Requisitos e Desafios de Segurança e Privacidade em Redes 6G

Cleitianne O. Silva[1], **Antonia Raiane S. Araujo Cruz**[1 2], **Rossana M. C. Andrade**[1], **Emanuel B. Rodrigues** [1]

[1]Universidade Federal do Ceará (UFC)

[2]Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

{cleitianne, raiane.santos}@alu.ufc.br, {rossana, emanuel}@dc.ufc.br,

Abstract. *The 6th generation of mobile networks will enable heterogeneous device communication, deep use of Artificial Intelligence, and also facilitate several new use cases. However, they must ensure real-time security and privacy, and differential and distributed data protection mechanisms. In this sense, this paper presents the main security and privacy challenges in 6G, summarizing their security requirements and the threats that can exploit their vulnerabilities.*

Resumo. *O avanço da 6ª geração de redes móveis possibilitará a comunicação de dispositivos heterogêneos, uso profundo da Inteligência Artificial e também facilitará novos casos de uso. Contudo, deverá garantir segurança e privacidade em tempo real, e mecanismos de proteção de dados diferenciais e distribuídos. Nesse sentido, este trabalho consiste em apresentar os principais desafios de segurança e privacidade em 6G, sumarizando os requisitos de segurança e as ameaças que exploram as vulnerabilidades.*

1. Introdução

A 6ª geração de redes móveis (6G) já define alguns casos de uso, principalmente no que se refere às suas características primordiais como inteligência nas redes de telecomunicações e redes avançadas com profunda aplicação de Inteligência Artificial (IA). Porém, as questões de segurança e privacidade em 6G ainda são um desafio. Para isso, é necessário pensar em mecanismos unindo também a tecnologia *Blockchain*, que oferece mecanismos que poderão tratar de forma mais eficiente essas questões [Abdel Hakeem et al. 2022].

Atualmente, com o 5G, aplicações de dados intensivos que tem como exigência elevadas taxas de dados foram beneficiadas [Ji et al. 2021], embora as especificações do 5G ainda estejam em processo de implementação e a cobertura parcial. Contudo, a sociedade demanda cada dia mais a evolução tecnológica no que se refere a mecanismos inteligentes [De Alwis et al. 2021].

Espera-se um crescimento exponencial do volume de dados móveis global até 2030, em torno de 5 zettabytes (ZB) por mês, conforme a pesquisa [ITU 2023]. Por conseguinte, o avanço da Internet das Coisas (*Internet of Things - IoT*) e o advento da Internet de Tudo (*Internet of Everything - IoE*) possibilita novas tecnologias promissoras.

Entretanto, as pesquisas em sistemas 6G ainda estão em estágio inicial e os principais serviços e tecnologias ainda passam por investigações [Porambage et al. 2021]. Com isso, é importante destacar que para a consolidação das redes 6G, os aspectos de segurança

e privacidade devem estar bem solidificados, considerando o impacto nas aplicações 6G previstos com os potenciais desafios das gerações anteriores e os desafios que surgirão com a implementação dos casos de uso 6G. Nesse contexto, o objetivo central deste trabalho é sintetizar os principais desafios de segurança e privacidade das diferentes aplicações ou serviços 6G, bem como os desafios mais latentes das tecnologias em 6G como IA e *Blockchain*.

2. Requisitos e Desafios de Segurança e Privacidade em Redes 6G

2.1. Requisitos 6G

A cada nova geração de telefonia celular é importante atualizar arquiteturas de segurança que satisfaçam os novos requisitos, tais como arquitetura colaborativa de confiança zero, nova autenticação e gestão de chaves, a fim de enfrentar os desafios diante das novas aplicações e modelos de negócio [Nguyen et al. 2021]. Com o 6G, tem-se requisitos[1] mais rigorosos com necessidade de aumento considerável de recursos de rede, como ilustrado na Figura 1.

