REDE 5G: Os Benefícios, Desafios, Vulnerabilidades e Segurança Da Quinta Geração De Redes Moveis. As AmeaçasSobre a Segurança e Privacidade Dos Usuários

Luiz Felipe Capela Santos

Faculdade de Computação – Universidade Federal do Pará (UFPA), Castanhal – PA –Brasil

{luizfelipecapela098@@gmail.com}

Abstract. 5G is the fifth generation of broadband cellular network technology that began to be deployed worldwide in 2019, broadly proposing several benefits and features that stand out with great difference from previous technologies. However, it is necessary to raise some questions about it. The security of this technology, as addressed in the 5G America report, published in July 2020: “security consideration for the 5G”, which was the reference that motivated the development of this work, resulting in some widely publicized points as characteristics and benefits of this technology, which oppose and equilibrate the balance of comparison between benefits and risks for users.

Resumo. O 5G é a quinta geração de tecnologia das redes de celulares de banda larga que começou a ser implantada mundialmente em 2019, propondo amplamente diversos benefícios e características que se destacam com grande diferença das tecnologias anteriores. No entanto, é necessário levantar algumas questões a respeito da segurança dessa tecnologia, como abordado no relatório da 5G América, publicado em julho de 2020: “security consideration for the 5G”, a qual foi a referencia que motivou o desenvolvimento desde trabalho, decorrendo alguns pontos amplamente divulgados como características e benefícios dessa tecnologia, o que contrapõem e equilibra a balança da comparação entre benefícios e riscos para os usuários.

1. INTRODUÇÃO

A quinta geração de tecnologia de Redes Móveis, notoriamente, oferece benefícios emgrande escala e desenvolvimento que ainda é difícil de se mensurar. Apesar de se ter uma ideia do que pode ser feito com esse avanço tecnológico no Brasil e no mundo quando, por sua vez, estiver implementado e acessível para todos.

1.1. Benefícios

É inquestionável os benefícios que este avanço da tecnologia sem fio proporcionará. No entanto, existem alguns risco e consequências que todo avanço tendea enfrentar e alguns problemas à se solucionar para caracterizar uma evolução, e neste caso a respeito da quinta geração de comunicação móvel não é diferente.

1.2. Objetivos

O presente trabalho tem como objetivo identificar os principais benefícios da tecnologia 5G no Brasil e possíveis falhas de segurança que possam ser utilizados para ataques cibernéticos aos usuários, pois em uma tecnologia que promete um aumento na capacidade de tráfego de dados e quantidades de usuários em um nó de rede em uma pequena área de conexão, é visível que esse cenário é um parque de diversão para que sejam feitos ataques cibernéticos, sendo possível obter dados de diversos usuários aproveitando de brechas que podem vir a aparecer na rede. Se fazendo, portanto, necessário a identificação dessas possíveis falhas e tipos de ataques cibernéticos que podem ser praticados.

1.3. Metodologia

A metodologia para este trabalho foi realizada primeiro através de pesquisas por meio de artigos, monografias, livros e sites especializados em tecnologia da comunicação. E com a posse dessas informações será feito uma análise sobre a tecnologia 5G NSA e SA e os prováveis ataques cibernéticos que podem ser possíveis nessas redes.

2. REDE 5G

O 5G é a evolução da sua tecnologia antecessora, mais conhecida como LTE,

popularmente chamada de 4G. A quinta geração de tecnologia móvel inicialmente será implementada utilizando a frequência do 5G, porém fazendo uso do núcleo do 4G. Essaé a implementação inicial do 5G NSA (Non Standalone Network) e posteriormente seráimplementado a versão final, que é o 5G SA (Standalone Network), dessa forma fazendo o uso de uma infraestrutura de conexão e frequência dedicada ao 5G.

Segundo a Anatel, as principais características dessa tecnologia móvel é a variedade de novas possibilidades ainda a serem exploradas. Por exemplo, o aumento das taxas de transmissões de dados que entrega uma maior velocidade de internet, uma maior densidade de conexões que diz respeito a um aumento da quantidade de dispositivos conectados em uma determinada área, a maior eficiência espectral que são incremento da quantidade de dados transmitidos por unidade de espectro eletromagnético, maior eficiência energética dos equipamentos, significando uma redução do consumo de energia, com consequente aumento da sustentabilidade [Anatel 2021]. A internet das coisas também é um tópico muito discutido, pois com a utilização de arquitetura baseada em nuvem o suporte a dispositivos conectados, carros autônomos, casas inteligentes, cirurgias remota, entre outras possibilidades propostas pelo 5G, proporcionará uma melhora significativa tanto para o aumento das produções das empresas, para a economia e para a comodidade e conforto dos usuários.

