se dá entre o *homespot* e os dispositivos Wi-Fi, limitada pelas tecnologias de distribuição Wi-Fi, como 802.11ax, 802.11ac, e 802.11n (BELLALTA, 2016).

Na literatura recente, alguns trabalhos visam melhorias na transmissão do Wi-Fi a fim de evitar gargalos (SCHULZ-ZANDER et al., 2014). Ademais, novas tecnologias, como o Wi-Fi 802.11ax, prometem altas taxas de bits/s em 5GHz. Baseado nestes dois fatores, entende-se a necessidade de um suposto cenário em que as tecnologias de transmissão, tanto cabeada por fibra ótica quanto Wi-Fi, precisam estar livres de gargalos e serem capazes de entregar altas taxas de bits/s. Mais ainda, esta capacidade deve ser significativamente superior a banda contratada por um cliente. Dessa forma, haveria capacidade física dos

meios de transmissão para que um *homespot* pudesse ser utilizado também pela rede pública.

Soluções atuais de mercado para o Wi-Fi comunitário permitem que um cliente consiga ter uma quantidade ilimitada de dispositivos conectados na sua rede privada, mais um número limitado de dispositivos em trânsito, ou seja, conectados em redes públicas ofertadas nas residências de outros clientes. Nessas soluções, em geral, também limita-se a banda contratada para os dispositivos em trânsito. Como exemplo, assume-se um cenário em que o limite de banda para cada dispositivo em trânsito seja de 20%, e que um usuário possa ter até quatro dispositivos em trânsito. Além disso, neste cenário, todos os clientes possuem contrato de 100 Mb/s com o provedor, e todas redes Wi-Fi estão livres de interferência. Assim, um determinado cliente conseguiria usufruir simultaneamente dos 100 Mb/s distribuídos nos dispositivos locais, e mais 80 Mb/s nos dispositivos em trânsito, totalizando uma banda de 180 Mb/s. Este exemplo demonstra um efeito adverso da solução atual, que permite o uso de um excesso de banda ou sobre-banda, e, se replicado em maior escala, poderia causar gargalo no *backbone* (OI, 2021).

Em um cenário mais justo, a soma de todos os dispositivos de um cliente não deveria ultrapassar o valor do contrato. Mais ainda, a banda disponível para usuários em trânsito deveria ser em função do próprio contrato do cliente, ao invés do contrato do cliente que fornece à rede pública. Dessa forma, seria possível estabelecer uma portabilidade do perfil de plano contratado, i.e., uma portabilidade de contrato. Assim, um usuário teria disponível o plano estabelecido pelo seu contrato mesmo quando estiver em trânsito. Para isso, um controle de banda distribuído é necessário, no qual a alocação de banda em equipamentos distribuídos pudesse ser feita de forma dinâmica, promovendo uma utilização de recursos de banda mais justa.

A rede definida por software (SDN), possui características interessantes para o desenvolvimento de cenários de distribuição de banda mais justos, como, capacidade de abstração de recursos de rede para um sistema virtualizado; separação de funções de encaminhamento e de controle de rede; capacidade de ser programada de forma centralizada. Além disso, as SDNs apresentam um componente interno chamado *meter*, que é útil para medição e controle de pacotes e bytes em dispositivos de rede, podendo inclusive trabalhar de forma centralizada junto ao protocolo *openflow* (Kreutz et al., 2015).

De acordo com nossa pesquisa, a maior parte da literatura sobre o Wi-Fi comunitário é datada em mais de uma década, e só recentemente novos trabalhos começaram a surgir, principalmente no escopo do uso do Wi-Fi comunitário em cidades/casas inteligentes e para segurança. Neste contexto, este trabalho busca contribuir com soluções para algumas das lacunas encontradas na literatura, em específico, este trabalho busca apresentar soluções para a distribuição de banda de forma justa, utilizando a capacidade de adaptação de redes programáveis para o desenvolvimento de soluções. Assim, a questão de pesquisa,

hipótese, objetivos, e contribuições deste trabalho podem ser dadas como:

a) Questão de pesquisa

   Como garantir a justiça na utilização do recurso contratado (largura de banda) pelos usuários/clientes de provedores mesmo quando eles estão fora de casa, em redes públicas?

b) Hipótese

   O uso dos *meters* e do protocolo *openflow* pode permitir o uso do recurso (banda) de forma eficiente e em equipamentos padrões de mercado?

1.2 Objetivo

O objetivo geral deste trabalho é apresentar um sistema capaz de melhorar o uso do recurso (banda) para o Wi-Fi Comunitário, usando tecnologias de redes definidas por software e protocolos padrões existentes no mercado.

1.2.1 Objetivos específicos

- avaliar o uso do *openflow* e dos *meters* no contexto apresentado;
- implementar o sistema proposto por meio de um protótipo no Gns3, permitindo a avaliação do sistema proposto em diferentes cenários de uso;
- desenvolver um sistema de medição e monitoramento que permita medir e controlar o uso da banda de acordo com o contrato.

1.3 Contribuições

Sistema de gerenciamento e controle de recurso de banda distribuídos em redes Wi-Fi comunitárias: Este trabalho propõe um sistema baseado no padrão SDN, adicionando, como mecanismo de controle, *meters openflow* (The Open Networking Foundation, 2012) em determinados dispositivos, em conjunto com uma aplicação que controla excessos de tráfego para usuários de Wi-Fi Comunitário. Ambos subsistemas são responsáveis pelo gerenciamento e controle de dispositivos topologicamente distribuídos, com função adicional de limitação de banda. Juntos, estes subsistemas colaboram para permitir a portabilidade de contratos, e também para impor uma taxa agregada no tráfego de um grupo de dispositivos pertencente a um contrato, permitindo o policiamento deste tráfego agregado em função do valor de banda estipulado no próprio contrato. O SDN se apresenta como uma solução completa, tanto para o projeto quanto para a

implementação. Este atende todos os pré-requisitos em uma única solução, com ferramentas de monitoramento dos fluxos, e de programabilidade e centralização do plano de controle. Assim, dispensa-se a necessidade de outras ferramentas ou aplicativos adicionais.

Além disso, está incluída neste sistema uma abstração chamada *contrato*, que, de forma análoga ao contrato real, define os dados necessários para aplicação do controle do tráfego agregado para os dispositivos no plano de dados. Para isso, o sistema utiliza limitadores de banda distribuídos de forma dinâmica e gerenciamento centralizado.

Este trabalho tem como foco uma parte específica do problema, aquela que engloba a portabilidade e o controle do tráfego de um grupo de dispositivos participantes de um contrato. Mais ainda, o trabalho se estende a como a banda agregada deve ser controlada dentro da política de um contrato.

Um dos desafios principais, no controle de banda distribuído, é permitir que fluxos individuais compitam dinamicamente por largura de banda; não apenas com fluxos que atravessam o mesmo limitador, mas também com fluxos que atravessam limitadores diferentes. Assim, os fluxos que chegam em limitadores diferentes devem atingir as mesmas taxas que atingiriam caso estivessem atravessando um único limitador de banda compartilhado (RAGHAVAN et al., 2007). Dito isso, o propósito principal do sistema proposto é fazer com que um grupo de limitadores de banda distribuídos colaborem em conjunto para garantir que a banda agregada de uma classe de tráfego (e.g., tráfego agregado de um grupo de dispositivos definido no contrato) seja imposta de acordo com o próprio contrato. Por exemplo, se cinco dispositivos participam de um mesmo contrato de 100 Mbps, o tráfego máximo agregado e simultâneo destes dispositivos não pode ultrapassar 100 Mbps mesmo em sítios distintos.

Método e avaliação da eficiência do controle de banda distribuído: Diferentes cenários de implementação do Wi-Fi comunitário foram comparados, envolvendo testes com grupos de limitadores distribuídos versus testes com um único limitador. Dessa forma, foi possível avaliar o comportamento do sistema, a dinâmica de utilização da banda, e os excessos de uso ocorridos. Esta análise também tornou possível a validação do sistema de controle proposto.

2 Conceitos Fundamentais e Estado da Arte

Este capítulo tem o objetivo de apresentar aspectos teóricos importantes para a compreensão do trabalho.

2.1 Redes definidas por software (SDN)

As redes atuais ainda são integradas verticalmente: os planos de controle e dados são agrupados dentro dos dispositivos de rede, reduzindo a flexibilidade e dificultando a inovação e evolução da infraestrutura de rede. Além disso, para expressar as políticas de rede, os operadores de rede precisam configurar cada dispositivo de rede individualmente usando comandos e protocolos específicos do fornecedor. A rede definida por software (SDN) se apresenta como proposta para mudar esta integração vertical separando a lógica de controle da rede, promovendo a centralização (lógica) do controle da rede e introduzindo a capacidade para programar a rede(Kreutz et al., 2015).

Uma das maiores vantagens na arquitetura SDN é a separação do plano de controle e plano de dados. Nesse contexto, o plano de controle entende-se pela inteligência e tomadas de decisões de rotas para fluxos de pacotes, enquanto o plano de dados é responsável pelo encaminhamento de pacotes para seu destino predeterminado pelo plano de controle. Além disso, a rede passa a ser programável, e o controle da rede passa a ser centralizado de forma que N *switches* possam ser compartilhados por um mesmo plano de controle. Uma das palavras chaves do SDN é a flexibilidade, promovida, entre outros, pela possibilidade de criação de novas abstrações de rede, contrapondo um ambiente legado (vertical), relativamente "engessado"e dominado pelos protocolos de roteamento convencionais. A separação do plano de dados e controle se dá através de 2 APIs: a *interface northbound* (NI) entre a aplicação e a plataforma de controle e *interface southbound* (SI) entre a plataforma de controle e os elementos da rede (comutadores de pacotes de dados). O SDN é definido como uma arquitetura com 4 pilares(Kreutz et al., 2015):

- Os planos de controle e dados são desacoplados. A funcionalidade de controle é removida dos dispositivos de rede que se tornará simples elementos encaminhadores de pacotes.
- As decisões de encaminhamento são baseadas em fluxo, em vez de destino como base.
- A lógica de controle foi movida para uma entidade externa, chamado controlador SDN ou NOS.

- A rede é programável através de software aplicativos executados sobre o NOS que interage com os dispositivos de plano de dados subjacentes.

O controle remoto das tabelas de encaminhamento, fruto da separação do plano de controle e dados, é alcançado com a tecnologia *OpenFlow*, que engloba o *OpenFlow Protocol* e *OpenFlow Switch*. O *OpenFlow Switch* consiste em uma ou mais *Flow Tables* e *Group Tables*, onde o lookup e forwarding de pacotes são executados, e um *OpenFlow Channel* para um controlador externo. Usando o *OpenFlow Protocol*, o controlador pode adicionar, atualizar e deletar *Flow Entries* nas tabelas de fluxo. (The Open Networking Foundation, 2012).

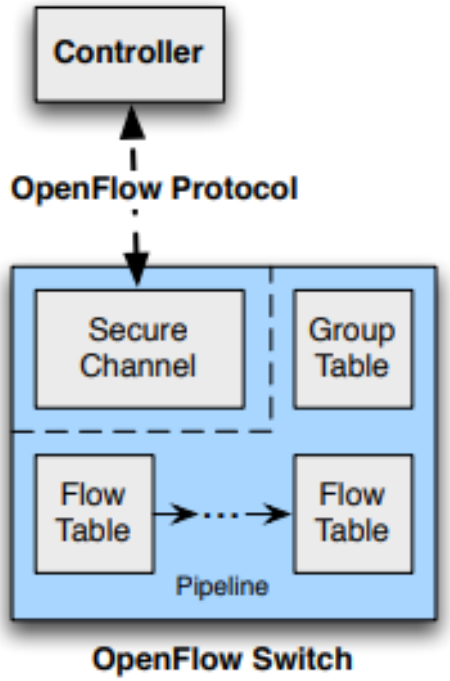


Figura 2 – Main components of an OpenFlow switch(The Open Networking Foundation, 2012)

2.1.1 Meter

Incorporado ao padrão *OpenFlow* a partir da versão 1.3, *meter* é um elemento lógico interno dos *OpenFlow Switchs* que pode medir e delimitar a taxa de bytes ou pacotes. O *meter* aciona um *meter band* se a taxa de pacotes ou bytes ultrapassam um limiar predefinido. Dentro do *OpenFlow Switch* existe ainda uma *Meter Table* onde todas as *Meter Entries* são registradas. Um *meter* mede a taxa de pacotes atribuídos a ele e permite controlar a taxa desses pacotes. Os *meters* são conectados diretamente às *Flow Entries* (em oposição às *Queues* que são conectadas às portas). Algumas *Flows Entries* podem especificar um *meter*, o *meter* mede e controla a taxa agregada de todas as *Flow Entries* ao qual está anexado. Se um *meter* dropa pacotes é chamado de limitador de banda(The

Open Networking Foundation, 2012).

É importante enfatizar que o *OpenFlow Protocol* define um conjunto de mensagens iniciadas por um *OpenFlow Header* contento a versão que está sendo usada, o tamanho total da mensagem, o tipo e o id da transação associada a este pacote. Alguns tipos de mensagens importantes para o entendimento deste trabalho são:

- **OFPT_PACKET_IN** - Tipo de mensagem enviada ao controlador quando um *switch* recebe um pacote que não combina com nenhuma *flow entry*. Normalmente respondida com uma mensagem do tipo OFPT_PACKET_OUT responsável por adicionar uma *flow entry* que combine com os pacotes subsequentes similares.

- **OFPT_METER_MOD** - Responsável por modificações em um *meter*. Sua estrutura possui os campos:

  - **meter_id** - Identificador do *meter*.
  - **flags** - Recebe valores para definições de taxas em *kb/s*, burst e coletas estatísticas.
  - **command** - Especifica um dos *openflow meter command* OFPMC_ADD, OFPMC_MODIFY ou OFPMC_DELETE que respectivamente adiciona, modifica ou deleta *meters* no *switch*.

- **OFPT_FEATURES_REQUEST** - Após uma sessão estabelecida o controlador envia esta mensagem e o *switch* responde com uma **OFPT_FEATURES_REPLY** com informações sobre a configuração iniciais importantes como o *datapath_id* que identifica os *switches* que passam a serem tratados como *datapath*.

