Capítulo 4

Aplicações em Redes de Sensores na Área da Saúde e Gerenciamento de Dados Médicos: Tecnologias em Ascensão

Allan C. N. dos Santos, Ricardo M. Firmino, Julio C. H. Soto, Dianne S. V. de Medeiros, Diogo M. F. Mattos, Célio V. N. de Albuquerque, Flávio Seixas, Débora C. Muchaluat-Saade e Natalia C. Fernandes (UFF)

Abstract

Sensor networks have become increasingly popular in healthcare due to the widespread use of cell phones and accessories capable of capturing medical data and the growth of remote patient monitoring initiatives. Medical data captured by sensors are sensitive and require the guarantee of authenticity, confidentiality, and privacy in the context of the Brazilian regulations, according to "Lei Geral de Proteção de Dados" (LGPD). Besides, the management and guarantee of medical data interoperability depend on the use of syntax and semantics following international standards. Therefore, the cloud computing and the Internet of Things are enabling tools for digital technologies to improve patient care. In this chapter, we present and discuss sensor networks' main concepts and the collection, processing, and protection of data from sensitive medical data.

Resumo

As redes de sensores têm se tornado cada vez mais populares na área de saúde devido à ampla disseminação dos celulares e acessórios aptos a captar dados médicos e ao crescimento de iniciativas de monitoramento remoto de pacientes. Dados médicos são considerados dados sensíveis e como tal requerem a garantia de autenticidade, confidencialidade e privacidade no contexto da Lei Geral de Proteção de Dados (LGPD). Paralelamente, a gerência e garantia de interoperabilidade de dados médicos dependem do uso de sintaxe e semânticas de acordo com padronizações internacionais. Assim, a utilização da computação em nuvem e a Internet das Coisas são facilitadores para o desenvolvimento de tecnologias digitais para melhorar o atendimento ao paciente. Considerando esse cenário, este capítulo apresenta e discute os principais conceitos relacionados às redes de sensores e à coleta, tratamento e proteção de dados de médicos sensíveis.

4.1. Introdução

A recente pandemia de COVID-19 mudou a forma como o mundo vê as relações interpessoais e o provimento de atendimento em saúde. Dada a necessidade de distanciamento social, atividades de telessaúde foram repensadas, mudando a perspectiva da comunidade médica e da sociedade como um todo sobre o tema. Nesse sentido, ganha cada vez mais importância a capacidade de se monitorar pacientes à distância e também acessar e gerenciar dados médicos.

As redes inteligentes de sensores fornecem uma tecnologia de monitoramento da saúde de forma ininterrupta. Com o advento das redes móveis e um acesso mais amplo da sociedade a redes de banda larga, tornou-se possível fornecer meios de comunicação de alta disponibilidade e alta taxa de transferência. Dentro desse cenário, o número de dispositivos conectados à Internet vem crescendo aceleradamente em função da popularização de celulares inteligentes (*smartphones*) e da diversidade de dispositivos de Internet das Coisas (*Internet of Things* - IoT). Estima-se que, ao final de 2020, o número de objetos conectados à Internet ultrapasse 50 bilhões [Mattos et al., 2018] e os dispositivos portáteis de saúde estão entre os de crescimento mais rápido nesse mercado.

O uso de redes de sensores para o monitoramento de pacientes e transferência de dados médicos já é uma realidade [Matthew Pike e Brusic, 2019]. As aplicações de redes de sensores na área da saúde são cada vez mais amplas, como no monitoramento de sinais vitais, na atenção a acidentes, como quedas de idosos em suas residências, e ainda em aplicações médicas específicas para acompanhamento de doenças. De fato, hoje em dia, até mesmo a posição geográfica é vista como um dado de saúde, em iniciativas que visam, por exemplo, detectar as probabilidades de contágio em diferentes regiões, de acordo com os locais onde pessoas infectadas transitaram.

Este capítulo tem como objetivo discutir aplicações de destaque utilizando redes de sensores na área da saúde e o gerenciamento dos dados coletados. Através da descrição das novas tecnologias em redes e gerenciamento de dados médicos, são discutidos aspectos técnicos e sociais relacionados ao uso da tecnologia no monitoramento diário e no acompanhamento de doenças.

Entre as redes de sensores utilizadas para monitorar a saúde humana, observa-se um uso mais amplo das redes de sensores sem fio (*Wireless Sensor Networks* -WSN). Essas redes são caracterizadas como um conjunto de sensores especializados distribuídos espacialmente que simultaneamente são capazes de monitorar, registrar e comunicar dados representando medições de variáveis ambientais ou de um determinado sistema. Nesse sentido, cabe destaque às redes corporais sem fio (*Wireless Body Area Networks* - WBAN), que permitem a comunicação entre diversos sensores e atuadores corporais. Este capítulo tem como objetivo apresentar o panorama atual dessas tecnologias, bem como os seus desafios.

Entre esses desafios, a segurança das redes de comunicação e da informação ganha grande destaque. Para manipular qualquer tipo de dado médico, há que se garantir a autenticidade, confidencialidade e privacidade na gestão do acesso à informação. Esse é um tema de bastante importância, em especial devido à Lei Geral de Proteção de Dados

(LGPD)[1]. De fato, qualquer tipo de dado de saúde é considerado como sensível, por expor o indivíduo em sua privacidade.

Ainda com relação ao tratamento da informação, outra questão relevante na gerência e garantia de interoperabilidade de dados médicos é o uso de sintaxe e semânticas de acordo com padronizações internacionais. A coleta de dados de saúde pode se dar de inúmeras formas, mas o armazenamento necessita seguir padrões comuns, para que os dados possam ser aproveitados e trocados entre diferentes sistemas. Sem esse tipo de padronização, há até mesmo o risco de interpretação incorreta de dados coletados.

Outra questão importante, também discutida neste capítulo, diz respeito à utilização da computação em nuvem para armazenar o alto volume de dados que podem ser coletados [Badidi e Moumane, 2019]. Essa grande massa de dados, se devidamente processada, pode ser aproveitada para melhorar o atendimento ao paciente, otimizar processos e ajudar as partes interessadas e os aplicativos do setor de saúde a tomar decisões mais rápidas e precisas.

Este capítulo está organizado como descrito a seguir. Primeiramente, na Seção 4.2, são apresentados os principais conceitos relacionados às redes de sensores. Na Seção 4.3, são apresentadas algumas utilizações das redes de sensores para monitoramento de dados de saúde. São apresentados exemplos relacionados ao monitoramento de quedas, do ambiente, de dados gerados por *smart devices*, de grandes massas na disseminação de doenças, entre outros. Na Seção 4.4, são apresentados os principais desafios de segurança no tratamento de dados coletados, considerando questões como a transmissão e gerência de dados, além dos impactos advindos da LGPD. Na Seção 4.5, são discutidas as aplicações para armazenamento de dados em nuvem. São apresentados conceitos básicos sobre a tecnologia de computação em nuvem, além da utilização de objetos inteligentes no contexto da saúde. Na sequência, na Seção 4.6, são discutidas questões relacionadas à interoperabilidade entre sistemas e ao processamento em fluxo. São apresentados também os principais padrões para dados médicos internacionais. Por fim, o minicurso é concluído na Seção 4.7, aonde são apresentados alguns comentários finais sobre o tema.

4.2. Redes de Sensores na Área da Saúde

A transmissão frequente de informações sensoriais ocorre utilizando dispositivos de baixo custo e cada vez menores, capazes de detectar o mundo físico e comunicar esses dados através de redes sem fio. Torna-se cada vez mais evidente que as redes de sensores, em breve, fecharão a lacuna entre o mundo virtual e o real [Gama e Gaber, 2007]. Com redes de sensores e atuadores, pode-se expandir o monitoramento ambiental, aumentar a segurança de edifícios, melhorar a precisão de operações militares, fornecer melhores cuidados de saúde e oferecer ajuda bem direcionada, entre muitas outras aplicações. De muitas maneiras, as redes de sensores são significativamente diferentes das redes sem fio clássicas e redes móveis. A diferença reside no fato de que o desenho de uma rede de sensores é fortemente orientado por sua aplicação específica. Uma outra diferença é que os nós sensores são altamente limitados em termos de consumo de energia, complexidade e custo de produção. Além disso, o objetivo comum dos nós leva a reunir e transmitir in-

[1]Lei nº 13.709/2018, acessível em `http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm`.

formação onde a cooperação pode ser utilizada como fonte de eficiência. Estas particularidades das redes de sensores levam a solução de problemas de pesquisa muito relevantes e desafiadores.

