

Net-Opp: Um Middleware Transparente Para Formação de Redes e Troca de Conteúdos Para Aplicações Oportunistas

Charles T. B. Garrocho¹, Maurício J. da Silva¹, Ricardo A. R. Oliveira¹

¹ Laboratório IMóbilis

Departamento de Computação – DECOM

Universidade Federal de Ouro Preto (UFOP) – Ouro Preto, MG – Brazil

{ctgarrocho,badriciobq,rrabelo}@gmail.com

Abstract. *Opportunistic networks are one of the most interesting evolutions of MANETs, which allow various applications, such as in reduce cell traffic load, communications in emergency situations and contour censorship. The increasing number of mobile devices should, in theory, promote opportunistic networks. However, in practice, current technologies for opportunistic networks, such as Wi-Fi Ad-Hoc, Bluetooth and Wi-Fi Direct, either are not available in current devices, or require user unwanted interaction to establish connectivity. To overcome these shortcomings, we propose a middleware that uses the Wi-Fi Tethering technology for formation of the communication network and allow the exchange of content between devices without user interaction. An application that employs the use of middleware is displayed. Results showed that the middleware could abstract the formation of the network and the exchange of content between multiple devices simultaneously transparently.*

Resumo. *Redes oportunistas são uma das evoluções mais interessantes de MANETs, onde permitem diversas aplicações, como reduzir a carga de tráfego celular, comunicações em situações de emergência e contorno a censura. O crescente aumento de dispositivos móveis deve, em tese, promover redes oportunistas. Porém, na prática, as tecnologias atuais para redes oportunistas, como Wi-Fi Ad-Hoc, Bluetooth e Wi-Fi Direct, ou não são disponíveis nos dispositivos atuais, ou exigem interação indesejada do usuário para estabelecer conectividade. Para superar essas deficiências, é proposto um middleware que utiliza a tecnologia Wi-Fi Tethering para formação da rede de comunicação e permitir a troca de conteúdos entre os dispositivos sem a interação do usuário. É apresentada uma aplicação que emprega o uso do middleware. Resultados mostraram que o middleware conseguiu abstrair a formação da rede e a troca de conteúdos entre vários dispositivos simultaneamente de forma transparente.*

1. Introdução

Hoje em dia, as redes de comunicação sem fio tornaram-se essenciais na sociedade. As pessoas podem se conectar a redes de dados em qualquer lugar, por meio de diferentes dispositivos e tecnologias de comunicação [Ganti 2011]. Dispositivos móveis como smartphones e tablets vêm se popularizando e evoluindo muito nos últimos anos, tornando a interação do usuário com o dispositivo uma experiência menos virtual e mais realista. A integração de diversos recursos de comunicação (por exemplo, Bluetooth, Wi-Fi Direct, 3G e LTE) abriu novas possibilidades de redes [Ma 2014].

Redes oportunistas são uma das evoluções mais interessantes de *MANETs* (*Mobile Ad hoc Networks*) [Pelusi 2006]. Nas redes oportunistas os dispositivos móveis podem se comunicar uns com os outros, mesmo se uma rota para conectá-los não existe [Boldrini 2014]. Redes oportunistas podem trazer benefícios para redes baseadas em infraestrutura sem fio (3G e LTE), como na utilização eficiente do espectro radioelétrico disponível [Vukadinovic 2010] ou em reduzir a carga de tráfego celular [Han 2010]. Além disso, ela é ótima para lidar com falhas de infraestrutura de comunicação, parciais ou totais causadas por desastres naturais [Dekker 2013], censura do governo [Helft 2010] ou por até uma interrupção de Internet e telemóvel [Chen 2011].

Redes oportunistas têm sido um tema de pesquisa há anos, produzindo arquiteturas de comunicação [Ott 2012, Pitkanen 2012] e aplicações [Ott 2011, Lindgren 2011]. No entanto, rede oportunista entre dispositivos móveis depende das capacidades de tais dispositivos para estabelecer comunicação entre si. Embora as tecnologias de interface sem fio, Wi-Fi Ad-Hoc, Wi-Fi Direct e Bluetooth oferecem tais capacidades em teoria, limitações da especificação do protocolo, chipsets e sistemas operacionais em dispositivos móveis tornam essas tecnologias em grande parte inútil na prática.

Dispositivos móveis atuais (smartphones e tablets) não suportam Wi-Fi Ad-Hoc [IEEE 2007], a não ser com firmwares customizados que exigem acesso root ao dispositivo, como feito em [Dubois 2013] e [Arnaboldi 2014]. Bluetooth é limitado em termos de alcance de comunicação e largura de banda, bem como descoberta sem interação humana [Haartsen 2000]. Além disso, o Bluetooth leva muito tempo para parear e muitas das tentativas de pareamento não são feitas com sucesso [Pietilainen 2009]. Comunicação via Wi-Fi Direct é outra opção, mas requer pareamento, podendo demorar até 2 minutos para formação de grupo e ainda requer interação do usuário [WiFiAlliance 2009].

Essas características das tecnologias citadas, impedem na prática o desenvolvimento de aplicações que necessitam de comunicação transparente, isto é, a formação da rede de comunicação e a troca de conteúdos sem a necessidade de interação do usuário com o dispositivo. Para superar essas deficiências é proposto o middleware Net-Opp. Net-Opp é baseado na tecnologia Wi-Fi Tethering de dispositivos móveis (smartphones e tablets), onde seu principal objetivo é possibilitar a capacidade de comunicação entre os dispositivos de forma transparente, sem que haja pareamento entre os dispositivos. Net-Opp automaticamente analisa pontos de acesso disponíveis no ambiente e se associa com um ponto. Se nenhum ponto de acesso for encontrado, Net-Opp torna o dispositivo em um ponto de acesso para prover uma rede de comunicação para outros dispositivos. Além disso, Net-Opp possibilita a troca transparente de conteúdos entre os dispositivos. Todo esse processo do middleware é realizado automaticamente sem exigir pareamento entre os dispositivos e sem alterações nos sistemas operacionais dos dispositivos.

