Capítulo 2

Um Panorama dos Serviços de Saúde Avançados: Conectividade e Segurança em Sistemas de Vida Assistida

Adriana V. Ribeiro (UFBA), Fernando Nakayama (UFPR), Michele Nogueira (UFMG), Leobino N. Sampaio (UFBA)

Abstract

An ambient assisted living is an advanced health service that includes smart space applications and location-independent individual monitoring. The development of assisted living applications relies on several technologies, such as the Internet of Things, short and long-range communication protocols, middlewares, cloud computing, and artificial intelligence. The heterogeneity of the architectural components and communication protocols arises challenges in providing network and security requirements. This chapter overviewes this service and identifies the main communication and security requirements and the challenges to address them.

Resumo

O ambiente de vida assistida é um serviço avançado de saúde que inclui aplicações em espaços inteligentes e o monitoramento da saúde de indivíduos, independente de sua localização. O desenvolvimento dessas aplicações segue diferentes tecnologias, como a Internet das Coisas, protocolos de comunicação de curto e longo alcance, middlewares, computação em nuvem e inteligência artificial. A heterogeneidade dos componentes que fazem parte dessas arquiteturas e dos próprios protocolos de comunicação utilizados geram desafios para alcançar os requisitos de rede e segurança das aplicações. Este capítulo apresenta uma visão geral desse serviço, identifica os principais requisitos de comunicação e segurança e os principais desafios para endereçá-los.

2.1. Introdução

Em 2017, o Ministério da Saúde do Brasil informou que as hospitalizações de pessoas idosas no Sistema Único de Saúde (SUS) custam aproximadamente 30% a mais

quando comparadas às de adultos entre 25 e 59 anos [Heemann and Hermsdorf 2017]. Paralelo a isso, o Instituto Brasileiro de Geografia e Estatística (IBGE) estima que o número de pessoas com idade superior a 65 anos no Brasil será equivalente a 25.5% da população até 2060 [IBGE 2018]. Embora esses sejam dados brasileiros, essa mudança demográfica e o aumento dos custos na área de saúde têm sido observados ao redor do mundo [United Nations 2020], intensificando a necessidade de pesquisas que contribuam com o desenvolvimento de soluções economicamente viáveis [Maskeliūnas et al. 2019, Tun et al. 2021]. Além da questão econômica, também é importante ressaltar que a mudança demográfica mundial requer uma maior quantidade de profissionais de saúde para atender à população. Portanto, a tecnologia é vista como aliada para oferecer saúde de qualidade e a um menor custo.

Com o objetivo de produzir soluções mais baratas e eficazes, a Internet das Coisas da Saúde (do inglês, *Internet of Health Things* – IoHT) se baseia no uso de dispositivos e aplicações de Internet das Coisas (do inglês, *Internet of Things* – IoT) e em arquiteturas de rede para dar suporte às aplicações e serviços de saúde [Rodrigues et al. 2018]. A IoHT auxilia na diminuição dos custos da saúde pública e privada, através de mecanismos de monitoramento e análise de dados que possibilitem a prevenção de eventos adversos e, consequentemente, a redução de hospitalizações [Tun et al. 2021]. Como as aplicações da IoHT podem estar relacionadas a diversos públicos e funcionalidades, existem vários critérios que podem ser utilizados para classificá-las. Em [Rodrigues et al. 2018], os autores as classificam em quatro áreas principais: monitoramento de saúde remoto, soluções de saúde baseadas em *smartphones*, dispositivos vestíveis e Ambiente de Vida Assistida (do inglês, *Ambient Assisted Living* – AAL).

A AAL é um serviço que faz uso de sistemas e aplicações IoT para promover mais independência e bem estar às pessoas idosas ou com deficiência [Rodrigues et al. 2018], bem como para avaliar e identificar padrões em populações [Wang et al. 2022]. Os principais tipos de aplicações AAL incluem o monitoramento do espaço físico (e.g., segurança do local, temperatura e umidade) e do indivíduo (e.g., frequência cardíaca, pressão sanguínea e temperatura corporal). No entanto, as soluções de AAL comumente estão restritas a um espaço e cobrem apenas uma área previamente estabelecida. Assim, o monitoramento é interrompido caso o usuário saia do espaço monitorado. Para que haja um acompanhamento efetivo da saúde do indivíduo, as atividades de monitoramento devem ocorrer independente de sua localização [Nakayama et al. 2022]. Portanto, o uso de dispositivos móveis na coleta e encaminhamento dos dados de forma contínua é imprescindível para o funcionamento de diversas aplicações.

As aplicações de saúde mais simples geralmente têm um objetivo específico e são baseadas no monitoramento de poucas características. Por exemplo, uma aplicação simples para controle de diabetes pode envolver a utilização de sensores de glicose para monitorar o nível de açúcar no sangue e emitir algum alerta para o indivíduo, um familiar ou membro da equipe médica em caso de problemas. No entanto, algumas soluções de saúde atuais têm caráter mais complexo pois buscam ofertar serviços de saúde holísticos e mais inteligentes. O aumento na complexidade das aplicações introduz a necessidade de outras tecnologias para dar suporte aos serviços de saúde avançados. Em [Philip et al. 2021], os autores destacam cinco tecnologias principais para o desenvolvimento de soluções de saúde: aplicações IoT, computação em nuvem, utilização de *middlewares*, comunicações

de rede de curto alcance e sensores. O uso dessas tecnologias deve considerar os requisitos do usuário e da aplicação para que haja uma adoção efetiva das soluções.

Alguns requisitos gerais que os sistemas de vida assistida devem atender incluem a utilidade do serviço, a facilidade de uso e a curva de aprendizado. Além disso, a adoção de soluções na área de saúde é influenciada diretamente por aspectos como idade, gênero e escolaridade dos indivíduos [Maskeliūnas et al. 2019]. Tendo em vista que, em muitos casos, a população idosa tem menos familiaridade com o manuseio de equipamentos tecnológicos, é preciso considerar o conforto do dispositivo, sua capacidade de gerenciamento e facilidade de uso para que haja sucesso na adoção dessas soluções. No entanto, em um sistema como esse, envolvendo uma arquitetura com diversos componentes distribuídos, também é fundamental pensar em questões relacionadas à conectividade e à segurança dos dados e sistema. A conectividade é essencial para que haja comunicação entre os componentes do sistema. Enquanto a segurança gera a proteção do sistema e da aplicação contra ações de modificação dos dados e recursos, acesso indevido aos mesmos e indisponibilidade do serviço.

Os requisitos de comunicação e de segurança relacionados às aplicações de saúde são discutidos ao longo deste capítulo de livro considerando os diferentes processos que acontecem para que uma aplicação IoHT funcione adequadamente: coleta de dados, transmissão local e encaminhamento de dados para serviços remotos. Além disso, também serão tratados os requisitos gerais envolvendo conectividade, mobilidade, Qualidade de Serviço (do inglês, *Quality of Service* – QoS) e Qualidade de Experiência (do inglês, *Quality of Experience* – QoE). Do ponto de vista de segurança, é preciso observar os requisitos voltados aos princípios básicos, como disponibilidade, integridade, confidencialidade, privacidade e controle de acesso.

Como a saúde é a área que mais tem desenvolvido soluções baseadas em IoT [Rodrigues et al. 2018], é imprescindível que os protocolos e os dispositivos criados consigam ser utilizados de forma efetiva para proporcionar soluções nessa área, pois isso também influencia o desenvolvimento da própria IoT. O desenvolvimento de soluções reais depende do uso de mecanismos que garantam ou deem suporte à segurança e à privacidade dos dados [Rodrigues et al. 2018]. Essa temática tornou-se popular nos últimos anos, mas o uso de protocolos de comunicação e serviços eletrônicos e a preocupação com questões de privacidade e segurança são tópicos tratados há um tempo. O potencial para uso desses serviços tem aumentado e a área de saúde tem liderado o *ranking* de pesquisas envolvendo IoT. Uma característica interessante nas aplicações atuais é a necessidade do monitoramento holístico do indivíduo para o desenvolvimento de serviços inteligentes. Considerando isso e a relevância dessas aplicações para a saúde dos indivíduos, este minicurso discute o processo de evolução do uso da tecnologia na saúde de idosos e as características das aplicações atuais. Ele também apresenta os conceitos relacionados à IoHT, os requisitos de conectividade e segurança das aplicações e como novos modelos e arquiteturas de rede suportam essas soluções. Por fim, serão apresentados dois estudos de casos e ambientes de experimentação associados à área.

2.2. Evolução do uso da tecnologia na saúde de idosos

Nos últimos 20 anos foram desenvolvidas as principais tecnologias utilizadas nas soluções de saúde atuais, incluindo dispositivos e aplicações IoT, *smartphones*, equipamentos vestíveis e computação em nuvem. Na Figura 2.1, são listadas as características e os aspectos marcantes dessa evolução entre os anos 2000 e 2020. Uma pesquisa publicada em 2004 indicou aplicações passíveis de beneficiar os cuidados com a saúde de idosos: auxílio em situações de emergência, prevenção de queda, monitoramento de temperatura e de parâmetros fisiológicos, sistemas de segurança para a casa, monitoramento de medicação, entre outros [Demiris et al. 2004]. Apesar disso, as soluções da época estavam mais voltadas à telemedicina, à criação de sistemas eletrônicos para a saúde e à utilização de e-mail, SMS e fax para facilitar a comunicação entre o indivíduo e a equipe médica. Havia iniciado o uso de câmeras para fazer monitoramento dos indivíduos, mas a privacidade era uma preocupação dos idosos já nesse período. Outras preocupações incluíam a substituição da assistência humana pela tecnologia, o uso de dispositivos amigáveis e a necessidade de treinamentos específicos. Além disso, algumas características das redes sem fio, como alto custo e dificuldade de interoperabilidade, limitaram o desenvolvimento de soluções móveis [Istepanian and Lacal 2003].

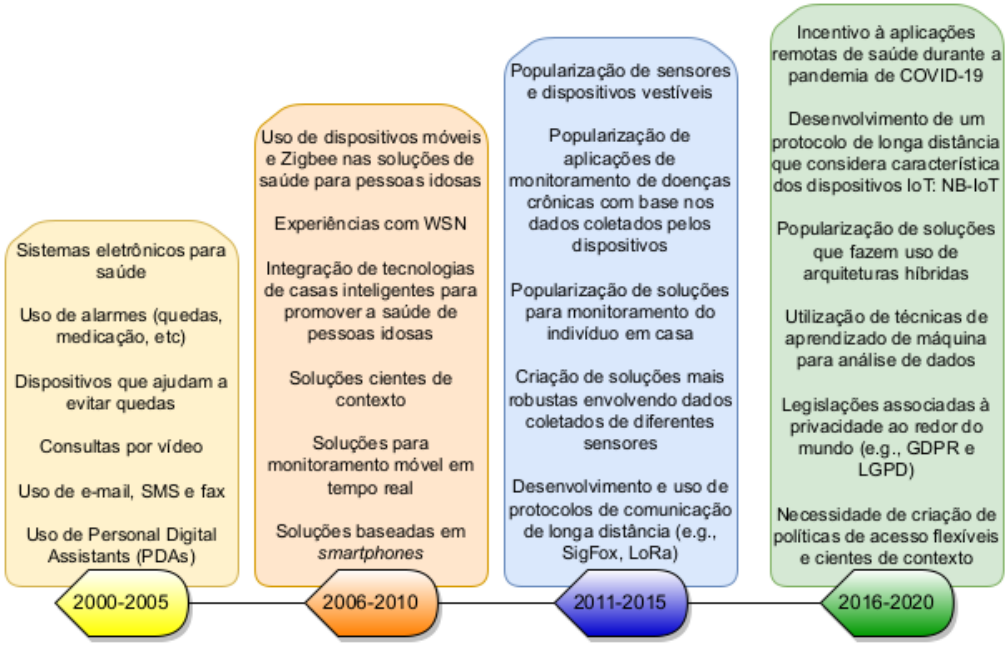

Figura 2.1. Marcos importantes para o desenvolvimento e uso de aplicações de saúde para pessoas idosas.

Entre 2006 e 2010, o desenvolvimento e a popularização dos *smartphones* e a primeira geração de serviços de nuvem influenciaram o crescimento de novas soluções de saúde. Uma pesquisa publicada por [Steele et al. 2009] em 2009 demonstrou que a independência é um dos aspectos mais valorizados por pessoas idosas e que há uma abertura maior ao uso de sistemas e serviços que possam prolongar esse sentimento. Nesta mesma pesquisa, os autores indicaram que as preocupações associadas ao uso de redes de sensores sem fio (do inglês, *Wireless sensors networks* – WSN) estavam relacionadas a fatores como custo, impacto social do uso de dispositivos, possíveis efeitos colaterais causados

pelas ondas de radiofrequência emitidas pela WSN, ansiedade, privacidade, confidencialidade e confiabilidade do sistema. Os participantes destacaram ainda suas preferências em relação ao uso de sensores embutidos em relógios e/ou anéis, para que houvesse mais privacidade em relação ao uso de um dispositivo de monitoramento de saúde. Nesse período, as soluções híbridas começaram a ser pensadas e houve um aumento na diversidade de aplicações, que variavam desde o monitoramento da casa ao monitoramento de sinais vitais e doenças crônicas [Arcelus et al. 2007, Jones et al. 2010].

De 2011 até 2015, ocorreu um cenário mais propício para o desenvolvimento dos atuais serviços de saúde avançados. Os dispositivos vestíveis começaram a se tornar itens mais populares entre as pessoas, independente da idade. Esse fator é importante ao pensar em soluções de saúde para pessoas idosas, uma vez que elas relatam preocupação em relação ao desconforto e impacto social de ter que utilizar sensores de monitoramento de saúde. Além da popularização dos vestíveis, tem-se a popularização de aplicações de monitoramento de doenças crônicas e do ambiente do indivíduo. Em [Rashidi and Mihailidis 2012], os autores destacam as aplicações e as tecnologias associadas ao uso de AAL. Esse trabalho trouxe uma lista dos principais tipos de sensores de ambiente e dispositivos vestíveis usados na época e foi possível observar o uso de algoritmos de reconhecimento de imagens e aplicações voltadas ao monitoramento de atividades cardíacas, cerebrais e musculares, glicose, pressão sanguínea e outras. A integração dessas soluções possibilitou propostas de aplicações mais robustas. Em [Kim et al. 2014], os autores apresentaram soluções de cuidados da saúde com diferentes arquiteturas e envolvendo o acesso à informação por várias partes, como equipe médica e indivíduo. As comunicações entre os dispositivos dentro do ambiente eram baseadas em protocolos de curto alcance, como Zigbee, Bluetooth, RFID e Wi-Fi. Enquanto as comunicações de longa distância se baseavam, principalmente, nos sistemas de telecomunicações móveis [Amiribesheli et al. 2015]. Apesar do grande salto no desenvolvimento de dispositivos e dos aspectos positivos possibilitados através das soluções na época, algumas pessoas idosas relataram não utilizar as aplicações de saúde, pois achavam que não melhorariam sua qualidade de vida de forma significativa [Heart and Kalderon 2013].

A evolução dos serviços remotos de saúde continuou e a evidência de sua necessidade foi ainda mais acentuada durante a pandemia de COVID-19. No primeiro ano da pandemia, muitas consultas e cirurgias eletivas foram suspensas devido à necessidade de concentrar os recursos de saúde no enfrentamento à COVID-19. Além disso, como os idosos faziam parte do grupo de risco, houve receio em ir aos médicos para suas consultas de rotina. A necessidade de alternativas remotas fez com que o governo brasileiro aprovasse a Lei 13.989/2020, que permitia aos profissionais de saúde a realização de atendimentos online. Embora essa lei tenha sido revogada, o senado aprovou o PL998/2020 que garantia que qualquer profissional de saúde pudesse realizar atendimento online. Outras medidas legislativas também foram adotadas no Brasil nesse período e influenciam diretamente as aplicações de saúde. Uma dessas medidas foi a Lei Geral de Proteção de Dados (LGPD) que busca garantir o direito à privacidade dos usuários através da regulamentação do tratamento dos dados pessoais.

Durante os últimos 10 anos, houve mudanças legislativas e tecnológicas que impulsionaram o desenvolvimento e a preocupação com aplicações de saúde. Houve o desenvolvimento de novos dispositivos e tecnologias de suporte, além da adoção de arqui-

teturas híbridas, uso de técnicas e algoritmos de inteligência artificial (IA) e a criação de protocolos de comunicação de longa distância específicos para IoT. A junção dessas soluções tem possibilitado a proposta e o desenvolvimento de aplicações cada vez mais robustas e inteligentes que relacionam dados do indivíduo para possibilitar tratamentos personalizados e, ao mesmo tempo, permitem avaliar políticas de saúde pública e auxiliar na análise e na correlação de fatores associados a diversas doenças. A expectativa – que tem se tornado realidade – é que a IoHT ajude a endereçar diversos problemas associados a pessoas idosas, como limitações em suas atividades diárias, risco de queda, monitoramento de doenças crônicas, demência, desordens mentais e gerenciamento de medicamentos [Maskeliūnas et al. 2019]. A seguir, serão descritas algumas dessas aplicações atuais e suas características gerais.

2.2.1. Cenários de aplicação

Algumas das doenças mais comuns em pessoas idosas incluem problemas cardíacos, diabetes, hipertensão, câncer e Alzheimer. O monitoramento do ambiente e da saúde do indivíduo é essencial para manter essas doenças sob controle, principalmente nos casos das chamadas "doenças silenciosas", como a hipertensão. A Tabela 2.1 apresenta uma relação dos domínios de aplicações de saúde associados às pessoas idosas. Esses domínios têm pontos de intersecção nas aplicações de saúde: por exemplo, o monitoramento de uma doença crônica pode ser realizado com vestíveis, através de aplicações móveis ou mesmo com uso de AAL. Além disso, o monitoramento dos parâmetros de saúde auxilia na prevenção e no diagnóstico de novas doenças. A Tabela 2.2 resume as aplicações de saúde para pessoas idosas.

Tabela 2.1. Domínios de monitoramento associados à saúde de pessoas idosas.

Domínio	Contribuições
Vestíveis e sensores	Executam funções como a detecção de quedas, o monitoramento de padrões de sono, condições cardíacas, níveis de oxigênio no sangue, pressão arterial, temperatura corporal e comportamentos sedentários. Permitem o monitoramento contínuo do indivíduo e podem emitir alertas para familiares e/ou equipe médica em casos de emergência.
AAL	Coleta variáveis do ambiente, como qualidade do ar e intensidade da luz para avaliar suas implicações na saúde do indivíduo. Além disso, é possível integrar aplicações de AAL com robôs, equipamentos vestíveis e tecnologias móveis. Essa integração viabiliza a criação de aplicações mais robustas.
Telemedicina	Definida como o uso da tecnologia para realizar diagnósticos e tratamentos de forma remota. Bastante popular durante a pandemia de COVID-19 e cada vez mais utilizada. É uma alternativa para proporcionar acesso a profissionais de saúde para pessoas em áreas remotas.
Aplicações móveis	Usam serviços de nuvem para armazenar os dados e diferentes pessoas (e.g., equipe médica e familiares) acessam as informações através de aplicativos. Auxilia no monitoramento de inúmeras condições e doenças, bem como possibilita *feedbacks* aos indivíduos com tratamento personalizado.

A relevância no desenvolvimento dessas aplicações é demonstrada através de dados estatísticos: dados do Sistema de Mortalidade do Brasil (SIM), disponibilizados pelo

Tabela 2.2. Aplicações de saúde para pessoas idosas.

