Segurança em Telecirurgia Robótica Baseada em Redes 5G

Caio Souza *†, Felipe Mendonça*, Renata Reis *†, Maria Damasceno *†, and Andson Balieiro*
* *Centro de Informática (CIn) - Universidade Federal de Pernambuco, Recife, Brasil*
†*Sidia Institute of Science and Technology , Manaus, Brazil.*
Email: {caio.souza, renata.gomes, maria.lima}@sidia.com, fasm@softex.cin.ufpe.br, amb4@cin.ufpe.br

***Abstract*—Ao proporcionar velocidades de transmissão elevadas, latência reduzida e capacidades massivas de conexão, as redes 5G pavimentam o caminho para a telecirurgia robótica, delineando uma era de avanços notáveis na prestação de cuidados de saúde, com cirurgias remotas mais precisas e acessíveis e promovendo uma revolução no paradigma cirúrgico. A área da saúde, por natureza, é caracterizada por padrões rigorosos de segurança e proteção de dados, além de exigir alta confiabilidade e disponibilidade. A integração com as redes 5G traz mais desafios, uma vez que elas embarcam diversos tipos de serviços e uma variedade de tecnologias de suporte, tornando-as mais complexas de gerenciar e ampliando a superfície de ataques e falhas. Neste sentido, este trabalho endereça a interseção as redes 5G com a área de saúde sob a ótica de segurança. Através de uma Revisão Sistemática da Literatura (RSL), busca-se fornecer um panorama das implicações de segurança inerentes à implementação do 5G no contexto da saúde, com foco especial em telecirurgia robótica. Este mapeamento não apenas revela os características e desafios desse campo, mas também se aponta direções e estratégias que enderecem as questões de segurança.**

***Index Terms*—Redes 5G, Telecirurgia Robótica, Segurança Cibernética.**

I. Introdução

A Quinta Geração de redes móveis (5G) tem se revelado fundamental na transformação do cenário de comunicação global e seu impacto alcança diferentes áreas, entre elas a da saúde. Nesse contexto, a telecirurgia robótica emerge como um campo promissor em redes 5G, delineando uma era de avanços notáveis na prestação de cuidados de saúde. Ao proporcionar velocidades de transmissão elevadas, latência mínima e capacidades massivas de conexão, o 5G pavimenta o caminho para cirurgias remotas mais precisas e acessíveis, promovendo uma revolução no paradigma cirúrgico [1].

Atualmente, tem-se observado uma adaptação crescente de sistemas robóticos para viabilizar a realização remota de procedimentos médicos, incluindo cirurgias, diagnósticos e monitoramento. A integração desses sistemas proporciona uma alternativa mais eficiente para a execução de procedimentos tradicionais no âmbito de saúde à distância. Esse cenário ganhou mais relevância após a pandemia do coronavírus (COVID-19) e as restrições de distanciamento físico implementadas globalmente. Apesar dos avanços, a teleoperação enfrenta desafios significativos, destacando-se falhas de comunicação, atrasos na transmissão, limitações de largura de banda e preocupações com violações de segurança como desafios importantes a serem superados [2].

A área da saúde, por natureza, é caracterizada por padrões rigorosos de segurança e proteção de dados, além de exigir alta confiabilidade e disponibilidade. A integração com as redes 5G faz essas demandas alcançarem um nível mais crítico, uma vez que, para cumprir os diferentes tipos de serviços e requisitos, as redes 5G incorporam uma variedade de tecnologias de suporte, como a Virtualização de Funções de Rede (NFV), Computação de Borda Multi-Acesso (MEC) e Redes Definidas por Software (SDN), dentro de uma Arquitetura Baseada em Serviços (SBA), tornando-as mais complexas de gerenciar e ampliando a superfície de ataques e falhas.

Os sistemas de telecirurgia robótica existentes enfrentam desafios relacionados à segurança, privacidade e latência, o que limita sua aplicabilidade em procedimentos cirúrgicos a curto prazo em todo o mundo. No entanto, atender aos requisitos necessários por meio das redes 5G não é isento de desafios significativos, especialmente no que diz respeito à segurança da informação e à integridade das operações cirúrgicas [3]. Neste sentido, este trabalho endereça a interseção as redes 5G com a área de saúde sob a ótica de segurança. Através de uma Revisão Sistemática da Literatura (RSL), busca-se fornecer um panorama das implicações de segurança inerentes à implementação do 5G no contexto da saúde, com foco especial em telecirurgia robótica. Este mapeamento não apenas revela as características e desafios desse campo, mas também se propõe a apontar direções e estratégias que enderecem às questões de segurança. Dessa forma, este estudo pode servir como um guia inicial para profissionais interessados nessa área, oferecendo fundamentos para a tomada de decisões e a construção de um ecossistema 5G de saúde conectado e seguro. Este artigo encontra-se assim organizado. A Seção II conceitua as redes 5G, telecirurgia, retrata desafios de segurança nas redes 5G, bem com aqueles oriundos da interseção entre as duas áreas. A metodologia adotada na condução do mapeamento sistemático é apresentada na Seção III. A Seção IV sintetiza os trabalhos selecionados no estudo. Resultados e Discussão são destacados na Seção V. Por fim, a Seção VI conclui este artigo.