Os principais benefícios do middleware proposto podem ser avaliados sob o ponto de vista dos desenvolvedores de aplicações oportunistas. O sistema oferece uma camada de interoperabilidade entre as diferentes aplicações e a rede oportunista. O middleware cria a abstração de uma rede oportunista e da troca de conteúdos, fornecendo serviços para as várias aplicações, facilitando o trabalho do desenvolvedor, liberando-o de se preocupar com a infraestrutura da rede e a troca de conteúdos. O usuário pode escrever sua aplicação e conectá-la sem impacto ao middleware Net-Opp. Essas características tornam o middleware uma abordagem prática para aplicações de redes oportunistas.

O presente trabalho apresenta a arquitetura do middleware proposto e a descrição do seu funcionamento. Além disso, como prova de conceito foi criada a aplicação *Crowd Wi-Fi*, que permite o compartilhamento transparente de arquivos de uma pasta local do dispositivo para outros dispositivos conectados à rede oportunista promovida por Net-Opp. Resultados mostraram que o middleware Net-Opp conseguiu abstrair a formação da rede e a troca de conteúdos entre os dispositivos, conseguindo compartilhar conteúdos entre vários dispositivos simultaneamente de forma transparente, mostrando-se escalável com uma alta taxa de transmissão e um baixo tempo de atraso de pacotes.

O restante do artigo está organizado da seguinte forma: na Seção 2 são apresentados os trabalhos relacionados. Na Seção 3 é apresentado a visão geral da arquitetura do middleware Net-Opp. Na Seção 4 é apresentado a aplicação *Crowd Wi-Fi*, que foi desenvolvida sobre Net-Opp. Na Seção 5 é feita uma avaliação do middleware, sendo que na Subseção 5.1 são apresentados os cenários e métricas avaliadas, e na Subseção 5.2 são apresentados os resultados dos experimentos. Finalmente na Seção 6 são apresentadas as conclusões e os trabalhos futuros.

2. Trabalhos Relacionados

Existem na literatura diversas soluções cuja meta é auxiliar no processo de desenvolvimento de aplicações voltadas para o ambiente social móvel [Hu 2014]. Essas soluções fazem uso de diferentes arquiteturas, tecnologias de rede, entre outras características. Entretanto, algumas pesquisas recentes demonstram que são poucas as soluções voltadas para as redes oportunistas [Wang 2014].

Projeto Hagggle [Su 2007] é a primeira arquitetura abrangente de redes autônomas e oportunistas, projetado para permitir a comunicação na presença de conectividade de rede intermitente, que possibilita a troca de conteúdos entre os dispositivos em possíveis encontros. Hagggle utiliza o Bluetooth para estabelecer a conexão de rede e possibilitar a troca de conteúdos.

MobiClique [Pietilainen 2009] é um middleware que possibilita as pessoas se corresponderem e estenderem as suas redes sociais. Para alcançar esse objetivo, MobiClique foi desenvolvido de forma descentralizada e faz uso de uma rede ad hoc móvel onde a comunicação é feita via Bluetooth, de modo que as conexões oportunistas são criadas entre dispositivos vizinhos. Porém MobiClique necessita de conexão à Internet para sincronizar o perfil do usuário às redes sociais.

Shair [Dubois 2013] é um middleware para compartilhamento de recursos P2P móvel sem a necessidade de conexões à Internet. Especificamente, baseado no middleware Shair, um aplicativo Android, MobileP2P Photo Sharing App, foi desenvolvido, no qual, as fotos podem ser compartilhadas diretamente através de dispositivos das pessoas sem conexões com a Internet, utilizando Bluetooth ou Wi-Fi Ad-Hoc.

No trabalho CAMEO [Arnaboldi 2014] é proposto um middleware que utiliza a tecnologia Wi-Fi Ad-Hoc para fornecer aos desenvolvedores das aplicações móveis um conjunto de funcionalidades para o recolhimento, partilha e elaboração de informações de contexto sobre redes oportunistas.

O middleware Net-Opp difere dos middlewares apresentados no estabelecimento de conexão de rede e na troca de conteúdos entre os dispositivos. Em Net-Opp não é

necessário nenhum pareamento para formação de rede e nem para troca de conteúdos, diferente de como ocorre em [Su 2007, Pietilainen 2009, Dubois 2013], onde é necessária interação humana para o pareamento entre os dispositivos. Para a utilização de Net-Opp, os desenvolvedores necessitam apenas de importar o middleware e se comunicar pela API de comunicação, sem a necessidade de alterações no Sistema Operacional do dispositivo, diferentemente como ocorre em [Dubois 2013] e [Arnaboldi 2014], onde é necessário a utilização de firmwares customizados que exigem acesso root ao dispositivo para habilitarem a tecnologia Wi-Fi Ad-Hoc. Todas essas vantagens oferecidas por Net-Opp são alcançadas através de um processo customizado e transparente para formação de rede utilizando a tecnologia Wi-Fi Tethering.

A tecnologia Wi-Fi Tethering é suportada por todos os principais fabricantes de dispositivos e está disponível em todas as principais plataformas de sistemas operacionais, tais como iOS 4.3+ [Apple iOS], Android 2.2+ [Android Phone] e Windows 7.5+ [Windows Phone]. Enquanto este modo é inicialmente concebido para compartilhar o acesso de uma Internet 3G e LTE para clientes, ela pode ser usada para comunicações móveis de cliente para cliente e comunicações ponto de acesso para cliente, permitindo assim comunicações oportunistas.