Aplicação	Características
Monitoramento de parâmetros de saúde	Medição de parâmetros como nível de oxigênio no sangue, pressão arterial, pulsação, níveis de açúcar, temperatura corporal, ritmo de caminhada, equilíbrio, perfil lipídico, entre outros. Geralmente são utilizados para realizar o monitoramento de doenças crônicas e detecção de quedas.
Monitoramento de doenças crônicas	Faz uso do monitoramento de parâmetros de saúde e podem apresentar requisitos de baixa latência e monitoramento em tempo real. Pode incluir soluções de monitoramento para doenças como Alzheimer e Parkinson.
Rastreamento de atividades	Faz uso de dispositivos como sensores, acelerômetros e GPS para mapear e incentivar a prática de atividade física por pessoas idosas. Os dados coletados podem ser utilizados para aplicações de detecção de queda ou mesmo como insumo para o monitoramento de doenças mentais.
Gerenciamento de medicação	São aplicações que alertam o indivíduo para tomar suas medicações. Além disso, as informações coletadas por aplicações de monitoramento de parâmetros de saúde podem ser usadas como insumo para realizar ajustes medicamentosos pela equipe médica.
Monitoramento da saúde mental e de doenças cognitivas	As doenças mais comuns associadas à saúde mental de idosos incluem Alzheimer, Parkinson, demência, depressão e esquizofrenia. O uso de informações de rastreamento de atividades diárias possibilita avaliar a progressão dessas doenças a partir da análise de padrões e mudanças na rotina. Embora esses aplicativos não substituam o acompanhamento humano, podem auxiliar no bem estar desses indivíduos.
Serviços de emergência	Em emergências, esses serviços são utilizados para enviar alertas e possibilitar acesso ao histórico médico por familiares e/ou equipe médica.

DataSUS[1], mostram que entre o período de 2015 e 2020 foram registrados aproximadamente 4,8 milhões de óbitos de pessoas com idade igual ou superior a 65 anos. Mais de 50% dessas mortes foram ocasionadas por três causas principais: 31,8% às doenças do aparelho circulatório, 16,1% a tumores e 15% às doenças do aparelho respiratório. A maioria dessas doenças pode se beneficiar de soluções IoHT: uma aplicação de monitoramento de diabetes demonstrou uma melhora do controle glicêmico em 0,8% para diabetes do tipo 2 e 0,3% para diabetes do tipo 1 [Kitsiou et al. 2017]. Em outro estudo, foi demonstrado que o monitoramento de pacientes com problemas cardíacos reduziu as taxas de hospitalizações e mortalidade [Bui and Fonarow 2012].

2.3. Principais Conceitos dos Sistemas de Vida Assistida

Os serviços de saúde avançados que têm como foco o atendimento às pessoas idosas, são suportados por cinco tecnologias principais: dispositivos IoT e *mHealth*, protocolos de comunicação de curto e longo alcance, arquiteturas baseadas em computação em nuvem e em névoa, *middlewares* e uso de técnicas de aprendizado de máquina. Cada uma dessas tecnologias tem papel fundamental no desenvolvimento de soluções mais inteligentes e serão discutidas nesta seção.

[1] http://tabnet.datasus.gov.br/cgi/deftohtm.exe?sim/cnv/obt10uf.def

2.3.1. IoHT e *mHealth*

Os dispositivos IoT possibilitam funções de coleta e armazenamento de dados e a execução de ações autônomas com o uso de atuadores [Rodrigues et al. 2018]. As características desses dispositivos variam de acordo com sua aplicação, protocolos de comunicação, mecanismos de coleta, mobilidade, custo, entre outros. Essa heterogeneidade de dispositivos possibilita o desenvolvimento de diferentes aplicações, ao mesmo tempo que as demandas por mais serviços de saúde requerem melhorias e novas funcionalidades nos dispositivos. A arquitetura IoHT segue um modelo definido em três camadas: percepção, rede e aplicação. A Figura 2.2 ilustra essa arquitetura e o papel de cada uma dessas camadas é discutido ao longo desta seção. Existem variações desta arquitetura que incluem um modelo estendido em mais camadas com o objetivo de explicitar algumas funcionalidades e tecnologias, como o uso de *middlewares*.

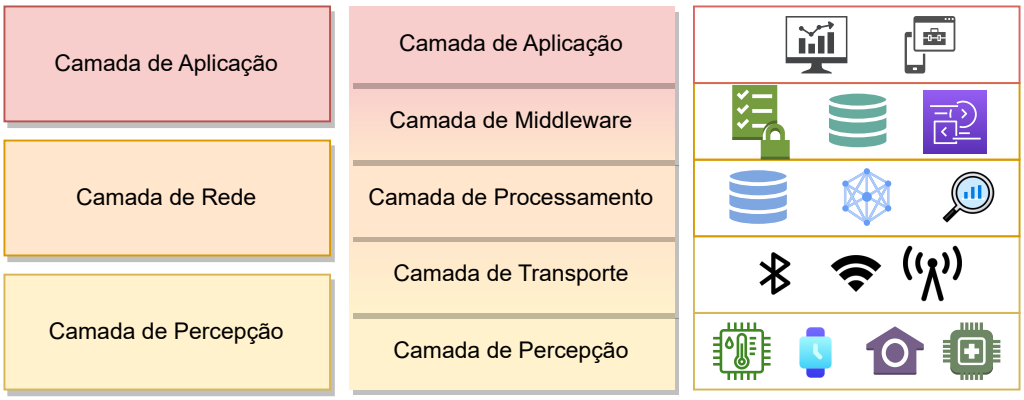

Figura 2.2. Representação em camadas da arquitetura IoT e seus componentes.

Na **camada de percepção**, estão localizados os sensores e atuadores. Os sensores associados à área de saúde podem coletar dados como sinais vitais, pressão sanguínea e temperatura corporal. Em fase de prototipagem, esses sensores comumente são associados às placas de Arduíno ou Raspberry Pi. Em cenários industriais, destacam-se os *smartwatches* como exemplo de equipamento vestível que possui sensores e que tem se tornado popular [Rodrigues et al. 2018]. Os sensores e dispositivos IoT podem variar em relação a inúmeros aspectos, como capacidade de processamento, protocolos de comunicação e papel que executa na arquitetura. Alguns desses dispositivos são considerados inteligentes e, além da coleta de dados, também executam algum tipo de processamento local. Em geral, os dispositivos comunicam-se entre si e/ou com um *gateway* para troca de informações e envio de dados para processamento remoto. O *gateway* é um dispositivo com mais recursos e autonomia energética que centraliza ações de coordenação e gerenciamento dos dispositivos, além de garantir a comunicação com equipamentos e serviços remotos. Nesse sentido, além de serem equipados com sensores, os dispositivos também possuem um ou mais mecanismos de comunicação.

Considerando a heterogeneidade dos dispositivos, foi estabelecida uma taxonomia baseada em recursos que os classifica em três categorias: classe 0, classe 1 e classe 2 [Bansal and Kumar 2020]. A classe 0 é composta pelos sensores e atuadores, que são dispositivos que geralmente têm poucos recursos e muitas limitações de segurança. Já

a classe 1, engloba elementos que podem atuar como *gateways* básicos, suportam múltiplos protocolos de comunicação e têm recursos superiores aos dispositivos de classe 0. Por fim, os dispositivos associados à classe 2 são mais robustos, possibilitam o uso de técnicas de IA e aprendizado de máquina (do inglês, *Machine Learning* – ML), dão suporte a vários protocolos de comunicação (e.g., Gigabit Ethernet, Wi-Fi e Bluetooth) e podem usar mecanismos de segurança mais avançados. Na Tabela 2.3 há um comparativo entre as classes de dispositivos com base na taxonomia de [Bansal and Kumar 2020].

Tabela 2.3. Classificação dos dispositivos IoT.

Classificação	Comunicação	Dispositivos	Características gerais
Classe 0 **Sensores** **Atuadores**	Protocolos *lightweight* (e.g., IEEE 802.15.4)	Telos Open mote Waspmote Tmote Sky	Muito vulneráveis às ameaças de segurança
Classe 1 ***Gateways***	Múltiplos protocolos (e.g., Wi-Fi)	Arduíno Netduino Tessel 2 ESP8266	Suporte à criptografia São *gateways* básicos em arquiteturas IoT
Classe 2 **Controladores**	Praticamente todos os tipos de protocolos	Raspberry Pi Orange Pi Banana Pi Cubieboard Beagleboard	Tem mais recursos de memória, processamento e armazenamento Suportam aplicações de IA, ML e processamento de linguagem São *gateways* mais complexos

Além da capacidade de recursos, os dispositivos IoT podem ser classificados e tratados com base em outros critérios. Por exemplo, quando um equipamento é classificado como dispositivo médico nos Estados Unidos, ele precisa ser aprovado pela FDA (*Food and Drug Administration*). Essas ações são essenciais para tentar minimizar a liberação de dispositivos que possam causar riscos à saúde do indivíduo ou desconforto devido a questões como tamanho, frequências de comunicação e aquecimento [Philip et al. 2021, Cornet et al. 2022]. Os dispositivos médicos têm buscado possibilitar a autonomia do indivíduo e a acurácia dos dados coletados. Em paralelo, os sensores têm sido utilizados para fornecer diferentes mecanismos de monitoramento: ECG, acelerômetro, SPo2, frequência cardíaca, etc [Philip et al. 2021]. Esses sensores estão embutidos em acessórios cotidianos, como pulseiras e relógios, para promover mais conforto físico e social ao indivíduo. Além disso, há a preocupação de que suas baterias sejam recarregáveis e fáceis de substituir, pois em aplicações de monitoramento contínuo, a inatividade do dispositivo e a inacurácia dos dados pode gerar diagnósticos incorretos [Cornet et al. 2022]. Tanto dispositivos médicos quanto equipamentos vestíveis e *smartphones* têm sido utilizados para acompanhamento de doenças crônicas através do monitoramento contínuo dos parâmetros de saúde do indivíduo [Perez et al. 2022].

O monitoramento contínuo depende de dispositivos que garantam a transmissão dos dados independente da localização do indivíduo. A *mHealth* refere-se ao uso de dispositivos móveis aplicados à área da saúde. Nessa área, é importante que os dispositivos suportem protocolos de comunicação de longa distância para encaminhar os dados em tempo real para a aplicação. Além disso, a importância do suporte à mobilidade também é importante pois a coleta de dados de mobilidade é um dos aspectos que mais contribui

para detecção na variação da saúde de pessoas idosas [Tun et al. 2021].

Para conseguir transmitir os dados coletados, os dispositivos precisam comunicar-se e trocar informações entre si. Portanto, é comum que dispositivos de classe 0 e classe 1 comuniquem-se e enviem dados para armazenamento e processamento. A conectividade entre os dispositivos ou entre a rede local e serviços remotos é feita com protocolos de comunicação de curta e longa distância. Esses protocolos são utilizados na transmissão dos dados e estão associados às funcionalidades da **camada de rede** na arquitetura representada na Figura 2.2. A escolha do protocolo de comunicação vai depender dos requisitos da aplicação e das características dos protocolos, que podem variar em banda de frequência, taxa de transmissão, latência e consumo energético. Além disso, também deve-se considerar aspectos como mobilidade, interoperabilidade e métricas de QoS. Informações sobre os protocolos que atuam na camada de rede e os principais requisitos associados à conectividade são discutidos nas Seções 2.3.2 e 2.4, respectivamente.

A camada de rede possibilita a troca de mensagens entre as camadas de percepção e a aplicação. A **camada de aplicação** é responsável por prover serviços para usuários finais (e.g., indivíduos, familiares e equipe médica). Como foi visto na Seção 2.2.1, as aplicações podem incluir monitoramento de parâmetros de saúde, gerenciamento de medicação, serviços de emergência, entre outras funcionalidades e podem ser realizadas a partir de diferentes domínios, como uso de vestíveis ou AAL. Os requisitos da camada de aplicação servirão como guia na definição de quais dispositivos e protocolos de comunicação devem ser utilizados. Além disso, aplicações mais robustas incluem serviços de computação em nuvem, desenvolvimento de *middlewares* e uso de técnicas de ML. Alguns desses tópicos serão abordados nas seções seguintes.

2.3.2. Protocolos de comunicação

Os dispositivos IoT e sensores utilizados em sistemas de vida assistida apresentam propriedades de comunicação variadas. Essa variação tem relação direta com a função executada pelo dispositivo e com as características dos dados coletados (e.g., volume dos dados e frequência de coleta). Na Tabela 2.4 estão listadas as propriedades de algumas aplicações de saúde em relação às características da comunicação, como frequência de banda, taxa de transmissão, latência e consumo energético. Uma das consequências dessas variações de requisitos é a utilização de diferentes protocolos de comunicação.

Tabela 2.4. Relação entre aplicações de saúde e características do meio de comunicação. Adaptado de [Cornet et al. 2022].

Aplicação	Bandas de frequência	Taxa de transmissão	Latência	Uso de energia
Voz	–	100kbps	< 250ms	–
Sensor de movimento	30-100Hz	4.8-35kbps	< 250ms	–
Streaming de vídeo	–	< 10Mbps	< 250ms	Alto
Pressão sanguínea	< 100Hz	< 10kbps	< 150ms	Alto
ECG	< 500Hz	3kbps	< 150ms	Alto
Streaming de áudio	–	1Mbps	< 250ms	Alto
Fluxo sanguíneo	< 40Hz	480kbps	< 150ms	Baixo
Temperatura	< 1Hz	120bps	< 150ms	Baixo
Nível de glicose	< 50Hz	< 1kbps	< 150ms	Muito baixo

Os protocolos de comunicação utilizados em sistemas de vida assistida geralmente são classificados em protocolos de curta ou longa distância. Os protocolos de curta distância estão associados, principalmente, a dois tipos de redes: redes de área corporal sem fio (do inglês, *Wireless Body Area Networks* – WBAN) e WSN. Os protocolos de longa distância geralmente são utilizados para possibilitar a comunicação entre os dispositivos locais e a nuvem, através da Internet. Os protocolos de curto e longo alcance variam em cobertura e frequência do sinal, consumo energético, largura de banda, mecanismos de comunicação, entre outros. Na Tabela 2.5 é realizada uma comparação entre esses diferentes protocolos, considerando suas principais características. Fazendo uma relação dessa tabela com a anterior, observa-se que para sensores com baixa frequência de sinal (e.g., temperatura), utilizar uma tecnologia como o Bluetooth Low Energy (BLE) é suficiente. Enquanto para sensores com frequência de sinal mais alta e que requerem mais largura de banda (e.g., *streaming* de áudio), é possível utilizar Wi-Fi [Philip et al. 2021]. Além disso, no caso de aplicações que são baseadas em monitoramento de vídeo ou voz, também é importante considerar métricas de rede, como latência.

Tabela 2.5. Tecnologias de comunicação sem fio usadas em sistemas de vida assistida. Fonte: [Nogueira et al. 2021].

	Tecnologia	Bandas de frequência	Alcance	Taxa de transmissão	Uso de energia
Curta distância	RFID	125 - 134 kHz, 13.56 MHz, 860 - 960 MHz	Até 100m	Depende da frequência	Muito baixo
	NFC	13.56 MHz	<0.2 m	Até 424 kbps	Muito baixo
	BLE (802.15.1)	2.4 - 2.48 GHz	Até 100m	Até 24 Mbps	Baixo
	Zigbee (802.15.4)	868 - 868.6 MHz, 902 - 928 MHz, 2.4 - 2.49 GHz	Até 100m	Depende da frequência	Muito baixo
	Wi-Fi (802.11a/b/g/n)	2.4 - 2.48 GHz, 4.9 - 5.8 GHz	20-250 m	2-600 Mbps	Médio
	Wi-Fi 5 (802.11ac)	4.9 - 5.8 GHz	Até 70m	Até 3.5 Gbps	Alto
	Wi-Fi 6 (802.11ax)	1 - 6 GHz	Até 120m	Até 9.6 Gbps	Alto
Longa distância	NB-IoT	Frequências da LTE	Até 15Km	Até 250 kbps	Baixo
	LTE-M	Frequências da LTE	Até 10Km	Até 1 Mbps	Baixo
	LoRa	867 - 869 MHz	Até 25Km	50 kbps	Muito baixo
	Sigfox	868–878.6 MHz	Até 40Km	100 bps	Muito baixo

Dentre os protocolos apresentados na Tabela 2.5, os protocolos NB-IoT, Lora e Sigfox foram criados especificamente para dispositivos IoT. A importância de criar protocolos específicos para IoT se dá, principalmente, porque esses protocolos consideram as características e limitações dos dispositivos. Nesse sentido, o padrão 3GPP (5G IoT) tem sido bem avaliado como alternativa para fornecer conexões celulares de baixa potência, baixa taxa de dados e ampla cobertura de sinal [Philip et al. 2021]. Além disso, o desenvolvimento de protocolos de longa distância que consumam baixa energia é essencial para o monitoramento contínuo de idosos. A proposta de sistemas de vida portátil [Nakayama et al. 2022] destaca a necessidade de utilização de mecanismos de comunicação que garantam a continuidade do serviço à medida que o indivíduo se movimente e ocupe diferentes espaços. Na proposta, os autores sugerem e avaliam o uso de protocolos de múltiplos caminhos como uma alternativa para prover resiliência na comunicação.

Ao considerar as comunicações de curta distância, há a predominância de três protocolos: BLE, Zigbee e Wi-Fi. Esses protocolos atuam, em geral, em uma frequên-

cia de banda de 2.4GHz, que é considerada o padrão para WBANs. No entanto, tem-se observado que essa frequência será insuficiente para atender os requisitos de comunicação de alta velocidade e tempo real exigidos por algumas aplicações [Cornet et al. 2022]. Além disso, como muitos serviços existentes utilizam também a frequência de banda de 2.4GHz, isso pode causar prejuízos na confiabilidade do funcionamento da rede de comunicação. Em decorrência disso, as frequências de onda milimétricas (do inglês, *milimeter wave* – mmWave) têm sido considerada uma alternativa para proporcionar altas velocidades a um custo baixo de processamento. Uma das principais limitações no uso de altas frequências é que estão mais propensas a sofrer com ruídos, reflexão e difração. No entanto, esse problema pode ser menos crítico para as comunicações de curto alcance. Além disso, há a possibilidade de usar métodos propostos para o funcionamento adequado das redes 5G, como o *beamforming*, que envia o sinal em apenas uma direção (a direção do destinatário) em vez de ser enviado em todas as direções.

A comunicação fim a fim em sistemas de vida assistida é caracterizada por múltiplos protocolos de comunicação sem fio ou cabeado, de curta e longa distância, cujas taxas de transmissão de dados e latência fim a fim são determinadas pelas taxas de transmissão e latências intermediárias. Assim, é preciso identificar e evitar possíveis gargalos na rede sem perder de vista que altas taxas de envio de dados e retransmissões entre os dispositivos podem significar um maior consumo energético. Os autores em [Rodrigues et al. 2018] ressaltam, ainda, a dificuldade em criar soluções de segurança completas que considerem as características de diferentes protocolos de comunicação, cabeados e sem fio. No entanto, apesar de a segurança dos canais de comunicação ser algo essencial para as aplicações de IoHT, é preciso assegurar que as soluções de privacidade não causarão sobrecarga nos canais de comunicação, principalmente aqueles com baixa capacidade, visto que isso pode ocasionar falhas ou erros no funcionamento da aplicação [Mukherjee et al. 2018]. Além disso, as soluções de segurança devem considerar os dispositivos e canais envolvidos na coleta (segurança de sensores e dispositivos em geral), transmissão (protocolos de comunicação), armazenamento e processamento de dados (computação em nuvem).

2.3.3. Computação em nuvem

A computação em nuvem tem sido utilizada no contexto de IoHT com duas funções principais: armazenamento e processamento de dados. O armazenamento pode ser realizado em nuvem pública, pessoal, privada, híbrida ou comunitária [Yang et al. 2020]. Existem vantagens e desvantagens no uso de cada tipo de armazenamento. Comparando, por exemplo, a nuvem pública com a privada, percebe-se que para manter uma nuvem privada é necessário investimento em infraestrutura física e profissionais para administrar os equipamentos e serviços. Isso gera um custo elevado de gerenciamento, mas aumenta as garantias relacionadas à confidencialidade e privacidade dos dados. Já com a utilização de nuvens públicas, os usuários pagam proporcionalmente ao serviço contratado e o gerenciamento é mais simples. No entanto, a principal preocupação no uso de nuvens públicas em IoHT está associada à segurança dos dados. Dentre os principais aspectos de segurança que devem ser observados ao armazenar dados em nuvem, é importante citar:

- **Confidencialidade, integridade e disponibilidade dos dados**: é preciso garantir que os dados não sejam alterados ou acessados por pessoas indevidas, e que os

dados enviados são exatamente os mesmos dados armazenados na nuvem. Além disso, os dados devem estar disponíveis sempre que necessário.