II. Conceitos-Chave

A. 5G

As redes 5G estão em implantação ao redor do globo e trazem inovação nas comunicações móveis, oferecendo acesso à internet de alta velocidade, baixa latência na comunicação, alta densidade de conexões, maior flexibilidade na implantação da rede e provimento de serviço, e conectividade as pessoas, dispositivos e máquinas. Elas suportam aplicações organizadas em três categorias, largura de banda móvel aprimorada (eMBB), comunicação massiva do tipo máquina (mMTC) e comunicação com latência muito baixa e confiabilidade muito alta (URLLC). Esta última possui requisitos estritos de latência, confiabilidade e disponibilidade [4], abrangendo aplicações de carros autônomos, Internet tátil e telecirurgia, por exemplo. Para isso, demanda tecnlogias-chave tais como NFV e MEC para que seja suportada [5].

Além disso, a Quinta Geração de Redes Móveis emerge como uma peça fundamental na transformação digital da sociedade, desempenhando papel crucial na promoção da saúde inteligente, mitigando as disparidades na alocação de recursos médicos e impulsionando avanços na medicina. Por exemplo, através das redes 5G, as pessoas podem ter maior consciência e controle sobre sua saúde, permitindo testes e monitoramento em domicílio. Na combinação com Inteligência Artificial (IA), culmina numa rede de dispositivos inteligentes interligados, ampliando o escopo para tomada de decisões e crescimento do ecossistema médico, bem como o desenvolvimento de cuidados médicos inteligentes [6].

B. Desafios de Segurança na Implementação do 5G

A implantação das redes 5G busca prover conexão a bilhões de sensores e milhões de dispositivos, representando um investimento com impactos significativos globais. Dada essa influência, a resolução de questões de segurança torna-se uma prioridade crucial para empresas, investidores, pesquisadores e usuários individuais. O aumento esperado no número e diversidade de dispositivos conectados naturalmente amplia a superfície de ataques para hackers explorarem a rede em diversas camadas do modelo OSI, assim como a diversidade de serviços. Embora a criptografia baseada em aplicações ofereça proteção, ela não é adequada para assegurar dados que transitam pelas redes móveis 5G, devido ao vazamento de informações na sinalização sem fio [8].

Adicionalmente, as redes 5G incorporam uma variedade de tecnologias de suporte, como NFV, MEC, SDN, fatiamento de redes, dentro de uma arquitetura baseada em serviços, tornando-as mais complexas de gerenciar, com maior escopo de ataque e risco de segurança. Neste sentido, tem-se promovido o uso intenso de IA tanto para gerenciamento e operação da rede e serviços, quanto na composição de soluções de segurança. Entretanto, apesar de suas vantagens, elas também podem sofrer ataques, os chamados ataques adversariais [7] . Assim, as redes 5G exigirão abordagens distintas em termos de técnicas criptográficas, com soluções viáveis no domínio [8].

Por exemplo, os autores de [9] destacam a necessidade de soluções de segurança personalizadas para garantir a integridade, confidencialidade e autenticação de dados em redes 5G. À medida que as aplicações implementam sensores e atuadores em ambientes totalmente inteligentes, a segurança envolve a proteção integral da arquitetura de implantação contra ameaças internas e externas. Garantir a segurança dos dados em redes 5G, a detecção de nós confiáveis e maliciosos, o monitoramento adequado, o registro e a transmissão são requisitos essenciais para qualquer sistema de segurança.

C. Telecirurgia robótica

A telecirurgia emprega redes sem fio e tecnologia robótica para viabilizar a realização de cirurgias por parte de cirurgiões em locais distantes. Esta tecnologia não apenas alivia a atual escassez de cirurgiões, mas também supera barreiras geográficas que dificultam a intervenção cirúrgica oportuna e de alta qualidade, reduzindo a carga financeira, minimizando complicações e eliminando a necessidade de viagens arriscadas de longa distância. Além disso, o sistema proporciona uma precisão cirúrgica aprimorada e assegura a segurança dos cirurgiões [1].