Existem na literatura algumas soluções cuja meta é encontrar uma alternativa de rede para aplicações oportunistas utilizando a tecnologia Wi-Fi Tethering. Dentre esses trabalhos, em WiFi-Opp [Trifunovic 2011] é sugerido vários modos de operação: nós móveis analisam pontos de acesso no ambiente e se associam com um ponto de acesso. Se nenhum ponto de acesso for encontrado, o dispositivo torna-se um ponto de acesso para facilitar a comunicação para outros nós.

No trabalho MA-Fi [Wirtz 2011] os autores utilizaram a virtualização de rede nos dispositivos, nesse caso computadores pessoais, para permitir que os dispositivos simultaneamente assumissem os papéis de ponto de acesso e cliente, possibilitando assim comunicação multihop. No entanto, a virtualização das interfaces de rede não é suportado em dispositivos móveis, como smartphones e tablets.

Nos estudos dos trabalhos [Trifunovic 2011] e [Wirtz 2011], os autores investigam o impacto de vários parâmetros (por exemplo, o tempo de baliza, intervalo de varredura, tempo de conexão) por meio de simulações e comparam o consumo de energia com Wi-Fi Ad-Hoc, mas eles não analisam o tempo de formação de uma topologia de rede, nem mesmo como a rede se comporta com tráfego de conteúdos em aplicações distribuídas.

Enquanto que nos trabalhos [Trifunovic 2011] e [Wirtz 2011] é apresentado a criação desta estrutura de rede com a tecnologia Wi-Fi Tethering e feito comparações com o Wi-Fi Ad-Hoc, em nosso trabalho é feito uma extensão desses trabalhos, onde é proposto um middleware personalizado que é capaz de abstrair detalhes da formação desta estrutura de rede e também da troca de conteúdos para as aplicações oportunistas em dispositivos móveis pessoais (smartphones e tablets).

O middleware Net-Opp proposto neste trabalho é baseado na tecnologia Wi-Fi Tethering de dispositivos móveis, que estabelece a comunicação semelhante ao Wi-Fi Direct, porém sem necessitar de pareamento nas operações de formação topológica de rede e na troca de conteúdos entre os dispositivos. Além disso, como caso de uso do middleware é apresentado uma aplicação e através dela é avaliado o tempo de formação

topológica desta estrutura de rede e o impacto do compartilhamento de conteúdos entre dispositivos através do middleware Net-Opp em um cenário real com dispositivos móveis pessoais (smartphones e tablets), enquanto que os demais trabalhos, ou apresentam apenas simulações [Trifunovic 2011], ou utilizam computadores pessoais, como notebooks para transformar os dispositivos em pontos de acessos [Wirtz 2011].

3. Visão Geral da Arquitetura do Middleware Net-Opp

A arquitetura do middleware Net-Opp foi projetada tendo como objetivo principal dar suporte a comunicação transparente entre dispositivos móveis pessoais (smartphones e tablets). Para atingir essa meta, a arquitetura foi dividida em módulos, conforme é ilustrado na Figura 1, onde cada um é responsável por gerenciar uma parte dos recursos do middleware. Os módulos que compõem Net-Opp são: *API*, *Gerenciador de Informações*, *Gerenciador de Rede* e *Provedor de Conteúdos*.

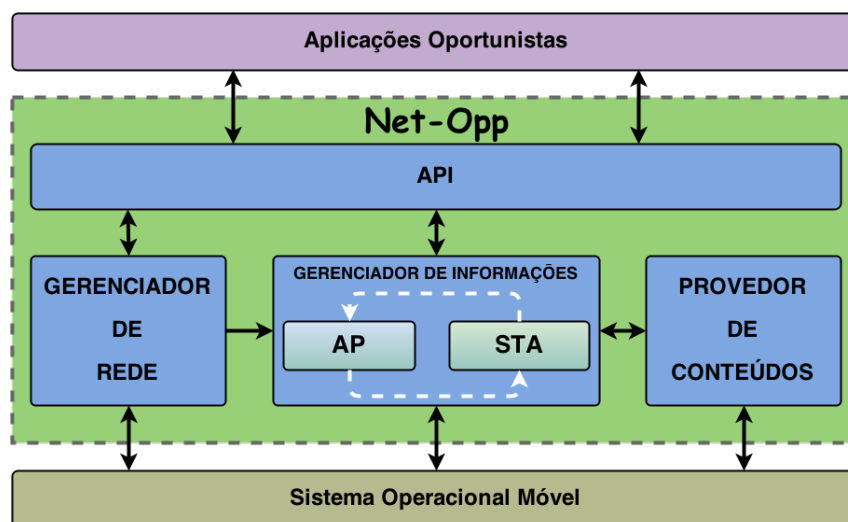


Figura 1. Arquitetura do Middleware Net-Opp.

3.1. Funcionamento dos Módulos

O módulo *API* foi projetado para permitir que os desenvolvedores possam usufruir das funcionalidades do Net-Opp. Este módulo disponibiliza uma interface de acesso ao Net-Opp que pode ser utilizada pelos desenvolvedores para explorar os recursos desse middleware. Para isso, a *API* do Net-Opp foi desenvolvida visando o paradigma de comunicação entre processos, o *IPC* (*Inter-Process Communication*).

O módulo *Gerenciador de Informações* é responsável por gerenciar as informações referente a rede e os conteúdos disponibilizados pelos dispositivos. Este módulo é dividido entre os submódulos *AP* e *STA*. A execução e o gerenciamento dos submódulos *AP* e *STA* é realizado pelo módulo *Gerenciador de Rede*.

O módulo *Gerenciador de Rede* é responsável pela formação e manutenção da rede oportunista. Para realizar essas atividades, conforme é ilustrado na Figura 2, este módulo faz uso de artifícios (por exemplo, a tecnologia Wi-Fi Tethering, o modo de escaneamento de redes Wi-Fi e o nível de bateria do dispositivo) do Sistema Operacional. O módulo *Gerenciador de Rede* é dividido em duas etapas.

