

Aplicações Virtualizadas em Gateways Domésticos

Lucas Federici Matheus A. Cunha Ítalo Cunha

¹Departamento de Ciência da Computação
Universidade Federal de Minas Gerais

{cilf, mcunha, cunha}@dcc.ufmg.br

Abstract. *We present PUROMALTE, a virtualized platform for network service deployment that runs on home gateways. One feature that sets PUROMALTE apart from similar projects is making resources—compute, bandwidth, and storage—available to the research community and application providers. PUROMALTE allows the development of applications on varied operating systems and isolates concurrent applications using virtualization. Moreover, PUROMALTE completely replaces existing home gateways, locating itself at the ideal position to monitor and control all network traffic in the home. Given its ideal positioning and features, PUROMALTE has the potential to empower new applications and allow evaluation of novel solutions in more realistic scenarios.*

Resumo. *Neste artigo apresentamos PUROMALTE, uma plataforma virtualizada em roteadores domésticos para implantação de serviços em rede. Uma característica que separa PUROMALTE de outros projetos similares é o compartilhamento de recursos—processamento, banda e armazenamento—com a comunidade acadêmica e desenvolvedores. PUROMALTE permite desenvolvimento de aplicações em vários sistemas operacionais e executa aplicações concorrentemente de forma isolada usando virtualização. Além disso, PUROMALTE substitui por completo os roteadores domésticos atuais, ficando no local ideal para obter visibilidade e controle sobre todo o tráfego da rede doméstica. Devido ao posicionamento e funcionalidades dos dispositivos, PUROMALTE é uma plataforma que pode possibilitar o desenvolvimento de novas aplicações e permitir avaliações em cenários mais realistas.*

1. Introdução

A maioria dos clientes de banda larga não têm conhecimento para identificar e solucionar problemas de rede. Porém, com a diversificação dos dispositivos com interfaces de rede—computadores, *laptops*, *tablets*, telefones, impressoras, vídeo games e outros—esses clientes precisam atuar como operadores de redes domésticas cada vez mais complexas. Usuários ficam frustrados quando o desempenho da rede é insuficiente para atender os requisitos de uma aplicação porque eles têm poucos ou nenhum recurso para entender, contornar ou solucionar o problema.

Este problema levou ao desenvolvimento de *gateways* inteligentes com objetivo de reduzir a complexidade e automatizar o gerenciamento de redes domésticas [Feamster 2010, Dixon et al. 2012]. Mesmo estes *gateways* inteligentes disponibilizam apenas um conjunto pré-definido de serviços. Usuários, pesquisadores e desenvolvedores não podem modificar o funcionamento de *gateways* atuais.

Argumentamos que *gateways* extensíveis permitiriam o desenvolvimento de aplicações inovadoras. Por exemplo, *smartphones* disponibilizam milhares de aplicações aos usuários em lojas virtuais. Várias destas aplicações utilizam o contexto dos *smartphones*—dispositivos móveis, sempre próximos ao usuário, equipados de vários sensores e com conectividade contínua—para prover serviços inovadores antes inexistentes. Como *smartphones*, *gateways* domésticos têm um contexto específico—conectividade contínua, visibilidade e controle sobre o tráfego de todos os dispositivos na rede, bem como menor latência e maior banda com dispositivos na rede doméstica. *Gateways* domésticos podem permitir a criação e facilitar a implantação de serviços inovadores hoje inexistentes.

Neste artigo apresentamos PUROMALTE, uma plataforma para implantação de serviços de rede em *gateways* domésticos usando virtualização. PUROMALTE compartilha os recursos disponíveis no *gateway*. O uso de virtualização provê flexibilidade para pesquisadores e desenvolvedores executarem aplicações e implantarem serviços em redes domésticas. PUROMALTE substitui o *gateway* doméstico atual e se coloca no ponto central da rede doméstica, o que possibilita visibilidade e controle sobre todo o tráfego da rede. Por exemplo, PUROMALTE pode suportar serviços como monitoramento de redes, compartilhamento de arquivos, automatização de *backups*, coordenação de sensores, otimização do tráfego de rede e acesso remoto. Novas tecnologias desenvolvidas com PUROMALTE poderão melhorar diretamente a experiência de usuários na Internet bem como disponibilizar novos serviços.