- **Controle de acesso granular e compartilhamento seguro de dados em grupos dinâmicos**: é preciso garantir políticas de controle de acesso com diferentes níveis de granularidade e flexibilidade. Assim, será possível compartilhar dados com diferentes partes de acordo com o contexto e fazer revogações de acesso, se necessário.
- **Privacidade e remoção completa dos dados**: a privacidade dos dados tem que ser definida de tal forma que profissionais que trabalham no provedor de nuvem não tenham acesso aos dados. E, caso a contratação do serviço de nuvem seja encerrada, os dados devem ser completamente excluídos.

Para garantir alguns requisitos de segurança, como confidencialidade e privacidade dos dados, geralmente são utilizados mecanismos criptográficos. Na Tabela 2.6, há um resumo dos mecanismos citados em [Yang et al. 2020]. A escolha do tipo de mecanismo utilizado vai ser determinada por diversos fatores e determina o uso de diferentes funções (e.g., busca em dado criptografado) e níveis de segurança.

Tabela 2.6. Características de protocolos criptográficos usados em ambientes de nuvem.

Características	Classificação dos algoritmos	Revogação de Acesso
Identity-Based Encryption		
-Mecanismo tradicional de Infraestrutura de Chave Pública -Confirma a identidade através de Autoridade Certificadora confiável -Utiliza a chave pública do usuário para criptografar os dados	-N/A	-Existem alternativas na literatura [Boneh and Franklin 2001, Li et al. 2013] -Em [Boneh and Franklin 2001], a chave pública é definida utilizando ID + período de validade
Attribute-Based Encryption		
-Utiliza um conjunto de atributos para criptografar os dados -Apenas usuários com os atributos conseguem acessar os dados -Permite controle de acesso granular	-Key Policy Attribute-Based Encryption -Ciphertext-Policy Attribute-Based Encryption	-Oferta esquemas de revogação indireta ou direta [Xu et al. 2019, Attrapadung and Imai 2009, Shi et al. 2015]
Homomorphic Encryption		
-Possibilita a realização de operações algébricas nos dados criptografados -A acurácia do resultado deve ser avaliada	-Partial Homomorphic Encryption -Somewhat Homomorphic Encryption -Full Homomorphic Encryption	-N/A
Searchable Encryption		
-Busca em dados criptografados -Adequada para cenários com quantidade limitada de palavras-chave e volume de dados reduzido	-Searchable Symmetric Encryption -Public Key Encryption with Keyword Search	-N/A

Os mecanismos criptográficos garantem requisitos de privacidade e confidencialidade no armazenamento dos dados. No entanto, em alguns casos os dados precisam ser descriptografados na nuvem para processamento. Como esse processo pode deixá-los suscetíveis a acessos indevidos, tem-se observado a utilização de ambientes confiáveis de execução (do inglês, *Trusted Execution Environment* – TEE), cujo objetivo é proteger os dados no momento do processamento através da garantia de requisitos de confidencialidade e integridade. No entanto, há alguns desafios no uso de TEE, pois esses ambientes têm acesso limitado à memória e os aceleradores de renderização de gráficos (e.g., GPU) e de tarefas de aprendizado profundo (e.g.,TPU) ainda não proveem esse serviço. Portanto,

o uso de TEE para processamento de dados provê um mecanismo de processamento mais seguro, mas aumenta o tempo de análise. Em [Narra et al. 2019], os autores propõem uma solução denominada Origami para endereçar os problemas de eficiência ao utilizar TEE para processamento de dados sensíveis. Na solução proposta, os dados criptografados são enviados para o TEE, onde são descriptografados e particionados. Em seguida, o Origami aplica uma técnica de blindagem criptográfica para ofuscar os dados e encaminhá-los para processamento em um ambiente não seguro, como uma GPU.

Além dos processos de armazenamento e processamento dos dados, as aplicações de saúde necessitam também de políticas de acesso que possibilitem o compartilhamento seguro das informações geradas. A possibilidade de utilizar serviços de nuvem para compartilhar informações de saúde do indivíduo entre profissionais de saúde, cuidadores e os próprios pacientes minimiza os riscos de perda de registros, mas pode adicionar riscos associados à segurança e privacidade dos dados [Dang et al. 2019]. Nesses casos, os processos criptográficos e de autenticação devem considerar aspectos como liberação e revogação de acesso a diferentes usuários, mecanismos cientes de contexto para lidar com situações atípicas e/ou de emergência e soluções dinâmicas e flexíveis para controle de acesso [Yang et al. 2020]. Por exemplo, um indivíduo pode consentir que seus dados sejam acessados por equipes médicas para obter um tratamento personalizado, mas pode restringir o uso dos dados para usos secundários, como pesquisas governamentais sobre uma determinada doença [Philip et al. 2021]. É importante ressaltar que o múltiplo acesso às informações pode ocorrer entre diferentes provedores de nuvem. Então, é preciso atentar-se à interoperabilidade de estratégias de armazenamento de dados e segurança entre provedores distintos. Todos esses pontos relacionados à segurança são fundamentais para viabilizar aplicações em IoHT. No entanto, as características da comunicação entre os dispositivos e a nuvem também impactam o desenvolvimento dessas soluções.

A comunicação entre a borda da rede (sensores e dispositivos IoT) e a nuvem pode apresentar diferentes latência, largura de banda e níveis de segurança. Como algumas aplicações na área de saúde tem requisitos mais rigorosos em relação à conectividade e segurança, a computação em névoa tem sido usada como solução em algumas arquiteturas. Em [Aazam et al. 2020], os autores sugerem o uso de computação em névoa como uma espécie de *middleware* entre a borda e a nuvem. Os autores argumentam que a distância entre os servidores da nuvem e os equipamentos de borda limita o desenvolvimento de soluções de tempo real em IoHT. Além disso, os autores também argumentam que com o uso de computação em névoa, é possível prover um monitoramento mais individualizado dos dispositivos IoT, bem como estabelecer mecanismos de segurança e privacidade mais adequados às aplicações. É importante ressaltar, entretanto, que os dispositivos localizados na névoa não têm a mesma capacidade de armazenamento e processamento da computação em nuvem. Além disso, como os dispositivos estão mais próximos dos indivíduos ou instituições, em caso de desastres, é possível que ambos (borda e névoa) fiquem indisponíveis. Assim, fica clara a necessidade de usar uma arquitetura híbrida para possibilitar o desenvolvimento de aplicações que tenham requisitos de QoS mais estritos e para garantir premissas de segurança, como armazenamento de backup em locais distantes. Para realizar a integração e segurança entre os inúmeros componentes das aplicações baseadas em arquiteturas híbridas envolvendo borda, névoa e nuvem, comumente são utilizados *middlewares*.

2.3.4. *Middlewares*

Middlewares são *softwares* que atuam entre a aplicação e o sistema operacional e/ou rede. No contexto de IoHT, os *middlewares* são utilizados para endereçar requisitos da infraestrutura e da aplicação [Zgheib et al. 2019]. Em relação aos requisitos de infraestrutura, destaca-se a interoperabilidade entre os dispositivos, escalabilidade (quantidade de dispositivos), interações entre os equipamentos e diversidade da infraestrutura de comunicação. Já em relação aos desafios associados à aplicação, o foco é na disponibilidade e confiabilidade do serviço, tolerância a falhas, monitoramento em tempo real e aspectos de segurança e privacidade. Além disso, há uma necessidade de desenvolvimento de *middlewares* semânticos, visto que o uso de semântica pode auxiliar na redução de número de sensores utilizados e no desenvolvimento de aplicações mais inteligentes.

Os *middlewares* associados à saúde podem ser classificados em sete categorias: baseado em névoa, em modelo *publish/subscribe*, na Web das Coisas, em arquitetura orientada a serviço, orientado a eventos e orientado a mensagens [Fersi 2020]. A partir dessa classificação, os autores consideram a névoa como um *middleware* entre a borda e a nuvem, que possibilita alcançar requisitos de aplicação, como baixa latência. De acordo com essa classificação, não há um único tipo de *middleware* adequado para todas as aplicações de IoHT, portanto é possível combiná-los para tentar endereçar os requisitos da aplicação. Além disso, os *middlewares* de segurança devem ter constantes atualizações, para garantir eficácia à medida que novos mecanismos de ataque são identificados.

Pesquisadores da Universidade da California - Irvine (UCI) desenvolveram um *middleware* denominado Tippers[2] para gerenciamento de dados de sensores em espaços inteligentes. O Tippers consegue reduzir a complexidade do desenvolvimento de aplicações ao funcionar como um concentrador de dados de fontes variadas. A solução é considerada escalável e de fácil adaptação, uma vez que permite que novos sensores e tipos de sensores sejam adicionados sem que haja mudança no código da aplicação. Além disso, o Tippers também considera a implantação de estratégias de gerenciamento de dados que possibilita a integração de técnicas que garantam a privacidade dos usuários. Esse *middleware* tem sido utilizado no desenvolvimento de várias soluções que consideram questões como conectividade e privacidade dos usuários [Lin et al. 2020, Mehrotra et al. 2020, Ghayyur et al. 2020]. Atualmente, o Tippers tem sido usado no contexto do projeto CareDEX[3], que se trata de uma plataforma inteligente que tem como objetivo melhorar o tratamento de pessoas idosas, em cenários de desastre, através da troca segura de informações entre equipes de primeiros socorros, cuidadores e idosos em instituições de repouso. O Tippers também tem sido utilizado em outros campi para apoiar serviços de localização. O principal requisito endereçado por esse *middleware* é a interoperabilidade entre os dispositivos e transparência para a aplicação.

Em [Madureira et al. 2019] os autores desenvolveram um *middleware*, denominado My-AHA, com o objetivo de integrar soluções de saúde para pessoas idosas de forma segura. Os autores sinalizam que a maioria dos *middlewares* desenvolvidos são focados na interoperabilidade de dispositivos e eles expandem essa interoperabilidade para as soluções. O My-AHA é composto por um conjunto de conectores responsáveis por

[2] https://tippers.ics.uci.edu/

[3] https://sites.uci.edu/caredex/

coletar os dados disponibilizados pelas plataformas externas. Essa função é executada rotineiramente para que a aplicação tenha uma versão atualizada dos dados. A arquitetura da solução também é composta por um mecanismo de autenticação e autorização. Os usuários devem conceder acesso ao My-AHA, para que os conectores consigam consultar novos dados. Os dados advindos de outras plataformas são armazenados de forma anonimizada em uma base de dados do My-AHA. Os usuários podem interromper o compartilhamento de dados e solicitar que os dados enviados anteriormente sejam removidos da plataforma. Por fim, o My-AHA utiliza um mecanismo *publish/subscribe* para garantir o acesso dos dados coletados para diferentes partes. Esse *middleware* endereça requisitos como segurança e interoperabilidade de dispositivos e plataformas.

Em [Mukherjee et al. 2018], os autores propõem um *middleware* para prover segurança de forma flexível para aplicações de saúde. A proposta é promover um mecanismo de segurança flexível, que atenda os requisitos de segurança de cada aplicação, baseado nos recursos dos dispositivos na borda e na nuvem. Para identificar a melhor abordagem de segurança que deve ser utilizada, os autores consideram a intermitência da rede e restrições dos dispositivos (e.g., energia, computação, armazenamento, etc). De acordo com essas informações, é definido um esquema de segurança que inclui mecanismos de autenticação, criptografia dos dados e códigos de autenticação de mensagem. Caso haja problemas de intermitência na comunicação de rede, a solução faz uso de algoritmos de retomada de sessão, que reutilizam sessões criptografadas anteriormente por um mesmo dispositivo para retomar a conexão que foi interrompida. Além disso, o *middleware* também é responsável por determinar qual o melhor esquema de segurança para um cenário, considerando os requisitos da aplicação e as características dos dispositivos.

2.3.5. Aprendizado de máquina

O uso de técnicas de ML é comum nas aplicações e serviços de saúde para correlacionar e analisar os dados coletados pelos sensores, tornando possível a identificação de padrões, predição de eventos e sugestão de melhorias no tratamento dos indivíduos [Maskeliūnas et al. 2019, Wang et al. 2022]. Como os dispositivos IoT possuem restrições energéticas e baixa capacidade de armazenamento e processamento, os dados são enviados para serem armazenados e processados em outro local. Assim, as técnicas de ML podem ter funções variadas no contexto de saúde, como a análise de dados de conectividade que contribuem com o monitoramento do indivíduo ou com o desenvolvimento de novas técnicas de aprendizado que considerem requisitos de privacidade.

Ao executar as funções básicas de conectividade, os dispositivos de rede geram informações que podem beneficiar as aplicações. Em [Lin et al. 2020], os autores propõem a utilização de dados de conectividade Wi-Fi para localizar indivíduos em áreas internas de um espaço físico, como salas dentro de um prédio. Eles aplicam técnicas de pré processamento para melhorar a qualidade dos dados e aplicam uma técnica de aprendizado semi supervisionado e método probabilístico para realizar uma identificação semântica da localização do indivíduo. O uso desse sistema tem sido explorado no projeto CareDEX para identificar a localização de residentes dentro de instituições de repouso. Com a localização semântica dos residentes, é possível usar a aplicação para auxiliar na evacuação de idosos em cenários de emergência, bem como para identificar mudanças na rotina dos indivíduos. Nessa solução, os autores utilizaram um mapeamento entre identificador do

usuário, endereço MAC do dispositivo vestível, conexões dos dispositivos com os pontos de acesso e localização dos pontos de acesso na construção da solução. Além das informações utilizadas pelos autores, a análise de dados disponibilizados pelos equipamentos de rede e coletados por meio de protocolos como o *Simple Network Management Protocol* (SNMP) podem auxiliar as aplicações. Por exemplo, a análise automatizada de informações como frequência de *reboots* e aumento da temperatura do equipamento, quando associadas às informações de contexto, como localização dos dispositivos e horário, podem auxiliar na identificação e predição de problemas no local.

Do ponto de vista de segurança, embora o uso de TEE possa garantir algum nível de confidencialidade e privacidade dos dados, há casos em que a centralização de dados para processamento em um único local não é viável ou recomendada. Os dados dos indivíduos e de diferentes instituições podem ser utilizados, juntos, para avaliar e prover políticas de saúde para a população. No entanto, o compartilhamento desses dados é regulamentado por diferentes legislações e/ou termos de privacidade e o envio dos dados para processamento centralizado pode violar premissas de privacidade. Portanto, tem-se observado o uso de aprendizado federado, que permite que diferentes instituições compartilhem um modelo de aprendizado global enquanto mantém seus dados localmente, preservando requisitos de privacidade e confidencialidade. A arquitetura proposta para uso do aprendizado federado por ser vista na Figura 2.3. As instituições médicas atuam como nós de borda que executam localmente um modelo de aprendizado e deve encaminhá-lo periodicamente para o nó agregador. Esse nó agregador recebe os modelos de cada instituição e cria um modelo de treinamento global. O modelo de treinamento global é enviado novamente para as instituições. Durante esse processo, os dados são mantidos nas instituições e apenas os parâmetros e pesos utilizados no modelo são encaminhados entre os nós [Konečnỳ et al. 2016]. Esse método traz mais garantias de privacidade mas os resultados têm menos acurácia. Além disso, apesar de a solução não encaminhar dados médicos entre os nós, é importante avaliar se os parâmetros e pesos encaminhados entre os nós podem gerar vazamentos em relação à privacidade.

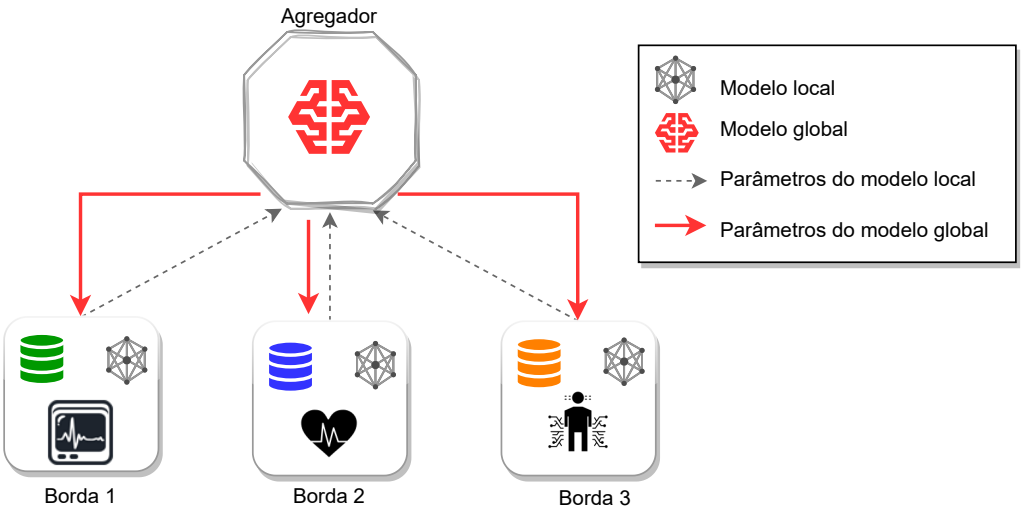

Figura 2.3. Representação do funcionamento da técnica de aprendizado federado.

Os autores em [Du et al. 2020] fazem uma análise de diferentes técnicas de aprendizado de máquina em relação a aspectos como distribuição de dados, acurácia, comunicação e privacidade. O aprendizado centralizado é aquele que possui maior acurácia, pois todos os dados estão no mesmo local. No entanto, isso significa mais riscos à privacidade e maior consumo de banda, visto que todos os dados devem ser enviados para um nó centralizador. O aprendizado federado é o que menos consome banda e mais preserva a privacidade, mas tem menor acurácia. Assim, a solução de aprendizado par-a-par pode ser considerada um meio termo entre essas soluções, pois também preserva a privacidade do usuário e tem uma acurácia moderada. O aspecto negativo é um consumo de banda superior às técnicas de aprendizado federado. Em suma, é preciso avaliar quais tipos de técnicas de ML são adequadas a cada aplicação considerando seus requisitos.

2.4. Requisitos de Comunicação e Segurança da Informação

A adoção de soluções de sistema de vida assistida dependem diretamente do tratamento dos requisitos dos usuários e das aplicações. Como a comunicação e a segurança são aspectos essenciais na viabilidade desses sistemas, a forma de tratamento desses requisitos é descrita nesta seção. Inicialmente, serão discutidos os requisitos gerais, e, em seguida, os principais requisitos em termos de conectividade, mobilidade, QoS e QoE. Em seguida, serão abordados os aspectos relacionados à segurança, considerando princípios como disponibilidade, integridade e confidencialidade.

2.4.1. Requisitos Gerais e de Comunicação

Em geral, os requisitos dos sistemas de vida assistida estão associados a três etapas: *(i)* coleta dos dados e transmissão até um ponto de acesso, *(ii)* transmissão dos dados através das redes de acesso até a Internet e *(iii)* a integração das informações coletadas e da transmissão de dados via comunicação fim-a-fim. A Figura 2.4 ilustra essas etapas da comunicação em sistemas apoiados pela IoHT e as principais entidades envolvidas.

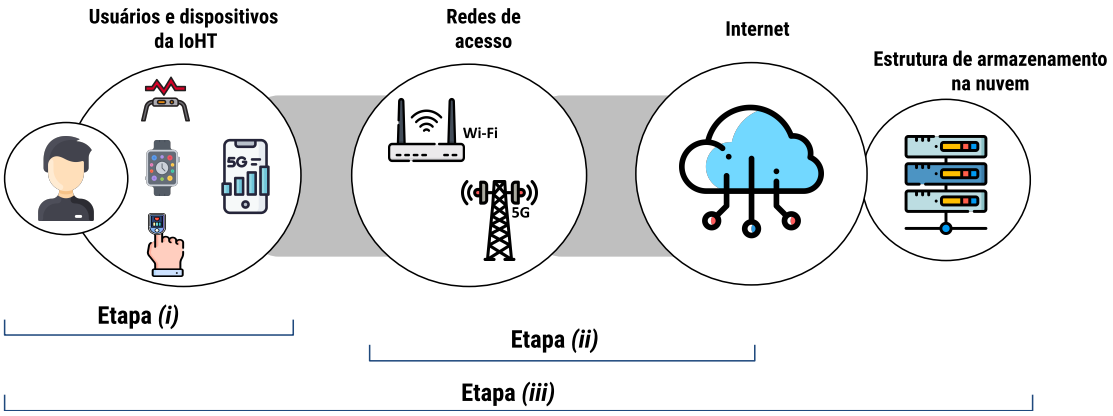

Figura 2.4. Etapas da comunicação em sistemas baseados na IoHT.