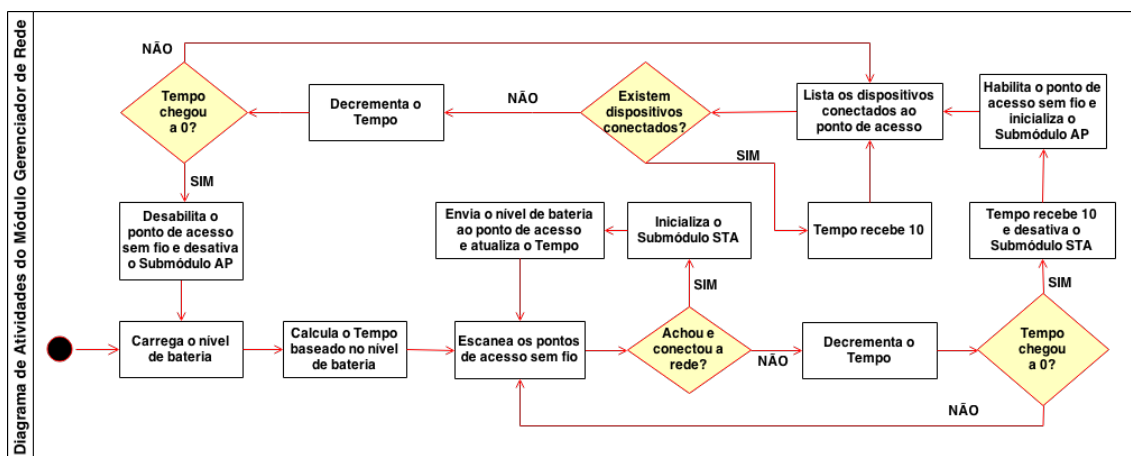


Figura 2. Diagrama de Atividades do Módulo *Gerenciador de Rede*.

Quando inicializado, o módulo *Gerenciador de Rede* executa a primeira etapa, onde ele obtém o nível de bateria do dispositivo e calcula um tempo para o escaneamento de redes. Quanto menor o nível de bateria, maior é o tempo de escaneamento e quanto maior o nível de bateria, menor é o tempo de escaneamento de redes. Caso o dispositivo consiga se conectar a uma rede, o submódulo *STA* é inicializado. Caso contrário, e não seja encontrado nenhuma rede, ou não seja possível conectar, o tempo de escaneamento vai decrementando, e quando o tempo chegar a zero, automaticamente o módulo *Gerenciador de Rede* habilita a tecnologia Wi-Fi Tethering do dispositivo, inicializa o submódulo *AP* e desativa caso necessário o submódulo *STA*, pulando para a segunda etapa do módulo. Após esta primeira etapa, o módulo *Gerenciador de Rede* verifica se existem outros dispositivos conectados ao ponto de acesso. Caso não exista, a tecnologia Wi-Fi Tethering e o submódulo *AP* são desativados. A desativação do ponto de acesso é o fim da segunda etapa do módulo *Gerenciador de Rede*. Dessa forma, o módulo volta para a primeira etapa, continuando a execução de suas tarefas e pesquisando novas redes, garantindo a manutenção desta estrutura de rede.

A Figura 3 ilustra quais módulos estão em execução quando a estrutura de rede está estabelecida pelo módulo *Gerenciador de Rede*. O submódulo *AP* só é executado em um dispositivo ponto de acesso, o submódulo *STA* é executado apenas em dispositivos clientes, e os módulos *API* e *Provedor de Conteúdos* são executados em todos os dispositivos.

O submódulo *AP* é um servidor que possibilita conexões simultâneas. Ele trata três tipos de requisições: adicionar um conteúdo a rede; adicionar um nível de bateria de um dispositivo; e listar endereços *IP* (*Internet Protocol*), conteúdos e o novo tempo de escaneamento de redes. Todas essas requisições são efetuadas pelo submódulo *STA* dos dispositivos clientes utilizando como identificador do dispositivo o seu endereço *MAC* (*Media Access Control*).

Qualquer dispositivo pode disponibilizar e requisitar conteúdos nessa rede. Os submódulos *AP* e *STA* são responsáveis por requisitarem os conteúdos a outros dispositivos. Já o módulo *Provedor de Conteúdos* é responsável por receber as requisições e transmitir os conteúdos para qualquer dispositivo da rede.

