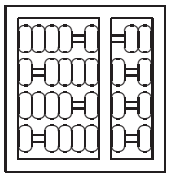


INSTITUTO DE COMPUTAÇÃO
UNIVERSIDADE ESTADUAL DE CAMPINAS

Projeto de uma rede de anonimização de tráfego

Diego F. Aranha *Julio López*

Technical Report - IC-07-25 - Relatório Técnico

August - 2007 - Agosto

Projeto de uma rede de anonimização de tráfego

Diego F. Aranha* Julio López*

Resumo

Neste trabalho, propõe-se uma rede de anonimização de tráfego a partir da criação de uma política de roteamento anonimizada e eficiente com boa qualidade de anonimato para envio, resposta e par comunicante. A organização, arquitetura e topologia utilizadas na rede são extensamente analisadas e suas características de eficiência e qualidade de anonimato são verificadas empiricamente através de simulações. Aprimoramentos adicionais são ainda propostos para aperfeiçoamento da topologia utilizada.

1 Introdução

Os serviços de segurança da informação mais comumente agregados a protocolos são o sigilo, a integridade e a autenticação. Entretanto, uma propriedade desejável em diversos cenários é o obscurecimento, ou anonimato, das identidades das partes comunicantes, tanto entre si como em relação a terceiros. Alcançar este objetivo normalmente requer estratégias peculiares, às vezes exigindo a combinação entre heurísticas e técnicas formais.

Este documento é organizado como se segue. A seção 2 apresenta as definições e métricas para anonimato computacional. A seção 3 compara características de organizações não-estruturadas e estruturadas com a finalidade de comunicação anônima. A seção 4 descreve e propõe técnicas de roteamento para comunicação anônima em redes de organização estruturada. A seção 5 apresenta critérios de seleção de uma topologia estruturada para comunicação anônima e utiliza simulações para validar uma topologia adequada. Por fim, aprimoramentos adicionais que agregam novas propriedades à topologia são discutidos na seção 6 e as conclusões pertinentes são apresentadas na seção 7.

2 Definições

A palavra *anonimato* é derivada do grego $\alpha\nu\omega\nu\upsilon\mu\iota\alpha$, e significa a qualidade daquilo que não tem nome e mais originalmente, daquilo que não tem lei[1]. Coloquialmente, o termo se refere a uma pessoa cuja identidade ou qualquer informação relacionada não é conhecida. Quando se refere a uma entidade arbitrária (humano, objeto, computador), dentro de um

*Instituto de Computação, Universidade Estadual de Campinas, 13084-971, Campinas - SP. Pesquisa financiada pelo CNPq, processo número 1318202005-2.

[1]Extraído de `http://dictionary.reference.com/`.

conjunto bem-definido, o anonimato é a propriedade de não ser identificável dentro deste conjunto [1].

O anonimato não é absoluto, ou seja, a *qualidade de anonimato* que cada entidade possui pode variar. Freqüentemente, é diretamente proporcional ao tamanho do conjunto de entidades associado, chamado comumente de *conjunto de anonimato* [1]. O objetivo da entidade que deseja manter-se anônima é maximizar o tamanho deste conjunto, para agir dentro de uma multidão cada vez maior de entidades similares. Esta definição qualitativa implica ainda que, dado um evento particular, pode-se construir um conjunto de possíveis origens, mas a exatidão na determinação de uma única origem deve ser *difícil*. Claramente, a dificuldade cresce com o aumento da qualidade do anonimato, e vice-versa. Pode existir ainda a figura do *adversário*, que tem como objetivo exclusivo impedir que as entidades tornem-se anônimas.

Esta definição tradicional falha em capturar um aspecto fundamental: também não é desejável que seja fácil apontar a origem única de um evento com *grande probabilidade*. De nada adianta contar com um conjunto de anonimato com 100 entidades se uma delas pode ser apontada como origem de um evento com 90% de probabilidade. Esta observação agrega um novo requisito ao conceito de anonimato: a *distribuição* dos eventos dentro do conjunto de anonimato deve ser o mais uniforme possível. A qualidade do anonimato passa a depender não só do conjunto de entidades, mas da distribuição dos eventos ocorridos entre os componentes do conjunto.

Esta definição mais acurada pode ser instanciada a partir do conceito de *quantidade de informação* na Teoria da Informação de Shannon [2, 3], e baseia-se nos comportamentos contrastantes do adversário e sua vítima: o primeiro deseja obter informação que identifique unicamente o segundo, enquanto o segundo procura simultaneamente aumentar o trabalho do primeiro em obtê-la. Com esta nova definição, a qualidade do anonimato é diretamente proporcional à quantidade de informação que um adversário necessita angariar para indicar unicamente uma ligação entre origem e evento [4].

Recentemente, o anonimato também foi modelado como um problema criptográfico complexo [5], incluindo ataques análogos aos normalmente confrontados por sistemas criptográficos, realizados por um adversário com poder computacional limitado polinomialmente.

2.1 Classificação de anonimato

A definição de anonimato pode ser contextualizada em um ambiente de comunicação: as entidades são usuários que trocam mensagens, os eventos são o envio e recebimento destas mensagens e a comunicação ocorre sob a observação de um adversário, que objetiva relacionar eventos de envio e recebimento aos seus *emissores* e *receptores*, respectivamente.

Os papéis dos usuários são diferenciados em *emissor* e *receptor*, quando a mensagem é o referencial. Se considerarmos um determinado *serviço* como referência, os usuários se especializam em *consumidor* e *provedor* do serviço. Entende-se por serviço uma entidade controlada por um usuário, que disponibiliza alguma funcionalidade para os demais usuários por meio de troca de mensagens. O consumidor é tipicamente o emissor da primeira mensagem que estabelece comunicação para disponibilização do serviço. Uma entidade pode atuar como emissor e receptor de mensagens distintas, bem como consumidor e provedor

de serviços distintos simultaneamente. Dada esta taxonomia, costuma-se classificar o anonimato em três tipos [1]:

- *Anonimato de envio*: é difícil determinar o emissor de uma mensagem particular e, dado um usuário, é difícil atribuir uma mensagem particular como enviada por ele;
- *Anonimato de resposta*: é difícil determinar o receptor de uma mensagem particular e, dado um usuário, é difícil atribuir uma mensagem particular como recebida por ele;
- *Anonimato de par comunicante*: é difícil determinar um par de usuários comunicantes, ou seja, relacionar o emissor ao receptor de uma mensagem. Em comparação às anteriores, representa uma noção mais fraca de anonimato, já que é possível relacionar o emissor à mensagem enviada e o receptor à mensagem recebida, atuando-se apenas na associação entre estas duas mensagens.

Idealmente, o anonimato deve abranger os três aspectos acima definidos. A ausência de anonimato de envio provoca intimidação e conseqüente escassez de usuários (diminuição do *conjunto de anonimato*). A ausência de anonimato de resposta expõe os usuários que disponibilizam serviços anônimos. A ausência de desligamento entre emissor e receptor permite o rastreamento das mensagens trocadas no sistema, expondo potencialmente tanto os emissores quanto os receptores.

2.2 Métricas de anonimato

De posse de uma certa quantidade de informação a respeito de um evento de envio ou recebimento, obtida a partir de observação ou manipulação direta do ambiente, o adversário pode inferir a probabilidade de cada entidade ter participado do evento como emissor ou receptor.

Seja $\mathcal{A}$ um conjunto finito de usuários e seja $r \in \mathcal{R}$ o papel de um usuário $\mathcal{R} = \{\mathsf{emissor}, \mathsf{receptor}\}$, em relação a uma certa mensagem $m \in \mathcal{M}$. A *probabilidade de envolvimento* é a distribuição de probabilidade p dos usuários $a_i \in \mathcal{A}$ terem o papel r em relação a m, tomada pelo adversário.

O anonimato é descrito pela distribuição de probabilidade $p : \mathcal{A} \times \mathcal{R} \rightarrow [0, 1]$. Dependendo das circunstâncias, a função p pode atribuir valores extremos no intervalo $[0, 1]$. Se por exemplo, a_j for observado como o receptor direto da mensagem m, $p(a_j, \mathsf{receptor}) = 1$ e $\forall a_i \in \mathcal{A}, i \neq j$, $p(a_i, \mathsf{receptor}) = 0$. Claramente, tem-se que:

$$\sum_{a_i \in \mathcal{A}} p(a_i, r) = 1. \tag{1}$$

2.2.1 Entropia

A qualidade do anonimato pode ser quantificada por uma métrica de entropia [6]. A *entropia* H da distribuição de probabilidade p das probabilidades de envolvimento p_{a_i} associadas a cada usuário é dada por:

$$H = -\sum_{a_i \in \mathcal{A}} p_{a_i} \cdot \log_2 (p_{a_i}). \tag{2}$$

Esta métrica mede o grau de incerteza do adversário em identificar um usuário. Representa ainda a quantidade de informação que precisa ser obtida para que o usuário a_i seja identificado corretamente com papel r para a mensagem m. É fácil mostrar que se um usuário a_j possui probabilidade de envolvimento 1, a entropia é 0, ou seja, o adversário já detém informação suficiente para identificar a_j. São propriedades adicionais desta métrica:

- Para qualquer conjunto não-vazio de usuários $\mathcal{A}$, a entropia é tal que $0 \leq H \leq \log_2 |\mathcal{A}|$, e o valor $\log_2 |\mathcal{A}|$ é obtido quando p é uma distribuição uniforme;
- Se $H = 0$, o canal de comunicação não fornece anonimato;
- Se $H = \log_2 |\mathcal{A}|$, o canal de comunicação fornece *anonimato perfeito*;
- Se $H = h$, o canal de comunicação fornece anonimato equivalente a um canal de comuni-cação perfeito com 2^h usuários. A grandeza 2^H é chamada de *tamanho efetivo do conjunto de anonimato.*

Entropia mínima

A qualidade do anonimato também pode ser quantificada por uma métrica de *entropia mínima*, que representa o grau de exposição do usuário mais exposto. Idealmente, esta grandeza deve ser maximizada. Caso contrário, o adversário pode identificar um usuário e seu papel com grande probabilidade.

A entropia mínima H_{min} da distribuição de probabilidade p é dada por:

$$H_{min} = -\log_2 (\max_{a_i \in \mathcal{A}} p_{a_i}). \tag{3}$$

Entropia condicional

As grandezas de entropia e entropia mínima são parametrizadas a partir das observações de um adversário. Entretanto, existem situações nas quais nem sempre o adversário pode observar a transmissão de uma mensagem. A *entropia condicional* é a entropia média, calculada a partir da probabilidade p' de um adversário não observar uma mensagem e da entropia H' da distribuição de probabilidade das mensagens não-observadas pelo adversário.

A entropia condicional H_c da distribuição de probabilidade p, dadas as grandezas p' e H' é dada por:

$$H_c = (1 - p')H + p'H'. \tag{4}$$

A entropia condicional também pode ser formulada diretamente a partir da Teoria da Infor-mação. Sejam A e Y duas variáveis aleatórias que modelam os usuários e as observações do adversário, respectivamente. Percebe-se que as métricas de entropia apresentadas nas seções anteriores dizem respeito à distribuição da variável A dada uma observação

particular y, ou seja, calculam $H(A|Y = y)$. A entropia condicional $H(A|Y)$ pode ser calculada como a média ponderada das entropias individuais [4]:

$$H(A|Y) = \sum_{y} Pr[Y = y]H(A|Y = y) = \mathcal{E}_y H(A|Y = y). \quad (5)$$

A entropia condicional é uma métrica de esperança, mais apropriada para a avaliação do anonimato em um ambiente persistente, em que um grande número de mensagens são trocadas durante um longo período de tempo. Entretanto, esta métrica não captura totalmente o potencial de exposição de um usuário. Mesmo que uma mensagem m seja observada com uma probabilidade $p' < 1$, é importante estimar o risco de exposição de um usuário se esta mensagem for observada.

A *entropia condicional mínima* calcula o grau potencial de exposição que um usuário pode ter que lidar. A entropia condicional mínima H_w da distribuição de probabilidade p é dada por:

$$H_w = \min_{y} H(A|Y = y). \quad (6)$$

2.2.2 Grau de anonimato

Cada um dos tipos de anonimato pode ainda ser avaliado de acordo com o *grau de anonimato* conferido, de acordo com as probabilidades de envolvimento tomadas pelo adversário [7]:

- *Privacidade Absoluta:* um usuário possui privacidade absoluta contra um adversário se o adversário não pode distinguir as situações em que um usuário participa de uma comunicação daquelas em que o usuário não participa;
- *Fora de suspeita:* um usuário está fora de suspeita se, do ponto de vista do adversário, mesmo existindo evidência da participação do usuário em um comunicação, a probabilidade do usuário ter participado não é significativamente maior do que a probabilidade de qualquer outro usuário ter participado;
- *Inocência provável:* um usuário é provavelmente inocente se, do ponto de vista do adversário, a probabilidade do usuário ter participado de uma comunicação não é maior do que a probabilidade do usuário não ter participado. Esta noção é mais fraca do que a anterior, no sentido de que o adversário tem informação suficiente para destacar um usuário entre os demais como provável participante na comunicação, mas a probabilidade do usuário ter participado da comunicação ainda é menor do que a probabilidade do usuário não ter participado;
- *Inocência possível:* um usuário é possivelmente inocente se, do ponto de vista do adversário, há uma probabilidade significativa do participante real em uma comunicação ser outro usuário;
- *Exposto:* um usuário está exposto se o adversário pode identificar o usuário como participante de uma comunicação com absoluta certeza;

- *Comprovadamente exposto:* o adversário não só pode identificar o usuário como participante de uma comunicação como pode provar este fato para terceiros.

Pode-se observar que, para alcançar grau de privacidade absoluta, o adversário sequer pode detectar que o usuário participou de alguma comunicação: o envio de uma mensagem, por exemplo, não pode resultar em qualquer efeito perceptível para o adversário. Ou seja, é necessário combinar uma primitiva de comunicação anônima perfeita a um mecanismo de anoni-mização perfeito da própria primitiva, impedindo efetivamente que o adversário detecte quando o usuário comunica-se com qualquer outro usuário. É possível implementar grau de privacidade absoluta combinando a primitiva de comunicação anônima com *esteganografia*[2].

Em grande parte das aplicações reais, o grau de inocência provável já é considerado suficiente. A diferença entre a probabilidade do usuário não ter participado e a probabilidade do usuário ter participado de uma comunicação impede que o adversário defenda posições conclusivas.

3 Arquitetura

Mecanismos de anonimização devem ter arquitetura descentralizada. A descentralização da estrutura do mecanismo elimina pontos únicos de falha e dificulta a monitoração por adversários poderosos. A descentralização do protocolo distribui a implementação das técnicas de anonimização entre os participantes e minimiza a influência de participantes maliciosos.

Uma arquitetura do tipo *peer-to-peer* satisfaz ambos os requisitos. Sistemas *peer-to-peer* são sistemas distribuídos compostos por nós interconectados com o propósito de compartilhar recursos – como conteúdo, processamento, armazenamento e banda – e capazes de se adaptar a falhas e acomodar populações transientes de nós, enquanto mantém conectividade e desempenho aceitáveis sem requerer a intermediação ou suporte de um servidor central ou autoridade global [8]. A utilização de sistemas *peer-to-peer* na solução de problemas computacionais distribuídos é prática tradicional. Aplicações *peer-to-peer* famosas são os projetos *SETI@Home*[3] e *Folding@Home* [4].

