Controle de banda global em sítios distribuídos para portabilidade de acesso à redes Wi-Fi comunitárias

Glauber L. Dourado[1], **Magnos Martinello**[1],
Rodolfo S. Villaça[1]

[1] Núcleo de Estudos em Redes Definidas por Software (Nerds)
Universidade Federal do Espírito Santo (Ufes) – Vitória/ES – Brasil

glauber.dourado@gmail.com

Abstract. *Public Wi-Fi and Community Wi-Fi proved to be a great option to attract new customers and keep them within internet service providers infrastructure. Residential hotspots or "homespots"offer an excellent infrastructure with a large number of small cells of high capacity, low range, and high density mainly in urban environments. Internet access management in distributed software-defined networks still lacks ready-to-use architectures for specific cases such as Community Wi-Fi. This article presents an architecture for management and control of community Wi-Fi access, and the implementation of an aggregated traffic controller to devices from users sharing the same contract, even though they are geographically distant and connected to remote residential homespots. In this way, a user can have a certain degree of pervasive access by connecting to any homespot within the community and have the same permission to access the band as if he/she was inside his/her own home. The solution was implemented using Openflow, Ryu controller, and a python orchestrator sending messages to the controller via REST API.*

Resumo. *O Wi-fi Público e o Wi-Fi comunitário se mostram como ótimas opções para promover novas adesões e retenção de clientes dentro dos provedores de internet. Os roteadores Wi-Fi residenciais oferecem uma excelente infraestrutura com um grande número de pequenas células de alta capacidade, baixo alcance e alta densidade, principalmente em ambientes urbanos. O gerenciamento de acesso à internet em redes distribuídas definidas por software ainda carece de arquiteturas prontas para uso em casos específicos como em Wi-Fi Comunitário. Este artigo apresenta uma arquitetura de gerenciamento e controle de acesso para Wi-Fi comunitário, bem como traz a implementação de um controlador de tráfego agregado entre dispositivos participantes de um mesmo contrato, permitindo que estes estejam geograficamente distantes e conectados a distintos pontos de acesso residenciais. Desta forma, um usuário pode ter certo grau de acesso ubíquo e pervasivo, conectando-se a um ponto de acesso qualquer dentro da comunidade, e com o mesmo acesso à banda como se estivesse dentro de sua própria residência. A solução foi implementada utilizando o protocolo Openflow, controlador Ryu e um orquestrador em Python, que comunica com o controlador via API REST.*

1. Introdução

A quantidade de pontos de acesso Wi-Fi públicos tende a alcançar, nos próximos 3 anos, o patamar de 628 milhões no mundo todo, com 429 milhões a mais do que em 2018

[CISCO 2020]. O Wi-Fi público tem fornecido acesso à Internet em uma ampla variedade de locais como shoppings, aeroportos, praças públicas, dentre outros. Recentemente o Wi-Fi tem ganhado um novo aliado, o modelo conhecido como Wi-Fi comunitário, que permite a seus usuários privados (e.g., assinantes de Internet banda larga fixa de um provedor) disponibilizar parte da sua conexão residencial para o uso da comunidade, i.e., para o uso de outros assinantes do mesmo provedor.

Há poucos anos, o Wi-Fi comunitário era tratado como um problema na visão do provedor. No entanto, percebendo os avanços no acesso à internet e também compreendendo as necessidades do mundo moderno, esse modelo de negócio vem sofrendo transformações, e estudos apontam que este pode vir a ser peça chave para o futuro [Micholia et al. 2018]. Para melhor entender esse cenário considere os seguintes casos: um conjunto de quatro moradores, cada um representando uma residência, formando uma comunidade como apresentada na região alaranjada da Figura 1-a. Essa comunidade contrata um plano com um provedor, e este instala equipamentos em uma das quatro residências. Feito isso, a comunidade compartilha por conta própria o acesso via Wi-Fi entre as residências remanescentes, rateando os custos com equipamentos e mensalidades. Com isso, temos quatro residências compartilhando o acesso à Internet proveniente de um único contrato com o provedor, o que não é muito vantajoso. Nesse caso, o que é interessante para o provedor é vender um contrato por morador representante de cada casa. Considere agora um novo modelo de Wi-Fi Comunitário, representado na Figura 1-b. Nessa, há usuários comunitários que possuem acesso à estrutura de rede da comunidade. Tais usuários têm liberdade de sair de suas casas e ter seu acesso, inclusive nas residências de outros assinantes, sem requerer novas autenticações (e.g., reinserir usuário e senha). Para isso, tecnologias são necessárias para garantir a segurança e o isolamento desses acessos. Nesse segundo modelo, o provedor passa a investir também em Wi-Fi públicos, como *hotspots* em restaurantes, aeroportos, praias e certos locais públicos, que, juntos com os *homespots*, aumentam a cobertura do acesso para usuários da comunidade [Ganti 2014].