As redes 5G funcionam por meio de ondas de rádio frequência, assim como as gerações anteriores. Porem, faz uso do espectro coberto pela quinta geração da banda larga móvel, sendo maior que os anteriores, distribuindo-se entre 700 MHz e 2,3 GHZ destinados inicialmente para o 4G (Tecnologia 5G NSA) e as frequências 3,5 GHz e 26 GHZ destinados ao 5G SA (Autônomo) [Anatel 2021].

Os primeiros lançamentos comerciais da nova tecnologia móvel estão aproveitando as especificações do 5G não independentes da versão 15 do 3GPP, o que significa que as primeiras redes 5G serão a NSA que precisam usar os protocolos de plano de controle LTE e a rede LTE Evolved Packet Core (EPC). Os lançamentos iniciais do 5G NSA fornecerão apenas banda larga móvel aprimorada (eMBB), que é um dos três casos de uso da ITU (International Telecommunications Union) para o 5G. Esses casos de usos são classificados como banda larga móvel

aprimorada (eMBB - enhanced mobile broadband), comunicações massivas do tipo máquina (mMTC -massive machine-type communications) e comunicações ultra confiáveis e de baixa latência (URLLC - ultra-reliable and low-latency communications)[Americas 2020].

A proposta do 5G é dar uma evolução na tecnologia atual, trazendo maiores velocidades e largura de banda, menor latência e um ambiente propício ao desenvolvimento de tecnologias disruptivas que serão importantes para o desenvolvimento das telecomunicações e indústria em geral.

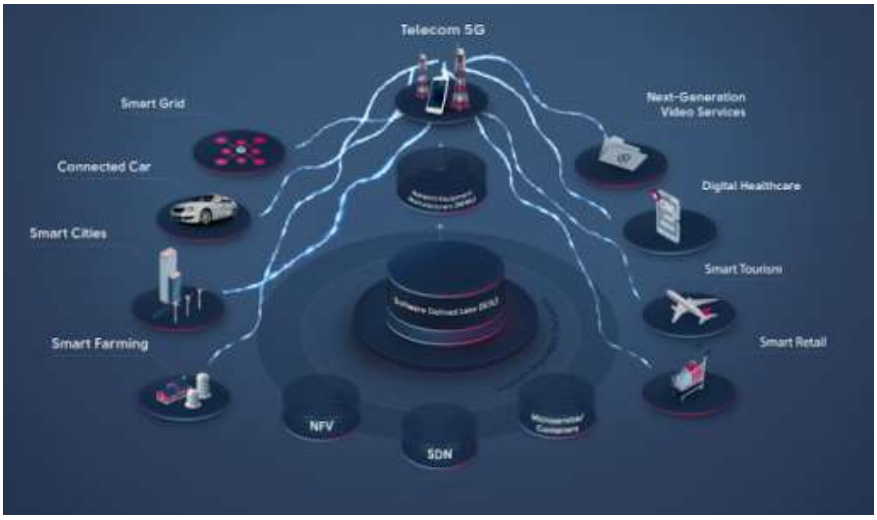

Figura 1. Tecnologia 5G [Alencar 2021]

É possível dizer que o 5G tem como objetivo levar a Internet para inúmeros dispositivos conectados como veículos, casas, câmeras de segurança e diversas outras aplicações de IoT (Internet of Things), bem como viabilizar acesso de banda larga fixa com velocidades ainda mais altas do que as ofertadas pelo 4G. Mas também é possível observar que o desenvolvimento da nova tecnologia está se expandindo além dos usuários tradicionais de redes móveis, pois inclui novos setores como a indústria automotiva, a agroindústria, o setor de saúde, e o advento de cirurgias a distância e outros avanços tecnológicos.

Novos modelos de negócio passam a ser desenvolvidos, como é o caso das chamadas redes privadas [Anatel 2021]. Sua proposta de valor é que estas poderão ser implementadas e operadas independentemente das grandes operadoras de telefonia, como, por exemplo, em um cenário rural. Este novo modelo de negócio possibilita que uma fazenda possa ter sua própria rede 5G apenas com uma estação rádio base podendo ter um operador local [Anatel 2021]. Esse modelo será possível

devido a um novo conceito implementado, o “slicing network”. O conceito de slicing ou fatiamento de frequências permite uma maneira inteligente de segmentar a rede para um determinado setor, negócio ou aplicação.