3.1 Organizações

Sistemas *peer-to-peer* podem diferir quanto à organização. O tipo de organização normalmente define uma topologia e determina a alocação de identificadores para os nós conectados e para a localização dos recursos. Estes identificadores são necessários para um nó conectado ao sistema poder ser encontrado e para se controlar a divisão dos recursos compartilhados entre os nós. A topologia pode governar o número de conexões que cada nó deve manter, bem como os pares de nós que podem se conectar. Quanto à organização, os sistemas dividem-se em estruturados e não-estruturados [8].

[2] Esteganografia é o estudo e uso de técnicas para ocultar a existência de uma mensagem dentro de outra.
[3] `http://setiathome.berkeley.edu`
[4] `http://folding.stanford.edu/`

3.1.1 Sistemas não-estruturados

Em um sistema não-estruturado, os identificadores utilizados pelos nós são alocados arbitrariamente e a localização dos recursos independe da topologia. A busca de recursos pode ser realizada por comunicação em *multicast* e caminhos aleatórios. Sistemas não-estruturados possuem topologia irregular, que apresenta diferenças de densidade e outros desequilíbrios de organização, sendo mais apropriados para acomodar populações de nós transientes [8]. Exemplos de sistemas não-estruturados são Gnutella[5] e KaZaA[6]. Exemplos de redes anônimas não-estruturadas são as redes *Tor* [9] e *Freenet* [10].

3.1.2 Sistemas estruturados

Em um sistema estruturado, os identificadores e as conexões obedecem a um algoritmo e a localização dos recursos compartilhados depende fortemente da topologia. Geralmente, as estruturas compartilham um esquema básico: todas utilizam um espaço de endereçamento grande, como anéis de inteiros $\mathbb{Z}_{2^{128}}$ e $\mathbb{Z}_{2^{160}}$, de onde são alocados os identificadores. As conexões dependem de uma relação matemática entre os identificadores, para aproximar a topologia de um grafo regular, como um hipercubo. A estrutura garante que cada nó mantenha um número de conexões constante ou logarítmico no tamanho total da rede e que, similarmente, todo caminho entre dois pontos quaisquer do espaço de endereçamento tenha comprimento logarítmico no tamanho da rede. A busca de recursos é realizada por algoritmos e políticas de roteamento que utilizam esta regularidade da topologia para obter eficiência. Existem vários tipos de estruturas com propriedades distintas, entre elas Chord [11], Pastry [12] e Tapestry [13]. Para anonimização, temos como exemplo a rede estruturada *AP3* [14].

Os sistemas estruturados foram concebidos para minimizar os problemas típicos decorrentes da ausência de estrutura, especialmente relacionados à disponibilidade e escalabilidade. Apesar de exigirem procedimentos adicionais para a entrada e saída de nós e para manutenção da estrutura, costumam apresentar vantagens que compensam esta sobrecarga.

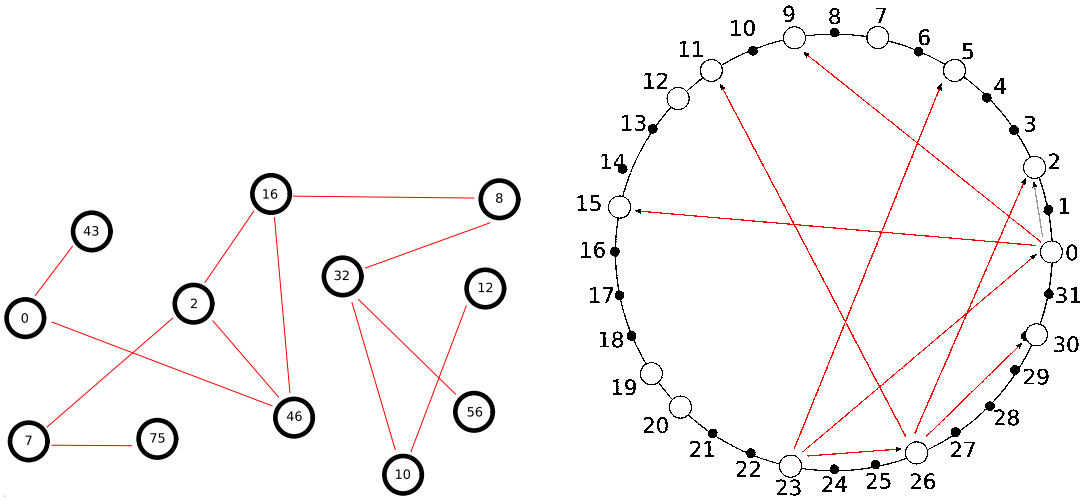
A Figura 1 apresenta dois esboços de sistema não-estruturado e estruturado. As setas em vermelho representam conexões entre pares de nós.

3.2 Escolha da organização

Como apontado anteriormente, a qualidade do anonimato não só depende do número de participantes, mas também da distribuição dos eventos entre os participantes. A uniformidade na distribuição dos eventos depende intimamente da organização do sistema e da política de roteamento utilizada.

Sistemas não-estruturados são construídos arbitrariamente e, por isso, suportam não-deter-minismo intrínseco que a princípio pode parecer útil para comunicação anônima. Entretanto, este mesmo não-determinismo tende a provocar desequilíbrios que prejudicam a distribuição da qualidade do anonimato entre os participantes, como comprovado por [15] a

[5] `http://www.the-gdf.org/`
[6] `http://www.kazaa.com/`



(a) Exemplo de sistema não-estruturado. (b) Exemplo de sistema estruturado.

Figura 1: Comparação entre sistema não-estruturado e sistema estruturado.

partir de simulação exaustiva da *Freenet*. Outras desvantagens de sistemas não-estruturados incluem a falta de confiabilidade no roteamento (pode não ser possível encontrar um recurso mesmo ele estando presente) e a dificuldade em se estimar ou derivar limites para aspectos de desempenho e balanceamento de carga. A grande vantagem de sistemas não-estruturados é a baixa sobrecarga de manutenção da rede.

Sistemas estruturados, por sua vez, fornecem roteamento mais eficiente e confiável. Como as conexões são governadas por propriedades matemáticas, cada nó conectado à rede possui um conhecimento limitado dos demais nós, e este limite pode ser controlado com rigor. Esta propriedade de visão limitada controla a quantidade de informação que um adversário pode obter da rede. A topologia regular também distribui a responsabilidade uniformemente entre os nós, o que inibe a existência de pontos mais vulneráveis para ataque. As propriedades de regularidade e simetria têm o potencial de fornecer qualidade de anonimato mais uniforme que abordagens não-estruturadas [15]. As características determinísticas de sistemas estruturados ainda permitem simulações mais fiéis ao comportamento real das redes, o que facilita sua análise. Limites rigorosos podem ser particularmente obtidos para métricas de desempenho e balanceamento de carga e até para a eficiência de ataques efetuados por um adversário.

Sistemas estruturados fornecem maior potencial para comunicação anônima e são utilizados no projeto da rede de anonimização desenvolvido neste trabalho. As discussões subseqüentes irão se restringir, portanto, a sistemas estruturados.

4 Comunicação anônima em sistemas estruturados

A funcionalidade básica de sistemas estruturados é fornecer uma primitiva de *tabela de hash distribuída* (*Distributed Hash Table - DHT*) [11]. Em uma tabela de *hash* distribuída, as operações básicas são de *armazenamento* e *recuperação*, implementadas a partir de troca de mensagens entre os nós. Os recursos compartilhados são mapeados para o espaço de endereçamento utilizado pelos nós a partir da aplicação de uma função de *hash* ao conteúdo ou descrição do recurso. A localização de cada recurso é baseada na similaridade entre os identificadores do recurso e dos nós conectados, calculada por uma função de distância. Para se garantir o balanceamento da carga de armazenamento, o controle do espaço de endereçamento é particionado eqüitativamente entre todos os nós conectados. Um esquema de particionamento comumente utilizado é conferir para cada nó o controle da porção de endereços maiores que o identificador do seu predecessor e menores ou iguais ao seu próprio identificador.

O primeiro passo para se suportar comunicação anônima em sistemas estruturados é anonimizar o roteamento que transporta as operações de armazenamento e recuperação de recursos. Esta modificação agrega anonimato de envio à estrutura. A anonimização destas operações básicas transforma a tabela de *hash* distribuída em sua versão anonimizada. Isto permite a anonimização direta de diversas aplicações que utilizam tabelas de *hash* distribuídas, especialmente para publicação de documentos [16].

Como o mesmo roteamento que transporta uma requisição de operação através da rede pode também ser utilizado para o envio de uma mensagem qualquer, a anonimização do roteamento possibilita a utilização de um sistema estruturado para comunicação anônima genérica. Na seção seguinte, um sistema estruturado é adaptado para suportar anonimato de envio. Modificações adicionais são necessárias para suporte a anonimato de resposta e são discutidas posteriormente.

4.1 Anonimato de envio

O roteamento em sistemas estruturados é *recursivo*. O nó que efetua uma operação de armazenamento ou recuperação utiliza a chave do recurso compartilhado para avaliar cada um dos seus vizinhos quanto à distância e selecionar o próximo ponto na rota. Os nós intermediários repetem o procedimento recursivamente até que o nó detentor da porção de endereçamento compatível com o recurso seja encontrado. A característica de regularidade da estrutura do sistema permite que um destino único sempre seja encontrado e que o roteamento seja *convergente*. Similarmente, um nó que envia uma mensagem qualquer para um nó de destino utiliza o identificador do destino como chave no roteamento. As respostas são encaminhadas percorrendo a mesma rota utilizada para envio, em sentido contrário.

A Figura 2 apresenta em setas pretas a rota percorrida por uma mensagem enviada pelo nó com identificador 23 para o nó de destino 12. Na figura, é possível observar o espaço de endereçamento $\mathbb{Z}_{2^5}$, com os nós conectados representados na cor branca. É possível também observar em vermelho as conexões mantidas pelo nó 23, o círculo que delimita a porção do endereçamento sob controle do nó 23 e a atuação de uma função de distância nas decisões de roteamento.

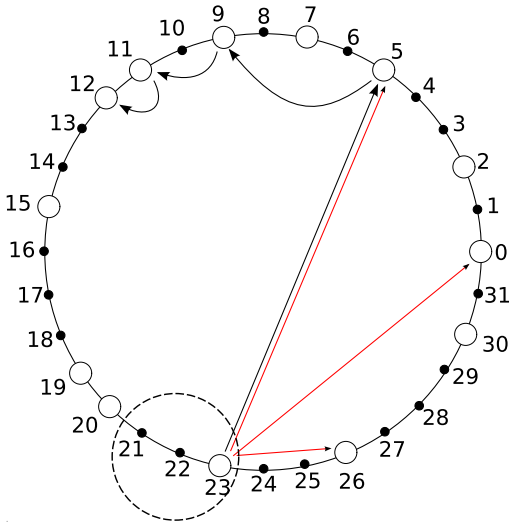


Figura 2: Exemplo de roteamento determinístico em um sistema estruturado.

É fácil perceber que o roteamento determinístico revela informações úteis para um adversário. Um nó intermediário pode calcular, por exemplo, a distância entre o seu identificador e o destino para inferir o identificador do nó emissor. O primeiro nó intermediário da rota também pode identificar a origem da mensagem com grande probabilidade. Os identificadores dos nós não podem ser mantidos em segredo, já que precisam ser conhecidos pelos seus vizinhos para roteamento e manutenção da estrutura. Logo, descobrir o identificador do emissor de uma mensagem é praticamente equivalente a quebrar o seu anonimato de envio.

Uma solução para o problema do roteamento determinístico [14] utiliza uma idéia da rede *Crowds* [7]: um caminho aleatório é percorrido antes da entrega da mensagem ao destino real. O nó emissor primeiramente seleciona um nó arbitrário na rede e encaminha a mensagem. O nó selecionado realiza um sorteio p_r condicionado por uma *probabilidade de encaminhamento* $0 \leq p_f < 1$ e decide se a mensagem deve ser encaminhada novamente para outro nó arbitrário ou deve ser entregue ao destino final. Cada nó intermediário repete o procedimento até que o sorteio falhe e a mensagem seja devidamente entregue. A Figura 3 apresenta o esquema: as setas tracejadas correspondem a sorteios que decidiram pelo encaminhamento para outro nó e a seta restante corresponde ao sorteio que decidiu pela entrega da mensagem.

Aplicando a idéia em um sistema estruturado, o roteamento divide-se em duas partes: a primeira parte percorre um caminho aleatório entre os nós da estrutura e a segunda parte corresponde ao roteamento recursivo determinístico. O nó emissor da mensagem seleciona um identificador aleatório no espaço de endereçamento e executa o algoritmo de roteamento determinístico para entregar a mensagem. Cada nó intermediário repete o procedimento até que um deles decida por entregar a mensagem para o destino e execute a segunda fase do roteamento. Desta forma, as mensagens roteadas atingem um ponto aleatório na rede

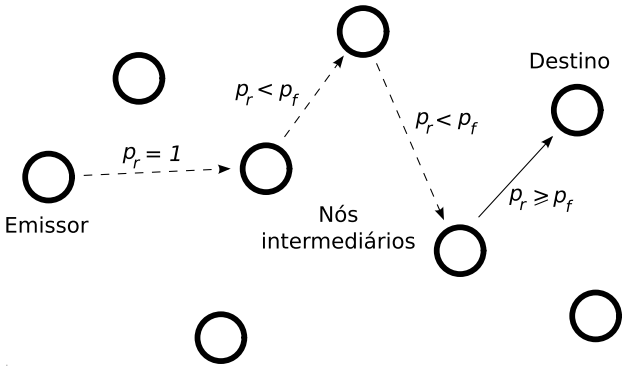


Figura 3: Exemplo de anonimização de envio na rede *Crowds*.

antes de serem encaminhadas para o destino final.

A Figura 4 apresenta o roteamento em duas fases utilizado pela rede *AP3* [14]. Na figura, o nó 23 envia uma mensagem para o nó 12, e sorteios sucessivos da probabilidade p_r são realizados, alternados por execuções do algoritmo de roteamento determinístico. Cada sorteio $p_r < p_f$ provoca uma execução do roteamento determinístico no caminho aleatório e o sorteio $p_r \geq p_f$, realizado pelo nó 20, provoca a entrega da mensagem.

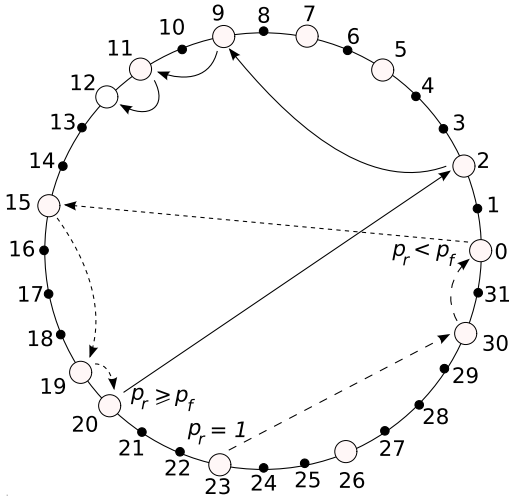


Figura 4: Exemplo de anonimização de envio na rede *AP3*.

