Análise dos impactos de um ataque de negação de serviço em funções do núcleo da rede 5G

Mateus O. Nascimento[1], **José A. A. Gomes**[1], **João H. Corrêa**[1]

[1]Universidade Federal do Ceará (UFC) – Campus de Itapajé

{mateusnas, joseagaci}@alu.ufc.br, joaocorrea@ufc.br

Abstract. *Denial-of-Service (DoS) attacks are constant and growing threats in computer networks, as their objective is to cause service unavailability. In the context of 5G networks, this type of attack can cause even more issues for users, especially if the targets are the virtualized network functions of the 5G core. Thus, this work proposes an analysis of the impacts of a Denial-of-Service attack on 5G core network functions. Using a scenario built on the Fabric testbed and the free5GC platform, experiments were conducted with real traffic through the 5GAD-2022 dataset. The results show an increase in the registration time of network functions, as well as an increase in CPU consumption. Finally, Quality of Service (QoS) metrics were degraded due to DoS attacks.*

Resumo. *Ataques de negação de serviço (DoS) são ameaças constantes e crescentes em redes de computadores, pois têm como objetivo gerar a indisponibilidade a serviços. No contexto das redes 5G, esse tipo de ataque podem gerar mais problemas para os usuários, principalmente se os alvos desses ataques forem as funções de redes virtualizadas do núcleo da rede 5G. Dessa forma, este trabalho propõe uma análise dos impactos de um ataque de negação de serviço contra as funções do core da rede 5G. Com cenário construído com o testbed Fabric, utilizando a plataforma free5GC, experimentos foram realizados com tráfego real, por meio do dataset 5GAD-2022. Resultados apresentam um aumento no tempo de registro das funções da rede, além de aumento no consumo de CPU. Por fim, métricas de qualidade de serviço (QoS) foram deterioradas devido aos ataques de DoS.*

1. Introdução

A evolução das redes móveis tem sido marcada por avanços significativos ao longo das décadas. Desde a primeira geração (1G), que introduziu a comunicação móvel analógica limitada a serviços de voz, até a quarta geração (4G/LTE), que representou um salto nas taxas de transferência de dados — alcançando até 100 Mbps e viabilizando aplicações como streaming de vídeo e jogos online — cada nova geração trouxe não apenas incrementos de velocidade, mas mudanças estruturais na forma como a sociedade se conecta [Ojope 2024]. A migração do sistema analógico para o digital na segunda geração (2G) permitiu o surgimento do serviço de mensagens curtas (SMS) e maior capacidade de rede, enquanto a terceira geração (3G) tornou possível o acesso à internet móvel, com serviços como videochamadas, navegação na web e transmissão de música [Ojope 2024].

A quinta geração (5G) não é apenas um incremento em velocidade, mas uma mudança estrutural na forma como as redes móveis são concebidas. Diferentemente

das gerações anteriores, o 5G foi projetado com uma arquitetura flexível, baseada em funções de rede especializadas que podem ser implementadas de forma independente [Liao 2023]. O núcleo da rede 5G (5GC - *5G Core*) é composto por funções como a *Access and Mobility Management Function* (AMF), responsável pelo registro e mobilidade dos usuários; a *Session Management Function* (SMF), que gerencia as sessões de dados; e a *User Plane Function* (UPF), responsável pelo encaminhamento dos pacotes [Håkegård et al. 2024]. Essa arquitetura baseada em serviços (SBA - *Service-Based Architecture*) permite maior flexibilidade e escalabilidade, mas também introduz novos vetores de ataque [Lando et al. 2023].

Paralelamente à evolução das redes, o cenário de ameaças cibernéticas também tem se intensificado. Ataques de negação de serviço — *Denial-of-Service* (DoS) e sua forma distribuída (DDoS) — têm como objetivo causar indisponibilidade em sistemas ou serviços por meio da sobrecarga de recursos computacionais, ou de rede. Relatórios recentes indicam um crescimento significativo tanto na frequência quanto na magnitude desses ataques. Em maio de 2025, a Cloudflare reportou a mitigação do maior ataque DDoS já registrado, atingindo um pico de 7,3 terabits por segundo (Tbps), superando recordes anteriores e evidenciando a rápida evolução da capacidade ofensiva desses ataques [1]. Esse cenário reforça a necessidade de estudos voltados à análise da resiliência de infraestruturas críticas, como as redes móveis de quinta geração.

No contexto das redes 5G, a problemática se torna ainda mais complexa devido à interdependência entre as funções de rede. Farooqui *et al.* apresenta a problemática de um ataque de DoS direcionado a funções específicas do núcleo da rede podem ter impactos variados [Farooqui et al. 2022]. Por outro lado, na literatura, normalmente verifica-se que a ocorrência de um ataque de negação de serviço tem como alvo clientes e serviços que utilizam uma rede 5G. As funções da rede 5G não são objetos de análise dos impactos que um ataque de DoS gerados contra essas funções [Shehab et al. 2025].

Dessa forma, o presente trabalho se norteia pela seguinte questão de pesquisa: Quais os impactos, na própria função de rede ou em clientes que a utilizam, ocasionados quando uma função de rede virtual (NFV - *Network Function Virtualization*) do núcleo da rede 5G recebe um ataque de negação de serviço? Assim, este trabalho apresenta uma análise desses impactos, de forma experimental, utilizando um cenário controlado em que as funções de redes recebem os ataques de DoS.