4.2.1. Conceito de Redes de Sensores sem Fio

Uma rede de sensores, em uma visão mais ampla, consiste na interligação de estações, usualmente muito pequenas, capazes de monitorar um ou mais tipos de dados e transmiti-los. Essas estações são chamadas de nós sensores. A principal função dos nós sensores é monitorar, registrar e notificar uma condição específica em vários locais para outras estações através de uma infraestrutura de comunicação. A condição específica de um local se traduz em parâmetros, tais como temperatura, umidade, pressão, direção do vento, velocidade, intensidade da iluminação, localização, funções vitais do corpo, como respiração, frequência cardíaca, arritmias, pressão sanguínea arterial, nível de açúcar no sangue, etc.

O avanço na área de microprocessadores, novos materiais de sensoriamento, microssistemas eletro-mecânicos e comunicação sem fio tem estimulado o desenvolvimento e uso de sensores inteligentes em áreas ligadas a processos físicos, químicos, biológicos, dentre outros. Normalmente, o termo *sensor inteligente* é aplicado ao chip que contém um ou mais sensores com capacidade de processamento de sinais e comunicação de dados. A tendência é produzir esses sensores em larga escala, diminuindo o seu custo, e investir ainda mais no desenvolvimento tecnológico desses dispositivos, levando a novas melhorias e capacidades.

Os aplicativos para redes de sensores sem fio podem ser variados, geralmente envolvendo algum tipo de parâmetro monitoramento [Montoya et al., 2010]. Nós sensores podem ser vistos como computadores pequenos, extremamente básicos em termos de suas interfaces e de seus componentes. Embora esses dispositivos possuam capacidade restrita, eles apresentam recursos substanciais de processamento quando estão em funcionamento. Cada nó em uma rede de sensores é normalmente equipado com um transceptor de rádio ou outro dispositivo de comunicação sem fio, um pequeno microcontrolador e uma fonte de energia, geralmente uma bateria. Assim, usualmente, as redes de sensores sem fio estão sujeitas a restrições de energia. Um nó sensor pode variar de tamanho de acordo com sua aplicação. Uma rede de sensores sem fio normalmente constitui uma rede ad-hoc sem fio, o que significa que cada sensor suporta um algoritmo de roteamento multi-salto. Normalmente, toda a rede é gerenciada por um controlador, também chamado de Nó Coordenador [Montoya et al., 2010].

Existem vários protótipos de redes de sensores diferentes disponíveis para uso. O estado da arte está bem representado por uma classe de nós sensores multiuso chamados *motes*, que foram originalmente desenvolvidos na Universidade de Califórnia, Berkeley, e estão sendo implantados e testados por vários grupos de pesquisa e empresas iniciantes. Sensores típicos, como MICA, MICAZ ou TELOS-B, consistem em de uma combinação de módulos diferentes, particularmente um cartão de aquisição de dados, um *mote* processador (512 Kb), uma interface de radio (300 - 2500 MHz) e bateria (similar a pilha AAA). Outro exemplo de nós sensores, ainda em estado de protótipo, foi desenvolvido pela Universidade Livre de Berlim, sendo chamados de *Embedded Sensor Board* (ESB). Esses

sensores são semelhantes aos MICA, mas oferecem um consumo de energia mais baixo. No modo inativo e no modo ativo, um ESB requer $8\mu A$ e cerca de $10mA$, com taxas de transmissão médias de 0.8 bytes por segundo, o que resulta em vida útil da rede de 5 a 17 anos. Na maioria das implementações atualmente disponíveis, os nós sensores são controlados por sistemas operacionais baseados em módulos, como o TinyOS e linguagens de programação como nesC ou TinyScript/Maté [Gama e Gaber, 2007]. Para gestão dos sistemas dos sensores, existem plataformas para Mica Motes[2], Tmote Sky[3], BTnodes[4], Waspmotes[5], Sun Spots[6], G-Nodes[7], para motes da série TIP[8], entre outras [Montoya et al., 2010].

No início do desenvolvimento da tecnologia, os principais desafios enfrentados pelas redes de sensores sem fio eram restrições de hardware e recursos energéticos limitados. Agora, os principais problemas estão relacionados à capacidade de capturar, processar, armazenar, sincronizar e gerenciar vários fluxos de dados de redes de sensores sem fio grandes e dinâmicas, além de poder responder em tempo real quando necessário. Segundo estimativas, a quantidade total de dados dobra a cada dois anos, ou até mais rapidamente [Pike et al., 2019]. Ou seja, os sistemas baseados em sensores geram enormes quantidades de dados, que estão crescendo exponencialmente. Enquanto a análise de dados tradicional emprega principalmente estatísticas, o volume de dados gerado pelas redes de sensores, que pode ser considerado em algumas aplicações como *Big Data*, geralmente requerem o uso de aprendizado de máquina, modelagem matemática e inteligência artificial. Nesse sentido, esses dados usualmente requerem um pré-processamento de dados em tempo real para reduzi-los a um tamanho viável, sincronização de diferentes fluxos de dados que permitem a extração de informações críticas, novos algoritmos para respostas em tempo real, e gestão do conhecimento e sua implantação em tempo real [Matthew Pike e Brusic, 2019].

Pesquisadores estão trabalhando para tornar possível a ampla visão da saúde inteligente. A importância de integrar tecnologias como radiofrequência (RFID), Bluetooth, ZigBee e sensores, juntamente com redes sem fio de grande escala para fornecer aplicativos sensíveis ao contexto é cada vez mais clara. Além de fornecer a difusão de tecnologias de rede sem fio existentes e relativamente mais maduras, o desenvolvimento de dispositivos pequenos e discretos permite não apenas coletar informações precisas, mas também a entrega confiável de dados. Além disso, é importante a combinação das tecnologias dos sensores, dos pacientes e das pessoas envolvidas para formar o ciclo geral de um sistema de saúde. Finalmente, há também um esforço significativo de pesquisa no desenvolvimento de sensores sem fio minúsculos, de preferência integrados a tecidos ou outras substâncias que possam ser implantados no corpo humano [Alemdar e Ersoy, 2010].

[2]http://www.xbow.com
[3]http://www.moteiv.com
[4]http://www.btnode.ethz.ch
[5]http://www.libelium.com/products/waspmote
[6]http://www.sunspotworld.com/SPOTManager
[7]http://sownet.nl/index.php/en/products/gnode
[8]http://www.maxfor.co.kr

4.2.1.1. Redes Corporais sem Fio

Uma rede corporal sem fio (WBAN - *Wireless Body Area Network*) consiste normalmente de uma coleção de dispositivos heterogêneos miniaturizados e invasivos, de baixo consumo de energia, ou dispositivos leves e não invasivos, com recursos de comunicação sem fio que operam nas proximidades do corpo humano. Esses dispositivos podem ser colocados dentro, sobre ou ao redor do corpo e geralmente são nós sensores sem fio que podem monitorar as funções e características do corpo humano a partir do ambiente a sua volta [Cavallari et al., 2014]. Cada sensor tem requisitos específicos e é usado para diferentes missões. Esses dispositivos são usados para medir alterações nos sinais vitais de um paciente e detectar emoções como medo, estresse, felicidade, etc. Eles se comunicam com um Nó Coordenador, que geralmente é menos restrito a energia e tem mais capacidade de processamento. O Nó Coordenador é responsável pelo envio de sinais biológicos do paciente ao sistema de saúde ou diretamente ao médico, a fim de permitir diagnóstico em tempo real e oferecer suporte à tomada de decisões médicas [Negra et al., 2016].

De fato, os aplicativos WBAN cobrem vários aspectos para melhorar a qualidade de vida dos usuários. Essas aplicações podem ser categorizadas principalmente de acordo com o uso na área médica ou não médica. As aplicações não médicas incluem detecção de movimento e gestos para aplicativos interativos de monitoramento de jogos, reconhecimento cognitivo e emocional para assistência ao motorista ou interações sociais, e assistência em eventos de desastre, como ataques terroristas, terremotos e incêndios. As aplicações médicas compreendem soluções de assistência médica para a população em geral. Exemplos típicos incluem a detecção precoce, prevenção e monitoramento de doenças, assistência a idosos em casa, reabilitação após cirurgias, aplicações de *biofeedback*[9] que controlam estados emocionais e aplicações de vida assistida que melhoram a qualidade de vida de pessoas com deficiência [Negra et al., 2016]. As WBANs permitem novos mercados possíveis com relação a suas aplicações, porém seu planejamento é afetado por vários problemas que exigem novos padrões e protocolos. As WBANs criam um conjunto de desafios técnicos com uma grande variação em termos de métricas de desempenho esperadas, como taxa de transferência ou atraso. Assim, é necessário novas arquiteturas, protocolos flexíveis, recursos computacionais, etc [Cavallari et al., 2014].