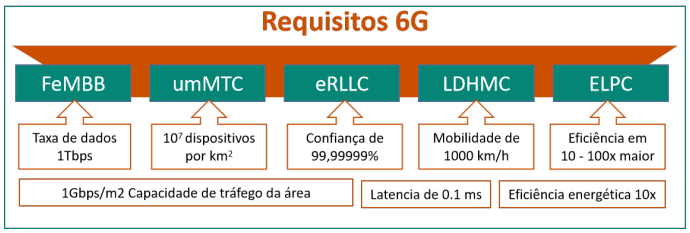

Figura 1. Requisitos 6G.

O estudo realizado em [Porambage et al. 2021] destaca que com o crescimento do número de dispositivos conectados que se comunicam entre si e com a infraestrutura, outro requisito que aparece é a oferta de serviços colaborativos de maneira autônoma e autodirigida.

2.2. Requisitos de Segurança

O avanço do 6G efetivará novos cenários de migração dos serviços de segurança [Nguyen et al. 2021]. A Figura 2 apresenta a taxonomia de segurança 6G e destaca os principais requisitos de segurança que são definidos com o intuito de suportar uma variedade de casos de uso importantes do 6G. Esses requisitos [Porambage et al. 2021] são classificados como: confidencialidade e integridade ultra-alta, segurança automatizada de toque zero, privacidade dos assinantes, segurança ultraleve, segurança em tempo real e eficiência energética.

Os requisitos de segurança em 6G evoluíram diante dos desafios recorrentes das novas tecnologias e dos novos casos de uso, porém é notável que dos requisitos de segurança apresentados na Figura 2, destacam-se a proteção de segurança em tempo real e a total automatização da segurança como requisitos chaves, conforme afirma [Nguyen et al. 2021].

[1]FeMBB: further-enhanced mobile broadband; ERLLC: extremely reliable and low-latency communications; LDHMC: long-distance and high-mobility communications; ELPC: extremely low-power communications; umMTC: ultra-massive machine-type communications.

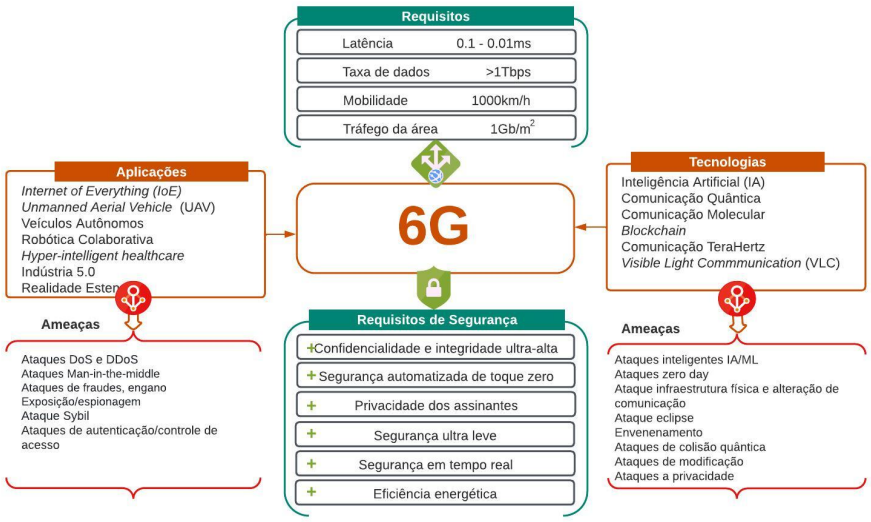

Figura 2. Taxonomia de Segurança 6G (Adaptado de [Porambage et al. 2021] e [Nguyen et al. 2021]).

Para além disso, a Figura 2 também busca abordar as principais tecnologias e os desafios ainda em aberto, assim como nas aplicações 6G (detalhado nas seções 2.3 e 2.4), de forma a listar as ameaças mais comuns.