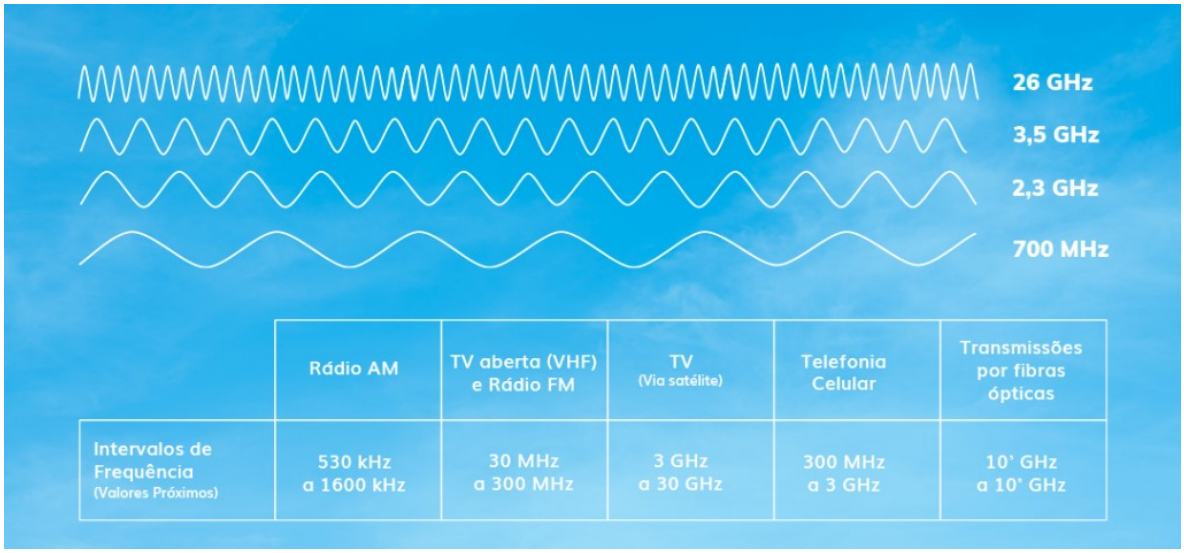

Figura 2. Espectro 5G [SOFT **2021]**

Para ter cobertura nacional, o Brasil vai precisar de mais de 1 milhão de novas antenas espalhadas pelos estados, o que é 10 vezes mais do que o número de antena da tecnologia de geração antecedente, a tecnologia 4G[Puentes 2021]. Para oferecer essa cobertura nacional, as agências operadoras de rede de telecomunicações terão que trabalhar em determinadas faixas de largura de banda. Foram leiloadas no ano de 2021 quatro faixas de frequências em licitação para essas agências operarem. Corresponde essas faixas de frequência 700MHz, 2,3GHz, 3,5GHz e 26GHz.

Tabela 1. Frequência do 5G

700 MHz	Contem uma ampla abrangência geográfica, ela oferece a maior cobertura, e conta com largura de banda de 10 MHz. Com capacidade baixa, seu foco é promover cobertura, e atende operações simples, como fazer uma chamada, enviar uma mensagem. É uma faixa interessante para o agro-negócio[Sgarioni 2021].
2,3 GHz	É a faixa que tem cobertura compatível com as redes 4G de hoje. Traz de 40 a 50 MHz de largura de banda. O potencial dessa faixa é o de ofertar capacidade muito boa dentro do 4G, com taxas de dados altas. Entretanto, sua cobertura é menor, e vai até 10 km[Sgarioni 2021].

3,5 GHz	Oferece um sinal de longo alcance e Internet de qualidade [Santos 2022], com largura de banda de 80 a 100 MHz por canal, É a mais usada no mundo inteiro para o 5G, adequada para qualquer dispositivo, com uma cobertura estimada de 3 km a 10 km[Sgarioni 2021].
26 GHz	faz parte das chamadas faixas de “ondas milimétricas”. Possui altíssima capacidade e baixíssima latência[Sgarioni 2021]. Exige a instalação de mais antenas pelo país, pois tem o alcance limitado e dificuldade para passar por obstáculos físicos, como prédios e árvores[Santos 2022]. No entanto, atende bem em áreas como estádios de futebol, parques abertos e shopping centers.[Sgarioni 2021]

2.1. Segurança do 5G NSA

Os padrões gerais das redes 5G são desenvolvidos pelo consórcio da 3rd Generation Partnership Project (3GPP). estes padrões descrevem protocolos que tem como objetivo fornecer garantias de segurança aos assinantes, usuários e prestadores deserviço das redes moveis. No começo da implementação do 5G será utilizado o padrão 3GPP release 15[Americas 2020], contudo, os padrões e protocolos do 5G autónomo jaforam desenvolvidos e estão descritos no padrão 3GPP release 16.