A Figura 4.1 mostra a arquitetura comum da WBAN, que consiste em comunicações em três camadas: comunicações Intra-BAN, comunicações Inter-BAN e comunicações além da BAN. As comunicações Intra-BAN denotam as comunicações entre os sensores corporais sem fio e o nó coordenador da WBAN. As comunicações inter-BAN envolvem comunicações entre o nó coordenador e dispositivos pessoais, como *notebooks*, robôs de serviço doméstico e outras WBANs. A camada além da BAN conecta o dispositivo pessoal à Internet [Negra et al., 2016]. A comunicação entre diferentes partes é suportada por várias tecnologias, como IEEE 802.15.4, IEEE 802.15.6 e *Bluetooth Low Energy*. Tais tecnologias são abordadas amplamente na Subseção 4.2.2 [Cavallari et al., 2014, Negra et al., 2016, Taha et al., 2018].

[9] O biofeedback envolve o monitoramento e o uso de informações fisiológicas através de aparelhos sensores eletrônicos para ensinar os pacientes a modificar funções fisiológicas específicas de forma voluntária [McKee, 2008]

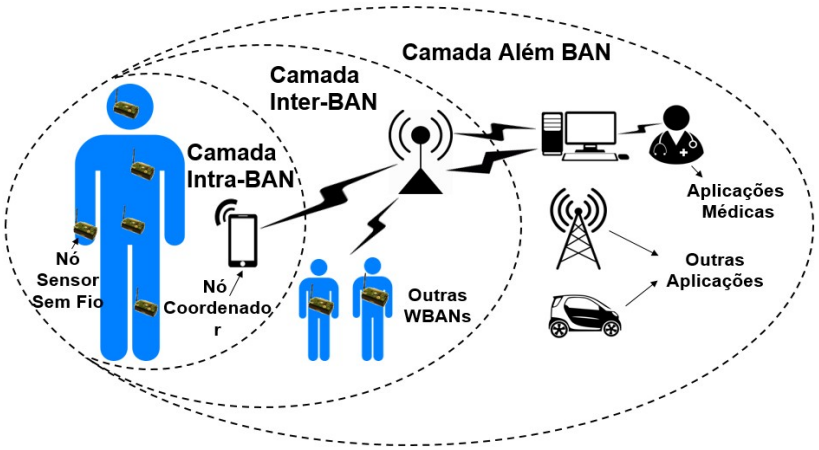

Figura 4.1. Arquitetura das WBANs (Comunicação intra, inter e além da BAN).

As WBANs precisam definir a melhor solução para sua comunicação, diante do grande número de padrões disponíveis, dependendo dos requisitos da aplicação. Com respeito aos principais problemas a serem considerados no desenho de uma WBAN, o impacto do meio sem fio, a vida útil da bateria e a coexistência com outras redes sem fio são de fundamental importância. A presença do corpo humano afeta a propagação das ondas de rádio, levando a um canal de rádio específico e peculiar que deve ser adequadamente considerado no desenvolvimento dos protocolos. A necessidade de vida útil e de longa duração da bateria deve ser atendida através de soluções eficientes em termos de energia, uma vez que as substituições frequentes da bateria devem ser evitadas, sendo uma tarefa muito difícil em algumas aplicações (por exemplo, aplicações médicas nas quais os nós são implantados). A terceira questão principal a ser levada em consideração é a ocorrência de interrupções devido à coexistência com outras redes sem fio operando na mesma faixa de frequência [Cavallari et al., 2014].

De acordo com [Taha et al., 2018], utilizando WBANs nos setores médicos, os custos com saúde podem ser significativamente reduzidos e o monitoramento regular do paciente no hospital pode ser evitado. De fato, o pensamento humano sobre a gestão da saúde pode se transformar consideravelmente devido ao uso de WBANs, de forma similar à maneira que a Internet transformou nossas visões em direção à comunicação de grande volume de informação rapidamente. As WBANs são eficazes para automatizar a interação humana com variedades de tecnologias da informação, onde as vantagens dos sensores inteligentes podem ser exploradas para amostrar, monitorar, processar e comunicar sinais de dados úteis entre várias partes do corpo de maneira rápida e confiável. Além disso, médicos e enfermeiros podem fornecer *feedback* em tempo real ao paciente. A WBAN pode examinar continuamente os parâmetros fisiológicos do paciente com mobilidade e flexibilidade extras. Além disso, gera uma quantidade de dados muito grande do ambiente e do paciente, o que auxilia os médicos a obterem uma visão mais ampla e compreensível da situação do paciente. No entanto, a aceitação prática de WBANs requer sobrepor enormes desafios sociais, legais e técnicos. Tais desafios podem abrir muitos novos caminhos em termos de planejamento e implementação de sistemas. Os principais objetivos da WBAN são obter atraso mínimo, produtividade ideal, longa durabilidade da

rede e baixo uso de energia na comunicação. Alguns dos pré-requisitos significativos do usuário para WBANs incluem segurança, privacidade, compatibilidade, confiabilidade e baixo custo.

4.2.2. Infraestrutura de Redes de Sensores

Nos últimos anos, os pesquisadores fizeram progressos consideráveis na caracterização do ambiente de propagação da área corporal através de estudos baseados em medições e simulações, a fim de apoiar a previsão do desempenho do canal em configurações alternativas de implantação de sensores e o desenvolvimento de antenas mais eficazes. Esses trabalhos foram realizados em diferentes bandas de frequência. Em cada uma das faixas de frequência, foram estudados os canais para *intra-body*, *on-body* e externo. A Figura 4.2 mostra uma exemplificação das tecnologias utilizadas em uma WBAN.

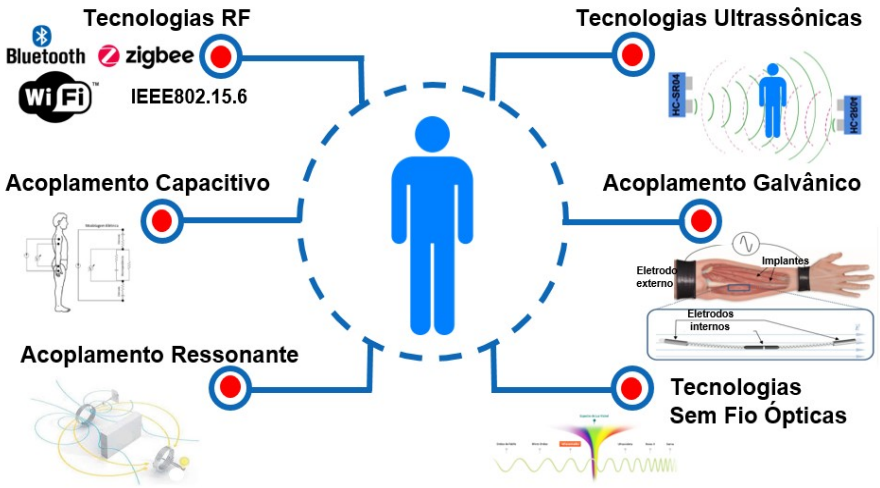

Figura 4.2. Tecnologias utilizadas em WBANs.

- *Tecnologias RF*: A maioria das comunicações atuais das redes sensores sem fio são baseadas nas tecnologias WPAN (*Wireless Personal Area Network*) IEEE 802.15, que operam na faixa ISM (*Industrial Scientific and Medical*) de 2.4 GHz. O *Bluetooth* é um sistema de comunicação de curto alcance, que em sua quarta versão conhecida como *Bluetooth Low Energy* (BLE), é projetado para suportar comunicações dispositivo para dispositivo com baixa complexidade, baixo custo e baixo consumo de energia, oferecendo taxas de dados de até 2 Mbps. A quinta versão do *Bluetooth* foi desenvolvida especialmente para conectividade de dispositivos IoT, possuindo diferentes classes de potência que podem atender a diferentes distâncias de 100, 10 e 1m, com uma potência máxima de transmissão de $100, 2, 5$ e $1mW$ respectivamente [Haddad e Khalighi, 2019, Cavallari et al., 2014, Negra et al., 2016]. A topologia em estrela, que o *Bluetooth* fornece, oferece um melhor suporte à mobilidade para os nós em uma comunicação interna em redes corporais sem fio. As comunicações inter-redes corporais sem fio podem ser realizadas através de um segundo rádio ou usando um chip de modo duplo, no entanto, o custo é maior no consumo de energia [Cao et al., 2009].