2.3. Desafios de Segurança das Tecnologias 6G

Considerando que os futuros casos de uso 6G terão requisitos rigorosos e exigirão mais recursos de rede do que as atuais redes 5G, diversos problemas de segurança existentes como roubo de informações, *Denial of Service (DoS)*, *Distributed Denial of Service (DDoS)* e *Man-In-The-Middle (MITM)*, que são ataques comuns, também afetarão as redes 6G. Além disso, irão recorrer aos desafios relacionados a *Software Defined Network (SDN)* que podem incluir vulnerabilidades no controlador do SDN e ataques nas máquinas virtuais e até mesmo em seus gerenciadores em se falando da Virtualização das Funções da Rede (*Network Functions Virtualization* - NFV).

Ao contrário das redes móveis anteriores, 6G suportará larga aplicação de serviços IA para uma tomada de decisão ágil e inteligente [Letaief et al. 2021]. Deste modo, a IA em 6G pode ser aplicada como mecanismo de segurança para a implementação de detecção de intrusões, análise de tráfego, detecção de ataques, *botnets* e *malwares* diversos e criptografia. Assim, como o tráfego deve ser tratado local e dinamicamente em vários segmentos de rede, as soluções de segurança distribuídas podem ajudar a aliviar esses problemas.

Ainda assim, mesmo onde a IA é responsável por proporcionar a inteligência conectada para o 6G, também são encontrados desafios de segurança e privacidade [Siriwardhana et al. 2021], especialmente os sistemas ML (*Machine Learning)*, os quais estão sujeitos a sofrer ataques de envenenamento, injeção, manipulação dos dados e corrupção lógica, além das possibilidades de extração e inversão de modelo.

Utilizadas inicialmente para atingir uma velocidade de transmissão em Tbps, as comunicações terahertz são bandas de frequência que podem suportar altas taxas de trans-

missão, além de um robusto controle de interferência, integração simples de detecção e comunicações [Abdel Hakeem et al. 2022]. Entretanto, essa tecnologia também apresenta alguns problemas, como comportamentos anormais, difícil gestão de espionagem e ataques de captura de sinais, como definido em [Katz and Ahmed 2020].

Outra tecnologia com vasta aplicação em 6G é a comunicação quântica (*Quantum communications*), com a vantagem de poder aumentar significativamente a segurança e fiabilidade da transmissão de dados, através da tecbologia *Quantum Key Distribution* - QKD [Wang et al. 2020], entretanto a integração de soluções criptográficas resistentes a ataques, erros de atenuação e operação ainda são um desafio. Problemas como ataques de clonagem quântica, questões de privacidade no canal de comunicação e criptografia quântica já são objetos de estudos, no sentido de envio de mensagem sem a necessidade de utilizar chaves privadas e mecanismos de proteção para a distribuição de chaves quânticas.

As futuras redes de comunicação devem usar a tecnologia *Blockchain* para gerenciar grandes quantidades de dados onde cada bloco é estruturado e protegido por criptografia. Entretanto, desafios como vulnerabilidade da maioria, que ocorre quando o *Blockchain* constrói confiança sem a necessidade de terceiros, exigindo um consenso da maioria dos participantes.

Outros desafios relacionados ao *Blockchain* são os gastos duplos que são um tipo de ataque que visa quebrar a integridade do livro-razão distribuído com criptomoedas, quando um usuário conclui duas transações distintas com a mesma quantidade de moeda. Por fim, o vazamento de privacidade de transações do *Blockchain* é outro desafio. Isto porque depende de transações transparentes, logo essa tecnologia pode comprometer a privacidade de usuários [Nguyen et al. 2020].

A comunicação molecular (*Molecular Communication*), definida em [Porambage et al. 2021], é uma tecnologia muito promissora para as comunicações 6G, principalmente nas inovações de cuidados de saúde. Envolve nanotecnologia e comunicação das bio nanomáquinas através de sinais químicos. No entanto, já foram encontradas várias questões de segurança e privacidade, autenticação e encriptação [Wang et al. 2020]. Daí a importância de discussões a respeito de criptografia bioquímica.