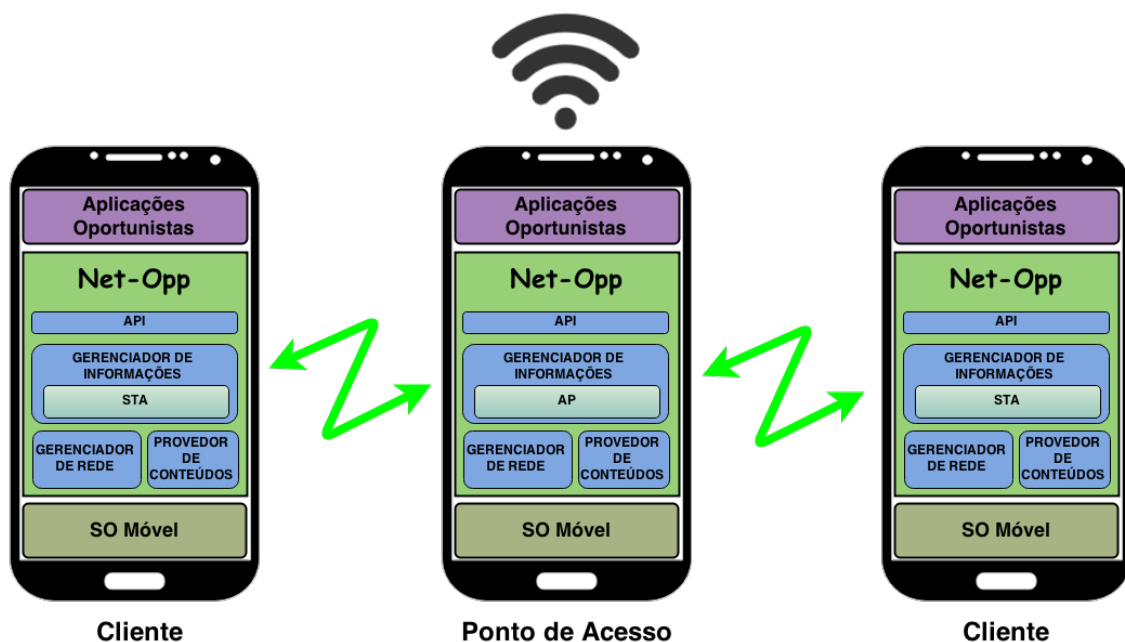


Figura 3. Módulos em execução com a rede de comunicação estabelecida.

Para saber quais conteúdos podem ser transmitidos pelo dispositivo, o módulo *Provedor de Conteúdos* interage com os submódulos *STA* ou *AP* do dispositivo requisitado de forma a verificar quais conteúdos foram compartilhados pelo dispositivo.

Com a rede de comunicação está estabelecida pelo módulo *Gerenciador de Rede*, o submódulo *STA* dos dispositivos clientes envia o nível de bateria do dispositivo para o submódulo *AP* do dispositivo ponto de acesso. O submódulo *AP* adiciona esses níveis de bateria em uma lista de acordo com os endereços *MAC* de cada dispositivo. Essa lista é ordenada de acordo com o nível de bateria e de forma decrescente.

Quando o submódulo *STA* de um dispositivo cliente solicita a terceira requisição de listagem, o submódulo *AP* do dispositivo ponto de acesso verifica qual a posição desse dispositivo na lista de níveis de bateria e retorna sua posição multiplicado por dez. Assim, o dispositivo que tiver maior nível de bateria, será a posição zero da lista, zero é multiplicado por dez, no que resulta em um tempo zero. Dessa forma, caso a rede seja destruída por algum motivo, o dispositivo com maior nível de bateria terá um tempo zero para o escaneamento de redes, transformando-se automaticamente em um ponto de acesso. Enquanto isso, os demais dispositivos, terão como tempo de escaneamento de pontos de acesso, respectivamente, dez segundos, vinte segundos, e assim sucessivamente.

3.2. Gerenciamento das Informações da Rede

Em uma infraestrutura de rede *WLAN* (*Wireless Local Area Network*), o dispositivo que é o ponto de acesso tem todas as informações referentes a rede. Apesar de um cliente estar conectado a um ponto de acesso, ele desconhece quais os outros dispositivos atuais na rede, a não ser o dispositivo ponto de acesso que sempre fica com o endereço inicial da rede.

Para que todos os clientes possam se comunicar pela rede, o submódulo *AP* do ponto de acesso fornece ao submódulo *STA* dos clientes uma lista de endereços *IP* dos

dispositivos conectados a rede. Essa lista é requisita pelo cliente de tempo em tempo, com o objetivo de estar com a lista de endereços *IP* sempre atualizada, para evitar o caso de um dispositivo sair da rede e um endereço inválido ficar armazenado.

Para que os arquivos compartilhados nessa rede sejam identificados por cada dispositivo, o nome do arquivo é identificado pela concatenação do endereço *MAC* do dispositivo mais o nome do arquivo. Dessa forma, além do arquivo ter uma identificação única, os dispositivos que receberem essa identificação do arquivo saberão qual o dispositivo que disponibilizou o conteúdo na rede através do endereço *MAC*, não necessitando de baixar todos os conteúdos da rede.

3.3. Segurança e Privacidade

O middleware armazena o *SSID* (*Service Set Identifier*) e o *PSK* (*Pre-Shared Key*) para prover a rede de comunicação, não sendo possível sua modificação. Dessa forma, dispositivos clientes podem escanear e se conectarem automaticamente as redes encontradas comparando com o *SSID* e *PSK* do middleware. Se não encontrarem uma rede, ativarão a tecnologia Wi-Fi Tethering definindo o *SSID* e o *PSK* da rede configurado no middleware.

O objetivo do middleware é possibilitar comunicação transparente entre os dispositivos. Desta forma, o middleware não tem uma forte ênfase na segurança da comunicação entre dispositivos, como é feito no Bluetooth e Wi-Fi Direct com a segurança de pareamento. Assim, para manter a comunicação transparente, é definido que a segurança das informações trocadas entre os dispositivos são feitas utilizando *SSL* (*Secure Socket Layer*).

Em Net-Opp não é definido nenhuma privacidade dos usuários em sua rede de comunicação. Privacidade, apesar de trazer mais segurança ao usuário, também traz limitações em questões de troca de conteúdos em aplicações que não necessitam esse tipo de mecanismo. Portanto, as políticas de privacidade devem ser definidas na camada de aplicação.

4. Prova de Conceito: Aplicação Crowd Wi-Fi

Nesta seção é apresentado um exemplo de aplicação oportunista, a qual foi desenvolvida sobre o Net-Opp. A implementação dessa aplicação teve como objetivo gerar os cenários para a avaliação do middleware. Esta aplicação permite o compartilhamento de conteúdos de uma pasta do dispositivo para vários outros dispositivos através da comunicação com o middleware Net-Opp. Os principais exemplos de utilização dessa aplicação, é em eventos onde há uma pequena concentração de pessoas, como em um restaurante, museu ou uma sala de aula. Tanto a aplicação quanto o middleware, foram desenvolvidos utilizando o Sistema Operacional Android 4.1.