O caminho aleatório composto por uma seqüência de roteamentos determinísticos apresenta uma desvantagem. Como o comprimento da rota entre dois pontos quaisquer na rede não tem tamanho fixo, apesar de ser limitado logaritmicamente pelo tamanho da rede, a previsão do tamanho do caminho aleatório percorrido é inacurada: as rotas determinísticas utilizadas têm tamanhos variados e podem resultar em caminhos aleatórios muito longos

e de baixo desempenho. Um aperfeiçoamento desta idéia foi proposto por Borisov [15] e utiliza as conexões do sistema estruturado nas decisões do caminho aleatório. Ao invés de encaminhar a mensagem para um identificador aleatório, cada nó encaminha a mensagem para um dos vizinhos que conhece, sorteado aleatoriamente, até que a segunda fase do roteamento seja iniciada. A mesma probabilidade de encaminhamento p_f é utilizada para decidir se a mensagem é encaminhada novamente ou entregue ao destino. Um caminho aleatório desta natureza e suficientemente longo irá atingir um ponto aleatório na rede, independente da origem, e a partir do qual o roteamento pode ser completado. Este novo algoritmo de roteamento é referenciado posteriormente como *roteamento randomizado* e é utilizado como algoritmo de roteamento para o envio de qualquer mensagem na rede.

A Figura 5 ilustra o algoritmo de roteamento randomizado. Novamente o nó 23 envia uma mensagem para o nó 12, mas os sorteios de probabilidade são agora alternados com encaminhamentos diretos da mensagem para um nó vizinho. Cada sorteio $p_r < p_f$ provoca a retransmissão da mensagem para um vizinho selecionado aleatoriamente e o sorteio $p_r \geq p_f$, realizado pelo nó com identificador 5, inicia a entrega da mensagem com roteamento determinístico.

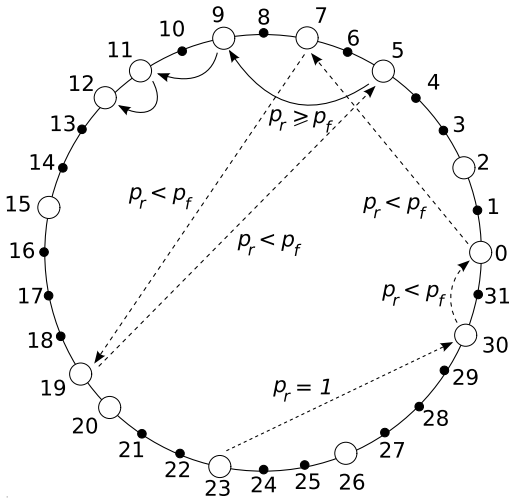


Figura 5: Exemplo de anonimização de envio com roteamento randomizado.

4.2 Anonimato de resposta

Apesar do anonimato de envio proteger a identidade do emissor das mensagens, é insuficiente para suportar os fluxos de requisição e resposta presentes na maioria dos protocolos. Para permitir resposta, cada mensagem enviada deve transportar um endereço de resposta, a partir do qual o emissor pode ser encontrado. O endereço de resposta deve ser independente do identificador do emissor para não comprometer sua identidade.

Uma solução simples para o problema é proposta em [14] e utiliza endereços de resposta aleatórios. Antes de enviar uma mensagem, o emissor cria um *canal de resposta* identificado

por um endereço aleatório no espaço de endereçamento. Para criar o canal, o emissor envia uma mensagem especial utilizando roteamento randomizado até o nó que detém a porção de endereçamento que contém com o endereço do canal. Cada nó intermediário do caminho aleatório que recebe esta mensagem especial grava a direção pela qual a mensagem foi recebida em uma *tabela de resposta* local. A mensagem especial eventualmente atinge o seu destino e o canal é completado quando o nó de destino concorda em atuar como *ponto de entrada*, utilizando o canal no sentido contrário para encaminhar todas as mensagens destinadas ao seu criador. A criação do canal deve estar condicionada a um limite de tempo que, quando ultrapassado, força a expiração do canal antigo e obriga o estabelecimento de um novo canal.

A Figura 6 ilustra a criação de um canal de resposta pelo nó 23 com ponto de entrada 9. Na figura, as setas de maior espessura indicam o canal de resposta, e os nós com identificadores 23 e 12 trocam mensagens. A requisição R transporta a mensagem m para o nó 12 utilizando roteamento randomizado e especifica o endereço do nó 9 como endereço de resposta. A requisição R apenas revela o endereço do ponto de entrada do canal de resposta, protegendo a identidade do emissor. A resposta R' é encaminhada para o nó 9, por meio do qual atinge o emissor percorrendo o canal na ordem inversa de criação. O nó 12 não utiliza canal de resposta para receber mensagens.

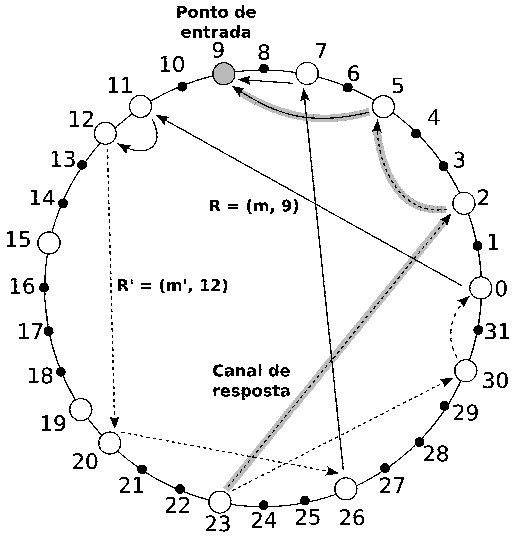


Figura 6: Exemplo de anonimização de resposta na rede *AP3*.

A qualidade do anonimato de resposta é intuitivamente dependente da qualidade do anonimato de envio, já que utiliza as mesmas primitivas de comunicação. A modificação desta técnica para anonimato de resposta permite ainda o estabelecimento de pseudônimos.

4.2.1 Pseudônimos

As técnicas de roteamento randomizado e de canais de resposta são ideais para troca eventual de mensagens. Entretanto, não há qualquer impedimento para um adversário personificar qualquer emissor para forjar mensagens ou modificar o endereço de resposta de mensagens interceptadas para que atravessem um dos nós que controla. É necessário, portanto, a utilização de um mecanismo que agregue reputação e permita aos nós confirmar a autenticidade da parte com a qual se comunicam.

Sendo desconhecida a identidade real dos nós conectados, a reputação é construída em torno de um identificador persistente e cuja posse pode ser provada criptograficamente. Um identificador com estas características qualifica-se como um *pseudônimo*.

Para um nó a_i estabelecer um pseudônimo confiável, deve gerar um par de chaves assimétrico (e_{a_i}, d_{a_i}) e calcular um pseudônimo dependente do seu par de chaves. O pseudônimo α_i é derivado a partir da aplicação de uma função de *hash* criptográfica h à chave pública. Um canal de resposta autenticado utiliza o *hash* do pseudônimo $h(\alpha_i) = h(h(e_{a_i}))$ como ponto de entrada. Qualquer nó que conheça o pseudônimo previamente pode confirmar a autenticidade da chave pública, pois detém um *hash* da mesma, e verificar a prova da chave privada correspondente utilizando assinatura digital [14]. Ataques de *espelhamento* (do inglês, *man-in-the-middle attack*) são completamente evitados [17].

A Figura 7 ilustra o estabelecimento de pseudônimo por parte do nó com identificador 12 e de um canal de resposta autenticado pelo pseudônimo $h(e_{12})$ e com ponto de entrada $h(h(e_{12})) = 19$. O nó 23 envia uma mensagem para o nó 12, utilizando o ponto de entrada do canal autenticado. O nó 23 deriva o ponto de entrada do canal autenticado a partir do conhecimento prévio do pseudônimo. Como na figura anterior, o nó 23 mantém um canal de resposta não-autenticado com ponto de entrada 9.

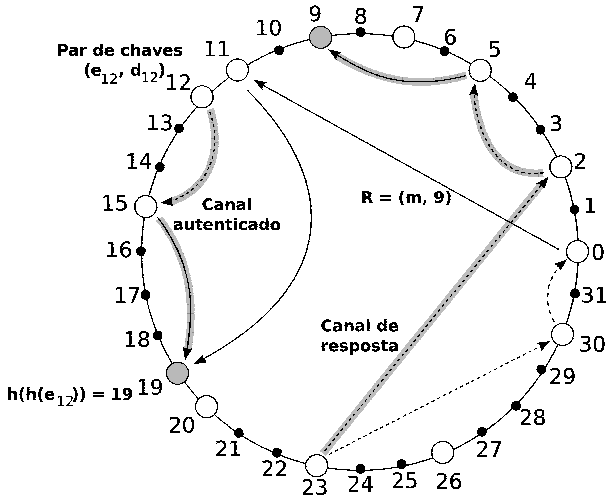
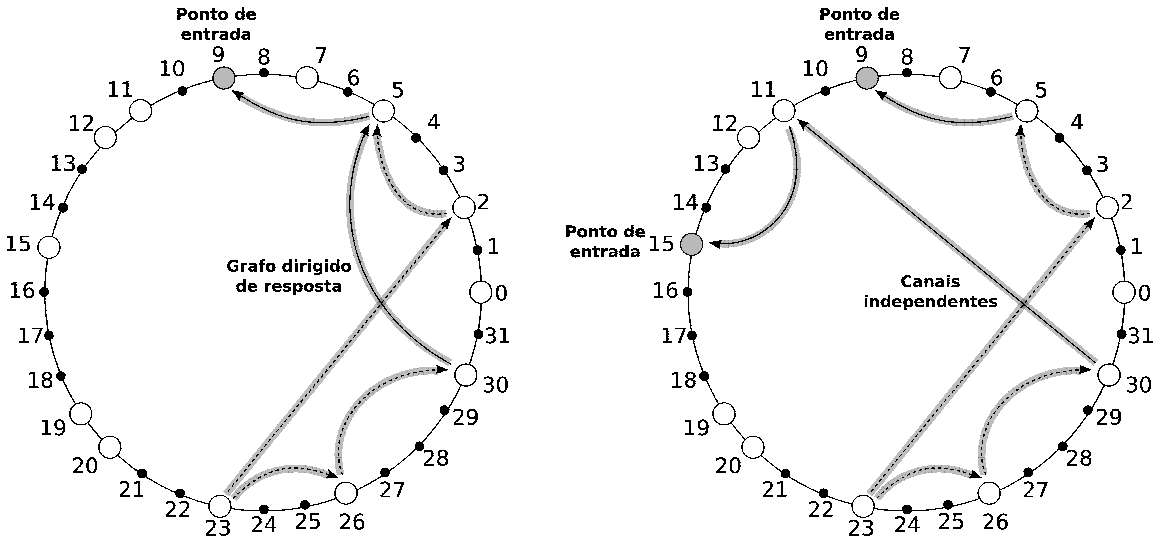


Figura 7: Exemplo de estabelecimento de pseudônimo na rede *AP3*.

4.2.2 Aprimoramento

A proposição original apresenta limitações práticas relacionadas a desempenho e resistência a ataques. A utilização de um único canal de resposta que concentra todas as respostas a variadas requisições pode prejudicar muito a latência de transmissão. Além disso, nós controlados pelo adversário presentes no canal de resposta podem descartar as mensagens, realizado um ataque efetivo de negação de serviço.

As soluções para ambas as limitações partem do estabelecimento de múltiplos canais de resposta com endereços distintos. Uma proposta na literatura sugere a utilização de *grafos dirigidos de resposta* [18]. Para formar o grafo dirigido, o criador seleciona um ponto de entrada e solicita o estabelecimento do canal de resposta para vários nós. Cada um dos nós que recebe a solicitação realiza um sorteio ponderado e replica a solicitação para outro nó em caso de sucesso. Quando um nó falha no sorteio, conecta-se diretamente ao ponto de entrada. O grafo dirigido funciona como um canal único, tendo um ponto único de entrada e um ponto único de saída e diversas bifurcações internas. As desvantagens desta abordagem são a centralização do ponto de entrada e o alto custo de estabelecimento e renovação do grafo. Além disso, a carga e a responsabilidade dos nós próximos às pontas do canal é maior, pois a indisponibilidade repentina dos nós próximos às pontas acarreta conseqüências graves em desempenho e confiabilidade.



(a) Exemplo de grafo dirigido de resposta.

(b) Exemplo de canais de resposta múltiplos e independentes.

Figura 8: Diferentes estratégias para estabelecimento de canais múltiplos de resposta.

Uma alternativa é proposta e utilizada neste trabalho e envolve o estabelecimento independente de múltiplos canais de resposta com pontos de entrada distintos. Canais de resposta não-autenticados podem ser utilizados se os vários endereços de resposta de um emissor acompanharem suas mensagens enviadas. O suporte a pseudônimos é mantido se

os endereços dos canais corresponderem a aplicações sucessivas da função de *hash* h ao pseudônimo: $h(\alpha_i)$, $h(h(\alpha_i))$, $h(h(h(\alpha_i)))$. A vantagem desta nova abordagem é a possibilidade de se estabelecer canais múltiplos paralelamente, distribuindo o custo de renovação no decorrer do tempo. O ponto de entrada centralizado também é eliminado. Qualquer nó que conheça o pseudônimo previamente continua podendo verificar a posse do par de chaves associado ao pseudônimo e pode contatar o criador do canal utilizando vários pontos de entrada simultaneamente. A descentralização adicional ainda distribui a carga e a responsabilidade igualmente entre os canais e os nós que os compõem.

A Figura 8 apresenta duas estratégias de estabelecimento de canais múltiplos de resposta, ilustradas por um grafo de resposta simplificado (Figura 8(a)) e um par de canais de resposta independentes (Figura 8(b)). As vantagens da alternativa proposta, como descentralização do ponto de entrada e distribuição de responsabilidade, são evidenciadas na figura: a indisponibilidade repentina do nó 5 no grafo dirigido de resposta invalida todo o grafo, enquanto a indisponibilidade do nó 5 no canal independente, invalida apenas o canal em que participa.

Para o projeto da rede de anonimização, canais múltiplos e independentes são utilizados para fornecimento de anonimato de resposta.

4.3 Anonimato de par comunicante

A randomização do roteamento, utilizada para fornecer anonimatos de envio e de resposta, espalha as mensagens trocadas por vários nós intermediários, implementando a técnica de indireção. Entretanto, o conteúdo das mensagens permanece às claras e suscetível à análise por parte de um adversário externo:

- Um adversário local externo pode identificar pares comunicantes com algum esforço, correlacionando a informação às claras capturada nas conexões da rede que monitora;
- Um adversário global externo que monitora todo o sistema de comunicação pode identificar trivialmente rotas e pares comunicantes.

A utilização de cifração impede a eficácia destes ataques. Para o projeto da rede de anoni-mização, a cifração é adicionada em dois níveis: inicialmente no nó emissor, utilizando a chave pública do receptor, cujo pseudônimo conhece; e posteriormente nas conexões diretas utilizadas para roteamento. A cifração nas partes comunicantes propriamente ditas impede o descarte sistemático de mensagens por nós intermediários e a cifração nas conexões intermediárias limita a observação de adversários externos. Técnicas já discutidas de igualdade entre mensagens são ainda utilizadas para obscurecer o tráfego.

Adversários internos, entretanto, ainda podem obter informação a respeito de rotas percorridas examinando as mensagens cifradas que atravessam os nós que controla. Esta limitação não oferece perigo significativo, já que cada mensagem enviada na rede utiliza um caminho aleatório diferente.

A utilização de cifração de dois níveis fornece ainda *repudiação*: todos os nós podem negar convictamente o conhecimento do tráfego que roteiam. As técnicas descritas para anonimato de envio e resposta também colaboram para a qualidade de anonimato do par comunicante.