Considerando inicialmente a **comunicação entre um dispositivo de coleta de dados e um ponto de acesso**, os principais requisitos estão relacionados com os dispositivos e com os protocolos de comunicação de curto alcance. Em relação aos dispositivos, tem-se os seguintes requisitos: os dispositivos de coleta de dados devem funcionar de maneira

ininterrupta para aplicações críticas (e.g., monitoramento da frequência cardíaca), deve haver compatibilidade entre os dispositivos, os dispositivos devem alcançar um ciclo de vida de bateria longo e utilizar baterias que sejam facilmente recarregadas ou substituídas. Além disso, os protocolos de comunicação devem considerar a eficiência energética e os dispositivos devem ter recursos de armazenamento para evitar perda de dados nos casos de instabilidade da rede ou desconexões. Por fim, o sistema deve gerenciar a entrada e saída de nós de forma automática e seus componentes devem ser facilmente substituídos e atualizados, favorecendo requisitos de gerenciamento, manutenibilidade e escalabilidade.

A segunda etapa de comunicação está relacionada com **o acesso da rede interna à Internet**. A comunicação entre os pontos de acesso e a Internet pode ocorrer de maneiras distintas nos sistemas de vida assistida, dependendo do nível de mobilidade envolvido. Os sistemas mais tradicionais usam dispositivos estáticos e pontos de acesso fixos atrelados a redes estruturadas. No entanto, esse mecanismo de conexão tem cobertura de sinal limitada e restringe a mobilidade do usuário. Assim, é comum o uso de redes móveis, como as redes 4G/5G, que permitam a comunicação de dispositivos portáteis ou vestíveis à Internet mesmo quando o usuário está em movimento. Independente do tipo de rede utilizada, o principal requisito dessa etapa é que os dados coletados cheguem até a infraestrutura que irá armazená-los. Para garantir essa premissa, é importante que haja redundância nos canais ou tecnologias de comunicação e redundância de dispositivos de rede, como os pontos de acesso. Embora essas garantias de redundância possam ser difíceis de serem alcançadas em cenários domésticos devido às restrições de custo ou mesmo por falta de conhecimento técnico, essas alternativas devem ser consideradas imprescindíveis em instituições de saúde como hospitais ou casas de repouso para idosos.

A etapa da **comunicação fim-a-fim** compreende todo o caminho percorrido pelos dados. Os requisitos desta etapa incorporam as duas etapas anteriores e todos os elementos envolvidos. No entanto, mesmo atendendo os requisitos citados anteriormente, ainda há problemas que podem impactar as aplicações. Por exemplo, mesmo que haja redundância e que os problemas de compatibilidade sejam sanados, ainda pode haver variações no desempenho da comunicação. Neste caso, torna-se necessária a redundância ou variação nas tecnologias de comunicação que garantam a transmissão das informações em tempo hábil e de forma íntegra. Alguns protocolos, como o BFD (*Bidirectional Forwarding Detection*), são utilizados para detecção de falhas e mudanças de rota de forma proativa. Esses protocolos geralmente funcionam adequadamente em casos de desconexões, realizando a migração para o caminho redundante, mas podem apresentar comportamento indesejado em casos de instabilidade de enlaces: perdas de pacotes no enlace principal podem gerar mudanças frequentes entre as rotas principal e secundária. Por fim, as mesmas garantias de disponibilidade sinalizadas anteriormente devem ser ofertadas considerando o destino final da informação, seja o armazenamento em um dispositivo remoto ou na nuvem. O não cumprimento desses requisitos pode implicar em dados corrompidos, ausentes ou entregues com alto atraso, inviabilizando o uso de algumas aplicações.

Outros requisitos relacionados à infraestrutura, mas complexos de serem alcançados incluem: redundância de dispositivos de coleta de dados, multiplicidade de dispositivos com mesma funcionalidade e tecnologias de comunicação distintas, pontos de acesso que suportam múltiplas tecnologias de comunicação de curto alcance e atendam diversos dispositivos, mecanismos de proteção contra a interferência cruzada causada pela vari-

edade de tecnologias de comunicação, interoperabilidade de dispositivos proprietários e sua integração transparente ao ambiente. A dificuldade em alcançar esses objetivos ocorre por duas razões principais: falta de integração entre as etapas da comunicação e excesso de padrões existentes e em desenvolvimento para cada uma delas. A variedade de padrões dificulta a comunicação em cenários que diferentes dispositivos se comunicam entre si em busca de oferecer serviços mais robustos aos usuários, como é o caso de sistemas de vida assistida. Alguns dispositivos IoT suportam protocolos M2M, como o CoAP, MQTT e AMQP, mas é preciso ainda garantir a interoperabilidade entre esses protocolos e dispositivos médicos que são baseados em outros protocolos de troca de mensagem.

Alguns requisitos dos sistemas de vida assistida estão relacionados à adoção dos dispositivos e do sistema pelos usuários. De uma forma geral, os usuários buscam requisitos como simplicidade de uso, adaptabilidade, uso de contexto, intuitividade, utilidade e confiabilidade. Além disso, muitos dispositivos são posicionados no corpo do indivíduo e devem ser anatômicos e não causar desconforto ao usuário. A não garantia desses requisitos pode gerar fracasso na adoção das soluções. Assim, dispositivos portáteis e vestíveis com interfaces de toque na tela devem ter operação intuitiva e facilitada para que pessoas de diferentes faixas etárias consigam utilizá-las. As funcionalidades e os dispositivos do sistema devem ser expostos ao usuário para que o mesmo não tenha dúvidas sobre como e com qual finalidade os dados serão utilizados. Em relação aos dados coletados, para garantir suporte aos sistemas de vida assistida, é importante endereçar requisitos como veracidade, integração, privacidade, confiabilidade e segurança. Uma discussão mais aprofundadas desses tópicos será realizada na Seção 2.4.4.

2.4.2. Mobilidade

A mobilidade nos sistemas de vida assistida pode ocorrer de duas formas: de maneira mais tradicional como nas aplicações AAL, cujo objetivo é fornecer mobilidade em um espaço delimitado e restrito por um tecnologia sem fio de curto alcance, como o Wi-Fi; ou em uma vertente mais atual, com uso de sistemas de vida assistida portáteis que visam oferecer uma mobilidade maior ao usuário, empregando tecnologias de comunicação de longo alcance e permitindo uma maior área de cobertura e comodidade para o usuário. Os sistemas de vida assistida portáteis promovem uma maior mobilidade e qualidade de vida para o usuário ao criar um ambiente mais imersivo e integrado em termos de dispositivos e tecnologias de comunicação. Isso é possível pois os dispositivos da IoHT são dotados de tecnologias de comunicação cada vez mais eficientes e versáteis. Os *smartphones* incorporam processadores de alta capacidade e complexidade computacional e oferecem as tecnologias de comunicação mais recentes. Em geral, a configuração inicial dos sistemas de vida assistida portáteis usa um *smartphone* como coordenador dos dispositivos de coleta de dados. Esses dispositivos confiam no coordenador para executar as funções que demandam mais processamento e memória, e para garantir o acesso à Internet. Essa configuração é cômoda para o usuário uma vez que grande parte da população possui um *smartphone* para executar tarefas básicas e se conectarem à Internet quando estão em movimento. Além disso, esses equipamentos contam com tecnologias de curto alcance como Bluetooth e NFC para a sincronização de dispositivos.

Considerando a miniaturização dos componentes e a inclusão de novas tecnologias de comunicação em equipamentos vestíveis, uma nova configuração para os dispositivos

da IoHT começa a surgir: os dispositivos estão sendo disponibilizados nativamente com conexões de longa distância, como a LTE. Isso modifica a arquitetura tradicional baseada em um dispositivo coordenador e traz mais liberdade para os usuários pois sensores e equipamentos vestíveis com tecnologias de longo alcance permitem a conexão constante com a Internet e dispensam o uso de um coordenador ou um ponto de acesso fixo.

2.4.3. Qualidade de Serviço e Qualidade de Experiência

Sistemas baseados em IoT conectam, além de pessoas, vários dispositivos que, de maneira ativa ou passiva, compõem o sistema. Para integrar esses componentes, empregam-se diferentes protocolos e tecnologias de comunicação com capacidades distintas de oferecer QoS. Entretanto, para garantir que as aplicações apoiadas nesses sistemas funcionem conforme o esperado torna-se necessário enfrentar os desafios em termos de variação de desempenho e heterogeneidade de tecnologias. Na Tabela 2.7 há uma lista de dispositivos empregados na IoHT, as tecnologias de comunicação disponíveis e os respectivos requisitos para comunicação relacionados com algumas métricas de QoS e QoE. Nota-se que dispositivos com mais recursos apoiam mais aplicações e possuem requisitos mistos, enquanto dispositivos de transmissão de áudio e vídeo têm requisitos estritos em termos de latência e capacidade, e sensores específicos para aplicações de saúde requerem altos índices de confiabilidade e baixa latência devido à criticidade das informações.

Tabela 2.7. Requisitos de comunicação para os dispositivos da IoHT e suas tecnologias. Adaptado de [Devi et al. 2023].

Dispositivo	**Tecnologias**	**Requisitos para Comunicação**		
		Latência	**Capacidade**	**Confiabilidade**
Smartphone	LTE, Bluetooth, mmWave Celular, WLAN	Regulares	Regulares/Altos	Regulares
Relógio ou Óculos Inteligente	LTE, Bluetooth	Regulares	Regulares	Baixos
Disp. de Realidade Virtual e Realidade Aumentada	mmWave Celular, WLAN	Altos	Altos	Baixos
Tablet	LTE, Bluetooth, mmWave Celular, WLAN	Regulares	Regulares/Altos	Regulares
Roupa ou Tênis Inteligente	Zigbee, Bluetooth	Baixos	Baixos	Baixos
Sensores Médicos	LTE, Bluetooth	Altos	Baixos	Altos

Garantir QoS em sistemas de vida assistida é um grande desafio devido às variações de desempenho das tecnologias de comunicação empregadas. Essas variações ocorrem devido às especificações heterogêneas das tecnologias de comunicação, aos múltiplos enlaces que podem ocasionar gargalos na comunicação e à multiplicidade de aplicações concorrentes que utilizam o sistema. A falha ao atender os requisitos de QoS tem impactos negativos na percepção do usuário ao utilizar as aplicações que requerem interação humana, ocasionando baixa QoE. A ligação entre QoS e QoE é evidente, mas existe um desafio ao aferir a QoE para as aplicações nos sistemas de vida assistida que não exigem participação específica de um usuário. Embora os cumprimentos dos requisitos de QoS sejam um bom parâmetro, eles não garantem uma boa experiência para o usuário final.

Existem diversos trabalhos na literatura que exploram o levantamento de requisitos de QoS para aplicações apoiadas na IoT tradicional [Adil et al. 2022]. Entretanto,

os sistemas de vida assistida demandam alterações na identificação dos requisitos e nas implementações em nível operacional para o cumprimento dos mesmos. A Tabela 2.8 ilustra algumas diferenças fundamentais entre a IoT e a IoHT. As características da IoHT em termos de criticidade das aplicações de saúde, necessidade de mobilidade, resiliência das informações e eficiência energética são os principais pontos que diferenciam a IoHT e a IoT e que demandam requisitos mais estritos. Apesar dessas diferenças serem significativas, poucos trabalhos disponíveis na literatura abordam a QoS e QoE em IoHT.

Tabela 2.8. Particularidades operacionais da IoT e IoHT. Adaptado de [Adil et al. 2022].

Particularidades da IoT tradicional	Particularidades da IoHT
Aplicações para diversas finalidades	Aplicações relacionadas à saúde
Aplicações com requisitos variados	Aplicações com requisitos estritos
Aplicações não demandam alta precisão nos resultados	Requer resultados precisos e específicos
Facilidade de implementação e configuração	Precisão depende da correta configuração
Falhas não impactam o sistema de forma crítica	Falhas colocam em risco a saúde do usuário
Tráfego de dados intermitente e volumoso	Tráfego crítico e eventual
Eficiência energética impacta o custo do sistema	Eficiência energética impacta a qualidade de vida

Considerando as particularidades da IoHT e observando os requisitos de comunicação e segurança nos sistemas de vida assistida, encontramos os seguintes desafios ao propor níveis de QoS que satisfaçam a necessidade das aplicações: desafios relacionados à coleta dos dados, às arquiteturas de rede, à segurança, à interoperabilidade e à escalabilidade. A coleta dos dados requer rapidez e acurácia por parte de sensores e dispositivos, para que isso aconteça uma série de outros requisitos devem ser cumpridos sob risco da incidência de atrasos e informações faltantes. Sendo assim, os desafios na etapa da coleta de dados acabam se estendendo para a correta instalação e uso dos dispositivos por parte dos usuários ou prestadores de serviço, pois o atraso por falhas ou uso inadequado de um dispositivo irá se propagar para os serviços dependentes da informação. A necessidade da informação sempre à disposição impacta ainda os dispositivos alimentados por baterias e a capacidade dos canais de comunicação estarem sempre disponíveis.

Uma das formas de lidar com os problemas relacionados à garantia da QoS em ambientes IoHT envolve o estudo de protocolos de roteamento mais eficientes. Entretanto, a segmentação das redes em conjunto com o uso de tecnologias proprietárias, principalmente nas redes dos dispositivos de coleta de dados, causam problemas de interoperabilidade e dificultam o cumprimento dos requisitos de QoS. Outros problemas que afetam a entrega de QoS incluem: mecanismos proprietários de criptografia dos dados e autenticação dos usuários, formatos específicos de compressão dos dados que impactam no cálculo do atraso, dificuldade em estimar os tempos de gravação e recuperação dos dados em ambientes distintos como nuvem, névoa, bordas ou em um dispositivo específico.

A avaliação de QoE depende da interpretação do usuário, do desempenho do sistema e do contexto de utilização. Geralmente, aplicações com um fluxo constante de dados tem maior impacto na percepção do usuário. Aplicações que envolvam áudio e vídeo permitem que os usuários detectem falhas mais facilmente e estão presentes na telemedicina e no monitoramento de pacientes em tempo real. No entanto, a interconexão exclusivamente entre dispositivos é uma das características da IoHT, incluindo a ausência completa de interação humana em diversas etapas do ciclo da informação. Isso traz difi-

culdade para mensurar a QoE uma vez que os dispositivos não têm a mesma percepção de um usuário e não é possível confiar somente nos requisitos da QoS devido aos problemas relacionados à heterogeneidade do ambiente. Nesse sentido, algumas propostas para prover a QoS de forma autônoma a partir de diversos parâmetros de configuração e requisitos, começam a surgir na literatura. No trabalho proposto em [Bardalai et al. 2022], os autores empregam modelos de aprendizado de máquina para auxiliar na tomada de decisão, fortalecendo o provisionamento tanto de QoS quanto de QoE.

Existe uma diversidade de pontos em aberto envolvendo QoS e QoE em ambientes complexos, como a IoHT. Os esforços estão direcionados para resolver os problemas em cada etapa da comunicação e os desafios são numerosos. Ainda assim, mesmo que um segmento específico consiga cumprir todos os requisitos e garantir os requisitos de QoS isoladamente, ainda existe o problema relacionado à segmentação dos serviços, como o atraso e as falhas em cascata, onde um problema original causa transtornos nos serviços subsequentes. Uma solução seria a possível orquestração dos serviços dependentes, mas essa integração é complexa uma vez que em geral não existe controle sobre os enlaces mais distantes do usuário como as redes de acesso e a própria nuvem e seus canais de comunicação. Nesse cenário, a QoE torna-se um parâmetro avaliativo útil porém sem uma indicação específica que contribua para redefinir os requisitos de QoS.

2.4.4. Segurança da Informação

Os princípios básicos de segurança aplicados aos sistemas tradicionais como: disponibilidade, integridade, confidencialidade e privacidade, são ainda mais importantes em sistemas de vida assistida devido à sensibilidade das informações coletadas e distribuídas. Em geral, os dados existentes nesses sistemas representam informações pessoais e privadas. Sendo assim, sua disseminação não autorizada pode ter consequências graves para os usuários do sistema, prestadores de serviço e fabricantes de dispositivos. Adicionalmente, as informações armazenadas e transmitidas devem estar imunes de manipulação por entidades não autorizadas e disponíveis sempre que uma entidade autorizada necessitar acessá-las. Finalmente, não deve ser possível identificar um usuário do sistema através de dados coletados nos canais de comunicação ou armazenados em dispositivos e bases de dados, sem a devida autorização. A Figura 2.5 ilustra os princípios básicos de segurança nos sistemas de vida assistida e as principais ameaças a cada um deles.

A segurança de um sistema, como um todo, é proporcional às garantias de segurança do elo mais fraco e os princípios de segurança apresentam relações entre si. A partir da Figura 2.5, é possível observar relações de interdependência entre os princípios de segurança e a diversidade de alvos em relação aos tipos de ataque. Por exemplo, ataques que afetam a autenticação e autorização de dispositivos podem comprometer a integridade do sistema como um todo. Neste sentido, tem-se o desafio de desenvolver e usar soluções de segurança que sejam integráveis ou interoperáveis para prover uma alternativa de segurança que contemple todos os componentes do sistema. Durante esse processo, deve-se avaliar os recursos dos componentes e as alternativas que podem ser utilizadas. Em paralelo, esses mecanismos de segurança devem ainda atender às regulações de privacidade – que podem variar em diferentes países e estados – e proporcionar políticas de controle de acesso que podem variar em diferentes níveis (e.g., borda, névoa e nuvem) e contextos (e.g., emergências e desastres). Alguns desses pontos serão discutidos nas próximas

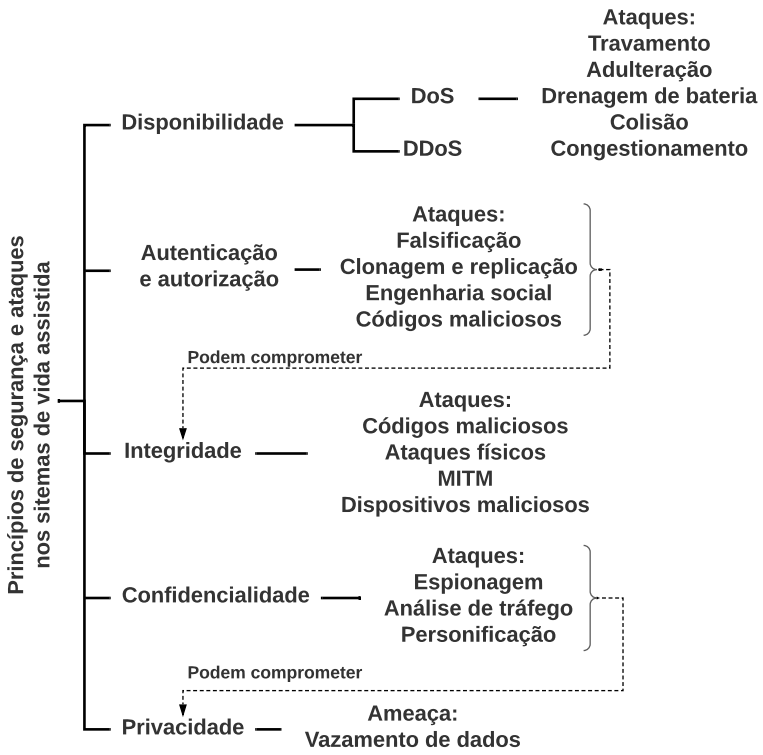

Figura 2.5. Princípios básicos e ameaças de segurança em sistemas de vida assistida.

seções, onde serão explorados os requisitos associados à segurança em IoHT.

2.4.4.1. Disponibilidade

O princípio da disponibilidade está associado com o acesso às informações e visa assegurar que os dados e serviços estejam disponíveis, quando necessário, e que os serviços prestados não sejam negados a nenhum usuário ou subsistema autorizado. Nos sistemas de vida assistida, a disponibilidade das informações e serviços está diretamente relacionada com a confiabilidade do sistema pelos indivíduos, familiares e equipe médica. Isso se dá, principalmente, porque interrupções na oferta de serviços ou a indisponibilidade dos dados requisitados pode ocasionar situações que coloquem o usuário em perigo, incluindo casos de risco à vida. Nestes cenários, os riscos associados à disponibilidade e as estratégias para mitigá-los devem considerar as características dos elementos do sistema: sensores e dispositivos IoT, canais de comunicação e serviços de nuvem.