Os requisitos tecnológicos para o sucesso da telecirurgia robótica são diversos, entre os quais está a necessidade de criação de um ambiente imersivo seguro e eficiente, com sistema de comunicação confiável, de baixa latência e suporte a vídeos de alta definição [10]. Esse ambiente deve garantir a interação transparente entre os componentes críticos da cirurgia, reduzindo os riscos de falhas técnicas em eventos cirúrgicos. Nesse sentido, redes com taxa de dados alta e baixa latência são cruciais para prover a transmissão de vídeos para os cirurgiões e transmitir os comandos para os robôs. Geralmente, em condições comuns, o tempo de reação humana dos sentidos de audição, visão e tato são da ordem de 100 ms, 40 ms e 1ms, respectivamente. Assim, qualquer infraestrutura para telecirurgia robótica deve imitar esses valores [10].

Além de aspectos de desempenho, a privacidade e segurança dos dados são cruciais na prática médica. Transmitir dados e imagens entre instituições remotas expõe os dados dos pacientes a ameaças de segurança, bem como ao acesso não autorizado. Ataques cibernéticos são ameaças potenciais em telecirugias, podendo acontecer de formas múltiplas (ex. negação de serviço, captura de pacotes) e endereçar os diferentes componentes do ambiente telecirgurico (ex. atuadores, sensores, braços robóticos e rede de comunicação) [11].

D. 5G, telecirurgia robótica e segurança

O uso de sistemas de telecirurgia robótica na rede pública expõe riscos significativos de segurança e privacidade, podendo impactar a eficácia das operações e a segurança dos pacientes. A ameaça inclui a possibilidade de sequestro remoto por programas maliciosos, realização de tarefas não autorizadas e ataques de negação de serviço. A implementação de medidas de segurança, como controle de acesso e autenticação, é crucial. No entanto, equilibrar a segurança com os requisitos de atraso e instabilidade na telecirurgia é um desafio, pois

a criptografia e os protocolos de segurança podem gerar sobrecarga na comunicação, afetando a qualidade do serviço. O projeto de esquemas de criptografia e segurança para sistemas de teleoperação em tempo real é um desafio em aberto que exige considerações cuidadosas [12]. Assim, verificar a perspectiva atual de segurança no cenário de redes 5G e a telecirurgia robótica é um imperativo.

III. Metodologia

Para investigar o emprego de segurança na adoção de redes 5G no âmbito da saúde, com ênfase na telecirurgia robótica, realizou-se uma Revisão Sistemática da Literatura. O protocolo utilizado é apresentado a seguir.

A. Questões da pesquisa

O principal objetivo desse trabalho é obter uma perspectiva sobre a segurança na aplicação de redes 5G no cenário de telecirurgia robótica. Com esse objetivo, duas Questões de Pesquisa (QP) principais foram definidas, conforme a seguir:

QP1: Uma vez que a telecirurgia robótica é uma atividade em tempo real, com requisitos estritos de latência e confiabilidade, as tecnologias aplicadas para atendimento desses requisitos atendem também aos requisitos de segurança?

Justificativa: Deseja-se saber como a segurança é empregada em sistemas de telecirurgia robótica.

QP2: Quão o nível de preocupação com a segurança na adoção de sistemas que usam redes 5G para telecirurgia robótica e quais as ameaças de segurança reportadas nesse cenário?

Justificativa: Deseja-se entender a preocupação dos pesquisadores sobre a segurança no uso de redes 5G para a telecirurgia.

B. String de pesquisa e fontes de dados

Com base nas questões de pesquisa, foram identificadas palavras-chave que orientaram a formulação das duas strings de busca. As palavras-chave e seus sinônimos foram estruturados de acordo com uma forma normal conjuntiva. A string de busca relacionada a telecirurgia robótica é: (“5G“ OR “fifth generation“) AND (“robotic telesurgery“ OR “telesurgery“) AND (“security“ OR “cyber security“ OR “cyber defense“). Como o tema de pesquisa é muito específico, optou-se por buscar uma string de pesquisa geral para aumentar o número de trabalhos relevantes. Para responder às questões de pesquisa, consideramos publicações indexadas por fontes de dados nas seguintes bases científicas: IEEE Xplore, ACM Digital Library, Science Direct, SpringerLink e PubMed.

