

Redes Orientadas a Conteúdo Baseadas em Controladores Hierárquicos

João Vitor Torres, Lino Henrique G. Ferraz, Otto Carlos M. B. Duarte

¹Universidade Federal do Rio de Janeiro - GTA/COPPE/UFRJ
Rio de Janeiro, Brazil
Email: {jvitor, lino, otto}@gta.ufrj.br

Abstract. *Content Centric Network (CCN) routing schemes must learn routes to named data locations, so routers know where to send interest packets. Nevertheless, the huge amount of named data and non-aggregated prefixes challenge path evaluation, because routers proportionally store more routes and exchange more control messages. This article proposes a routing scheme based on control plane separation assuring router memory consumption proportional to traffic and reducing control message exchange for routing flatly named data. The routing scheme employs a hierarchy of multiple controllers which have two main functions: i) acquire topology and calculate routes, and ii) store named data locations. Distributed hash tables distribute the storage of named data locations efficiently. Furthermore, as the proposal runs on top of CCN, it preserves Content Centric Network features. The initial assessment points that the data location distribution and on demand route installation scheme produces scalable routing of named data.*

Resumo. *As Redes Orientadas a Conteúdo precisam aprender a localização dos conteúdos para definir rotas e encaminhar os pacotes de interesse. Contudo, a enorme quantidade de prefixos distintos de nome de conteúdo constitui um desafio para tarefa de localização, pois amplia proporcionalmente o número de rotas por roteador, e também de mensagens de controle trocadas pelos protocolos de roteamento. Este artigo propõe um esquema de roteamento para redes orientadas a conteúdo baseado em separação de planos que garante consumo de memória no roteador proporcional ao tráfego e número reduzido de mensagens de controle no roteamento de conteúdo com nomes planos. O esquema de roteamento proposto utiliza uma hierarquia de múltiplos elementos controladores com duas funções principais: i) monitorar a topologia e calcular as rotas, e ii) armazenar a localização dos conteúdos. Tabelas hash distribuídas armazenam as localizações dos conteúdos e todos os pacotes são orientados ao conteúdo, preservando as propriedades das Redes Orientadas a Conteúdo. A análise inicial indica que a proposta de separar e dividir a tarefa de localização de conteúdos aliada à instalação de rotas por demanda fornece roteamento de nomes planos com uso escalável e eficiente de recursos.*

1. Introdução

As Redes Orientadas a Conteúdo (*Content Centric Network* - CCN) [Jacobson et al. 2009b, Zhang et al. 2010] mudam drasticamente os princípios de

Este trabalho foi realizado com recursos da FINEP, FUNTTEL, CNPq, CAPES, FUJB, FAPERJ, CTIC e UOL.

roteamento, passando o foco diretamente para o nome do conteúdo e não mais o endereço da máquina, ou hospedeiro, como é hoje na Internet. Isto tem a grande vantagem de permitir que cópias locais do conteúdo sejam armazenadas em diferentes pontos e, conseqüentemente, mais perto do usuário ao invés de solicitadas repetidamente à fonte. Um dos principais desafios da rede orientada a conteúdo é a escalabilidade da localização e do roteamento uma vez que a quantidade de conteúdo é bem maior que a quantidade de hospedeiros. Para tratar a tarefa de localização de forma escalável, a proposta de rede orientada a conteúdo (CCN) utiliza nomeação hierárquica de conteúdos, organizando os nomes em uma estrutura em níveis vinculada à topologia de nós da rede. Esta estrutura permite a agregação dos nomes de conteúdo em seus prefixos comuns na direção do nível mais alto da hierarquia e a divulgação concisa de sumários de localização.

Para garantir esta agregação, a localização do conteúdo fica restrita a sua posição na hierarquia de nomes e não são divulgadas rotas para cópias fora do caminho até a fonte. Sob estas premissas, a proposta CCN usa esquemas de roteamento baseados em anúncios de prefixos de nomes tornando-os roteáveis. Estes esquemas, como por exemplo, *Open Shortest Path First for Named Data Network* (OSPFN) [Wang et al. 2012], herdaram as características do IP vinculadas ao roteamento por disseminação e agregação de prefixos. Estas abordagens são sensíveis em relação à quantidade de prefixos não agregados de nomes de conteúdo, bem maior do que de prefixos IP, pois consomem recursos ao proativamente (periodicamente) difundir na rede a localização de todos os conteúdos. Além disso, a crescente mobilidade, a replicação e a hospedagem multidomicílio de conteúdos desagregam prefixos e aumentam ainda mais o consumo de recursos, pois exigem alto tráfego de controle e grandes tabelas de encaminhamento, o que as torna economicamente inviáveis atualmente [Perino e Varvello 2011].

Este artigo propõe um esquema de roteamento para Redes Orientadas a Conteúdo (CCN) baseado em controladores hierárquicos. A ideia básica é garantir a escalabilidade e uma melhor utilização de recursos através da separação e estruturação do plano de controle em uma hierarquia de elementos controladores para monitorar a topologia, calcular rotas entre nós, localizar e rotear conteúdos. A hierarquia divide cada nível em zonas permitindo sua programação conjunta a partir do nível superior. Em cada zona, inicialmente são instaladas rotas entre os nós roteadores e controladores. Em seguida os conteúdos são registrados e, finalmente as rotas para conteúdos podem ser instaladas por demanda dos consumidores de conteúdo.

O esquema de roteamento proposto não requer novas mensagens e, portanto, utiliza apenas os pacotes de interesse e os de dados próprios da rede CCN, preservando integralmente todas as propriedades CCN tais como: armazenamento local, controle de congestionamento, detecção de falha de rede e diversidade de caminhos. A semântica dos pacotes de interesse é estendida para reduzir a sobrecarga de controle ao embutir comandos de controle nos seus prefixos.