Todas as soluções de comunicação e segurança para os sensores e dispositivos IoT precisam respeitar a limitação dos recursos, como tempo de bateria, baixo poder computacional e memória. Desta forma, os processos que são executados nos dispositivos precisam ser simples e ter baixo consumo energético. A preocupação com o consumo energético impacta na relação entre a disponibilidade e outros princípios de segurança, como confidencialidade. Para garantir confidencialidade, geralmente são utilizados mecanismos criptográficos, mas o processo de criptografar os dados coletados pelos sensores antes do envio gera a necessidade de mais processamento nos dispositivos. Esse processamento adicional implica em consumo energético, que pode diminuir o tempo de vida

da bateria e afetar a disponibilidade.

Outro aspecto fundamental relacionado à disponibilidade é a necessidade de monitoramento e detecção de falhas. A variação nas características de coleta e envio de dados pelos sensores e dispositivos IoT pode gerar a necessidade de uso de diferentes mecanismos de monitoramento. O monitoramento e a detecção de falhas é mais simples em dispositivos que realizam coletas e envio de dados constantes ou em uma frequência predefinida, visto que a própria falta de recebimento dos dados pela aplicação pode indicar uma falha na rede ou no equipamento. No entanto, alguns dispositivos são programados para enviar informações apenas em situações específicas. Para esses casos, torna-se imprescindível a utilização de alternativas de monitoramento, como o envio de *heartbeats*. Nos casos em que é necessário gerar tráfego adicional para realizar o monitoramento, é importante considerar o *tradeoff* com o consumo energético e ajustar o algoritmo de acordo com as necessidades do sistema. Por exemplo, seria importante definir um intervalo ótimo entre o envio dos *heartbeats* e o consumo energético, de forma que fosse possível detectar as falhas em um período considerado adequado para a aplicação sem exaurir a bateria do dispositivo apenas com mensagens desse tipo.

Devido às características computacionais restritas, torna-se desafiador implementar mecanismos de segurança para proteger os dispositivos que compõem um sistema de vida assistida, deixando-os vulneráveis a uma série de problemas de segurança conhecidos. Como foi observado na Figura 2.5, as principais ameaças de segurança que impactam a disponibilidade em um sistema de vida assistida estão relacionadas a ataques de adulteração, ataques de travamento, drenagem de bateria, ataques de colisão e congestionamentos na rede. Essa gama de ataques é comumente conhecida como ataques de negação de serviço (do inglês, *Denial of Service* – DoS). Variações desses ataques ganharam notoriedade nos últimos anos na forma de ataques DoS distribuídos (DDoS). Tanto os ataques DoS quanto os DDoS oferecem riscos aos sistemas de vida assistida, porém em fases diferentes do processo de aquisição e armazenamento de dados. Os ataques direcionados aos dispositivos da IoHT têm o objetivo de desabilitar temporariamente ou em definitivo um dispositivo. A indisponibilidade do dispositivo pode ocasionar dados faltantes e prejudicar a acurácia da aplicação. Para lidar com ataques DoS e DDoS, é interessante que o problema seja tratado o mais próximo possível da fonte de ataque. Desta forma, é interessante aplicar estratégias de detecção e mitigação de ataques DoS no dispositivo coordenador e no roteador de borda da rede. Assim, se houver um ataque com origem interna, o coordenador pode auxiliar na detecção e mitigação do ataque. Em paralelo, se houver um ataque com origem externa, é possível fazer uso de regras no roteador de borda para tentar efetuar o bloqueio do tráfego malicioso.

Já a disponibilidade associada aos serviços de nuvem geralmente é de responsabilidade do próprio provedor. Apesar disso, em alguns casos é possível contratar serviços que aumentam as garantias de disponibilidade da conexão e da aplicação. Ataques DDoS em estruturas de nuvem exigem o uso de múltiplos dispositivos que são coordenados remotamente para gerar um grande fluxo de dados para um alvo específico com o objetivo de desabilitar temporariamente o serviço prestado. Esses ataques são menos comuns devido ao uso de soluções robustas de mitigação de DDoS pelos prestadores de nuvem e à complexidade dos ataques para que sejam efetivos. Em relação a esses ataques, é importante proteger os dispositivos IoHT utilizados no monitoramento do indivíduo para

que eles não sejam comprometidos por usuários maliciosos e usados para realizar ataques em outras estruturas. Esse tipo de ação evita o consumo energético dos dispositivos para atividades maliciosas e colabora com a segurança da Internet.

Além da garantia de disponibilidade dos sensores, dispositivos IoT e da nuvem, também é importante observar a disponibilidade dos mecanismos de comunicação. Como foi citado anteriormente, a garantia da disponibilidade da rede geralmente está associada ao uso de equipamentos, tecnologias e caminhos redundantes. Algumas discussões a respeito disso foram tratadas quando foram apresentados os requisitos de comunicação. Em relação ao monitoramento dos canais de comunicação, é preciso pensar em aplicações de monitoramento simples de serem instaladas e utilizadas em WBAN e/ou WSN. Neste sentido, há também a necessidade de definição de quem será responsável pelo monitoramento e suporte da rede, bem como quais são os níveis de acordo de serviço em relação à manutenção em caso de problemas. Esses aspectos são essenciais para o uso de aplicações de sistema de vida assistida por usuários comuns, em particular, por pessoas idosas.

2.4.4.2. Integridade

O princípio da integridade visa assegurar que os dados não sejam alterados ou destruídos de maneira não autorizada. No contexto dos sistemas de vida assistida o princípio da integridade busca preservar a exatidão das informações sobre um usuário, sejam dados de saúde, localização ou demais informações pessoais. Recentemente, a popularização dos dispositivos IoT aplicados aos sistemas de saúde impulsionou o debate acerca da necessidade de um maior cuidado com a integridade dos dados que trafegam nesse tipo de ambiente. As características dos dispositivos e canais de comunicação presentes nos sistemas de vida assistida, especialmente quando a mobilidade é um fator preponderante, cria uma diversidade de pontos de vulnerabilidade que podem ser explorados. As medidas corretivas e a utilização de programas, dispositivos e tecnologias de comunicação que estejam alinhadas com políticas de proteção da integridade dos dados são fatores cruciais para a aceitação e adoção em massa dos sistemas de vida assistida.

As principais ameaças para a integridade dos dados nos sistemas de vida assistida estão relacionadas à manipulação da informação de maneira indevida durante sua transmissão. Isso pode ocorrer através de um código malicioso que infecta um dispositivo e captura e modifica informações relevantes, ou através de um ataque direcionado aos canais de comunicação. Outra possibilidade é um ataque físico diretamente ao dispositivo, no qual o usuário malicioso consegue obter e manipular os dados coletados. Em geral, esse tipo de ataque requer alguma informação inicial para acesso ao dispositivo como um nome de usuário, senha ou ambos. Um dos ataques direcionados aos meios de transmissão é o ataque *Man-in-the-middle* (MITM), onde um atacante consegue personificar um dos agentes do sistema e a partir dessa ação passa a alterar as informações recebidas e enviadas. Por fim, também pode acontecer a inserção de um dispositivo malicioso no sistema para coletar informações relevantes e enviar dados manipulados. É importante ressaltar que no contexto da IoHT esses ataques são de difícil execução devido à mobilidade envolvida e a proximidade dos dispositivos em relação ao usuário. Algumas contramedidas que podem ser adotadas para evitar ataques de integridade estão relacionadas com o uso de canais de transporte criptografado, mecanismos de autenticação e autorização dos dispositivos e mudança de configurações padrões, como usuário e senha de acesso.

É comum que as preocupações relacionadas à integridade estejam associadas à ameaças externas, como usuários maliciosos. No entanto, a garantia da integridade também inclui aspectos como corretude e acurácia dos dados pois, na IoHT, a inacurácia dos dados coletados pode causar riscos superiores à ausência de dados. Esses problemas na acurácia dos dados podem ocorrer por vários motivos, como mau posicionamento do sensor, interferência de sinal, problemas no funcionamento do dispositivo, configurações de data e hora incorretas, falta de calibração, entre outros. Assim, é importante que sejam adicionados mecanismos de detecção de anomalias aos sistemas de detecção de falhas. Além disso, é importante que seja feito um período de adaptação de uso do sistema de vida, para determinação de um *baseline* que possa servir como parâmetro tanto para as aplicações de saúde, quanto para as aplicações de detecção de falhas e anomalias.

2.4.4.3. Confidencialidade

O princípio de confidencialidade estabelece que as informações de cunho confidencial não sejam compartilhadas com entidades não autorizadas. Nos sistemas de vida assistida a confidencialidade se refere, por exemplo, à proteção dos dados de um indivíduo que são compartilhados com um médico ou prestador de serviço de saúde e não devem ser repassados a terceiros e utilizados para fins distintos do que foi autorizado. Os dados do usuário devem ser protegidos ainda contra invasores que vasculham os canais de comunicação em busca de informações sensíveis, e quando armazenados devem ser protegidos contra intrusão. Ao adotar medidas de proteção que substanciam o princípio da confidencialidade torna-se mais complexa a tarefa de identificar um usuário a partir dos dados coletados de maneira indevida, auxiliando o princípio da privacidade dos dados.

As principais ameaças à confidencialidade em sistemas de vida assistida ocorrem quando um atacante monitora e subtrai informações dos canais de comunicação [Hasan et al. 2022]. Geralmente esse tipo de ataque ocorre em duas etapas: obtenção dos fluxos de dados através de monitoramento passivo e análise do tráfego capturado. Os ataques de espionagem (do inglês, *eavesdropping attacks*), ocorrem quando o atacante "escuta" os canais de comunicação disponíveis em busca de informações relevantes. Considerando as tecnologias de comunicação sem fio, o alcance da tecnologia será o principal fator para determinar o raio de ação do atacante. Sendo assim, tecnologias de alcance muito curto, como o Bluetooth, dificultam a ação dos atacantes, enquanto tecnologias como o Wi-Fi permitem que o atacante monitore a rede de uma distância maior.

Após capturar uma quantia significativa de dados, o atacante analisa os dados coletados em busca de informações importantes [Brezolin et al. 2022]. A filtragem inicial busca por palavras-chave, nomes de usuário, identificações únicas dos dispositivos, e demais informações que podem ser obtidas facilmente. Em uma verificação mais profunda, o atacante pode tentar correlacionar características específicas disponíveis no conjunto de dados para identificar um usuário ou um dispositivo. Caso o atacante tenha sucesso em identificar o usuário, os dispositivos que compõem o ambiente ou consiga definir o comportamento de ambos, além da confidencialidade o atacante estará atuando contra o princípio da privacidade dos dados. Outro tipo de ataque que pode afetar a confidencialidade são os ataques de personificação. Nesse caso, após a análise de tráfego e identificação de credenciais válidas um atacante personifica um usuário ou um dispositivo com o objetivo de obter informações continuamente. Caso tenha sucesso, o atacante pode repassar

informações distorcidas dentro do sistema, impactando o princípio da integridade.

A maioria das soluções relacionadas com confidencialidade envolve o uso de criptografia no canal de comunicação e nos dados. Do ponto de vista dos dados, é possível utilizar diferentes mecanismos criptográficos para garantir a confidencialidade e privacidade. Alguns desses mecanismos foram abordados na Seção 2.3.3 quando foi tratado do armazenamento e processamento em nuvem. O processo criptográfico deve ser realizado antes dos dados serem enviados para a nuvem. Como os sensores têm capacidade de recurso bastante limitada, a comunidade científica tem buscado soluções *lightweight* que garantam a confidencialidade sem exaurir os recursos dos sensores e dispositivos IoT. Na comunicação fim a fim, é comum a utilização de protocolos como o TLS (*Transport Layer Security*) ou alternativas de criação de túnel, como IPSec. Além disso, também há recomendação de segurança que devem ser adotadas de acordo com o tipo de protocolo sem fio utilizado [Souppaya and Scarfone 2012, Fan et al. 2017, Padgette et al. 2017].

Em [Kumar et al. 2018], há a sugestão de uso de *blockchain* para alcançar requisitos de segurança em aplicações de saúde. O uso da *blockchain* garante o princípio da integridade, visto que uma vez que a informação estiver no livro-razão, não poderá ser modificada. Além disso, também contribui com a disponibilidade ao distribuir os dados e processamento em diferentes nós. Por fim, auxilia na garantia da confidencialidade e privacidade ao fazer uso de contratos inteligentes para controlar o acesso aos dados. Além do uso de *blockchain*, tem-se sugerido o desenvolvimento de soluções de criptografia "pós computação quântica". Os algoritmos criptográficos atuais são baseados em problemas matemáticos complexos que não podem ser resolvidos por computadores tradicionais em tempo hábil para realização de ataques. No entanto, há a expectativa de que com a computação quântica esses algoritmos tornem-se quebráveis. Assim, espera-se o desenvolvimento de novos algoritmos que considerem esse cenário [Yang et al. 2020].

2.4.4.4. Privacidade

O princípio da privacidade é a propriedade de um sistema que busca assegurar que os dados particulares de um usuário sejam protegidos contra divulgação não autorizada ou tentativas de exploração ilegal dessa possível divulgação. As principais preocupações associadas à quebra da privacidade em sistemas de vida assistida estão relacionadas ao uso indevido dos dados e suas implicações, como a divulgação de informações em redes sociais, o uso das informações para ameaças, e a divulgação de dados não autorizada por parte de prestadores de serviço. Para um usuário do sistema de vida assistida qualquer vazamento de informação proveniente de um dispositivo participante pode representar a divulgação não autorizada de uma condição de saúde, da sua localização, de um comportamento ou rotina específica além de informações complementares que podem ser empregadas em golpes ou tentativas de extorsão. Para fabricantes de equipamentos ou prestadores de serviço, o vazamento de informações privadas pode representar a perda da credibilidade, trazendo danos imensuráveis.

A informação sensível armazenada por prestadores de serviço de saúde é um dos principais focos de vazamento de dados [Alhaj et al. 2022]. Sendo assim, todos os pontos de armazenamento devem ter mecanismos de controle de acesso e identificação de identidade para garantir a confidencialidade da informação sensível do usuário e evitar a violação da sua privacidade. Entretanto, como essa informação geralmente é confiada a

um sistema de armazenamento na nuvem, ela se torna vulnerável a um vazamento de dados. Como resultado, os dados armazenados podem ser obtidos através de um ataque ou serem intencionalmente expostos por qualquer entidade que tenha acesso ao sistema. Outra tendência atual que requer os mesmos cuidados com relação aos vazamentos de dados são as operações de análise em *Big Data*. Para inferir informações valiosas relacionadas à saúde dos usuários, um prestador de serviços de saúde pode confiar a informação a terceiros para análise e identificação de características. Nesses casos, todo o processo deve ser protegido de forma a garantir a privacidade do usuário [Onesimu et al. 2022]. As empresas que prestam serviços que estão relacionados com o armazenamento e processamento dos dados devem seguir as regulamentações para garantir que o direito à privacidade seja garantido. No Brasil, é preciso seguir as indicações da LGPD e deixar explícito quais dados serão coletados, a finalidade desses dados e como serão tratados.

2.4.4.5. Autenticação e Autorização

A complexidade do ambiente que apoia os sistemas de vida assistida torna a autenticação uma operação árdua, uma vez que ela deve acontecer considerando diversas redes e dispositivos heterogêneos. A autenticação deve acontecer tanto para as entidades que fazem parte do sistema quanto para a informação que será transmitida. A autenticação da entidade visa garantir que uma parte interessada e autenticada do sistema se conecte a outra parte interessada, se e somente se, a segunda parte também estiver autenticada. Já a autenticação da informação é o processo pelo qual uma entidade é verificada como a origem dos dados gerados. Atualmente, uma das principais tendências para os protocolos de autenticação é a chamada autenticação leve, uma vez que as limitações de memória e processamento dos dispositivos na IoHT torna impraticável a adoção de protocolos mais robustos. A autorização visa assegurar que somente entidades reconhecidas podem acessar um determinado serviço ou recurso, como um dispositivo ou os dados de um usuário.

Todos os dispositivos participantes do sistema devem ter mecanismos de autenticação nativos. Entretanto, devido a baixa capacidade computacional os dispositivos na IoHT não possuem mecanismos de autenticação ou possuem versões simplificadas de mecanismos tradicionais, sendo vulneráveis a uma série de ataques. Outro problema reside na incompatibilidade de mecanismos de autenticação entre os fabricantes. Uma vez que não existe consenso sobre uma forma exclusiva de autenticação, cada fabricante adota uma medida de segurança, tornando complexa a tarefa de adicionar e gerenciar os dispositivos conectados. Adicionalmente, tecnologias de comunicação para redes pessoais como o Bluetooth possuem várias versões vigentes, algumas sem nenhum mecanismo de autenticação para sincronizar um dispositivo. Os principais ataques visando interferir com mecanismos de autenticação e autorização consistem em ataques de falsificação, ataques de clonagem e replicação, ataques de engenharia social e ataques que envolvem a infecção através de códigos maliciosos [Papaioannou et al. 2022].

Nos ataques de falsificação, um invasor tenta utilizar um dispositivo, subsistema ou outra parte autenticada como suporte para construção de uma identidade válida. Depois de acessar o sistema o atacante passa a fraudar o sistema com informações falsas ou ganha acesso a funções privilegiadas. Em ataques de clonagem e replicação, um usuário compromete um dispositivo e cria um número significativo de clones para subverter o sistema. Nota-se que na IoHT esses ataques não são descartados mas são extremamente raros, uma

vez que a quantidade de dispositivos e a exclusividade dos mesmos dificultam sua execução. Um outro tipo de ataque direcionado à quebra da autorização é consideravelmente mais simples e eficiente: ataques de engenharia social. Muitos usuários dos dispositivos da IoHT possuem pouca ou nenhuma afinidade com tecnologia, sendo alvos relativamente fáceis para atacantes. Caso um atacante consiga acessar um dispositivo inteligente, como um relógio ou *smartphone*, ele terá acesso a uma infinidade de aplicações, incluindo as aplicações de saúde. Nesse sentido, existem vários problemas associados como: senhas simplificadas, senhas padrão nos dispositivos e falta de configuração em mecanismos que reforçam a segurança (e.g., autenticação em duas etapas e biometria). Finalmente, os ataques que envolvem a infecção através de códigos maliciosos podem colocar um atacante no controle parcial ou total de um dispositivo da IoHT, posteriormente o atacante pode desativar sensores, serviços e demais funções disponíveis no sistema de vida assistida.

2.5. Arquiteturas e Redes de próxima geração

Novas arquiteturas e redes de próxima geração podem contribuir com o desenvolvimento de aplicações de saúde ao endereçar alguns requisitos de comunicação e segurança. Nesta seção, serão expostos trabalhos relacionados ao uso de redes de próxima geração na área de saúde, explorando benefícios e desafios associados a esses requisitos. Além disso, também será discutido como algumas arquiteturas de Internet do Futuro podem auxiliar no desenvolvimento dessas aplicações.

2.5.1. Redes de próxima geração (e.g., 5G e 6G)

Pesquisas envolvendo 5G na área de saúde têm se tornado popular devido a algumas características da 5G, como baixa latência. A Tabela 2.9 resume as características entre as gerações de redes móveis e, ao comparar as características das redes 4G com 5G, observa-se que a rede 5G apresenta maior taxa de transmissão, latência baixa e suporte a maior quantidade de dispositivos por km^2. Portanto, o potencial de uso da 5G associado aos dispositivos IoT para prover soluções de saúde é alto. As características das redes 6G tornam esse cenário ainda mais promissor, principalmente por causa da sua integração com satélite, que pode facilitar o uso de serviços de saúde avançados em áreas remotas.

Tabela 2.9. Comparação entre as características das redes 4G, 5G e 6G.