Em resumo, este trabalho apresenta as seguintes contribuições:

- A análise dos impactos causados por ataque de DoS contra funções de rede do núcleo da rede 5G, verificando métricas de recursos computacionais;
- A análise das métricas de Qualidade de Serviço (QoS - *Quality-of-Service*) de clientes legítimos que utilizam a rede 5G, enquanto as funções de redes recebem um ataque de negação de serviço;
- A verificação da análise realizada em um ambiente real, com tráfego de ataque oriundo de *dataset* real.

O artigo está estruturado da seguinte maneira: na Seção 2 será discutido os trabalhos relacionados. Na Seção 3 será abordado os materiais e métodos deste trabalho, bem

[1]Disponível em: https://blog.cloudflare.com/pt-br/defending-the-internet-how-cloudflare-blocked-a-monumental-7-3-tbps-ddos/ acesso em: 26 mar. 2026.

como a criação do cenário de experimentos. Na Seção 4 são apresentados os resultados obtidos nos testes e por fim, na Seção 5, o trabalho é concluído, apresentando também as indicações de trabalhos futuros.

2. Trabalhos Relacionados

Diversos estudos recentes têm investigado aspectos relacionados à implementação, desempenho e gerenciamento de redes 5G, especialmente no contexto de soluções de código aberto utilizadas em ambientes acadêmicos e experimentais. Esses trabalhos contribuem para o entendimento do comportamento do núcleo 5G (5GC) e das tecnologias associadas, embora poucos abordem explicitamente aspectos relacionados à segurança e à resiliência da arquitetura frente a ataques.

Lando *et al.* realizou uma avaliação comparativa de diferentes implementações de núcleo 5G de código aberto, incluindo free5GC, Open5GS e OpenAirInterface. O estudo analisou métricas de desempenho como tempo de registro de usuários, latência e capacidade de throughput, buscando identificar diferenças de eficiência entre as plataformas. Os resultados indicaram que as implementações apresentam comportamentos distintos dependendo da configuração do ambiente e da carga de usuários simulados, evidenciando a importância de avaliações experimentais para compreender o funcionamento dessas soluções [Lando et al. 2023].

No contexto de implantação prática de ambientes experimentais, Medeiros *et al.* apresentaram um guia para implementação de uma infraestrutura 5G utilizando o núcleo Open5GS em conjunto com o simulador de rede de acesso UERANSIM. O trabalho descreve os procedimentos necessários para configuração do ambiente, incluindo integração entre os componentes da rede e testes de conectividade. Essa abordagem facilita a reprodução de cenários experimentais e tem sido amplamente utilizada em pesquisas que envolvem experimentação em redes 5G [Medeiros et al. 2024].

Mercres et al. (2025) investigaram o desempenho do Open5GS quando integrado a uma rede de acesso comercial, analisando como diferentes configurações de hardware influenciam o comportamento do núcleo da rede. O estudo demonstrou que fatores como capacidade de processamento, memória disponível e configuração de virtualização podem impactar diretamente métricas de desempenho, como latência e taxa de transferência de dados. Esses resultados reforçam a relevância de considerar aspectos de infraestrutura ao avaliar sistemas baseados em arquiteturas 5G [das Mercres et al. 2025].

Em uma perspectiva mais voltada à arquitetura e aos mecanismos de gerenciamento da rede, Liao (2023) explorou aspectos relacionados à qualidade de serviço (QoS) e ao uso de *network slicing* em redes 5G. O estudo discute como a arquitetura baseada em serviços do núcleo 5G permite a criação de fatias de rede com características específicas de desempenho e prioridade, possibilitando atender diferentes tipos de aplicações e requisitos de serviço [Liao 2023].

Apesar das contribuições desses trabalhos para o entendimento da arquitetura e do desempenho de implementações 5G, observa-se que a maioria das pesquisas concentra-se em aspectos de implantação, desempenho ou gerenciamento da rede. *Surveys* recentes ([Ji and Kumar Mishra 2024, Singh et al. 2024, Shehab et al. 2025]) apresentam diversos mecanismos na literatura, que visam realizar a detecção e/ou mitigação dos ataques de

negação de serviço em redes 5G. No entanto, são poucos que tem como alvo desses ataques as funções de redes do núcleo 5G.

Nesse contexto, o presente trabalho busca contribuir para essa área ao realizar uma avaliação experimental para analisar os impactos de ataques DoS direcionados às funções do *core* 5G.

3. Materiais e Métodos

Um núcleo da rede 5G é composto por diversas funções de rede virtualizadas (NFV - *Network Function Virtualization*), responsáveis pelo funcionamento da rede. Essas funções são organizadas em uma arquitetura baseada em serviços, na qual cada entidade desempenha papéis específicos nos planos de controle e de dados.

Nesse contexto, a AMF (*Access and Mobility Management Function*) é responsável pelo gerenciamento de acesso e mobilidade dos usuários, enquanto a SMF (*Session Management Function*) realiza o gerenciamento das sessões de dados. A UPF (*User Plane Function*) atua no plano de dados, sendo encarregada do encaminhamento de pacotes. A AUSF (*Authentication Server Function*) e a UDM (*Unified Data Management*) são responsáveis pela autenticação e pelo gerenciamento das informações dos clientes, enquanto a PCF (*Policy Control Function*) define políticas de rede, incluindo regras de qualidade de serviço.