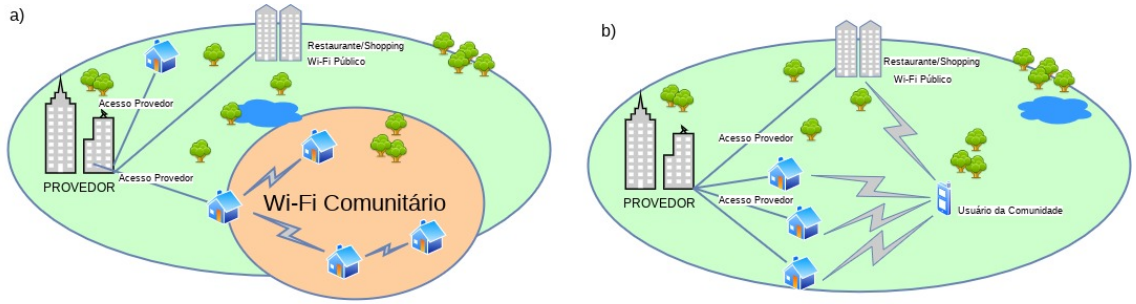

Figura 1. Duas formas de abordagem do Wi-Fi Comunitário

O conjunto de roteadores ou pontos de acesso residenciais habilitados para o Wi-Fi comunitário (*homespot*) pode proporcionar aos usuários de Internet fixa, restritos antes ao uso apenas em suas residências, ganhos em mobilidade, colocando-os em melhores condições de utilização, assemelhando-os a usuários de 5G móvel, que já possuem nativamente esta funcionalidade.

Atualmente, a gerência do Wi-Fi comunitário ainda é feita no próprio *homespot*. Dessa forma, cada usuário precisa acessar o seu equipamento e executar configurações como: padrões de segurança, autenticação e limitação da largura de banda para o usuário da comunidade. Além disso, controle de banda para um usuário da comunidade em um *homespot* é feito em função da largura de banda disponível de um usuário privado. Essa realidade pode ser melhorada com o desenvolvimento de um controle de banda global, capaz de fazer com que a largura de banda disponibilizada pelo provedor para um usuário da comunidade migre com ele quando conectado a uma rede comunitária fora de sua residência. Isso garante a portabilidade do plano do usuário, e deve ser feito sem que interfira na largura de banda contratada de um usuário privado que possa estar cedendo sua infraestrutura para o Wi-Fi comunitário. A banda de um usuário pode ser compartilhada entre um grupo específico, e pré-estabelecido, de dispositivos, chamado de *contrato*. Para isso, é desejável uma arquitetura que viabilize a gerência de todas essas conexões de usuários, privados e comunitários, e as manipule globalmente, possibilitando a organização e o compartilhamento justo.

Nesse trabalho, uma solução de portabilidade de acesso à rede comunitária é apresentada, incluindo uma arquitetura funcional que beneficie a gerência e controle, bem como a implementação de um controle de banda distribuído.

1.1. Trabalhos Relacionados

Existe um grande interesse por parte das empresas em Wi-Fi comunitário. Em [Micholia et al. 2018], os autores apresentam a influência, nas últimas duas décadas, do Wi-Fi comunitário nos paradigmas de construção, manutenção e compartilhamento de infraestruturas. Relata também que todos estes paradigmas de redes comunitárias convergem em um desafio em comum: a sustentabilidade. O foco do artigo está nas múltiplas, muitas vezes complementares, maneiras pelas quais diferentes iniciativas da redes comunitárias buscam sua sustentabilidade, dentro do contexto econômico, sociocultural e político. Quanto a questões técnicas e tecnológicas, o artigo usa referencias externas que porventura são da primeira década do século atual. Esse distanciamento entre o interesse moderno e atual das redes comunitárias e as datas das soluções encontradas para redes comunitárias são motivadores adicionais na realização do presente artigo. Além disso, o relacionamento entre cidades inteligentes e Wi-Fi comunitário é bastante vantajoso, pois as cidades inteligentes demandam acesso ubíquo a uma infinidade de dispositivos, fazendo com que a estrutura do Wi-Fi comunitário contribua para essas operações, principalmente em ambientes urbanos e densos de pontos de acessos. Em [Yucel 2018], o autor aborda questões como: quem deveria pagar a conta fornecida por acesso comunitário em cidades inteligentes, uma vez que o acesso de um dispositivo pode atravessar a estrutura de um assinante de um provedor ou operadora? Na solução proposta nesse artigo essa questão seria irrelevante, pois cada dispositivo pertence a um contrato e tem disponível exclusivamente a sua banda contratada, mesmo usando a infraestrutura de outro usuário.

