# QKD Simulador

O simulador de distribuição de chaves quânticas é um simulador (QKDNetSim) é um modulo de simulação projetado para expandir o simulador de rede NS-3 com as funcionalidades de rede de QKD criem modelos detalhados de protocolos de rede, dispositivos de rede e topologias de rede. O principal objetivo do simulador de rede é a análise de diferentes abordagens para as organizações de redes QKD, a simulação de tecnologias de rede considerando a integração de sistemas QKD nas redes de comunicações existentes, com referência à segurança da rede.

**Comentado [DT1]:** O que é NS-3?
NS-3 significa Network Simulator 3, é um ambiente de simulação de código aberto usado para modelar e simular redes de computadores. O NS-3 é altamente configurável e permite que os usuários criem modelos detalhados de protocolos de rede, dispositivos de rede e topologias de rede.

1° passo do simulador
Escolher os pontos de conexão, após escolher dois abrirá uma caixa para modificar os parâmetros da conexão de configuração do sistema QKD para gerar chaves secretas usadas, sendo eles:
distance (meter) - a distância em metros

Key rate (bps) - a quantidade média de chaves secretas (bits) em um período de tempo (segundos). Que estará marcada como automática, mas é possível personalizar

key Size (bit) - o tamanho das chaves criptografas que serão geradas

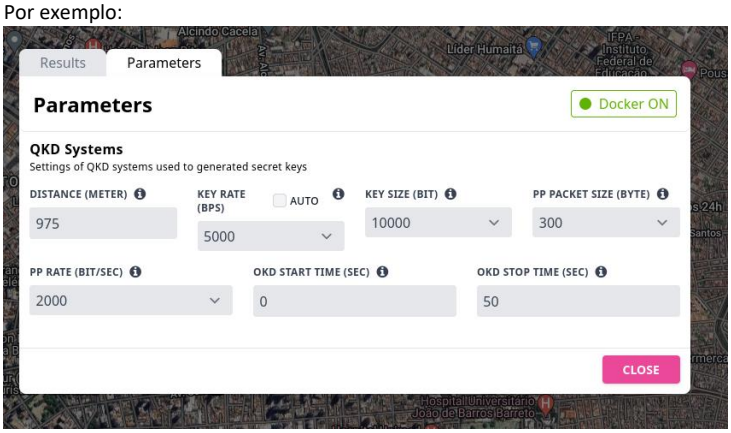
pp Packet Size (byte) - o tamanho dos pacotes de tráfego trocados no pós-processamento do QKD.

pp Rate (bit/sec) - a quantidade de tráfego que irá ter no pós processamento do QKD

OKD Start Time (sec) - o tempo quando o sistema QKD começa a gerar as chaves

OKD Stop Time (sec) - o tempo quando o sistema irá parar de gerar as chaves

2° passo
A cada parâmetro mudado se tem um resultado
Por exemplo:

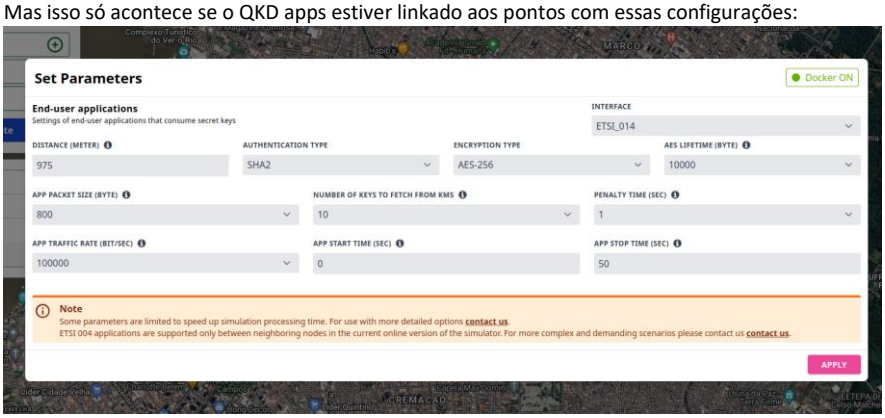



Usando esses parâmetros usando como base a distância entre o museu Emilio Goeldi até a escola de música da UEPA que estão a 975 metros um do outro. Usando poucas chaves geradas por segundo (5000) o que não é normal dada a distância, o tamanho da chave criptográfica sendo 10000 e a quantidade de tráfego trocada sendo 300 e quantidade de tráfego no pós processamento sendo 2000

Temos o resultado de:


Quanto mais bits de pares de chaves geradas mais segura é a conexão nesse modo foram geradas 240,000 chaves, sendo consumidas 34,000 dessas chaves, o que sugere que a conexão ficou estável e bem protegida, todas essas chaves foram geradas em um intervalo de 50 segundos

Mas isso só acontece se o QKD apps estiver linkado aos pontos com essas configurações:



No QKD APP, temos que linkar entre dois pontos bem parecido com apenas o link do simulador, contendo as modificações:

Interface – tem dois tipos de interface sendo a ETSI_014 e a ETSI_004

Na interface ETSI_014 tem todas essas opções:

distance (meter) - Distância em metros

authentication type – o tipo de autenticação que são apenas 3, (não autenticada, vmac e sha2)

encryption Type – tem três tipos de autenticação também, sendo elas (não encriptada, One-time pad e AES-256)

app Packet Size (byte) - o tamanho dos pacotes da apliação

number Of Keys To Fetch from kms – quantidade de chaves criptográficas que um sistema solicita ao Serviço de Gerenciamento de Chaves (KMS) em uma única operação.

Penalty time (sec) - Quanto tempo esperar antes de enviar uma nova solicitação GET_KEY para o Serviço de gerenciamento de chaves (KMS) após receber uma resposta de que não há chaves suficientes disponíveis

app Traffic Rate (bit/sec) - a quantidade de tráfego que o aplicativo consome de chaves

APP Start Time (sec) - o tempo de gerar as chaves

APP Stop Time (sec) - o tempo de parar

Na interface ETSI_004 o number Of Keys To Fetch from kms é substituida pelo encryption buffer capacity (key) (Quantas chaves devem ser armazenadas em um buffer local de QKDApp004 para criptografia) e o penalty time é substituido pela authentication buffer capacity (key) ((Quantas chaves devem ser armazenadas em um buffer local de QKDApp004 para autenticação)