C. Procedimento de seleção

Para selecionar publicações relevantes para responder às nossas questões de pesquisa, seguimos um procedimento de seleção que compreende cinco etapas. Esse procedimento foi aplicado por um pesquisador, que foi responsável pela execução das cinco etapas. Como citado anteriormente, foi escolhido um tema principal para pesquisa, relacionado a telecirurgia robótica. A Fig. 1 ilustra as etapas do fluxo de seleção. Na Etapa 1, a string de busca foi aplicada nas bases de dados científicas selecionadas em 01/12/2023. A busca recuperou um total de 124 publicações organizadas da seguinte forma: 6 (IEEE Xplore), 18 (ACM Digital Library), 54 (Science Direct), 45 (SpringerLink) e 2 (PubMed). Seguindo, na etapa 2, todos os resultados foram agrupados e as duplicatas removidas, totalizando 124 estudos relacionados a telecirurgia robótica.

Nas fases subsequentes, os estudos foram meticulosamente filtrados de acordo com critérios predefinidos de inclusão e exclusão, seguindo uma abordagem uniforme e imparcial. Os critérios de inclusão compreendiam a seleção de (i) artigos individuais, (ii) estudos que descrevem a aplicação de 5G com telecirurgia robótica e abordem o tema de segurança, (iii) publicações desde o lançamento da primeira rede 5G em 2019 até 2023, (iv) estudos escritos em inglês e (v) aqueles disponíveis na íntegra. Em contraste, os critérios de exclusão consistiam em não considerar (i) anais, índices e documentos análogos, (ii) artigos de dimensões reduzidas (com menos de duas páginas), (iii) publicações não alinhadas aos objetivos do presente estudo, (iv) estudos publicados antes de 2019 e (v) estudos em idiomas distintos do inglês.

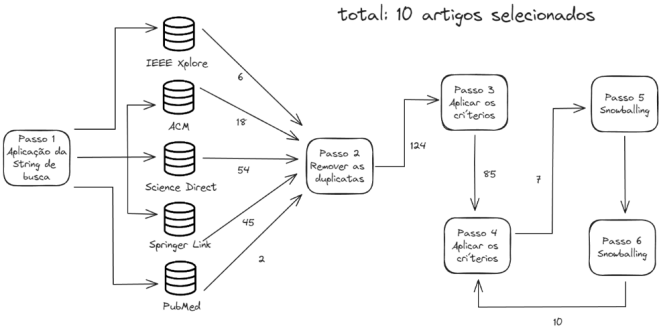

Fig. 1. Procedimento de Seleção dos Estudos.

Na etapa 3 realizou-se a leitura do título e resumo de cada artigo e a aplicação dos critérios de inclusão e exclusão. Esta etapa selecionou 85 publicações entre os 124 estudos retornados na etapa 2. A etapa 4 aplicou os critérios de inclusão e exclusão aos 85 estudos selecionados na etapa anterior, mas desta vez após a análise das seções inicial e final de cada artigo, compreendendo a introdução e a conclusão. Além disso, foi realizada ainda uma filtragem rápida por palavras-chave como “telesurgery” e “security” nos artigos, com o intuito de acelerar o processo de filtragem. Este estágio de filtragem reduziu o conjunto de estudos desta RSL para 7 publicações relacionadas ao tema da pesquisa. Na etapa 5 procedeu-se a leitura integral dos artigos a adicionalmente foram incluídos 3 novos estudos baseados referências das publicações selecionadas (snowballing) com a análise deles na etapa 6. Ao final, foram identificadas 10 publicações nesta RSL para responder às questões de pesquisa colocadas.

IV. Resumo dos Estudos Selecionados

O resultado da seleção abrange trabalhos publicados entre 2019 a 2022, com a maioria sendo de 2020 e nenhum de

TABLE I
ESTUDOS SELECIONADOS.

ID	Ano	Autores	Tipo	Ref.
EP1	2022	Moglia, Andrea, et al.	J	[13]
EP2	2022	Alekseeva, Daria, et al.	J	[14]
EP3	2022	Rohde, Jannik, et al.	C	[15]
EP4	2022	Navarro, Emmanuel M. et al.,	C	[16]
EP5	2020	Asif, M. R. A., and R. Khondoker.	C	[17]
EP6	2020	Gupta, Rajesh, et al..	C	[3]
EP7	2020	Tiwari, Kumud, et al..	C	[18]
EP8	2019	Gupta, Rajesh, et al.	C	[19]
EP9	2019	Iqbal, Sohail, et al.	J	[20]
EP10	2018	Zhang, Q., et al.	C	[12]

*Conferências (C) ou Periódicos (J)

2023. Sete artigos foram publicados em conferências e três em periódicos. A Tabela I fornece detalhes bibliográficos dos 10 estudos primários (EP) selecionados. A seguir, apresenta-se um resumo de cada estudo primário (EP) selecionado, enfatizando suas principais características.