Características	Desempenho		
	4G	5G	6G
Taxa de transmissão	1Gbps	20Gbps	1Tbps
Frequênca máxima	6GHz	90GHz	10THz
Latência fim a fim	10ms	1ms	100μs
Mobilidade	350km/h	500km/h	1000km/h
Dispositivos	100k/km^2	1000k/km^2	10^7/km^2
Arquitetura	MIMO	MIMO massivo	Superfície inteligente
Integração com satélite	Não	Não	Sim

Os benefícios das redes 5G podem ser observados em diferentes aplicações de saúde: monitoramento de indivíduos, prevenção de doenças infecciosas, realização de ci-

rurgias remotas, entre outros [Devi et al. 2023]. No caso dos serviços de monitoramento, as aplicações podem beneficiar-se do aumento na taxa e velocidade de transmissão de dados, baixa latência, rede com maior eficiência energética e uso de espectro de frequência mais eficiente. Alguns desses benefícios são explorados no desenvolvimento de uma solução de monitoramento remota em tempo real [Zhang et al. 2020]. A solução usa 5G, IA e computação de borda móvel para endereçar três questões: transmissão de dados contínua, baixa latência e utilização de mecanismos de análise de dados.

Os trabalhos envolvendo 5G e a área de saúde podem ser classificados de acordo com diferentes critérios, como tecnologias de comunicação, requisitos, objetivos, métricas de desempenho e abordagens [Ahad et al. 2019]. A classificação baseada em abordagem é categorizada em controle de congestionamento, agendamento e roteamento. Os trabalhos que buscam lidar com controle de congestionamento, geralmente tem benefícios como redução de perda de pacotes e do atraso fim a fim. Já as estratégias de agendamento são caracterizadas por propiciar otimização de recursos e garantias de QoS. Alguns desses trabalhos fazem uso de redes definidas por software (do inglês, *Software Defined Networking* – SDN) e funções de rede virtualizadas (do inglês, *Network Functions Virtualization* – NFV) para reservar e instanciar recursos. Por fim, os trabalhos associados ao roteamento têm o objetivo de melhorar a comunicação entre os dispositivos. Em muitas situações, as soluções acabam mesclando características de diferentes abordagens. A Tabela 2.10 apresenta um resumo de alguns desses trabalhos.

Tabela 2.10. Soluções de 5G associadas à comunicação e segurança.

Abordagem	Referência	Contribuições
Controle de congestionamento	[Tshiningayamwe et al. 2016]	Sistema de detecção e notificação de congestionamento baseado em limiares que definem três situações: sem congestionamento, congestionamento moderado e congestionamento elevado. No caso de congestionamento moderado, o algoritmo considera o tamanho do *buffer* e nível de energia do nó para tomada de decisões de encaminhamento. Caso haja congestionamento elevado, há a redução da taxa de dados trafegados. Os benefícios da solução são aumento da vazão, redução da perda de pacotes e do atraso fim a fim.
Priorização de tráfego	[Besher et al. 2022]	Estratégia de priorização de tráfego em redes 5G com congestionamento: os pacotes relacionados com a área de saúde são marcados com uma *flag*, que é utilizada pelo comutador SDN para classificá-lo de acordo com sua prioridade e encaminhá-lo através da rede. Os pacotes marcados como prioritários são processados primeiro e têm redução do atraso fim a fim. No entanto, nenhum mecanismo para minimizar o congestionamento é adotado.
Roteamento	[Ahad et al. 2021]	Protocolo de roteamento baseado em *cluster* para reduzir o atraso na transmissão dos dados, melhorar a eficiência energética e estender a vida útil da rede. O algoritmo seleciona o líder do agrupamento com base em critérios como distância entre os nós e a estação base, energia e velocidade dos nós. A partir da eleição do líder, os grupos são estabelecidos e os nós que fazem parte do agrupamento encaminham suas mensagens para o líder, que irá comunicar-se com uma das estações base. Nesse processo, os autores fazem uso de mecanismos de aprendizado por reforço para que os nós e o líder identifiquem a rota mais eficiente energeticamente.

Embora a implementação de 5G ainda esteja em seus estágios iniciais no Brasil e no mundo, a comunidade acadêmica e a indústria já tem realizado pesquisas a respeito da sexta geração de redes móveis. Em [Koren and Prasad 2022], os autores discutem questões de privacidade e segurança relacionados às aplicações de saúde em redes 6G. As principais ameaças sinalizadas pelos autores são uso de computação quântica para quebrar mecanismos criptográficos atuais, dispositivos IoT comprometidos ou não autorizados, roubo de dados de dispositivos IoT, espionagem nos canais de comunicação e bloqueio de sinal. Além desses pontos, os autores ainda ressaltam que as redes 6G podem herdar vulnerabilidades de segurança das redes 5G, como ataques direcionados ao controlador SDN e ataques relacionados à NFV. Na Tabela 2.11, é possível observar algumas das principais ameaças envolvendo as principais tecnologias utilizadas nas redes 5G e 6G.

Tabela 2.11. Ameaças associadas às tecnologias utilizadas nas redes 5G. Adaptado de [Mangla et al. 2022]

Ameaças	Alvo	Tecnologia afetada			
		SDN	NFV	Nuvem	MIMO
Ataque DoS	Elementos de controle centralizados	x	x	x	
Ataque de configuração	Switches e roteadores SDN	x	x		
Ataques hijacking	Controlador SDN e hypervisor	x	x		
Ataques de saturação	Controlador e switches SDN	x			
Eavesdropping	Canais de controle	x			x
Ataques TCP	Comunicação entre controlador e switch SDN	x			
MITM	Comunicação entre controlador e switch SDN	x			
Vazamento de dados	Sistemas de armazenamento em nuvem			x	
Intrusão na nuvem	Sistemas de nuvem			x	

Após identificar as principais ameaças relacionadas às redes 5G e 6G, os autores em [Mangla et al. 2022] destacam soluções baseadas em computação quântica para lidar com ataques DoS e DDoS [Price et al. 2020], MITM, *replay*, *eavesdropping* e roubo de sessão [Srivastava et al. 2020], segurança em SDN e NFV [Aguado et al. 2017] e segurança de redes heterogêneas [Kakkar 2020]. Técnicas de aprendizado de máquina e uso de criptografia homomórfica também são soluções que têm sido exploradas para promover segurança e privacidade em redes 5G e 6G [Koren and Prasad 2022].

2.5.2. Redes Definidas Por Software

O paradigma SDN [McKeown 2009] estabelece uma separação entre o plano de controle e o plano de dados dos dispositivos da rede. O plano de controle é centralizado em um nó, denominado controlador, que tem uma visão global da rede e define as regras de encaminhamento dos fluxos. Essas regras são enviadas aos comutadores de rede, que são responsáveis por encaminhar os pacotes. A centralização da rede possibilita a programabilidade do encaminhamento dos fluxos de forma mais flexível e dinâmica. Tais propriedades são favoráveis ao desenvolvimento de arquiteturas de redes para IoHT, visto que os nós encaminhadores não precisam realizar o processamento dos pacotes localmente. Além disso, a manutenção das regras de encaminhamento é feita no controlador de acordo com condições predefinidas, permitindo que o tráfego possa ser redirecionado automaticamente diante da detecção de gargalos [Cicioğlu and Çalhan 2019], para aplicar técnicas de

priorização de tráfego [Yaseen et al. 2022, Kamboj et al. 2021, Misra et al. 2020], fazer balanceamento de cargas e otimização da rede [Li et al. 2020], promover eficiência energética [Cicioğlu and Çalhan 2020], direcionar o tráfego com base na classe da aplicação [Kamboj et al. 2021], ou até mesmo realizar agregação de dados [Madureira et al. 2020].

Embora o uso de SDN tenha se tornado popular, uma das principais críticas está relacionada com a centralização da operação. No entanto, como em cenários IoHT é comum haver a presença de coordenadores locais, a centralização trazida pelo uso da SDN não adiciona complexidade ou desvantagens à aplicação. Neste sentido, a visão global da rede favorece o gerenciamento de dispositivos, principalmente em cenários de mobilidade ou na presença de falhas em função de esgotamento de recursos computacionais. O controlador SDN pode, portanto, monitorar os dispositivos e aplicar ações de gerenciamento em tempo real a partir das informações obtidas, definindo dinamicamente rotas por onde um fluxo deve passar [Cicioğlu and Çalhan 2019]. Essa definição das rotas pode, inclusive, considerar aspectos como temperatura e nível de bateria dos equipamentos.

Outro aspecto relevante no uso de soluções baseadas em SDN é a possibilidade de distribuir ou compartilhar o processamento e armazenamento de dados coletados por sensores em infraestruturas de névoa e nuvem. Recursos computacionais da névoa estão mais próximos da origem dos dados e mitigam os possíveis atrasos de transmissão, enquanto aumentam a disponibilidade e reduzem a sobrecarga. Nas aplicações IoHT em arquiteturas híbridas, as decisões de encaminhamento dos dados podem ser baseadas de acordo com níveis de prioridade, para implementar estratégias de priorização de tráfego, ou níveis de sensibilidade, para garantir requisitos de confidencialidade e privacidade. Nesses casos, é importante avaliar o *tradeoff* entre os recursos computacionais necessários para analisar os dados da aplicação e os seus requisitos de segurança [Misra et al. 2020]. Neste sentido, algumas propostas na literatura sugerem o gerenciamento de QoS de dados de saúde por meio do uso de SDN e técnicas de aprendizado de máquina [Kumari and Jain 2022, Misra et al. 2020]. Em tais propostas, as camadas de névoa e nuvens são adotadas para apoiar o armazenamento e processamento dos dados de saúde coletados por sensores na borda da rede.

Além do uso da SDN para melhorar a comunicação da rede e alcançar requisitos de QoS das aplicações, existem abordagens que exploram o modelo centralizado e a flexibilidade da programabilidade da SDN para prover serviços customizados ao usuário de sistemas de saúde. Por exemplo, em [Misra et al. 2023], os autores apresentam uma arquitetura de rede em que um controlador é utilizado para definição dinâmica de regras de encaminhamento dos *switches* de modo a apoiar a distribuição de módulos de *analytics* de um sistema de diagnóstico de pacientes à luz do QoS da rede. Assim como abordagens anteriores, a proposta faz um ranqueamento de prioridade dos fluxos. O conceito de programabilidade da rede também pode ser utilizado para desenvolver soluções de segurança. Em [Uddin et al. 2019], os autores desenvolveram um *framework* denominado *PrivacyGuard* que busca preservar a privacidade dos dados das aplicações através da construção de políticas de privacidade programáveis. As principais características desse *framework* é que ele utiliza informações de contexto relacionadas ao usuário, aplicação, dispositivo e rede para definir as políticas de privacidade. Além disso, há a premissa de que as políticas sejam transparentes para a aplicação, sem que haja necessidade de quaisquer mudanças no cliente ou no servidor.

2.5.3. Redes Centradas na Informação

As Redes Centradas na Informação (do inglês, *Information-Centric Networking* – ICN) [Jacobson et al. 2009, Sampaio et al. 2021] é um paradigma de Internet do Futuro que se baseia no fato de que os usuários estão interessados no conteúdo e não necessariamente onde ele está armazenado. Partindo dessa premissa, foi proposto um modelo de rede que desvincula o identificador e o localizador de um conteúdo e que executa funções de rede baseada em nome. As Redes de Dados Nomeados (do inglês, *Named-Data Networking* – NDN) [Zhang et al. 2014] é a arquitetura mais popular do paradigma ICN e suas principais características são: uso de um esquema de nomeação hierárquico e semântico para nomear dados e elementos da rede, *cache* nos dispositivos de rede, segurança a nível de dados e plano de encaminhamento com estado [Sampaio et al. 2021].

O esquema de nomeação semântico e o roteamento baseado em nome, característicos da NDN, possibilitam uma relação direta entre a aplicação e a rede. Essa associação oferece vantagens para adição de semântica ao tráfego, permitindo que nós da rede possam identificar classes dos dados e oferecer serviços diferenciados, tais como manutenção de dados em *caches*, priorização de tráfego ou até mesmo a adoção de estratégias de encaminhamento específicas e cientes de contexto. Esse tipo de funcionalidade pode ser utilizada em cenários de IoHT, para priorizar alertas médicos e o envio dos dados coletados pelos sensores. Além disso, o esquema de nomeação também auxilia outras funcionalidades úteis para aplicações de saúde, como a disponibilidade de serviços de *bootstrapping* e políticas de controle de acesso [Aboodi et al. 2019]. O processo de *bootstrapping* em dispositivos IoT está associado às configurações iniciais de conectividade e segurança dos dispositivos. Neste contexto, a NDN possibilita a divulgação desse serviço na rede e o envio de comandos para configuração dos dispositivos através do nome de pacotes de interesse. Esta mesma funcionalidade pode ser utilizada para enviar comando aos atuadores. Por exemplo, um pacote de interesse na camada de rede pode ter o nome "sala/luz/desligar" para indicar ao atuador localizado na sala que a luz deve ser desligada [Shang et al. 2016].

A NDN também tem sido explorada para endereçar requisitos de segurança na área da saúde [Saxena and Raychoudhury 2017, Boussada et al. 2019, Dulal et al. 2022]. Em [Dulal et al. 2022] os autores apresentam um sistema baseado em NDN, denominado *mGuard*, para desenvolver políticas de controle de acesso cientes de contexto e com alta granularidade. A solução faz uso de criptografia baseada em atributos e da semântica do esquema de nomeação para explorar os benefícios da NDN nesse cenário. Já em [Boussada et al. 2019], os autores demonstram os benefícios do uso do PP-NDNoT, um sistema desenvolvido para garantir requisitos de integridade, autenticação mútua e privacidade orientada ao conteúdo e baseada em contexto para aplicações de saúde em NDN.

As características da NDN, quando incorporadas à IoT, podem impulsionar o desenvolvimento de aplicações em diferentes áreas, como sistemas ciberfísicos, redes veiculares, *smart home*, *smart city* e saúde [Aboodi et al. 2019]. Na Tabela 2.12, há um resumo das características da NDN e uma breve discussão sobre como essas características podem beneficiar (ou não) as aplicações IoHT. Também foram listados desafios associados ao uso da NDN nesses cenários.

Tabela 2.12. Características e desafios da incorporação da NDN na área de saúde.

Características	Desafios
Esquema de nomeação semântico	
O esquema de nomeação é usado para nomear todos os componentes da rede, incluindo usuários, dispositivos e dados. Quando é adicionada semântica ao esquema de nomeação, é possível utilizá-lo para para suportar outros recursos e serviços, como encaminhamento de pacotes, *multicast*, suporte à mobilidade, roteamento, segurança e configuração de dispositivos.	-Quais características do esquema de nomeação podem ser utilizadas para auxiliar no desenvolvimento de serviços para saúde? -Qual o tipo de de esquema de nomeação mais adequado para esses cenários? -Quais são as implicações na privacidade ao fazer uso de nomeação semântica na camada de rede?
***Cache* nos dispositivos de rede**	
A NDN implementa *cache* oportunístico na rede para armazenar cópias dos dados. Em aplicações de saúde, o *cache* pode ser benéfico para garantir a entrega de conteúdo em caso de problemas na rede. Apesar disso, é preciso avaliar se o *cache* teria uma boa taxa de acerto, já que o envio de dados coletados pelos sensores é constante e irá gerar mudanças frequentes na *cache*.	-Quão benéfico é o uso de *cache* em sistemas de vida assistida? -Que tipo de políticas de *cache* seriam adequadas para aplicações de saúde? -Como o uso de *cache* poderia auxiliar no suporte à mobilidade nesses cenários?
Estratégias de encaminhamento e Diferenciação de tráfego	
É possível utilizar diferentes estratégias de encaminhamento com base no prefixo do nome do conteúdo ou mesmo, essas estratégias podem adaptar-se ao contexto, a depender das regras definidas. Essa característica, associada à semântica do esquema de nomeação, pode ser utilizada para proporcionar serviços de priorização de tráfego em aplicações de saúde.	-Quais requisitos devem ser levados em consideração na definição das estratégias de encaminhamento? –Como estratégias de encaminhamento podem melhorar o QoS em sistemas de vida assistida? -Como considerar as métricas da rede e a semântica da aplicação nas definições de encaminhamento e roteamento?
Configuração e Gerenciamento de dispositivos	
O esquema de nomeação semântico pode ser usado para registro de serviços, descoberta de vizinhos e configuração de dispositivos. Esses processos tem relação direta com requisitos de interoperabilidade, auto-configuração e escalabilidade em aplicações de saúde.	-Quais tipos de serviços devem ser divulgados na rede? -Que tipo de padrões devem ser incluídos no esquema de nomeação para dar suporte aos serviços de configuração e gerenciamento de dispositivos?
Segurança e Políticas de Controle de Acesso	
Os requisitos de integridade e autenticidade são alcançados na NDN através da assinatura de pacotes pelo produtor, mas a arquitetura não oferece suporte nativo à confidencialidade, sendo necessário o uso de soluções adicionais [Zhang et al. 2018]. A semântica do esquema de nomeação pode ser utilizada na definição de políticas de controle de acesso granulares e cientes de contexto. Neste sentido, serviços facilitados na NDN, como auto-configuração dos dispositivos, podem auxiliar no processo de *bootstrapping* das funções de segurança.	-Como a arquitetura NDN pode fornecer serviços de segurança e tolerância a falhas no nível de rede? -Quais são os principais ataques de rede que devem ser evitados em tais cenários? -Quais características dos dispositivos, comunicação, serviços e aplicativos devem ser consideradas ao endereçar os requisitos de segurança e as políticas de controle de acesso? -Como fornecer segurança a nível de dados considerando a limitação de recursos dos dispositivos?

2.6. Estudos de caso

Esta seção apresenta dois estudos de caso relacionados, respectivamente, à conectividade e segurança em aplicações IoHT. O primeiro estudo de caso trata do monitoramento de problemas cardíacos em idosos localizados em áreas remotas. O segundo estudo de caso descreve um mecanismo de autenticação que emprega biossinais para garantir segurança na transmissão de dados.

2.6.1. Monitoramento de idosos em áreas remotas

O estado do Amazonas, na região Norte do Brasil apresenta as piores qualidades de enlace[4]. Esse problema é ocasionado por fatores como dificuldade de acesso geográfico e falta de investimentos em infraestrutura. As consequências desses fatores não se limitam às redes de computadores e são observadas em áreas como educação e saúde. Com o intuito de oferecer melhores condições de saúde para a população, a Fundação Amazônia Sustentável[5] (FAS) desenvolveu um programa denominado Saúde na Floresta, cujo objetivo é promover o atendimento de atenção básica de saúde e auxiliar na formação de profissionais da área. Esse programa engloba ações de telessaúde, políticas públicas, educação e pesquisa em saúde. O uso da telessaúde traz grandes benefícios pois possibilita a oferta de serviços de saúde em áreas remotas. No entanto, outras aplicações também podem ser utilizadas para ampliar os serviços de saúde nessas regiões e melhorar as condições de vida dos indivíduos.

As doenças do aparelho circulatório é a maior causa de mortes e hospitalizações de idosos no Brasil [Heemann and Hermsdorf 2017] e, na região Norte, o percentual de óbitos em pessoas idosas com essa causa se aproximou de 25% em 2020. O diagnóstico e o acompanhamento dessas doenças ocorrem através do mapeamento de sintomas físicos (e.g., dor no peito, pernas inchadas e desmaios), do monitoramento de parâmetros de saúde do indivíduo (e.g., pressão arterial, saturação de oxigênio e frequência cardíaca) e através de eletrocardiogramas. Aplicativos, sensores e equipamentos vestíveis coletam esses dados. Como citado anteriormente, os sensores e equipamentos vestíveis têm poucos recursos computacionais e, geralmente, encaminham os dados coletados para o *gateway*. A comunicação física entre os sensores e o *gateway* segue protocolos de comunicação de curto alcance suportados pelos dispositivos. Além da comunicação local, essas aplicações necessitam da conectividade entre o *gateway* e a nuvem, onde serão realizados os processos de armazenamento permanente e análise dos dados. No entanto, a necessidade de comunicação com a nuvem pode impossibilitar o uso dessas aplicações em áreas remotas. Nessas regiões, o acesso à Internet comumente acontece através de comunicações a rádio ou via satélite. Enquanto a comunicação a rádio é mais suscetível a interferências de sinal e apresenta maior incidência de perda de pacotes, a comunicação via satélite tradicional resulta em alta latência. Essas duas características inviabilizam o uso de aplicações de monitoramento de doenças cardíacas, pois essas aplicações são sensíveis a perdas e precisam de baixa latência.