O armazenamento da localização de conteúdos é balanceado entre diversos elementos de tabelas *hash* distribuídas (*Distributed Hash Table* - DHT), sendo utilizada uma DHT em cada zona da hierarquia. No nível superior da hierarquia de controle, um processo distribuído garante a troca de informação entre controladores e convergência da rede. Isto permite a entrada e saída de conteúdos, roteadores, controladores e membros da DHT com redistribuição de carga.

O restante deste artigo está organizado da forma a seguir. Na Seção 2 os principais trabalhos relacionados são apresentados. A proposta é detalhada na Seção 3. Na Seção 4 discute-se o impacto das mensagens de controle, a mobilidade, a segurança, a falha e o particionamento da rede e a distribuição de carga. Por fim, na Seção 5 ressaltam-se as principais conclusões e os trabalhos futuros.

2. Trabalhos Relacionados

Jacobson *et al.* propuseram o paradigma de paridade entre pacotes de interesse e de dados através do modelo de rede orientada a conteúdo (*Content Centric Networking* - CCN) [Jacobson et al. 2009b, Jacobson et al. 2009a]. A sua proposta resultou no projeto *Named Data Network* (NDN), cujo objetivo é construir uma nova arquitetura de rede [Zhang et al. 2010]. O modelo CCN permite, através de uma camada de estratégia, a rápida detecção de problemas na rede e uso de caminhos alternativos [Yia et al. 2012]. Contudo, os esquemas atuais de roteamento aplicados no CCN constroem as regras de encaminhamento baseadas no OSPF. O OSPF inunda toda a rede com atualizações de prefixos não agregados, impondo fortes limitações de escalabilidade quanto ao número de prefixos distintos e a mobilidade do conteúdo [Wang et al. 2012].

Baid *et al.* utiliza um esquema que mapeia os prefixos de conteúdo em nomes planos únicos e este nomes em endereços topológicos de rede, reduzindo os requisitos de memória e de troca de mensagens de controle. Este esquema utiliza um sistema de DHT para prover este mapeamento [Baid et al. 2012]. D'Ambrosio *et al.* utiliza um esquema de múltiplas DHTs organizadas em hierarquia, na qual cada DHT mapeia a localização do conteúdo em identificadores topológicos de diferentes níveis, como por exemplo, máquina, rede e sistema autônomo [D'Ambrosio et al. 2011]. Este esquema distribui a tarefa de mapeamento em camadas e reduz o número de identificadores em cada nível.

Outras propostas também focam o conteúdo como o CCN, mas utilizam uma abordagem baseada numa arquitetura de subscrição com publicador e assinante [de Brito et al. 2012]. Nestas abordagens, ao contrário do CCN, o roteamento é iniciado do produtor para o consumidor de conteúdo e a tarefa de escalabilidade é entregar o conteúdo apenas para os respectivos assinantes. Carzaniga *et al.* compara a requisição de conteúdo por demanda e o balanço de fluxo do CCN com abordagens de subscrição sem este suporte, mas capazes de assinar canais de conteúdo com uma única requisição. Eles apresentam uma solução híbrida com uso reduzido e seletivo de estado nos roteadores quanto aos fluxos de pacotes [Carzaniga et al. 2011].

Propostas do tipo redes definidas por *software* (*Software Defined Networks* - SDN) empregam um controlador para, por demanda, instalar nos nós da rede regras de encaminhamento de pacotes por fluxo [Mattos et al. 2011, Fernandes et al. 2011, McKeown et al. 2008]. Estas propostas fazem a separação das funções de roteamento em plano de controle, que calcula as rotas, e plano de dados, que executa o encaminhamento dos pacotes. Um controlador processa as mensagens de controle e, assim, reduz os requisitos de memória e de processamento dos nós comutadores. As redes definidas por *software* são boas candidatas para redes da próxima geração [FITS 2012].

A proposta CCN garante o balanço de fluxo de pacotes através da paridade interesse e dado, o que é fundamental para prover adaptabilidade a falhas. Porém, os protoco-

los de roteamento tradicionais não são escaláveis para os requisitos de quantidade de prefixos distintos do CCN. O uso de DHTs nas propostas listadas acima fornece um serviço de resolução de nome, mas o encaminhamento dos pacotes é baseado nos identificadores topológicos de rede perdendo as propriedades CCN. As propostas SDN com separação de planos utilizam identificadores topológicos de rede para encaminhamento de pacotes e também perdem as propriedades CCN. Este artigo une a resolução de localização do conteúdo baseado em DHTs, a qual permite nomes planos de forma escalável, com a separação de planos e cálculo de rotas por controladores, os quais instalam por demanda nos comutadores regras de encaminhamento de pacotes baseadas diretamente nos nomes de conteúdo e mantém as propriedades CCN. A instalação de regras utiliza ainda pacotes de interesse com semântica estendida reduzindo a sobrecarga de comunicação ao embutir semântica adicional nos prefixos, prática introduzida na proposta Voice over CCN (VoCCN) [Jacobson et al. 2009a].

3. O Esquema de Roteamento Proposto

O esquema de roteamento proposto não requer nenhum tipo de pacote adicional e, portanto, é integralmente suportado apenas com os pacotes CCN de interesse e dados. O encaminhamento de pacotes em cada roteador segue o processamento padrão CCN: i) buscando e armazenamento cópias de conteúdo no repositório CS (*Content Store*), ii) utilizando as entradas na PIT (*Pending Interest Table*) para indicar o caminho reverso ao do interesse e, encaminhar para interface de saída na direção do consumidor do conteúdo o pacote de dados e, iii) encaminhar o pacote de interesse de acordo com a FIB (*Forwarding Information Base*) [Zhang et al. 2010]. O controle da rede se baseia na separação dos planos de dados e controle, usando, portanto, elementos específicos, chamados controladores, para instalação das rotas de encaminhamento no plano de dados, ou seja, as entradas na FIB dos roteadores. A interface de comunicação entre roteadores e controladores é baseada em pacotes de interesse nos quais se estendeu a semântica para obter tratamento específico nos nós da rede.