- **OFPMP_METER** - pode tanto enviar solicitação de status de um *meter* especificado no *meter_id* ou de todos os *meters* quando o *meter_id* = OFPM_ALL. Quanto receber resposta com os campos:

  - **meter_id**
  - **flow_count** - Número de *fluxos* associados ao *meter*.
  - **packet_in_count** - Número de pacotes na entrada do *meter*.
  - **byte_in_count** - Número de bytes na entrada do *meter*.
  - **duration_sec** - Tempo de duração do *meter* em segundos.
  - **duration_nsec** - Tempo de duração do *meter* em nanosegundos. Para calcular a duração de um *meter* em nanosegundos usa-se duration_sec x 10^9+ duration_nsec.

Para se fazer a leitura de um *meter*, o controlador envia uma OFPMP_METER *request* para um relevante *switch* com o meter_id do *meter* e aguarda o OFPMP_METER *reply* com os dados estatísticos, assumindo que em um determinado momento q1 coleta-se do campo byte_in_count B_{q1} em bytes, do campo duration_sec $DSEC_{q1}$ em segundos e do campo duratios_nsec $DnSEC_{q1}$ em nanosegundos. Se este processo se repete num intervalo de tempo t é possível se calcular a banda utilizada. Após um intervalo t temos um novo momento q2 que coleta-se B_{q2}, $DSEC_{q2}$ e $DnSEC_{q2}$. Calcula-se a banda do *meter* com:

$$Banda = [(B_{q2} - B_{q1})/T] * 8 \quad bits/s \tag{2.1}$$

onde

$$T = (DSEC_{q2} + \frac{DnSEC_{q2}}{10^9}) - (DSEC_{q1} + \frac{DnSEC_{q1}}{10^9}) \quad segundos \tag{2.2}$$

A coleta dos contadores de duração no *openflow* traz características desejáveis como sincronismo facilitado e precisão. Uma vez que a coleta de contadores de bytes e duração são feitas de forma independente para cada leitura em cada *switch*, certas preocupações relacionadas a latência de rede influenciando no cálculo de banda são descartadas. Isso contrapõe um formato onde o servidor entra como referência única de tempo.

2.2 Trabalhos Relacionados

2.2.1 Soluções de mercado para Wi-Fi Comunitário

A quantidade de acesso de alta velocidade local sem fio, somado aos altos preços dos serviços comerciais como hotspots exclusivamente públicos em ampla cobertura, motivou empresas como a FON(ASHERALIEVA; ERKE; KILKKI, 2009) que veio satisfazer esta necessidade utilizando infraestrutura já existente de vários provedores de serviços.

A FON possui uma solução de mercado para Wi-Fi comunitário que utiliza o roteador FON com OpenWRT embarcado e priorização do usuário na rede privada. O acesso a rede pública ocorre sem limitação de banda, porém, com prioridade baixa e limitação na quantidade de usuário visitantes. Esta configuração é totalmente implementada localmente no próprio equipamento sem intervenções dinâmicas do provedor. Dessa forma, um cliente consegue ter acesso a 200% da banda contratada, sendo 100% na sua rede privada (priorizado), mais 100% da banda de outra rede pública com banda sobrando.

Testes feitos neste trabalho relacionado apontam tanto para um problema de gargalo e perda de pacote na rede pública ocasionada pelo uso privado priorizado, quanto

para a limitação do número de usuários que podem levar a acessibilidade deficiente do serviço.

Outra solução de mercado para wi-fi comunitário é a wi-sh(AI; SRINIVASAN; THAM, 2009), que requer a instalação de um software no dispositivo final dos usuários. A solução wi-sh foca em questões como incentivo para os clientes compartilharem sua largura de banda, estes incentivos são dados impedindo certas trapaças e computando vantagens injustas. Funciona com um sistema de crédito ganhos por usuários que compartilham e punindo ou precificando usuários pegos trapaceando. Com o sistema wi-sh usuários não podem receber mais do que merece, um mecanismo baseado em crédito contabiliza o quão bem o cliente compartilha para obter algo em troca.

Todas soluções de mercado apresentadas atacam problemas tendo como aspecto de justiça uma realidade de compartilhamento de banda entre clientes imutável, ou seja, a troca de banda entre clientes não pode ser mudada. Esta troca é definida como, por exemplo, um cliente A que usa parte ou toda banda de B, e vice-versa, B usa banda de B (ou C). Dessa forma, é criado um ambiente complexo de permuta de tráfego e gerando, em todos os casos apresentados, possibilidade de um cliente exceder a banda contratada usando, simultaneamente através de seus usuários, sua rede privada e uma rede pública qualquer. Com o controle distribuído proposto neste trabalho, essa realidade de troca imutável muda, o excesso é tratado, tendendo a não ocorrer garantindo certa justiça em relação a usuários mal intencionados. Além da troca de banda deixar de existir, o que passa a ocorrer é que um cliente A usa a sua banda na sua rede privada ou pública qualquer de forma que a soma entre todos usuários nunca ultrapassem o contrato, enquanto um cliente B tem direitos iguais de A, cada um usa a sua própria banda.

Como dito anteriormente neste trabalho, a solução final do nosso trabalho, similar a solução FON, requer priorização do usuário privado sobre os clientes visitantes é requerida para evitar que o usuário privado tenha seu serviço significativamente degradado, porém não faz parte do escopo deste trabalho, ficando para trabalhos futuros.

2.2.2 Soluções de artigos e literatura

Em (RAGHAVAN et al., 2007) é apresentado o projeto e implementação de limitadores de bandas distribuídos, de forma análoga ao trabalho aqui proposto, que operam impondo um controle global agregado distribuído a vários sites. Assim, a abordagem proposta pelos autores permite o policiamento de serviços de rede baseado em nuvens como *Google Docs, Windows Live* e *Amazon Elastic Compute Cloud*. Nele, um conjunto de limitadores de banda controlam uma classe de tráfego impondo um único limite global agregado, evitando, em um provedor de serviço, por exemplo, exceder o serviço contratado por uso simultâneo dos centros de hospedagem ou um limite punitivo excessivo por divisão do serviço contratado por cada centro de hospedagem. Ainda neste trabalho

relacionado, um mecanismo de vigilância de tráfego similar ao *Token Bucket Algorithm* foi implementado. Cada limitador funciona de forma idêntica e independente, não possuindo um plano de controle separado e centralizado. Em cada limitador podem ser atribuídas duas tarefas: estimação e comunicação – que consiste na utilização de um protocolo que mescla estimativas locais e globais do tráfego agregado e comunica com outros limitadores através de um protocolo UDP desenvolvido –; e alocação – que utiliza queues a nível de ambiente de usuário linux e iptables para capturar pacotes IPs completos, passando esses pacotes para um limitador designado que impede que este prossiga para o encaminhamento via kernel. Por fim, os limitadores de banda possuem tarefas adicionais, e os códigos são implementados localmente, divergindo do trabalho aqui apresentado ao qual os limitadores têm a função apenas de encaminhar pacotes baseado numa tabela. Além disso, o trabalho citado, não possui um plano de controle e aplicação centralizada.

Com um número crescente de dispositivos IOT e com o grande avanço das tecnologias voltadas à smart homes, (JANG; LIN, 2017) apresenta uma solução para gerenciamento de largura de banda baseada em SDN. Nesse trabalho, como pode ser visto na Figura 3, os autores trabalham com uma arquitetura contendo duas abstrações: uma SDN smart home cloud, do lado do provedor, e diversas smart homes, do lado dos clientes. Estas duas abstrações se comunicam através do protocolo *openflow*. Dentro das smart homes, duas classificações são criadas, a de comunicação M2M – entre dispositivos internos da residência do cliente –, e a Não M2M – entre dispositivos internos e a internet –. Na primeira classificação, é também feita uma outra subdivisão em relação aos tipos de serviços utilizados (e.g., conversação por voz, jogos em real time, conversação de vídeo, transferência de dados sensíveis a atraso, streaming de vídeo). O sistema primariamente prioriza estas categorias de serviços, e depois define estratégias de alocação de banda por serviço para garantir QoS e QoE (qualidade na experiência), ambas dentro da limitação de banda da conexão de internet com o provedor ou capacidade da rede interna. A solução usa openvswitch (linux), controlador Ryu, e mininet como testbed. A solução do artigo citado também, de forma análoga, controla banda de determinados grupos de equipamentos, impondo um controle baseado em políticas e abstrações. Por fim, o artigo citado evidencia a relevância do controle e alocação de recursos de banda, além de utilizar tecnologias similares a deste trabalho como *openflow* e Ryu.

O uso de múltiplos roteadores e extensores de sinais trazem vantagens tanto para usuários do lar quanto para entrega de Wi-Fi para a comunidade. No entanto, redes com essa configuração são vulneráveis à violações de segurança, pois padrões de segurança, como o acesso protegido ao Wi-Fi WPA2, têm sua proteção limitada ao dispositivo do cliente e o ponto de acesso. Já entre o ponto de acesso e o *wireless access gateway* (WAG), há uma lacuna de proteção, em que o dono da rede privada pode ter acesso às informações da rede pública ou da comunidade. Esta lacuna de segurança é apresentada na Figura 4, junto a uma arquitetura existente de Wi-Fi Comunitário.

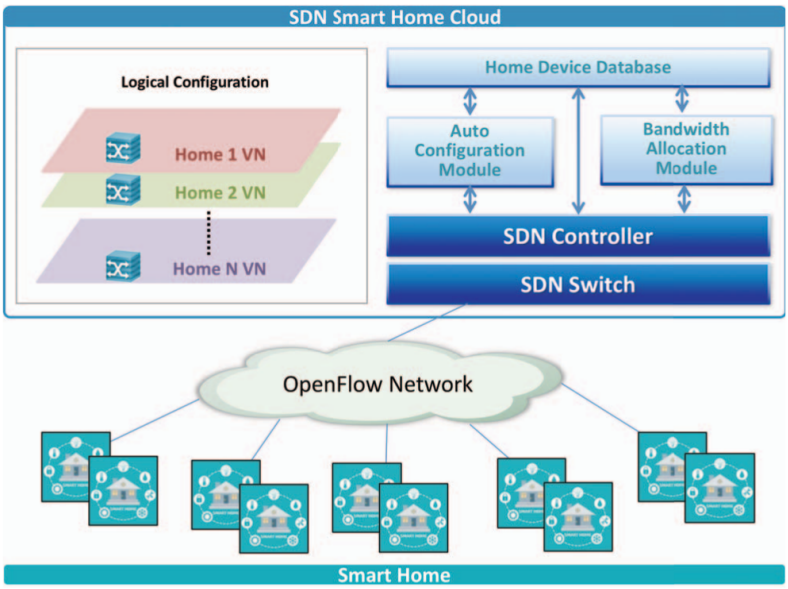


Figura 3 – Arquitetura de casa inteligente baseada em SDN (JANG; LIN, 2017).

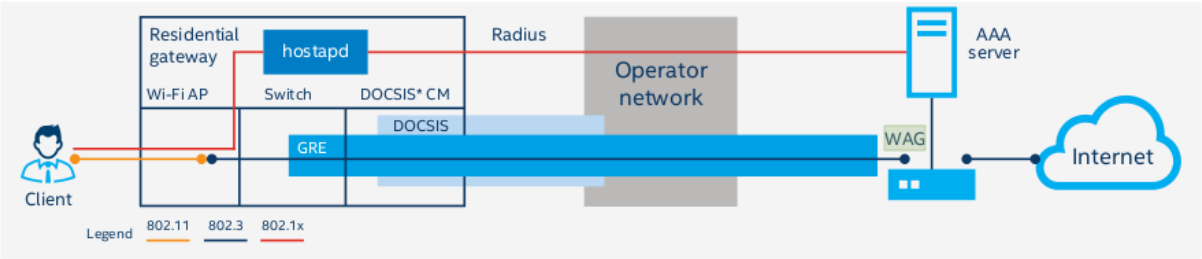


Figura 4 – Arquitetura de Wi-Fi Comunitário (INTEL, 2018).

Para tratar esse problema, os autores em (INTEL, 2018) apresentam uma proposta na qual a proteção do WPA2 se estende para fora do domínio da rede sem fio e atravessa a rede cabeada ou fibra até a nuvem do provedor. Dessa forma, tanto redes privadas como públicas estariam protegidas, evitando ataques por esse tipo de falha. Nesta arquitetura, um ponto interessante é que o roteador Wi-Fi, além de executar funções de segurança, gerenciamento de clientes, e gerenciamento de recursos, age como ponto de acesso, ou seja, encaminha pacotes de uma interface WLAN para uma LAN em modo ponte. Para isso, ele realiza a conversão do protocolo 802.11 MAC para 802.3 (ethernet), estendendo o domínio de broadcast entre uma interface e outra; enquanto a função de gateway fica do lado do provedor no WAG. No mesmo trabalho, é apresentado o exemplo da empresa belga Telenet, que investiu fortemente nesse segmento, colhendo bons frutos e mostrado o quão grande pode se tornar uma Internet pública e comunitária. Isso reforça a importância que deve ser dada à segurança na implementação deste tipo de rede. A arquitetura utilizada pela Telenet pode ser visualizada na Figura 5.

Em (LIBERATO et al., 2016), é apresentada uma proposta para atender emergentes demandas relacionadas à mobilidade de usuários. Uma solução denominada "redes

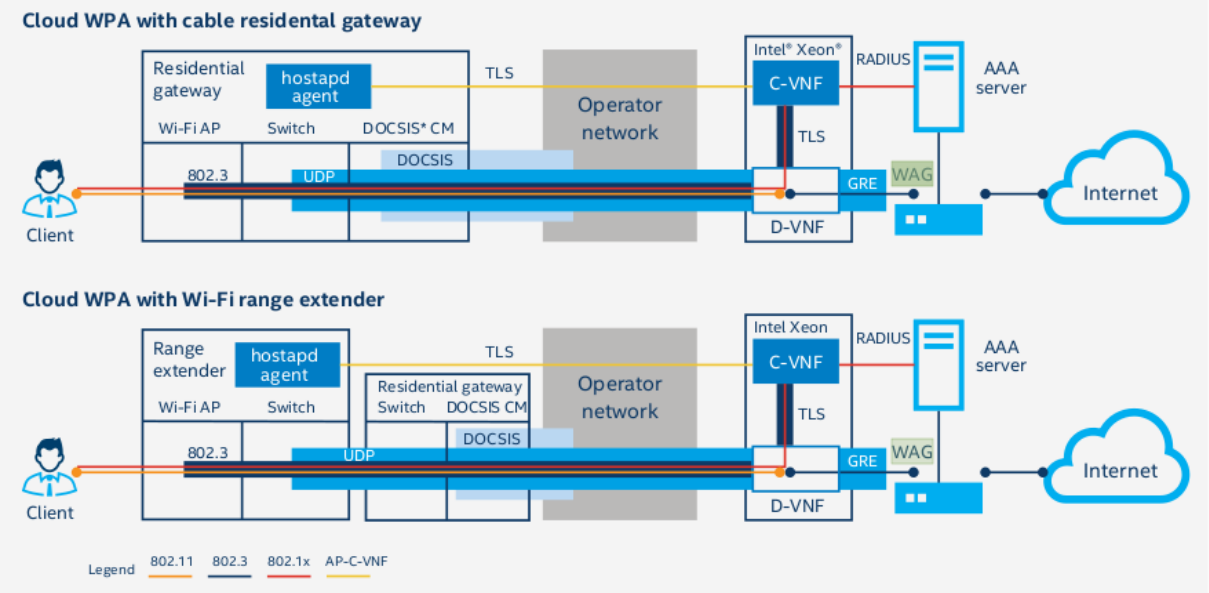


Figura 5 – Arquitetura de Wi-Fi Comunitário Cloud WPA2 (INTEL, 2018).

convergentes efêmeras"oferece suporte para a conectividade continua de dispositivos móveis, por meio de um *backhauling* dinâmico que monta e desmonta rotas rapidamente enquanto usuários se movem e as redes se adaptam. Combinando recursos heterogêneos (sem fio e ópticos) por meio de virtualização, agregado ao Openflow, esta solução entrega em redes ponta-a-ponta conectividade contínua com baixa latência na reconfigurabilidade de rotas.

