Uma arquitetura para prover autenticidade em comunicações *Multicast*

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

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

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

19 de Setembro de 2019

ESTRUTURA DO TRABALHO

Comunicações *multicast* por definição permitem que um único emissor envie uma mensagem a diversos destinatários de maneira a reduzir tráfego de rede, largura de banda e o processamento. Entretanto, qualquer dispositivo que descubra o endereço *Internet Protocol* (IP) do grupo pode participar do mesmo, bem como enviar mensagens.

As comunicações *multicast* tem como requisito que apenas participantes possam ler e enviar mensagens relacionadas ao grupo. Dessa forma, é importante garantir que os nós participantes e as mensagens sejam autênticas.

Arquiteturas de gerenciamento de chaves:

- Protocolos de gerenciamento de chaves centralizado;
- Arquiteturas descentralizadas;
- Protocolos de gerenciamento de chaves distribuídos.

Para ingressar na rede DHT, um nó verifica uma lista que contém os nós de *bootstrap* possíveis, escolhe um, realizam um canal de comunicação *Diffie-Hellmann*. Em sequência trocam-se os certificados digitais e verificam-se os mesmos.

O nó de *bootstrap* ao autenticar um dispositivo para ingressar na rede, salva a chave pública do mesmo e o identificador em uma estrutura de dados. Então, o mesmo gera uma nova chave de sessão, encripta com cada uma das chaves públicas dos nós, concatena ao identificador de cada e publica na rede DHT. Então os nós recebem essa estrutura, buscam pelo seu identificador e decifram a chave de sessão. O mesmo processo ocorre quando um dispositivo tem o certificado revogado.

Arquitetura Proposta - Autenticação de Pacotes IP

Com posse da chave de sessão, ao comunicar-se com o endereço *multicast*, ocorre o processo mostrado na figura abaixo.

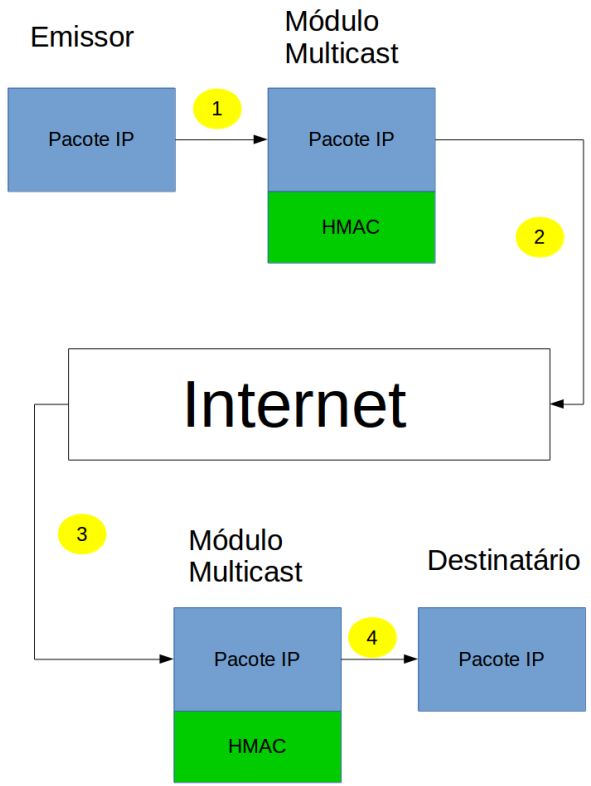

Figura: Processo de autenticação de pacotes IP *multicast*

Para colocar a arquitetura em funcionamento, foi utilizado o utilitário de emulação de rede Common Open Research Emulator (CORE). Foi montado um ambiente com 30 dispositivos. O primeiro teste foi sobre o tempo de convergência de chave de sessão, foi realizado o tempo médio de três rodas com 10, 15, 20, 25 e 30 nós com resultado apresentado na figura abaixo.