Outra solução é o padrão ZigBee/IEEE 802.15.4, desenvolvido para conectividade sem fio de baixo custo para aplicativos com potência limitada e requisitos de produtividade relaxados. Com um protocolo simples e flexível, oferece taxas de dados de 20 a 250 Kbps dentro de um intervalo típico de 10 m e uma potência de transmissão limitada a 10 mW. O Zigbee é uma tecnologia de baixo custo e baixo consumo de energia, construída na parte superior do padrão IEEE 802.15.4 [Haddad e Khalighi, 2019, Cavallari et al., 2014]. O perfil de aplicativo público do *ZigBee Health Care* recentemente concluído fornece uma estrutura flexível para atender aos requisitos da *Continua Health Alliance* para monitoramento remoto da saúde e do condicionamento físico. O *ZigBee Health Care* possui as características de alcance, energia e dispositivos conectados simultaneamente para suportar dispositivos dos domínios de telessaúde e telecuidado em uma única tecnologia sem fio. Além disso, adotando o padrão ZigBee, permite controlar dispositivos sem fio médicos como sensores corporais. Essas soluções se adéquam melhor aos cenários de implantação de uma rede corporal sem fio em uma área limitada (por exemplo, um hospital ou uma casa) [Cao et al., 2009, Negra et al., 2016].

O IEEE 802.11 é um padrão que oferece conjunto de indicadores para uma WLAN (*Wireless Local Area Network*). Baseado no padrão IEEE 802.11 e 802.11ah (especifica o uso de frequências abaixo de 1 GHz), o Wi-Fi permite que os usuários naveguem pela Internet, mudem de banda e também estejam conectados a um ponto de acesso (AP) ou no modo ad hoc, no qual a rede se forma sob demanda, sem requisitos de infraestrutura prévia. É ideal para grandes transferências de dados ao permitir a conectividade confiável de alta velocidade. Essas vantagens podem ser adotadas pelos sensores sem fio, mas o alto consumo de energia é um inconveniente importante [Negra et al., 2016].

O padrão IEEE 802.15.6 de baixa potência e baixo alcance foi projetado especificamente para redes corporais sem fio, oferecendo taxa de dados de até 15 Mbps com uma potência de transmissão entre 0.1 e $1mW$. O padrão define a transmissão em banda estreita nas bandas ISM, WMTS (*Wireless Medical Telemetry Service*) e MICS (*Medical Implant Communication Service*), bem como a banda UWB (*Ultra-Wideband*) e a comunicação HBC (*Human Body Communication*). As taxas de transmissão nas faixas variam de 57.5 até 971.4 Kbps para transmissão em banda estreita, 0.487 até 15.6 Mbps para UWB e 164 Kbps até 1.3 Mbps para HBC (operando a 21 MHz) [Haddad e Khalighi, 2019]. Como relatado, o padrão IEEE 802.15.6 provavelmente empregará UWB, de acordo com propostas recentes [Cao et al., 2009]. O padrão pretende dotar os sensores da próxima geração nas proximidades ou dentro do corpo humano [Cavallari et al., 2014, Negra et al., 2016, Ferreira et al., 2018].

De acordo com a *Federal Communications Commission* (FCC), o UWB refere-se a qualquer tecnologia de rádio com uma largura de banda de transmissão superior a 500 MHz ou 20% da frequência central. A FCC também regula o uso de UWB sem licença na faixa de $3.25 - 4.75GHz$ e $6.6 - 10.25GHz$, para ter uma emissão de densidade espectral de potência relativamente baixa. Isso leva à adequação das aplicações UWB em ambientes internos e de curto alcance, além de ambientes sensíveis às emissões de RF (por exemplo, em um hospital). O UWB também oferece,

à tecnologia de radio, aplicações como localização precisa que complementa o GPS no ambiente interno para rastreamento na rede corporal sem fio [Cao et al., 2009]. Um dispositivo compatível com a banda UWB deve suportar uma transmissão e recepção em pelo menos uma das seguintes bandas de frequência: $863-870MHz$, $902-928MHz$, $950-958MHz$, $2360-2400MHz$ e $2400-2483.5MHz$. Em particular, este último está na banda ISM e é extremamente interessante por causa de sua disponibilidade mundial, mas pode haver problemas de coexistência com outros padrões que trabalham na mesma banda [Cavallari et al., 2014].

- *Tecnologias Ultrassônicas*: As comunicações ultrassônicas são possibilitadas pela propagação de ondas acústicas no interior do corpo humano em frequências superiores a 20 KHz. Elas têm o potencial de complementar ou substituir as tecnologias de RF para comunicação por meio de implantes, graças à sua baixa atenuação nos tecidos humanos. Os transceptores usados para comunicações ultrassônicas são principalmente transdutores piezoelétricos [Haddad e Khalighi, 2019]. O ultrassom tem sido utilizado em aplicações médicas com baixa potência irradiada que permite uma melhor margem de segurança, fornecendo uma largura de banda necessária para a aplicação. Estudos em comunicação intra-corporal ultrassônica mostram que é possível alcançar taxas de dados de 90 kbps até 700 Kbps, com um consumo de energia de 36 mW até 40 mW [Santagati e Melodia, 2016, Demirors et al., 2016]. Além disso, mostraram que a atenuação é menor que as comunicações de RF. O ultrassom é um método de comunicação promissor para as redes de sensores sem fio, especialmente para aplicativos que requerem transmissão de alta taxa de dados [Tomlinson et al., 2018].

- *Acoplamento Capacitivo*: Os métodos de acoplamento geralmente são baseados na transferência de energia entre um conjunto de transmissores e receptores para gerar um sinal elétrico que se propaga através do corpo humano [Callejon et al., 2013]. O sinal elétrico gerado pelos métodos de acoplamento é de baixa frequência (abaixo de 200 MHz) e baixa potência (na ordem de μW), em comparação com os sinais eletromagnéticos tradicionais. O acoplamento capacitivo ocorre quando dois circuitos que compartilham o mesmo campo elétrico causam um fluxo de energia de um circuito para o outro. No caso de acoplamento capacitivo intra-corpo, o campo elétrico comum do corpo e seu ambiente causam um fluxo de corrente induzido por um transmissor para um receptor na forma de eletrodos. Um eletrodo transmissor e um receptor são conectados (ou permanecem próximos) ao corpo, enquanto outros dois estão flutuando, atuando como eletrodos de aterramento. O corpo atua como um condutor do potencial elétrico e o solo atua como um caminho de retorno para o sinal. Pesquisas recentes sobre acoplamento capacitivo tem alcançado taxas de dados de 2 até 60 Mbps em faixas de 1-200 MHz. Os métodos de acoplamento tornaram-se um componente popular das pesquisas em andamento sobre redes de sensores, uma vez que sua baixa potência e baixa frequência obedecem às considerações de segurança e diminuem o consumo de energia [Tomlinson et al., 2018].

- *Acoplamento Galvânico*: O acoplamento galvânico é um método que usa o corpo humano como um canal para propagar o sinal elétrico criado por um par de eletrodos acoplados. A diferença entre esse método e o acoplamento capacitivo é que a

corrente alternada é acoplada dentro do corpo, em vez de entre o corpo e o ambiente. No lado de transmissão e recepção, existem dois eletrodos, onde uma tensão é aplicada entre os dois eletrodos de transmissão e o fluxo de corrente alternada passa através do corpo para ser medido diferencialmente nos eletrodos receptores. A corrente se propaga devido ao conteúdo de íons do corpo humano. As duas propriedades do corpo que permitem a propagação dos sinais são a permissividade relativa e a condutividade elétrica. As taxas de transmissão de dados parecem ser inferiores às do acoplamento capacitivo, em frequências do sinal que variam de 10 kHz a 100 MHz. O acoplamento galvânico pode ser usado para comunicação entre pele, músculo e tecido adiposo, onde suas propriedades são afetadas pela camada de tecido usada como meio, assim como também pela localização dos eletrodos no corpo. O acoplamento galvânico é um método seguro e eficiente, mas é relativamente novo [Tomlinson et al., 2018].

- *Acoplamento Ressonante*: O acoplamento ressonante utiliza as propriedades da ressonância eletromagnética para gerar um campo magnético em todo o corpo. Cria um campo de transmissão sem fio de energia elétrica entre duas bobinas colocadas ao redor do corpo, impulsionando a propagação do campo. Seus benefícios potenciais surgem de baixos requisitos de energia. A faixa de espectro mais comumente utilizada nesta tecnologia é 50 MHz, produzindo uma atenuação máxima de apenas 8.1 dB, para uma distância de 40 cm percorrida [Park e Mercier, 2015]. Ainda não se tem concluídas taxas de transmissão exatas. O funcionamento da tecnologia apresenta interferência com outros campos magnéticos, incluindo máquinas elétricas e, por esse motivo, ainda precisa de uma investigação mais profunda [Tomlinson et al., 2018].