5 Avaliação de topologias

Utilizando técnicas propostas em diversos trabalhos [7, 17, 14, 15] e aprimoramentos como canais múltiplos de resposta e cifração em dois níveis, um sistema estruturado genérico pôde ser adaptado para comunicação anônima. Deve-se, por último, escolher qual das topologias estruturadas propostas na literatura tem maior potencial para anonimato.

5.1 Critérios de seleção

A *capacidade de mistura* de um sistema estruturado é a capacidade do sistema em atingir um ponto independente da origem após o percorrimento de um caminho aleatório em sua topologia. Sistemas têm melhor capacidade de mistura quando são capazes de atingir um ponto aleatório na rede com um caminho aleatório de menor comprimento. Esta grandeza está intimamente relacionada à qualidade de anonimato e, mais especificamente, ao compromisso entre desempenho e anonimato. Sistemas estruturados com melhor capacidade de mistura devem fornecer melhor desempenho e comunicação anônima de melhor qualidade [15].

A capacidade de mistura é medida a partir da *distância de variação* entre a distribuição uniforme e a distribuição dos nós finais em caminhos aleatórios. Recentemente, várias topologias estruturadas foram avaliadas de acordo com a capacidade de mistura [15]. O objetivo deste estudo foi apontar, a partir de simulação, as topologias com melhor capacidade de mistura para utilização em comunicação anônima.

Para selecionar uma topologia estruturada útil para comunicação anônima, neste trabalho, optou-se pela realização de novos experimentos análogos aos descritos em [15] e com o mesmo objetivo, mas com critérios de avaliação distintos. A seleção de uma topologia adequada foi condicionada à observação do comportamento de cada uma das topologias avaliadas quando utilizadas para comunicação anônima. O critério de seleção não foi a capacidade de mistura, mas a métrica de entropia. O compromisso entre a métrica de entropia e o desempenho, ou entre a qualidade do anonimato e desempenho, também foi considerado. A capacidade de resistência das estruturas a ataques de negação de serviço também foi rapidamente examinada. Esta abordagem aponta com maior clareza as vantagens das topologias selecionadas e deve confirmar a relação íntima entre capacidade de mistura e entropia.

A métrica de entropia é calculada a partir da simulação de redes comunicando-se anonimamente. As redes são construídas dinamicamente e de forma não-determinística. A entropia poderia ser calculada formalmente a partir das fórmulas apresentadas anteriormente, mas a complexidade do sistema e de sua população impossibilita esta abordagem. A utilização de simulações é motivada diretamente por esta complexidade.

5.2 Candidatos

Foram consideradas algumas das topologias estruturadas mais populares na área de pesquisa em sistemas estruturados: *Chord* [11], *Chord* randomizado [19], hipercubo [12, 13], hipercubo randomizado [20], *SkipGraph* [21], *SkipNet* [22] e *Koorde* [23]. As diferenças em relação ao experimento original são:

- Inclusão da versão randomizada da topologia *Chord*;
- Inclusão das topologias de hipercubo e hipercubo randomizado, para suplantar as topologias *Pastry* [12], *Tapestry* [13] e variantes;
- Inclusão das topologias *SkipGraph* e *SkipNet*;
- Remoção das topologias *CAN* [24] e *Viceroy* [25], por apresentarem resultados muito desfavoráveis no experimento original [15];
- Simulação da segunda fase do roteamento randomizado, resultando em uma simulação mais realista do ambiente;
- Avaliação de diversas variantes da topologia *Koorde*; e
- Análise dos percentuais de chegada de pacotes comprimentos de rota descritos.

A razão para a inclusão das topologias *SkipGraph* e *SkipNet* é a presença de um grau extra de randomização no procedimento de construção da rede, que pode ser favorável para comunicação anônima e merece ser observado. Esta mesma observação também motivou a inclusão das topologias *Chord* randomizado e hipercubo randomizado.

Nas descrições subseqüentes, n é o número de nós conectados à rede e o espaço de endereça-mento é o anel de inteiros $\mathbb{Z}_{2^b}$. O sucessor e o predecessor de um nó são os nós que o precede e o sucede, respectivamente, com a ordenação no sentido anti-horário do anel. Cada nó é responsável pela porção de endereçamento compreendida entre o primeiro identificador após o seu predecessor e o seu próprio identificador. A atribuição de identificadores é aleatória, para que o espaço de endereçamento seja dividido eqüitativamente entre os nós. As conexões são denotadas por setas em vermelho, podendo ser unidirecionais ou bidirecionais. Em todas as topologias, além das conexões determinadas por relação matemática, cada nó deve manter pelo menos uma conexão com o seu sucessor na estrutura. As conexões de cada nó para o seu sucessor são necessárias para que uma coesão mínima da rede seja mantida na presença de falhas consecutivas de uma porção significativa dos nós conectados.

A Figura 9 ilustra estes conceitos. São apresentados os nós sucessor e predecessor do nó 0, o círculo que delimita o espaço de endereçamento sob controle do nó 0 e as conexões que o nó 0 mantém com os nós 2, 5, 9 e 19, governadas por uma topologia hipotética.

Nos tópicos subseqüentes, as topologias avaliadas são resumidamente apresentadas.

5.2.1 *Chord* [11]

A topologia *Chord* é uma das mais populares. Nesta topologia, um nó com identificador x conecta-se ao seu sucessor e a b outros nós, com identificadores $x + 2^i \pmod{2^b}$ para $0 \leq i < b$.

Como normalmente a rede é esparsa, tendo muito menos que 2^b nós, um nó com identificador x conecta-se aos nós que possuem os identificadores $x + 2^i \pmod{2^b}$ para $i = 0, 1, \ldots, b-1$ nas porções do espaço de endereçamento que controlam. Conseqüentemente, algumas das conexões mantidas por um nó terminam em um mesmo vizinho.

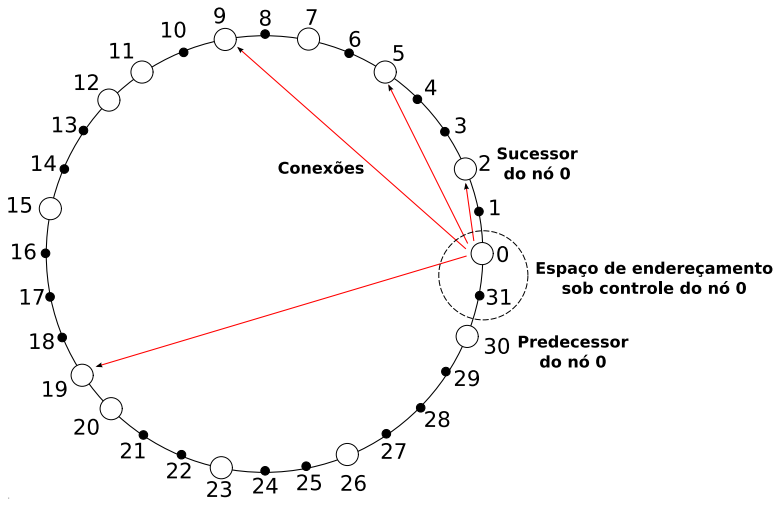
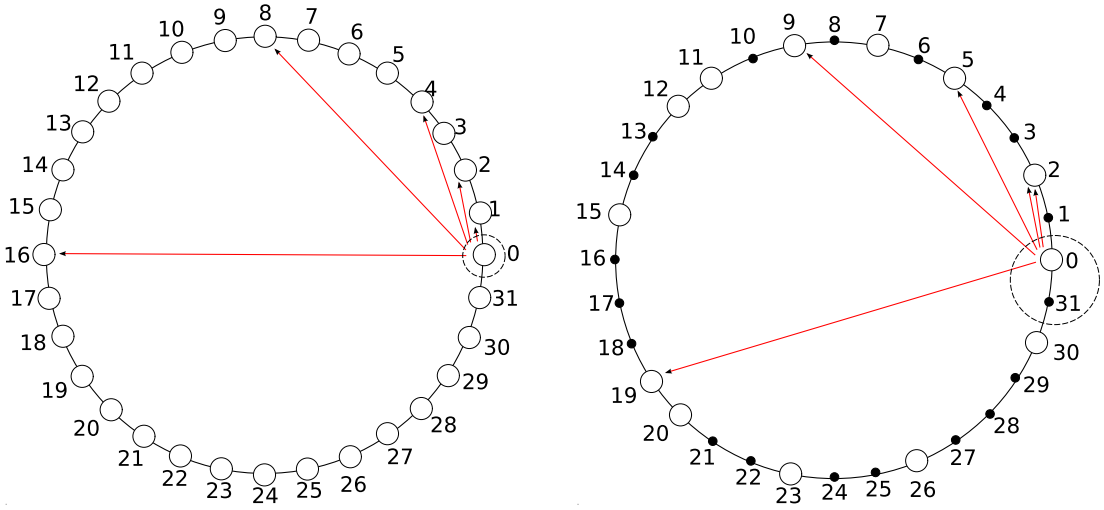


Figura 9: Exemplo de topologia estruturada, ilustrando a participação de um nó particular.

A Figura 10 ilustra a topologia *Chord*, em uma configuração ideal (rede completa) e em uma configuração prática (rede esparsa). Em ambas as configurações, as conexões estabelecidas pelo nó com identificador 0 apresentam-se em vermelho, bem como a porção de endereçamento de responsabilidade do nó 0. Na rede esparsa, pode-se observar que a compensação da topologia determina os vizinhos do nó 0 a partir do particionamento do espaço de endereçamento.



(a) Exemplo de topologia *Chord* completa.

(b) Exemplo de topologia *Chord* esparsa.

Figura 10: Exemplos de configurações ideal e prática de uma topologia *Chord*.

5.2.2 *Chord* randomizado [19]

Chord randomizado é uma variante da topologia *Chord*. A diferença reside no não-deter-minismo da topologia: um nó com identificador x conecta-se ao seu sucessor e a b outros nós, com identificadores $x + 2^i + r(i) \pmod{2^b}$, com $0 \leq i < b$ e $r(i)$ um inteiro uniformemente aleatório no intervalo $[0, 2^i)$.

5.2.3 Hipercubo [12, 13]

Em uma topologia de hipercubo, cada nó conecta-se a seu sucessor e a b outros nós. Para $i \leq 1 \leq b$, um nó com identificador x conecta-se com um nó y, se os *bits* de x e y forem idênticos, com exceção do i-ésimo *bit*. As observações a respeito do caráter esparso da rede também se aplicam neste caso.

5.2.4 Hipercubo randomizado [20]

Em um hipercubo randomizado, para $1 \leq i \leq b$, um nó com identificador x conecta-se ao seu sucessor e aos nós que compartilham os mesmos i *bits* mais significativos e diferem no i-ésimo *bit*. Os demais *bits* são gerados aleatoriamente.

5.2.5 *SkipGraph* [21]

Em um *SkipGraph*, um nó possui um identificador x e um conjunto de conexões. As conexões são definidas por um *vetor de pertinência* m_x, formado por uma cadeia infinita de *bits* aleatórios. Vetores de pertinência são gerados independentemente por cada nó.

Como nas outras topologias, os nós escolhem identificadores no espaço $\{0, 1, \ldots, n-1\}$ e organizam-se em um círculo ordenado. O nó com identificador x conecta-se necessariamente ao seu predecessor e ao seu sucessor. As demais conexões são determinadas pelos vetores de pertinência. Seja $m_{x,i}$ os i primeiros *bits* de m_x e seja (x, y) o intervalo de identificadores entre x e y, em sentido anti-horário de x para y. Os nós x e y são conectados se para algum j, $m_{x,j} = m_{y,j}$, e não há qualquer nó $z \in (x, y)$ tal que $m_{z,j} = m_{x,j}$. Ou seja, dois nós estão conectados se os seus vetores de pertinência compartilham algum prefixo que não é compartilhado por nenhum dos nós entre eles. Com alta probabilidade, cada nó mantém um número de conexões logarítmico em n. Por esta razão, o vetor de pertinência pode ser instanciado sob demanda e, normalmente, apenas b *bits* do vetor de pertinência precisam ser instanciados.

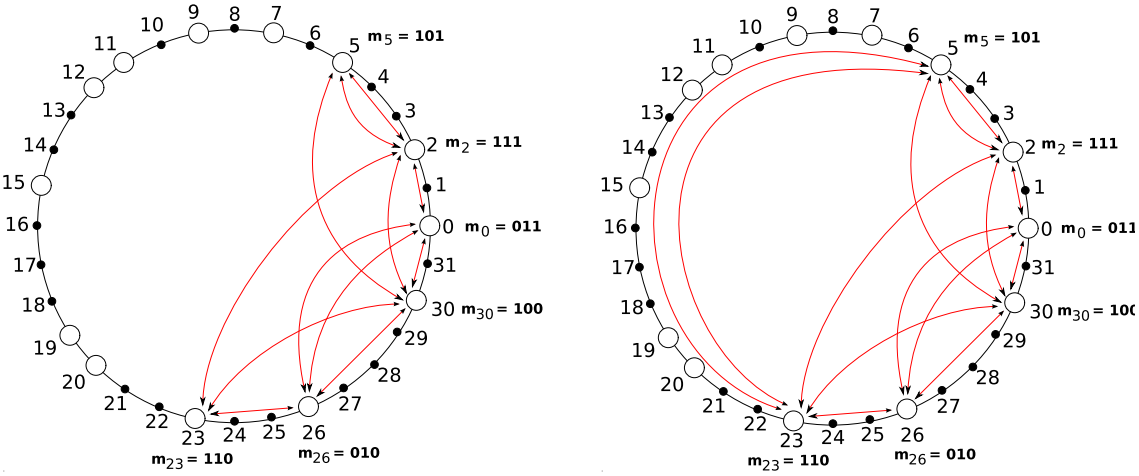
Uma propriedade útil do *SkipGraph* é que as conexões não dependem de propriedades matemáticas dos identificadores, mas apenas de sua ordenação e vetores de pertinência. Por isso, a topologia *SkipGraph* oferece funcionalidade de árvore e suporta buscas complexas, como a busca de recursos que se localizam dentro de um intervalo desejado [21].

5.2.6 *SkipNet* [22]

SkipNet é uma topologia bastante similar a *SkipGraph*, proposta independentemente. Uma *SkipNet* é uma superposição de múltiplos anéis, construídos probabilisticamente. Cada nó armazena um identificador numérico especial, que funciona como um vetor de pertinência.

Nós que compartilham um prefixo de j *bits* do identificador especial participam de um dos anéis de nível j.

A Figura 11 ilustra tanto um *SkipGraph* como uma *SkipNet*. Alguns nós da estrutura são desconsiderados na figura por simplificação. As conexões bidirecionais são apresentados e pode-se verificar a relação entre as conexões e os vetores de pertinência. A diferença essencial entre as duas topologias reside na superposição de anéis da topologia *SkipNet*, em contraste à superposição de listas da topologia *SkipGraph*.



(a) Exemplo de topologia *SkipGraph*.

(b) Exemplo de topologia *SkipNet*.

Figura 11: Comparação entre as topologias *SkipGraph* e *SkipNet*.