Existem três tipos de elementos de rede: roteador, controlador e nó de DHT. Os roteadores têm a função básica de encaminhamento de pacotes e, em especial, os roteadores diretamente conectados aos produtores de conteúdo são responsáveis pelo registro nos controladores da localização de conteúdos. Os controladores por sua vez, além de instalar regras na FIB dos roteadores, armazenam a localização dos conteúdos e calculam as entradas FIB de cada roteador até estes conteúdos. Este armazenamento é realizado utilizando um sistema de DHT.

Neste artigo, um nome ou prefixo de conteúdo se aplica a qualquer dado endereçável e alcançável, seja um arquivo, um serviço ou uma máquina na rede. Todos os roteadores e controladores possuem um ID, portanto são também endereçáveis na rede.

Os prefixos especiais utilizados no esquema são listados a seguir. O prefixo `"/HELLO"` busca o ID dos nós vizinhos imediatos; `"/router"` é seguido do ID do roteador e encaminha interesses para um roteador específico; `"/route"` é um comando de instalação de rota a ser processado pelos roteadores; `"/controller"` encaminha interesses para qualquer controlador e, se seguido do ID do controlador, aponta para um controlador específico; finalmente, o prefixo `"/register"` indica requisição de regis-

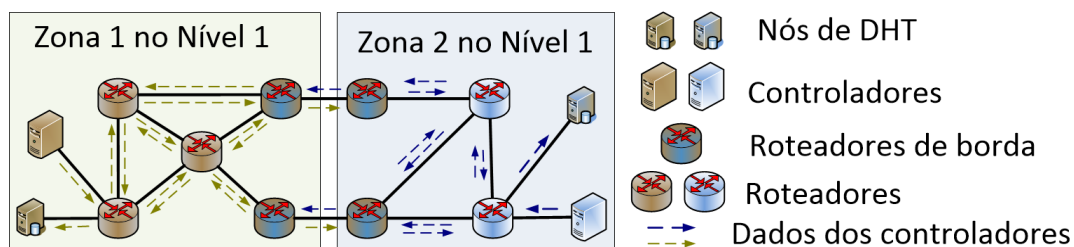


Figura 1. Exemplo de divisão de roteadores em zonas com um controlador, um nó DHT por zona e roteadores de borda. Os pacotes de interesse são omitidos para simplificação.

tro de novo nome de conteúdo.

Os roteadores inicialmente não tem nenhuma regra de encaminhamento na FIB, exceto as regras que endereçam a si próprios para processamento local, como `"/router/routerID"`, `"/route"`, `"/HELLO"` e `"/register"`.

A seguir, a estrutura de controladores hierárquicos e os procedimentos necessários para sua operação são apresentados. O uso de controladores hierárquicos tem três objetivos principais: i) reduzir o número de elementos de roteamento num único processo distribuído plano, ii) isolar as falhas restringindo aos níveis correspondentes e iii) visar menor tempo de convergência.

3.1. Controladores Hierárquicos

Os roteadores da rede são divididos em zonas, sendo cada zona controlada por um controlador, ver Figura 1. Por sua vez, os controladores de zona são agrupados em zonas com nível hierárquico mais elevado, Zonas de nível 2, e um controlador gerencia um grupo de controladores de Nível 2 formando uma Zona de Nível 3. Este agrupamento hierárquico e sucessivo permite adicionar novos níveis conforme necessário, ver Figura 2. No nível mais baixo, cada controlador é responsável pelas rotas entre roteadores internos a sua zona. Para rotas externas a sua zona, o controlador consulta o seu controlador de nível hierárquico superior para obter o próximo salto. No nível de hierarquia mais alto, cada controlador obtém os seus controladores vizinhos de mesmo nível e troca diretamente com estes vizinhos informações sobre a topologia de zonas possibilitando montar rotas externas a sua zona sem auxílio de um controlador superior.

Cada zona hierárquica utiliza uma DHT para armazenar a localização dos conteúdos alcançáveis na hierarquia de nível inferior, onde o *hash* do prefixo do conteúdo é a chave da DHT e o ID do controlador responsável pelo prefixo é o valor da entrada correspondente da DHT. No nível mais baixo o valor desta entrada é o ID do roteador. A DHT é composta por elementos auxiliares proporcionando distribuição de carga e escalabilidade. A distribuição de chaves entre nós da DHT é ordenada de acordo com o seu procedimento particular e não impõe uma implementação específica.

3.1.1. Divisão e Topologia de Zonas

A divisão dos roteadores em zonas é definida pela ordem temporal de chegada das respostas dos controladores à inundação de pacotes de interesse iniciada para descoberta de controladores, procedimento denominado Descoberta de Controladores, de-

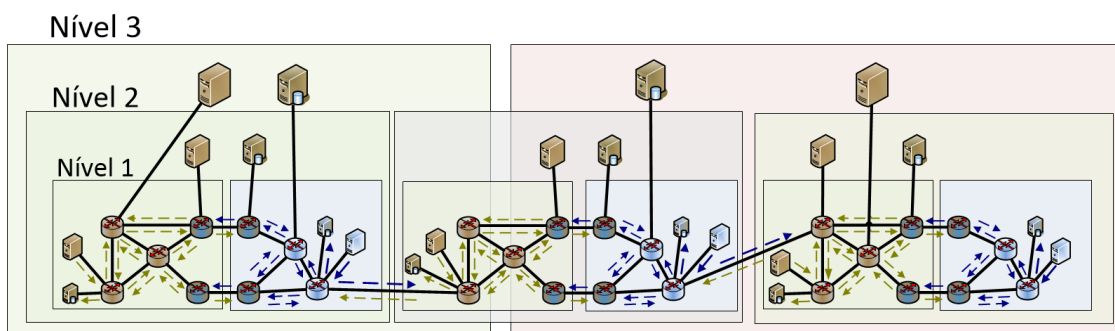


Figura 2. Exemplo em 3 níveis de divisão em controladores hierárquicos em zonas.