Nos lares, o uso de múltiplos roteadores e extensores de sinais que ampliam a cobertura de sinal traz vantagens tanto para usuários do lar quanto para entrega de Wi-Fi para a comunidade. Essa configuração é vulnerável a violações de segurança, pois padrões de segurança como o acesso protegido ao Wi-Fi WPA2 têm sua proteção limitada entre o dispositivo do cliente e o roteador. Já entre o roteador e o conversor ou modem de acesso, há uma lacuna de proteção, em que o dono da rede privada pode ter acesso às

informações da rede pública ou da comunidade. Para tratar esse problema, [INTEL 2018] apresenta uma proposta na qual a proteção do WPA2 se estende fora do domínio da rede sem fio e atravessa a rede cabeada ou fibra até a nuvem no provedor. Dessa forma, tanto redes privadas como públicas estariam protegidas, evitando ataques por esse tipo de falha. 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.

Em [Ai et al. 2009], é apresentada uma solução que requer troca do *firmware* dos roteadores dos clientes, e oferece bonificação para clientes que disponibilizam sua banda para a comunidade. No entanto, apesar da bonificação garantir que esse cliente não tenha sua banda reduzida ao fornecer estrutura para a rede comunitária, essa proposta não garante portabilidade da banda do usuário, enfraquecendo a ubiquidade da proposta.

1.2. Contribuições

Nesse contexto, o objetivo principal desse trabalho é propor uma solução para o controle de banda distribuído para usuários de uma rede Wi-Fi comunitária. Para alcançar esse objetivo este artigo apresenta a implementação de um sistema de gerenciamento e controle de banda distribuído para uma rede Wi-Fi comunitária. Além disso, o algoritmo de um limitador de banda distribuído é apresentando, viabilizando o controle de banda para N dispositivos participantes de um contrato com portabilidade dentro de uma rede comunitária. A solução proposta foi avaliada em ambiente simulado através do software GNS3 (Graphical Network Simulator-3), utilizando máquinas virtuais Linux e roteadores Mikrotiks. A solução incrementa a capacidade de gerenciamento de modo inovador ao utilizar dispositivos de rede programáveis por meio do protocolo OpenFlow que atuam como classificadores e encaminhadores de pacotes, controlador SDN (Software Defined Networking) e um orquestrador implementado em Python.

Este trabalho está organizado da seguinte forma. A Seção 1.1 apresenta trabalhos relacionados já presentes na literatura. A Seção 2 apresenta a proposta completa, a arquitetura e o limitador de banda, bem como seus respectivos componentes. Detalhes de implementação dos algoritmos são descritos na Seção 3. Na Seção 4, a validação da proposta é apresentada. Por fim, a Seção 5 traz as conclusões e propostas de trabalhos futuros.

2. Arquitetura de Controle para Acesso em Redes Wi-Fi Comunitárias

Esta seção apresenta detalhes sobre a arquitetura proposta para a utilização de redes comunitárias em um provedor de Internet, e também a implementação de um limitador de banda agregada disponível para um grupo de dispositivos distribuídos.

2.1. Arquitetura

A base estrutural da arquitetura proposta é a execução de todas as operações exclusivamente em L2, lidando apenas com agrupamento de endereços de controle de acesso ao meio (MAC) de origem e destino, e sua interação com os *meters*. No caso, o MAC de origem e destino são chaves de identificação do fluxo referente a um dispositivo que será associada a um *meter* e, consequentemente, a um plano contratado. Como toda operação

de autenticação e controle de banda não usa endereços IP , o L3 se torna bastante simples e livre, podendo inclusive ser implementado numa simples sub-rede IP. Algumas abstrações e métodos precisaram ser implementados para segregar o L2 e garantir a organização, controle e isolamento do sistema. Essas abstrações e métodos serão apresentados nas subseções a seguir.

2.1.1. Abstrações

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 dispositivos é fonte de inspiração para uma fundamental abstração da arquitetura 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.

Uma segunda abstração é a *célula*, que é a área de alcance útil de um ponto de acesso, ou *homespot*, específico. É o local onde usuários da comunidade podem ter seu acesso compartilhado, e esse pode fazer parte de uma residência ou de um lugar público. Assim, pode-se dizer que dois dispositivos pertencentes a um contrato podem estar acessando uma única célula (mesma residência), ou cada dispositivo está em uma célula distinta (cada um em sua própria residência).