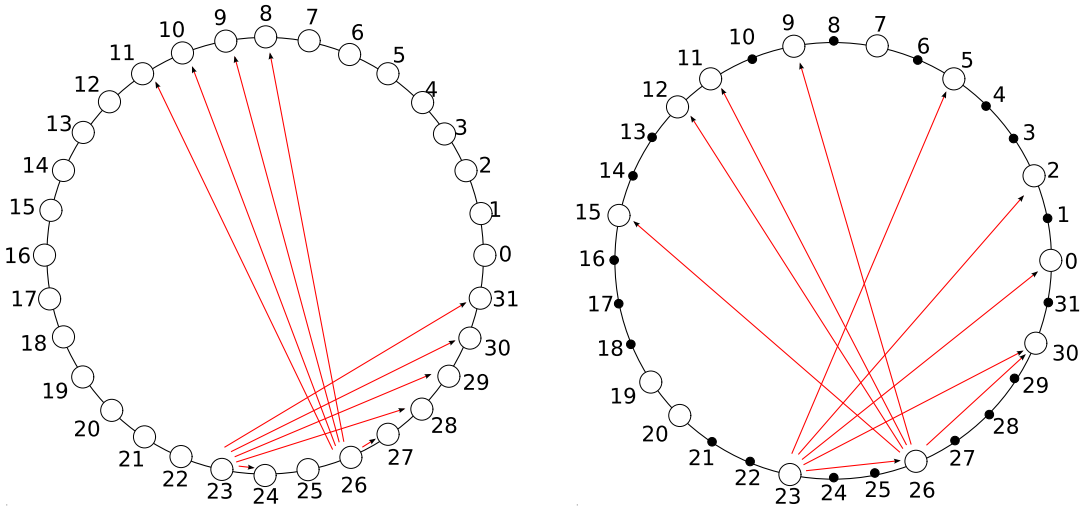
5.2.7 *Koorde* [23]

Koorde é uma estrutura baseada em grafos *de Bruijn* [26]. Um grafo *de Bruijn* com t dimensões é um grafo dirigido que representa sobreposições entre seqüências de símbolos. O grafo completo tem t^n vértices, consistindo em todas as seqüências de símbolos de comprimento n. Se um vértice v pode ser representado pelo deslocamento de todos os símbolos de um vértice u e adição de um novo símbolo à direita, então existe uma aresta dirigida de u para v. Grafos *de Bruijn* são favoráveis para aplicações *peer-to-peer* porque possuem grau constante.

Na topologia *Koorde*, um nó com identificador x conecta-se a seu sucessor e a d outros nós com identificadores $d \cdot x + j \pmod{2^b}$, com $0 \leq j < d$. Para um espaço de endereçamento binário, d é escolhido como uma potência de 2. Assim, os identificadores podem ser vistos como seqüências de $\frac{b}{\log_2 d}$ dígitos na base d, com as conexões definidas por um deslocamento à esquerda e inserção de um novo dígito à direita. Uma propriedade relevante de grafos *de Bruijn* é que um caminho aleatório iniciado no nó x com comprimento $\frac{b}{\log_2 d}$, termina em um nó com identificador totalmente diferente de x. A quantidade d é denominada *grau* da topologia.

A estrutura *Koorde* exige adaptação para redes esparsas: um nó com identificador x conecta-se ao nó $y = d \cdot x \pmod{2^b}$ e os d sucessores de y. Isto é necessário para que as propriedades de roteamento na rede sejam mantidas, especialmente o comprimento logarítmico de qualquer rota.

A Figura 12 ilustra configurações ideal e prática para uma topologia *Koorde*. Na figura, as conexões dos nós 23 e 26 são destacadas e o grau utilizado é $d = 4$. A notação *Koorde-d* é utilizada para denotar uma topologia *Koorde* de grau d.



(a) Exemplo de topologia *Koorde-4* completa. (b) Exemplo de topologia *Koorde-4* esparsa.

Figura 12: Exemplos de configurações ideal e prática de uma topologia *Koorde* de grau 4.

5.3 Adversário

O adversário é modelado como um conjunto de nós comprometidos e atuando em conluio, compartilhando conhecimento entre si. Considerando o contexto de sistemas *peer-to-peer* estruturados, é um adversário local, interno e passivo. As observações do adversário são realizadas por meio da captura de mensagens nos nós que controla. O ataque executado pelo adversário é um ataque de predecessor [27]: analisando os vizinhos imediatos que encaminharam as mensagens para os nós comprometidos, o adversário tenta inferir as verdadeiras origens das mensagens.

Como ataques de predecessor são particularmente efetivos em redes que utilizam roteamento por caminhos aleatórios [27], avaliar as topologias utilizando a efetividade de um ataque de predecessor é um procedimento válido de comparação. Entretanto, as conclusões obtidas são estritamente válidas para cenários que reproduzem com fidelidade as características do adversário e ataque considerados.

5.4 Simulação

Para cada uma das topologias estruturadas, um experimento é realizado. O número total de nós na rede é n, dos quais c nós são controlados por adversários. Em cada experimento, 22 comprimentos distintos de caminho aleatório são avaliados. Para cada comprimento, são executadas 50 simulações. Uma única simulação é composta pelas seguintes etapas:

1. Seleção de um nó não-controlado por adversário $a_d \in \mathcal{A}$, o destino único para todas as mensagens da simulação;

2. Execução de eventos de comunicação consecutivos, que simulam a transmissão de k mensagens de cada um dos participantes $a_i \in \mathcal{A}$ para o destino a_d. Os nós controlados pelo adversário e o destino a_d não participam da simulação como emissores de mensagem. Assim, o número total de eventos de comunicação de uma simulação é $k(n-c-1)$;

3. Gravação do predecessor observado para cada mensagem interceptada por nó malicioso. Os nós controlados pelo adversário descartam as mensagens capturadas imediatamente após a gravação da observação correspondente; e

4. Cálculo da métrica de entropia condicional do sistema, considerando as observações do adversário.

Para cada comprimento de caminho aleatório l, a média aritmética é tomada sobre as 50 medidas de entropia condicional calculadas. O resultado é a *entropia condicional do roteamento randomizado para um caminho aleatório de comprimento* l.

A simulação objetiva facilitar o cálculo da quantidade de informação que o roteamento randomizado revela a respeito da origem das mensagens. Ou seja, a simulação avalia as topologias apenas pela qualidade de anonimato de envio que fornecem. Mas, geralmente, os anonimatos de resposta e de par comunicante são também favorecidos por uma boa qualidade de anonimato de envio.

Para o cálculo da entropia, é utilizado o procedimento descrito por Borisov [15]. Primeiramente, é necessário obter a distribuição conjunta de probabilidade das variáveis A, Y, com A tomando valores no conjunto de participantes e Y tomando valores no domínio de observações do adversário. O domínio da variável A é o conjunto dos identificadores dos participantes $\mathcal{A} = \{1, 2, \ldots, n-c\}$. O domínio da variável Y é a união entre o conjunto dos identificadores dos nós que podem ser observados como predecessor e um elemento especial para indicar que nenhum predecessor foi observado (a mensagem não foi interceptada), ou seja, $\mathcal{Y} = \mathcal{A} \cup \{\varnothing\}$. Um contador $c_{a_i,y}$ é utilizado para cada par (a_i, y) e armazena o número de vezes que um predecessor $y \in \mathcal{Y}$ foi observado pelo adversário em eventos de comunicação iniciados pelo participante $a_i \in \mathcal{A}$.

Este procedimento permite estimar a distribuição conjunta de probabilidade A, Y empiricamente. A probabilidade estimada no ponto (a_i, y), é dada por $q_{a_i,y} = c_{a_i,y}/k$. Com a distribuição estimada de probabilidade, calcula-se a entropia estimada $\widetilde{H}(A|Y = y)$ de cada um dos predecessores observados. Este cálculo de entropia é realizado utilizando uma adaptação da expressão 2 para levar em conta as probabilidade estimadas:

$$\widetilde{H} = -\sum_{a_i \in \mathcal{A}} q_{a_i,y} \cdot \log_2 (q_{a_i,y}). \tag{7}$$

Para calcular a entropia condicional, é preciso estimar a probabilidade $Pr[Y = y]$ de cada observação $Y = y$ ocorrer. Esta probabilidade é estimada a partir da razão q_y entre o número total de observações de y como predecessor e o número de mensagens totais:

$$q_y = \frac{\sum_{a_i \in \mathcal{A}} c_{a_i,y}}{(n-c-1)k}. \tag{8}$$

A partir das entropias individuais, pode-se calcular a entropia condicional estimada $\widetilde{H_c}$ pela modificação da expressão 5:

$$\widetilde{H_c} = \sum_y q_y \cdot \widetilde{H}(A|Y = y). \tag{9}$$

5.4.1 Acurácia das estimativas

A acurácia das estimativas [15] depende da diferença entre as distribuições de probabilidade estimada empiricamente q e da probabilidade real p.

A estimativa de entropia é chamada de *estimador de máxima verossimilhança*. Este estimador tem distribuição normal, para uma média μ e uma variância σ^2 [28]. A variância depende do número de amostras $k(n-c-1)$ e tem limite superior:

$$\sigma^2 \leq \frac{\log_2 m}{k(n-c-1)}, \tag{10}$$

tendendo a 0 com o crescimento de k, onde m é o número de posições não-nulas da distribuição q. A média apresenta uma polarização negativa b limitada:

$$-\log_2 \left(1 + \frac{m-1}{k(n-c-1)}\right) \leq b \leq 0, \tag{11}$$

que também tende a 0 com o crescimento de k [28].

Para o cálculo da variância e da polarização da estimativa de entropia condicional, a seguinte identidade de entropia é necessária:

$$H(A|Y) = H(A,Y) - H(Y), \tag{12}$$

onde $H(A,Y)$ é a entropia da distribuição conjunta de probabilidade A, Y e pode ser estimada por

$$\widetilde{H}(A,Y) = \sum_{a_i \in \mathcal{A}, y \in \mathcal{Y}} q_{a_i,y} \log_2 (q_{a_i,y}). \tag{13}$$

Similarmente, pode-se estimar a entropia $H(Y)$ por:

$$\widetilde{H}(Y) = \sum_{y \in \mathcal{Y}} q_y \log_2 (q_y). \tag{14}$$

Sejam b_0 e b_1 os limites da polarização negativa para $\widetilde{H}(A, Y)$ e $\widetilde{H}(Y)$, respectivamente, e sejam σ_0^2 e σ_1^2 suas respectivas variâncias, todas calculadas a partir dos limites fornecidos anteriormente. Tanto b_0 e b_1, quanto σ_0^2 e σ_1^2, tendem a 0 quando $k \to \infty$. Para a entropia condicional estimada

$$\widetilde{H_c} = \widetilde{H}(A|Y) = \widetilde{H}(A, Y) - \widetilde{H}(Y), \tag{15}$$

o erro gerado pela polarização negativa encontra-se no intervalo aberto $(-b_0, b_1)$ e a variância é dada por [28]:

$$\sigma_c \leq \sigma_0^2 + \sigma_1^2 + 2\sigma_0\sigma_1. \tag{16}$$

Como as fontes de erro da estimativa diminuem com o crescimento do número de amostras $k(n-c-1)$, conclui-se que as estimativas de entropia e entropia condicional são acuradas e podem ser confiadas como resultados da experimentação.

A simulação não reproduz eventos de entrada e saída de nós na rede nem latências de comunicação. Apesar disso, é suficiente para comparar as topologias estruturadas para comuni-cação anônima, considerando o adversário e o tipo de ataque já descritos.

5.4.2 Validação

A rede *Crowds* foi utilizada para validar o ambiente de simulação construído [15]. A metodologia de validação consistiu em calcular analiticamente a entropia da rede *Crowds* (equação 2) e comparar o resultado com a entropia medida a partir de simulação.

Seja uma rede *Crowds* com n participantes e probabilidade de encaminhamento $0 < p_f < 1$. Quando um nó intermediário tenta determinar a origem de uma mensagem que encaminha, ele pode considerar um conjunto de anonimato de tamanho máximo $n - 1$ (excluindo a si mesmo). Entretanto, a probabilidade de que o predecessor observado da mensagem seja a origem é igual a probabilidade de que nenhum outro nó tenha encaminhado a mensagem para o predecessor:

$$p_p = 1 - \frac{p_f(n-2)}{n}. \tag{17}$$

A probabilidade de qualquer outro nó ter originado a mensagem é p_f/n [7].

Este cálculo pode ser estendido para o caso onde c dos n participantes são nós controlados pelo adversário atuando em conluio, ou seja, podem excluir-se entre si de suas conclusões. Neste caso, a probabilidade do predecessor observado ser a origem é:

$$p_p = 1 - \frac{p_f(n-c-1)}{n}, \tag{18}$$

enquanto a probabilidade de qualquer outro nó ter originado a mensagem continua a mesma. Esta diferença entre a probabilidade do predecessor ser a origem e a probabilidade de qualquer outro nó ser a origem motiva o ataque de predecessor: ao observar vários predecessores para um volume considerável de mensagens interceptadas, o adversário deve detectar uma distorção na distribuição de probabilidade, que fornece informação para identificação da verdadeira origem. A entropia da rede *Crowds* é calculada por [4]:

$$H = -\left(1 - \frac{p_f(n-c-1)}{n}\right)\log_2\left(1 - \frac{p_f(n-c-1)}{n}\right) - \left(\frac{n-c-1}{n}\frac{p_f}{n}\right)\log_2\left(\frac{p_f}{n}\right) \quad (19)$$

Por exemplo, uma rede *Crowds* com 100 nós, dos quais 10 são controlados por adversário, e com probabilidade de encaminhamento $p_f = 0.75$, tem entropia $H \approx 5.24$ *bits*. A entropia teórica ótima para um sistema assim corresponde à distribuição uniforme dos eventos sobre os $(n-c)$ nós legítimos: $\log_2(n-c) = \log_2 90 \approx 6.49$ *bits* de informação. O sistema revela pouco mais de 1 *bit* de informação para o adversário e o tamanho efetivo do conjunto de anonimato passa de 90 para $2^{5.24} \approx 38$ nós.

Deve-se ainda considerar o volume de mensagens que não são interceptadas por nós controlados pelo adversário. A probabilidade de uma mensagem atingir o destino passando apenas por nós honestos (não-controlados pelo adversário) é:

$$p' = \frac{n-c}{n}(1-p_f)\cdot\sum_{i=0}^{\infty}\frac{n-c}{n}(p_f)^i = 1 - \frac{c}{n-p_f(n-c)}. \quad (20)$$

Neste caso, a entropia dos eventos é $H' = \log_2(n-c)$, já que o adversário não captura nenhuma mensagem e não obtém informação. A entropia condicional, considerando os dois cenários é:

$$H_c = (1-p')H + p'H' = \frac{c}{n-p_f(n-c)}H + \left(1 - \frac{c}{n-p_f(n-c)}\right)\log_2(n-c). \quad (21)$$

Usando esta expressão, o sistema com as mesmas características anteriores ($n = 100$, $c = 10$ e $p_f = 0.75$) tem entropia condicional $H_c = 6.11$ *bits*. O tamanho efetivo do conjunto de anonimato passa a ser $2^{6.11} \approx 69$ nós.

A validação do experimento consiste na comparação entre a entropia condicional estimada por simulação e a entropia condicional calculada analiticamente. A Figura 13 apresenta a entropia teórica e a estimada por simulação. Os intervalos de confiança de 95% da estimativa de entropia, considerando a polarização negativa, são também apresentados. A partir deste gráfico, percebe-se que a entropia estimada converge para a entropia teórica e o erro diminui com o crescimento de amostras. A interpretação do gráfico ainda sugere que um número de amostras adequado para as simulações posteriores é da ordem de 1 milhão.