O middleware Net-Opp foi implementado para executar como um serviço para Sistema Operacional Android, sendo assim, ele executa todas as suas funções em segundo plano. Para a definição das interfaces da *API* do Net-Opp foi utilizado a *AIDL* (*Android Interface Definition Language*). Essa linguagem é provida pelo Android para a especificação de interfaces para o protocolo *IPC*. A partir das definições de interfaces feitas em *AIDL*, todo código necessário para a comunicação remota entre o cliente e o serviço remoto é gerado automaticamente.

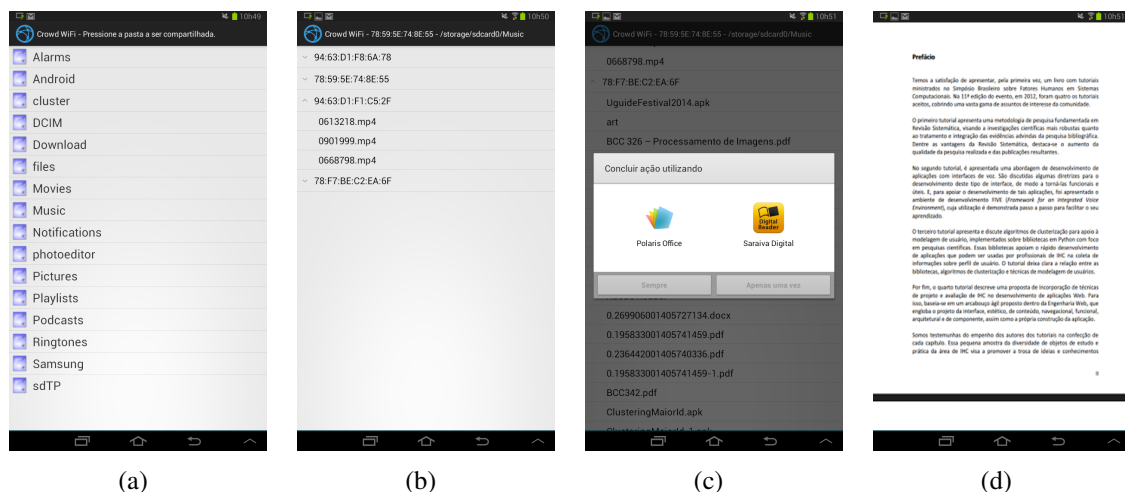


Figura 4. Imagens da Aplicação *Crowd Wi-Fi*.

Quando o *Crowd Wi-Fi* é instalado e executado pela primeira vez no dispositivo do usuário, é realizada a operação *bind* junto ao Net-Opp. Após o Net-Opp e o *Crowd Wi-Fi* estarem associados, é exibida uma tela com o título "Pressione a Pasta a Ser Compartilhada", conforme é ilustrado na Figura 4(a), nessa tela o usuário deve selecionar a pasta que ele deseja compartilhar na rede oportunista, essa tela é somente apresentada quando o usuário ainda não definiu uma pasta a ser compartilhada na aplicação.

Após a seleção da pasta, a Figura 4(b) ilustra a tela de lista de dispositivos que é automaticamente gerada pelo Net-Opp através de métodos da *API* que busca os conteúdos disponibilizados. Essas informações não são necessariamente os conteúdos em si, mas informações referentes a conteúdos compartilhados pelos dispositivos. Com um clique sobre um dos conteúdos listados, a aplicação *Crowd Wi-Fi* solicita ao Net-Opp o conteúdo, Net-Opp automaticamente requisita e baixa o arquivo de um dispositivo e a aplicação exibe uma mensagem na tela da aplicação permitindo o usuário escolher um serviço para execução do conteúdo, conforme é ilustrado na Figura 4(c). Após isso, o conteúdo é automaticamente executado pelo serviço escolhido, conforme é ilustrado na Figura 4(d).

5. Avaliação do Middleware Net-Opp

Uma das principais vantagens do middleware é facilitar o trabalho do desenvolvedor de aplicações oportunistas, liberando-o de se preocupar com a infraestrutura de rede e a troca de conteúdos. O usuário pode escrever sua aplicação e conectá-la sem impacto ao Net-Opp. A avaliação deste tipo de benefício não é possível de medir através de técnicas de simulação, mas deve ser levada em consideração.

5.1. Cenários e Métricas

A fim de provar a viabilidade de adotar o middleware em uma rede oportunista, é importante avaliar seu impacto no tempo de formação topológica de rede, tempo de atraso na transferência de arquivos e a taxa de transmissão. Estes três experimentos foram realizados em laboratório, de maneira controlada, onde os dispositivos ficaram sobre uma mesa com uma média de três metros de distância, não sendo considerado interferências.

No primeiro experimento, foi medido o tempo de associação topológica de rede entre os dispositivos. O tempo é obtido através do Log da aplicação Android. Este experimento é importante para avaliar o impacto que a quantidade de dispositivos promove no tempo de formação da rede de comunicação.

No segundo experimento, a aplicação foi alterada de modo que oito dispositivos requisitassem um arquivo de 9MB a um dispositivo. Foi medido a taxa de transmissão de pacotes entre os dispositivos através do cálculo dos tempos e do tamanho do arquivo. O objetivo é avaliar como a rede se comporta quando um dispositivo realiza a transmissão de um arquivo para vários dispositivos (quantidades diferentes) ao mesmo tempo.

No terceiro experimento foi realizado comparações com os middlewares CAMEO e Hagggle. Foi medido o tempo de atraso para a transferência de um arquivo de 6.4MB entre dois tablets. O atraso é o intervalo de tempo que se inicia quando o aplicativo envia uma solicitação para o middleware (Net-Opp, CAMEO ou Hagggle) para baixar o arquivo, e termina quando o middleware notifica a transferência concluída a aplicação.