O EP1 [13] afirma que para o sucesso da implantação da telecirurgia, a latência entre o operador e o equipamento é fundamental, onde o ideal é que seja menor que 100 ms, evitando problemas como manipulação imprecisa, que podem surgir com latência maior que 300ms. Os autores ressaltam que os riscos de cibersegurança evoluem ao longo do tempo e, consequentemente, a eficácia dos controles de segurança cibernética pode se degradar à medida que novos riscos, ameaças e métodos de ataque surgem. Eles consideram que computação quântica e blockchain são essenciais para lidar com os problemas de segurança em redes 5G. Por exemplo, eles citam que os sistemas de segurança propostos atualmente baseiam-se na Criptografia Pós-Quântica (PQC), sendo considerados inquebráveis e o blockchain tem um potencial considerável para proteger dados para aplicações na área da saúde, embora a adoção de blockchain em uso clínico seja limitada atualmente.

O EP2 [14] destaca que a telecirurgia robótica requer a operação do serviço e comunicações de alta precisão e alta confiabilidade para fornecer cirurgias minimamente invasivas, onde atrasos excessivos podem ser fatais. Assim, a latência não pode ultrapassar 0,75 ms e a disponibilidade tem que ser superior a 99.9999%. Para isso, é recomendado que a computação seja realizada próxima ao usuário, ou seja, na borda. Em termos de segurança, os autores ressaltam que o paradigma de Fog Computing (FOG) geralmente fornece melhores serviços de segurança e privacidade para endpoints. Entretanto, algumas características do FOG, como descentralização, restrições de recursos, homogeneidade e sistemas virtualizados, ainda são vulneráveis a uma grande variedade de problemas de segurança e privacidade em comparação com a computação em nuvem centralizada. Adicionalmente, a falta de padronização das contramedidas, medidas de segurança e proteção de dados altamente efetivas na maioria dos paradigmas computacionais inviabiliza adoção e integração delas no domínio da saúde.

O EP3 [15] ressalta que casos de uso exigentes e de missão crítica, como a telecirurgia, têm requisitos desafiadores, como baixa latência e alta confiabilidade do canal de comunicação, que podem ser atendidos pelas redes 5G. Os autores apresentam uma arquitetura 5G para a teleoperação de um robô industrial a longa distância. O ambiente de teste utilizado pelo autor inclui três institutos localizados na Alemanha. Dois deles possuem redes privadas de campus 5G, que operam nas faixas de frequência de 3.73,8 MHz, no modo standalone (SA) e suportam a Release 15 em duas delas. A conexão entre todos os institutos é construída pela internet pública. Para garantir a segurança dos dados transmitidos, o OpenVPN também é usado como uma rede privada virtual (VPN). Devido aos algoritmos de criptografia implementados, a conexão é mais lenta, porém mais segura do que uma conexão direta com a Internet entre o controlador e o dispositivo. Para resolver o problema de segurança ao usar uma conexão direta com a internet, os dispositivos têm que fornecer medidas de segurança, como autenticação forte, autorização de acesso, criptografia e falhas de segurança constantemente corrigidas no software.

O EP4 [16] oferece uma breve revisão histórica e tendências futuras da telecirurgia. Ele propõe um valor que pode facilitar a prática da telecirurgia em unidades médicas remotas. O estudo foca nas implementações e benefícios que as redes 5G podem proporcionar ao desenvolvimento da telecirurgia como oportunidade de desenvolvimento da práxis médica ligada ao crescimento acelerado das redes de alta velocidade no mundo conectado. Quanto à segurança, os autores citam que a telecirurgia precisa se aprofundar em protocolos de segurança que protejam o fluxo de informações em ambientes adversos, descontrolados e hostis. Informações confidenciais e até mesmo a vida dos pacientes podem ser comprometidas devido a ataques cibernéticos e que inovações em criptografia precisam ser implementadas para garantir a segurança dos procedimentos.

O EP5 [17] pontua que embora a telecirurgia permita que os cirurgiões realizem procedimentos em pacientes remotamente com o avanço de robôs cirúrgicos e tecnologias de comunicação em rede, há problemas potenciais, como a latência de comunicação e a segurança cibernética. Alguns pesquisadores destacam que o uso das redes 5G é uma mudança radical na redução da latência. Entretanto, a segurança cibernética para proteger o sistema de telecirurgia dos invasores ainda é uma questão em aberto. Neste aspecto, os autores aplicam o método de modelagem de ameaças da Microsoft chamado STRIDE para identificar e enumerar ameaças. Ao fim do estudo, eles identificam, categorizam e enumeraram quarenta e oito ameaças à segurança cibernética de um sistema genérico de telecirurgia.