5.5 Resultados experimentais

As topologias descritas anteriormente foram submetidas ao experimento de simulação, que permitiu a coleta das observações realizadas pelo adversário. Os experimentos simularam redes com 256 nós comunicando-se anonimamente, sendo 10% destes nós controlados

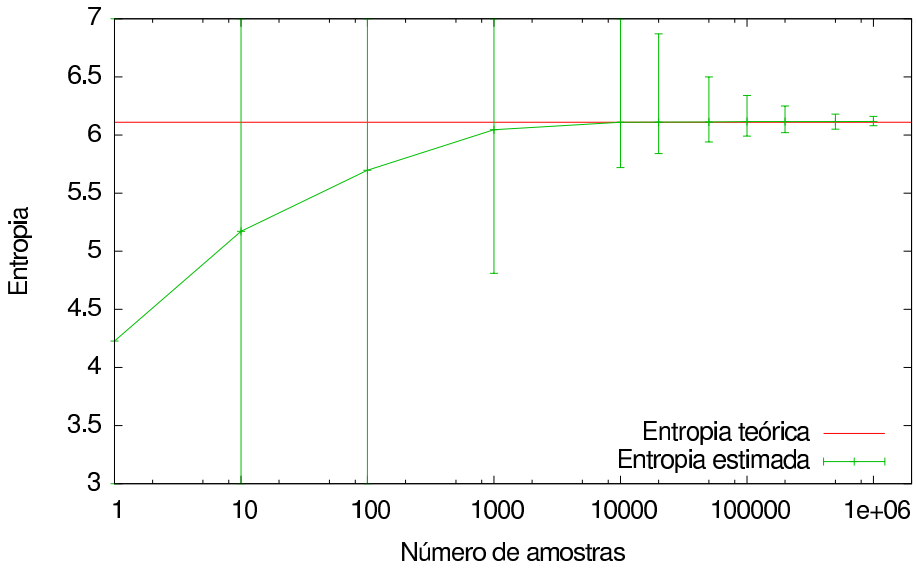


Figura 13: Estimativa de entropia condicional na rede *Crowds*.

pelo adversário. Nos gráficos subseqüentes, cada ponto corresponde a uma média aritmética de 50 simulações sucessivas e cada simulação reproduz 1 milhão de eventos de comunicação. O espaço de endereçamento utilizado foi o anel de inteiros $\mathbb{Z}_{2^{160}}$.

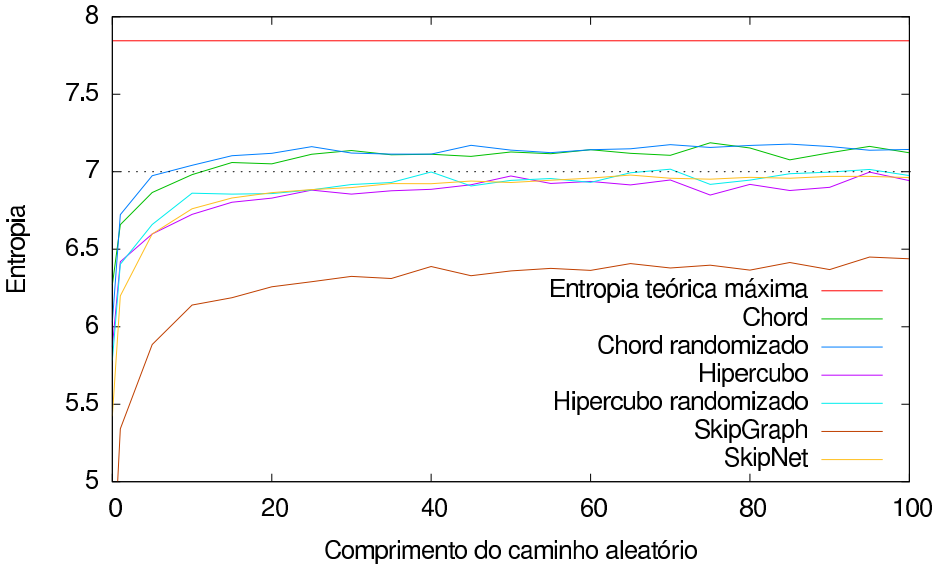
Segundo os critérios de seleção adotados, as topologias foram avaliadas de acordo com a métrica de entropia, a resistência da topologia a ataques de negação de serviço e o compromisso entre desempenho e qualidade de anonimato.

5.5.1 Entropia

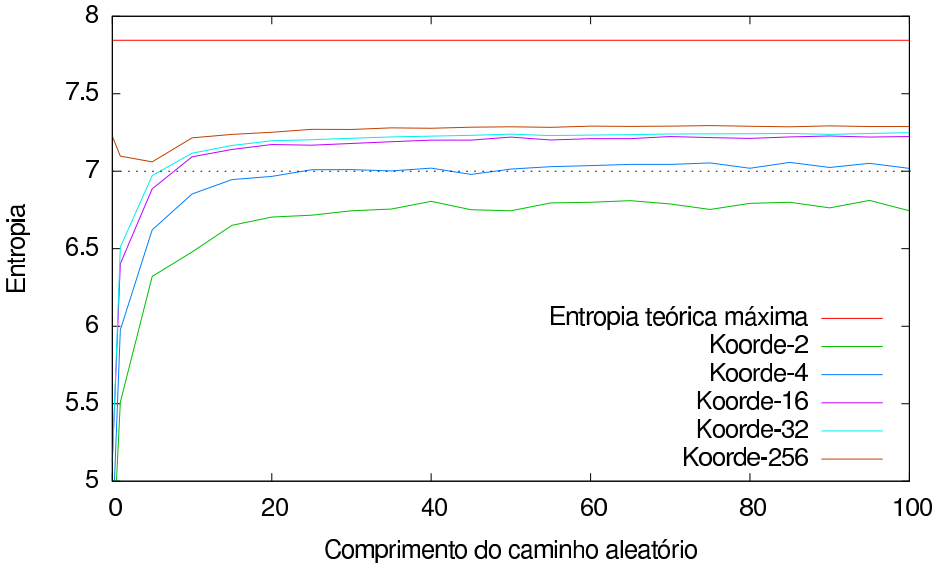
Os resultados experimentais da métrica de entropia condicional encontram-se na Figura 14. As topologias estruturadas foram divididas em dois conjuntos para facilitar a visualização dos resultados. O valor rotulado como entropia teórica máxima é o nível $\log_2(n-c)$. O nível 7 de entropia também foi acrescentado para facilitar a comparação entre as curvas dos dois gráficos.

A partir dos gráficos, pode-se concluir que:

- O aumento do grau nas topologias *Koorde* colabora para o aumento de entropia;
- Os resultados da rede *Koorde-256* representam uma espécie de limite prático para a topologia *Koorde*. Isto se deve ao fato de que em uma rede *Koorde* com 256 nós e grau 256, cada um dos nós conecta-se a todos os outros. Este é um cenário ideal, do ponto de vista prático;
- A entropia nas topologias *Koorde-32* e *Koorde-16* é superior à entropia de qualquer topologia presente no primeiro gráfico;



(a) Primeiro conjunto de topologias.



(b) Segundo conjunto de topologias.

Figura 14: Resultados experimentais de entropia condicional.

- A topologia *Koorde-16* é superior às topologias *Koorde-32* e *Koorde-256*, considerando uma razão entre custo e benefício, já que as três possuem entropias bastante próximas e a primeira tem uma sobrecarga de manutenção muito inferior às demais (menor número de conexões para manter);

- As versões randomizadas das topologias fornecem ganho em relação às topologias

originais. Isto mostra que um certo grau de aleatoriedade presente na topologia pode colaborar com a entropia;

- As topologias com maior aleatoriedade e menor regularidade, *SkipGraph* e *SkipNet*, obtiveram alguns dos piores resultados. Pode-se inferir que o aumento de aleatoriedade, apesar de contribuir com o ganho de entropia, deve vir combinado a um certo grau de regularidade para ser útil. A topologia *SkipNet* obteve resultado superior à topologia *SkipGraph*, por causa da organização orientada a anéis, que garante aos nós um maior número de possibilidades de roteamento durante o caminho aleatório; e

- A seqüencia *Koorde*, *Chord* e Hipercubo, em ordem decrescente de entropia, é idêntica à seqüência obtida por [15], em ordem decrescente de capacidade de mistura. Isto confirma experimentalmente a hipótese intuitiva de que a capacidade de mistura é uma grandeza intimamente relacionada à entropia.

5.5.2 Resistência à negação de serviço

Considerando que os nós controlados pelo adversário descartam todas as mensagens que deveriam rotear, as mesmas simulações são utilizadas para examinar a eficácia deste ataque distribuído de negação de serviço no funcionamento da rede. A resistência à negação de serviço foi medida a partir do percentual de mensagens que chegaram com sucesso em seus destinos. Os resultados experimentais para o percentual de chegada encontram-se na Figura 15.

As conclusões do experimento são:

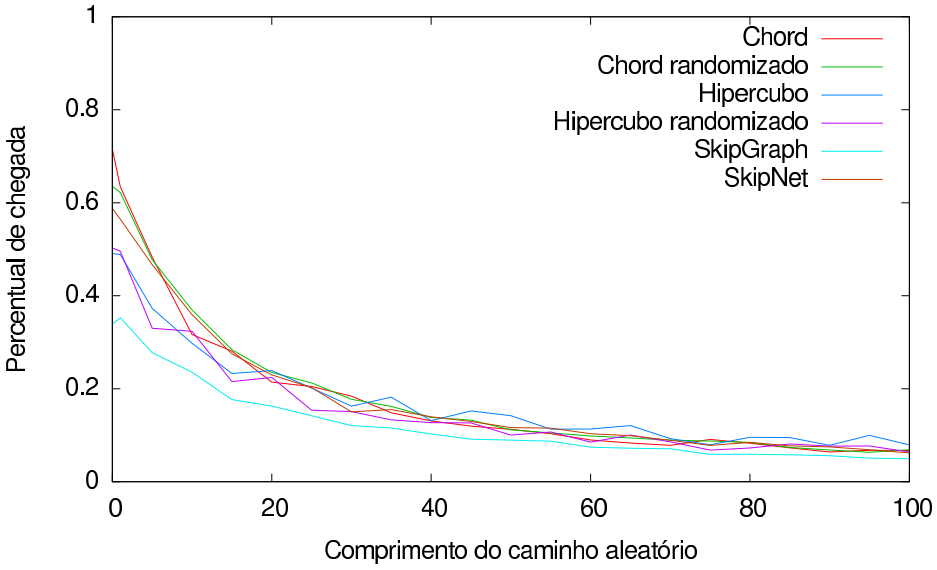
- A topologia *Koorde-256* apresentou resultado extremamente superior às demais topologias, como esperado. Percebe-se que a taxa de chegadas das mensagens, para um caminho aleatório de comprimento mínimo, chega a 90% – justamente a proporção de nós íntegros em relação aos nós totais. A razão para este fenômeno é que o percorrimento do caminho aleatório, apesar de aumentar a entropia, eleva as chances de captura e descarte por um nó malicioso;

- O aumento de grau nas topologias *Koorde* não só colabora com o aumento de entropia, como verificado anteriormente, mas também aumenta a resistência a ataques de negação de serviço executados por um adversário interno;

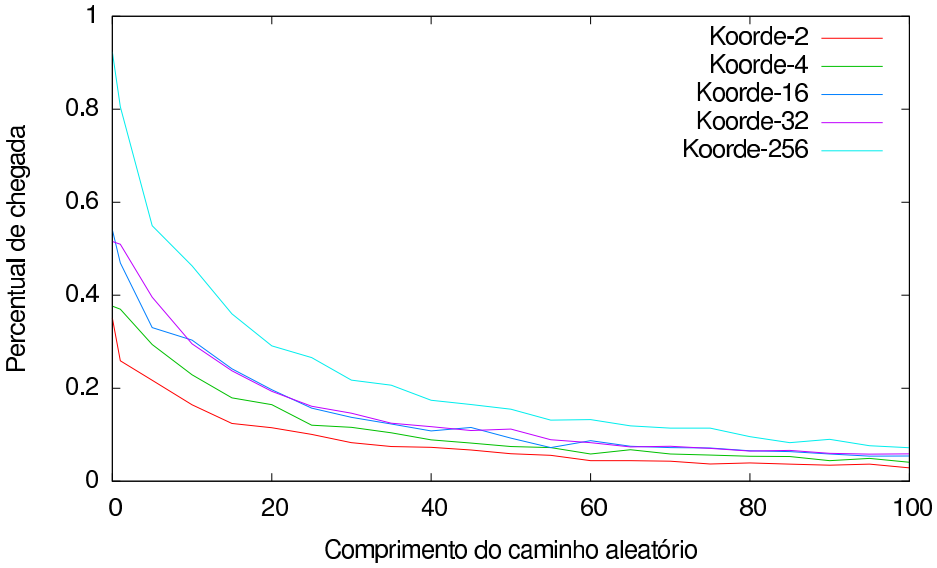
- A randomização das topologias não provoca ganhos significativos na taxa de chegada de mensagens;

- Apesar das topologias *Koorde* apresentarem resultado inferior às demais topologias nesta categoria, a diferença não é muito significativa; e

- Existe uma relação entre entropia e taxa de chegada: topologias que distribuem melhor as mensagens têm chance maior de entregá-las com sucesso. Várias das topologias que obtiveram as maiores entropias, também apresentaram as melhores taxas de chegada.



(a) Primeiro conjunto de estruturas.



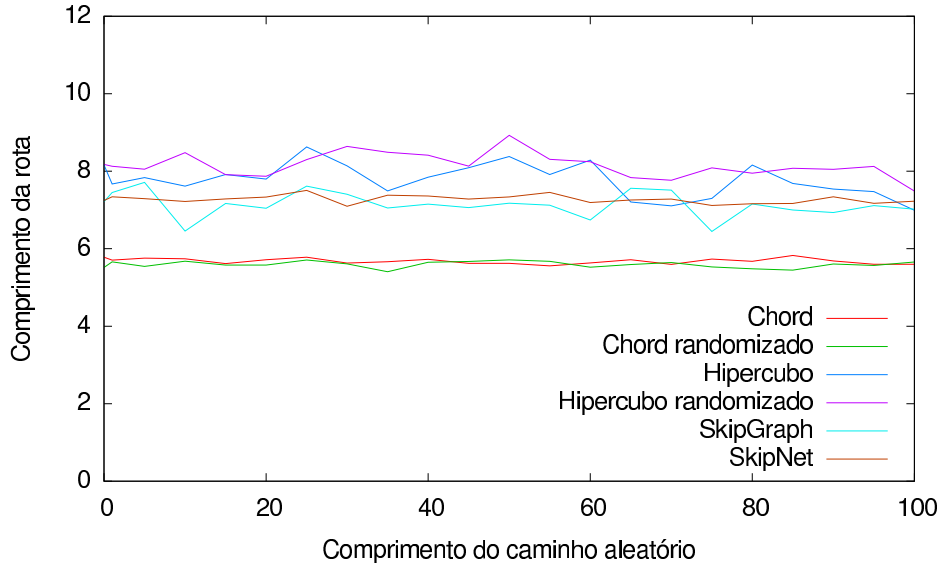
(b) Segundo conjunto de estruturas.

Figura 15: Resultados experimentais de resistência à negação de serviço.