Na utilização de dispositivos conectados em redes 5G, como em qualquer contexto computacional, os protocolos de autenticação são componentes essenciais nasgarantias dos requisitos de segurança como confidencialidade, integridade e autenticidade. Os padrões em redes 5G descrevem mecanismos e protocolos de segurança que visam garantir autenticação segura na comunicação entre dispositivos,servidores e outros equipamentos de rede.

2.1.1 Ameaças e ataques cibernéticos possíveis do 5G NSA

Qual o problema de se ter dados, Informações confidenciais obtidas passiva ou ativamente? O problema é que, dependendo do alvo algumas informações podem ser explorados pela organização de contra inteligência de outro país para uma variedade de propósitos, incluindo suborno de indivíduos para obter informações

monetárias ou coleta de informações confidenciais adicionais (ou seja, recrutamento de espiões)[Americas 2020], além de ter sua privacidade invadida, podendo ser exposto a vida pessoal, rotina, informações privadas, etc. Para o serviço eMBB inicial, quaisquer ameaças e vulnerabilidades LTE também existirão na rede 5G NSA. Mesmo após as operadoras atualizarem seus sites celulares com rádios 5G (gNBs - Next Gen Node Base station) usando a arquitetura NSA, alguns desses sites celulares 5G NSA podem operar por anos após o lançamento comercial da arquitetura 5G autónoma [Americas 2020]. alguns ataques conhecidos das gerações anteriores como, downgrade de rede, negação de serviços - DOS, Man-in-the-Middle - MITM entre outros, paras usuários desprevenidos e desavisados esses ataques são extremamente difícil de se descobrir, até pelo motivo de serem muito eficientes.

2.1.2. Ataques de downgrade 2G/3G

Os ataques de downgrade permitem que os adversários forcem um UE (User Equipament) conectado por LTE a regredirem para tecnologia mais baixa como o 2G ou 3G, que possui controles de segurança significativamente menores. Em última análise, os adversários podem realizar ataques ativos man-in-the-middle (MiTM) e/ou ataques passivos (por exemplo, espionagem) para coletar informações confidenciais de um cliente.

Por exemplo, se os clientes experimentaram historicamente conexões 4G/LTE confiáveis em uma área específica e bem conhecida (por exemplo, trabalho, casa, cafetaria, etc.), mas se conexões repentinamente reverteram para 2G/3G [Americas 2020], é uma indicação que esses clientes foram alvos dessa pratica e que esse ataque foi um sucesso. Os clientes normalmente podem saber se estão conectados a 2G ou 3G a partir da indicação de conexão em seus telefones. Em vez de indicar LTE e/ou 4G, a tela normalmente exibirá um “E”, “G” ou outro símbolo[Americas 2020].

2.1.3. Rastreamento IMSI (Privacidade)

O IMSI (Identidade Internacional do Assinante Móvel) é um número único que pode ser capturado no ar. Stingrays (Dispositivo de espionagem) de alto custo não são mais necessários para esse ataque, porque rádios definidos por software

(SDRs) de baixo custo podem ser adquiridos pela Internet. Isso pode permitir que os maus atores busquem alvos de menor valor, resultando em preocupações de privacidade para o público em geral. Esses mesmos SDRs de baixo custo provavelmente seriam usados por um adversário para rastrear e explorar alvos de maior valor por vários motivos. Os adversários podem determinar o valor do alvo com base no movimento desse alvo[Americas 2020].

Contudo, esse ataque funciona atualmente de maneira bem abstrata, de forma que dispositivos de vigilância simulam o funcionamento das torres de telefonia e são capazes de captar sinais de telefones móveis. São enviados pacotes e sinais que fraudam os celulares, fazendo com que, os aparelhos transmitam sua localização e propaguem suas informações para a torre espiã. Assim, fazem com que os celulares daquela região se conectem e compartilhem seu número de IMSI e o ESN (Electronic Serial Number), dessa forma podendo até revelar a localização exata do usuário. Além de o dispositivo conseguir reconhecer onde está aquele aparelho, ele também pode receber informações de celulares que estão próximos [Americas 2020]. As versões mais sofisticadas são capazes até de escutar ligações principalmente quando o ataque de downgrade combinado é usado, forçando os equipamentos a se conectar à internet usando uma conexão 2G, uma forma muito menos segura do que as demais.

2.1.4. Ataques Man-in-the-Middle

O tráfego aéreo do Plano de Usuário do AS (Access Stratum) não é adequadamente protegido pelos algoritmos de segurança da Proteção de Integridade. Isso potencialmente se traduz em um cenário em que a mensagem de um cliente e/ou o fluxo de comunicação podem ser interceptados no meio entre o UE e o servidor, Ou Seja, Um adversário pode manipular a mensagem do cliente e/ou o fluxo de comunicação entre o UE e o servidor [Americas 2020].