Além disso, a NRF (*Network Repository Function*) possibilita a descoberta e a comunicação entre as funções da rede, enquanto a NSSF (*Network Slice Selection Function*) realiza a seleção de *network slices* apropriados para cada usuário ou serviço. Por fim, a UDR (*Unified Data Repository*) atua como repositório central de dados, armazenando informações utilizadas por diversas funções do núcleo, conforme especificado na arquitetura do sistema 5G [3GPP 2020].

Assim, para verificar o impacto de um ataque de negação de serviço na utilização de uma rede 5G, bem como o impacto nas funções específicas no núcleo 5G, foi criado o cenário de experimento, apresentado na Figura 1.

Nos experimentos, foi utilizado o *testbed* Fabric [FABRIC Testbed 2026], criando quatro máquinas virtuais (VM - *Virtual Machine*), cada uma com 4 núcleos de CPU, 16 GB de memória e sistema operacional Ubuntu 22.04[2]. A primeira VM foi instanciado um ambiente Kubernetes[3], na sua versão 1.35, em seguida, foi instalado o *core* da rede 5G com o free5GC[4]. Para coletar as métricas de telemetria do*core* da rede 5G, foi utilizado o Prometheus[5], em conjunto com o Kubernetes-metrics[6], resgatando valores de uso de CPU, Memória, disco e rede.

[2]Para evitar interferência na latência provocada pela distribuição geográfica do Fabric, todas as máquinas virtuais foram instanciadas no mesmo nó do *testbed*.

[3]Uma plataforma de código aberto utilizada para o gerenciamento e orquestração de aplicações em contêineres, permitindo a automação da implantação, escalabilidade e gerenciamento desses serviços. Disponíve l em: https://kubernetes.io/pt-br/docs/concepts/ acesso em 2 abr. 2026

[4]Um projeto de código aberto para redes centrais móveis de 5ª geração. Disponível em: https://free5gc.org/ acesso em 2 abr. 2026

[5]Um conjunto de ferramentas de código aberto para monitoramento de sistemas e geração de alertas. Disponível em: https://prometheus.io/docs/introduction/overview/ acesso 3 abr. 2026

[6]Disponível em: https://kubernetes.io/docs/reference/instrumentation/metrics/ acesso em 3 abr. 2026

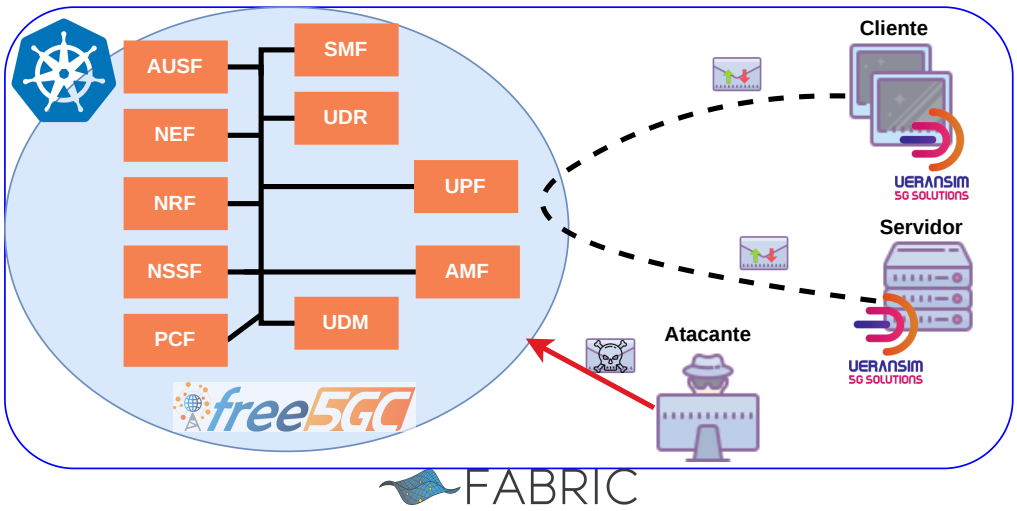

Figura 1. Cenário de testes.

Na segunda e terceira máquina virtual, na Figura 1 apresentadas como `Cliente` e `Servidor`, foi utilizado o simulador UERANSIM[7], um simulador de código aberto que implementa as funções de *User Equipment* (UE) e da rede de acesso rádio (RAN - *Radio Access Network*) do 5G, habilitando o tráfego entre as VMs por meio da rede 5G. No `Servidor`, foi instanciado um servidor *web* NGINX[8] de código aberto, ofertando uma página estática. Enquanto no `Cliente`, foi utilizada a ferramenta Siege[9], uma ferramenta de código aberto para testes de carga e *benchmark* de servidores *web*, capaz de simular múltiplos usuários realizando requisições HTTP simultaneamente. Por fim, na máquina virtual `Atacante`, o *dataset* apresentado na Seção 3.1 foi inserido no *core* da rede 5G utilizando a ferramenta TCPReplay[10].