Enquanto que no segundo experimento foi utilizado dois tablets, no primeiro e segundo experimentos foram utilizados nove tablets, e todos os experimentos foram executados 30 vezes em cada dispositivo simultaneamente. Os dados dos três experimentos foram obtidos realizando cálculos na própria aplicação *Crowd Wi-Fi*, sendo considerado um intervalo de confiança de 95%. Foi utilizado quadros de controle RTS/CTS e potência TX padrão do dispositivo de 20 dBm.

5.2. Resultados

Antes de apresentar os resultados, vale ressaltar, que em todos os experimentos, os dispositivos comunicaram-se automaticamente, sem a necessidade de um usuário para intervir no processo, diferentemente como ocorre em [Su 2007, Pietilainen 2009, Dubois 2013], onde é necessária interação humana para o pareamento entre os dispositivos. Todo esse processo transparente foi conseguido graças as funcionalidades do middleware Net-Opp.

A Figura 5 ilustra os resultados do primeiro experimento. Pode-se observar na Figura 5 que quando há poucos dispositivos, o tempo de formação topológica de rede é grande, e sua faixa de erro também. Porém, quando a quantidade de dispositivos aumenta, o tempo de formação topológica de rede diminui e a taxa de erro também. Isso acontece por que quando há poucos dispositivos, a probabilidade dos dispositivos ficarem ao mesmo tempo escaneando ou se tornando ponto de acesso é maior do que quando há uma quantidade maior de dispositivos.

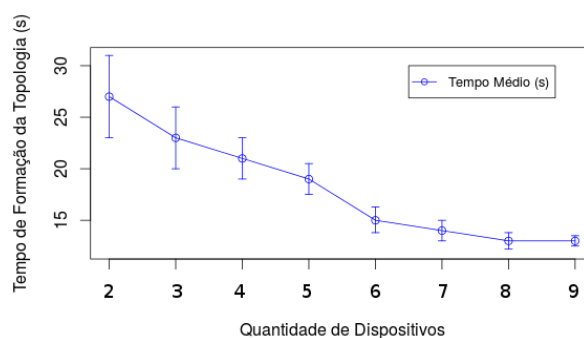


Figura 5. Tempo de associação da rede de comunicação.

No segundo experimento, pode-se observar na Figura 6, que a quantidade de dispositivos também influencia na taxa de transmissão, onde a taxa diminui de acordo que a quantidade de dispositivos que recebem um arquivo aumenta. Isso acontece porque o dispositivo servidor que está cuidando de transmitir o arquivo, tem um trabalho maior com quantidade maiores de dispositivos, e assim a banda de conexão desse dispositivo está mais ocupada com várias conexões simultâneas e mais pacotes para serem processados.

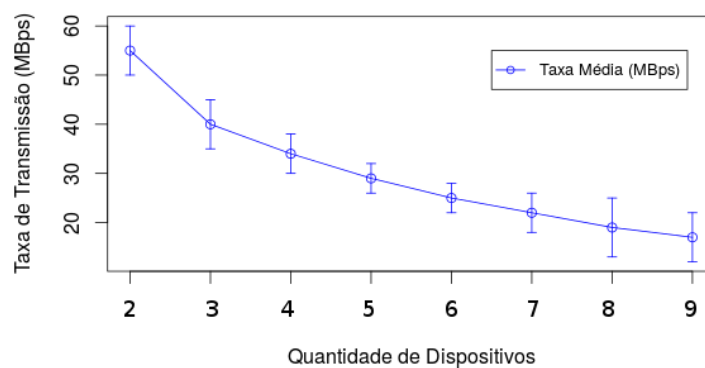


Figura 6. Taxa de transmissão de pacotes.

No terceiro experimento, Net-Opp conseguiu ser mais eficiente que CAMEO e Haggie no atraso de transmissão de arquivos. Na Figura 7, pode-se observar que Net-Opp teve um atraso médio de 4000ms para transferência do arquivo de 6.4MB, enquanto que CAMEO e Haggie, tiveram respectivamente 10000ms e 75000ms. Essa eficiência é principalmente devida às características internas da arquitetura de Net-Opp. Por ser uma arquitetura simples, uma quantidade menor de mensagens são trocadas entre os módulos do middleware Net-Opp em relação aos middlewares CAMEO e Haggie. A modularidade excessiva das arquiteturas de CAMEO e Haggie resultou numa sobrecarga de mensagens internas que afetaram o desempenho dos serviços ativos.

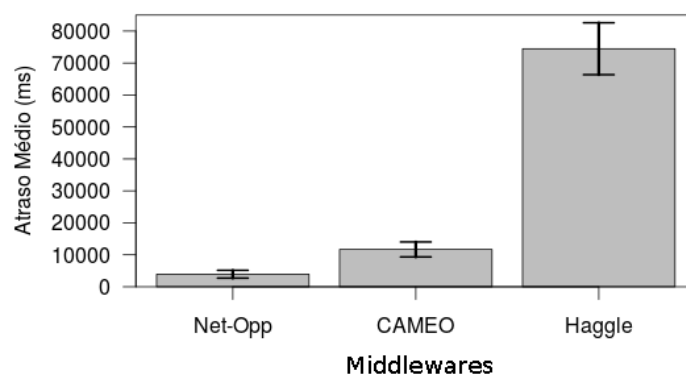


Figura 7. Tempo de atraso na transferência de arquivos.

6. Conclusão e Trabalhos Futuros

Neste artigo, foi apresentado Net-Opp, um middleware que permite o desenvolvimento fácil e eficiente de aplicações oportunistas. Net-Opp cria uma camada de abstração dos

recursos de comunicação entre o Sistema Operacional e as aplicações, promovendo a formação de redes e a troca de conteúdos entre os dispositivos móveis. Com o Net-Opp, o programador conta com um ambiente confiável de comunicação, onde todo o processo de formação de rede é realizado de forma automática e transparente, sem necessidade de pareamento entre os dispositivos e interação humana.