2. Objetivos

A figura 1 mostra uma rede doméstica típica com vários dispositivos conectados a um roteador via interfaces Ethernet (linhas sólidas) e Wi-Fi (linhas tracejadas); o roteador transmite os pacotes para um modificador (*modem*) que conecta-se à rede do provedor de acesso. Nossa plataforma, PUROMALTE, executa em computadores que substituem o roteador e o modificador da rede doméstica de usuários voluntários a hospedar um dispositivo PUROMALTE.

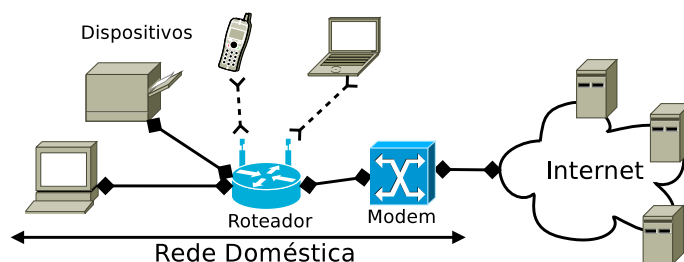


Figura 1. Uma rede doméstica típica.

Desenvolvemos PUROMALTE para substituir roteadores e moduladores em redes domésticas porque estes dispositivos estão numa posição privilegiada para execução de aplicações e serviços. Roteadores são o ponto central de uma rede doméstica, funcionando como ponto de acesso à rede sem fio e comutador (*switch*) Ethernet. Além disso, moduladores concentram todo o tráfego que entra e sai da rede doméstica. Combinando estas funcionalidades, PUROMALTE terá visibilidade e controle sobre todo o tráfego na rede doméstica.

Desenvolvemos PUROMALTE para ser uma plataforma poderosa, genérica e compartilhada. Em particular, trabalhamos para atender os seguintes requisitos:

Visibilidade. PUROMALTE deve monitorar detalhadamente todo o tráfego entrando e saindo da rede doméstica. Dados completos e detalhados permitem caracterização do tráfego e facilitam a solução de problemas; tarefas propícias a erros quando os dados são incompletos ou imprecisos.

Controle. PUROMALTE deve permitir controle sobre o tráfego entrando e saindo da rede doméstica. Este é um requisito para a implantação de técnicas de monitoramento que inserem sondas na rede, mecanismos de controle de banda, filtros de tráfego e técnicas para tratamento de problemas que precisam alterar pacotes em trânsito.

Compartilhamento. PUROMALTE deve suportar execução simultânea de múltiplos serviços e aplicações. Técnicas executando em paralelo não podem impactar umas às outras. Nosso objetivo é permitir que PUROMALTE seja utilizada simultaneamente por múltiplos pesquisadores, maximizando sua utilidade.

Desempenho. PUROMALTE deve ser capaz de executar serviços e aplicações sem reduzir o desempenho observado pelos usuários. Em caso de capacidade de processamento ou banda de rede insuficiente, o tráfego do usuário deve ter prioridade. PUROMALTE deve também prover recursos e desempenho satisfatórios para aplicações e serviços executando na plataforma.

Privacidade. PUROMALTE deve garantir a privacidade dos usuários e segurança das aplicações. Dados de usuários devem ser agregados, filtrados ou anônimos, impedindo a identificação de indivíduos e coleta de informações sensíveis.

2.1. Comparação com abordagens alternativas

Uma alternativa para desenvolver uma plataforma distribuída similar a PUROMALTE é criar serviços que usuários instalam ou acessam em seus dispositivos [Shavitt and Shir 2005, Joumblatt et al. 2011, Chen et al. 2009, Kreibich et al. 2010]. A maior vantagem desta abordagem é o baixo custo, pois o dispositivo é provido pelo usuário. Infelizmente, esta abordagem tem vários problemas.