O EP6 [3] indica que a telecirurgia com Internet Tátil assistida pela rede 5G tem um potencial grande para fornecer serviços cirúrgicos ultra responsivos em tempo real, de forma remota, com qualidade e precisão altas, o que é benéfico para a sociedade na perspectiva de diagnósticos cirúrgicos de alta precisão. No entanto, os sistemas de telecirurgia existentes têm problemas de segurança, privacidade, latência e custo de

armazenamento de blockchain, restringindo sua aplicabilidade em procedimentos cirúrgicos em curto prazo. Para mitigar tais problemas, os autores propõem uma abordagem chamada AaYusH - Ethereum Smart Contract (ESC) e sistema de telecirurgia baseado em InterPlanetary File System (IFPS). Os problemas de segurança e privacidade no AaYusH podem ser resolvidos por meio do ESC, enquanto os problemas de custo de armazenamento via protocolo IPFS. Os autores avaliam o desempenho do AaYusH em termos de latência e custo de armazenamento de dados, onde os resultados mostram que a solução proposta supera o sistema de telecirurgia tradicional.

Em EP7 [18], os autores citam que a telecirurgia tem uma perspectiva de fornecer serviços médicos urgentes e surgiu com diferentes oportunidades para fornecer médicos altamente qualificados globalmente. Neste aspecto, a telecirurgia requer tecnologias como redes 5G, internet tátil e IA para reduzir problemas de escalonamento de recursos. Os autores realizam uma análise tecnológica da telecirurgia robótica baseada nestas três tecnologias e propõem uma estrutura padronizada que implementa o conceito de camada FOG para reduzir a latência e superar os desafios de escalabilidade, ambientes controlados, interoperabilidade e reduzir o custo da telecirurgia.

Em EP8 [19] os autores destacam que o sistema de telecirurgia atual enfrenta desafios de segurança, privacidade e interoperabilidade, limitando sua utilidade a centros de saúde globalmente no futuro. Para endereçar esses problemas, propõem uma estrutura chamada HaBiTs (Telecirurgia Interoperável Baseada em Blockchain), onde a segurança é garantida pela imutabilidade e interoperabilidade por meio de Contratos Inteligentes (SCs). Os SCs são códigos escritos em Solidity ou outras linguagens de blockchain para estabelecer confiança entre todas as partes conectadas e eliminar a necessidade de intermediários para compartilhamento de dados. Dessa forma, o HaBiTs é uma estrutura de telecirurgia segura baseada em blockchain, que gerencia de forma segura a saúde, eliminando a dependência de intermediários para estabelecer confiança entre especialistas e organizações de saúde. A natureza distribuída do blockchain elimina a necessidade de autenticação multinível, melhorando o desempenho do sistema e reduzindo os custos de serviços de saúde. Além disso, eles argumentam que o HaBiTs resolve vários problemas de segurança e privacidade do sistema de telecirurgia tradicional, como acesso instantâneo a dados, interoperabilidade do sistema, segurança e consistência de dados, além de redução de custos.

Já o EP9 [20] propõe um framework, chamado SecureSurgiNET, para garantir a segurança em ambientes de telecirurgia, denotado de SecureSurgiNET. Ele é baseado principalmente em um conjunto de protocolos bem estabelecidos para fornecer um sistema robótico telecirúrgico livre de falhas. Para aumentar a eficiência de ambientes de telecirurgia seguros, os autores introduzem a ideia de uma autoridade de telecirurgia, que garante a integridade, o gerenciamento de identidade, a implementação de políticas de autenticação e a segurança dos dados pós-operatórios. Além disso, o uso de certificados digitais garante autenticação forte e protege contra ataques de mascaramento e repetição. A implementação de políticas apropriadas, regras de autorização e gerenciamento de identidade reforça o sistema contra o sequestro de sessão. Por fim, os autores fornecem uma análise descrevendo a segurança e a taxa de transferência do Advanced Encryption Standard (AES) durante a fase intraoperatória do SecureSurgiNET. Além disso, eles listam os possíveis ataques ao SecureSurgiNET juntamente com as medidas defensivas elaboradas.

Por fim, o EP10 [12] frisa que a telecirurgia robótica tem potencial para fornecer serviços de saúde extremos e urgentes e trazer oportunidades sem precedentes para fornecer competências altamente especializadas mundialmente. No entanto, ressaltam que o desempenho da telecirurgia robótica atualmente depende na maioria do desempenho da rede em termos de latência, jitter e perda de pacotes, especialmente quando o sistema telecirurgião está equipado com feedback tátil. Quanto à segurança, os autores ressaltam que devem ser implementados esquemas de segurança para controle de acesso, autenticação, confidencialidade e integridade de dados. Embora a segurança da rede de comunicação e do sistema ciberfísico tenha sido avançada, é um desafio fornecer simultaneamente segurança e cumprir os requisitos de atraso e estabilidade na telecirurgia, uma vez que a criptografia e os protocolos de segurança consomem recursos computacionais e introduzem sobrecarga de comunicação.