A utilização de protocolos de criptografia ponta a ponta é essencial para a segurança. A ameaça contra os clientes e sua privacidade é limitada, no entanto, nota-se que nem todas as comunicações destinadas à Internet são protegidas por protocolos de criptografia de segurança de ponta a ponta [Americas 2020]. Se a comunicação do cliente estiver protegida por protocolos de criptografia de segurança de ponta a ponta (por exemplo, SSL, TLS, IPSec, VPN, etc.), esse ataque

será impossível. A maioria das comunicações corporativas, comerciais e de mídia social (por exemplo, VPN corporativa, bancos, Facebook, Twitter, etc). são protegidos de ponta a ponta [Americas 2020].

2.1.5. Roaming 5G NSA - LTE

O roaming é uma tecnologia usada para permitir que usuários que não estão na área de cobertura onde foi gerado a sua linha de transmissão de dados ou voz utilizem uma rede, fazendo ser possível que uma linha que possua um DDD (Discagem Direta à Distância) de origem diferente da local, se comunique em uma área fora da sua cobertura.

O roaming LTE é fortemente dependente dos protocolos SS7 e Diameter. O SS7(Sistema de Sinalização 7) foi desenvolvido inicialmente em 1975 para a rede telefónica pública comutada (PSTN), mas foi a base das comunicações de voz em redes 2G e 3G[Americas 2020]. É uma rede digital dedicada, usada para inicialização e controle de chamadas. Cada ponto de sinalização na rede SS7 é unicamente identificado por código numérico de ponto. Códigos de ponto são carregados em mensagens de sinalização trocados entre pontos de sinalização para identificar a fonte e o destino de cada mensagem. O ponto de sinalização utiliza uma tabela de roteamento para selecionar o caminho apropriado para cada mensagem[Junqueira 1997].

Diameter é um protocolo de autenticação e autorização definido em 1988 para substituir o protocolo RADIUS[Americas 2020]. O Diameter é baseado no radius, porem tentar reparar as deficiências apresentadas no protocolo anterior. Ambos os protocolos SS7 e Diameter têm sido usados em larga escala e possuem vulnerabilidades de segurança conhecidas que têm sido foco de ataques há anos. Como uma transição do SS7, muitos operadores implantaram voz sobre LTE (VoLTE), que usa o SIP-RTP (Session Initiation Protocol / Realtime Transport Protocol) em vez do SS7. O Diameter ainda é usado em LTE para funções de autenticação, autorização e PCC (Policy Charging and Control). Diâmetro e SS7 são vulneráveis a escutas, incluindo chamadas de voz, leitura de mensagens de texto e rastreamento de telefones. Muitas operadoras possuem firewalls SS7 e/ou diameter, mas esses firewalls estão sujeitos a vários ataques de protocolo cruzado [Americas 2020].

2.2. 5G SA - “puro” (Autónomo)

O 5G puro, é de fato a tecnologia da quinta geração, chamada oficialmente de 5G SA (Standalone), com sua implementação completa utilizando a arquitetura, frequência, núcleo entre outras infraestrutura pensadas e configuradas para funcionarem em sua totalidade apenas para sua transmissão e função. As principais características da nova geração de Internet móvel. São a baixa latência que varia entre 1 e 5 milissegundos, velocidade na casa dos gigabits por segundo(Gb/s), a redução de consumo de bateria, maior cobertura, infraestrutura que promete massificar e diversificar a Internet das coisas nos principais setores como segurança pública, tele-medicina, educação à distância, cidades inteligentes, automação industrial e agrícola – entre tantos outros. A infraestrutura por de trás dessa evolução é a utilização de algumas tecnologias emergente como a Arquitetura baseada em Serviços, Cadeia de Suprimentos – Hardware e Software, Software de Código Aberto e entre outros [Americas 2020].

2.3. Diferença entre o 5G NSA e 5G SA.

Figura 3. Comparação entre 4G e 5G [UFABC 2022]

O 5G NSA como o próprio sigla sugere é uma rede (non-satandalone) dependente da tecnologia subjacente para funcionar, é uma maneira encontrada pelas grandes empresas para implementar o 5G para utilizar inicialmente a arquitetura do LTE e gradualmente ir implementando o 5G independente. Já a arquitetura de rede independente foi projetada para utilizar:

Redes definidas por software (SDN): um modelo usado para a adaptabilidade de rede independente da tecnologia utilizada, em síntese é uma maneira de digitalizar a rede, o que se converte em alguns benefícios como redução de custos com monitoramento, configuração, gerenciamento e controle, além de se ter redes mais inteligentes. Em sua essência, os sistemas e funções 5G são módulos de software programáveis [Americas 2020].