O presente trabalho estende a abordagem proposta em (DOURADO; MARTINELLO; VILLAçA, 2020), ao permitir escalabilidade e novas possibilidades de uso, reprojetando o ambiente na tecnologia de micro serviços e containerização. Do ponto de vista de controle de banda, os *meters* implantandos em *switches* OF distribuídos possibilitaram a regulação da banda distribuída de um contrato. Além disso, ao monitorar o tráfego por contrato, índices de sobrebanda (excesso) e sub-banda (penalização) foram propostos e avaliados.

3 Sistema de Controle de banda global em redes Wi-Fi comunitárias

Como instância do SDN, o openFlow é um protocolo padrão aberto que permite a programação dos elementos ativos da rede, tais como roteadores, *switches* ou pontos de acesso sem fio. Embora tenha o openflow tenha iniciado com fins acadêmicos(MCKEOWN et al., 2008), ele vem ganhando muita atenção, ganhando força significativa também na indústria nos últimos anos. A maioria dos fornecedores de *switches* comerciais agora inclui suporte da API OpenFlow em seus equipamentos.

Neste trabalho, é apresentada uma proposta composta de *switches* comerciais de prateleira (OpenvSwitch) e servidores Linux, ambos a princípio emulados, com a finalidade de coordenar um conjunto de limitadores de banda distribuídos. Com isso, é possível impor um limite de banda agregado a um grupo predefinido de dispositivos finais de rede, por exemplo, celulares e notebooks, sendo que estes possam ter seus tráfegos atravessando, simultaneamente, distintos caminhos de rede e distintos limitadores de banda. Esta finalidade, neste trabalho, é definida como controle de banda global, pois se trata de limitadores de bandas distribuídos que colaboram através de um controlador *openflow*, operando de forma centralizada para limitar a banda de dispositivos distribuídos.

A arquitetura do sistema está dividida em 3 planos: plano de dados, plano de controle, e plano de aplicações; conforme ilustrado na Figura 6. Entre o plano de dados e o plano de controle, a comunicação é feita através do protocolo *openflow*. Enquanto entre o plano de controle e o plano de aplicações, optou-se por uma comunicação utilizando a arquitetura REST (SHELBY, 2012).

3.1 Plano de Dados

O plano de dados é constituído por uma malha de *switch* OpenFlow, topologicamente distribuído, que realiza um conjunto de operações elementares. Primariamente, o plano possui a função básica de encaminhamento de pacotes, entre suas interfaces, ditada pela tabela interna de fluxos. Esta tabela é dinamicamente populada diretamente pelo plano de controle e indiretamente pelo plano da aplicação. Uma segunda função adicionada a este plano é a de controlar banda através de *meters*. Essa modificação é mostrada na Figura 7. Os *meters* estão associados a grupos de dispositivos através de identificadores de chaves de fluxos e suas correspondências no plano da aplicação, permitindo, assim, um controle de banda agregado nestes dispositivos tanto de forma centralizada em um único *switch* ou em um conjunto de *switches*.

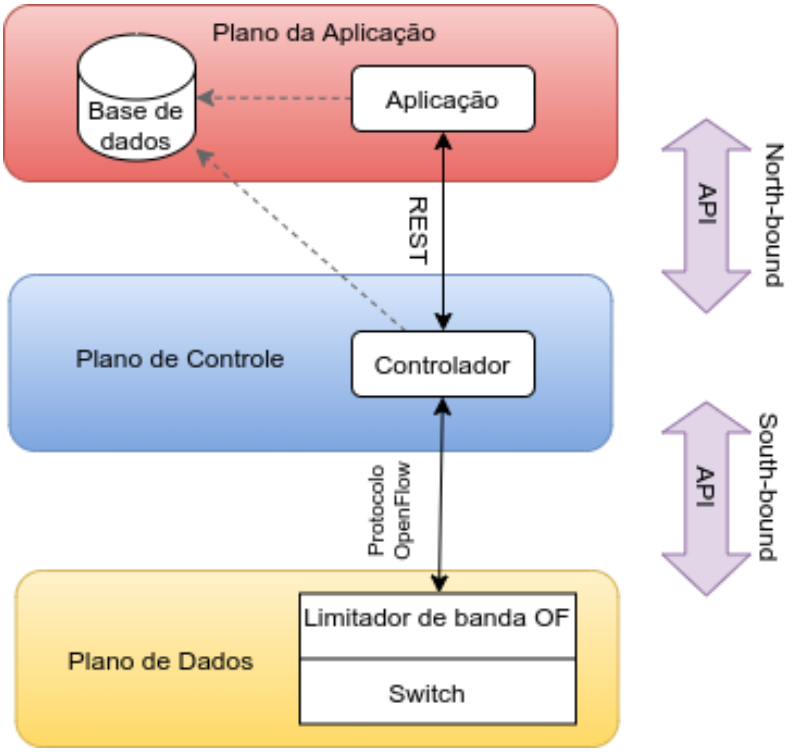


Figura 6 – Base da arquitetura do Controlador de Banda Comunitário.

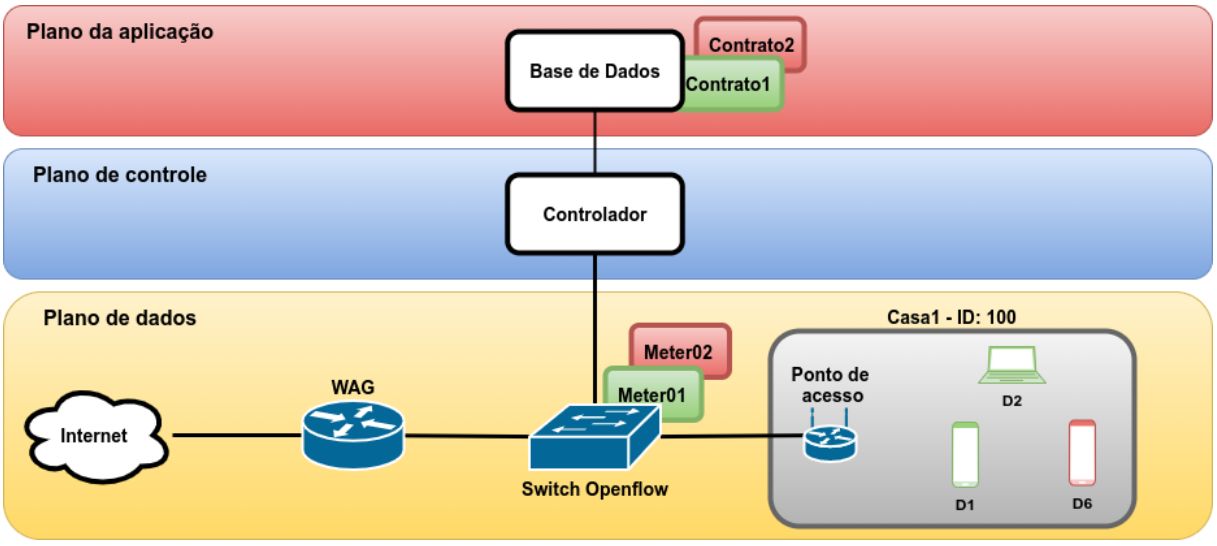


Figura 7 – Modificações adicionadas na instância da arquitetura padrão SDN.

Um *switch* OpenFlow costuma iniciar sua operação com sua tabela de fluxos quase vazia, contendo apenas uma entrada que permite a comunicação com o controlador (flow-miss). Esta tabela é posteriormente populada através de sucessivas mensagens do *openflow*. Entretanto, a remoção destas entradas pode ocorrer tanto por mensagens, quanto por adição de um parâmetro que limita seu tempo de existência, decorrendo assim, em uma remoção automática pelo próprio *switch*.

Ao receber o primeiro pacote, supondo que esteja com a tabela de fluxos ainda quase vazia, o *switch* verifica as informações do cabeçalho deste pacote. Se estas possuíssem alguma correspondência com alguma entrada preexistente, nele terá a instrução de como proceder com este pacote, normalmente uma instrução de encaminhamento para alguma interface. Como neste caso a tabela de fluxo está quase vazia, o pacote fica aguardando uma instrução do *switch* por algum tempo, enquanto isso, este envia os dados do cabeçalho do pacote para o controlador através de uma mensagem PACKET_IN – procedimento padrão do *openflow*. O controlador pode responder esta mensagem com uma mensagem PACKET_OUT contendo uma instrução a ser adicionada na tabela do *switch*. A partir daí, se não estiver expirado, o pacote é encaminhado seguindo orientação desta nova entrada adicionada. Este processo de PACKET_IN e adições em tabelas geram um certo aumento na latência dos pacotes, um problema já conhecido para quem lida com *switches openflow*.

Em nossa instância especializada da arquitetura SDN, os dados de cabeçalhos que chegam no controlador através do PACKET_IN são respondidos com ações extras: a primeira é o pedido de instalação do respectivo *meter*, obtido por consulta ao plano de aplicação através do comando OFPMC_ADD; a segunda é a adição de uma instrução extra na mensagem PACKET_OUT, que adiciona o identificador do respectivo *meter* nesta mensagem de solicitação de adição na tabela de fluxos, sendo que isto ocorre de forma adicional à informação da interface de saída do *switch* que também está incluída nesta mensagem. É importante saber que estas ações extras só ocorrem caso os dados do cabeçalho do pacote, que gerou este processo, obtiver correspondência aos dados do contrato. Caso contrário, uma instrução de descarte será inserida, que uma vez instalada na tabela do *switch*, faz com que este passe a descartar pacotes subsequentes com as mesmos dados no cabeçalho, além de evitar novas mensagens do tipo PACKET_IN. Este processo é ilustrado na Figura 8.

Outra função dos *switches openflow* é fornecer dados estatísticos sobre o status atual dos *meters*. Assim, estes geram condições para o plano de controle, em conjunto com plano de aplicação, calcular a banda local no determinado *switch*. Estas consultas serão melhor detalhadas na Seção 3.3.

Em determinados momentos, em casos de usos reais, poderá ocorrer uma alta quantidade de entradas na tabela de *meters* registradas em um determinado *switch*. Isso ocorre pois os *meters* não possuem mecanismo de auto exclusão, ou parâmetro de tempo

de vida (time_out) como as entradas de fluxos na tabela de fluxo. Para impedir possíveis acúmulos indevidos, uma rotina com limpezas periódicas de entradas de *meters* é desejável.

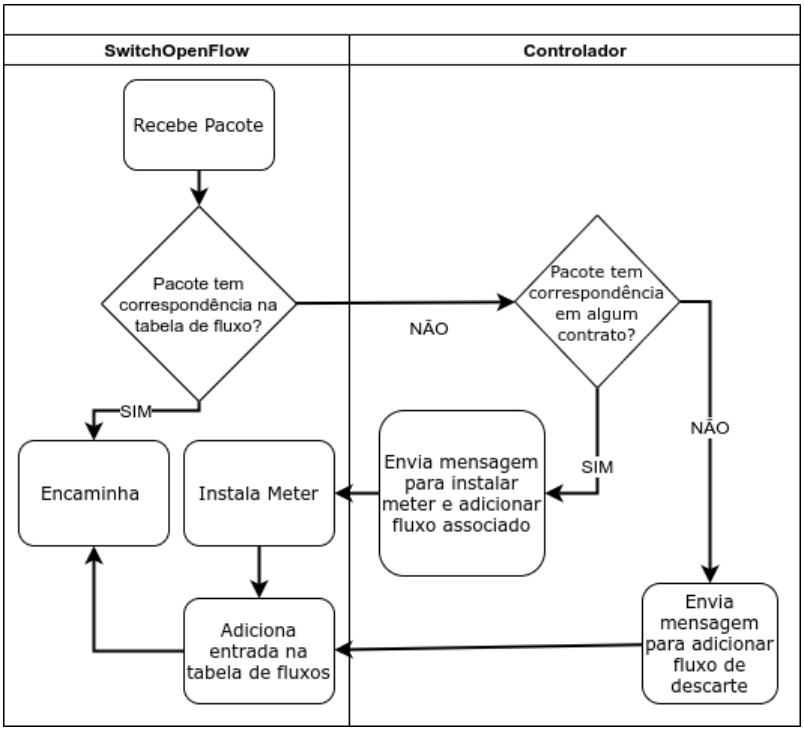


Figura 8 – Fluxo de instalação dos *meters*

Outra característica relevante dos *meters* é a capacidade de limitar a banda em dois sentidos. Isso é possível ao associar duas regras de tráfego (*ingresss* e *egress*) referente a um mesmo par de hosts da rede no mesmo *meter*. Assim tanto o tráfego de download e upload compartilharam o mesmo *meter* e, consequentemente, a mesma limitação de banda.

3.2 Plano de Controle

Os dispositivos no plano de dados são programados por elementos do plano de controle por meio de instruções bem definidas na API SI. O plano de controle é a peça chave de suporte para a lógica e aplicativos de controle serem capazes de gerar a configuração de rede com base nas políticas definidas pelo projetista de rede. Semelhante a um sistema operacional tradicional, a plataforma de controle abstrai os detalhes no nível inferior de conexão e interage com plano de dados, ou seja, materializa as políticas de rede (Kreutz et al., 2015).