- *Tecnologias Sem Fio Ópticas*: As comunicações ópticas sem fio acontecem nas faixas infravermelha, visível ou ultravioleta do espectro. São uma alternativa potencial ou complemento às tecnologias de RF para redes corporais sem fio médicas, graças à sua alta imunidade a interferências externas. Além disso, a potência de transmissão nos sistemas de comunicação óptica sem fio não é restringida pelos regulamentos como para os homólogos de RF. O interesse das tecnologias ópticas sem fio foi investigado em vários trabalhos para aplicações médicas corporais e extra-corporais. Esses estudos mostraram um consumo de energia de $17mW$ para uma taxa de dados de 10 Kbps, que é muito menor à máxima potência emitida para comunicações infravermelhas [Haddad e Khalighi, 2019]. Alguns estudos são apresentados em [Trevlakis et al., 2019, Parmentier et al., 2008, Liu et al., 2012].

4.3. Sensoriamento de Eventos na Assistência em Saúde e Bem-Estar

As redes de sensores fornecem uma tecnologia para monitoramento da saúde de forma ininterrupta. Com o advento das redes móveis 5G de baixa potência, se tornou possível fornecer meios de comunicação de alta disponibilidade e alta taxa de transferência, viabilizando muitas aplicações de monitoramento. Esta seção tem como objetivo descrever aplicações de rede de sensores na área da saúde.

O surgimento da tecnologia IoT (*Internet of Things*) vem afetando profundamente o ecossistema da saúde. Essa tecnologia tem o potencial de mudar a maneira como as

instalações e os prestadores de assistência médica coletam e usam dados para os serviços oferecidos aos pacientes. Nos serviços de saúde mais modernos, existe uma grande quantidade de dados oriundos dos sensores de dispositivos IoT que monitoram em tempo real as operações dos vários sistemas.

É importante mencionar que os dados gerados pelas redes de sensores são diferentes daqueles gerados por registradores de dados, porque os sensores individuais geram dados cooperativamente e esses dados são frequentemente processados e filtrados na fonte [Matthew Pike e Brusic, 2019]. Pode-se citar, como exemplo de redes de sensores, aqueles incorporados em *smartphones* e *smartwatches, health bands*, casas inteligentes, sistemas de seguranças, veículos como carros, ônibus e aviões. Há um tempo atrás, os dados coletados pelos dispositivos eram tipicamente coletados e analisados *offline* para futuras decisões. Alguns casos especiais eram aplicações críticas em tempo real, por exemplo, gerenciamento de rede elétrica, terapia intensiva, sistemas de monitoramento ou piloto automático. Essas aplicações antigas não eram adaptativas. Elas foram projetadas para responder a partir de um conjunto de condições. As redes de sensores contemporâneas são sistemas multi-agentes que podem medir variáveis e perceber o estado e comportamento do ambiente. A partir dessas medições, o sistema pode responder de acordo com o contexto [D. Ovalle e Montoya, 2010].

Outras questões estão relacionadas à tecnologia e à técnica de acesso, aos tipos e quantidade de sensores distribuídos ou à possibilidade de utilização de diferentes faixas de frequência. O tipo de aplicação, seja ele de natureza individual ou de saúde coletiva, e a área de abrangência da rede modificam os tipos de dados coletados, a frequência de coleta, o volume coletado, e até mesmo o tipo de comunicação utilizado. As redes de sensores demandam que os fluxos de dados sejam combinados e sincronizados para interpretá-los adequadamente de maneira contínua [Matthew Pike e Brusic, 2019].

Um objetivo comum das pesquisas em redes de sensores é permitir um comportamento inteligente [D. Ovalle e Montoya, 2010], isto é, compreender, interpretar, aprender com os dados e fornecer respostas ou ações adequadas. Isso requer a aplicação de técnicas de aprendizado de máquina [Matthew Pike e Brusic, 2019]. É importante notar que entender esses novos tipos de dados gerados pela rede de sensores é fundamental para a sua análise de requisitos. Entre os diferentes domínios de dados, os dados biomédicos podem estar entre os mais complexos de gerenciar e usar. Os dados gerados pelos sensores biomédicos são abrangentes, diversificados, heterogêneos e devem ser isolados para proteger a privacidade dos indivíduos.

4.3.1. Monitoramento de Ambientes

Considerando todas essas questões, as aplicações de monitoramento ambiental relacionadas à saúde buscam uma variedade de fins, como o monitoramento de quedas, monitoramento do ambiente hospitalar, monitoramento da qualidade do ar dentro e fora de *smart homes*, monitoramento de hábitos e humor para detecção de situações de risco e potenciais enfermidades, entre diversos outros.

4.3.1.1. Monitoramento de Quedas

Uma queda é definida como um evento no qual uma pessoa se move rapidamente de uma posição mais alta para uma mais baixa de nível sem controle. As quedas são um problema sério de saúde pública e as pessoas com mais de 65 anos de idade estão entre as mais vulneráveis às lesões sérias decorrente de uma queda. De acordo com a Organização Mundial da Saúde, quase 40% das mortes relacionadas a lesões são devido a quedas de pessoas idosas na maioria dos países [Todd e Skelton, 2004]. Portanto, as quedas são a segunda principal causa de morte, estando logo após os acidentes de trânsito. As quedas resultam em 90% das fissuras no quadril e no pulso, além de 60% dos ferimentos na cabeça das pessoas idosas [G. Fortino, 2015]. Ainda acrescenta-se o fato de que as quedas podem afetar negativamente a mentalidade de um indivíduo idoso, resultando em uma péssima autoestima, por se tornar dependente de uma pessoa constantemente o monitorando, além do desgosto de constantes idas para o hospital. Uma abordagem natural e prática para os idosos ou para as pessoas com dificuldade de locomoção exige um sistema eficaz para verificar remotamente o seu bem-estar aonde eles estiverem.

Assim, uma das principais aplicações de monitoramento ambiental em *smart homes* é o monitoramento de quedas, especialmente em ambientes com idosos. Detectar e responder às quedas rapidamente, em especial quando o idoso está sozinho, é de primordial importância para reduzir os impactos do problema [Sposaro e Tyson, 2009, Mano et al., 2016a].

O primeiro sistema para detecção de quedas foi desenvolvido no início da década de 1970 e enviava mensagens de alerta quando um botão de emergência era pressionado [Pannurat et al., 2014]. Os sistemas atuais são bem mais sofisticados e capazes de atuar sem a necessidade de ações por parte de pessoa que caiu. Muitos sistemas para detecção de quedas de idosos são baseados na premissa de que o idoso estará portando o seu telefone. Nesse sentido, os sensores do telefone, tais como acelerômetros, giroscópios e magnetromêtros [Sposaro e Tyson, 2009, Mao et al., 2017] são usados em algoritmos que detectam quando a queda aconteceu. Outras abordagens usam *wearable motes*, utilizando lógicas semelhantes à do uso do celular para detectar e notificar a queda [Paoli et al., 2012]. Uma crítica comum aos sistemas baseados em celular e/ou *wearable motes* é que não é verdade que os idosos estarão sempre portanto os dispositivos necessários para detectar a queda. Assim, outros sistemas usam o monitoramento efetivo do ambiente para detectar as quedas, não dependendo que o idoso porte nenhum dispositivo. Tais tipos de sistema utilizam câmeras, câmeras infravermelhas, sensores de videogames, como o *Microsoft Kinect*, sensores de pressão e de vibração no piso, *arrays* de microfones, sensores de presença, entre outros [Pannurat et al., 2014, Noury et al., 2000].

A Figura 4.3 mostra a arquitetura típica de sistemas de monitoramento de queda em tempo real. Dados de movimentação capturado por sensores são enviados para uma unidade de processamento. Quando a queda é detectada, uma ação ou um alarme é disparado, tal como: alertas sonoros, que notificam outras pessoas no mesmo prédio; intervenção imediata, pelo acionamento da atuação de *airbags* infláveis, por exemplo; e envio de mensagens para parentes ou cuidadores, informando dados como local e hora do acidente e estado do idoso, por exemplo, se está consciente, se levantou ou se está incapacitado de se mover após a queda [Pannurat et al., 2014].