Um problema é que vários dispositivos de rede, como TVs e impressoras, não aceitam instalação ou execução de aplicações. Outro problema é que usuários podem não instalar aplicações de monitoramento em dispositivos com bateria, como celulares e *tablets*, para não reduzir a autonomia do dispositivo. Além disso, dispositivos na rede doméstica rodam sobre *hardware* e sistemas operacionais diversos, o que aumenta significativamente o custo de desenvolvimento e manutenção do *software*. Apenas entre *laptops* e *tablets* precisamos implementar aplicações em Windows, MacOS, GNU/Linux, Android, e iOS. Outro problema é que monitoramento do tráfego de um dispositivo tem visibilidade incompleta do tráfego da rede doméstica. Por exemplo, uma aplicação de monitoramento rodando no *laptop* mostrado na figura 1 não tem visibilidade sobre o tráfego entre o computador e a impressora, ou sobre o tráfego entre o computador e um servidor externo. Essa visibilidade incompleta do tráfego compromete a utilidade de serviços para coordenação de dispositivos ou controle do tráfego, por exemplo, quando o computador está utilizando toda a banda de rede numa atualização de *software* comprometendo acesso ao Netflix a partir do *laptop*.

Projetos em curso já propuseram aplicações e soluções baseadas em *gateways* inteligentes para redes domésticas. Alguns destes projetos já demonstraram a utilidade de

gateways inteligentes para monitoramento de redes domésticas [Sundaresan et al. 2011, Grover et al. 2013, Sundaresan et al. 2013]. O HomeOS [Dixon et al. 2012] propõe interfaces de comunicação para integrar dispositivos de uma rede doméstica. PUROMALTE pode ser combinado com as interfaces propostas no HomeOS para executar no *gateway* aplicações para integrar dispositivos da rede doméstica. O PUROMALTE é similar a esforços recentes do projeto BISmark para suportar ferramentas de monitoramento desenvolvidas por terceiros [Sundaresan et al. 2014]. PUROMALTE, porém, almeja executar aplicações em geral, não apenas ferramentas de monitoramento de redes.

3. Arquitetura

Implantação do PUROMALTE em redes domésticas reais é essencial para coleta de dados e avaliação de aplicações em cenários realistas. Para cobrir um conjunto diverso de redes domésticas—com usuários de perfil de uso diferentes, conectadas a diferentes provedores de serviço, conectadas por diferentes planos de banda larga e geograficamente distribuídas—estamos instalando protótipos PUROMALTE na casa de voluntários. Abaixo detalhamos nossa abordagem para atender cada um dos requisitos descritos para PUROMALTE na seção 2. Detalharemos a implementação atual na seção 4.

Visibilidade. Para monitorar todo o tráfego, PUROMALTE substitui roteadores e moduladores existentes em redes domésticas atuais. PUROMALTE executa em computadores com múltiplas interfaces Ethernet e uma interface Wi-Fi. *Gateways* PUROMALTE também possuem um modulador ADSL interno para conectar-se diretamente à rede do provedor de acesso. Estas interfaces permitem PUROMALTE centralizar todo o roteamento de dados na rede doméstica. Todas as interfaces de rede do PUROMALTE dão suporte à captura de pacotes de rede, o que permite PUROMALTE interceptar e monitorar comunicações entre quaisquer dois nós da rede doméstica ou entre qualquer nó da rede doméstica e nós externos.

Controle. PUROMALTE controla o tráfego da rede doméstica usando *software* livre existente, como *firewalls* e modeladores de tráfego (*traffic shapers*) no Linux. PUROMALTE provê acesso remoto a pesquisadores e desenvolvedores via SSH. O acesso remoto dá acesso a uma máquina virtual no PUROMALTE, que permite o uso dos recursos computacionais, como processamento, armazenamento e banda de rede. PUROMALTE disponibiliza diferentes mecanismos de virtualização (VirtualBox, KVM e contêineres) para suportar aplicações com diferentes requisitos, como aceleração 3D, e execução de outros sistemas operacionais, como Windows ou Android. Pesquisadores e desenvolvedores podem utilizar os recursos de PUROMALTE para implantar novos serviços e aplicações nas máquinas virtuais.

Compartilhamento. Dois desafios no compartilhamento de recursos são impedir que uma aplicação prejudique outra e impedir que uma aplicação use mais recursos do que permitido. PUROMALTE garante isolamento entre diferentes aplicações e faz alocação de recursos usando técnicas de virtualização como contêineres Linux [Soltesz et al. 2007, Merkel 2014], KVM [Kivity et al. 2007] e Xen [Barham et al. 2003]. Cada aplicação terá acesso a uma fração dos recursos da plataforma PUROMALTE independente de outras aplicações em execução.