Neste estudo de caso, propusemos a adoção de redes de satélites de baixa órbita (do inglês, *Low Earth Orbit*) para possibilitar o uso de aplicações de monitoramento de

[4]Dados disponibilizados pelo NIC.br: `https://qualidadedainternet.nic.br/`

[5]`https://fas-amazonia.org`

condições cardíacas em áreas remotas, garantindo requisitos de alta capacidade e baixa latência para realização de monitoramento contínuo e em tempo real. Comparado com as redes de satélite tradicionais, a LEO apresenta características como baixo atraso de propagação, pequena perda de propagação e cobertura global. Além disso, há a expectativa de que o uso de constelações de satélite ofereçam latências inferiores às conexões via fibra óptica para distâncias superiores a 3000km [Handley 2018].

A Figura 2.6 ilustra o cenário proposto e dos seus elementos. Os sensores são responsáveis por coletar os dados e enviar para o *gateway* local, que irá se comunicar com o terminal de satélite do usuário. Após receber os dados do *gateway*, o terminal transmite o tráfego para o satélite mais próximo. A maioria desses terminais têm características favoráveis a sua adoção, como tamanho pequeno, tempo de vida útil longo e baixo consumo energético. Além disso, como os satélites estão em movimento, a comunicação entre o terminal e o satélite acontece mesmo quando há obstáculos próximos ao terminal [Qu et al. 2017]. Depois de receber o tráfego, os satélites comunicam-se através de *lasers* e encaminham os dados até chegar no terminal de destino. Assim, o usuário consegue acessar a Internet e a infraestrutura de nuvem pela aplicação. Na infraestrutura de nuvem é possível definir políticas de controle de acesso que permitam aos profissionais de saúde visualizarem os dados e avaliarem as condições de saúde do indivíduo. A partir dessa análise, os profissionais estão aptos a encaminhar tipo de *feedback* ao usuário, como solicitação de ajuste medicamentoso e encaminhamento do indivíduo para profissionais de saúde locais. Essas ações podem reduzir situações de emergência e mortes.

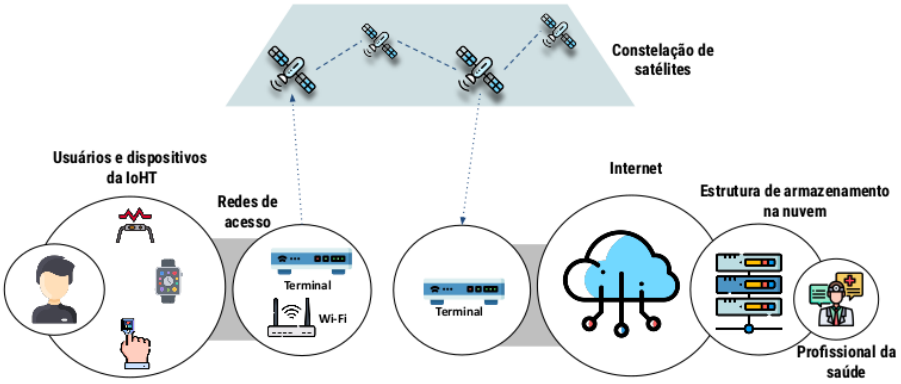

Figura 2.6. Utilização de LEO para possibilitar uso de aplicações IoHT em áreas remotas.

Alguns benefícios obtidos através da junção entre LEO e IoT são as características de QoS e velocidade da rede e a facilidade de uso dessa estrutura em ambientes remotos. Embora as redes LEO ainda estejam em processo de implementação, já existem trabalhos que relacionam o uso dessas redes para facilitar a comunicação em cenários IoT [Qu et al. 2017]. Alguns desafios de pesquisa que envolvem essa adoção incluem a adequação de protocolos IoT terrestres para comunicação via satélite.

2.6.2. Uso de biossinais na autenticação de usuários

A autenticação de usuários e dispositivos é um mecanismo fundamental para garantia de requisitos de segurança em sistemas de vida assistida. O processo de autenticação segue três abordagens: algo que se sabe (e.g., senha), algo que se tem (e.g.,

smartphone ou chave USB) e algo que se é (e.g., biometria). Como um dos principais públicos alvo dos sistemas de vida assistida são as pessoas idosas, a dependência de senhas e dispositivos físicos pode gerar aversão ao uso sistema devido ao esquecimento das senhas ou à dificuldade em interagir com o dispositivo de entrada. Paralelo a isso, alguns dispositivos na IoHT têm baixo poder de processamento e armazenamento, dificultando a implementação de mecanismos de autenticação de alta complexidade computacional. Assim, os sinais biométricos que capturam características de um indivíduo através de interfaces homem-máquina são candidatos promissores para promover a autenticação de um usuário. A impressão digital é o método mais comum de identificação biométrica, entretanto, pessoas idosas podem apresentar perda ou mudança da impressão digital e muitos dispositivos mais simples na IoHT, como monitores de atividade física e *smartwatches*, não possuem um leitor de impressão digital.

Neste estudo de caso, analisamos a adoção da variação da frequência cardíaca, medida através dos sensores pletismográficos encontrados nos dispositivos da IoHT, no processo de identificação e autenticação do usuário. A teoria empregada é que, assim como no caso das impressões digitais, cada ser humano tem uma variação de frequência cardíaca única e exclusiva, que pode ser utilizada em processos de autenticação. Embora essa alternativa possa resolver a autenticação de usuários, ainda há ameaças que podem afetar o processo de autenticação. Na Seção 2.4, foram expostas as principais ameaças considerando a autenticação e autorização dos dispositivos e um dos principais problemas está relacionado à transmissão das informações através de tecnologia de comunicação sem fio. Nesses casos, um atacante pode escutar o canal de transmissão e obter informações, incluindo senhas e dados biométricos empregados no processo de autenticação. Sendo assim, o processo de autenticação também deve considerar a segurança do canal de comunicação. A tecnologia de acoplamento galvânico permite que uma quantidade de dados seja transmitida utilizando o tecido corporal (pele) como meio de transmissão. Esse processo de autenticação é ilustrado na Figura 2.7 e segue as fases de (i) aquisição de dados e pré-processamento; (ii) comunicação galvânica e (3) processo de autenticação.

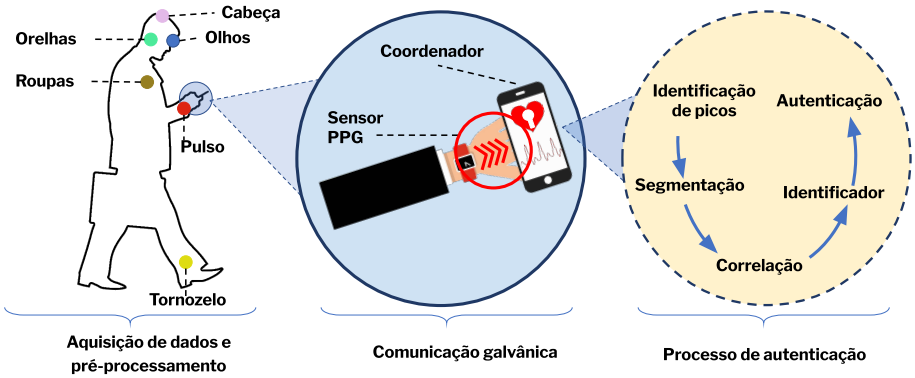

Figura 2.7. Mecanismo de autenticação através de sinal biométrico e transmissão segura de informações.

Na fase de aquisição de dados e pré-processamento os dispositivos com capacidade de coletar os biossinais do fotopletismograma (do inglês, *photoplethysmogram* – PPG), através dos sensores pletismográficos, coletam o sinal que será utilizado para inferência da variação da frequência cardíaca. Esses sensores podem estar posicionados

em diversos pontos do corpo humano de acordo com a necessidade e de modo a oferecer maior conforto para o usuário. Antes de ser enviado ao dispositivo coordenador para autenticação os dados coletados passam por uma etapa de pré-processamento básico para otimização do mecanismo. Uma vez que os dispositivos estão em contato com a pele do usuário, o envio dos dados até o coordenador ocorre através da tecnologia de acoplamento galvânico (fase de comunicação galvânica), utilizando a pele e tecidos como meio de transmissão. O acoplamento galvânico dificulta a interceptação da transmissão dos dados. De posse dos dados PPG, o coordenador executa o pós-processamento dos dados e identifica uma série de características do sinal (subfases no processo de autenticação). Finalmente, o coordenador autoriza o usuário a utilizar as funções do sistema, ou nega o acesso e encerra o processo de autenticação.

Essa alternativa de autenticação foi desenvolvida e avaliada no contexto do projeto *NSF/RNP US-Brazil Healthsense*[6], cujos dois objetivos principais são: *i)* analisar e explorar as características dos dispositivos vestíveis, aplicações e protocolos de rede, e *ii)* propor técnicas para resiliência através do uso do corpo para transmitir informações de forma segura. O detalhamento do mecanismo de autenticação utilizado como base neste estudo de caso e o repositório contendo informações relevantes e arquivos de coletas de sinais PPG estão publicamente disponíveis através dos trabalhos desenvolvidos no escopo do projeto [Nakayama et al. 2019a, Nakayama et al. 2019b].

2.7. Ambientes de Experimentação e *Datasets*

Nesta seção serão apresentadas ferramentas e *datasets* para experimentação relacionada à comunicação e segurança na área de saúde. É desafiador conseguir executar experimentos envolvendo os vários componentes de um sistema de vida assistida, que variam desde sensores em uma WBAN a recursos na nuvem. Geralmente o processo de experimentação é realizado através da segmentação da arquitetura para avaliar diferentes partes da rede, como a WBAN ou WSN, as redes de acesso e a comunicação com a nuvem. Simuladores de redes tradicionais, como o NS-2, NS-3 e o OMNeT++ podem ser utilizados para realizar experimentos envolvendo essas aplicações. No entanto, existem ferramentas que foram desenvolvidas especificamente para a experimentação de aplicações em IoT, incluindo cenários de saúde. Assim, é possível citar:

- **IoTFY**[7]: plataforma que facilita a prototipação, dimensionamento e gerenciamento de aplicações IoT na nuvem, em grande escala e de forma realista. A plataforma inclui particularidades da IoT, como o uso de comunicações M2M e a caracterização do tráfego dos dispositivos. Na comunicação M2M, o simulador suporta protocolos como MQTT, CoAP e HTTP. Além disso, implementa soluções de comunicação que consideram os princípios associados aos protocolos de comunicação sem fio de curta e longa distância e suas características em relação às métricas de rede, como latência. Esse simulador tem uma versão básica que é gratuita, mas para utilizar todas as funcionalidades desenvolvidas, é necessário utilizar a versão paga.
- **IotNetSim**: permite a execução de simulação em três níveis: camada IoT, borda e

[6] https://www.healthsenseproject.net/
[7] https://docs.iotify.io/

nuvem. A camada IoT é onde estão os sensores que geram dados para enviar para o *gateway*. O *gateway* processa os dados e os envia para a camada de borda, que trata os dados e encaminha para a nuvem [Salama et al. 2019].

- **MoSIoT**: permite a simulação de aplicações de monitoramento da saúde do indivíduo baseado no paradigma de engenharia orientada a modelos. Os autores validam a ferramenta utilizando uma aplicação associada à doença de Alzheimer e os códigos do simulador são disponibilizado em [Meliá et al. 2021].

Experimentos que envolvem o uso de arquiteturas e modelos de Internet do Futuro podem incluir simuladores e emuladores como o NDNSim[8], Mininet[9] e o MiniNDN[10]. No caso do uso de emuladores, é comum a integração com o módulo de rede sem fio do NS-3 para conseguir mapear as características do ambiente sem fio na emulação. Nos últimos anos, também foram apresentadas algumas soluções no salão de ferramentas do SBRC que podem ser utilizadas na criação de *testbeds*, experimentação e adoção de mecanismos de gerenciamento e segurança. Dentre as ferramentas, tem-se o OTALab [Cussuol et al. 2022], IoTFogSim [Pereira et al. 2021], IMAIoT [Heideker et al. 2019] e o SentryIoTOAuth [Andrade and Monteiro 2019].

O mapeamento das características do tráfego em aplicações de saúde varia muito a depender da aplicação. Algumas aplicações são caracterizadas por envio de tráfego contínuo, enquanto outras podem ter uma frequência e taxa de chegada de pacotes diferente. Além disso, é possível ter esses comportamentos variados em diferentes sensores que envolvem uma aplicação. Conseguir mapear essas características na simulação é um processo desafiador. Como alternativas, é possível criar *testbeds* utilizando dispositivos como Arduínos e Raspberry Pi para verificar as características do processo de geração e transmissão de dados ou utilizar *datasets* como insumo nas simulações. Alguns *datasets* relacionados à área de saúde são citados a seguir:

- **ECU-IoHT**[11]: *dataset* construído em um ambiente IoHT para possibilitar experimentos envolvendo segurança cibernética. Os dados incluem diferentes ataques e exploram várias vulnerabilidades.

- ***mHealth dataset***[12]: dados de movimento corporal e sinais vitais coletados por dez voluntários durante a realização de atividades físicas. Os dados incluem informações como monitoramento cardíaco.

- ***Healthsense dataset***[13]: dados de sinais PPG que podem ser utilizados para pesquisas envolvendo o processo de autenticação por meio de biossinais, conforme abordado no segundo estudo de caso [Nakayama et al. 2019b].

[8] https://ndnsim.net
[9] http://mininet.org/
[10] https://github.com/named-data/mini-ndn
[11] https://ro.ecu.edu.au/datasets/48/
[12] http://archive.ics.uci.edu/ml/datasets/mhealth+dataset
[13] https://github.com/Healthsense-Project

As métricas utilizadas na condução da avaliação dependem do tipo de solução proposta, mas é importante sempre avaliar o consumo energético atribuído ao custo da solução. Além disso, os parâmetros da rede, dos dispositivos e do tráfego podem variar dependendo do tipo de aplicação e é interessante emular ou simular essa heterogeneidade de dispositivos e recursos nas avaliações.

2.8. Considerações finais

O desenvolvimento de aplicações de vida assistida envolve a utilização de várias tecnologias que trazem consigo novas contribuições, possibilidades de aplicação, casos de uso e desafios de pesquisa. Nos últimos anos, tem-se observado a evolução da área de IoHT ao desenvolver soluções que não se limitem fisicamente a um lugar (e.g., a casa da pessoa) e que garantam o uso contínuo de serviços de vida assistida, independente de onde o indivíduo esteja. Essas aplicações são vistas como uma possível solução para lidar com o aumento dos custos na área de saúde e com o envelhecimento da população mundial. O desenvolvimento dessas soluções depende de diversas tecnologias, como IoT, computação em nuvem e Inteligência Artificial. Essas tecnologias são utilizadas como componentes em uma arquitetura que visa coletar dados, transmiti-los e processá-los de forma segura. Para que essas soluções sejam amplamente adotadas, é preciso atender aos requisitos das aplicações e dos usuários, que têm relação direta com os mecanismos de comunicação e segurança da rede e dos dispositivos.

Neste minicurso, foram apresentados os principais conceitos associados às aplicações de vida assistida, a partir da perspectiva da conectividade e da segurança. Assim, foi possível observar como os requisitos dos usuários e das aplicações têm impulsionado o desenvolvimento de dispositivos, protocolos de comunicação específicos para a IoT e alternativas mais seguras de armazenamento e processamento de dados. Os requisitos de conectividade e segurança em sistemas de vida assistida são transversais e precisam considerar a heterogeneidade dos dispositivos, tráfego e aplicações. De uma forma geral, observa-se que os requisitos associados à conectividade, QoS, integridade e disponibilidade têm uma relação direta com a confiabilidade do sistema pelos usuários. É preciso garantir que o sistema funcione de forma precisa e confiável em relação aos dados coletados pelos sensores e trafegados na rede. Também, a confiabilidade torna-se maior com a garantia de que o sistema trata questões de confidencialidade e privacidade dos usuários.

Cenários de aplicação associados à saúde de idosos impõem desafios relacionados a diferentes áreas. Embora seja desafiador experimentar soluções que considerem amplamente as características de cenários reais, é importante que os protocolos e soluções desenvolvidos sejam interoperáveis, pois o desenvolvimento de soluções compatíveis entre si impulsiona a criação de aplicações reais. Além disso, os protocolos precisam levar em conta as restrições de capacidade dos dispositivos para que seu uso seja realista. Existem soluções para esses cenários que se baseiam no uso de redes de próxima geração e arquiteturas de Internet do Futuro para alcançar requisitos de rede e segurança. Ao longo dos próximos anos, observaremos o crescimento de aplicações que necessitam da integração de dados e dispositivos para conseguir prover soluções inteligentes. Assim, o avanço de novos algoritmos e protocolos específicos para os sistemas voltados aos cuidados da saúde serão observados nas áreas de redes de computadores, sistemas distribuídos, segurança de redes e de informação, computação em nuvem e Inteligência Artificial.

Agradecimentos

Este trabalho foi realizado com o apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq – 432064/2018-4, 316208/2021-3, 402854/2022-5, 200404/2022-9, 313844/2020-8, 426701/2018-6), da Fundação de Aparo à Pesquisa do Estado da Bahia (FAPESB – TIC0004/2015), da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP – #2021/06733-6) e da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

Referências

[Aazam et al. 2020] Aazam, M., Zeadally, S., and Harras, K. A. (2020). Health fog for smart healthcare. *IEEE Consumer Electronics Magazine*, 9(2):96–102.

[Aboodi et al. 2019] Aboodi, A., Wan, T.-C., and Sodhy, G.-C. (2019). Survey on the incorporation of ndn/ccn in iot. *IEEE Access*, 7:71827–71858.

[Adil et al. 2022] Adil, M., Alshahrani, H., Rajab, A., Shaikh, A., Song, H., and Farouk, A. (2022). Qos review: smart sensing in wake of covid-19, current trends and specifications with future research directions. *IEEE Sensors Journal*.

[Aguado et al. 2017] Aguado, A., Lopez, V., Martinez-Mateo, J., Szyrkowiec, T., Autenrieth, A., Peev, M., Lopez, D., and Martin, V. (2017). Hybrid conventional and quantum security for software defined and virtualized networks. *Journal of Optical Communications and Networking*, 9(10):819–825.

[Ahad et al. 2021] Ahad, A., Tahir, M., Sheikh, M. A., Ahmed, K. I., and Mughees, A. (2021). An intelligent clustering-based routing protocol (crp-gr) for 5g-based smart healthcare using game theory and reinforcement learning. *Applied Sciences*, 11(21):9993.

[Ahad et al. 2019] Ahad, A., Tahir, M., and Yau, K.-L. A. (2019). 5g-based smart healthcare network: architecture, taxonomy, challenges and future research directions. *IEEE access*, 7:100747–100762.

[Alhaj et al. 2022] Alhaj, T. A., Abdulla, S. M., Iderss, M. A. E., Ali, A. A. A., Elhaj, F. A., Remli, M. A., and Gabralla, L. A. (2022). A survey: To govern, protect, and detect security principles on internet of medical things (iomt). *IEEE Access*, 10:124777–124791.

[Amiribesheli et al. 2015] Amiribesheli, M., Benmansour, A., and Bouchachia, A. (2015). A review of smart homes in healthcare. *Journal of Ambient Intelligence and Humanized Computing*, 6:495–517.

[Andrade and Monteiro 2019] Andrade, R. B. d. S. and Monteiro, J. A. S. (2019). Sentryiotoauth: um provedor de serviço de autenticação e autorização para casas inteligentes baseado no processo ace-oauth. In *Anais Estendidos do XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 73–80. SBC.

[Arcelus et al. 2007] Arcelus, A., Jones, M. H., Goubran, R., and Knoefel, F. (2007). Integration of smart home technologies in a health monitoring system for the elderly. In

21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), volume 2, pages 820–825. IEEE.

[Attrapadung and Imai 2009] Attrapadung, N. and Imai, H. (2009). Attribute-based encryption supporting direct/indirect revocation modes. In *Cryptography and Coding: 12th IMA International Conference, Cryptography and Coding 2009, Cirencester, UK, December 15-17, 2009. Proceedings 12*, pages 278–300. Springer.

