Um serviço para prover autenticação e revogação de nós na rede DHT

Jean T. Garcia, Lucas Vargas Dias e Tiago Antonio Rizzetti

Universidade Federal de Santa Maria
Curso Superior de Tecnologia em Redes de Computadores

{*jeangarcia,lucas_dias*}*@redes.ufsm.br*, *rizzetti@ctism.ufsm.br*

19 de Setembro de 2019

ESTRUTURA DO TRABALHO

Em uma rede baseada em *distributed hash table* (DHT), cada nó armazena uma tabela de *hash* na qual contém um par de chave e valor que qualquer nó pode recuperar ou alocar. Isso torna a rede DHT vulnerável.

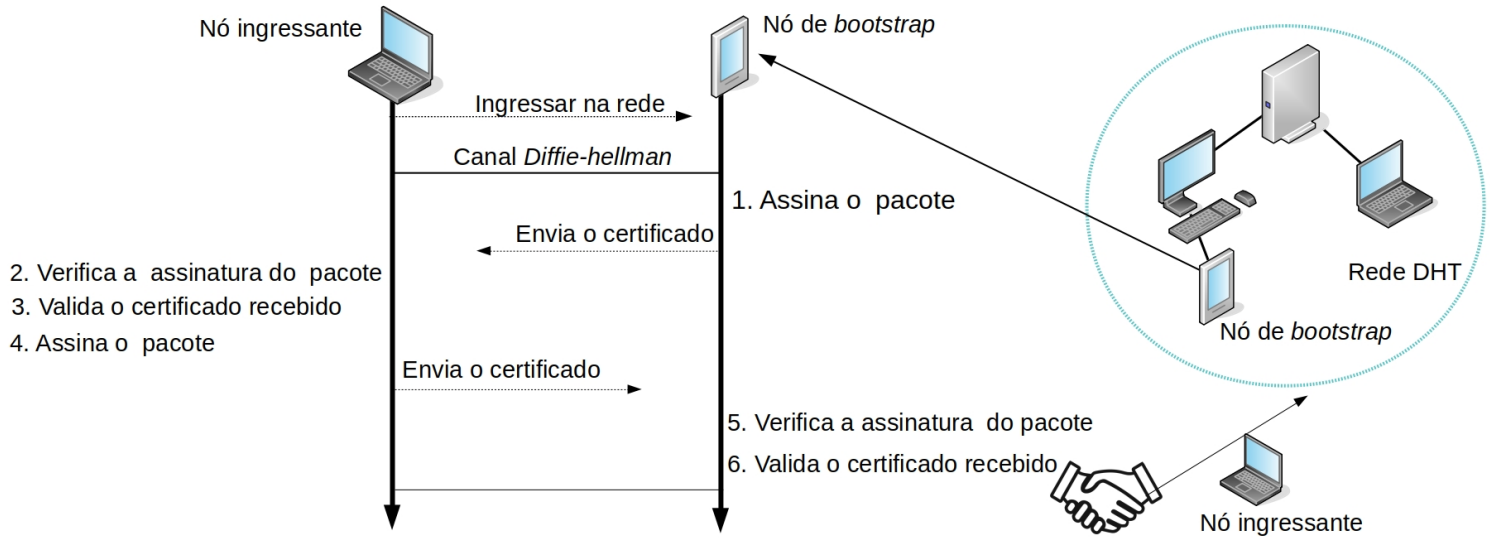
Neste sentido, o trabalho concentra-se em propor e implementar um serviço reativo que fornece autenticação e revogação de nós através de uma infraestrutura de chave pública (ICP).

[Pecori 2015] apresenta um mecanismo de confiança aplicado ao protocolo Kademlia. O mecanismo baseia-se em uma pontuação de confiança em cada operação de obtenção ou alocação de dados na rede DHT.

Já o trabalho de [Kohnen et al. 2011] utiliza autenticação baseado em certificados digitais junto ao protocolo Kademlia. O trabalho assume que cada nó possui um certificado autenticado por uma autoridade certificadora e que cada nó confia nos demais que também possuam.

O serviço proposto é composto por duas partes, a autenticação e a revogação dos nós. Em primeiro lugar a lista de revogação de certificados é periodicamente publicada na rede DHT pela autoridade certificadora.

Para ingressar na rede, um nó deve contatar outro já inserido, chamado de nó de *bootstrap*. Cada nó já ingressa com um certificado válido emitido pela CA, o processo pode ser visto abaixo.



No que se refere ao serviço de revogação de nós, cada nó na rede DHT terá um identificador, sendo este uma *infohash* do número de série do certificado. Um exemplo de comunicação pode ser visualizado na figura abaixo.