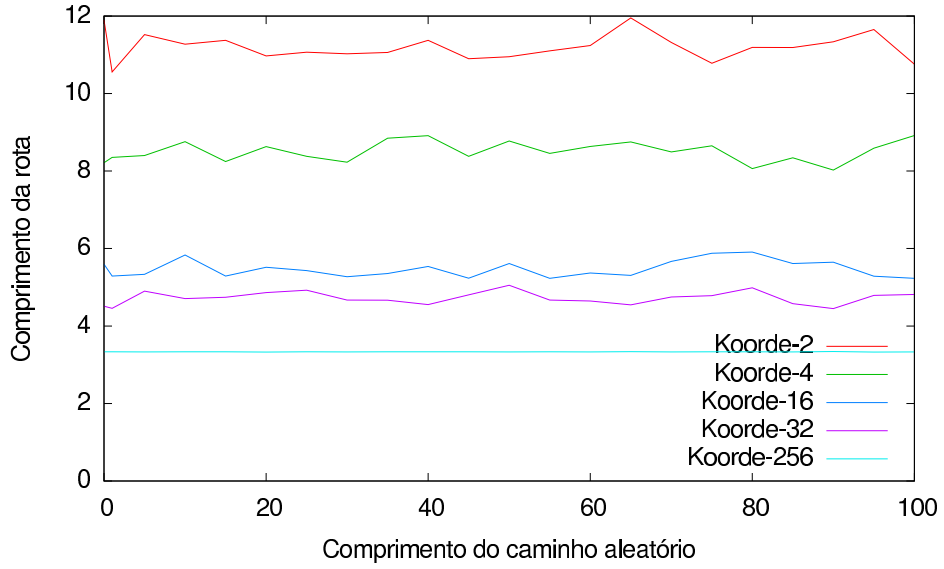
5.5.3 Desempenho

O critério final de avaliação foi a medida do comprimento das rotas percorridas durante a segunda fase de roteamento. A primeira fase de roteamento é ignorada, porque está condicionada à uma probabilidade de encaminhamento idêntica para todas as topologias. A seleção de uma topologia com rotas curtas e que privilegia a métrica de entropia é decisiva,

por representar um compromisso ótimo entre desempenho e anonimato. Os resultados experimentais de comprimento de rotas encontram-se na Figura 16.



(a) Primeiro conjunto de estruturas



(b) Segundo conjunto de estruturas

Figura 16: Resultados experimentais de desempenho.

A partir da interpretação dos gráficos, conclui-se que:

- O aumento do grau na topologia *Koorde* também diminui o comprimento das rotas, incrementando diretamente o desempenho da topologia;

- A randomização das topologias não provoca ganhos significativos de desempenho;
- As topologias com melhor entropia também apresentaram as rotas mais curtas; e
- A topologia *Koorde-32* apresenta desempenho favorável em relação à topologia *Koorde-16*, mas a diferença no tamanho médio das rotas não chega a alcançar 1 nó.

5.6 Seleção da topologia

Apesar da topologia *Koorde-256* apresentar os melhores resultados em todas as categorias, a sobrecarga de manutenção da rede é muito elevada. O número de conexões simultâneas que esta estrutura exige para funcionamento correto é bem superior a 256 conexões por nó, somando-se as conexões que o nó inicia com as conexões iniciadas pelos demais que terminam no nó. Avaliar a sobrecarga de manutenção é importante, visto que o percentual de banda útil para as aplicações anonimizadas depende diretamente da complexidade de manutenção da rede.

Considerando todas as conclusões apresentadas na seção anterior, para os critérios de entropia, desempenho e resistência a ataques de negação de serviço, a topologia que apresentou os melhores resultados foi a topologia *Koorde* com grau 16. Tendo entropia muito próxima das variantes de grau 32 e 256, bom desempenho e resistência razoável a ataques de negação de serviço, a topologia *Koorde-16* permite a construção de uma rede anônima eficiente e com boa qualidade de anonimato que exige baixa sobrecarga de manutenção. Apesar da topologia *Koorde-32* apresentar rotas um pouco menores, a baixa sobrecarga de manutenção da topologia *Koorde-16* privilegia a latência de transmissão em uma rede funcional, e deve compensar o maior comprimento das rotas com transmissões mais rápidas. Além disso, o baixo número de conexões que cada nó deve manter fornece maior flexibilidade para a modificação de algumas das características da estrutura. Isto é decisivo para o aprimoramento da topologia, realizado no restante deste capítulo.

6 Aprimoramento da topologia

Apesar de já oferecer entropia elevada, bom desempenho e resistência razoável à negação de serviço, a topologia *Koorde-16* ainda fornece amplo espaço para aperfeiçoamento. Nesta seção, diversas estratégias são sugeridas e avaliadas experimentalmente para aprimorar ainda mais as vantagens desta topologia. O objetivo é aproximá-la dos ótimos resultados da topologia *Koorde-256*, mantendo uma relação aceitável entre custo e benefício. O interesse por trás dos aprimoramentos é obter o máximo de entropia possível com o menor comprimento esperado de caminho aleatório.

6.1 Probabilidade de encaminhamento

A atribuição de uma probabilidade de encaminhamento adequada é vital para se construir uma rede de anonimização que apresente bom desempenho. Quanto maior a proba-

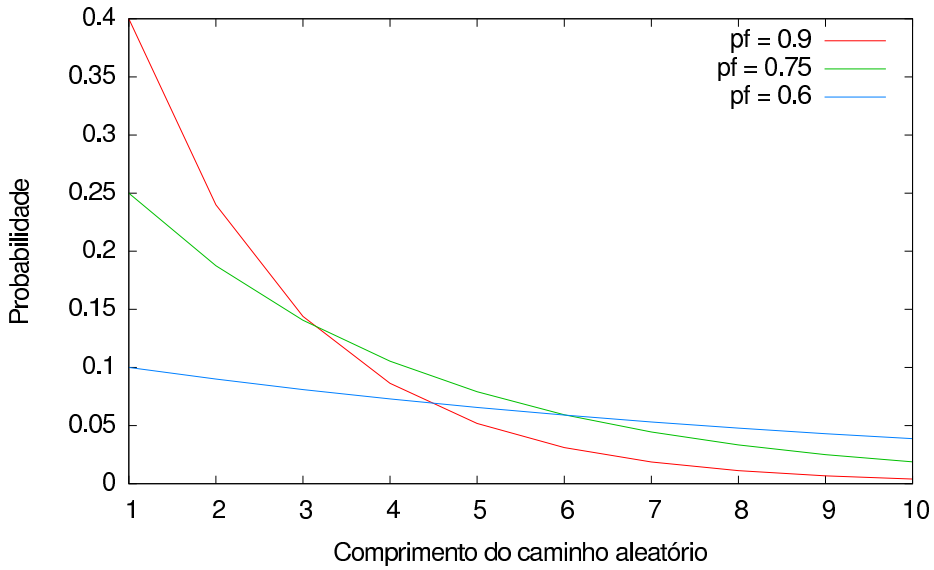


Figura 17: Distribuição de probabilidade do comprimento de um caminho aleatório.

bilidade de encaminhamento, maior o comprimento dos caminhos aleatórios e, conseqüentemente, maior a latência de transmissão. Em uma topologia *Koorde* com n nós de grau d, os caminhos aleatórios devem ter comprimento esperado de $\log_d n$ idealmente, para que alcancem um identificador aleatório [23].

Assim como na rede *Crowds*, a probabilidade de uma mensagem percorrer um caminho aleatório de comprimento l com probabilidade de encaminhamento p_f é dada por

$$p_l = {p_f}^l \cdot (1 - p_f). \tag{22}$$

O comprimento esperado l_e de um caminho aleatório associado a uma probabilidade de encaminhamento p_f é

$$l_e = \sum_{i=0}^{\infty} (i+1){p_f}^i(1-p_f) = \frac{1}{1-p_f}. \tag{23}$$

Inversamente, para se percorrer um caminho aleatório de comprimento aproximado l_e, cada nó deve encaminhar a mensagem para um de seus vizinhos com probabilidade $p_f = \frac{l_e-1}{l_e}$ e iniciar a segunda fase do roteamento com probabilidade $\frac{1}{l_e}$ [15]. A Figura 17 ilustra a distribuição de probabilidade do comprimento de um caminho aleatório para probabilidades de encaminhamento 0,6, 0,75 e 0,9.

É possível escolher a probabilidade de encaminhamento a partir da magnitude da rede. Para a escolha particular da topologia *Koorde-16* com suporte a uma rede anônima composta por 2^{20} nós, um nó com identificador x atinge um identificador aleatório após um caminho aleatório de comprimento esperado igual a $l_e = 5$. A probabilidade de encaminhamento condicionada ao comprimento do caminho aleatório é $p_f = \frac{5-1}{5} = 0,8$. Entretanto,

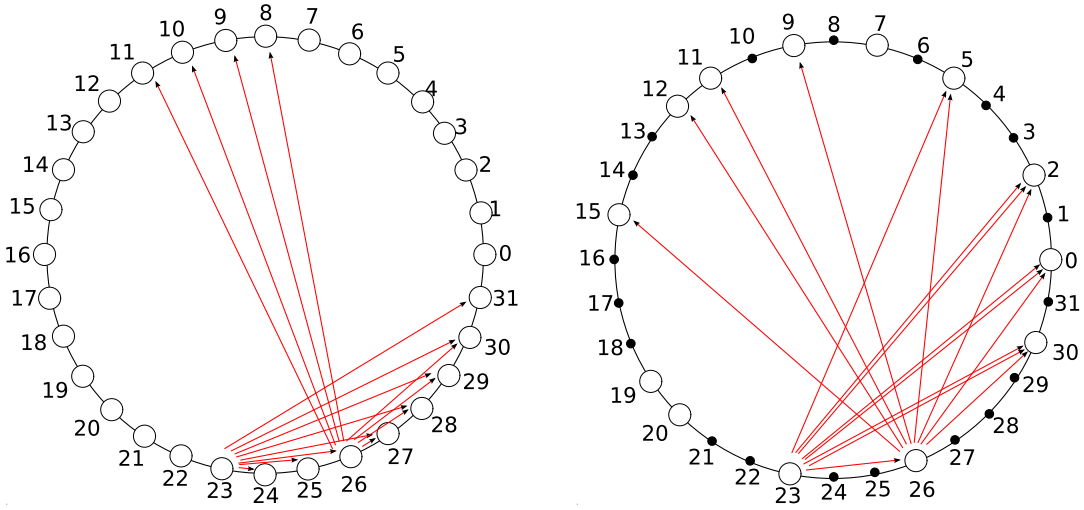
considerando-se que o não-determinismo proveniente do caráter esparso da rede, pode inserir pequenos desequilíbrios em sua estrutura, utiliza-se um comprimento esperado do caminho aleatório maior do que o comprimento estritamente necessário. Em compatibilidade com o valor sugerido por [15], utiliza-se uma probabilidade de encaminhamento correspondente ao dobro do comprimento aleatório necessário para se atingir um ponto independente. Logo: $p_f = \frac{(2l_e-1)}{2l_e} = 0,9$.

6.2 Tolerância a falhas

Tolerância a falhas refere-se à capacidade do sistema em continuar sua operação após a falha de uma porção significativa do sistema.

A formulação original da topologia *Koorde* sugere que, independente do grau, deve-se ter conexões adicionais para que a estrutura forneça tolerância a falhas. Um nó da estrutura *Koorde* com identificador x conecta-se a dois conjuntos de nós em locais diferentes do espaço de endereçamento: o seu sucessor e d nós com identificadores próximos a $d \cdot x \pmod{2^b}$. A conexão com o sucessor é extremamente importante, já que a coesão da estrutura em face da falha simultânea de uma porção significativa dos nós na rede depende diretamente da integridade das conexões entre os nós e seus sucessores. Assim, ao invés de manter uma única conexão com o seu sucessor, cada nó deve manter conexões com os seus d sucessores. Adicionalmente, cada nó deve ainda manter conexões com os d predecessores do nó $d \cdot x \pmod{2^b}$ [23]. A topologia modificada e tolerante a falhas é denominada *Koorde-t*.

A Figura 18 ilustra a modificação quando efetuada nas configurações apresentadas na Figura 12. As conexões dos nós 23 e 26, representadas por setas em vermelho, incluem as conexões necessárias para a topologia fornecer tolerância a falhas.



(a) Exemplo de topologia *Koorde-t-4* completa.

(b) Exemplo de topologia *Koorde-t-4* esparsa.

Figura 18: Configurações ideal e prática de uma topologia *Koorde-t* de grau 4.

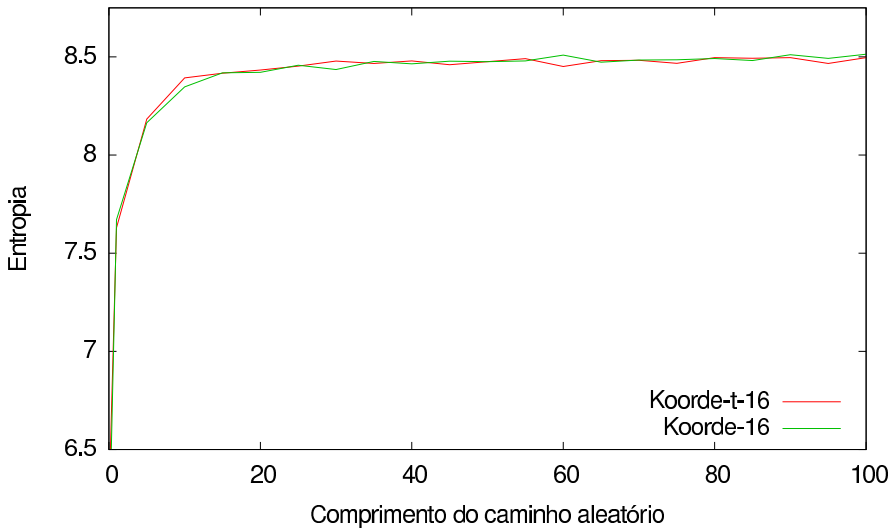


Figura 19: Resultados experimentais de entropia condicional da topologia *Koorde-t-16*.

Entretanto, é importante verificar se as novas conexões, quando utilizadas na seleção alea-tória de vizinhos da primeira fase do roteamento randomizado, exercem alguma influência na entropia da estrutura modificada. Para examinar esta hipótese, um novo experimento de simulação foi realizado para a estrutura *Koorde-t*. As mesmas características de simulação dos experimentos anteriores foram conservadas, alterando-se apenas o tamanho da rede para $n = 1024$ e o número de nós comprometidos para $c = 102$. A entropia teórica máxima deste sistema é $\log_2(n - c) \approx 9.85$. Os experimentos subseqüentes simularão redes com estas exatas características, visto que o aumento do tamanho da rede eleva a precisão e o rigor do experimento.

Foram testadas duas formas distintas de combinar as conexões para tolerância a falhas com as conexões convencionais da topologia *Koorde*. A primeira consiste na seleção aleatória de vizinhos dentre as 48 possibilidades totais (32 conexões para tolerância a falhas e 16 convencionais). A segunda consiste na seleção aleatória entre uma conexão para um nó próximo ao sucessor e 16 conexões convencionais, totalizando 17 possibilidades. Quando a conexão para um nó próximo ao sucessor é selecionada, um sorteio uniforme adicional entre as 32 conexões para tolerância a falhas escolhe o vizinho. Foi verificado experimentalmente que a primeira estratégia diminui a entropia da rede, porque as conexões para nós próximos ao sucessor tem menor entropia e são tomadas com probabilidade muito alta na seleção aleatória de vizinho. A Figura 19 mostra que a segunda estratégia aumenta a entropia da rede, especialmente para a probabilidade de encaminhamento $p_f = 0,9$, apesar do ganho ser pouco significativo.