O tráfego de fundo, gerado pelo Cliente e o Servidor é utilizado para verificar o impacto gerado pelo ataque de DoS nas funções de rede do núcleo da rede 5G. A ferramenta Siege, que realiza requisições HTTP ao servidor *web*, oferta um relatório completo, com informações de quantidade de clientes que obtiveram sucesso na requisição, tempo de resposta, entre outras métricas relacionadas a Qualidade de Serviço (QoS - *Quality-of-Service*). Por meio dessas métricas será possível fazer a análise do impacto do ataque de negação de serviço, realizado contra elementos do *core* da rede 5G, na utilização do serviço por um cliente legítimo. Foram gerados 2000 clientes legítimos, que enviavam requisições HTTP GET ao servidor *web* durante todo o experimento, e cada cliente variava entre uma requisição e outra um tempo aleatório entre 0 e 3 segundos. A escolha da quantidade de clientes foi baseada na capacidade de atendimento do servidor *web* Nginx com sua configuração padrão. Essa quantidade é o limite em que o servidor consegue

[7]Disponível em: https://github.com/aligungr/UERANSIM acesso em 3 abr. 2026
[8]Disponível em: https://nginx.org/ acesso em 3 abr. 2026
[9]Disponível em: https://github.com/JoeDog/siege acesso em 3 abr. 2026
[10]TCPReplay é um conjunto de utilitários Open Source gratuitos para edição e reprodução tráfego de rede capturado anteriormente. Disponível em: https://tcpreplay.appneta.com/ acesso em 5 abr. 2026

responder a todos os clientes sem haver alteração em suas métricas. A ideia é manter o servidor em sua capacidade máxima, mas que a indisponibilidade seja causada pelo ataque em si.

3.1. Dataset

Para a realização dos experimentos, em vista da análise dos impactos de um ataque de Negação de Serviço (DoS) nos elementos de uma rede 5G, foi utilizado o *dataset* 5G Attack Detection (5GAD-2022) [Coldwell et al. 2022]. Este *dataset* consiste em tráfego interceptado de uma rede 5G, incluindo tráfego normal e de ataque, em formato PCAP. O *dataset* foi coletado em um ambiente de 5G simulado, utilizando o free5GC com toda a implementação das funções de rede do core 5G.

O tráfego normal do *dataset* foi gerado simulando atividades típicas de um usuário comum, como requisições de sites, *streaming* de vídeos, *downloads* de arquivos e participação em vídeo chamadas, utilizando um simulador do equipamento do usuário (UE - *User Equipment)*. O tráfego atacante é composto por 10 tipos de ataques, categorizado por ataques de Reconhecimento, Reconfiguração de Rede e DoS. Todos os ataques exploram vulnerabilidades contra uma rede de núcleo 5G [Coldwell et al. 2022]. Nos experimentos deste artigo, foi utilizado apenas dos ataques de DoS, foco deste trabalho, e foi alterado os PCAPs modificando o endereço IP de origem e de destino para os correspondentes endereços no cenário do presente artigo, possibilitando o encaminhamento correto dentro da estrutura criada. Por fim, o *dataset* utilizado contém 90% de tráfego normal e 10% de tráfego malicioso. Essa separação reflete um cenário real, em que há mais tráfego de cliente legítimo do que atacante.

4. Resultados

Com o cenário construído e instanciado, de acordo com as informações apresentadas na Seção 3, e realizado os experimentos, os dados foram coletados e apresentados a seguir. Os experimentos foram realizados dez vezes, apresentando um intervalo de confiança aos resultados apresentados.

A primeira métrica de análise é o tempo de registro da função de rede, no *core* 5G, apresentada na Figura 2. Verifica-se que todas as funções do núcleo da rede 5G tem tempo de registro maior que 490 ms. Dentre elas, destaca-se que o AMF (*Access and Mobility Management Function*) obteve o maior tempo de registro durante o ataque de negação de serviço, atingindo uma média de 1275 ms para realizar o registro da função, mostrando assim que a função AMF é bastante suscetível ao ataque de negação de serviço, no quesito de registro da função na rede 5G. Isso é um problema para rede, visto que o AMF é a função do núcleo responsável por gerenciar o registro, autenticação, autorização e a movimentação (mobilidade) dos dispositivos dos usuários (UE) entre as células da rede 5G. Dessa forma, o AMF sendo impactado seu funcionamento por um ataque de negação de serviço, toda a funcionalidade dessa função fica comprometida na rede, impactando diretamente os novos usuários ou usuários já existentes em seu processo de movimentação na rede 5G.

Outra função de rede que teve impacto no tempo de registro, durante um ataque de DoS, conforme a Figura 2, foi o UPF (*User Plane Function*), com 524 ms para registrar no núcleo 5G. Essa função, apesar de não ser uma das funções que tiveram o maior