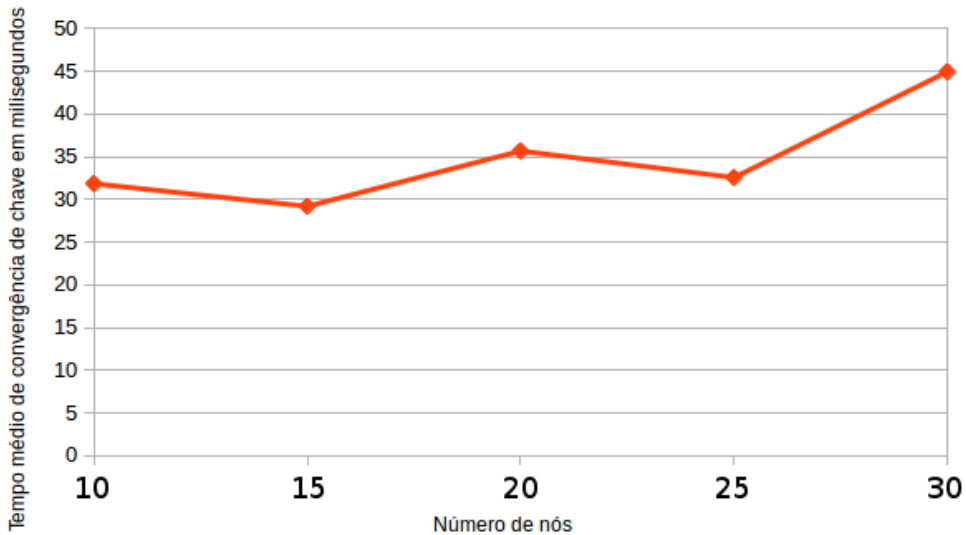

Figura: Resultado do tempo de sincronismo com diferentes quantidades de nós

O segundo teste realizado foi a comparação entre o tempo de montagem de pacotes autenticados e pacotes comprometidos, também foi realizado três rodadas de testes e feito a média entre os resultados, sendo esse mostrado na figura abaixo.

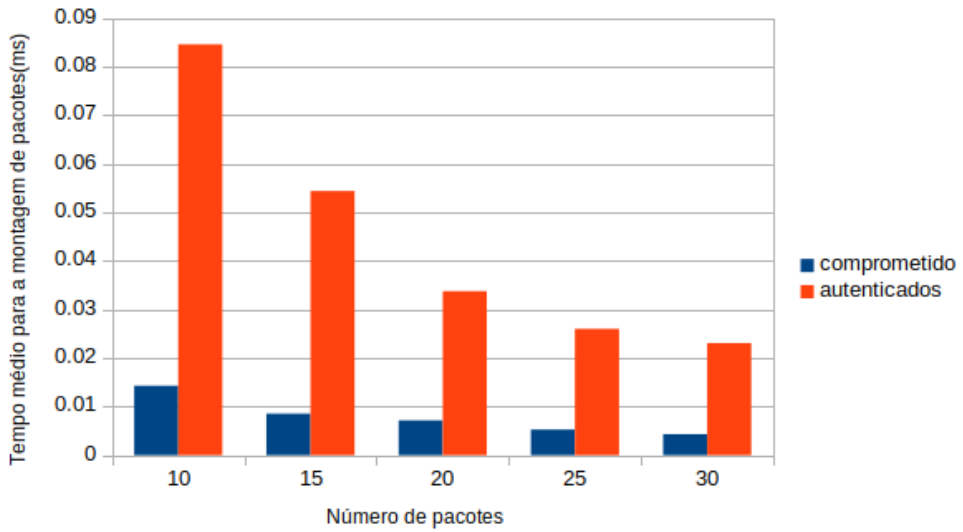

Figura: Resultado do tempo médio d montagem de pacotes

Os resultados mostram que a arquitetura tem um tempo de convergência de chaves baixo. Isso se dá pelo fato da característica da rede DHT. Cada nó que tiver posse de uma informação, passa a fornecer a mesma na rede.

DÚVIDAS?