Por fim, a tecnologia de comunicação por luz visível (*Visible Light Communication Technology - VLC*), que embora seja uma abordagem promissora em 6G, já vem sendo estudada há alguns anos e já implantada em sistemas como redes VANETs (*Vehicular Ad Hoc Network*), mas ainda assim perdura questões como comportamentos maliciosos e espionagem [Abdel Hakeem et al. 2022] [Katz and Ahmed 2020].

2.4. Desafios de Segurança das Aplicações 6G

As redes veiculares (*Vehicle and Unmanned Aerial Vehicle* - UAV) requerem requisitos como latência extremamente baixa e inteligência em tempo real, o que impossibilitou sua aplicação ainda no 5G. Sua implementação no 6G é acompanhada ainda de alguns problemas de segurança críticos, visto que diferentemente de outras aplicações, os UAVs são extremamente dinâmicos, de alta mobilidade e incontroláveis [Abdel Hakeem et al. 2022]. Além de altamente vulneráveis a ataques de interferência de sinal e roubo de dados.

Uma vez que os UAV devem basear-se em grande maioria dos serviços na IA, é importante visar a mitigação das vulnerabilidades e ataques relacionados com IA. Ade-

mais, para [Wang et al. 2020], quando utilizado controladores SDN, os UAV se tornam alvo fáceis, além dos ataques de escutas e sequestro de informações, *spoofing* e DoS.

Em relação aos veículos autônomos é mais preocupante questões de privacidade dos utilizadores [Wang et al. 2020], mecanismos inteligentes para condução autônoma que suporte autenticação de dois fatores e localização.

Tabela 1. Principais requisitos de segurança para Aplicações 6G.

Aplicação	Requisitos de Segurança	Problemas de Segurança e Privacidade
UAV e Veículos Autônomos	Confidencialidade e integridade ultra-alta, Segurança automatizada de toque zero, Privacidade dos assinantes, Segurança em tempo real e Eficiência energética [Nguyen et al. 2021]	Comportamento malicioso, Encriptação, Comunicação e Autenticação [Wang et al. 2020]
Realidade Estendida (XR)	Confidencialidade e integridade ultra-alta, Segurança ultraleve, Segurança automatizada de toque zero, Privacidade alta e Eficiência Energética [Nguyen et al. 2021] e [Porambage et al. 2021]	Comunicação, Comportamento malicioso e Controle de Acesso [Wang et al. 2020]
Indústria 5.0	Confidencialidade e integridade ultra-alta, Segurança automatizada de toque zero, Segurança em tempo real e Eficiência energética [Porambage et al. 2021]	Comportamento malicioso, Encriptação, Comunicação e Autenticação [Abdel Hakeem et al. 2022]
Hyper-intelligent healthcare	Confidencialidade e integridade ultra-alta, Segurança automatizada de toque zero, Segurança em tempo real e Eficiência energética, Privacidade dos assinantes	Comportamento malicioso e encriptação [Wang et al. 2020]

Os desafios de segurança e privacidade pendentes em aplicações XR incluem comportamento malicioso, controlo de acesso, e comunicação interna (Tabela 1). Já a indústria 5.0 deve satisfazer além dos requisitos básicos de segurança (como integridade, disponibilidade, autenticação e auditoria), segurança e proteção da integridade dos dados, sistema de restrição de acesso a recursos sensíveis. Uma tecnologia que pode empregar proteção da privacidade e integridade dos dados é o *Blockchain* [Porambage et al. 2021].

Em se falando das aplicações que visam os cuidados inteligentes com a saúde, impulsionados pela IA e visando qualidade de vida (*Quality of Life* - QoL), entre outros [Nayak and Patgiri 2021], é essencial trabalhar os aspectos éticos, como a privacidade dos dados dos utilizadores, dos registros de saúde dos pacientes, e o uso desses dados em modelos IA [Porambage et al. 2021], além da preocupação da aplicabilidade coerente de regulamentações como a LGPD.

3. Questões em Aberto

Além dos desafios citados anteriormente, as redes 6G também enfrentarão desafios relacionados a sua padronização, como por exemplo sua própria arquitetura. Desafios tecnológicos tais como flexibilidade de conexão, capacidade máxima e alta eficiência energética estão atrelados ao escopo da rede 6G.