O plano de controle proposto neste trabalho, é constituído por um controlador RYU OpenFlow que usa um canal de controle baseado em TCP. O aplicativo foi implementado em Python e executado no controlador como uma simples thread. Como resultado do uso do Ryu, o controlador não é distribuído e funciona em uma única máquina.

A implementação conta com algoritmos que estendem as preexistentes funções inerentes ao controlador RYU OpenFlow. Isso nos permite usar funcionalidades específicas em adição às já existentes no RYU, a fim de atender requisitos extras necessários por nosso sistema, como (i) configurações iniciais dos elementos do plano de dados com suporte a *meters* assim que suas respectivas sessões são estabelecidas; (ii) suporte a inclusão e exclusão de regras de fluxo integradas com o uso de *meters*; (iii) inclusão e exclusão de *meters*; (iv) comunicação com o plano de aplicação para obtenção de informação sobre política de controle de banda.

Quanto a portabilidade de contrato, apresentada no capítulo 1, desenvolvemos uma aplicação de controle de banda distribuído que será descrita na Seção 3.3.

3.3 Plano da Aplicação

É constituído pela aplicação de controle de banda distribuído, lidando com os excessos e subutilizações da banda agregada de um grupo de dispositivos de rede, e, adicionalmente, da base de dados onde é definido e guardada a abstração contrato. Esta base de dados na arquitetura é feita em um arquivo de texto, porém, futuramente, é desejável implantá-la em um servidor RADIUS, prática muito comum em arquiteturas atuais de mercado. Esta aplicação funciona com mensagens http para uma interface REST disponível no controlador e obtém respostas no formato XML JSON. O controlador converte estas mensagens em mensagens *openflow* para os *switches*.

Ademais, o plano de aplicação age proativamente para monitorar os dispositivos do plano de dados e reativamente no ajuste desses mesmos dispositivos quando necessário. Toda sua execução é ditada por um intervalo de leitura ou modificação gerada na própria aplicação, parte proativa da aplicação. Este intervalo define a granularidade da análise do tráfego, uma vez que o cálculo é feito sobre a média do tráfego dentro deste intervalo. Desta forma, janelas de análises são criadas, e quanto menor a janela mais "fina"e precisa será a análise, em contrapartida, gerando mais mensagens na estrutura. Excessos identificados em uma janela serão tratados na janela subsequente de forma reativa. Portanto, fica caracterizado um comportamento natural do sistema que é o de levar um tempo para agir. Este tempo de reação é em função do intervalo de leitura/atualização. Além disso, o intervalo de monitoramento/atualização é peça chave para ajuste de resultados da aplicação, que serão demonstrados Seção 4.2.

Com auxílio da Figura 9 elucida-se o objetivo geral do plano de aplicação. Nela, é apresentado o *Contrato 1*, representado no retângulo verde e que pode assumir uma banda de 100Mbits/s, e um *Contrato 2*, representado no retângulo vermelho e com uma banda de 50Mbits/s. Os retângulos em cinza representam três casas (residências ou sítios), identificadas como *Casa 1*, *Casa 2* e *Casa 3*. Em cada casa temos duas redes Wi-Fi, uma

privada e outra pública, contendo os dispositivos finais D1, D2, D3, D4, D5, D6 e D7 (e.g., notebooks, celulares), distribuídos conforme é ilustrado. A Casa 1 e Casa 2 tem seus pontos de acessos conectados ao *Switch Openflow 1* no lado do provedor de serviço, que entrega o serviço de acesso à internet através do roteador *WAG 1* (Wireless Access Gateway). Já a Casa 3, está conectada no *Switch Openflow 2* e entrega acesso a internet através do *WAG 2*. Nas casas, os dispositivos D1, D2, D3 e D4 (verdes) estão associados ao Contrato 1, enquanto D5, D6 e D7 (vermelhos) estão associados ao Contrato 2. Portanto, os dispositivos associados ao Contrato 1 devem compartilhar entre si uma banda de 100Mbits/s. Por outro lado, os dispositivos associados ao Contrato 2 deve compartilhar uma banda de 50Mbits/s. Como explicado na Seção 3.1, se, por exemplo, ao menos um dispositivos do grupo D1, D2 e D3, que estão na Casa 1 e Casa 2, transmitir dados que tentem atravessar o Switch Openflow 1 visando o WAG 1, desencadearia neste *switch* uma consulta ao plano de controle. Esta consulta, recursivamente, consultaria o plano de aplicação que permitiria este encaminhamento para o WAG 1 com uma instalação no Switch Openflow 1 do *meter* com identificador 100 (definido no contrato).

Porém, ao analisar D4, que se localiza na Casa 3, tentando acessar a internet via WAG 2, isto instalaria no Switch Openflow 2 um *meter* de 100Mbits/s. Dessa forma, teríamos 100Mbits/s compartilhados para D1, D2 e D3 no Switch Openflow 1, além de 100Mbits/s disponível para D4 no Switch Openflow 2. Se todos os quatro dispositivos deste contrato tentarem usufruir simultaneamente do serviço de internet, estes poderiam receber dados à uma taxa agregada de 200Mbits/s, o dobro do contratado. Daí se dá a necessidade da aplicação desenvolvida neste trabalho, que tem o papel de monitorar cenários como este em que grupos de dispositivos tem sua banda limitada por mais de um limitador, prevenindo este excesso de utilização da banda contratada.

Este processo se repete para cada dispositivo destes grupos, de forma que todos serão associados ao mesmo *meter* e compartilharão banda de acordo com o contrato. Ou seja, separam-se as bandas agregadas de cada grupo e as compara com o valor de banda estipulado no contrato. Ao se verificar situações de excesso ou subutilização da banda agregada global, o controle de banda passa a agir sobre a rede, tratando a situação em três etapas nomeadas *coleta*, *agregação*, e *redefinição de novas bandas locais*, que serão descritas na Seção 3.4.

3.3.1 Abstração Contrato

Em redes Fiber-to-the-Home (FTTH), é muito comum o provedor entregar em sua última milha o acesso ao assinante por uma ONU ou ONT, i.e., uma fibra ligada a um roteador Wi-Fi residencial, às vezes ambos em uma única caixa. Esse roteador residencial pode estar interconectado a outros roteadores ou a repetidores para garantir uma melhor área de cobertura do sinal (MARTIGNON et al., 2013). A rede interna formada por esses

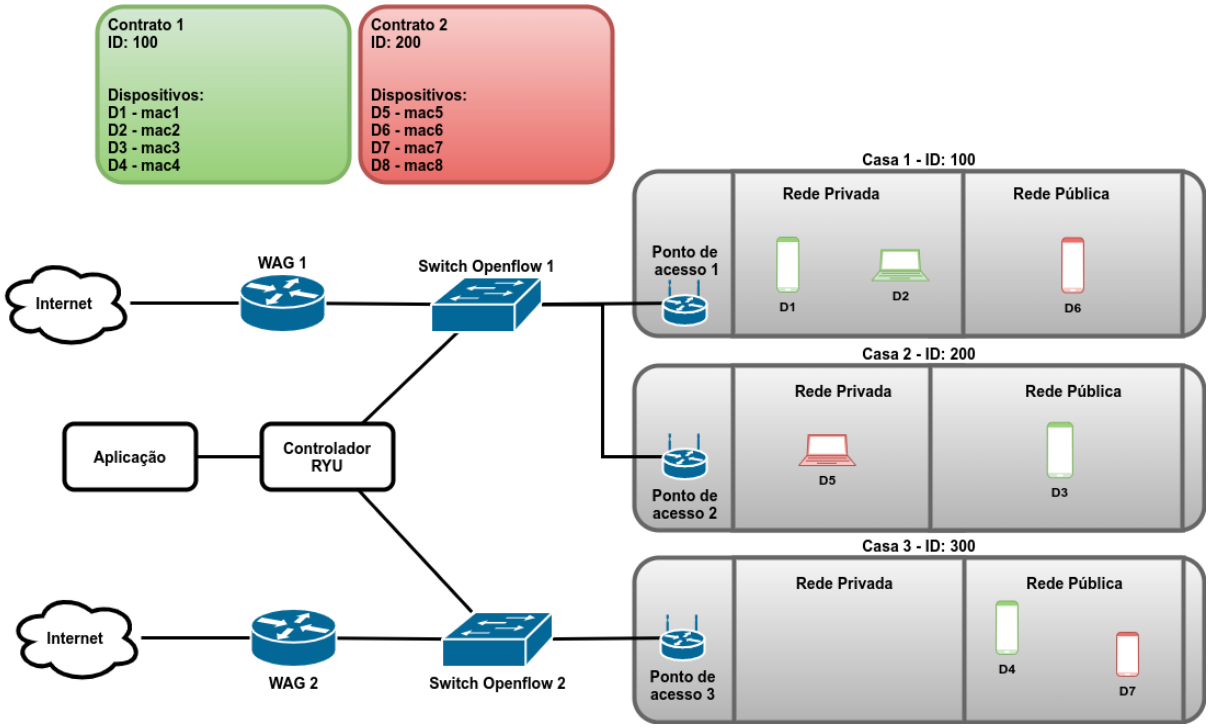


Figura 9 – Visão Geral do Wi-Fi Comunitário.

dispositivos é fonte de inspiração para a política proposta. Esse grupo de dispositivos e seus respectivos endereços MAC são agrupados numa classe chamada contrato. Os dispositivos pertencentes a um contrato são análogos a dispositivos em uma LAN com banda de acesso compartilhada. Por exemplo, um contrato com um plano de 50 Mbps opera dividindo de forma justa essa taxa de bits para todos os dispositivos pertencentes ao mesmo contrato. Um diferencial é que estes dispositivos não precisam estar centralizados em um único segmento de rede, podendo então estar em distintos segmentos, como, por exemplo, atravessando diferentes caminhos em distintos dispositivos *openflow*.

3.4 Processo de controle de excessos na rede Comunitária

A implementação deste processo é basicamente composta por uma aplicação que utiliza duas classes, uma classe chamada *Controlador* e outra chamada *Datapath*. As responsabilidades destas classes são simples: a Datapath é responsável pelas funções mais específicas dos *switches*, como obtenção de estatísticas individuais, um a um; por outro lado, a classe Controlador fornece funções para a aplicação, tratando todo plano de dados como um objeto único. Trazendo um exemplo, a classe Datapath consegue configurar a taxa de um específico *meter* em um específico *switch*, enquanto a classe Controlador consegue configurar a taxa de todos os *switches* que contêm um específico *meter*. Desta forma, a aplicação trabalha de forma simplificada, independente de como o Controlador vai executar certas funções para "baixo"na arquitetura. Estas classes imitam o comportamento da arquitetura SDN e contribuem na reutilização do código. Na Figura 10 temos a ilustração

destas classes.

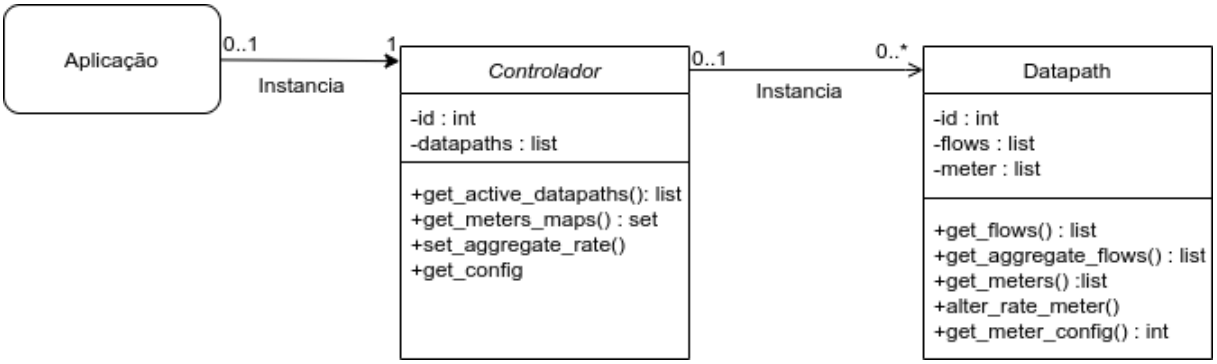


Figura 10 – Diagrama de classes.

Conforme dito anteriormente, o processo de controle de excessos é dividido em 3 etapas:

a) Coleta

Esta etapa é iniciada pela aplicação que primeiramente solicita da base de dados todos os contratos existentes e, consequentemente, os respectivos contrato_id's e bandas contratadas para cada um deles.

Na sequência, inicia-se a coleta periódica de dados estatísticos extraídos do plano de dados via plano de controle em intervalos uniformes de tempo (t). Cada coleta retorna um mapa_tráfego_meters_base, como mostrado na Figura 11a, que além de fornecer uma visão geral de todo o plano de dados em relação a *switches* e *meters* ativos, disponibiliza a banda local de cada *switch* neste mesmo plano de dados.

Ainda nesta etapa, após uma coleta inicial do mapa_tráfego_meters_base, coletas subsequentes deste mesmo mapa são executadas. A coleta anterior a atual é guardada pela aplicação para cálculo de banda média dentro do intervalo (t). Desta maneira, um mapa_tráfego_meters_banda é gerado e enviado para próxima etapa, similar ao apresentado na Figura 11b.

b) Agregação

Com o mapa recebido pela etapa anterior, esta etapa tem a responsabilidade de transformar mapas similares ao apresentado na Figura 11b em mapas de mapa_tráfego_agregado, similares ao apresentado na Figura 11c. O mapa gerado nesta etapa contêm as bandas globais de cada contrato_id ativo no plano de dados, ou seja, fornece o consumo total de cada contrato, dentro de um cenário distribuído.

Adicionalmente, nesta etapa é gerado o mapa_meters_ativos, ilustrado na Figura 11d, com a quantidade de *meters* ativos por contrato_id, sendo este criado através da contabilização de *meters* com banda superior a zero por cada contrato_id.

a) Mapa_tráfego_meters_base

SW1	Meter A - Contadores de duração e bytes Meter B - Contadores de duração e bytes Meter C - Contadores de duração e bytes
SW2	Meter A - Contadores de duração e bytes Meter B - Contadores de duração e bytes
SW3	Meter D - Contadores de duração e bytes

b)Mapa_tráfego_meters_banda

SW1	Meter A - Banda local Meter B - Banda local Meter C - Banda local
SW2	Meter A - Banda local Meter B - Banda local
SW3	Meter D - Banda local

c)Mapa_tráfego_agregado(A)

Contrato A	Banda global
Contrato B	Banda global
Contrato C	Banda global
Contrato D	Banda global

d) Mapa_meters_ativos(Q)

Contrato A	Qt meters ativos
Contrato B	Qt meters ativos
Contrato C	Qt meters ativos
Contrato D	Qt meters ativos

e) Mapa_banda_configurada(X_{i-1})

Contrato A	Banda configurada local
Contrato B	Banda configurada local
Contrato C	Banda configurada local
Contrato D	Banda configurada local

Figura 11 – Estrutura de dados de comunicação entre etapas.