A síntese desse conjunto de abstrações e alguns elementos concretos é demonstrada na Figura 2. Na parte superior é possível observar dois exemplos de *contratos*, o contrato 1 e o contrato 2. Esses estão relacionados respectivamente às *células* 100 e 200. Cada contrato contém quatro dispositivos dentro do escopo d1 a d8, e seus respectivos MACs são descritos por mac1 a mac8. Os dispositivos d1 e d5 são *master* de seus respectivos *contratos*, i.e., são os equipamentos que têm privilégios de administrador dentre os demais dispositivos.

A Figura 2 apresenta também um esboço de uma estrutura de Wi-Fi comunitário, evidenciando três *células* e possíveis composições internas. Dispositivos do contrato 1 estão representados na cor verde, enquanto dispositivos do contrato 2 estão na cor vermelha. Cada dispositivo apresenta basicamente 3 atributos: identificação, mac e condição (*home* ou *roam*). Assim, os atributos de identificação e mac são úteis para diferenciação dos dispositivos, enquanto a condição define se o dispositivo pertence ou não à esta célula, sendo a condição home significando que o dispositivo pertence à célula atual e a condição roam significando que o dispositivo não pertence à célula atual. Na proposta deste trabalho, dispositivos de mesmo contrato, representados na mesma cor, compartilham de forma justa a largura de banda contratada com o provedor.

O isolamento deve ser assegurado pelo *homespot*, pois, em função de sua posição dentro da topologia, possui a condição ótima para executá-lo. Dispositivos de um mesmo

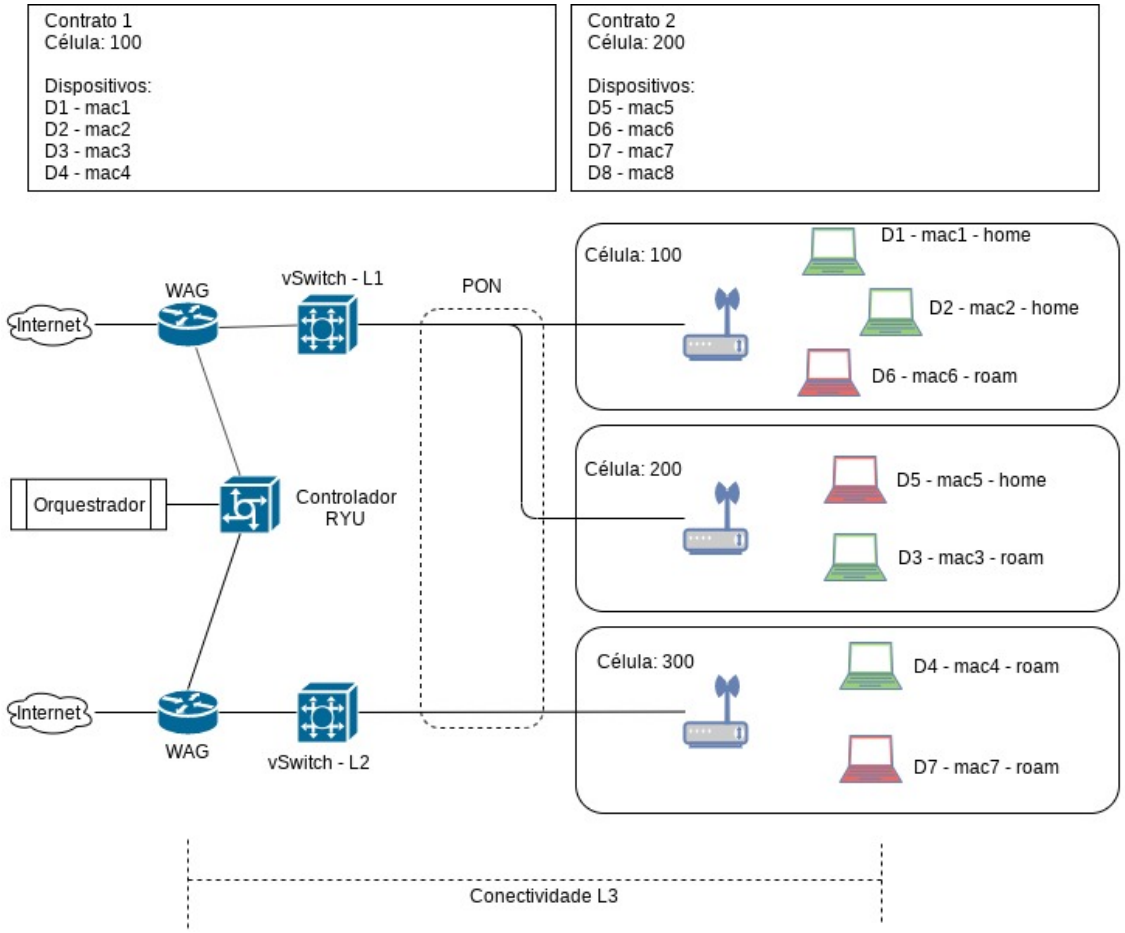

Figura 2. Arquitetura e abstrações de Wi-Fi comunitário.

contrato em modo local, ou seja, pertencentes à mesma célula, podem interagir, enquanto dispositivos de contratos diferentes em uma mesma célula não podem se comunicar.