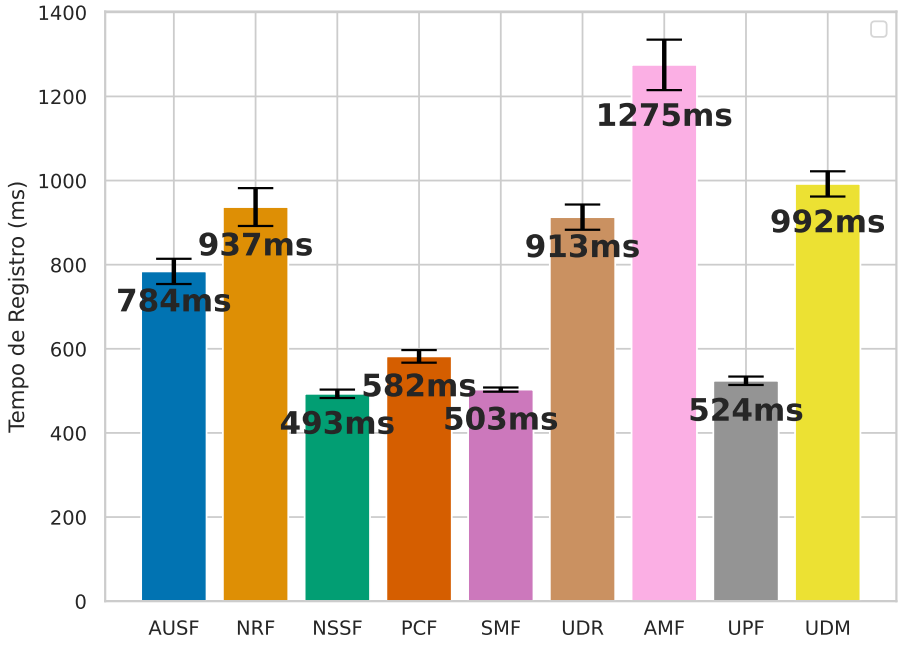

Figura 2. Tempo de registro da função de rede durante o ataque de negação de serviço, em milissegundos (ms).

tempo de registro, é vital para a troca de dados dos usuários na rede 5G. Imaginando um ataque que leve a essa função a necessidade de se registrar novamente na rede, os usuários precisarão esperar, em média, 524 ms para poderem ter seus dados encaminhados novamente. Levando em consideração que as redes 5G trazem consigo diversos requisitos e aplicações que exigem baixa latência, esse tempo de espera é muito grande, provocando quebras dessas aplicações.

A Tabela 1 apresenta, de forma resumida, os resultados médios de consumo de CPU e Memória, em cada uma da função de rede do *core* da rede 5G, durante o ataque de negação de serviço. Os resultados apresentam a média da métrica nos dez experimentos realizados. Os valores foram obtidos por meio do Prometheus. Verifica-se que a maior média de consumo de processamento é do AMF, com 98% de utilização. Esse resultado corrobora com a indicação de que os ataques de DoS geram um maior impacto a essa função de rede específica. A função UDM registrou a segunda maior média de consumo de CPU, com 95%.

Por outro lado, a função de rede UPF, responsável pela troca de dados dos usuários, teve uma média de consumo de 62%. Apesar de não estar próximo aos 100%, o consumo registrado para o UPF pode ser significativo e impactante para gerar algum tipo de distúrbio na comunicação do cliente. Por fim, o consumo médio entre as demais funções de rede variaram entre 30% (caso do NSSF e SMF) até 75% e 80%, caso da UDR e NRF, respectivamente.

Em relação ao consumo de memória, também apresentados na Tabela 1, verificou-

Tabela 1. Resultados de CPU e Memória das funções de rede

Função de Rede	CPU (%)	Memória (MB)
AUSF	68%	13.87MB
NRF	80%	17.56MB
NSSF	30%	5.79MB
PCF	47%	8.65MB
SMF	30%	77.41MB
UDR	75%	13.97MB
AMF	98%	12.87MB
UPF	62%	57.24MB
UDM	95%	7.42MB

se que não houve alteração do consumo normal da função de rede em relação ao ataque de negação de serviço. As funções do *core* 5G tiveram consumo baixo, variando entre 5MB até 17MB. A exceção é a função SMF que consumiu, em média, 77MB, e a função UPF com o uso de 57MB de memória RAM. É importante lembrar que todas as funções de rede, executadas via free5GC, estão utilizando uma infraestrutura de contêineres, por meio do Kubernetes. Essa característica pode corroborar no baixo consumo de memória, e mantendo um isolamento no uso dos recursos computacionais durante os ataques de negação de serviço.

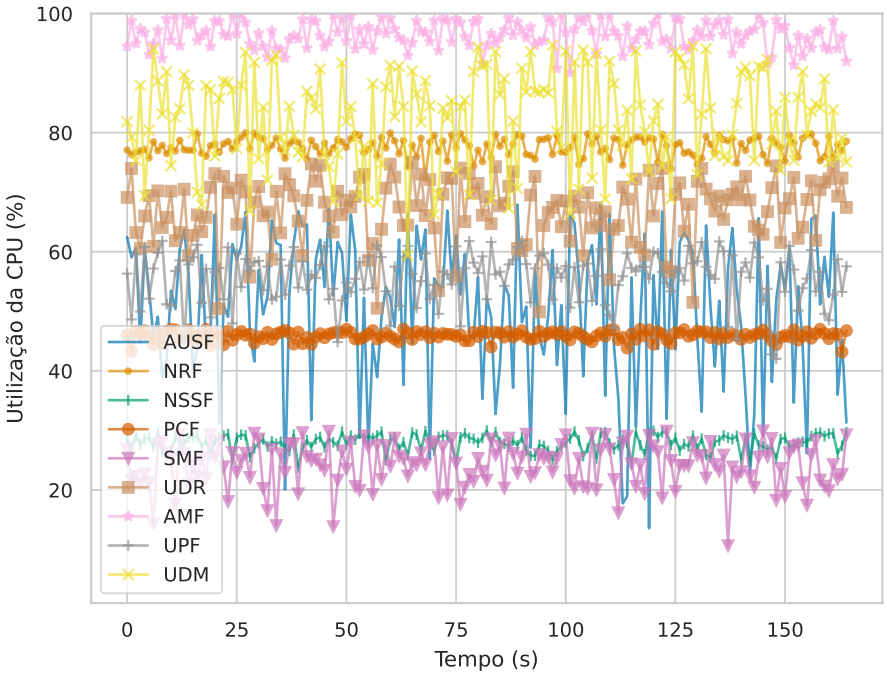

Figura 3. Consumo de CPU, em porcentagem, das funções de rede.