talhado a frente. Este procedimento atribui um controlador responsável por cada zona. Estes controladores, chamados de Controladores de Nível 1, replicam o procedimento de inundação na busca de seus controladores de nível superiores usando prefixos especiais do tipo `"/controller/levelX"`, onde "X" indica o nível superior. Assim, o procedimento de divisão em zonas se repete em cada nível. Este procedimento de inundação é repetido periodicamente e garante que os roteadores na borda entre zonas obtenham o controlador recebido pelo roteador vizinho. Os roteadores de borda informam seu controlador sobre os múltiplos controladores encontrados de cada nível definindo o último salto para a zona vizinha. Os controladores do nível "X" se registram nos controladores de nível "X+1" e, propagam a informação de vizinhança informada pelos roteadores.

No nível mais alto da hierarquia, para obter a topologia de controladores na rede, cada controlador envia para seus controladores vizinhos um pacote de interesse com o prefixo `"/controller/levelY/controllerID/topology"`. O controlador responde com a lista de controladores conhecidos e suas adjacências, permitindo o cálculo de rotas entre zonas. Além disso, os controladores também informam os controladores já conhecidos sobre novos controladores com um pacote de interesse para o prefixo `"/controller/controllerID/topologyUpdate"`. O controlador receptor confirma o recebimento e solicita a topologia atualizada.

3.1.2. Composição de Caminhos

Para comunicação entre zonas, cada controlador consulta seu controlador superior buscando a zona de próximo salto na direção do destino. No nível mais alto, todos controladores conhecem a topologia superior de zonas e calculam localmente a zona de próximo salto. Então, a zona de próximo salto é refinada a cada nível pelos controladores na hierarquia abaixo e, com a zona de próximo salto, o controlador de Nível 1 calcula e instala uma rota até o roteador de borda da sua zona na direção da zona de próximo salto. O roteador de borda da zona seguinte consulta seu próprio controlador para encaminhar adiante.

3.1.3. Operação da DHT

Os nós da DHT de cada zona se registram diretamente no respectivo controlador, o qual encaminha os pedidos e registros de conteúdo para o nó adequado. Os controladores

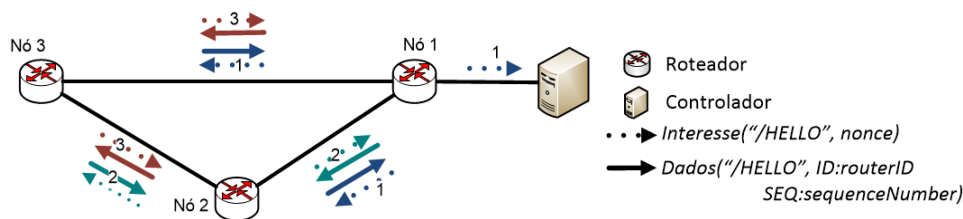


Figura 3. A Descoberta de Vizinhos através de difusão de pacotes de interesse "/HELLO". Os números nas setas indicam o gerador do pacote de interesse.

do nível mais alto divulgam entre si os seus nós da DHT formando uma única DHT. Quando um nó entra ou sai da DHT, as chaves armazenadas por ele são redistribuídas. Para conteúdos acessíveis em zonas fora da hierarquia inferior, o controlador propaga o registro para o controlador e DHT superiores acrescentando seu ID ao registro. O nível de registro e busca de conteúdos é incluído no interesse para evitar a busca recursiva em todos os níveis. Os prefixos específicos para manipulação dos nós da DHT e seus registros não são ilustrados aqui por limitação de espaço.

3.2. Inicialização e Monitoração de Topologia

Nesta fase, os roteadores localizam o controlador e se registram. Com os registros, o controlador adquire a topologia da rede e calcula rotas até os roteadores dentro da sua zona. A fase possui três procedimentos: a Descoberta de Vizinhos com Hello, a Descoberta de Controlador e o Registro de Roteador. Estes procedimentos rodam periodicamente para manter uma visão atualizada da topologia. A seguir os procedimentos e algoritmos para descoberta de rotas são descritos.

3.2.1. O Procedimento de Descoberta de Vizinhos com Hello

Para descobrir seus vizinhos imediatos, os roteadores enviam periodicamente pacotes de interesse em todas as interfaces. Cada roteador vizinho responde com um pacote de dados contendo seu próprio ID e um número de sequência. A Figura 3 ilustra o fluxo de pacotes. O número de sequência fornece coerência de topologia, sendo atualizado sempre que um roteador detecta alteração de um vizinho ou interface. O roteador recebe o pacote de dados e instala uma entrada na FIB para o prefixo `"/router/routerID"` apontando para a interface de recebimento. O `routerID`, o `sequenceNumber`, a interface de conexão com o vizinho e uma métrica para a interface são armazenados em uma tabela de vizinhos. Um exemplo de métrica é o tempo de ida e volta até o vizinho, calculado a partir do intervalo entre envio do interesse e recebimento do pacote de dados. Através deste procedimento, todos os roteadores tem uma lista atualizada de vizinhos.

3.2.2. O Procedimento de Descoberta de Controlador

No procedimento de Descoberta de Controlador, os roteadores inundam a rede com pacotes de interesse por múltiplos caminhos até o controlador. O caminho de resposta mais rápida é escolhido por cada roteador. Estes caminhos permitem acessar o controlador e registrar os roteadores, conforme descrito na próxima seção.