V. Resultados e Discussões

Esta seção apresenta os aspectos de segurança (preocupações) no uso das redes 5G para a telecirurgia robótica e ressalta as soluções propostas. Por exemplo, os trabalhos [13] e [16] destacam a importância do atendimento do requisito de latência na telecirurgia, indicando valores menores 100ms para garantir operações precisas. Além disso, indicam o potencial do 5G para impulsionar o desenvolvimento da telecirurgia, enfatizando a importância de abordagens de segurança eficazes. Nesse último ponto, [16] ressalta a necessidade de protocolos de segurança que protejam contra ameaças cibernéticas, evidenciando a necessidade de inovações em criptografia para garantir a segurança dos procedimentos. Já [13] aletar para a evolução contínua dos riscos de cibersegurança, recomendando o uso de computação quântica no enfrentamento dessas questões em redes 5G.

Já [18] e [12] destacam a perspectiva da telecirurgia robótica baseada em redes 5G e Internet Tátil, onde [18] apresenta uma estrutura padronizada que utiliza a camada FOG para superar desafios de latência, escalabilidade e custos, e reconhece a necessidade de tecnologias inovadoras para resolver os problemas de escalonamento de recursos. Ao passo que [12] foca nos desafios de desempenho da rede, especialmente quando equipada com instrumento de retroalimentação tátil. Adicionalmente, ele ressalta a importância de esquemas de segurança para controle de acesso, autenticação e confidencialidade, reconhecendo os desafios associados à criptografia na telecirurgia.

Na linha de requisitos de desempenho, [17] destaca a importância das redes 5G na redução da latência para a telecirurgia, reconhecendo, no entanto, os desafios persistentes em segurança cibernética. Já [15] propõe uma arquitetura 5G para teleoperação de robôs industriais, destacando a aplicação prática em casos de uso exigentes. Além disso, ressalta a importância da segurança dos dados transmitidos e utilizam uma conexão VPN para garantir a confidencialidade deles e sublinhando a necessidade de medidas de segurança nos dispositivos para mitigar potenciais ameaças. [14], por sua vez, aponta desafios de segurança relacionados à descentralização e as restrições de recursos no paradigma de FOG, chamando a atenção para a necessidade de padronização de medidas.

O uso de blockchain e contratos inteligentes é destacado em [3] e [19]. O primeiro destaca o uso combinado dessas tecnologias para melhorar a segurança e privacidade na telecirurgia, mas ressalta os problemas de segurança, privacidade e custo de armazenamento, oferecendo solução para estes desafios. O [19], por sua vez, propõe o uso conjunto para melhorar a segurança e interoperabilidade na telecirurgia, e apresenta o framework HaBiTs, que endereça problemas de segurança, privacidade e interoperabilidade, destacando a natureza distribuída do blockchain como benéfica para a saúde.

Por fim, [20] destaca a importância de uma autoridade de telecirurgia para garantia de integridade, gerenciamento de identidade e segurança dos dados pós-operatórios, e propõe um framework para lidar com esses desafios.

VI. Conclusão

A evolução dos robôs cirúrgicos e o surgimento das redes 5G tem impulsionado as telecirgurgias robóticas, que apresenta um grande potencial para superar as barreiras geográficas e melhorar os cuidados médicos dos pacientes. Entretanto, os desafios relacionados à segurança e à proteção de dados neste novo tipo de rede podem impactar o serviço dessa aplicação crítica e precisam ser considerados na implantação de sistemas telecirúrgicos. Neste sentido, este trabalho apresentou uma revisão sistemática da literatura, que buscou fornecer um panorama das implicações de segurança inerentes à implementação das redes 5G no contexto da saúde, com foco especial em telecirurgia robótica. O mapeamento não apenas revelou as características e desafios desse campo, mas também apontou direções e estratégias que endereçam as questões de segurança.

Por exemplo, abordagens para segurança em telecirurgia robótica, como a adoção de blockchain e contratos inteligentes, proposta de frameworks, além de soluções simples, como o uso de VPNs, foram identificadas. Uma parte dos estudos primários destacou a segurança como um fator importante na telecirurgia, mas sem propor solução. Nesse aspecto, evidencia-se a necessidade de desenvolvimento de soluções de segurança para a aplicação das redes 5G como suporte a telecirurgia robótica, além da exploração de todo o potencial do uso da telecirurgia em redes 5G. Como direções futuras, apontam-se o desenvolvimento e validação de soluções de segurança focadas nos requisitos de telecirurgia robótica em redes 5G e a análise do impacto da adoção de técnicas de inteligência artificial no suporte aos sistemas de telecirurgia robótica.