Desempenho. Para garantir que PUROMALTE terá desempenho suficiente para atender os requisitos de usuários e serviços, estamos avaliando diferentes técnicas de

virtualização para escolher a técnica com o melhor compromisso entre desempenho e funcionalidades. As métricas principais que consideramos são: (i) funcionalidades da técnica de virtualização (isolamento, migração, reserva de recursos); (ii) impacto na latência, perda de pacotes e banda de rede, e (iii) sobrecarga de CPU e memória. Para evitar problemas de desempenho oriundos de *hardware* com poucos recursos, como os utilizados em roteadores e moduladores domésticos atuais, PUROMALTE utiliza computadores com processadores Intel ou AMD de 64-bits com suporte nativo a virtualização [Neiger et al. 2006], 4 GB de memória RAM e 1 TB de armazenamento.

Privacidade. Nesta fase inicial do projeto garantimos a privacidade dos usuários exigindo que cada pesquisador utilizando PUROMALTE agregue, filtre e anonimize os dados coletados. Planejamos implementar um serviço onde os voluntários poderão consultar quais dados estão sendo utilizados por quais serviços executando em seu *gateway*, e permitir controle sobre os dados coletados. Para isolar e garantir segurança de aplicações utilizamos máquinas virtuais. Também planejamos implementar interfaces e serviços de compartilhamento de dados entre serviços para facilitar a integração de serviços de forma segura no PUROMALTE.

4. Implementação e implantação

Nesta seção descrevemos as funcionalidades do PUROMALTE e detalhamos como foram implementadas.

4.1. Substituindo um *gateway* doméstico

Para que o PUROMALTE substitua os *gateways* atuais é necessário prover as mesmas funcionalidades para usuários domésticos. O PUROMALTE provê uma interface de configuração via Web, que pode ser acessada de forma similar às interfaces dos *gateways* existentes. Atualmente a interface de configuração permite configurar a rede sem fio e a conexão DSL com o provedor de banda larga.

O PUROMALTE utiliza o *hostapd* para operar como um ponto de acesso de rede sem fio. O *hostapd* é responsável por determinar o SSID da rede sem fio, realizar autenticação de dispositivos, ajustar velocidade de transmissão (802.11b, 802.11n, 802.11g) e selecionar o canal de transmissão. Em laboratório já conseguimos conexões sem fio a 150Mbps entre *gateways* PUROMALTE protótipos e *laptops* de desenvolvedores. Para conectar-se à rede do provedor de acesso, o PUROMALTE utiliza o *pppoeconf* para configurar e executar o protocolo PPPoE. Para permitir funcionamento no PUROMALTE, a placa de rede sem fio e o modulador ADSL possuem *drivers* livres.

Para isolar o tráfego, configuramos diferentes subredes para máquinas virtuais executando aplicações e para dispositivos na rede doméstica. O roteamento é realizado pelo Linux. Máquinas virtuais e dispositivos são configurados automaticamente por um servidor DHCP que escuta em todas as redes. Pretendemos estender a interface de configuração para permitir usuários mapearem endereços MAC para endereços IP no servidor DHCP para fixar o endereço IP de alguns dispositivos ou máquinas virtuais. Para permitir que as várias máquinas virtuais e os vários dispositivos na rede doméstica se conectem à Internet, PUROMALTE utiliza o NAT (*Network Address Translation*) implementado no Linux (*IP masquerading*). Por último, o PUROMALTE executa um servidor

DNS local que coopera com o servidor DHCP para dar nome a todos os dispositivos e aplicações executando na rede doméstica. Desta forma, o usuário pode acessar a interface Web de configuração pelo endereço <http://puromalte.home> e seu computador de mesa pelo nome `desktop.home`.

4.2. Aplicações de exemplo

Aplicações virtualizadas são um diferencial do PUROMALTE. Cada aplicação executa em uma máquina virtual ou contêiner. Estas aplicações são armazenadas em discos virtuais. Para reduzir o consumo de armazenamento dos discos virtuais, aplicações são instaladas sobre um disco virtual base. PUROMALTE armazena apenas as diferenças resultantes de cada aplicação relativas ao disco virtual base usando *copy on write*, em geral algumas dezenas de megabytes. O disco virtual base contém Debian stable, mas planejamos criar também discos base com outras distribuições do Linux, Windows e Android.