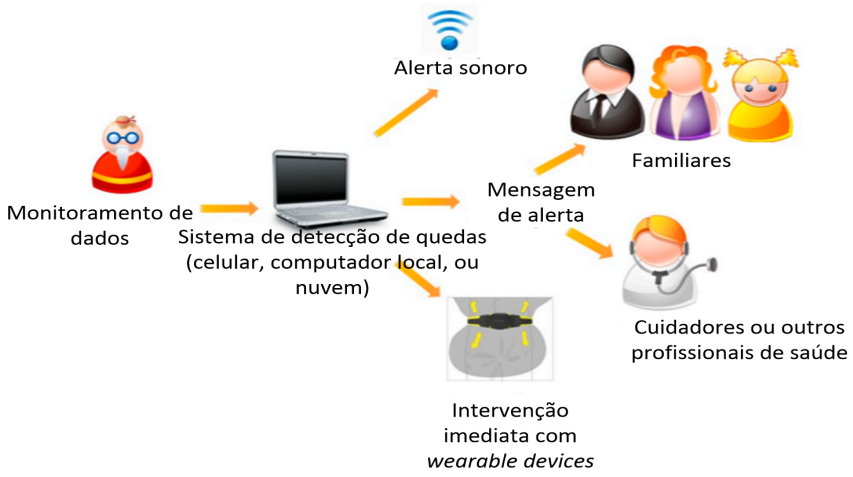

Figura 4.3. Exemplo de arquitetura típica de sistemas de detecção de quedas. Adaptado de [Pannurat et al., 2014].

4.3.1.2. Monitoramento de Hábitos e Emoções em *Health Smart Homes*

Um ambiente inteligente é aquele com capacidade de adaptar o ambiente aos habitantes e cumprir as metas de conforto e eficiência. Para atingir esses objetivos, as pesquisas em *Health Smart Homes* são usualmente focadas em sistemas que percebem o estado do ambiente usando sensores e que atuam, consequentemente, com os controladores de dispositivos.

Em [Medjahed et al., 2011], os autores exemplificam um sistema que integra sensores (infravermelho, sensores de mudança de estado, áudio, fisiológicos) conectados a um PC. O sistema multimodal para detecção de situações de problemas a saúde e angústia foi chamado de EMUTEM (Ambiente Multimodal para Televigilância *Médicale*), sendo aplicado em casas de repouso para idosos. A arquitetura desenvolvida consiste em: um conjunto de microfones colocados em todos os cômodos da casa dos idosos, que permitem o monitoramento remoto do sistema acústico; um dispositivo vestível, chamado RFpat, que pode medir dados fisiológicos como frequência cardíaca de pulso ambulatorial, detectar se a pessoa está em pé, sentada ou deitada, queda da pessoa equipada e sua taxa de atividade; um conjunto de sensores infravermelhos que detectam a presença da pessoa em uma determinada parte da casa, sua postura e também seu movimento; e um conjunto de sensores domóticos, como sensores de contato, sensores de temperatura e vários outros sensores domésticos, para monitoramento das condições do ambiente. Os dados são coletados para tratamento com algoritmos de lógica *fuzzy* visando detectar situações anormais.

O telemonitoramento automático de situações de perigo à saúde ou de angústia em um ambiente é de grande importância, e o telemonitoramento médico em casa pode ser uma solução interessante, pois oferece vigilância médica em um ambiente familiar para o paciente. Nesse sentido, pesquisas recentes estão desenvolvendo tecnologias para melhorar a segurança de um residente e monitorar as condições de saúde usando sensores

e outros dispositivos. Destacam-se, por exemplo, algumas referências [Medjahed et al., 2011] que se propõem a definir uma arquitetura genérica para sistemas de telemonitoramento, realizar experimentos de um sistema de monitoramento remoto em uma categoria específica de pacientes (com problemas cardíacos, asma, diabéticos, pacientes com doença de Alzheimer ou cognitiva, etc.) ou construir apartamentos interligados ambientados a rede de sensores e sistemas de alarme adaptados aos requisitos de telemonitoramento da saúde.

Outras iniciativas de monitoramento ambiental visam levantar hábitos e sentimentos humanos, com o fim de prever atividades potencialmente prejudiciais, ou ainda, que indiquem a presença de alguma doença, como a de [Mshali et al., 2018]. Nesse trabalho, os autores promovem o monitoramento de atividades diárias por meio de câmeras e usam um modelo de previsão para detectar modificações de comportamento que são potencialmente de risco. De forma similar, Yassine et al propõem um modelo baseado em *big data* e *smart homes* para descobrir e aprender padrões de atividades humanas para aplicações de cuidados em saúde [Yassine et al., 2017]. Nesse trabalho, os autores monitoram os padrões de uso de energia dentro das residências para inferir o comportamento dos moradores. Com base nesses padrões, são conhecidas as rotinas diárias, o que permite a identificação de atividades anômalas que podem indicar a dificuldade das pessoas de promover os seus próprios cuidados em saúde e bem-estar, como preparar a comida e tomar banho. Outros trabalhos em *smart homes* visam utilizar o aprendizado de máquina para detectar emoções humanas com câmeras em *smart homes* [Mano, 2018, Mano et al., 2016b].

4.3.1.3. Monitoramento da Qualidade do Ar em *Smart Homes* e *Smart Cities*

A qualidade do ambiente pode interferir tanto nos insumos armazenados quanto na saúde das pessoas que estão neste local. Cabra et al apresentam uma abordagem baseada em IoT e monitoramento ambiental para avaliar a temperatura e umidade relativa do ar em hospitais e farmácias, para garantir a qualidade dos produtos de saúde armazenados [Cabra et al., 2017]. De fato, um excesso de umidade ou uma temperatura elevada podem tornar nulo ou prejudicial o efeito de uma medicação, por exemplo.

A qualidade do ar também é abordada para outros fins relacionados à saúde. English et al descrevem as iniciativas da *Imperial County Community Air Monitoring Network*, que é um grupo colaborativo entre comunidades, pesquisadores, iniciativa privada e governo para o monitoramento da qualidade do ar e dos seus efeitos sobre a população. Essa iniciativa dos Estados Unidos utiliza processos de monitoramento do ar pelas comunidades utilizando sensores de baixo custo, cujos dados são repassados para a definição de planejamento social, direções de pesquisa e projetos de ação [English et al., 2017].

Outros trabalhos abordam o monitoramento da qualidade do ar em ambientes internos a *smart homes*. Patil el al [Patil et al., 2018] monitoram os níveis de oxigênio dentro da residência e emitem alarmes quando os níveis caem abaixo dos limites aceitáveis. Tal tipo de monitoramento é de especial importância em grandes centros urbanos com elevados graus de poluição.

4.3.2. Monitoramento Remoto para Detecção de Doenças

Esta seção tem como objetivo comentar sobre as possibilidades de uso dos dispositivos *smartwatches* e as tecnologias recentes para o sensoriamento da saúde. Dispositivos portáteis de saúde estão entre os de crescimento mais rápido no mercado da Internet das Coisas (IoT). Com o avanço da IoT, esses dispositivos móveis ganharam impulso no domínio das aplicações digitais biomédicas e de saúde.

A integração de sensores de saúde de baixo custo com *smartphones, health bands e smartwatches*, por exemplo, tem aumentado a capilaridade na assistência médica inteligente (*Smart Healthcare*). Essa integração permite que os prestadores de assistência médica possam fornecer um monitoramento remoto do paciente. Uma pesquisa realizada em 2015[10] mostrou que quase 84% dos provedores de serviços usam dispositivos móveis para monitoramento de pacientes. O *Remote Patient Monitoring* (RPM) permite que os médicos possam monitorar remotamente doenças, como por exemplo, apneia do sono, arritmia e Insuficiência Cardíaca Congestiva (ICC). Nesse tipo de serviço remoto, os dados dos sensores são enviados em fluxo usando *Bluetooth* ou *Wi-Fi* para um dispositivo móvel. Nesse dispositivo, vários eventos são correlacionados usando a linguagem *Continuous Query Language* (CQL) [Shivnath Babu, 2001], com o objetivo de detectar a complexidade e a ordem dos eventos. Geralmente, um evento complexo (*Complex Event* - CE) corresponde à ocorrência de múltiplos eventos nos sensores a partir da medição atingir um limiar específico, por exemplo. Os sensores incorporados nos dispositivos *smartwatches* como um giroscópio, acelerômetro e posicionamento global (GPS) também podem ser adicionados aos sensores de saúde para enriquecimento de contexto.

Algumas aplicações podem ser utilizadas em conjunto com dispositivos móveis na detecção de doenças ou em diagnósticos. O *Cooking Hacks*[11] oferece um serviço barato e eficiente de sensores de saúde sem fio habilitados para *Bluetooth* e *Wi-Fi*. Nesse sistema, os sensores podem encaminhar sinais fisiológicos para um aplicativo Android ou *iOS* usando sua interface de programação de aplicativos (*Application Programming Interface*).