Virtualização de funções de rede (NFV): tem a função de desconectar o software do hardware, substituindo diversas funções de rede, como firewalls, balanceadores de carga e roteadores, com instâncias virtualizadas, operando como software. O que possibilita novos serviços e recursos aprimorados. As funções que compunham o sistema 5G podem ser compostas por elementos de software de código aberto, mas sua segurança e integridade nem sempre são conhecidas[Americas 2020].

Arquiteturas nativas de nuvem: para escalabilidade de recursos[Americas 2020]. Essa infraestrutura de rede permite desagregação e virtualização, levando a um plano de controle e separação de plano de usuário (CUPS) com o 5G NSA e introduz recursos como fatiamento de rede e computação de borda multiacesso (MEC) com o 5G SA. Migrando para uma arquitetura baseada em serviços para que o 5G utilize um modelo de serviços ao consumidor produtor em vez de entidades funcionais fixas.

Fatiamento de Rede: refere-se à técnica de isolar o desempenho de ponta a ponta de uma parte da rede em comparação com outra. Envolve todos os três domínios do 5G: a RAN, a rede de transporte e o 5G Core. O fatiamento de rede é diferente das Redes Privadas Virtuais (VPNs) em que as VPNs são sobreposições sobre os recursos da rede física, enquanto o fatiamento particiona o recurso[Americas 2020].

2.4. Desafios Tecnológicos do 5G

Claramente a primeira necessidade do 5G é fornecer os serviços que já usamos, contudo, de forma mais eficiente, sem problemas de latência, conectividade intermitente ou conexões perdidas, mesmo em condições de rede desafiadoras, como ambientes lotados ou veículos em movimento. Um dos desafios das redes 5G, é melhorar a eficiência energética de dispositivos com restrição de bateria, e deve

adotar técnicas de proteção ambiental.

Espera-se que o 5G suporte[Teleco 2020]:

I. Capacidade de tráfego de 10Mbps por metro quadrado em áreas de hotspot.

II. Taxas de transferência de dados experimentadas pelo usuário de até 1 Gbps (Gigabit p/ segundo), com taxas de transferência de dados de pico na casa das dezenas de Gbps e volume total de tráfego de pelo menos 1 Tbps (Terabit) por quilômetro quadrado.

III. Latência (Delay) de 1 ms (milissegundo) para troca de dados com experiência do usuário.

IV. Densidade de conexão de até um milhão de conexões por quilómetro quadrado.

V. Alta mobilidade até 500km/hora em trens de alta velocidade e até 1.000km/hora em aviões, com experiência de usuário aprimorada.

2.5. Segurança do 5G SA

Um dos objetivos do 5G é tornar a rede flexível e programável. Isso pode ser alcançadopela virtualização de muitas funções e serviços previamente implementados em hardware. O software pode até tirar proveito dos módulos de open source, mas pode teralgumas vulnerabilidades associadas[Americas 2020].

A implementação do 5G produzirá muitos benefícios de desempenho e diversidade de aplicações por meio do amplo uso de recursos baseados na nuvem, virtualização, fatiamento da rede e outras tecnologias emergentes. Entretanto, também novos riscos de segurança, brechas e vulnerabilidades expostas dentro da arquitetura desegurança 5G passam a existir como desvantagem para a evolução da tecnologia.

Conforme a implementação do 5G avança e nós de desempenho crítico tornam-se cada vez mais virtualizados, as operadoras vão precisar monitorar e avaliar continuamente o desempenho da segurança. O que significa monitorar a segurança de rede de ponta a ponta em toda a arquitetura, nos dispositivos e nas aplicações do sistema.

A arquitetura 5G os usuários terão acesso a serviços específicos da rede. Quaisquer falhas atuais de hardware ou software (incluindo sistemas operacionais) também existirão na arquitetura 5G. Por fim, o 5G utilizará os conceitos de SDN e NFV, e ambos vêm com ameaças e vulnerabilidades exclusivas[Americas 2020].

2.5.1. Ameaças, vulnerabilidades e ataques do 5G SA

Segundo o relatório feito em 2020 pela 5G Américas, uma organização comercial da industria composta por provedores de serviços e fabricantes lideres das telecomunicações, o 5G mesmo após ser implementado completamente ainda possuirá vulnerabilidades conhecidas das tecnologias que o antecederam, alem de novas ameaçase vulnerabilidades da sua própria tecnologia. Como já dito, por não ser viável economicamente que as operadoras instalem a rede autónoma para que ela funcione em seu espectro e infraestrutura independente, obrigando a necessidade de utilizar o núcleo e alguns espectros do LTE, por causa disso, mesmo após está funcionando completamente independente, o 5G SA terá algumas vulnerabilidades do LTE que irá persistir por alguns anos. Contudo ainda terá de lidar com as brechas de segurança e ataques possíveis que surgirão com o passar do tempo com a sua própria arquitetura. Norelatório da 5G Américas, ela identifica algumas vulnerabilidades e ataques que são possíveis serem exploradas nessa tecnologia SA, algumas delas são:

Man-in-the-middle, Proteção de Integridade do Plano do Usuario: O 3GPP define algoritmos de integridade IP UP em suas especificações, mas muitos dos OEMs(Original equipment manufacturer) não os implementaram devido ao impacto na experiência do usuário (por exemplo, transferências de dados de download e upload). Habilitar o UP IP requer recursos computacionais consideráveis e adiciona sobrecarga que afeta diretamente as taxas de transferência máximas que podem ser medidas no dispositivo do usuário. O IP é habilitado nas mensagens do plano de controle, mas isso ainda deixa o tráfego de dados do usuário vulnerável porque o plano de controle e o plano do usuário são segregados. Por exemplo, a falta de UP IP pode permitir que uma estação base não autorizada manipule as mensagens de dados do usuário (ou seja, DNS)e redirecione um usuário para um site malicioso.

Privacidade SUPI/SUCI: No LTE, o IMSI é enviado “em claro” pelo ar,

permitindo que um adversário capture e rastreie um cliente de alto valor. O 3GPP abordou isso removendo o IMSI de texto simples e mudando para uma solução SUPI/SUCI. O IMSI em 5G agora é chamado de Identificador permanente de Assinatura (SUPI). O Identificador Oculto de Assinatura (SUCI) é enviado pelo ar em vez do SUPI, o que impede que um adversário rastreie um alvo de alto valor. A partir dehoje, existem alguns casos em que o cliente pode ser rastreado se o SUPI for enviado pelo ar. Esses casos são:

I. Dispositivos não autenticados tentando fazer uma chamada deemergência

II. Um UE(User Equipament) com um SIM(Subscribe Identity Module) legado que não foi provisionado com a chave pública 5G por meio de uma atualizaçãoOTA (Over-the-Air)

III. Clientes que trazem seus próprios dispositivos para a rede de umaoperadora com SIMs que não foram atualizados

Arquitetura da Nuvem e Segurança: A arquitetura de nuvem é a forma que os componentes de uma tecnologia se combinam para criar uma nuvem, na qual o recursossão agrupados pela tecnologia de virtualização e compartilhados em uma rede. Com isso, alguns questionamentos são levantados para as operadoras responsáveis pelas redes moveis a respeito do que elas tem de fazer, levando em conta o melhor para ela e para entregar o melhor em quesito de custo-benefícios para os usuários, ou seja: deve-seconstruir sua própria infraestrutura em nuvem ou aproveitar uma já existente (ou seja, comprar versus construir)? Como tirar proveito da alta disponibilidade e resiliência em uma nuvem específica? Como as comunicações entre processos – dentro da mesma nuvem ou entre nuvens – podem ser seguras?

Riscos de código Aberto em 5G: A maior transparência do código aberto significa que qualquer pessoa, incluindo criminosos cibernéticos, será capaz de inspecionar o código para identificar e explorar vulnerabilidades. O software de código aberto fornece aos invasores um ambiente rico em alvos devido ao seu uso generalizado.Quando o código aberto é usado como base para o produto de um fornecedor, quaisquer vulnerabilidades podem ameaçar a integridade da solução do

fornecedor.

2.5.2. Roaming do 5G SA

No 5G SA para mitigar as vulnerabilidades do roaming do 5G NSA, os fluxos de roaming serão consideravelmente diferentes, pois HTTP/2 e JavaScript Object Notation(JSON) serão usados em relação ao protocolo Diameter legado. No final de 2020 e/ou início de 2021, as operadoras começaram a implantar o Voice over New Radio (VoNR)que substituirá o VoLTE na rede 5G. O 5G apresenta um Security Edge Protection Proxy (SEPP) que estabelecerá uma conexão segura e criptografada com o SEPP do parceiro de roaming. Os SEPPs então passarão os fluxos do plano de controle HTTP/2SBA para autenticação e autorização. As mensagens do plano de controle serão transmitidas com segurança entre os proxies de proteção de borda de segurança VPLMN e HPLMN (SEPPs) por meio da interface N32. O tráfego do User Plane é transportado sobre GTP-U. Por Opção (1), GTP-U não fornece proteção de confidencialidade ou integridade do tráfego de dados do usuário, portanto, um túnel seguro entre VPLMN e HPLMN deve ser usado para proteger os fluxos de dados do usuário na interface N9.