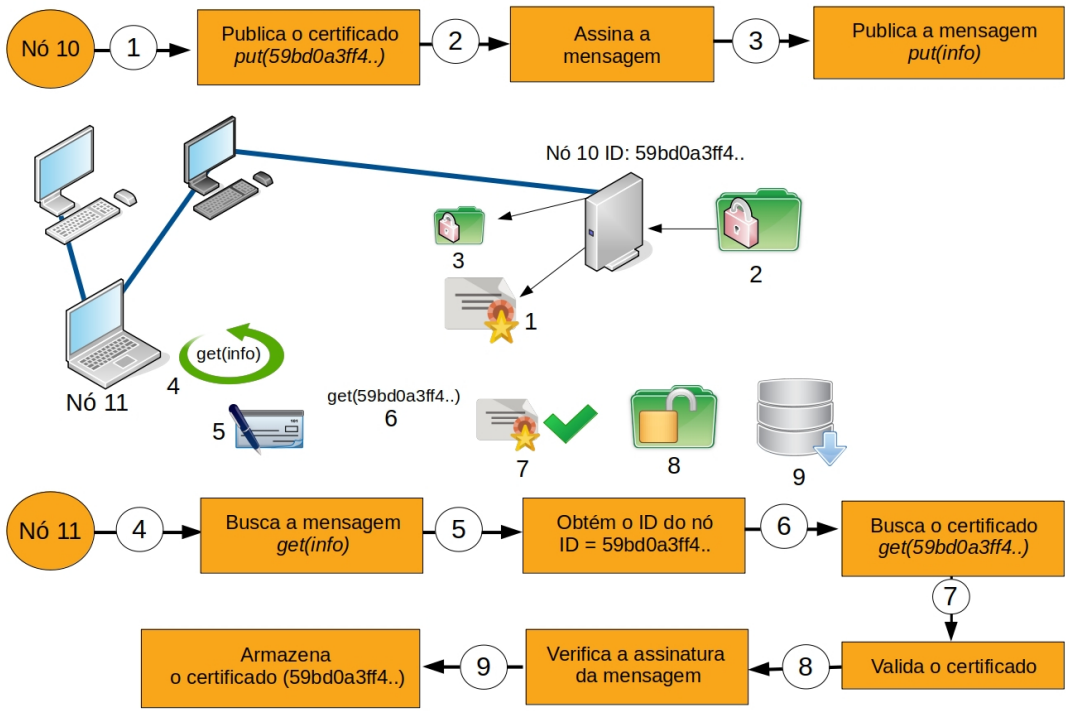


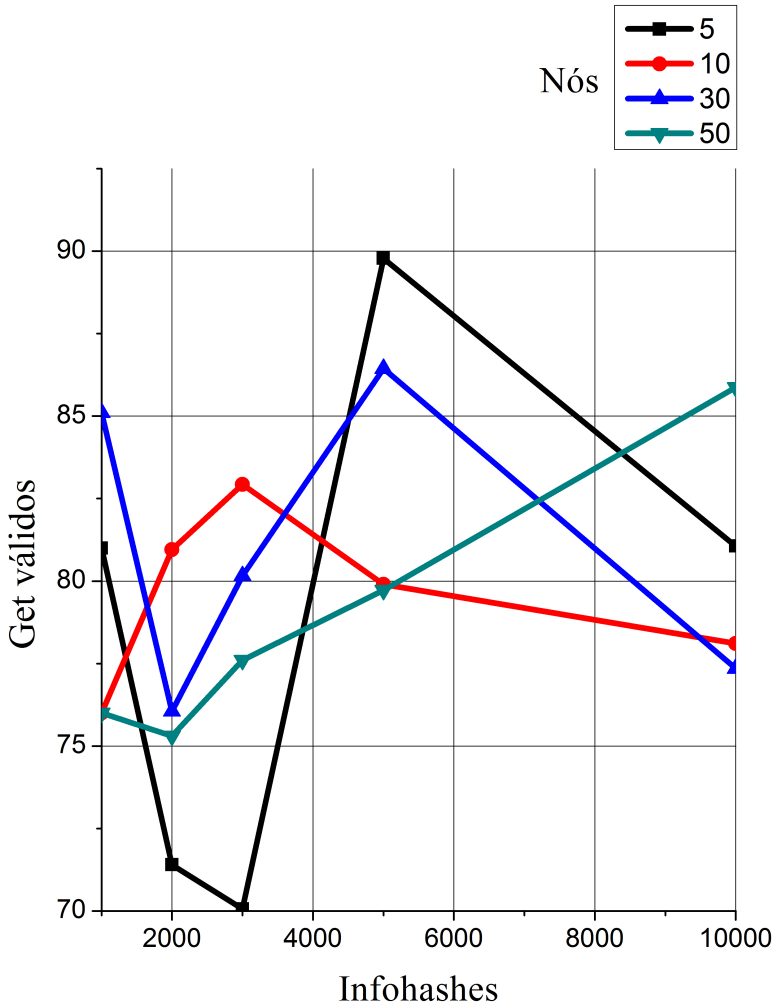
Figura: Funcionamento do serviço proposto

O cenário de testes com 50 nós foi criado na ferramenta de simulação de redes. CoreEmulator. Para implementação do serviço, utilizou-se da linguagem de programação C++ com a biblioteca OpenDHT. O equipamento utilizado possui as seguintes características:

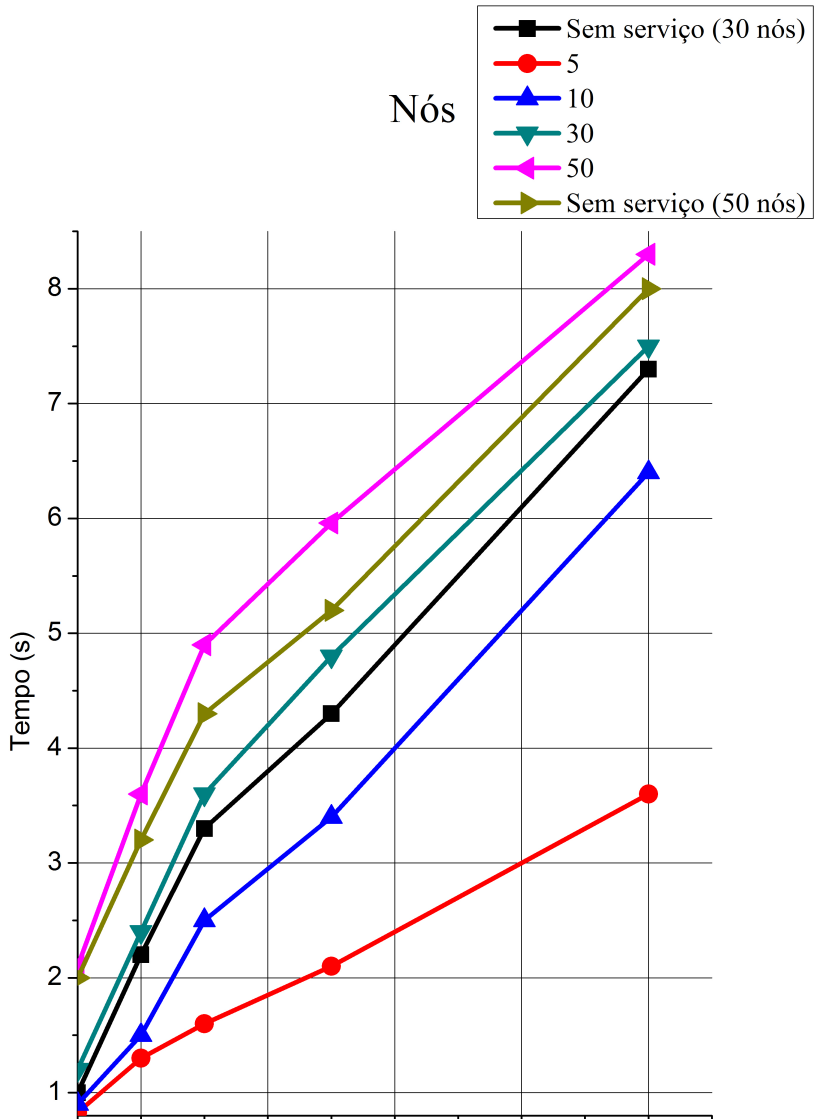
- Processador Intel Core i3;
- Memória RAM de 8 GigaBytes;
- Sistema Operacional Linux Mint 19.1 64 bits

Os testes foram executados em cinco rodas cada configuração.
As *Infohash*s publicas pelos nós foram geradas pseudo-aleatoriamer
dentro do espaço total de 50 nós.

Com 20% dos nós não autênticos no cenário, a taxa de sucesso de *get* com 50 nós e 5000 *Infohashs* foi de 79,4%. Uma visão geral pode ser vista na figura abaixo.



A figura abaixo demonstra que o serviço não degradou de forma significativa o desempenho da rede DHT.



No trabalho de Pecori 2015], o resultado de operações de *get* bem sucedidas é de cerca de 80%, com nenhum nó falso na rede. Já na proposta de [Kohnen et al. 2011] o resultado de busca considerando cerca de 40% dos nós maliciosos a taxe de sucesso de *get* é quase 70%.

O respectivo trabalho não impacta de maneira significativa o desempenho da rede DHT, além de verificar a autenticação do nó em tempo de comunicação na rede, isso faz com que a partir do momento de revogação de um nó, as *Infohash*s alocadas pelo mesmo serão desconsideradas.

Tendo como exemplo a rede do *Mainline* que utiliza das vantagens da rede DHT baseadas no Kademlia implementada na Internet com milhões de usuários ativos. A segurança da informação especialmente no pilar de autenticação, tem sido um grande desafio. Sendo assim,o trabalho apresentou um serviço para prover autenticação e revogação de nós em uma rede DHT no qual não tem tanto impacto sobre a rede.

- Pecori, R. (2015, July). Trust-based storage in a Kademlia network infected by Sybils. In 2015 7th International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-5). IEEE.
- Kohnen, M., Gerbecks, J., Rathgeb, E. P. (2011). Applying certificate-based routing to a kademlia-based distributed hash table. In Proceedings of the Third international Conference on Advances in P2P Systems.

DÚVIDAS?