2.1.2. Método de acesso aprimorado

Apesar do protocolo base para implementação de redes sem fio (IEEE 802.11), criado pelo Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE), não limitar a quantidade de *service set identifiers* (SSID) em um único ponto de acesso, roteadores Wi-Fi residenciais tradicionais costumam disponibilizar um limitado número de SSIDs (geralmente entre 1 a 5). Normalmente, roteadores disponibilizam dois SSIDs apenas, um primário ou *privado* e um secundário ou *visitante*. Algumas empresas utilizam o SSID visitante para entregar acesso de Wi-Fi comunitário. É comum o uso de políticas de qualidade de serviço (QoS) aplicadas para separar parte da banda total da interface sem fio para o SSID visitante [Maccari and Lo Cigno 2014]. Dessa forma, divide-se a banda em apenas duas classes, uma total e outra com parte deste total (e.g., 20% para o SSID visitante). O número total de classes nesses equipamentos fica a critério do fabricante e da configuração no próprio equipamento.

Com o método proposto de autenticação aprimorado apenas um SSID é ne-

cessário. Isso pois, uma vez que o dispositivo é autenticado conforme padrão WPA2 e com a base de dados no servidor por *Remote Authentication Dial In User Service* (RADIUS), ele é identificado e associado ao *contrato* a que pertence. Dessa forma, é possível coexistir *N* classes de *contratos* simultaneamente gerenciados globalmente pelo RADIUS ou outra base de dados que possa vir a ”alimentar”o RADIUS.

2.1.3. Limitador de banda aprimorado

Na Figura 2, os elementos identificados como vSwitch são os limitadores de banda. A principal diferença desses elementos para os limitadores de banda tradicionais é a utilização de um *meter* ao invés de um *queue* para limitar a banda.

O limitador de banda aprimorado pode atuar em um grupo selecionável de dispositivos. Por exemplo, pode-se selecionar subconjuntos de um conjunto de endereço MACs e limitar a banda dos dispositivos participantes desses subconjuntos independentemente. Tudo isso ocorre dinamicamente, seguindo um modelo de processo baseado em identificação, classificação e controle. Além disso, dispositivos podem entrar e sair dos subconjuntos a qualquer momento.

Outra característica do limitador de banda aprimorado está na capacidade de limitar a banda em dois sentidos. Enquanto um limitador de banda tradicional trabalha com duas *queues*, uma para entrada (*ingress*) e outra para saída (*egress*), o limitador aprimorado compartilha a mesma banda para entrada e saída. No escopo deste trabalho, o termo sítios ou *sites* limita-se à locais ou lugares que possuem ao menos um *switch* limitador de banda.

2.1.4. Controle e Orquestração

Com o controle de banda global, *N* dispositivos pertencentes a um contrato podem localizar-se em diferentes residências e acessando a Internet por diferentes *links*. Cada dispositivo precisa respeitar a banda total contratada, *B*. Se os *N* dispositivos gerarem fluxos simultaneamente teremos momentaneamente uma banda agregada *A*, que pode alcançar $A = N \times B$, extrapolando em muito a banda contratada, gerando prejuízo ao provedor de Internet. A função principal deste controle é não permitir que isso ocorra, identificando cada dispositivo e classificando, de acordo com seu contrato, a largura de banda disponível.

Figura 3. Comunicação entre elementos básicos da arquitetura.

A comunicação entre os elementos básicos da arquitetura é demonstrada na Figura 3. O controlador Ryu recebe sinais do orquestrador e os envia para os switches limitadores de banda. Entre o controlador e os switches a comunicação é feita através do protocolo OpenFlow. A comunicação entre o controlador e o orquestrador optou-se por uma comunicação utilizando a arquitetura REST. A escolha por arquitetura REST se

deve ao fato dessa possuir características interessantes no quesito segurança, habilitando a coexistência entre tecnologias como HTTPS, SSL, algoritmos de hashing, OAuth, dentre outras.