3. Conclusão

A tecnologia do 5G é inquestionavelmente um avanço tecnológico que mudará a vida de todos, com os inúmeros benefícios e possibilidades de configurações que são possíveis graças a essa evolução. No entanto é preciso se atentar sobre a seguranças de nossos dados e informações que circulam com e sem o nosso consentimento Ter mais atenção para com as informações compartilhadas e inseridas na internet, buscar conhecimento sobre o assunto é uma boa maneira de se prevenir e reduzir as chances deter a vida privada violada. As bases de segurança do 5G são de extrema importância para as redes, os fabricantes precisam de incentivo para aumentar seus esforços de segurança, assim como cooperar com empresas de cibersegurança para desenvolver soluções de criptografia, monitoramento, etc. E o consumidor precisar buscar mais conhecimento sobre a cibersegurança, para poder obter a melhor experiência que essa tecnologia poderá lhe proporcionar.

Referencias:

5G America, Security-Considerations-for-the-5G-Era-2020-WP-Lossless. Julho de 2020.Disponível em https://www.5gamericas.org/security-considerations-for-the-5g-era.Acesso em: 01 de Setembro de 2022.

Agência Nacional de Telecomunicações, Tecnologia 5G. Agência Nacional de Telecomunicações, 22 de Fevereiro de 2021 Disponível em: https://www.gov.br/anatel/pt-br/assuntos/5G/tecnologia-5g. Acesso em: 29 de Agosto de 2022.

VALENTE, Jonas. O que é a tecnologia 5G, Agencia Brasil, 30 de Março de 2020, Disponivel em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-03/agencia-brasil-explica-o-que-e-tecnologia-5g. Acesso 01 de Setembro de 2022.

PUENTE, Beatriz. 5G: país tem de instalar até 1 milhão de antenas para atingir cobertura nacional, CNN BRASIL, 08 de Novembro de 2021. Disponível em: https://www.cnnbrasil.com.br/business/5g-pais-tem-de-instalar-ate-1-milhao-de-antenas-para-atingir-cobertura-nacional/. Acesso em: 01 de Setembro de 2022.

SGARIONI, Mariana. 5G: um resumo sobre como será o maior leilão em volume de espectro da história do Brasil. Mobile Time, 1 de Novembro de 2021. Disponível em: https://www.mobiletime.com.br/noticias/01/11/2021/5g-um-resumo-sobre-como-sera-o- maior-leilao-em-volume-de-espectro-da-historia-do-brasil/. Acesso em: 01 de Setembro de 2022.

SANTOS, L. Vinícius. 5G no Brasil: o que muda e deixa de funcionar com a tecnologia? Tecmundo, 06 de Julho de 2022. Disponível em: https://www.tecmundo.com.br/mercado/241449-5g-brasil-muda-deixa-funcionar-tecnologia.htm. Acesso em: 01 de Setembro de 2022.

JUNQUEIRA, Flavio Paiva. Comunicações Pessoais Móveis - Uma visão geral sobre os sistemas. GTA/UFRJ. 12 de Março de 1997. Disponivel em: https://www.gta.ufrj.br/~flavio/commovel/Ss7.htm. Acesso em: 04 de setembro de 2022.

Teleco. 5G: Tecnologias de Celular, Teleco, Julho de 2020. Disponível em: teleco.com.br. Acesso em: 14 de Setembro de 2022.

ALENCAR, Felipe. Redes 5G: muito alem da velocidade. Disponivel em: https://www.felipealencar.net/2021/04/redes-5g-muito-alem-da-velocidade.html. Acesso em: 19 de Outubro de 2022

UFABC, Tecnologia de comunicação móvel 5G: a solução para integração da nova sociedade moderna, 05 de Março de 2022. Disponivel em: https://ufabcdivulgaciencia.proec.ufabc.edu.br/2022/05/05/tecnologia-de-comunicacao-movel-5g-a-solucao-para-integracao-da-nova-sociedade-moderna-v-5-n-5-p-2-2022/. Acesso em: 19 de Outubro de 2022.

BRASIL, Agencia. Tecnologia 5G vai a leilão hoje; entenda os impactos em 04 de novembro de 2021. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-11/tecnologia-5G-vai-a-leilao-hoje-entenda-os-impactos

Diogo Sousa, 5G chega ao Brasil, mas não da forma como você esperava. Disponível em: https://canaltech.com.br/telecom/5g-chega-ao-brasil-mas-nao-da-forma-como-voce-esperava-167409/

SOFT, IXC - Iniciativa 5G Brasil: conheça o projeto 7 de outubro de 2021. Disponível em:https://blog.ixcsoft.com.br/iniciativa-5g-brasil/