No PUROMALTE implementamos duas aplicações de exemplo. A primeira é um cliente BitTorrent e a segunda é um NAS (disco de rede). O NAS é implementado com Samba, que exporta um disco na rede. Unidades exportadas pelo Samba podem ser montadas em praticamente todos os sistemas operacionais de uso geral. O NAS possui uma pasta “a baixar” e uma pasta “baixado”. O usuário pode colocar arquivos torrent na pasta “a baixar”. A aplicação de BitTorrent detecta os arquivos, realiza o *download* e salva o conteúdo na pasta “baixado”. Todos os serviços descritos na seção 4.1 são encapsulados em uma única aplicação (máquina virtual) PUROMALTE.

4.3. Instalação Atual

A instalação atual do PUROMALTE conta com dois *gateways* em casas de voluntários em duas cidades diferentes da região metropolitana de Belo Horizonte. A quantidade reduzida de dispositivos deve-se à quantidade restrita de *hardware* disponível¹ e à necessidade que os voluntários tenham capacidade e disponibilidade de ajudar na resolução de problemas. Os voluntários atuais assinam Oi Velox, o maior provedor de acesso à Internet banda larga via DSL em na região metropolitana Belo Horizonte. Infelizmente implantar *gateways* em outros provedores é difícil. Por exemplo, o roteador do provedor NET é responsável por decodificar sinais de TV, o que não temos condição de fazer no PUROMALTE devido a restrições digitais (DRM).

Outra aplicação que implementamos no PUROMALTE é o gerenciador central de dispositivos, disponível em <http://puromalte.dcc.ufmg.br>. O gerenciador central atualmente lista os *gateways* PUROMALTE, informações de identificação e o endereço IP público do *gateway*. Cada *gateway* PUROMALTE periodicamente envia uma requisição de atualização de DNS contendo seu IP público usando `nsupdate` para o gerenciador central. Os *gateways* PUROMALTE também transmitem seu endereço IP público utilizando uma interface RESTful no servidor. Como *gateways* PUROMALTE recebem endereços IP dinâmicos, esta informação é essencial para permitir acesso remoto via SSH.

5. Demonstração

No salão de ferramentas iremos utilizar um *gateway* PUROMALTE equipado com placa de rede sem fio e modulador ADSL para demonstrar suas funcionalidades para usuários, desenvolvedores e pesquisadores.

¹ Temos quatro dispositivos adquiridos com verba do CNPq, mas um está em manutenção. Recentemente adquirimos e estamos preparando mais cinco dispositivos com verba da FAPEMIG.

Do ponto de vista do usuário, iremos demonstrar as funcionalidades do PUROMALTE como *gateway* doméstico. Por exemplo, iremos configurar o PUROMALTE para permitir participantes do SBRC conectarem-se à rede sem fio do PUROMALTE para acessar a Internet.² Iremos apresentar também a interface de configuração disponibilizada para os usuários domésticos.

Do ponto de vista do desenvolvedor, iremos mostrar como as imagens base de disco virtual que disponibilizamos para desenvolvimento no PUROMALTE podem ser estendidas para implantar novas aplicações. Em particular, iremos mostrar a instalação do serviço de compartilhamento de arquivos via BitTorrent numa máquina virtual e sua implantação no *gateway*.

Do ponto de vista do pesquisador, iremos mostrar como o PUROMALTE permite captura e modificação de pacotes. Em particular, iremos demonstrar captura de pacotes de rede e sumarização dos dados trafegados usando o TSTAT [Finamore et al. 2011]. Iremos também configurar priorização de tráfego para um subconjunto dos clientes conectados à rede sem fio usando políticas de fila disponíveis no Linux.

6. Conclusão e trabalhos futuros

PUROMALTE é uma nova plataforma em desenvolvimento e disponível a pesquisadores brasileiros para implantação e avaliação de aplicações em rede distribuídas em *gateways* domésticos. O potencial de PUROMALTE acompanha o aumento da penetração da Internet banda larga e sofisticação das redes domésticas.