Por conseguinte, diversos desafios de segurança e privacidade em 6G permanecem em aberto, como definição de políticas de privacidade no uso dos dados e anonimização em IA, definições de mecanismos ML específicos para redes móveis 6G. Importante refinar como a IA fornecerá proteção em tempo real contra ameaças conhecidas do 5G e ainda desconhecidas. E por agora, quais mecanismos poderão garantir segurança pós-quântica e como a criptografia pós-quântica será aplicada em 6G.

Inúmeros desafios de pesquisas são previstos para o 6G, a segurança e a proteção da privacidade dos dados são desafiadores neste ambiente. Portanto, deve ser considerada a fase inicial das pesquisas em 6G para mitigar esses desafios.

4. Considerações Finais

Neste trabalho, apresentamos os principais desafios de segurança e privacidade nas tecnologias e aplicações 6G, sumarizando os requisitos de segurança e as ameaças que exploram as vulnerabilidades ainda em investigação ou desconhecidas pelos pesquisadores. Ademais, orientamos investigações futuras sobre segurança e privacidade, citando alguns artigos relevantes nessa área. Com esses trabalhos, nota-se que há grandes avanços em 6G, de forma mais intensa com IA e *Blockchain*. Como próximos passos, é necessário investigar os diferentes ataques com profundidade e encontrar mecanismos para mitigação, provendo proteção para os aspectos mais críticos de segurança e privacidade.

Referências

(2023). Committed to connecting the world. urlhttps://www.itu.int/en/Pages/default.aspx.

Abdel Hakeem, S. A., Hussein, H. H., and Kim, H. (2022). Security requirements and challenges of 6g technologies and applications. *Sensors*, 22(5):1969.

De Alwis, C., Kalla, A., Pham, Q.-V., Kumar, P., Dev, K., Hwang, W.-J., and Liyanage, M. (2021). Survey on 6g frontiers: Trends, applications, requirements, technologies and future research. *IEEE Open Journal of the Communications Society*, 2:836–886.

Ji, B., Wang, Y., Song, K., Li, C., Wen, H., Menon, V. G., and Mumtaz, S. (2021). A survey of computational intelligence for 6g: Key technologies, applications and trends. *IEEE Transactions on Industrial Informatics*, 17(10):7145–7154.

Katz, M. and Ahmed, I. (2020). Opportunities and challenges for visible light communications in 6g. In *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pages 1–5.

Letaief, K. B., Shi, Y., Lu, J., and Lu, J. (2021). Edge artificial intelligence for 6g: Vision, enabling technologies, and applications. *IEEE Journal on Selected Areas in Communications*, 40(1):5–36.

Nayak, S. and Patgiri, R. (2021). 6g communication technology: A vision on intelligent healthcare. *Health informatics: A computational perspective in healthcare*, pages 1–18.

Nguyen, T., Tran, N., Loven, L., Partala, J., Kechadi, M.-T., and Pirttikangas, S. (2020). Privacy-aware blockchain innovation for 6g: Challenges and opportunities. *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pages 1–5.

Nguyen, V.-L., Lin, P.-C., Cheng, B.-C., Hwang, R.-H., and Lin, Y.-D. (2021). Security and privacy for 6g: A survey on prospective technologies and challenges. *IEEE Communications Surveys & Tutorials*, 23(4):2384–2428.

Porambage, P., Gür, G., Osorio, D. P. M., Liyanage, M., Gurtov, A., and Ylianttila, M. (2021). The roadmap to 6g security and privacy. *IEEE Open Journal of the Communications Society*, 2:1094–1122.

Siriwardhana, Y., Porambage, P., Liyanage, M., and Ylianttila, M. (2021). Ai and 6g security: Opportunities and challenges. In *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, pages 616–621. IEEE.

Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., and Zhou, W. (2020). Security and privacy in 6g networks: New areas and new challenges. *Digital Communications and Networks*, 6(3):281–291.