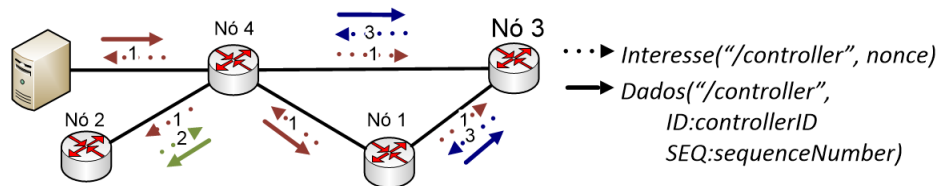


Figura 4. A Descoberta de Controlador através de inundação de pacotes de interesse para descoberta de caminhos. Inundação do nó 4 omitida.

Na inundação¹, os roteadores enviam pacotes de interesse de descoberta do controlador em todas as interfaces. Cada roteador, ao receber este pacote de interesse, adiciona uma entrada na sua *Pending Interest Table* (PIT) e responde a partir de sua CS ou encaminha o interesse para todas as demais interfaces. O controlador, ao receber o interesse, responde com um pacote de dados contendo seu ID e um número de sequência. O número de sequência é atualizado pelo controlador em intervalos ajustáveis de tempo. O roteador armazena o pacote de dados recebido na sua CS por um pequeno período e o encaminha de acordo com a PIT. A Figura 4 ilustra o fluxo de pacotes. O roteador instala ainda entradas na FIB para o prefixo `"/controller"` e `"/controller/controllerID"` através da interface de entrada do pacote de dados e armazena o ID e o número de sequência do controlador em uma tabela de controladores. Todos os roteadores enviam ou retransmitem o interesse, garantindo o recebimento do pacote e dados e a obtenção de rotas para o controlador. Pacotes de interesse atrasados são respondidos diretamente da CS reduzindo a sobrecarga do procedimento de inundação.

Periodicamente, cada roteador envia novos pacotes de interesse para descoberta e atualização de rotas para o controlador. Caso a resposta contenha um número de sequência igual ou inferior ao armazenado na sua tabela de controladores, o pacote de dados é assumido como antigo e o roteador não atualiza a FIB.

3.2.3. O Procedimento de Registro de Roteador

Assim que obtém o ID do controlador e um caminho para alcançá-lo, o roteador se registra no controlador enviando um pacote de interesse de semântica estendida com esta indicação. A Figura 5 ilustra o fluxo de pacotes, onde `controllerID` é o ID do controlador conhecido na tabela de controladores, `registerRouter` é uma palavra reservada que indica o pedido de registro para o roteador de ID `routerID`, e `seq/sequenceNumber` é o último número de sequência anunciado na Descoberta de Vizinhos. Cada roteador que encaminha o pacote de interesse em direção ao controlador, instala uma entrada na sua FIB para o prefixo `"/router/routerID"` através da interface de entrada do interesse. O controlador responde o interesse com um pacote de dados de confirmação e cria uma entrada na sua tabela de roteadores.

Após o registro, o controlador obtém os vizinhos deste roteador enviando um interesse específico para o roteador. Os roteadores no caminho já possuem entradas na FIB para o `routerID` e encaminham o interesse diretamente. O roteador `routerID` responde com um pacote de dados contendo o seu próprio ID, um número de sequência

¹Não há sincronia entre roteadores para início simultâneo da inundação.

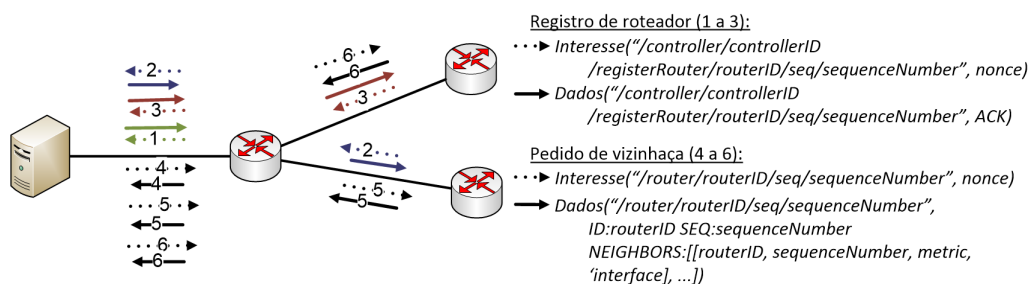


Figura 5. O controlador obtém a topologia da rede recebendo os registros dos roteadores e solicitando a lista de vizinhos de cada roteador.

e a sua lista de vizinhos, conforme Figura 5. Este pacote de dados atualiza o controlador com a lista de vizinhos do roteador. O número de sequência fornece ao controlador um parâmetro para comparar a coerência das informações enviadas por diferentes roteadores. Caso seja diferente, o controlador envia novo pacote de interesse para os roteadores que anunciaram o número de sequência antigo. Sempre que um roteador detecta uma mudança de topologia, o procedimento de registro é repetido, o número de sequência incrementado e o controlador obtém a topologia atualizada.

3.3. Roteamento para Obter Conteúdo

Os procedimentos da fase de Inicialização e Monitoração de Topologia permitem a todos os roteadores alcançar o controlador, atualizar a entrada e saída de nós e conexões e solicitar rotas. O controlador pode inferir a topologia da rede e, conseqüentemente, calcular as rotas entre dois pares quaisquer de roteadores. Contudo, na rede orientada a conteúdo o que interessa é a localização do conteúdo e o controlador não conhece a localização dos conteúdos. Para isto, os produtores precisam registrar os conteúdos no controlador e, assim o controlador pode instalar rotas para conteúdo nos roteadores.