PUROMALTE pode ser utilizado para desenvolvimento, avaliação e implantação de novas soluções de gerenciamento de rede, melhorando o desempenho observado por usuários. PUROMALTE pode ser utilizado também para implantação de novas técnicas para identificação de falhas em redes domésticas e em redes de provedores de acesso, e pode ter impacto direto na qualidade de serviço observada por usuários da Internet e reduzir custos de provedores de acesso. PUROMALTE pode ser utilizado em projetos de pesquisa para testes e avaliação de novas ferramentas ou protocolos. Por último, devido ao novo contexto coberto por PUROMALTE, a plataforma pode dar suporte ao desenvolvimento de aplicações em rede ainda inexistentes.

Nos próximos meses iremos implantar mais *gateways* PUROMALTE na casa de voluntários. Pretendemos também automatizar a instalação de *gateways* PUROMALTE para que outros pesquisadores possam instalar seus próprios *gateways* e assim impulsionar a expansão da plataforma. A longo prazo pretendemos estudar mecanismos para classificação de tráfego e priorização de tráfego automática em redes domésticas.

Referências

- Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., and Warfield, A. (2003). Xen and the Art of Virtualization. In *Proc. ACM SOSP*.
- Chen, K., Choffnes, D. R., Potharaju, R., Chen, Y., Bustamante, F. E., Pei, D., and Zhao, Y. (2009). Where the Sidewalk Ends: Extending the Internet AS Graph using Traceroutes from P2P Users. In *Proc. CoNEXT*.

²Como não prevemos ter plano de banda larga disponível no evento para acessar a Internet através do modulador ADSL, planejamos disponibilizar acesso via rede cabeada.

- Dixon, C., Mahajan, R., Agarwal, S., Brush, A. J., Lee, B., Saroiu, S., and Bahl, P. (2012). An Operating System for the Home. In *Proc. USENIX NSDI*.
- Feamster, N. (2010). Outsourcing Home Network Security. In *ACM SIGCOMM Home-Nets*.
- Finamore, A., Mellia, M., Meo, M., Munafò, M. M., and Rossi, D. (2011). Experiences of Internet Traffic Monitoring with Tstat. *IEEE Network*, 25(3):8–14.
- Grover, S., Park, M. S., Sundaresan, S., Burnett, S., Kim, H., Ravi, B., and Feamster, N. (2013). Peeking Behind the NAT: An Empirical Study of Home Networks. In *Proc. IMC*.
- Joumblatt, D., Teixeira, R., Chandrashekar, J., and Taft, N. (2011). HostView: Annotating End-host Performance Measurements with User Feedback. *ACM SIGMETRICS Perf. Eval. Rev.*, 38(3):43–48.
- Kivity, A., Kamay, Y., Laor, D., Lublin, U., and Liguori, A. (2007). KVM: the Linux Virtual Machine Monitor. In *Proc. of the Linux Symposium*.
- Kreibich, C., Weaver, N., Nechaev, B., and Paxson, V. (2010). Netalyzer: Illuminating The Edge Network. In *Proc. IMC*.
- Merkel, D. (2014). Docker: Lightweight Linux Containers for Consistent Development and Deployment. *Linux Journal*, 2014(239).
- Neiger, G., Santoni, A., Leung, F., Rodgers, D., and Uhlig, R. (2006). Intel Virtualization Technology: Hardware Support for Efficient Processor Virtualization. *Intel Technology Journal*, 10(3):167–177.
- Shavitt, Y. and Shir, E. (2005). DIMES: Let the Internet Measure Itself. *SIGCOMM Comput. Commun. Rev.*, 35(5):71–74.
- Soltész, S., Pözl, H., Fiuczynski, M. E., Bavier, A., and Peterson, L. (2007). Container-based Operating System Virtualization: a Scalable, High-performance Alternative to Hypervisors. In *Proc. ACM EuroSys*.
- Sundaresan, S., Burnett, S., Feamster, N., and de Donato, W. (2014). BISmark: A Testbed for Deploying Measurements and Applications in Broadband Access Networks. In *Proc. USENIX ATC*.
- Sundaresan, S., de Donato, W., Feamster, N., Teixeira, R., Crawford, S., and Pescapè, A. (2011). Broadband Internet Performance: a View from the Gateway. In *Proc. ACM SIGCOMM*.
- Sundaresan, S., Feamster, N., Teixeira, R., and Magharei, N. (2013). Measuring and Mitigating Web Performance Bottlenecks in Broadband Access Networks. In *Proc. IMC*.