6.3 Conexões adiantadas

Uma técnica recentemente proposta na área de pesquisa em sistemas *peer-to-peer*, para otimizar decisões de roteamento e a eficiência de sistemas estruturados [29], consiste em fornecer, para cada nó da rede, conhecimento privilegiado que antes era de exclusividade dos seus vizinhos. O algoritmo de roteamento determinístico, executado em cada nó que participa do roteamento, é adaptado para considerar informação a respeito da vizinhança dos vizinhos do nó. A adaptação altera a função de distância para que ela escolha nós cujos vizinhos são mais próximos do nó de destino, possibilitando a escolha antecipada de rotas mais curtas e o ganho conseqüente em desempenho [29].

Considerando esta técnica, o fornecimento de conhecimento privilegiado a respeito da topologia também foi verificado experimentalmente, em busca de ganhos na métrica de entropia. Cada nó da rede recebe informação a respeito de um vizinho de cada um dos seus vizinhos imediatos na topologia. A seleção deste vizinho é realizada aleatoriamente. Assim, cada nó recebe d conexões privilegiadas adicionais, chamadas *conexões adiantadas*, que passam a participar da seleção de vizinhos do caminho aleatório. A motivação desta modificação é que, encaminhando uma mensagem para um vizinho de um vizinho na topologia *Koorde*, o roteamento insere dois novos dígitos à direita do identificador em um único passo, acelerando a taxa em que se atinge um identificador aleatório.

A nova topologia, que acumula as modificações de tolerância a falhas e adiantamento de conexões, é denominada *Koorde-ta*. Nesta topologia, cada nó estabelece 64 conexões – 32 para tolerância a falhas, 16 convencionais e 16 adiantadas – e, durante a seleção de vizinho para um caminho aleatório, são consideradas 33 possibilidades – uma para nós próximos ao sucessor, 16 para conexões convencionais e 16 para conexões adiantadas. A vantagem das conexões adiantadas é que elas não são utilizadas durante a segunda fase (fase determinística) do roteamento randomizado, pois a topologia *Koorde* não permite flexibilidade nas decisões de roteamento [23]. Logo, as conexões adiantadas não precisam ser atualizadas com freqüência e não trazem sobrecarga significativa de manutenção.

A Figura 20 apresenta os resultados experimentais da métrica de entropia para a topologia *Koorde-ta-16*. Comparando-se o gráfico com a Figura 19, pode-se observar um ganho de entropia em relação à topologia *Koorde-t-16*.

6.4 Canais múltiplos

A utilização de canais múltiplos de resposta foi sugerida na Seção 4.2.2 para descentralizar o ponto de entrada e obter confiabilidade. Entretanto, esta possibilidade não foi explorada na experimentação, que considerou apenas um único destino por simulação. A hipótese de que o estabelecimento de canais múltiplos colabora com a métrica de entropia foi então testada experimentalmente. Em cada evento de comunicação, o destino é selecionado aleatoriamente entre os pontos de entrada e o emissor tem múltiplas opções de destino para o envio de cada mensagem. O número de pontos de entrada foi fixado em d, para equivalência com a natureza da topologia. A nova topologia, com as modificações prévias acumuladas, é chamada *Koorde-tac*.

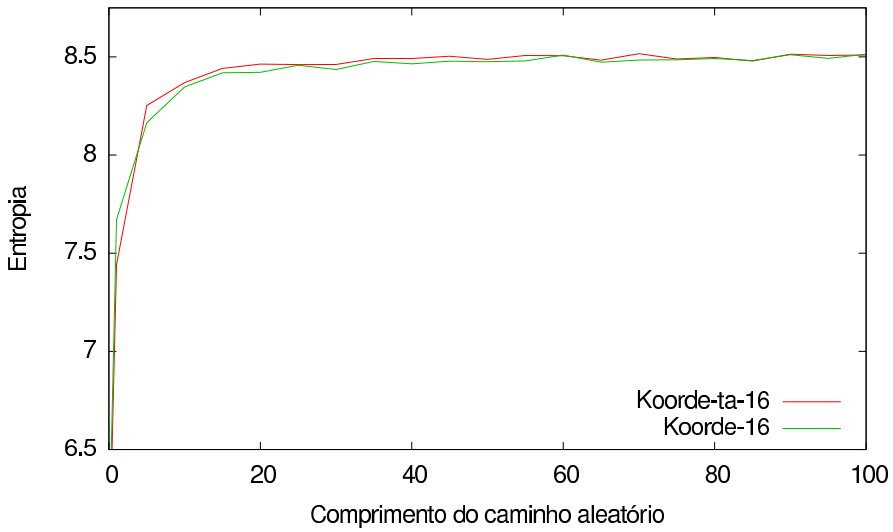


Figura 20: Resultados experimentais de entropia condicional da topologia *Koorde-ta-16*.

6.4.1 Nova simulação

O novo procedimento de simulação é composto pelas seguintes etapas:

1. Seleção de d nós não-controlados por adversário para servir como pontos de entrada para um nó a_d. Por simplificação, os canais de resposta são assumidos como íntegros e livres da presença de nós controlados pelo adversário. Esta simplificação não tem impacto na métrica de entropia, que, no caso, avalia estritamente a qualidade do anonimato de envio;

2. Execução de eventos de comunicação consecutivos que simulam a transmissão de k mensagens de cada um dos participantes $a_i \in \mathcal{A}$ para o nó a_d. Os nós controlados pelo adversário e o destino a_d não participam da simulação como emissores de mensagem. Cada uma das mensagens enviadas tem como destino real um dos pontos de entrada do nó a_d, selecionado aleatoriamente entre os d pontos de entrada disponíveis;

3. Gravação do predecessor observado para cada mensagem interceptada por nó malicioso. Os nós controlados pelo adversário descartam as mensagens capturadas imediatamente após a gravação da observação correspondente; e

4. Cálculo da métrica de entropia condicional do sistema, considerando-se as observações do adversário.

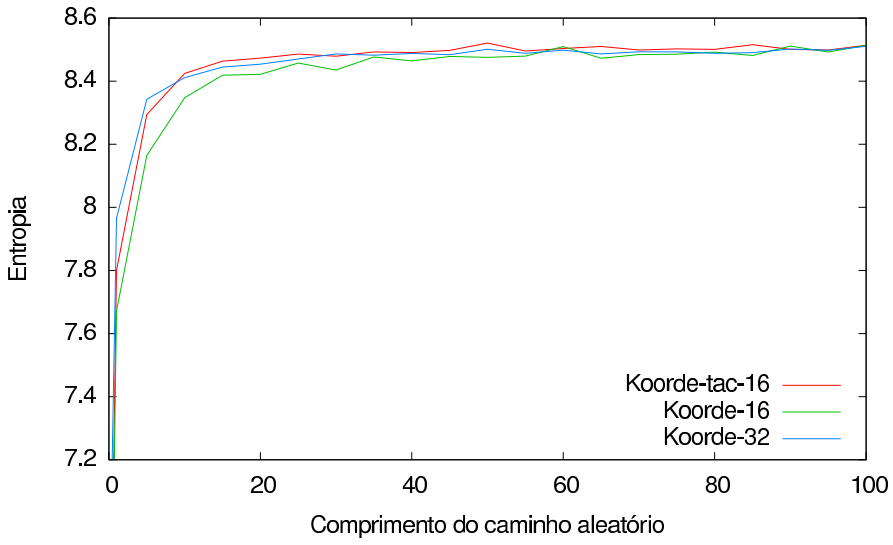


Figura 21: Resultados experimentais de entropia condicional da topologia *Koorde-tac-16*.

6.4.2 Novos resultados

A medida de entropia para a variante *Koorde-tac* é apresentada na Figura 21. Pode-se observar um ganho mais consistente de entropia da topologia *Koorde-tac-16* em relação à topologia original *Koorde-16*, com a descentralização do ponto de entrada. A topologia *Koorde-tac-16* também supera em entropia a topologia *Koorde-32* para caminhos aleatórios de comprimento superior a 10. O comprimento 10 é justamente o comprimento esperado dos caminhos aleatórios para a probabilidade de encaminhamento adotada $p_f = 0,9$. O projeto da topologia *Koorde-tac-16* mostra que a escolha cuidadosa dos recursos e da política de roteamento permite a construção de topologias com propriedades úteis e compromisso ótimo entre qualidade de anonimato e desempenho.

A análise detalhada do gráfico indica ainda que a topologia *Koorde-tac-16*, para caminhos aleatórios de comprimento 10, fornece a mesma entropia da topologia *Koorde-16* para caminhos aleatórios de comprimento 20. Ou seja, a entropia *Koorde-tac-16* apresenta uma relação entre desempenho e qualidade de anonimato duas vezes melhor que a topologia original, para caminhos aleatórios de comprimento esperado 10. Considerando apenas os caminhos aleatórios de comprimento 10, temos um conjunto efetivo de anonimato de tamanho $2^{8.34} \approx 325$ para a topologia *Koorde-16* e um conjunto efetivo de anonimato de tamanho $2^{8.42} \approx 344$ para a topologia *Koorde-tac*. Como a entropia é uma grandeza logarítmica, um ganho de quase 1% na entropia condicional provocou um aumento de 6% no tamanho do conjunto efetivo de anonimato. Espera-se que estes ganhos sejam bastante amplificados em redes mais populosas.

7 Conclusões

Neste trabalho, foi apresentada uma política de roteamento eficiente para comunicação anônima em sistema estruturados. Esta nova política fornece anonimatos de envio, resposta e de par comunicante. O anonimato de envio é resultante da utilização de roteamento randomizado, o anonimato de resposta é obtido a partir de canais de resposta independentes e o anonimato de par comunicante é proveniente de dupla cifração.

Por meio de verificação empírica, a topologia *Koorde* de grau 16 foi selecionada. Aprimoramentos significativos foram propostos e inseridos na topologia original, incluindo tolerância a falhas, conexões adiantadas e pontos de entrada múltiplos. Estes aprimoramentos permitiram a produção da topologia *Koorde-tac-16*, tolerante a falhas e favorável na métrica de entropia, o que indica ganho na qualidade de anonimato em relação à topologia *Koorde* original.

Referências

[1] A. Pfitzmann and M. Hansen. Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology. Draft, version 0.28, 2006.

[2] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[3] C. E. Shannon. Communication theory of secrecy systems. *Bell Systems Technology Journal*, 28:657–715, 1949.

[4] C. Diaz, S. Seys, J. Claessens, and B. Preneel. Towards measuring anonymity. In Roger Dingledine and Paul Syverson, editors, *Proceedings of Privacy Enhancing Technologies Workshop (PET '02)*, 2002.

[5] J. Kong. Formal notions of anonymity for peer-to-peer networks. Cryptology ePrint Archive, Report 2005/132, 2005.

[6] A. Serjantov and G. Danezis. Towards an information theoretic metric for anonymity. In Roger Dingledine and Paul Syverson, editors, *Proceedings of Privacy Enhancing Technologies Workshop (PET '02)*. Springer-Verlag, LNCS 2482, 2002.

[7] M. Reiter and A. Rubin. Crowds: anonymity for Web transactions. *ACM Transactions on Information Systems Security*, 1, 1998.

[8] S. Androutsellis-Theotokis and D. Spinellis. A survey of peer-to-peer content distribution technologies. *ACM Comput. Surv.*, 36(4):335–371, 2004.

[9] R. Dingledine, N. Mathewson, and P. F. Syverson. Tor: the second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, 2004.

[10] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong. Freenet: a distributed anonymous information storage and retrieval system. In *Proceedings of Designing Privacy*

Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, pages 46–66, July 2000.

[11] I. Stoica, R. Morris, D. Karger, F. Kaashoek, and H. Balakrishnan. Chord: A scalable peer-to-peer lookup service for Internet applications. In *Proceedings of the 2001 ACM SIGCOMM Conference*, pages 149–160, 2001.

[12] A. Rowstron and P. Druschel. Pastry: scalable, decentralized object location, and routing for large-scale peer-to-peer systems. *Lecture Notes in Computer Science*, 2218, 2001.

[13] B. Y. Zhao, J. D. Kubiatowicz, and A. D. Joseph. Tapestry: an infrastructure for fault-tolerant wide-area location and routing. Technical Report UCB/CSD-01-1141, UC Berkeley, April 2001.

[14] A. Mislove, G. Oberoi, A. Post, C. Reis, and P. Druschel. AP3: cooperative, decentralized anonymous communication. In *Proceedings of the 11th ACM SIGOPS European Workshop*, 2004.

[15] N. Borisov. *Anonymous routing in structured peer-to-peer overlays*. PhD thesis, University of California, Berkeley, 2005.

[16] M. Castro, P. Druschel, A. Kermarrec, and A. Rowstron. SCRIBE: A large-scale and decentralized application-level multicast infrastructure. *IEEE Journal on Selected Areas in communications (JSAC)*, 20(8):1489–1499, 2002.

[17] K. Bennett and C. Grothoff. GAP – practical anonymous networking. In Roger Dingledine, editor, *Proceedings of Privacy Enhancing Technologies workshop - PET '03*, 2003.

[18] B. Lipinski and P. MacAlpine. A security review of an anonymous peer-to-peer file transfer protocol. `http://www.lix.polytechnique.fr/~tomc/P2P/Papers/Systems/AP3.pdf`.

[19] K. Gummadi, R. Gummadi, S. Gribble, S. Ratnasamy, S. Shenker, and I. Stoica. The impact of DHT routing geometry on resilience and proximity. In *SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 381–394, New York, NY, USA, 2003. ACM Press.

[20] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D. S. Wallach. Secure routing for structured peer-to-peer overlay networks. In *Proceedings of the 5th USENIX Symposium on Operating Systems Design and Implementation - OSDI '02*, 2002.

[21] J. Aspnes and G. Shah. Skip graphs. In *SODA '03: Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 384–393, Philadelphia, PA, USA, 2003. Society for Industrial and Applied Mathematics.

[22] N. J. A. Harvey, M. B. Jones, S. Saroiu, M. Theimer, and A. Wolman. SkipNet: a scalable overlay network with practical locality properties. In *USENIX Symposium on Internet Technologies and Systems*, 2003.

[23] M. F. Kaashoek and D. R. Karger. Koorde: A simple degree-optimal distributed hash table. In *Proceedings of the 2nd International Workshop on Peer-to-Peer Systems (IPTPS '03)*, 2003.

[24] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker. A scalable content-addressable network. In *SIGCOMM '01: Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*, volume 31, pages 161–172. ACM Press, October 2001.

[25] D. Malkhi, M. Naor, and D. Ratajczak. Viceroy: A scalable and dynamic emulation of the butterfly. In *Proceedings of the 21st ACM Symposium on Principles of Distributed Computing*, 2002.

[26] N. G. de Bruijn. A combinatorial problem. *Nederl. Akad. Wetensch. Proc.*, 49:758–764, 1946.

[27] M. Wright, M. Adler, B. N. Levine, and C. Shields. The predecessor attack: an analysis of a threat to anonymous communication systems. *ACM Transactions on Information Systems Security*, 7:489–522, 2004.

[28] L. Paninski. Estimation of entropy and mutual information. *Neural Comput.*, 15(6):1191–1253, 2003.

[29] M. Naor and U. Wieder. Know thy neighbor's neighbor: better routing for SkipGraphs and small worlds. In *IPTPS*, volume 3279, pages 269–277. Springer, 2004.