Um último mapa gerado nesta etapa é o mapa_banda_configurada, que contém os valores atuais configurados em cada *meter* por contrato_id. Estes valores definem o quanto de banda um específico *meter* pode deixar passar localmente. Estes valores são os principais alvos da aplicação proposta neste trabalho, e são frequentemente variados a fim do controle da banda global. Todos os *meters* referentes a um mesmo contrato_id terão seus valores, assim que modificados pela aplicação, configurados de forma simétrica. Não havendo, portanto, *meters* de um mesmo contrato_id com valores diferentes.

c) Redefinição de novas bandas locais

Com todos os mapas gerados conforme foram descritos, inicia-se a etapa de análise dos tráfegos globais e redefinição de valores configurados locais para cada *meter* nos elementos do plano de dados, com intuito de controlar a banda global por contrato.

O primeiro passo consiste checar no mapa_tráfego_agregado, linha por linha, ou seja, contrato por contrato, onde ocorreu excesso $\mathbf{B} < \mathbf{A}$, em que $\mathbf{B}$ é a banda definida no contrato e $\mathbf{A}$ um tráfego momentâneo agregado dos dispositivos pertencentes a este contrato. Quando um excesso é encontrado, um algoritmo à parte, baseado no modelo matemático apresentado na Seção 3.5, é aplicado, calculando os novos valores locais que redefinirão os respectivos *meters* no plano de dados deste contrato. Assim, com sucessivas medições e redefinições, a aplicação vai tratando os excessos. Situações com $\mathbf{B} < \mathbf{A}$ também podem gerar redefinições de *meters* locais em casos específicos, e este processo é detalhado também na Seção 3.5.

3.5 Algoritmo de controle distribuído

É função da aplicação prevenir excessos e subutilização do tráfego agregado de usuários do Wi-Fi Comunitário que atravessam dispositivos limitadores de bandas distintos pertencentes a um mesmo contrato. Para isso é importante seguir as seguintes premissas:

- Todos os dispositivos precisam ter uma condição inicial com acesso à banda total se nenhum outro dispositivo estiver concorrendo à mesma banda;
- Se **N** dispositivos de um contrato estiverem consumindo simultaneamente a banda **B** contratada, a tendência é alcançar uma banda **B**/**N** para cada dispositivo;
- A condição inicial tende a ser restabelecida dinamicamente conforme os dispositivos vão deixando de consumir a banda.

Para atender a necessidade do controle de excessos em acordo com as premissas descritas acima, um modelo matemático foi desenvolvido.

Considerando um determinado contrato, denota-se $\mathbf{X}_i$ como o valor atual de banda configurada igualmente para todos os *meters* (m) ativos pertencentes ($contrato_{id} = meters_{id}$). $\mathbf{X}_{i-1}$ é o valor anterior desta mesma variável. **B** é a banda contratada. **A** é o tráfego agregado dos dispositivos pertencentes. $\mathbf{Z}_m$ o tráfego atual local de um determinado *meter* (m), e **Q** é a quantidade total de *meters* ativos. Portanto,

$$\mathbf{X}_i = \mathbf{X}_{i-1} + \delta, \tag{3.1}$$

sendo,

$$\delta = \frac{\mathbf{B} - \mathbf{A}}{\mathbf{Q}} \tag{3.2}$$

$$\mathbf{A} = \sum_{m=0}^{Q} \mathbf{Z}_m \tag{3.3}$$

e,

$$\delta = 0 \quad \text{se} \quad (\mathbf{B} - \mathbf{A}) = 0 \tag{3.4}$$

O principal mecanismo do modelo é que, a cada iteração, $\mathbf{X}_i$ vai se ajustando e tendendo a $\mathbf{X}_i = \frac{\mathbf{B}}{\mathbf{Q}}$ caso todos os usuários estejam usando o máximo de banda disponível. O modelo tende a atuar apenas quando $\mathbf{A} > \mathbf{B}$, representando instantes em que a soma do tráfego de dados dos dispositivos é maior do que a banda contratada, o que geraria prejuízo ao provedor. Para o caso em que $\mathbf{A} < \mathbf{B}$, não há prejuízo, independente da proporção utilizada por cada dispositivo. Neste caso, todos os *meters* retornam para situação inicial $\mathbf{X}_i = \mathbf{B}$, deixando a banda inteiramente disponível.

Para o cálculo de **A**, frequentes leituras com intervalos t nos limitadores de banda são executadas. Estas leituras retornam contadores de tempo (i.e., duração) e bytes dos *meters*. Os *meters* podem agregar fluxos pré-determinados, tendo seu *id* associado ao *id* do contrato. Mais ainda, podem controlar a banda dos fluxos nele agregado.

4 Prototipação e Validação Experimental

Este capítulo tem como objetivo apresentar o protótipo e uma validação experimental que juntos contribuem na avaliação da proposta desta dissertação. Mais especificamente, o protótipo foi desenvolvido como um ambiente satisfatório para execução da validação experimental. Enquanto a validação favorece a confiabilidade na proposta através de testes.

4.1 Prototipação

Nosso protótipo foi desenvolvido todo em um notebook DELL VOSTRO, monoprocessado, processador i5 de oitava geração, oito núcleos, 8Gb de memória RAM e sistema operacional (OS Base) Linux Mint 20.1.

O plano de dados da arquitetura foi implementado dentro do *Graphical Network Simulation* (GNS3) versão 2.2.15, um software emulador de redes que permite a combinação entre dispositivos físicos e virtuais. O GNS3 nativamente emula roteadores CISCO através do *Dynamips Emulator*, porém na versão utilizada é possível adicionar elementos de rede usando instâncias isoladas de espaço de usuário do sistema operacional compartilhando o mesmo núcleo (conteinerização). Portanto, cada elemento da rede é uma instância de container com grau de isolamento suficiente para nossos testes e com desempenho superior do que utilizando máquinas virtuais emuladas com sistemas operacionais inteiros embutidos.

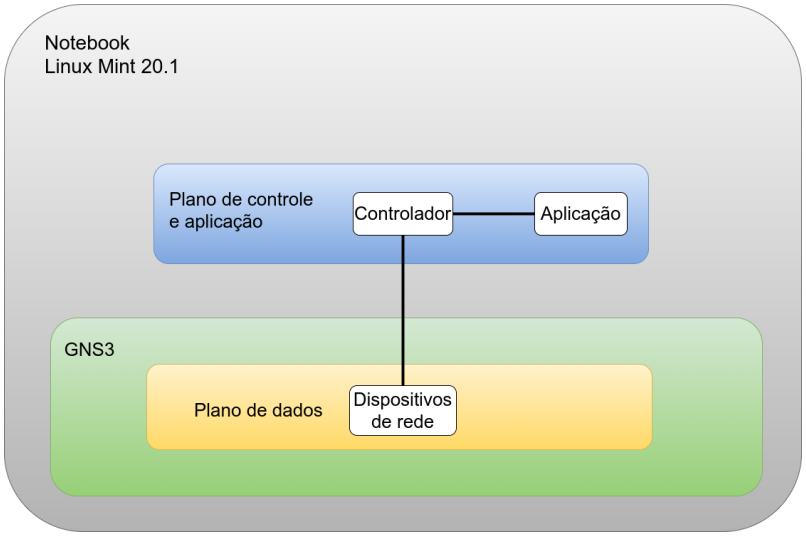


Figura 12 – Prototipação base para validação experimental.

Para uma implementação fiel da arquitetura, também baseada nas soluções existentes na literatura, ainda no plano de dados, era necessário, a princípio, emular dispositivos

de redes como o WAG, *switches openflow* controlador de banda (SwCB), e os dispositivos finais, presentes na Figura 12. Este roteador gateway de rede precisa de uma interface com IP e sub-rede bem definida o suficiente para distribuir IPs via serviço DHCP Server para os outros dispositivos finais na topologia, além de instalado a ferramenta iperf e nginx (servidor web). Nos dispositivos finais apenas o DHCP client, ferramenta wget e o iperf foram instalados.

O gerenciamento dos WAGs e dos dispositivos finais eram obtidos através de telas de console fornecidas pelo próprio GNS3. Os dispositivos não precisam "conversar"com o plano de controle e aplicação.

Os limitadores de banda, também presentes no plano de dados, exigem comunicação com o plano de controle. Neles foram instalados o pacote Open Vswitch 2.12.2, DBschema 8.0.0 e *openflow* 1.3.

O plano de controle e a aplicação foram implementados no próprio SO BASE do Notebook. A comunicação entre os elementos foi feita através de uma interface de túnel TAP, que é um dispositivo de rede virtual do kernel, totalmente suportado em softwares, diferente dos dispositivos de rede comuns que são apoiados em cima de adaptadores de rede físicos.

4.1.1 Simulando mobilidade no protótipo

Para testes com simulação de mobilidade, entre os SwCBs e os dispositivos finais uma topologia quase full mesh foi configurada, com cada SwCB interligado, via interfaces ethernet (802.3) virtuais, com cada dispositivo final participante do teste. Entre cada WAG e dispositivo final existia um caminho atravessando um único SwCB conforme ilustrado na Figura 13. Cada WAG possuía uma faixa de rede IP distinta e entregava endereços IPs dinâmicos pertencentes a respectiva faixa para os dispositivos finais via DHCP. Em todas as interfaces dos dispositivos finais os endereços MAC, identificadores chave dos fluxos nos limitadores de banda eram replicados. Desta forma, no exemplo da figura, o dispositivo final 1 tinha 3 interfaces ethernet com endereços IP diferentes, porém o mesmo endereço MAC. Cada WAG e seu respectivo SwCB representavam um sítio, assim por exemplo, quando o dispositivo final 1 fazia um download do WAG1 era como se este dispositivo estivesse no sítio 1, quando este mesmo dispositivo fazia um download no WAG2 era como se estivesse no sítio 2 e assim sucessivamente. O que não poderia ocorrer era um dispositivo fazer downloads simultâneos em dois WAGs diferentes, pois assim seria como estar em dois sítios diferentes ao mesmo tempo, o que é fisicamente impossível. Para um dispositivo final "mover"de um sítio para outro, bastava apenas, após encerrar um download, trocar o IP de destino da ferramenta de teste para um outro determinado WAG e executar um novo download.

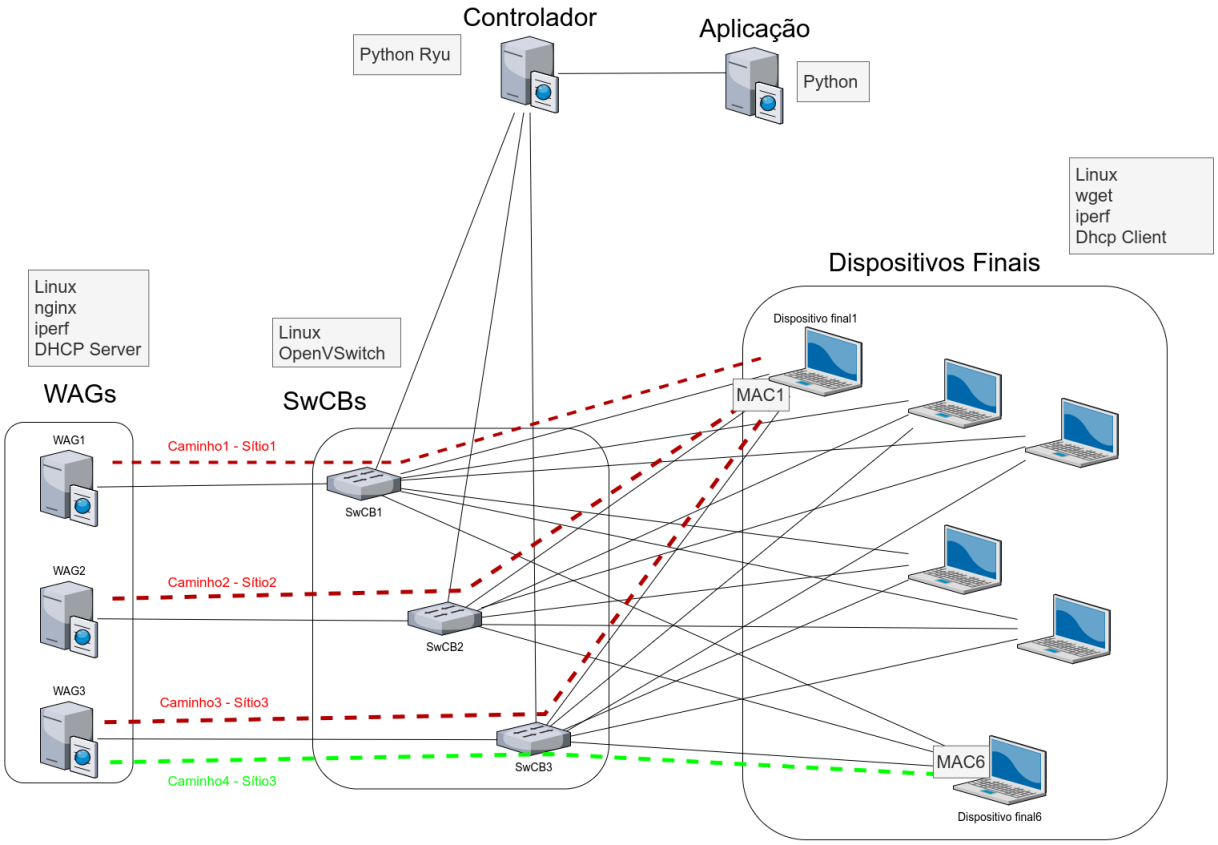


Figura 13 – Exemplo do protótipo configurado para simulação de mobilidade.

4.2 Validação Experimental

Nossa validação experimental é dividida em validações que tanto lidam especificamente com as finalidades do trabalho como portabilidade de contrato e controle de excessos, quanto, validações que lidam com o reconhecimento dos limites do protótipo e na compreensão do mecanismo *meter*.

O reconhecimento dos limites do protótipo é justificado pelo fato de se tratar de um ambiente emulado em um hardware monoprocessado. Sendo desejável então, encontrar uma zona segura para execução dos demais testes livre de interferência/gargalos de processos computacionais externos à emulação em si.