Os resultados apresentados neste artigo, mostraram em experiências reais a eficiência de Net-Opp na formação de rede e na troca de conteúdos entre os dispositivos móveis, sendo escalável e promovendo uma comunicação transparente não necessitando de interação humana. Por ser uma arquitetura voltada para comunicação *D2D (device-to-device)* oportunista e possibilitar uma comunicação transparente, Net-Opp também pode ser empregada em aplicações *M2M (machine-to-machine)* e *V2V (vehicle-to-vehicle)*.

Como trabalhos futuros, além do aprimoramento do middleware Net-Opp, pretende-se estender os estudos, empregando o uso do middleware em diferentes aplicações e maiores quantidades de dispositivos, com o propósito de avaliar mais profundamente o comportamento do middleware nessa estrutura de rede.

7. Agradecimentos

Agradecimentos a FAPEMIG, Gorceix, UFOP.

Referências

- R. K. Ganti, Fan Ye, e Hui Lei. (2011). Mobile crowdsensing: current state and future challenges. Em *Communications Magazine IEEE*, 49, 32–39.
- H. Ma, D. Zhao, e P. Yuan. (2014). Opportunities in mobile crowd sensing. Em *Communications Magazine, IEEE*, 52, 29–35.
- L. Pelusi, A. Passarella, M. Conti. (2006). Opportunistic networking: data forwarding in disconnected mobile ad hoc networks. Em *Communications Magazine, IEEE*, 44, 134–141.
- C. Boldrini, K. Lee, M. Onen, J. Ott, e E. Pagani. (2014). Opportunistic networks. Em *Computer Communications*, 48, 1–4.
- V. Vukadinovic, e G. Karlsson. (2010). Spectral efficiency of mobility-assisted podcasting in cellular networks. Em *International Workshop on Mobile Opportunistic Networking*, 51–57.
- B. Han, P. Hui, M. V. Marathe, e et al. (2010). Cellular traffic offloading through opportunistic communications: a case study. Em *Chants*, 31–38.
- M. Dekker, e C. Karsberg. (2013). Annual Incident Reports 2013. Em *Technical Report October*, ENISA.
- M. Helft, e D. Barboza. (2010). Google Shuts China Site in Dispute over Censorship. Em *The New York Times*, March(22).
- T. M. Chen. (2011). Governments and the executive 'internet kill switch'. Em *IEEE Netw*, 25 (2), 2–3.
- J. Ott, e J. Kangasharju. (2012). Opportunistic Content Sharing Applications. Em *Proc. of the ACM MobiHoc NOM workshop*, 19–24.

- M. Pitkanen, T. Karkkainen, J. Ott, e et al. (2012). SCAMPI: Service platform for soCial Aware Mobile and Pervasive computIng. Em *Proc. of the ACM workshop on Mobile Cloud Computing*, 503–508.
- J. Ott, E. Hyytia, P. Lassila, T. Vaegs, e J. Kangasharju, (2011). Floating Content: Information Sharing in Urban Areas. Em *IEEE Percom*, 136–146.
- A. Lindgren. (2011). Social networking in a disconnected network: fbDTN: facebook over DTN. Em *Proc. of ACM MobiCom CHANTS workshop (demo)*, 69–70.
- IEEE-SA (2007). IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Em <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>
- A. K. Pietilainen, e C. Diot. (2009). Experimenting with Opportunistic Networking. Em *Proc. of the ACM MobiArch Workshop*, 28–36.
- J.C. Haartsen. (2000). The Bluetooth radio system. Em *Personal Communications, IEEE*, 28–36.
- Wi-Fi Alliance, P2P Technical Group (2009). Wi-Fi Peer-to-Peer (P2P) Technical 7 Specification. Em http://wi-fi.org/Wi-Fi_Direct.php
- Y. Wang, A. V. Vasilakos, Q. Jin, e J. Ma (2014). Survey on mobile social networking in proximity (MSNP): approaches, challenges and architecture. Em *Wireless networks*, 20(6), 1295–1311.
- X. Hu, T.H.S. Chu, V.C.M. Leung e et al. (2014). A Survey on Mobile Social Networks: Applications, Platforms, System Architectures, and Future Research Directions. Em *Communications Surveys & Tutorials, IEEE*.
- J. Su, J. Scott, P. Hui, e et al. (2007). Hagggle: Seamless Networking for Mobile Applications. Em *UbiComp 2007: Ubiquitous Computing*, 391.
- A. K. Pietilainen, E. Oliver, J. LeBrun, e et al (2009). MobiClique: middleware for mobile social networking. Em *Proc. of the ACM workshop on Online social networks*, 49–54.
- D.J. Dubois, Y. Bando, K. Watanabe, e H. Holtzman. (2013). Shair: Extensible middleware for mobile peer-to-peer resource sharing. Em *In Proc. of Joint Meeting on Foundations of Software Engineering*, 687–690.
- V. Arnaboldi, M. Conti, e F. Delmastro (2014). CAMEO: A novel context-aware middleware for opportunistic mobile social networks. Em *Pervasive and Mobile Computing*, 11, 148–167.
- Apple iOS Em <http://developer.apple.com/technologies/ios/>
- Android Phone Em <http://www.android.com>
- Windows Phone Em <http://www.windowsphone.com>
- H. Wirtz, T. Heer, R. Backhaus, e K. Wehrle. (2011). Establishing mobile ad-hoc networks in 802.11 infrastructure mode. Em *Proc. of the ACM workshop on Challenged networks*, 49–52.
- S. Trifunovic, B. Distl, D. Schatzmann, e F. Legendre. (2011). WiFi-Opp: ad-hoc-less opportunistic networking. Em *Proc. of the ACM workshop on Challenged networks*, 37–42.