Outros dispositivos de monitoramento de saúde comercial incluem o *Zeo Sleep Monitor*[12], o qual monitora distúrbios do sono, como apneia do sono. O indivíduo começa usando a faixa para cabeça Zeo todas as noites. A faixa para a cabeça usa a tecnologia de sensor *SoftWave*, para medir com precisão e segurança seus padrões de sono através dos sinais elétricos produzidos naturalmente pelo cérebro. À medida que a pessoa passa por diferentes níveis de sono, mais leve a mais profundo ou vice-versa, o Zeo *Headband* rastreia a qualidade do sono.

O *ViSi Mobile*[13] pode medir parâmetros vitais como pulso, taxa de respiração, saturação de oxigênio (Spo2) e temperatura da pele [Dhillon et al., 2018]. Foi desenvolvido para fornecer tecnologias inovadoras no monitoramento de vigilância e integrar os sensores, algoritmos e análises do paciente para reduzir custos e melhorar a flexibilidade do fluxo de trabalho. Desenvolvido pela *Sotera Wireless*, o sistema de monitoramento

[10] *www.spyglass-consulting.com*

[11] *www.my-signals.com*

[12] https://www.amazon.com/Zeo-Model-ZEOBP01-Personal-Sleep-Manager/dp/B002IY65V4

[13] https://www.soterawireless.com/

de pacientes *ViSi Mobile* é um sistema projetado para aprimorar a segurança do paciente, permitindo a detecção de problemas críticos à saúde do paciente e conectando os médicos a seus pacientes em qualquer lugar e a qualquer momento. Ele é uma plataforma para monitoramento abrangente de sinais vitais que mantém os médicos conectados a seus pacientes.O sistema permite o monitoramento preciso e contínuo de todos os sinais vitais essenciais, com pressão arterial não invasiva, batimento a batimento, bem como atividade e postura do paciente. O sistema pode ser integrado através de um *middleware*, como o *Capsule*.

A maioria das metodologias atuais de monitoramento de pacientes remoto coletam os sinais de saúde usando um dispositivo móvel, como um *tablet, health bands* ou *smartwatches*, e encaminha os dados para um servidor hospitalar remoto para a detecção de eventos complexos. Portanto, essa técnica requer que o dispositivo móvel esteja sempre conectado à rede. Sendo assim, é importante realçar que esses tipos de sistemas podem levar a um grande uso da rede móvel. A indisponibilidade do serviço de rede ou uma rede limitada, como por exemplo, as de zonas rurais, pode gerar entregas de dados atrasados e fora de serviço, ocasionando quedas de desempenho no funcionamento da aplicação.

4.3.3. Monitoramento de Grandes Massas contra Disseminação de Pandemias

O uso de telemetria (sistema tecnológico de monitoramento, utilizado para comandar, medir ou rastrear alguma coisa à distância) tem sido feito com sucesso pelo mundo. Esse monitoramento é usado inclusive para observar grandes massas contra a disseminação de epidemias internacionais [Kim et al., 2016]. Por trás desse tipo de sistema, usualmente, existe uma complexa rede de algoritmos que usa inteligência artificial, aprendizado de máquina e análise comportamental para gerar os resultados. O monitoramento também é importante para enfrentar as epidemias sazonais, que ocorrem, em geral, no inverno com mais ou menos intensidade conforme uma série de fatores[14]. Por exemplo, tem-se o impacto do surto de COVID-19, que tornou-se motivo de grande preocupação para praticamente todos os países do mundo. A escassez de recursos para suportar o surto de COVID-19, combinada com o medo de sistemas de saúde sobrecarregados, forçou a maioria dos países ao estado de isolamento social. Pessoas infectadas têm sido submetidas a tratamentos com isolamento e monitoramento a fim de minimizar o risco de alastramento da doença. As autoridades iniciaram o uso de *scanners* de temperatura em aeroportos e estações de trem e ônibus. Pessoas com sinais de febre recebem máscaras, são registradas e encaminhadas a hospitais e clínicas. A transmissão de informações está sendo aliada no controle e isolamento, quanto também no desenvolvimento de pesquisas e tratamentos para as pessoas infectadas.

Em situações como essa, redes de sensores podem ajudar de diversas formas, como no monitoramento remoto do paciente sem oferecer risco de contaminação para os profissionais. Um exemplo é o aplicativo móvel para assistência médica que processa dados de sensores de umidade e temperatura [Aileni, 2015]. Esse aplicativo é baseado em computação em nuvem - modelo de computação em nuvem SaaS (software como ser-

[14]http://agenciabrasil.ebc.com.br/saude/noticia/2019-06/monitorar-mutacoes-do-virus-da-gripe-envolve-esforco-internacional

viço). Esse aplicativo utiliza a infraestrutura *Sensor-Cloud*, que tornou-se popular porque pode fornecer uma estrutura aberta, flexível e reconfigurável para monitorar e controlar aplicativos. Ela é utilizada em aplicações de rede de sensores sem fio para serviços de saúde, mas também pode ser utilizada para fins militares, monitoramento de infraestrutura crítica, monitoramento de ambiente e área de fabricação. As informações de assistência médica armazenadas em uma nuvem podem ser compartilhadas facilmente. A infraestrutura de computação em nuvem para os sensores pode ser usada para implantar aplicativos que fornecem monitoramento aos pacientes (umidade, temperatura ou pressão sanguínea). Os dados são enviados e armazenados em servidor para serem analisados posteriormente por médicos ou profissionais de saúde.

Outro uso interessante das redes de sensores contra epidemias como a de COVID-19 é a detecção da propagação da doença. É impressionante como, em boa parte do tempo, as pessoas estão próximas de seus dispositivos móveis, onde o dispositivo está ao alcance dos braços. Com isso, os *smartphones* se tornam uma ótima ferramenta para realizar o rastreamento de contatos.

Em [Altuwaiyan et al., 2018], o objetivo é usar *smartphones* para coletar os dados necessários de cada usuário, executando a varredura sem fio adaptável de tempos em tempos. Com os dados, pode-se identificar se houve a aproximação de determinados usuários da rede, servindo como base para o estudo de casos de transmissão de doenças. O sistema utiliza *smartphones*, dispositivos sem fio de curto alcance, como pontos de acesso e dispositivos *Bluetooth*, e um servidor. O *smartphone* coleta os dados brutos necessários sobre os sinais sem fio nas proximidades de *Wi-Fi* e *Bluetooth* e criptografa esses dados antes de enviá-los ao servidor. O *smartphone* coleta os seguintes dados em cada verificação de rede: identificador exclusivo de dispositivo sem fio (BSSID - *Basic Service Set Identifier*), indicação de intensidade do sinal recebido sem fio (RSSI - *Received signal strength indication*), e o tipo de sinal sem fio (*Wi-Fi, Bluetooth*). O RSSI é uma função que, usando a potência de transmissão, ajuda a determinar a distância ao receptor. O *smartphone*, então, carrega os dados criptografados, juntamente com o registro de data e hora de cada escaneamento de rede, para o servidor. Todas as informações são criptografadas pelo *smartphone* do usuário antes de enviá-las ao servidor. Além disso, o sistema utiliza um método de correspondência que preserva a privacidade, que usa criptografia homomórfica para combinar dispositivos sem fio comuns entre o usuário infectado e o usuário comum. Todas as operações acontecem sem a necessidade do usuário divulgar outras informações confidenciais. Nesse sistema, a distância entre os usuários é um fator importante. O alcance médio da cobertura do *Wi-Fi* é de cerca de 80 metros ao ar livre e 50 metros no interior, ou seja, a maior distância entre dois usuários diferentes conectados ao mesmo ponto de acesso *Wi-Fi* é de cerca de 160 metros ou 100 metros no caso de cobertura interna. Suponha que o dispositivo tenha reconhecido um usuário infectado. O dispositivo deve divulgar todas as informações ao servidor para que o servidor possa usá-las posteriormente para calcular as pontuações correspondentes. Para aumentar a precisão correspondente, é preciso coletar o máximo de informações possível sobre o ambiente sem fio ao redor do usuário. Assim, foi desenvolvido um método de pontuação correspondente baseado em peso, que usa recursos diferentes, como os valores de RSSI e o número de dispositivos sem fio comuns. As informações médicas e laudos clínicos de cada paciente são carregado no servidor, assim o sistema irá identificar monitorar o

contato com pacientes infectados. Todos os outros usuários regulares são notificados para verificar suas pontuações correspondentes, que indicam se um usuário esteve em contato com a interface que estava conectada ao dispositivo do usuário infectado no passado.

Outra iniciativa para detectar o contágio utilizando *smartphones* é proposta por Zhang et al [Zhang et al., 2013b]. Os autores propõem uma integração de redes corporais sem fio (WBANs) para a coleta de sinais vitais corporais com telefones celulares visando à detecção de interação social para ajudar no controle de epidemias e localização de focos. Esse estudo exige que os usuários utilizem sensores em seus corpos, o que torna o sistema mais difícil e caro de implementar.