No decorrer da validação, quando necessário, alguns testes foram executados em séries e rodadas. Cada série contendo 10 rodadas. De uma série para outra, altera-se apenas uma variável, denominada de variável independente, sendo as demais denominadas variáveis monitoradas e usadas nas análises dos resultados. De uma rodada para outra nenhuma variável é alterada. O resultado de uma série é a média dos resultados das suas rodadas. Nas tabelas apresentadas a seguir deste capítulo, quando existir, a variável independente sempre estará na coluna mais à esquerda.

Nos testes foram utilizados protocolos UDP e(ou) TCP conforme especificado no próprio teste. Nos testes UDP, o controle de banda de um fluxo foi feito exclusivamente

na ferramenta (iperf). Enquanto nos testes TCP, este controle foi feito exclusivamente nos *meters* através da aplicação do sistema. Além disso, é importante frisar que a natureza do protocolo TCP de usar toda a banda disponível não foi manipulada. Todos testes foram executados no protótipo apresentado no início deste capítulo. O plano de dados do protótipo era configurado de acordo a atender a quantidade de dispositivos e limitadores de banda necessários para o respectivo teste. Logo, o protótipo pôde assumir 4 configurações aqui abreviadas como protótipo C1, C2, C3 e C4.

4.2.1 Validação da capacidade de transferência útil do protótipo

Este teste foi desenvolvido para encontrar o limite máximo e útil de transferência de dados dentro do protótipo. O objetivo é encontrar uma faixa segura de taxa de transferência agregada para execução dos demais testes relativamente livres de gargalos de barramento e processador do ambiente emulado. O protótipo C1 Figura 14, contendo um WAG, um SwCB e um dispositivo final foi utilizado.

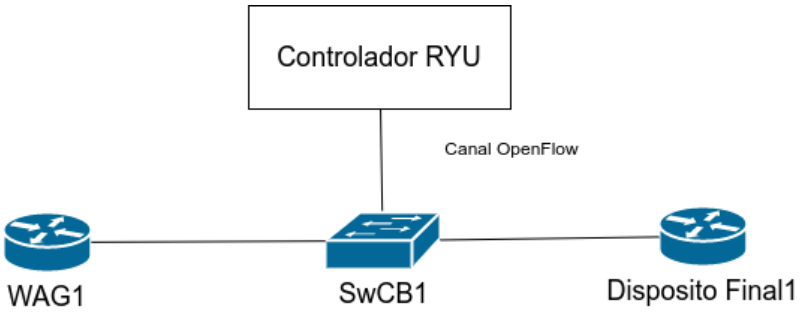


Figura 14 – Protótipo C1.

Em cada uma de 10 rodadas por série, um fluxo UDP, escolhido por ser mais simples e leve, gerado com iperf era gerado entre o WAG e o dispositivo final (atravessando o SwCB). A variável independente era o controle de banda configurado na ferramenta iperf (ba), enquanto as variáveis dependentes monitoradas eram o uso do cpu do SwCB, perda de pacotes entre o WAG e o dispositivo final, jitter, pacotes fora de ordem, tráfego médio reportado pela ferramenta no final do teste.

- Resultado da validação da capacidade de transferência útil do protótipo.

O resultado apresentado na TABELA 1 demonstra que, apesar do sistema conseguir alcançar taxas de 1,75 Gb/s, em 100 Mb/s a ferramenta reportou pacotes fora de ordem, e em 50 Mb/s reportou perda de pacotes. Assumindo esse *protótipo* como um teste de qualidade, pode-se propor um limite de ba em 20 Mb/s. No entanto, como margem de segurança extra, optou-se por definir 10 Mb/s como limite. A partir deste teste, todos os demais testes tiveram que se enquadrar dentro da limitação de 10 Mb/s de tráfego agregado.

Tabela 1 – Perda de pacotes com tráfego de aproximadamente 50Mb/s e presença de pacotes fora da ordem com tráfego de aproximadamente 100Mb/s.

Banda configurada no iperf (Kb/s)	SW CPU (%)	Perda de pacote (%)	Jitter (segundos)	Pacote fora de ordem (pacotes)	Tráfego médio no plano de dados (Kb/s)
1000	0,5	0	0,035	0	1028
10000	0,52	0	0,043	0	10285
20000	0,4	0	0,022	0	20218
50000	0,24	0,00047	0,02	0	51432
100000	0,37	0,00039	0,064	1	102857
200000	0,22	0,006	0,04	4	205719
500000	0,27	0,015	0,001	10	514285
1000000	0,18	0,15	0,001	16	1028672
2000000	0,23	13	15,247	1528	1891005

4.2.2 Validação da ausência de interferência da leitura/manipulação dos *meters* em relação ao plano de dados

O foco deste trabalho não é a escalabilidade, apesar de entender-se que para uma solução completa, este quesito é muito importante e não deve ser descartado em trabalhos futuros. Mesmo assim, do ponto de vista da escalabilidade não relacionada à quantidade de elementos no plano de dados, mas sim, no comportamento de um elemento sob um alta quantidade de leituras/manipulações ou com um grande número de *meters* instalados, desenvolvemos alguns testes que avaliam como o plano de dados se comporta perante a leitura/manipulação dos *meters*. O intuito era responder a seguinte questão. Será que ler e manipular *meters* afetam o desempenho do plano de dados?

No capítulo 3.3 mostramos uma aplicação que executa frequentes leituras/manipulações, com um determinado intervalo de tempo, via plano de controle, em elementos do plano de dados. Especificamente, o objetivo deste teste é avaliar o comportamento do plano de dados enquanto frequentes leituras/manipulações são feitos no plano de controle em variados casos relevantes para a finalidade da validação.

O teste foi dividido em 4 etapas. Todas etapas foram implementadas no protótipo C1 14, contendo no plano de dados, um WAG, um dispositivo final e entre eles um SwCB, enquanto nos outros planos um controlador e uma aplicação.

Na primeira e na segunda etapa foram executadas durante os testes leituras de *meters*, enquanto na terceira e quarta manipulações de *meters* foram executados. De volta a primeira etapa, as leituras de *meters* incidiam em *meters* associados ao fluxo monitorado no plano de dados. A variável independente, ou seja, que varia de uma série para outra, era o intervalo de leitura, enquanto as variáveis monitoradas eram a cpu do SwCB, a perda de pacotes, o jitter e o tráfego médio entre o Wag e o dispositivo final, o tráfego e a quantidade

de pacotes por segundo no canal de controle entre o controlador e SwCB. Um fluxo UDP de 10 Mb/s foi gerado atráves da ferramenta *iperf* durante os testes. Na segunda etapa o valor do intervalo de leitura foi fixada para 1 (um) segundo, e a variável independente torna-se a quantidade de *meters*, enquanto as variáveis monitoradas continuam as mesmas. Na terceira etapa, ao invés de leituras, é são feitas manipulações no valor de banda de um *meter* adjacente. Ou seja, um *meter* não associado ao fluxo monitorado no plano de dados. O intuito disto é avaliar possíveis interações entre *meters* adjacentes em um mesmo SwCB. Na quarta etapa o *meter* manipulado está associado ao fluxo monitorado no plano de dados. Aqui o intuito é saber se um *meter* com fluxo e tráfego associado pode ser manipulado sem restrições.

Cada etapa consistia de N séries, N definido pela quantidade de variações da variável independente, cada série com 10 rodada de 10 minutos, e resultados da série sendo o valor médio dos resultados de cada rodada da respectiva série.

- Resultado da validação da ausência de interferência da leitura/manipulação dos *meters* em relação ao plano de dados.

a) Teste de leitura variando intervalo de tempo

Tabela 2 – Ausência de interferência no plano de dados em função do intervalo de monitoramento de leitura.

Intervalo de leitura (segundo)	Switch CPU (%)	Perda de pacote (%)	Jitter (segundos)	Tráfego plano controle (Kb/s)	Taxa no plano controle (pacotes/s)	Tráfego médio no plano de dados (Kb/s)
inf	0,47	0	0,506	0	0	9740
1	0,53	0	0,189	2,93	4,15	9710
0,5	0,6	0	0,368	5,3	7,45	9730
0,1	0,97	0	0,218	19,76	24,15	9750
0,01	1,52	0	0,201	75,67	75,64	9710
0,001	2,14	0	0,414	216,6	187,48	9700
0,0001	2,24	0	0,416	285,01	226,79	9700
0,00001	2,31	0	0,398	291.35	232,34	9710
≈ 0	2,33	0	0,333	295,13	236,61	9690

Na primeira etapa, o resultado mostrado na TABELA 2 sugere que a diminuição do intervalo de monitoramento (t) no teste gerou pequeno aumento no tráfego no plano de controle, até um máximo de 295Kb/s, e no processamento do SwCB, até um máximo de 2,3%. Demais variáveis monitoradas não sofreram alterações significativas, principalmente o tráfego médio na ferramenta iperf. Os resultados

sugerem certa robustez do SwCB em relação à interferência do plano de controle sob o plano de dados, pois os dados referentes ao plano de dados permanecem inalterados.

b) Teste de leitura variando a quantidade de *meters*

Tabela 3 – Ausência de interferência no plano de dados em função da quantidade de *meters* em leituras com intervalo de 1 (um) segundo.

Meters instalados (unidade)	Switch CPU (%)	Perda de pacote (%)	Jitter (segundos)	Tráfego plano controle (Kb/s)	Taxa no plano de controle (pacotes/s)	Tráfego Plano Dados (Kb/s)
1	0,54	0	0,164	3,08	4,37	9730
10	0,57	0	0,287	7,57	5,01	9740
50	0,62	0	0,133	24,42	6,66	9740
100	0,57	0	0,521	45,73	7,96	9720
1000	1,26	0	0,231	371,3	26,28	9750
10000	1,61	0	0,48	1541,31	143,71	9700

Na segunda etapa, a interferência de sucessivas leituras, variando a quantidade de *meters* instalados no SwCB, no plano de dados não foi observada nos testes tanto UDP quanto TCP. O único aumento significativo ocorreu no canal *openflow*, como era esperado, o tráfego com 10000 *meters* alcançou um patamar de 1540Kb/s e 143 pacotes por segundo. O resultado em TCP é exibido na TABELA 3. No protótipo emulado quando a quantidade de *meters* alcançou 20000 unidades o *protótipo* começou a apresentar instabilidade e erros de execução.

c) Teste de manipulação de *meter* adjacente

Na terceira etapa, durante este teste, nenhuma variável monitorada apresentou dados ou informações significativas que invalidasse o *protótipo*. Isso nos leva a acreditar na boa robustez do sistema proposto. Mesmo com pequenos valores de (t), o fluxo monitorado não sofreu interferência significativa durante as frequentes alterações de um *meter* não associado a ele.

d) Teste de manipulação do *meter* com fluxo monitorado

Na quarta etapa, os resultados para os testes usando UDP e TCP podem ser vistos nas Tabelas 4 e 5, respectivamente. Nos testes UDP, o resultado foi muito similar ao do teste de manipulação de *meter* adjacente. O sistema apresentou-se robusto às manipulações no plano de controle. Ou seja, a manipulação do *meter* não afetou significantemente a comutação de pacotes no plano de dados. Porém, em TCP, o fluxo de dados sofreu alterações (Tabela 5). Apesar do controle de fluxo (bm) estar setado para 10000Kb/s, a banda média entregue na ferramenta sofreu alterações, alcançando até 1380000Kb/s com $t \approx 0$.

Tabela 4 – Ausência de interferência em fluxos UDP em função do intervalo de manipulação de *meters*

Intervalo de manipulação (segundo)	Switch CPU (%)	Perda de pacote (%)	Jitter (segundo)	Tráfego no plano de controle (Kb/s)	Taxa no plano de controle (pacotes/s)	Tráfego médio no plano de dados (Kb/s)
inf	0,47	0	0,029	0	0	10000
1	0,47	0	0,019	1,54	3,71	10000
0,5	0,52	0	0,019	2,68	5,72	10000
0,1	0,95	0	0,04	10,45	17,98	10000
0,01	2,08	0	0,034	52,06	84,97	10000
0,001	3,05	0	0,031	167,22	267,46	10000
0,0001	3,62	0	0,035	245,57	391,56	10000
0,00001	3,68	0	0,033	249,66	392,1	10000
≈ 0	3,77	0	0,024	282,42	415,45	10000

Este resultado nos mostra que atualizar o parâmetro banda de um *meter* altera sua capacidade de controlar seus fluxos associados. Análises visuais durante o teste transmitem uma ideia de indisponibilidade temporária no controle de fluxo no momento da atualização, como se por uma fração de segundo o controle "desligasse". Adicionalmente, indica que o valor de (t) deve ser alterado com cautela, pois atualizar um *meter* com muita frequência pode acarretar em um resultado contrário do desejado no controle do tráfego.

Tabela 5 – Influência do intervalo de manipulação de *meters* sobre fluxos TCP.

Intervalo de manipulação (segundo)	Switch CPU (%)	Perda de pacote (%)	Jitter (segundo)	Tráfego no plano de controle (Kb/s)	Taxa no plano de controle (pacotes/s)	Tráfego médio no plano de dados (Kb/s)
60	0,52	0	0,123	0,91	2,31	9780
30	0,52	0	0,118	0,72	2,32	10300
10	0,52	0,06	0,131	0,9	2,2	11400
5	0,52	0,16	0,149	1,2	2,64	15286
2	0,52	0,3	0,128	0,98	2,77	18000
1	0,52	0	0,285	1,54	3,67	26400
0,5	0,58	0	0,3	2,68	5,58	42800
0,1	1,02	0	0,732	10,48	18,89	89200
≈ 0	2,87	3,34	0,402	262,12	429,89	1380000

4.2.3 Validação da portabilidade de contrato

Nesta subseção apresentamos a validação da portabilidade de contrato através de nosso protótipo.

O objetivo dos testes desta validação é mostrar através de nosso ambiente emulado uma simulação de um dispositivo final se movendo de um sítio para o outro, mantendo sempre a largura de banda estipulada em seu respectivo contrato. Cada sítio representa uma residência no mundo real, logo, com o teste apresentado desejamos mostrar que independentemente de qual sítio este dispositivo esteja situado, seu plano deve ser dinamicamente alocado pelo sistema, sem interações humanas locais no SwCB. De forma centralizada e dinâmica, via nosso sistema de controle global.