A Figura 3 apresenta um extrato do consumo de CPU durante a execução do ataque de negação de serviço, sendo cada linha os valores verificados para cada função de

rede do núcleo 5G. Assim como mostrado na Tabela 1, a função de rede que teve maior consumo foi o AMF, seguido pelo UDM e NRF. Esse consumo elevado indica que essas funções de redes são impactadas pelos ataques de negação de serviço. Analisando as curvas, verifica-se uma maior variabilidade do consumo de CPU na função de rede AUSF e UDM. Essa variação também é um indicativo, apesar do consumo não ser tão alto, de que essas funções são suscetíveis aos ataques de DoS. Por outro lado, as funções PCF, NRF e NSSF apresentaram um consumo médio constante, sem variação de valores, o que leva a constatar que apesar do ataque, as funções mantêm o consumo constante. Um ponto a investigar é a função NRF, que apesar de manter seu consumo constante, apresentou um uso de CPU na média de 80%.

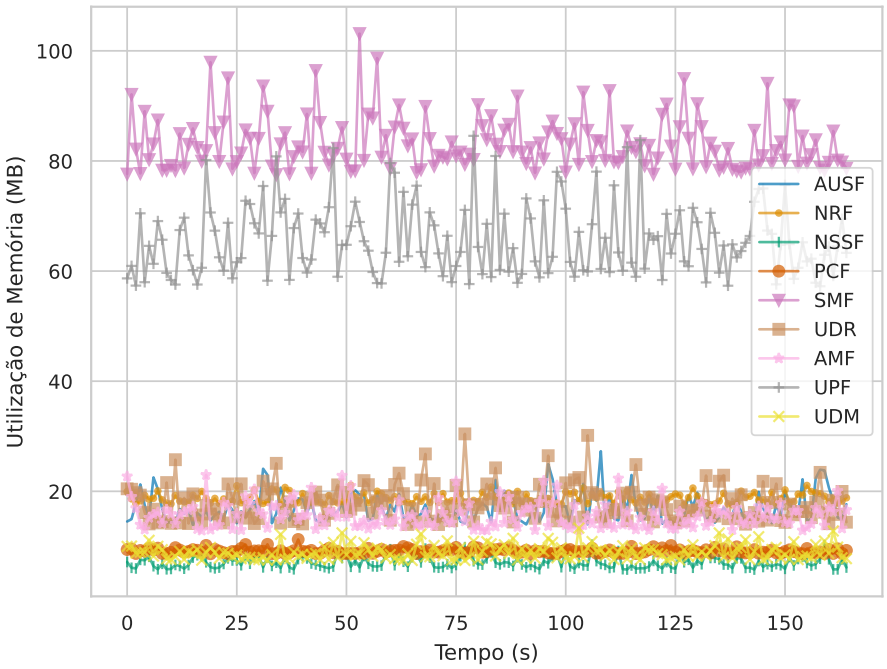

Figura 4. Consumo de Memória, em Mega Bytes, das funções de rede.

Os resultados do consumo de memória, em Mega Bytes, das funções de rede do núcleo 5G durante um ataque de DoS está apresentado na Figura 4. Pode-se verificar que a maioria das funções de rede apresentam pouca variabilidade durante os experimentos, com consumo variando entre 5MB e 17MB. No entanto, um fato que manifesta atenção é que as duas funções que obtiveram um maior consumo, SMF e UPF, também obtiveram uma maior variabilidade na utilização de memória. A média do uso de memória dessas duas funções foi de 77MB e de 57MB para SMF e UPF, respectivamente.

Novamente, essa variação no consumo, mostra que as funções de rede SMF e UPF são impactadas pelos ataques de negação de serviço realizadas contra essas funções, podendo interferir nas suas execuções, apesar de efetivamente o consumo não ser tão alto, chegando com um pico de um pouco mais de 100MB, para o SMF.

4.1. Resultados na perspectiva do cliente

Os próximos resultados são oriundos das análises do tráfego de fundo, em que o cliente está realizando requisições ao servidor *web*, por meio da rede 5G. A Figura 5 apresenta a disponibilidade dos clientes. Ou seja, de todos os clientes que solicitaram a página ao servidor *web*, quantos foram atendidos e receberam a página. No gráfico da esquerda, em azul, é apresentado os resultados na rede 5G em pleno funcionamento, enquanto o gráfico da direita, em amarelo, apresenta o resultado enquanto está havendo um ataque de negação de serviço no *core* 5G. Verifica-se que sem ataque, os clientes tiveram 100% das requisições atendidas. Por outro lado, durante o ataque de DoS, percebeu-se que a disponibilidade diminuiu, apresentando, em média, 78% de disponibilidade, com um desvio padrão de 4,5. Isso significa que, mesmo sem ser alvo do ataque de DoS, o servidor *web* tem dificuldades para prover, de forma satisfatória, aos clientes que solicitam as requisições. Nas análises realizadas durante os experimentos, não teve como verificar se os pacotes que não obtiveram sucesso foram perdidos ainda na solicitação do cliente, no momento que entra na rede 5G, ou se foram após a resposta do servidor *web* com a página.