3.3.1. Procedimento de Registro de Conteúdo

No registro de um novo conteúdo, o produtor envia um pacote de interesse com semântica estendida, Interesse 1 na Figura 6, onde "register" indica a intenção de registrar o nome "myprefix". O roteador diretamente conectado recebe este pacote, adiciona uma entrada na PIT e também adiciona uma entrada na FIB com o nome "myprefix" apontando para a interface de entrada do interesse. Na sequência, ao invés de encaminhar o pacote de interesse para uma de suas interfaces, o roteador gera e envia um novo interesse indicando a localização do conteúdo na direção do controlador, Interesse 2 na Figura 6. Ao receber este interesse, o controlador armazena o routerID como a localização do conteúdo "/myprefix" na tabela de localização de conteúdos. O controlador responde para o roteador com um pacote de dados de confirmação e o roteador responde em confirmação para o produtor.

3.3.2. Procedimento de Instalação de Rotas

Para obter um conteúdo, o consumidor de conteúdo envia um pacote de interesse para a rede, Interesse 1 na Figura 7. O primeiro roteador recebe este pacote e adiciona

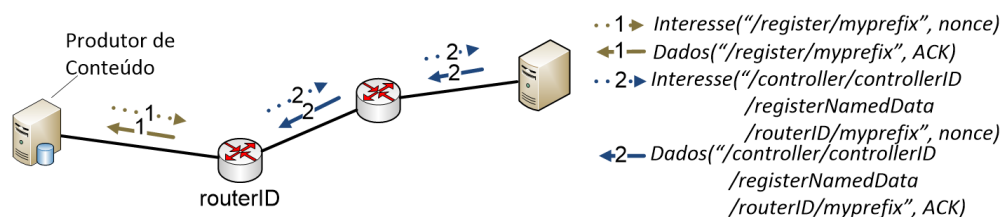


Figura 6. O Registro de Conteúdo realizado pelo roteador diretamente conectado ao Produtor de Conteúdo.

uma entrada na PIT. Caso não tenha entrada na FIB, o roteador solicita nova rota com um interesse de semântica estendida indicando este pedido, Interesse 2 na Figura 7. Neste pacote de interesse, "routeFrom/sourceRouterID" indica o roteador origem do pedido de rota. Visto que o prefixo "wantedprefix" já está registrado, o controlador sabe a rota para o destino. Então, o controlador calcula a melhor rota da origem até o destino e fornece a rota com um pacote de dados em resposta.

A resposta contém a informação a ser utilizada na instalação de rota, a qual abrange todo o caminho da origem ao destino. O controlador pode ainda incluir rotas alternativas no pacote de resposta ao pedido de rota, ver pacote de Dados 2 na Figura 7. Esta resposta inclui as palavras reservadas "installRouteAndForwardInterest" e "installRoute" para indicar o começo da rota, "endroute" para o fim da rota, "routingPreference" para a preferência de rota, e "toprefix" para indicar o prefixo desejado.

O roteador origem, ao receber o pacote de dados com a rota resposta, procura pelo seu ID e obtém o próximo salto. Então, o roteador adiciona uma entrada na sua FIB para o prefixo "/wantedprefix" através da interface de comunicação com o próximo salto.

Em seguida, o roteador origem usa a informação recebida do controlador para criar um pacote de interesse semanticamente estendido para instalar a rota nos roteadores do caminho. O próximo salto recebe este pacote de interesse e usa a informação contida no prefixo para criar uma entrada na FIB. Este procedimento se repete até o interesse atingir o roteador de destino, o qual já possui uma entrada na FIB para o "/wantedprefix". Caso o prefixo especial use a palavra reservada "installRouteAndForwardInterest", cada roteador no caminho adiciona uma entrada na PIT para o "/wantedprefix", porém não adiciona entrada na PIT referente ao pacote de interesse de instalação de rota. A Figura 8 ilustra o fluxo de pacotes para a instalação de rota.

Caso o prefixo especial tenha a palavra reservada "installRouteAndForwardInterest", o roteador destino também adiciona uma entrada para o "/wantedprefix" na sua PIT, cria e encaminha um pacote de interesse para o "/wantedprefix", Item (b) na Figura 8. Caso o prefixo especial contenha "installRoute", o roteador destino apenas responde com um pacote de dados de confirmação, Item (a) na Figura 8.

4. Discussão

Esta seção discute algumas questões que afetam a operação do esquema.

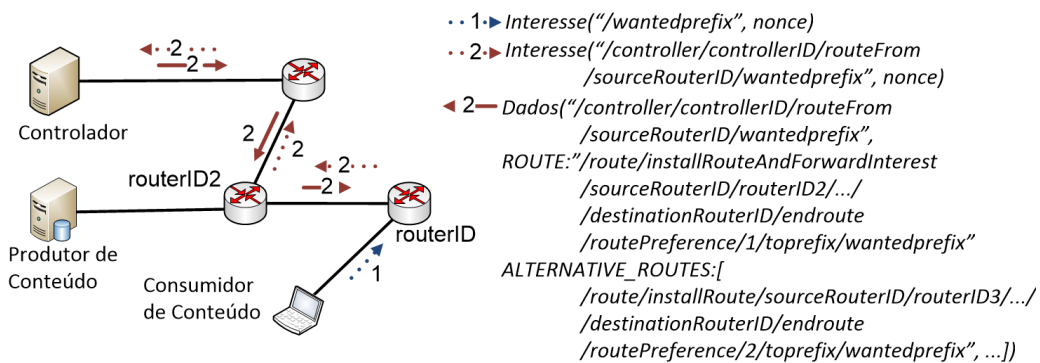


Figura 7. Solicitação de conteúdo do Consumidor (1) e Pedido de Rotas entre roteador e controlador (2).