3. Implementação

A implementação foi feita conforme especificações existentes na Seção 2. Para testar a implementação e demonstrar a viabilidade da proposta, simulações foram realizadas usando tecnologias virtualizadas amplamente utilizadas em muitos provedores de Internet.

Para simulação foi utilizado o GNS3 na versão 0.87, executando o QEMU 4.1.0 com imagens reais de roteadores commodities Mikrotik RouterOS versão 6.34.4 como *homespots*. VMs Linux Ubuntu 19.10 foram usados como limitadores de banda executando o *Open vSwitch 2.12.2* e o *DB schema 8.0.0*. Na máquina hospedeira, que executa o GNS3, foi instalado o Ryu 4.32 como controlador *Openflow* na versão 1.3 e a interface REST. De forma similar ao controlador Ryu, o orquestrador foi executado, sendo este uma aplicação em Python 3.7 que envia mensagens no formato JSON para o controlador Ryu.

3.1. Controlando banda em múltiplos sítios

Nesta subseção são apresentados detalhes da implementação do limitador de banda aprimorado. Como apontado na Seção 2.1.3, o objetivo é controlar um conjunto de limitadores de banda distribuídos para distribuir igualitariamente a banda contratada entre dispositivos pertencentes aos respectivos contratos.

Ao receber pacotes de fluxos não classificados, o limitador de banda aprimorado executa o *packet-in*, requisitando do controlador a instrução de qual ação deve tomar em relação aos próximos pacotes pertencentes a este fluxo. Por sua vez, o controlador, em conjunto com servidor RADIUS e o orquestrador, classifica este fluxo associando-o a um *meter* exclusivo para o respectivo contrato. Quando fluxos pertencentes a um mesmo contrato vindos de células diferentes atravessam o mesmo *switch* limitador de banda, a ação é associar todos os fluxos envolvidos a um mesmo *meter*. No entanto, quando estes fluxos se encontram em *switches* diferentes, é necessária a ação do algoritmo de controle igualitário desses *meters* localizados em *switches* distribuídos.

É função do orquestrador distribuir de forma igualitária a banda de dispositivos localizados em células com limitadores de bandas distintos. 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 conforme os dispositivos deixam de consumir a banda.

Para possibilitar a criação de regras para atender as premissas descritas acima, um modelo matemático foi desenvolvido. Denota-se X_i como a taxa atual de banda configurada igualmente para todos os *meters* ativos pertencentes a um mesmo contrato. X_{i-1} é a

taxa anterior desta mesma variável. B é a banda contratada. A é a somatória da vazão Z_m atual de cada *meter* (m) ativo, e Q é a quantidade total de *meters* ativos. Portanto,

$$X_i = X_{i-1} + \delta, \tag{1}$$

sendo,

$$\delta = (\frac{1}{2})\frac{B - A}{Q} \tag{2}$$

$$A = \sum_{m=0}^{Q} Z_m \tag{3}$$

e,

$$\delta = 0 \quad \text{se} \quad (B - A) = 0 \tag{4}$$

$$X_i = B \quad \text{se} \quad A < \frac{9}{10}B \tag{5}$$

O principal mecanismo do modelo é que, a cada iteração, X_i vai se ajustando e tendendo a $X_i = \frac{B}{Q}$. O modelo tende a atuar apenas quando $A > B$, 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 $A < B$, não há prejuízo, independente da proporção utilizada por cada dispositivo. Neste caso, todos os *meters* retornam para situação inicial $X_i = B$, deixando a banda inteiramente disponível. A exceção $X_i = B$ se $A < \frac{9}{10}B$ atua como um suavizador, evitando oscilações indesejadas na banda disponível causadas por pequenas flutuações de tráfego de dados próximos ao limiar. O coeficiente $\frac{1}{2}$ utilizado no cálculo de δ também atua como um suavizador, evitando alterações bruscas na banda agregada.

4. Validação da Proposta

A validação da proposta foi realizada com o objetivo de verificar experimentalmente a capacidade do algoritmo em distribuir igualitariamente a banda entregue aos dispositivos em sítios distintos.

4.1. Validação experimental

Todos os testes foram executados utilizando o mesmo ambiente de simulação descrito na Seção 3, e exibido na Figura 2. Dois testes foram implementados para testar a distribuição igualitária em sítios distintos.

Nos testes de distribuição T1 e T2 o objetivo é o mesmo, avaliar como o algoritmo compartilha a banda entre dois fluxos totalmente separados, i.e., que não atravessam em nenhum momento o mesmo enlace nem o mesmo equipamento. Para isso, dois fluxos TCP foram gerados com o *Bandwidth Test*, que é uma ferramenta nativa em *Routerboards* da Mikrotik. Cada um desses fluxos (Figura 4) tem como destino os dispositivos D6 ou D7, e como origem o seu respectivo WAG, atravessando apenas seu respectivo switch.