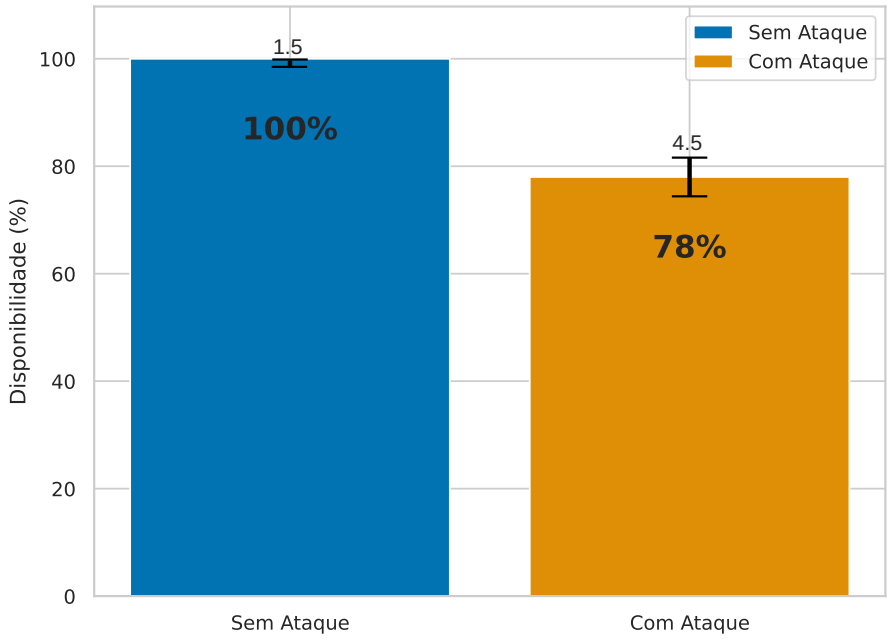

Figura 5. Disponibilidade, em porcentagem, de clientes que solicitaram a página web.

A Figura 6 apresenta o Tempo de Serviço (*Time-to-Service* - TTS), que é o tempo total que leva do cliente solicitar a página ao servidor *web*, o servidor receber e processar o pedido e a resposta retornar ao cliente, sendo a barra da esquerda, em azul, o TTS obtido nos experimentos sem ataque, enquanto a barra da direita, em amarelo, são os resultados dos experimentos durante o ataque de DoS estava sendo realizado nas funções de rede do núcleo 5G.

Nos experimentos realizados sem ataque, os clientes que realizaram a requisição

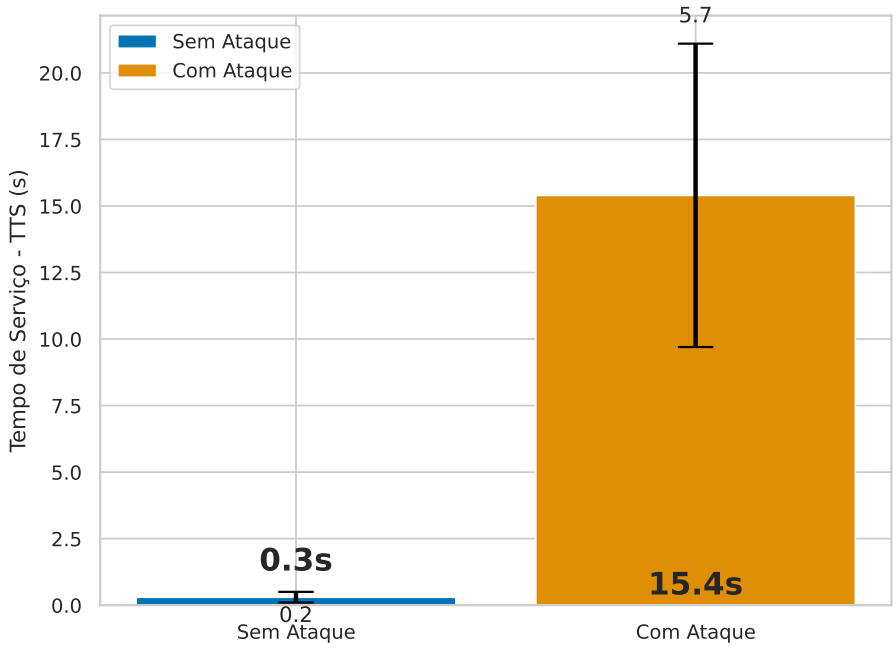

Figura 6. Tempo de serviço, em segundos, de clientes que solicitaram a página web.

da página *web* receberam a resposta em 0,3 segundos, em média, tempo este considerado adequado para o TTS em uma rede 5G. Por outro lado, verifica-se que os clientes experimentaram um longo tempo, em média 15,4 segundos, para receberem a página *web* do servidor, quando está acontecendo um ataque de negação de serviço nos elementos da rede 5G, com um desvio padrão de 5,7.

Fazendo uma análise entre os resultados apresentados na Figura 5 e 6, especificamente do cenário em que o ataque está acontecendo, verifica-se que, apesar da disponibilidade não ser tão baixa, 78% dos clientes tiveram sucesso, esses mesmos clientes tiveram que esperar, em média, 15 segundos para poderem ser atendidos. Esse é um tempo longo para que uma aplicação possa receber os dados. No caso dos experimentos realizados neste trabalho, um servidor *web*, os clientes ainda tiveram sucesso, sendo o *timeout* da aplicação bastante elástico. No entanto, para outras aplicações, como *streaming de vídeo* ou sensíveis à latência, não seria possível ter uma taxa de sucesso tão grande, devido à demora da entrega por parte da rede.