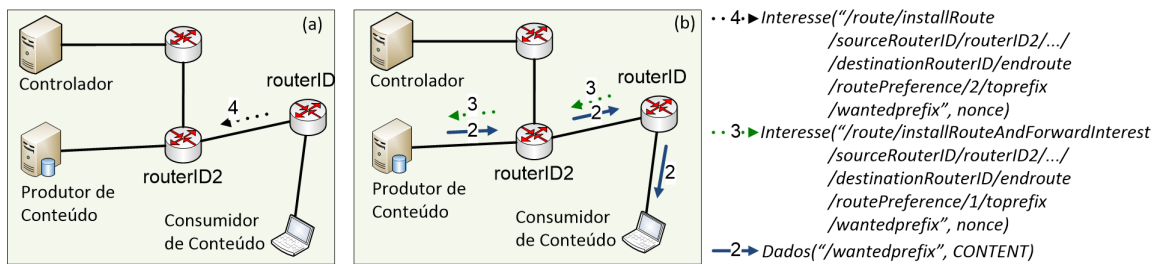


Figura 8. Instalação de Rotas. Item (a), instalação de rota sem busca de conteúdo. Item (b), instalação de rota e busca de conteúdo.

4.1. Número Estimado de Mensagens

O número de mensagens em cada procedimento é estimado a seguir. Na Descoberta de Vizinhos e na Descoberta de Controlador, o número é proporcional ao grau médio multiplicado pelo número de nós e se repete periodicamente. No Registro de Roteador, o número é proporcional ao número de nós multiplicado pela distância média entre roteador e controlador, ou diâmetro da rede. A taxa de alterações na topologia também afeta este último quantitativo.

No Registro de Conteúdo, o número de mensagens é proporcional à distância entre publicador e controlador e, também dependente do diâmetro da rede. A taxa de mobilidade de conteúdos também afeta este quantitativo. No Pedido de Conteúdo e Instalação de Rotas, o número é duplamente dependente do diâmetro da rede, primeiro na distância entre consumidor e controlador e segundo na distância entre consumidor e produtor. A correlação entre as solicitações de usuários afeta este quantitativo. É necessário ainda considerar as mensagens relativas à DHT.

Comparativamente, a divulgação de um prefixo não agregado via OSPF consome um número proporcional ao número de nós multiplicado pelo grau médio da rede. Outro ponto importante é a instalação de rotas com uma única consulta ao controlador que, comparada ao OpenFlow com consultas a cada salto, consome menos mensagens numa proporção relacionada ao diâmetro da rede.

4.2. Mobilidade

A mobilidade de consumidores e produtores afeta a entrega de conteúdos. No lado consumidor, basta o reenvio do interesse e novas rotas são instaladas. No lado produtor é mais complexo, pois é necessário informar a nova localização e apagar as rotas

já instaladas para a localização antiga. Para tanto, o produtor envia novo registro de seu conteúdo na nova localização e, o roteador da antiga localização responde aos interesses sem conteúdo com um pacote de dados "NACK No Data" que força a remoção das rotas até o consumidor.

Os controladores e a DHT atuam como um sistema de nome dinâmico fornecendo a localização. Isto permite o registro na DHT de cópias de conteúdo permitindo a busca de conteúdo fora do caminho até a fonte original. Para isto, DHT deve suportar múltiplas entradas de localização por conteúdo. O controlador ao receber múltiplas localizações tem opções para escolha da cópia mais adequada.

4.3. Segurança

Na rede CCN, todo produtor tem seu próprio par de chaves que pode ser usado para autenticar as mensagens. Porém, o controle da rede usando pacotes de interesse com prefixos semanticamente estendidos abre portas de ataque contra o funcionamento da rede. Estes pacotes alteram o comportamento dos elementos e normalmente não possuem informação assinada. Neste caso, os pacotes de interesse gerados devem carregar assinaturas conforme em VoCCN [Jacobson et al. 2009a]. Desta forma, os roteadores podem verificar que os pacotes de interesse foram assinados pelo controlador.

Na proposta CCN, ataques de negação de serviço (DOS) para conteúdo específico são naturalmente absorvidos com o controle de fluxo. Ataques distribuídos do mesmo tipo (DDOS) são absorvidos pela agregação de interesses e pelo controle de fluxo [Jacobson et al. 2009b]. Porém, ataques distribuídos para conteúdos distintos em um mesmo prefixo não são tratados originalmente. Nesta situação, a tabela PIT dos roteadores atendendo este prefixo cresce com o número de conteúdos solicitados, sendo que não há sequer verificação a priori da existência do conteúdo. Na nossa proposta, a existência do conteúdo é verificada no pedido de instalação de rotas, evitando na origem ataques usando nomes de conteúdo aleatórios.

4.4. Falhas e Partição da Rede

Falhas de circuitos ou nós podem ocasionar a partição da rede, isolando um ou mais controladores. A falha é detectada através da falta de resposta do controlador acima de um intervalo máximo de tempo. Caso ainda exista um controlador na partição, este pode ser encontrado através da Descoberta de Controlador. O controlador recebe os respectivos registros e obtêm a nova topologia. Os roteadores ligados ao produtor sempre possuem uma entrada FIB para conteúdos já registrados e renovam o registro no novo controlador. Caso a partição não possua controlador, os roteadores elegem um para assumir esta função. O processo de recuperação ocorre conforme a Inicialização e Monitoração de Topologia. No antigo controlador, os antigos registros de roteador e conteúdo expiram por tempo ou por sinalização de roteadores que detectem falha na busca de conteúdo não mais alcançável.

4.5. Distribuição de Carga

Em cenários de recuperação de falha ou inserção de novo controlador surge a necessidade de redistribuir os registros entre os controladores existentes e novos. Pela Descoberta de Controladores, os roteadores imediatamente conectados descobrem o novo

controlador. Esta descoberta é informada ao controlador existente no procedimento de Registro de Roteador.