Agradecimentos

Este estudo foi financiado pela Coordernaçao de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código 001. Este trabalho foi apoiado pelo projeto de cooperação em pesquisa e inovação entre a Softex (financiado pelo Ministério da Ciência, Tecnologia e Inovação através da Lei 8.248/91 no âmbito do Programa Prioritário Nacional) e o CIn-UFPE. Ele também contém resultados do Projeto AMAN, executado pelo Sidia Instituto de Ciência e Tecnologia em parceria com Samsung Eletrônica da Amazônia LTDA, de acordo com a Lei de Informática n.8387/91 e Art. 39 do Decreto 10.521/2020.

References

[1] Choi, Paul J., et al. "Telesurgery: past, present, and future." Cureus 10.5 (2018).

[2] Oliveira, Vítor M., et al. "Exploring current communication frameworks for medical teleoperation." 2021 IEEE 9th International Conference on Serious Games and Applications for Health (SeGAH). IEEE, 2021.

[3] Gupta, Rajesh, Arpit Shukla, and Sudeep Tanwar. "Aayush: A smart contract-based telesurgery system for healthcare 4.0." 2020 IEEE International conference on communications workshops (ICC Workshops). IEEE, 2020.

[4] Filippou, Miltiades C., et al. "Multi-access edge computing: A comparative analysis of 5G system deployments and service consumption locality variants." IEEE Communications Standards Magazine 4.2 (2020): 32-39.

[5] Dangi, Ramraj, et al. "Study and investigation on 5G technology: A systematic review." Sensors 22.1 (2021): 26.

[6] Javaid, Mohd, et al. "5G technology for healthcare: Features, serviceable pillars, and applications." Intelligent Pharmacy (2023).

[7] C. Benzaïd and T. Taleb, "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?," in IEEE Network, vol. 34, no. 6, pp. 140-147, November/December 2020, doi: 10.1109/MNET.011.2000088

[8] Sullivan, S., et al. "5G security challenges and solutions: a review by OSI layers." IEEE Access 9 (2021): 116294-116314.

[9] Kumar, G. Edwin Prem, M. Lydia, and Yoash Levron. "Security challenges in 5G and IoT networks: A review." Secure Communication for 5G and IoT Networks (2022): 1-13.

[10] Patel, V., Saikali, S., Moschovas, M.C. et al. Technical and ethical considerations in telesurgery. J Robotic Surg 18, 40 (2024). https://doi.org/10.1007/s11701-023-01797-3

[11] Bonaci, Tamara et al. "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots." ArXiv abs/1504.04339 (2015)

[12] Zhang, Q., J. Liu, and G. Zhao. "Towards 5G Enabled Tactile Robotic Telesurgery. 2018; 1-7." (2021).

[13] Moglia, Andrea, et al. "5G in healthcare: from COVID-19 to future challenges." IEEE Journal of Biomedical and Health Informatics 26.8 (2022): 4187-4196.

[14] Alekseeva, Daria, et al. "The future of computing paradigms for medical and emergency applications." Computer Science Review 45 (2022): 100494.

[15] Rohde, Jannik, et al. "Teleoperation of an Industrial Robot using Public Networks and 5G SA Campus Networks." 2022 Sixth IEEE International Conference on Robotic Computing (IRC). IEEE, 2022.

[16] Navarro, Emmanuel Mendoza, Adrielly Nahomee Ramos Álvarez, and Francisca Irene Soler Anguiano. "A new telesurgery generation supported by 5G technology: benefits and future trends." Procedia Computer Science 200 (2022): 31-38.

[17] Asif, M. R. A., and R. Khondoker. "Cyber Security Threat Modeling of A Telesurgery System." 2020 2nd International Conference on Sustainable Technologies for Industry. Vol. 4. 2020.

[18] Tiwari, Kumud, Sachin Kumar, and R. K. Tiwari. "FOG assisted healthcare architecture for pre-operative support to reduce latency." Procedia Computer Science 167 (2020): 1312-1324.
[19] Gupta, Rajesh, et al. "Habits: Blockchain-based telesurgery framework for healthcare 4.0." 2019 international conference on computer, information and telecommunication systems (CITS). IEEE, 2019.
[20] Iqbal, Sohail, et al. "SecureSurgiNET: A framework for ensuring security in telesurgery." International Journal of Distributed Sensor Networks 15.9 (2019): 1550147719873811.