5. Conclusão

Ataques de negação de serviço (DoS - *Denial-of-Service*) são problemas persistentes, pois visam gerar indisponibilidade em serviços. No contexto das redes 5G, esses ataques podem provocar ainda mais problemas para os usuários, principalmente se as funções de redes virtuais (NFV - *Network Function Virtualization*), responsáveis pelo funcionamento da rede 5G, for alvo de um ataque de negação de serviço. Normalmente, na literatura, há trabalhos que analisam os impactos de um ataque de DoS, mas como alvo um

servidor/serviço que está conectado na rede. No entanto, são poucos os que analisam os impactos desses ataques nas funções do *core* da rede 5G.

Diante disso, esse trabalho se propôs a fazer uma análise do impacto, em recursos computacionais e na qualidade de serviço (QoS - *Quality-of-Service*), de um ataque de negação de serviço realizado contra as funções de redes do núcleo da rede 5G. Para isso, experimentos foram realizados, utilizando o free5GC, dentro de um ambiente instanciado no *testbed* Fabric, utilizando o *dataset* de ataque 5GAD-2022.

Verificou-se que clientes legítimos tiveram uma diminuição da disponibilidade de 22% e um aumento expressivo no tempo de serviço (TTS - *Time-to-Service*), quando as funções do núcleo da rede 5G estavam recebendo um ataque de DoS. Especificamente, verificou-se um aumento de consumo de CPU nas funções de rede, especificamente no AMF e UDM, chegando a quase 100% de utilização do processador. Além disso, verificou-se que o SMF e UPF tiveram um crescimento de memória RAM utilizada.

Como trabalhos futuros, pretende-se fazer uma análise mais detalhada de qual função da rede do *core* 5G está sofrendo ataque é o responsável por tamanha degradação das métricas de QoS. Além disso, outra possibilidade é realizar a análise do comportamento das funções com outros tipos de ataques presentes no *dataset*, diferentes dos ataques de negação de serviço. Por fim, aprofundar na análise dos impactos dos ataques na qualidade de serviço e de experiência do usuário, com um tráfego legítimo de outras aplicações, como *streaming* de vídeo, *downloads* de arquivos e participação em vídeo chamadas.

6. Agradecimentos

Este trabalho recebeu financiamento de bolsas de Iniciação Científica (PIBIC) da UFC e do Programa de Educação Tutorial da UFC (PET-UFC). Além disso, os autores gostariam de agradecer o financiamento proveniente da Fundação de Apoio à Pesquisa do Estado de São Paulo (FAPESP) - Projeto de Pesquisa 2018/23097-3 - SFI2 - Slicing Future Internet Infrastructures.

Referências

3GPP (2020). System Architecture for the 5G System (5GS). Technical Report TS 23.501, 3rd Generation Partnership Project (3GPP). Release 16.

Coldwell, C., Conger, D., Goodell, E., Jacobson, B., Petersen, B., Spencer, D., Anderson, M., and Sgambati, M. (2022). Machine learning 5g attack detection in programmable logic. In *2022 IEEE Globecom Workshops (GC Wkshps)*, pages 1365–1370.

das Mercres, J. M. O., da Silva, R. L., Sousa, M. P., Araujo, A. S., de Alencar, A. V., Meneses, T. F., Dias, M. C., and Santos, D. F. S. (2025). Core 5g open source com ran comercial: Uma avaliação de desempenho em rede 5g privativa. In *XLIII Simpósio Brasileiro de Telecomunicações e Processamento de Sinais - SBrT*.

FABRIC Testbed (2026). About FABRIC - FABRIC Portal. `https://portal.fabric-testbed.net/about/about-fabric`. Acessado em: 27 mar. 2026.

Farooqui, M. N. I., Arshad, J., and Khan, M. M. (2022). A layered approach to threat modeling for 5g-based systems. *Electronics*, 11(12).

Håkegård, J. E., Lundkvist, H., Rauniyar, A., and Morris, P. (2024). Performance evaluation of an open source implementation of a 5g standalone platform. *IEEE Access*, 12:25809–25819.

Ji, S. and Kumar Mishra, A. (2024). 5g security issues challenges and solutions against ddos attacks:a survey. In *2024 2nd International Conference on Disruptive Technologies (ICDT)*, pages 1422–1427.

Lando, G., Schierholt, L. A. F., Milesi, M. P., and Wickboldt, J. A. (2023). Evaluating the performance of open source software implementations of the 5g network core. In *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, pages 1–7.

Liao, D. (2023). Implementação de qos em rede 5g através do network slicing. Trabalho de conclusão de curso, Universidade Federal de Santa Catarina, Blumenau.

Medeiros, L., Matos, I., Vieira, V., Lima, R., Correia, S., and Dias, M. (2024). Implementação de um ambiente 5g com recursos de código aberto. In *XLII Simpósio Brasileiro de Telecomunicações e Processamento de Sinais - SBrT*.

Ojope, F. R. M. (2024). Evolução das redes móveis e transição perfeita para 5g. Trabalho de conclusão de curso, Instituto Federal de Educação, Ciência e Tecnologia do Amazonas, Manaus.

Shehab, M. J., Aly, Y., Badawy, A., Mohamed, A., Barhamgi, M., and Salem, S. (2025). O-cloud security: A comprehensive survey of threats, mitigation strategies, and future directions. *IEEE Open Journal of the Communications Society*, 6:7037–7074.

Singh, V. P., Singh, M. P., Hegde, S., and Gupta, M. (2024). Security in 5g network slices: Concerns and opportunities. *IEEE Access*, 12:52727–52743.