Então o controlador existente pode solicitar diretamente ao novo controlador informações sobre capacidade total e livre de processamento, memória e disco, além do número de roteadores controlados e número de prefixos registrados. Baseado nessas informações, o controlador existente pode sinalizar a parte dos roteadores que alterne o registro para o novo controlador. Ao receber estes registros o novo controlador é informado sobre o controlador existente. A partir deste momento a comunicação entre os controladores é bidirecional estendendo o procedimento de distribuição de carga. Omitimos aqui o detalhamento de mensagens de sinalização deste procedimento.

Outro fator é a divisão dos registros de conteúdo entre os nós da DHT. A DHT é formada por elementos específicos e usa procedimentos próprios para distribuição de carga.

5. Conclusão

Este artigo propôs um esquema de roteamento para redes orientadas a conteúdo CCN superior a proposta OSPFN em termos de consumo de memória FIB e número de mensagens de controle. O esquema reusa a memória da tabela FIB dos roteadores instalando novas rotas em substituição das antigas a medida da necessidade. A substituição de rotas na FIB permite que a sua capacidade seja inferior ao exigido pelo OSPFN, o qual exige capacidade na FIB para o número total de conteúdos da rede com prefixos de nomes distintos. No esquema deste artigo, a demanda por capacidade de memória da FIB cresce de forma proporcional ao número de conteúdos com prefixos distintos em transito pelo roteador em simultâneo, isto é, de forma escalável com a demanda de tráfego.

O esquema proposto neste artigo separa as funções de roteamento em planos de controle e de dados. O plano de controle é composto por controladores estruturados em hierarquia. O total de mensagens da proposta é proporcional ao número de roteadores, níveis na hierarquia e prefixos distintos de conteúdo. Em redes com número de conteúdos de prefixos distintos muito maior do que de número de roteadores, o número de mensagens relativos ao registro e localização de conteúdo é dominante e proporcional ao diâmetro da rede. Este número é muito menor do que o exigido pelo OSPFN, proporcional ao número de roteadores da rede.

Como trabalhos futuros, pretende-se avaliar o desempenho da proposta através do simulador ndnSIM [Afanasyev et al. 2012], mensurando os efeitos de parâmetros como: tempo de armazenamento de rotas, padrões de mobilidade, número de nós por zona, tolerância a falhas, correlação de conteúdos solicitados, banda média por prefixo e os efeitos do número de níveis de controladores. Pretende-se também testar a proposta usando a distribuição CCNx [CCNx 2011] no Future Internet Testbed with Security (FITS) [FITS 2012].

Referências

Afanasyev, A., Moiseenko, I. e Zhang, L. (2012). ndnSIM: NDN simulator for NS-3. Technical report, University of California, Los Angeles.

- Baid, A., Vu, T. e Raychaudhuri, D. (2012). Comparing Alternative Approaches for Networking of Named Objects in the Future Internet. In *Computer Communications Workshops (INFOCOM WKSHPS), 2012 IEEE Conference on*, pages 298–303.
- Carzaniga, A., Papalini, M. e Wolf, A. L. (2011). Content-based Publish/Subscribe Networking and Information-centric Networking. In *Proceedings of the ACM SIGCOMM workshop on Information-centric networking, ICN '11*, pages 56–61. ACM.
- CCNx (2011). CCNx Project. Disponível: <http://www.ccnx.org/>.
- D'Ambrosio, M., Dannewitz, C., Karl, H. e Vercellone, V. (2011). MDHT: a Hierarchical Name Resolution Service for Information-centric Networks. In *Proceedings of the ACM SIGCOMM workshop on Information-centric networking, ICN '11*, pages 7–12. ACM.
- de Brito, G., Velloso, P. e Moraes, I. (2012). Redes Orientadas a Conteúdo: Um Novo Paradigma para a Internet. *Minicursos do Simpósio Brasileiro de Redes de Computadores-SBRC 2012*, pages 211–264.
- Fernandes, N., Moreira, M., Moraes, I., Ferraz, L., Couto, R., Carvalho, H., Campista, M., Costa, L. e Duarte, O. (2011). Virtual Networks: Isolation, Performance, and Trends. *Annals of Telecommunications*, 66:339–355.
- FITS (2012). Future Internet Testbed with Security. Disponível: <http://www.gta.ufrj.br/fits/>.
- Jacobson, V., Smetters, D. K., Briggs, N. H., Plass, M. F., Stewart, P., Thornton, J. D. e Braynard, R. L. (2009a). VoCCN: Voice-over Content-Centric Networks. *ReArch '09*, pages 1–6. ACM.
- Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H. e Braynard, R. L. (2009b). Networking Named Content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies, CoNEXT '09*, pages 1–12. ACM.
- Mattos, D., Fernandes, N., da Costa, V., Cardoso, L., Campista, M., Costa, L. e Duarte, O. (2011). OMNI: OpenFlow MaNagement Infrastructure. In *Network of the Future (NOF), 2011 International Conference on the*, pages 52–56.
- McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., S. e Turner, J. (2008). OpenFlow: Enabling Innovation in Campus Networks. *ACM SIGCOMM Computer Communication Review*, 38(2):69–74.
- Perino, D. e Varvello, M. (2011). A reality check for content centric networking. In *Proceedings of the ACM SIGCOMM workshop on Information-centric networking, ICN '11*, pages 44–49, New York, NY, USA. ACM.
- Wang, L., Hoque, A., Yi, C., Alyyan, A. e Zhang, B. (2012). OSPFN: An OSPF Based Routing Protocol for Named Data Networking. Technical report, University of Memphis and University of Arizona.
- Yia, C., Afanasyevb, A., Moiseenkob, I., Wangc, L., Zhanga, B. e Zhangb, L. (2012). A Case for Stateful Forwarding Plane. Technical report, University of Arizona, University of California, Los Angeles and University of Memphis.
- Zhang, L. et al. (2010). Named Data Networking (NDN) Project.