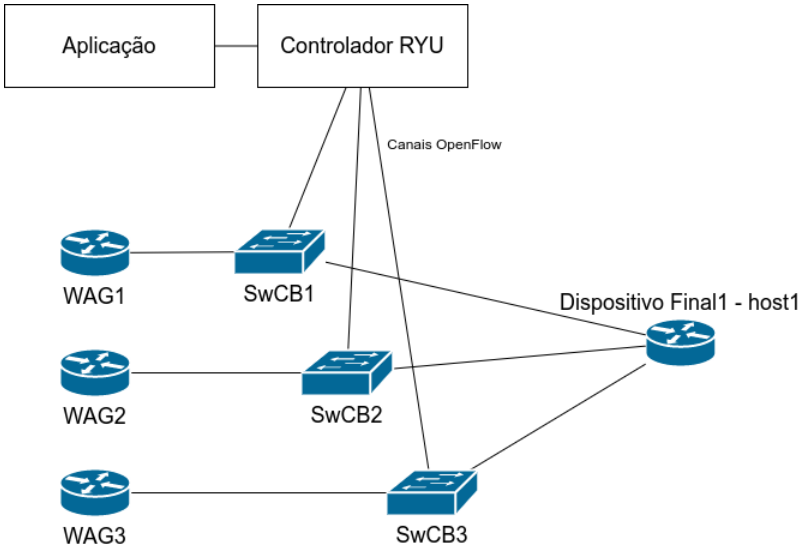


Figura 15 – Protótipo C2.

Neste teste o protótipo C2 Figura 15 será utilizado. Com fluxos TCP, sequenciais e sem sobreposições, gerados entre os WAGs e o dispositivo final, atravessando o SwCB. O controle de banda é feito nos *meters* de cada *switch* distribuído, alocado dinamicamente pelo processo ilustrado na Figura 8, com o valor de 1000Kbps estabelecido no contrato. A duração de um fluxo é definida pelo tamanho do arquivo baixado escolhido de forma aleatória, assim como o intervalo de tempo entre um fluxo e outro também é feito de forma aleatória, dentro de uma range finita de possíveis valores em segundos. Entre um fluxo e outro, mudanças de sítios vão ocorrendo aleatoriamente via script e o comportamento destes sendo analisados no decorrer do teste. A mudança de um sítio para outro simulando mobilidade é detalhada na seção 4.1.1.

- Resultado validação da portabilidade de contrato.

Na Figura 16 ilustra o resultado do teste. De forma bem simples este resultado mostra que o tráfego do dispositivo final aqui definido como host1 acompanha o dispositivo

Figura 16 – Validação da portabilidade com um único dispositivo final.

através dos 3 SwCB atravessados e seus respectivos WAGs. A natureza simples deste teste é intencional. Testes envolvendo mais dispositivos finais aconteceram no decorrer da validação experimental em conjunto com outras validações.

4.2.4 Validação do controle de excesso

Em nosso protótipo habilitado para mobilidade de contrato, testes com apenas um dispositivo final nunca apresentarão excessos. Entretanto, com o aumento no número de dispositivos finais pertencentes a um mesmo contrato, não é difícil imaginar uma situação , ao qual N dispositivos com tráfego simultâneos em sítios distintos, com seu plano contratado disponível, uma banda global agregada de N x B poderá ser alcançada. Esta banda superior a contratada já foi bem definida como excesso no decorrer deste trabalho.

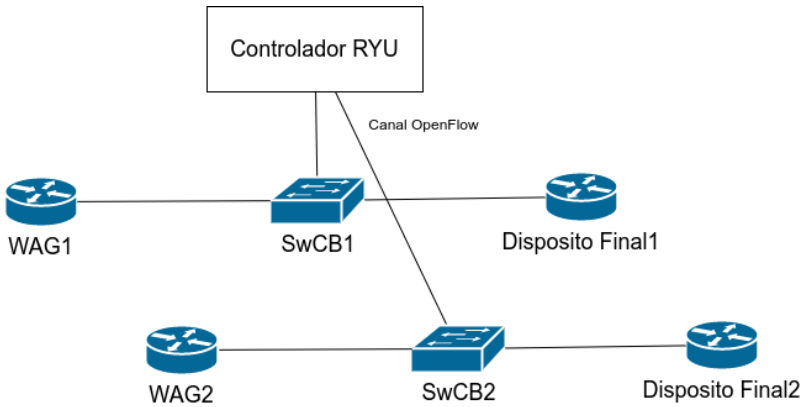


Figura 17 – Protótipo C3.

A aplicação, já apresentada na seção 3.3, tem a responsabilidade de tratar estes excessos, calculando frequentemente a banda global dos contratos em *meters* associados

e ativos, e de forma reativa redefinindo os valores, ao qual, os *meter* localmente são configurados para controle a fim de corrigir excessos na banda global.

O objetivo deste teste é validar o controle de excessos, feito por esta aplicação em determinados casos elementares. Este teste faz uso do protótipo C3. Apesar de executadas várias rodadas, como não observou-se alterações de comportamento entre rodadas, apenas uma delas será apresentada.

O teste foi executado em dois casos. Onde os fluxos de dois dispositivos finais, aqui denominado D6 e D7, que compartilham um mesmo contrato disputam um mesmo controle de banda, porém em SwCBs diferentes. No contrato uma banda de 5Mbits/s é imposta para o tráfego agregado em conjunto dos dois dispositivos. Intervalo de leitura/manipulação dos *meters* na aplicação era de 1 (um) segundo. A duração do teste era de 200 segundos.

No primeiro caso, sequência de fluxos TCP gerados pela ferramenta iperf entre o WAG1 e D6, e entre WAG2 e D7. Estes fluxos eram delimitados pelos *meters* nos *switches*. No caso 2, entre o WAG2 e D7 o fluxo foi alterado para UDP e a banda alterada na própria ferramenta via script, simulando de forma simples um aplicativo real de baixo consumo como comunicação de voz ao lado de um fluxo TCP simulando, e,g, aplicativo de *stream* de vídeo. Esta banda na ferramenta inicialmente foi configurada para 500Kb/s, depois alterada para 1Mb/s e por fim para 2Mb/s durante a execução do teste.

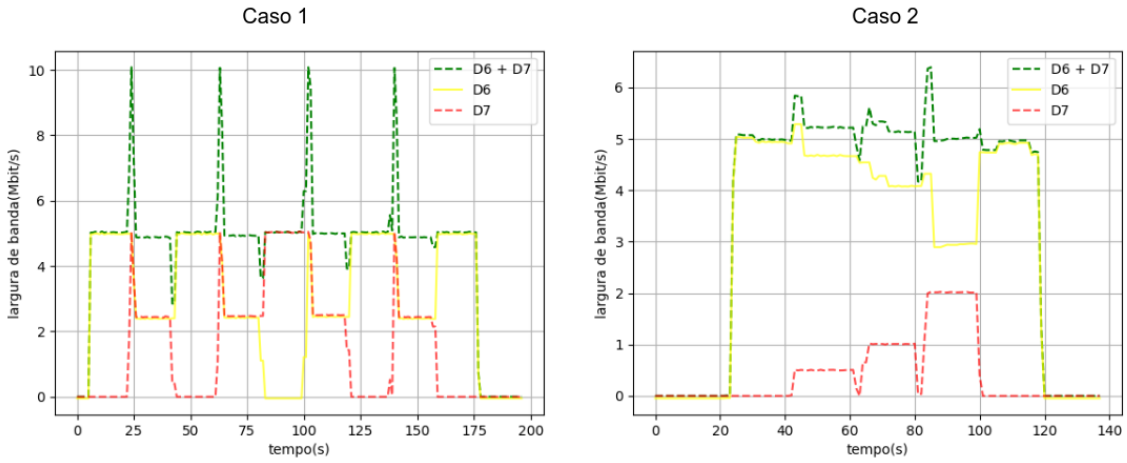


Figura 18 – Validação do controle de acesso.

- Resultado validação do controle de excesso.

Nos gráficos apresentados na Figura 18 a linha verde tracejada mostra o tráfego agregado entre os dois dispositivos atravessando SwCB distintos. Este tráfego agregado tendeu a se manter próximo do limite estabelecido pelo o contrato. O que demonstra que o sistema atuou como esperado. Os resultados representam usuários em sítios distintos compartilhando a mesma banda em situações elementares de carga de trabalho sem

mobilidade. Excessos e subutilizações de banda foram detectados e a aplicação redefiniu os *meters* em cada SwCB controlando o tráfego agregado. Mesmo com o intervalo de monitoramento de 1 (um) segundo, como a aplicação não executa manipulação de *meters* em todas interações conclui-se que em casos elementares, intervalos pequenos podem ser utilizados. Agora em casos reais de utilização de um usuário, padrões de fluxos mais complexos podem gerar alta frequência de manipulação de *meters* causando comportamento oposto ao esperado, este comportamento é explicado no resultado do teste em d).

4.2.5 Validação do controle de excesso com portabilidade de contrato

Neste teste o objetivo é mostrar como o plano de controle e aplicação trabalhando juntos se comportam, provendo mobilidade de contrato e controle de excesso simultaneamente. Este teste segue os mesmos padrões do teste 4.2.3 e 4.2.4 juntos. As diferenças estão na configuração do protótipo e sua quantidade de elementos, e na duração do teste que aqui é de 2500 segundos. O intervalo de leitura/manipulação continua 1 (um) segundo.

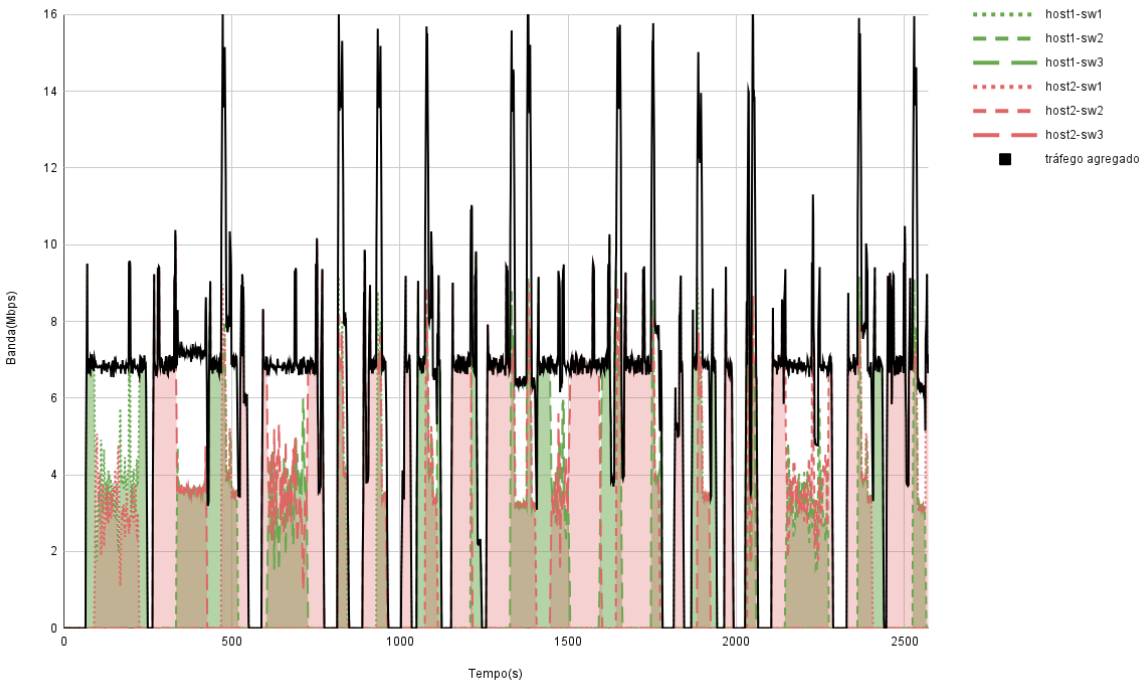


Figura 19 – Validação do controle de excesso com portabilidade com 2 dispositivos e 3 SwCB.

Como pôde ser visualizado na Figura 19 , em teste envolvendo controle de excesso e mobilidade o sistema se comportou como esperado, promovendo as duas condições, permitindo a mobilidade entre sítios distribuídos e prevenindo excessos.

4.2.6 Validação da eficiência do algoritmo controlador de banda

Os testes aqui apresentados têm como objetivo principal testar a eficiência do algoritmo controlador de banda. Para isso, foi feita uma comparação entre um primeiro caso onde dois fluxos são controlados por um mesmo *meter*, sem qualquer manipulação do algoritmo controlador de banda, e um segundo caso onde estes mesmos fluxos atravessam *meters* distintos em distintos SwCB. A intenção do teste é verificar se o algoritmo consegue manipular os dois SwCB de forma a obter um desempenho semelhante ao dos fluxos controlados por um mesmo *meter*.

Para esses testes, foram criadas diferentes cargas de trabalho para validação. A carga de trabalho define um padrão de fluxos que pode ser replicável através de script. Esse padrão pode ser entendido como uma sequência de downloads de arquivos via protocolo *http*, programados para serem executados em *hosts* específicos e em tempos específicos.

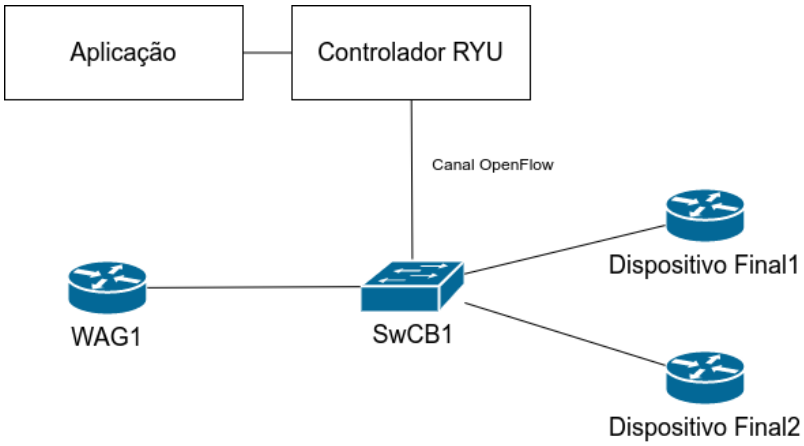


Figura 20 – Protótipo C4 - Modelo MR. dispositivos finais pertencem ao mesmo CONTRATO, i.e., compartilham a mesma banda. Além disso, ambos têm seus fluxos controlados pelo mesmo *meter* no mesmo SwCB.

Dois padrões de fluxos foram criados e suas características mostradas na TABELA 6. Para explicar a criação dos padrões de fluxos, vamos detalhar o PdF1, que é composto por um arquivo principal, ArquivoPrincipal, de 80Mbits, que será usado para criar o fluxo entre um WAG e um dispositivo final 1. Um arquivo secundário, ArquivoSecundario, de 8Mbits será usado para fluxos entre um WAG e o dispositivo final 2. A banda configurada no *meter* (bm) em todas rodadas é de 500Kb/s. O tc é o tempo de conclusão do download do ArquivoPrincipal, e, durante este tempo, será executado no teste o download do ArquivoSecundario por três vezes, de forma que a conclusão desses downloads secundários nunca ocorra após o tc do ArquivoPrincipal.