[Bansal and Kumar 2020] Bansal, S. and Kumar, D. (2020). Iot ecosystem: A survey on devices, gateways, operating systems, middleware and communication. *International Journal of Wireless Information Networks*, 27:340–364.

[Bardalai et al. 2022] Bardalai, P., Neog, H., Dutta, P. E., Medhi, N., and Deka, S. K. (2022). Throughput prediction in smart healthcare network using machine learning approaches. In *2022 IEEE 19th India Council International Conference (INDICON)*, pages 1–6. IEEE.

[Besher et al. 2022] Besher, K. M., OKidhain, I., Wick, L., and Ali, M. Z. (2022). Congestion control of healthcare packet routing in 5g edge computing networks. In *2022 International Conference on Engineering and Emerging Technologies (ICEET)*, pages 1–6. IEEE.

[Boneh and Franklin 2001] Boneh, D. and Franklin, M. (2001). Identity-based encryption from the weil pairing. In *Advances in Cryptology—CRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19–23, 2001 Proceedings*, pages 213–229. Springer.

[Boussada et al. 2019] Boussada, R., Hamdane, B., Elhdhili, M. E., and Saidane, L. A. (2019). Pp-ndnot: On preserving privacy in iot-based e-health systems over ndn. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE.

[Brezolin et al. 2022] Brezolin, U. Q., Prates Jr, N. G., Vergütz, A., and Nogueira, M. (2022). Um método para detecçao de vulnerabilidades através da análise do tráfego de rede iot. In *Anais do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 447–460. SBC.

[Bui and Fonarow 2012] Bui, A. L. and Fonarow, G. C. (2012). Home monitoring for heart failure management. *Journal of the American College of Cardiology*, 59(2):97–104.

[Cicioğlu and Çalhan 2019] Cicioğlu, M. and Çalhan, A. (2019). Sdn-based wireless body area network routing algorithm for healthcare architecture. *ETRI Journal*, 41(4):452–464.

[Cicioğlu and Çalhan 2020] Cicioğlu, M. and Çalhan, A. (2020). Energy-efficient and sdn-enabled routing algorithm for wireless body area networks. *Computer Communications*, 160:228–239.

[Cornet et al. 2022] Cornet, B., Fang, H., Ngo, H., Boyer, E. W., and Wang, H. (2022). An overview of wireless body area networks for mobile health applications. *IEEE Network*, 36(1):76–82.

[Cussuol et al. 2022] Cussuol, E. B., Sachetti, L. L., Santos, B. P., and Mota, V. F. (2022). Otalab: um ambiente de experimentação remota de protocolos e aplicações em internet das coisas. In *Anais Estendidos do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 73–80. SBC.

[Dang et al. 2019] Dang, L. M., Piran, M. J., Han, D., Min, K., and Moon, H. (2019). A survey on internet of things and cloud computing for healthcare. *Electronics*, 8(7):768.

[Demiris et al. 2004] Demiris, G., Rantz, M. J., Aud, M. A., Marek, K. D., Tyrer, H. W., Skubic, M., and Hussam, A. A. (2004). Older adults' attitudes towards and perceptions of 'smart home'technologies: a pilot study. *Medical informatics and the Internet in medicine*, 29(2):87–94.

[Devi et al. 2023] Devi, D. H., Duraisamy, K., Armghan, A., Alsharari, M., Aliqab, K., Sorathiya, V., Das, S., and Rashid, N. (2023). 5g technology in healthcare and wearable devices: A review. *Sensors*, 23(5):2519.

[Du et al. 2020] Du, Z., Wu, C., Yoshinaga, T., Yau, K.-L. A., Ji, Y., and Li, J. (2020). Federated learning for vehicular internet of things: Recent advances and open issues. *IEEE Open Journal of the Computer Society*, 1:45–61.

[Dulal et al. 2022] Dulal, S., Ali, N., Thieme, A. R., Yu, T., Liu, S., Regmi, S., Zhang, L., and Wang, L. (2022). Building a secure mhealth data sharing infrastructure over ndn. In *Proceedings of the 9th ACM Conference on Information-Centric Networking*, pages 114–124.

[Fan et al. 2017] Fan, X., Susan, F., Long, W., and Li, S. (2017). Security analysis of zigbee. *MWR InfoSecurity*, 2017:1–18.

[Fersi 2020] Fersi, G. (2020). Study of middleware for internet of healthcare things and their applications. In *The Impact of Digital Technologies on Public Health in Developed and Developing Countries: 18th International Conference, ICOST 2020, Hammamet, Tunisia, June 24–26, 2020, Proceedings 18*, pages 223–231. Springer.

[Ghayyur et al. 2020] Ghayyur, S., Pappachan, P., Wang, G., Mehrotra, S., and Venkatasubramanian, N. (2020). Designing privacy preserving data sharing middleware for internet of things. In *Proceedings of the Third Workshop on Data: Acquisition To Analysis*, pages 1–6.

[Handley 2018] Handley, M. (2018). Delay is not an option: Low latency routing in space. In *Proceedings of the 17th ACM Workshop on Hot Topics in Networks*, pages 85–91.

[Hasan et al. 2022] Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A., Abdel-Khalek, S., and Alkhassawneh, H. M. (2022). A review on security threats, vulnerabilities, and counter measures of 5g enabled internet-of-medical-things. *IET Communications*, 16(5):421–432.

[Heart and Kalderon 2013] Heart, T. and Kalderon, E. (2013). Older adults: are they ready to adopt health-related ict? *International journal of medical informatics*, 82(11):e209–e231.

[Heemann and Hermsdorf 2017] Heemann, M. and Hermsdorf, M. (2017). Custo de internações de idosos é 30% maior para o sus. Disponível em `https://infograficos.estadao.com.br/focas/planeje-sua-vida/custo-de-internacoes-de-idosos-e-30-maior-para-o-sus`. Acessado: 2023-03-12.

[Heideker et al. 2019] Heideker, A., Ottolini, D., Zyrianoff, I., Kleinschmidt, J., and Kamienski, C. (2019). Imaiot-infrastructure monitoring agent for iot: Um agente monitor de infraestruturas para ambientes de iot. In *Anais Estendidos do XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 9–16. SBC.

[IBGE 2018] IBGE (2018). Projeção da população 2018: número de habitantes do país deve parar de crescer em 2047. Disponível em `https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/21837-projecao-da-populacao-2018-numero-de-habitantes-do-pais-deve-parar-de-crescer-em-2047`. Acessado: 2023-03-12.

[Istepanian and Lacal 2003] Istepanian, R. S. and Lacal, J. C. (2003). Emerging mobile communication technologies for health: some imperative notes on m-health. In *Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE Cat. No. 03CH37439)*, volume 2, pages 1414–1416. IEEE.

[Jacobson et al. 2009] Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., and Braynard, R. L. (2009). Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, pages 1–12. ACM.

[Jones et al. 2010] Jones, V., Gay, V., and Leijdekkers, P. (2010). Body sensor networks for mobile health monitoring: Experience in europe and australia. In *2010 Fourth International Conference on Digital Society*, pages 204–209. IEEE.

[Kakkar 2020] Kakkar, A. (2020). A survey on secure communication techniques for 5g wireless heterogeneous networks. *Information Fusion*, 62:89–109.

[Kamboj et al. 2021] Kamboj, P., Pal, S., and Mehra, A. (2021). A qos-aware routing based on bandwidth management in software-defined iot network. In *2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, pages 579–584.

[Kim et al. 2014] Kim, H.-S., Lee, K.-H., Kim, H., and Kim, J. H. (2014). Using mobile phones in healthcare management for the elderly. *Maturitas*, 79(4):381–388.

[Kitsiou et al. 2017] Kitsiou, S., Paré, G., Jaana, M., and Gerber, B. (2017). Effectiveness of mhealth interventions for patients with diabetes: an overview of systematic reviews. *PloS one*, 12(3):e0173160.

[Konečnỳ et al. 2016] Konečnỳ, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., and Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492*.

[Koren and Prasad 2022] Koren, A. and Prasad, R. (2022). Iot health data in electronic health records (ehr): Security and privacy issues in era of 6g. *Journal of ICT Standardization*, pages 63–84.

[Kumar et al. 2018] Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E., and Ylianttila, M. (2018). Blockchain utilization in healthcare: Key requirements and challenges. In *2018 IEEE 20th International conference on e-health networking, applications and services (Healthcom)*, pages 1–7. IEEE.

[Kumari and Jain 2022] Kumari, N. and Jain, V. K. (2022). Fog based healthcare monitoring system in sdn-iot networks. In *2022 Second International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE)*, pages 1–6.

[Li et al. 2020] Li, J., Cai, J., Khan, F., Rehman, A. U., Balasubramaniam, V., Sun, J., and Venu, P. (2020). A secured framework for sdn-based edge computing in iot-enabled healthcare system. *IEEE Access*, 8:135479–135490.

[Li et al. 2013] Li, J., Li, J., Chen, X., Jia, C., and Lou, W. (2013). Identity-based encryption with outsourced revocation in cloud computing. *IEEE Transactions on computers*, 64(2):425–437.

[Lin et al. 2020] Lin, Y., Jiang, D., Yus, R., Bouloukakis, G., Chio, A., Mehrotra, S., and Venkatasubramanian, N. (2020). Locater: cleaning wifi connectivity datasets for semantic localization. *arXiv preprint arXiv:2004.09676*.

[Madureira et al. 2020] Madureira, A. L. R., Araújo, F. R. C., and Sampaio, L. N. (2020). On supporting iot data aggregation through programmable data planes. *Computer Networks*, 177:107330.

[Madureira et al. 2019] Madureira, P., Cardoso, N., Sousa, F., and Moreira, W. (2019). My-aha: middleware platform to sustain active and healthy ageing. In *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 21–26. IEEE.

[Mangla et al. 2022] Mangla, C., Rani, S., Qureshi, N. M. F., and Singh, A. (2022). Mitigating 5g security challenges for next-gen industry using quantum computing. *Journal of King Saud University-Computer and Information Sciences*.

[Maskeliūnas et al. 2019] Maskeliūnas, R., Damaševičius, R., and Segal, S. (2019). A review of internet of things technologies for ambient assisted living environments. *Future Internet*, 11(12):259.

[McKeown 2009] McKeown, N. (2009). Software-defined networking. *INFOCOM keynote talk*, 17(2):30–32.

[Mehrotra et al. 2020] Mehrotra, S., Sharma, S., Ullman, J. D., Ghosh, D., Gupta, P., and Mishra, A. (2020). Panda: Partitioned data security on outsourced sensitive and non-sensitive data. *ACM Transactions on Management Information Systems (TMIS)*, 11(4):1–41.

[Meliá et al. 2021] Meliá, S., Nasabeh, S., Luján-Mora, S., and Cachero, C. (2021). Mosiot: modeling and simulating iot healthcare-monitoring systems for people with disabilities. *International Journal of Environmental Research and Public Health*, 18(12):6357.

[Misra et al. 2023] Misra, S., Pal, S., Ahmed, N., and Mukherjee, A. (2023). Sdn-controlled resource-tailored analytics for healthcare iot system. *IEEE Systems Journal*, pages 1–8.

[Misra et al. 2020] Misra, S., Saha, R., and Ahmed, N. (2020). Health-flow: Criticality-aware flow control for sdn-based healthcare iot. In *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pages 1–6.

[Mukherjee et al. 2018] Mukherjee, B., Wang, S., Lu, W., Neupane, R. L., Dunn, D., Ren, Y., Su, Q., and Calyam, P. (2018). Flexible iot security middleware for end-to-end cloud–fog communication. *Future Generation Computer Systems*, 87:688–703.

[Nakayama et al. 2019a] Nakayama, F., Lenz, P., Banou, S., Nogueira, M., Santos, A., and Chowdhury, K. R. (2019a). A continuous user authentication system based on galvanic coupling communication for s-health. *Wireless Communications and Mobile Computing*, 2019:1–11.

[Nakayama et al. 2019b] Nakayama, F., Lenz, P., Cremonezi, B., Banou, S., Rosário, D., Chowdhoury, K., Nogueira, M., Cerqueira, E., and Santos, A. (2019b). Autenticação contínua e segura baseada em sinais ppg e comunicação galvânica. In *Anais do XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 707–720. SBC.

[Nakayama et al. 2022] Nakayama, F., Lenz, P., and Nogueira, M. (2022). A resilience management architecture for communication on portable assisted living. *IEEE Transactions on Network and Service Management*, 19(3):2536–2548.

[Narra et al. 2019] Narra, K. G., Lin, Z., Wang, Y., Balasubramaniam, K., and Annavaram, M. (2019). Privacy-preserving inference in machine learning services using trusted execution environments. *arXiv preprint arXiv:1912.03485*.

[Nogueira et al. 2021] Nogueira, M., Borges, L. F., and Nakayama, F. (2021). Das redes vestíveis aos sistemas ciber-humanos: Uma perspectiva na comunicação e privacidade dos dados. *Sociedade Brasileira de Computação*.

[Onesimu et al. 2022] Onesimu, J. A., Karthikeyan, J., Eunice, J., Pomplun, M., and Dang, H. (2022). Privacy preserving attribute-focused anonymization scheme for healthcare data publishing. *IEEE Access*, 10:86979–86997.

[Padgette et al. 2017] Padgette, J., Scarfone, K., and Chen, L. (2017). Guide to bluetooth security. *NIST special publication*, 800(121).

[Papaioannou et al. 2022] Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., and Lymberopoulos, D. (2022). A survey on security threats and countermeasures in internet of medical things (iomt). *Transactions on Emerging Telecommunications Technologies*, 33(6):e4049.

[Pereira et al. 2021] Pereira, R. S., Prazeres, C. V. S., Barbosa, M. T. M., Barros, E. B. C., and Peixoto, M. L. M. (2021). Iotfogsim: Um simulador orientado a eventos para avaliaçao de aplicaçoes baseadas em iot-fog-cloud. In *Anais Estendidos do XXXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 25–32. SBC.

[Perez et al. 2022] Perez, A. J., Siddiqui, F., Zeadally, S., and Lane, D. (2022). A review of iot systems to enable independence for the elderly and disabled individuals. *Internet of Things*, page 100653.

[Philip et al. 2021] Philip, N. Y., Rodrigues, J. J., Wang, H., Fong, S. J., and Chen, J. (2021). Internet of things for in-home health monitoring systems: Current advances, challenges and future directions. *IEEE Journal on Selected Areas in Communications*, 39(2):300–310.

[Price et al. 2020] Price, A. B., Rarity, J. G., and Erven, C. (2020). A quantum key distribution protocol for rapid denial of service detection. *EPJ Quantum Technology*, 7(1):8.

[Qu et al. 2017] Qu, Z., Zhang, G., Cao, H., and Xie, J. (2017). Leo satellite constellation for internet of things. *IEEE access*, 5:18391–18401.

[Rashidi and Mihailidis 2012] Rashidi, P. and Mihailidis, A. (2012). A survey on ambient-assisted living tools for older adults. *IEEE journal of biomedical and health informatics*, 17(3):579–590.

[Rodrigues et al. 2018] Rodrigues, J. J., Segundo, D. B. D. R., Junqueira, H. A., Sabino, M. H., Prince, R. M., Al-Muhtadi, J., and De Albuquerque, V. H. C. (2018). Enabling technologies for the internet of health things. *Ieee Access*, 6:13129–13141.

[Salama et al. 2019] Salama, M., Elkhatib, Y., and Blair, G. (2019). Iotnetsim: A modelling and simulation platform for end-to-end iot services and networking. In *Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing*, pages 251–261.

[Sampaio et al. 2021] Sampaio, L. N., Freitas, A. E. S., Araújo, F. R., Brito, I. V. S., and Ribeiro, A. V. (2021). Revisitando as icns: Mobilidade, segurança e aplicações

distribuídas através das redes de dados nomeados. In *Livro de Minicursos do XXXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) 2021*.

[Saxena and Raychoudhury 2017] Saxena, D. and Raychoudhury, V. (2017). Design and verification of an ndn-based safety-critical application: A case study with smart healthcare. *ieee transactions on systems, man, and cybernetics: systems*, 49(5):991–1005.

[Shang et al. 2016] Shang, W., Bannis, A., Liang, T., Wang, Z., Yu, Y., Afanasyev, A., Thompson, J., Burke, J., Zhang, B., and Zhang, L. (2016). Named data networking of things. In *2016 IEEE first international conference on internet-of-things design and implementation (IoTDI)*, pages 117–128. IEEE.

[Shi et al. 2015] Shi, Y., Zheng, Q., Liu, J., and Han, Z. (2015). Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation. *Information Sciences*, 295:221–231.

[Souppaya and Scarfone 2012] Souppaya, M. and Scarfone, K. (2012). Guidelines for securing wireless local area networks (wlans). *NIST Special Publication*, 800:153.

[Srivastava et al. 2020] Srivastava, G., Agrawal, R., Singh, K., Tripathi, R., and Naik, K. (2020). A hierarchical identity-based security for delay tolerant networks using lattice-based cryptography. *Peer-to-Peer Networking and Applications*, 13:348–367.

[Steele et al. 2009] Steele, R., Lo, A., Secombe, C., and Wong, Y. K. (2009). Elderly persons' perception and acceptance of using wireless sensor networks to assist healthcare. *International journal of medical informatics*, 78(12):788–801.

[Tshiningayamwe et al. 2016] Tshiningayamwe, L., Lusilao-Zodi, G.-A., and Dlodlo, M. E. (2016). A priority rate-based routing protocol for wireless multimedia sensor networks. In *Advances in Nature and Biologically Inspired Computing: Proceedings of the 7th World Congress on Nature and Biologically Inspired Computing (NaBIC2015) in Pietermaritzburg, South Africa, held December 01-03, 2015*, pages 347–358. Springer.

[Tun et al. 2021] Tun, S. Y. Y., Madanian, S., and Mirza, F. (2021). Internet of things (iot) applications for elderly care: a reflective review. *Aging clinical and experimental research*, 33:855–867.

[Uddin et al. 2019] Uddin, M., Nadeem, T., and Nukavarapu, S. (2019). Extreme sdn framework for iot and mobile applications flexible privacy at the edge. In *2019 IEEE International Conference on Pervasive Computing and Communications (PerCom*, pages 1–11.

[United Nations 2020] United Nations (2020). World population ageing 2020 highlights: Living arrangements of older persons (st/esa/ser.a/451). Disponível em `https://www.un.org/development/desa/pd/sites/www.un.org.development.desa.pd/files/undesa_pd-2020_world_population_ageing_highlights.pdf`. Acessado: 2023-03-12.

[Wang et al. 2022] Wang, Z., Xiong, H., Zhang, J., Yang, S., Boukhechba, M., Zhang, D., Barnes, L. E., and Dou, D. (2022). From personalized medicine to population health: a survey of mhealth sensing techniques. *IEEE Internet of Things Journal*.

[Xu et al. 2019] Xu, S., Yang, G., and Mu, Y. (2019). Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation. *Information Sciences*, 479:116–134.

[Yang et al. 2020] Yang, P., Xiong, N., and Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *IEEE Access*, 8:131723–131740.

[Yaseen et al. 2022] Yaseen, F. A., Alkhalidi, N. A., and Al-Raweshidy, H. S. (2022). She networks: Security, health, and emergency networks traffic priority management based on ml and sdn. *IEEE Access*, 10:92249–92258.

[Zgheib et al. 2019] Zgheib, R., Conchon, E., and Bastide, R. (2019). Semantic middleware architectures for iot healthcare applications. In *Enhanced Living Environments: Algorithms, Architectures, Platforms, and Systems*, pages 263–294. Springer.

[Zhang et al. 2014] Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Claffy, K., Crowley, P., Papadopoulos, C., Wang, L., and Zhang, B. (2014). Named Data Networking. *SIGCOMM Comput. Commun. Rev.*, 44(3):66–73.

[Zhang et al. 2020] Zhang, Y., Chen, G., Du, H., Yuan, X., Kadoch, M., and Cheriet, M. (2020). Real-time remote health monitoring system driven by 5g mec-iot. *Electronics*, 9(11):1753.

[Zhang et al. 2018] Zhang, Z., Yu, Y., Ramani, S. K., Afanasyev, A., and Zhang, L. (2018). Nac: Automating access control via named data. In *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*, pages 626–633. IEEE.