O *Bandwidth Test* possui vários parâmetros para personalizar o teste, dois deles são o *local-tx-speed* e o *remote-tx-speed*. Com eles é possível estipular a largura de

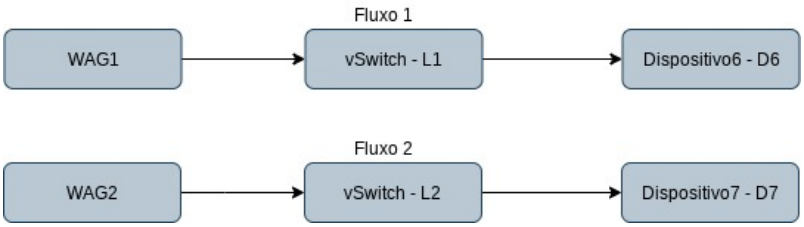

Figura 4. Fluxos nos testes de distribuição igualitária.

banda máxima almejada no fluxo gerado. A diferença entre elas é o sentido do tráfego gerado(*download* ou *upload*). Se os valores destes parâmetros ficarem em branco , a velocidade é controlada pelo protocolo *TCP*, tornando-se gradativamente crescente enquanto houver capacidade de banda disponível no enlace.

No teste de distribuição T1, dispõe-se 5 Mbps de banda compartilhada entre os dois fluxos. Esses foram gerados com o parâmetro *local-tx-speed* em branco, deixando a banda passante exclusivamente por conta do L1 ou L2. Na simulação, dois usuários estariam disputando toda a banda disponível. O objetivo de T1 é validar a capacidade do algoritmo em evitar que a soma dessas bandas ultrapasse o valor de 5 Mbps estipulado.

No teste de distribuição T2, o fluxo com destino D6 foi configurado com o parâmetro *local-tx-speed* em branco. Porém para os fluxos com destino D7, três valores para o parâmetro *local-tx-speed* foram introduzidos sequencialmente, 500, 1000 e 2000 Kbps. Nessa simulação, um usuário tentaria usar toda a banda disponível e um outro tentaria usar apenas uma pequena fração da banda. O objetivo de T2 é igual o de T1. Porém a diferença entre eles é que um dos fluxos não tenta disputar toda a banda. O propósito adicional nesse teste é conhecer o comportamento do algoritmo em situações adversas que podem ocorrer na realidade.

4.2. Teste de distribuição igualitária T1

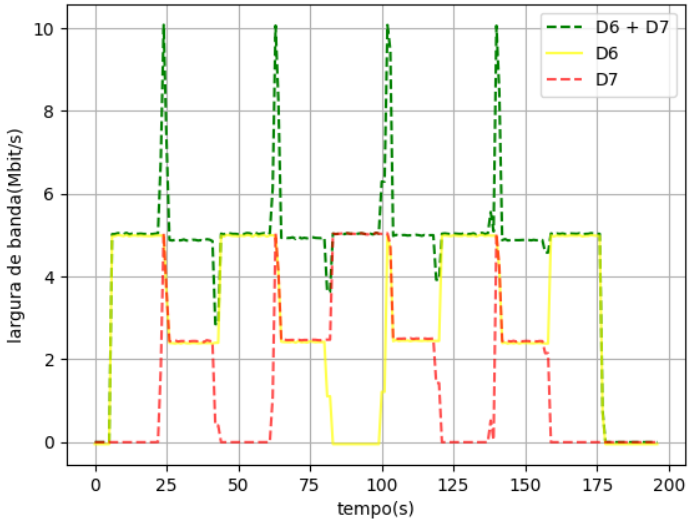

Figura 5. Controle de banda distribuído em 2 células.

Na Figura 5, pode-se visualizar que o fluxo com destino D6 foi acionado aos 5 segundos, tomando a banda total definida por L1 de 5 Mbps. Em sequência, aos 25 segundos foi acionado o fluxo para D7, controlado por L2, que inicialmente deixa a banda de 5 Mbps disponível, elevando a linha em verde tracejado, que representa a soma das bandas, para 10 Mbps.

Assim que o algoritmo detecta essa extrapolação, a correção pelo algoritmo proposto ocorre, setando ambos os limitadores L1 e L2 para 2,5 Mbps. Entre D6 e D7 o compartilhamento ocorreu como esperado. Durante o experimento, um dos fluxos foi propositalmente removido e reinserido de forma sucessiva, a fim de verificar a atuação dinâmica do algoritmo. É possível observar que o algoritmo reagiu como esperado, compensando igualitariamente a largura de banda em função do máximo valor possível estipulado.