Aplicando um PdF ao protótipo C4 apresentado na Figura 20 durante 10 rodadas, obtém-se o tempo de conclusão médio do teste tc_{C4}. O mesmo é feito no protótipo C3 apresentado na Figura 21, obtendo o tempo (tc_{C3}). Feito isso, os tempos obtidos são comparados.

Tabela 6 – Características dos padrões de fluxos PdF1 e PdF2.

Parâmetros dos padrões de fluxos:	PdF1	PdF2
ArquivoPrincipal	80Mb	400Mb
ArquivoSecundario	8Mb	80Mb
BandaMeter	500Kb/s	500Kb/s
TempoEstimadoDownloadArquivoPrincipal	164s	819s
TempoColetadoDownloadArquivoPrincipal	162s	811s
TempoEstimadoDownloadArquivoSecundario	16,38s	164s
TempoColetadoDownloadArquivoSecundario	15s	162s
QuantidadeVezesDownloadPrincipal	1	1
QuantidadeVezesDownloadSecundario	3	2
SomaTamanhoTodosDownloadNoTeste	13M	70M
TempoEstimadoTeste	213s	1147s
AtrasoInicioDownSecudario	10s	10s
IntervaloInicioDownSubsequente	50s	50s
Tempo de conclusão (tc)	212s	1107s

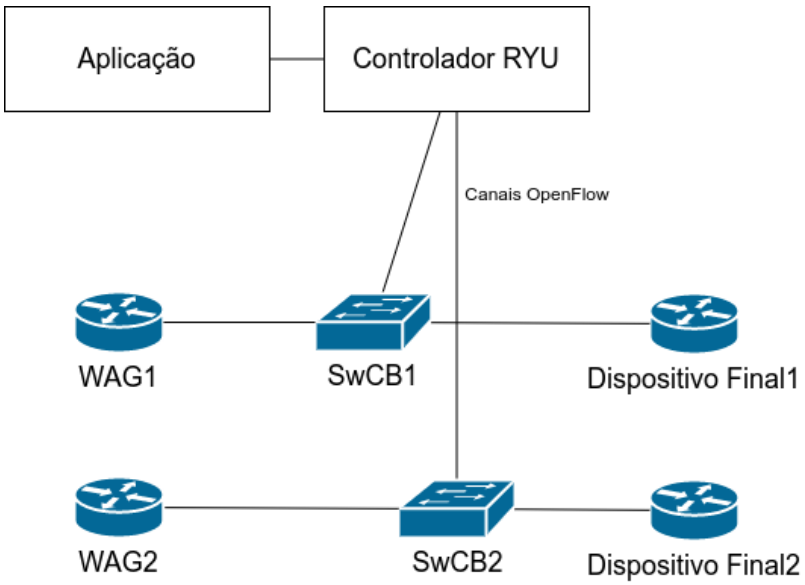


Figura 21 – Protótipo C3 – Modelo M. dispositivos finais pertencem ao mesmo CONTRATO, i.e., compartilham a mesma banda. Entretanto, seus fluxos são controlados por *meters* em SwCB distintos.

Depois de coletado o tc do PdF usando C4 (tc_C4) e o tc do PdF usando M (tc_C3), calcula-se o indicador de eficiência (IE) que é a razão entre $\frac{tc_C4}{tc_C3}$. Neste indicador, quanto mais próximo o valor estiver de 1 (um), mais próximo estará o desempenho do modelo proposto em relação ao modelo de referência. Nos testes a variável independente (t) é o intervalo de leitura de *meters* requisitado pela aplicação.

Os resultados obtidos para este teste podem ser visualizados na Figura 22. Este teste demonstrou que a eficiência do algoritmo, de forma geral, é melhor em fluxos de maior duração. Fluxos de menores durações têm eficiência relativamente melhores apenas em intervalos de monitoramento entre 0,4s $<$ t $<$ 2s. Compreendendo o significado

desse resultado juntamente com o resultado da Validação da ausência de interferência da leitura/manipulação dos *meters* em relação ao plano de dados, é possível concluir que ao combinar algoritmo e arquitetura (protótipo), obtém-se maior eficiência em fluxos de maior duração. Por outro lado, intervalos de monitoramento t < 30 podem gerar um efeito inverso no controle de fluxo.

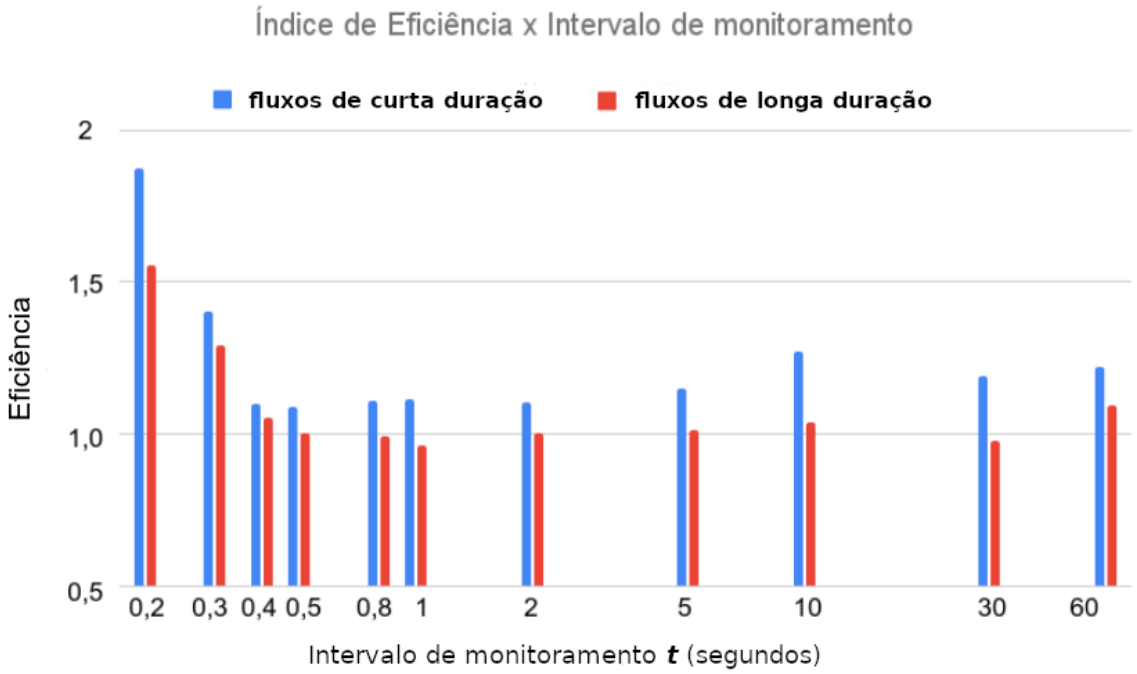


Figura 22 – Fluxos de curta duração com PdF1 e longa duração com PdF2

4.3 Considerações finais sobre os resultados

Após análise dos testes apresentados, entendemos que um significativo passo foi dado em direção à validação das soluções propostas. A Validação da capacidade de transferência útil do protótipo e a Validação da ausência de interferência da leitura/manipulação dos *meters* em relação ao plano de dados, como testes de calibração e sanidade, nos concederam um limite máximo de 10 Mb/s nas taxas de transferência de dados agregada interna nos demais testes do protótipo. E também, um limite mínimo de 30 segundos no intervalo de manipulação de um *meter* podendo acarretar um comportamento inverso no controle de banda do mesmo caso este limite seja ignorado. Estes limites são válidos apenas para nosso protótipo.

A Validação do controle de excesso, Validação da portabilidade de contrato e Validação do controle de excesso com portabilidade de contrato, como testes funcionais, simulam casos, elementares e em menor escala, de cenários reais nos entregando resultados dentro do esperado sobre a funcionalidade da portabilidade de contrato e controle de

excesso.

Durante o estudo e implementação do trabalho, uma vez alcançado o entendimento do impacto do intervalo de leitura/manipulação dos *meters* na precisão e no tempo de resposta da solução, intervalos cada vez menores foram buscados, desejando aumento na precisão e diminuição do tempo de resposta do sistema. Porém, a Validação da ausência de interferência da leitura/manipulação dos *meters* em relação ao plano de dados, nos trouxe uma compreensão importante relacionada a altas frequências de manipulação de *meters*, podendo inclusive fazer com que o sistema se comporte de maneira oposta a esperada, deixando de controlar banda e gerando excessos. Isto acabou motivando o desenvolvimento de uma de nossas validações mais importantes, a Validação da eficiência do algoritmo controlador de banda, que nos concedia uma quantificação dos excesso em determinados testes. Estas duas validações combinadas nos levaram a conclusão mais importante do trabalho: o sistema tende a uma melhor eficiência conforme aumenta a duração média dos fluxos e que intervalo de manipulação de *meters* menor do que 30 segundos pode gerar um efeito inverso no controle de fluxo.

5 Conclusão e Trabalhos Futuros

As opções atuais sobre Redes de Wi-Fi comunitário oferecem mobilidade em troca de um ambiente propício a injustiças no compartilhamento de tráfego entre clientes participantes e provedores. Além disso, especificamente sobre este tema, ainda existe carência em soluções encontradas usando redes programáveis ou outras tecnologias mais recentes.

Este trabalho apresentou um sistema baseado no padrão SDN como instância especializada para Wi-Fi comunitário adicionando *meters*, implementado em *openflow* e RYU que são tecnologias de fácil acesso no mercado. Este sistema de controle de banda distribuído, que integra uma aplicação e um algoritmo especializado, possibilita a portabilidade do perfil de plano contratado, além da reduzir excessos no tráfego global entre usuários em sítios distintos. Por fim, um protótipo emulado como ambiente para validação experimental foi apresentado.

Como pôde ser observado nos resultados da validação experimental, o sistema alcançou a portabilidade do perfil de plano contratado. Além disso, o tráfego compartilhado entre usuários emulados em testes distribuídos simulando vários sítios foi controlado de forma bem próxima dos testes centralizados como se os usuários estivessem em um mesmo sítio. Esta comparação é feita com base numa metodologia comparativa que demostrou uma eficiência que aumenta conforme aumenta a duração media dos fluxos.

Como trabalhos futuros evoluções e melhorias são necessárias como: suporte QoS, escalabilidade, interação entre provedores, avanços em interfaces de gerenciamento como WEB, integração com RADIUS, desenvolvimento de WAGs em VNFs, melhorias na limpeza de meters inativos, melhorias na coleta de contratos e leituras de meters que podem ser feitas por demanda ao invés de forma totalitárias, entre outros.

Referências

AI, X.; SRINIVASAN, V.; THAM, C.-K. Wi-sh: A simple, robust credit based wi-fi community network. In: IEEE. *IEEE INFOCOM 2009*. [S.l.], 2009. p. 1638–1646. Citado na página 33.

ASHERALIEVA, A.; ERKE, T. J.; KILKKI, K. Traffic characterization and service performance in fon network. In: IEEE. *2009 First International Conference on Future Information Networks*. [S.l.], 2009. p. 285–291. Citado na página 32.

BELLALTA, B. Ieee 802.11 ax: High-efficiency wlans. *IEEE Wireless Communications*, IEEE, v. 23, n. 1, p. 38–46, 2016. Citado na página 24.

CARREL, D. et al. *A Method for Transmitting PPP Over Ethernet (PPPoE)*. RFC Editor, 1999. RFC 2516. (Request for Comments, 2516). Disponível em: <https://rfc-editor.org/rfc/rfc2516.txt>. Citado na página 24.

DOURADO, G.; MARTINELLO, M.; VILLAçA, R. Controle de banda global em sítios distribuídos para portabilidade de acesso à redes wi-fi comunitárias. In: *Anais do XXV Workshop de Gerência e Operação de Redes e Serviços*. Porto Alegre, RS, Brasil: SBC, 2020. p. 223–234. ISSN 2595-2722. Disponível em: <https://sol.sbc.org.br/index.php/wgrs/article/view/12463>. Citado na página 36.

GANTI, V. *Community Wi-Fi – A Primer*. [S.l.], 2014. Citado 2 vezes nas páginas 15 e 24.

INTEL. *New Approach to Delivering Secure Community Wi-Fi*. [S.l.], 2018. Citado 4 vezes nas páginas 15, 23, 35 e 36.

JANG, H.-C.; LIN, J.-T. Sdn based qos aware bandwidth management framework of isp for smart homes. In: IEEE. *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. [S.l.], 2017. p. 1–6. Citado 3 vezes nas páginas 15, 34 e 35.

Kreutz, D. et al. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, v. 103, n. 1, p. 14–76, 2015. Citado 3 vezes nas páginas 25, 29 e 40.

LIBERATO, A. et al. Dynamic backhauling within converged networks. In: *Proceedings of the 2016 workshop on Fostering Latin-American Research in Data Communication Networks*. [S.l.: s.n.], 2016. p. 31–33. Citado na página 35.

MCKEOWN, N. et al. Openflow: enabling innovation in campus networks. *ACM SIGCOMM computer communication review*, ACM New York, NY, USA, v. 38, n. 2, p. 69–74, 2008. Citado na página 37.

OI. *Oi Wi-Fi FON*. 2021. <http://oiwifi.com.br/howitworks>. [Online; acessado em 08/06/2021]. Citado na página 25.

RAGHAVAN, B. et al. Cloud control with distributed rate limiting. *SIGCOMM Comput. Commun. Rev.*, Association for Computing Machinery, New York, NY, USA, v. 37, n. 4, p. 337–348, ago. 2007. ISSN 0146-4833. Disponível em: <https://doi.org/10.1145/1282427.1282419>. Citado 2 vezes nas páginas 27 e 33.

SCHULZ-ZANDER, J. et al. Programmatic orchestration of wifi networks. In: *2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14)*. [S.l.: s.n.], 2014. p. 347–358. Citado 2 vezes nas páginas 23 e 24.

SHELBY, Z. *Constrained RESTful Environments (CoRE) Link Format*. RFC Editor, 2012. RFC 6690. (Request for Comments, 6690). Disponível em: <https://rfc-editor.org/rfc/rfc6690.txt>. Citado na página 37.

The Open Networking Foundation. *OpenFlow Switch Specification*. 2012. Citado 4 vezes nas páginas 15, 26, 30 e 31.

Apêndices