4.3. Teste de distribuição igualitária T2

Como apresentado na Figura 6, inicialmente, o controle foi gerado com 500 Kbps, depois alterado para 1 Mbps e, por fim, 2 Mbps. É possível observar que o fluxo em D6 também reagiu da forma esperada, bem como é possível verificar que a soma manteve-se dentro do limite estipulado.

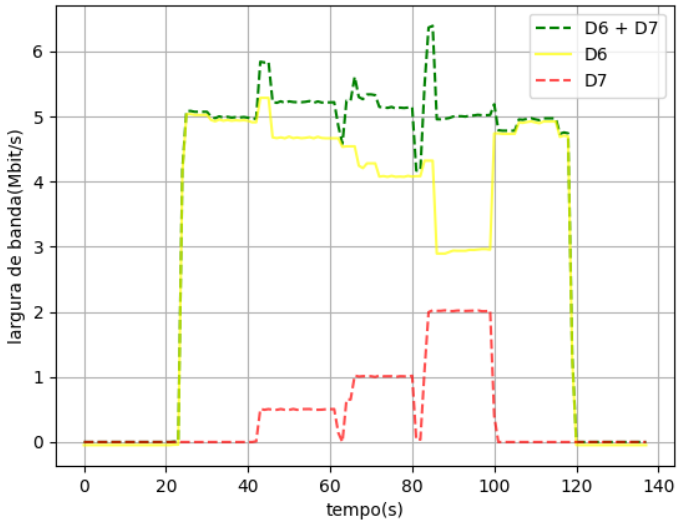

Figura 6. Banda pré-fixada no gerador em D7.

5. Conclusão e Trabalhos Futuros

Este artigo apresentou a proposta de uma arquitetura de controle de banda distribuída para redes Wi-Fi comunitárias, implementando um controlador de banda global, atendendo requisitos de compartilhamento e portabilidade. Além disso, um experimento foi realizado para validar os algoritmos propostos.

Conforme pôde ser observado nos resultados da validação, a arquitetura e algoritmos apresentados têm potencial para serem utilizados em novos modelos de negócios e serviços envolvendo Wi-Fi comunitárias. A significante ampliação na área de cobertura

do assinante, gerência centralizada, oferta de conectividade transparente e portabilidade do perfil contratado são parte das vantagens obtidas pela solução apresentada.

Como trabalhos futuros, pretende-se estender o suporte a garantias de QoS na interface Wi-Fi do cliente. Um outro caminho promissor é a integração entre provedores, onde o assinante de um provedor poderia compartilhar parte do contrato de outro assinante, estabelecendo-se portabilidade entre dispositivos conectados a diferentes provedores.

Agradecimentos

Gostaria de deixar aqui nossos sinceros agradecimentos a todos que contribuíram neste trabalho, principalmente a Francielle Matielo, Daniel Khéde e Luisa Khéde.

Referências

Ai, X., Srinivasan, V., and Tham, C. . (2009). Wi-sh: A simple, robust credit based wi-fi community network. In *IEEE INFOCOM 2009*, pages 1638–1646.

CISCO (2020). Cisco Annual Internet Report (2018–2023) White Paper. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html, acessado em:15/01/2020.

Ganti, V. (2014). Community Wi-Fi – A Primer. https://www.cablelabs.com/community-wi-fi-a-primer, acessado em:14/02/2020.

INTEL (2018). New Approach to Delivering Secure Community Wi-Fi. https://www.intel.com.br/content/www/br/pt/connected-home/deploying-cloud-based-wpa2-residential-hotspots.html, acessado em:15/01/2020.

Maccari, L. and Lo Cigno, R. (2014). A week in the life of three large wireless community networks. *Ad Hoc Networks*, pages –.

Martignon, F., Paris, S., Filippini, I., Chen, L., and Capone, A. (2013). Efficient and truthful bandwidth allocation in wireless mesh community networks. *IEEE/ACM Transactions on Networking*.

Micholia, P., Karaliopoulos, M., Koutsopoulos, I., Navarro, L., Baig Vias, R., Boucas, D., Michalis, M., and Antoniadis, P. (2018). Community networks and sustainability: A survey of perceptions, practices, and proposed solutions. *IEEE Communications Surveys Tutorials*, 20(4):3581–3606.

Yucel, S. (2018). Smart community wireless platforms: Costs, benefits, drawbacks, risks. In Çelebi, M. S., editor, *Recent Trends in Computational Science and Engineering*, chapter 5. IntechOpen, Rijeka.