Sareen et al. [Sareen et al., 2018] propõem uma nova arquitetura baseada no dispositivo de identificação por radiofrequência (RFID), tecnologia de sensor vestível e infraestrutura de computação em nuvem. O objetivo do trabalho foi impedir a propagação da infecção pelo Ebola na fase inicial do surto, por volta de fevereiro de 2014. O surto do vírus Ebola na África Ocidental causou grandes perdas de vidas e desequilíbrios econômicos e sociais na região, principalmente na Guiné, Libéria e Serra Leoa. Ela foi a epidemia que mais disseminou a doença pelo vírus Ebola na história. Os primeiros casos foram registrados na Guiné em dezembro de 2013. Essa arquitetura de computação em nuvem usa RFID e sensores para a detecção e o monitoramento de pacientes infectados pelo Ebola. A árvore de decisão J48 é usada para avaliar o nível de infecção em um usuário, dependendo de seus sintomas. O RFID é usado para detectar automaticamente as interações de proximidade entre os usuários. A análise de rede temporal é aplicada para descrever e monitorar o estado atual do surto usando os dados das interações de proximidade.

Zhang et al. [Zhang et al., 2013a] propõem protocolos para dispositivos móveis baseados em proximidade e rede social (PMSN - *Proximity-based mobile social networking*) para permitir que dois usuários realizem a correspondência de perfis sem divulgar nenhuma informação sobre seus perfis. Esses protocolos permitem uma diferenciação mais precisa entre os usuários do PMSN e podem suportar uma ampla variedade de métricas correspondentes em diferentes níveis de privacidade. Esse é um exemplo de trabalho sobre como coletar e armazenar os dados de um usuário de maneira a preservar a privacidade. Esse artigo aborda esse desafio ao projetar novos protocolos de correspondência privada. Esses protocolos permitem que dois usuários realizem a correspondência de perfis sem divulgar nenhuma informação sobre seus perfis além do resultado da comparação, o que permite uma diferenciação mais precisa entre os usuários do PMSN e podem suportar uma ampla variedade de métricas de correspondência em diferentes níveis de privacidade.

Al Qathrady et al. [Qathrady et al., 2016] introduzem uma estrutura sistemática de detecção de infecções utilizando tecnologias de comunicação móvel, incluindo dispositivos móveis, redes e estatísticas de encontros durante a infecção. Os autores usaram a rede WLAN no campus da universidade da Flórida em *Gainesville*, de seis edifícios e mais de 34 mil usuários, para realizar o experimento. Os métodos de rastreamento e filtragem são propostos usando técnicas probabilísticas de busca direta e reversa. Primeiro, o problema de rastreamento da infecção da doença é definido. Em seguida, é desenvolvida uma estrutura prática detalhada usando nós sem fio para facilitar o rastreamento da origem da infecção e identificar a população em risco, os nós que provavelmente estão infectados.

Assim, essa estrutura de detecção de infecções sistemática usa as redes móveis e estatísticas de encontro durante surtos de infecção. O projeto visa fornecer práticas e algoritmos e sistemas eficientes, para rastrear epidemias com alta precisão, baixa sobrecarga e com preservação da privacidade a partir de dispositivos sensores, da coleta e processamento de informações de encontros.

Além da detecção do contágio, outras formas de uso dos sensores podem ser feitas no combate à disseminação de doenças. Por exemplo, a vacinação é uma maneira muito eficiente de proteger as pessoas de terem suas saúdes comprometidas por doenças infecciosas. No entanto, algumas vezes não é possível vacinar todas as pessoas em uma comunidade devido a várias restrições de recursos ou distância. Sun et al fornecem uma alternativa para obter um melhor desempenho na vacinação direcionada [Sun et al., 2015]. Com base em sensores sem fio transportados por alunos, foram coletados os rastros de contato interpessoal em uma escola secundária. Com o sistema de sensores sem fio, foi possível registrar os contatos dos alunos dentro da distância de propagação da doença para construir um grafo de propagação da doença, modelando o contágio. Com base neste grafo, os autores propõem uma métrica de centralidade e conectividade para medir a importância de um nó durante a propagação da doença e projetar algoritmos baseados em centralidade para a vacinação direcionada. Os resultados das simulações de rastreamento mostram que os algoritmos podem ajudar a conter efetivamente doenças infecciosas. Através dos dados armazenados é possível realizar o monitoramento das vacinações até mesmo com aplicativos de *smartphones*. Também é possível utilizar as informações para auxiliar na assistência médica, em pesquisas ou nas etapas da produção de uma vacina.

4.4. Segurança e Gerenciamento de Dados Médicos

Conforme apresentado na seção anterior, as aplicações existentes para assistência médica remota podem ser disponibilizadas em diferentes tipos de redes. Além disso, os dados médicos podem ser processados e armazenados remotamente. Isso quer dizer que milhões de informações de pacientes trafegam por redes e dispositivos heterogêneos. Por isso, a segurança dos dados é uma das preocupações mais importantes nas redes que utilizam tecnologia sem fio e computação em nuvem. Atualmente, os aplicativos multimídia incluem redes móveis, sensores integrados e serviços de Internet das Coisas (IoT) [Sureshkumar et al., 2019]. Os dados médicos precisam de uma atenção especial, pois incluem informações sensíveis da vida privada dos indivíduos. Os desafios das redes de sensores incluem a garantia da segurança, privacidade, integridade dos dados e confidencialidade dos registros dos usuários durante todo o tempo. Alguns mecanismos são geralmente adotados para tentar garantir uma comunicação segura entre os dispositivos, como protocolos com criptografia, autenticação e atualização dos dados [Al-Janabi et al., 2017]. Entretanto, as redes de sensores sem fio têm vulnerabilidades, com ataques e mecanismos de segurança diferentes daqueles das redes tradicionais – devido às suas características peculiares como energia, memória e armazenamento limitados [Ramos e Filho, 2015].

Outro ponto de interesse no que tange à segurança é que os dados médicos costumam ficar armazenados em bancos de dados para consulta dos interessados autorizados. Por isso, também são necessárias ferramentas para controle de acesso, autenticação de usuários e garantia da integridade e da confidencialidade.

4.4.1. Transmissão dos Dados

Qualquer rede de comunicação de dados está propensa a sofrer tentativas de ataques e/ou invasões. Por isso, geralmente são utilizados mecanismos de segurança para manter os dados trafegando de maneira protegida. No caso das redes sem fio, um fator extra é acrescentado ao aspecto de segurança. A utilização do ar como meio de transmissão torna a rede susceptível a diversos ataques que vão desde uma simples escuta clandestina (espionagem) passiva das mensagens até interferências ativas com a criação, modificação e destruição das mensagens [Fernandes et al., 2006]. No caso das redes de sensores sem fio, outro aspecto importante a ser considerado é a ausência de centralização e de infraestrutura. Apesar de a descentralização ter como vantagem a robustez, devido à inexistência de pontos únicos de falha, a ausência de infraestrutura dificulta a aplicação das técnicas convencionais de autorização de acesso e de distribuição de chaves. Isto torna mais difícil a tarefa de distinguir os nós confiáveis dos nós não-confiáveis, pois nenhuma associação segura prévia pode ser assumida [Fernandes et al., 2006]. Dessa forma, alguns tipos de ataques são mais propensos a ocorrerem em redes de sensores sem fio. Os mais conhecidos são:

- **Espionagem**: É um ataque passivo, onde um receptor indesejado consegue capturar e analisar os dados que trafegam na rede. É um ataque de difícil detecção e fácil de ser realizado, pois basta que um receptor adequado fique em modo de escuta capturando dados. A intenção do invasor pode ser o conhecimento de informações confidenciais ou o conhecimento dos nós principais da rede, analisando as informações de roteamento, para preparar um ataque ativo [Al Ameen et al., 2012]. Nas aplicações de saúde, o invasor seria capaz de coletar os dados de um paciente, informações sobre o caminho de transmissão desses dados, e informações da rede, como por exemplo, endereços dos nós principais. Para evitar este tipo de ataque, uma das soluções adotadas é a criptografia dos dados. Assim, mesmo que o invasor consiga capturar os dados, precisaria de uma chave para descriptografar as informações.

- **Injeção de novo nó**: Neste ataque, um nó malicioso é introduzido na rede. A intenção do ataque pode ser o de roubar informações úteis, ou de injetar dados falsos para comprometer o funcionamento da rede (Negação de Serviço). Uma das maneiras de realizar este ataque é assumir a identidade de um ou mais nós da rede de forma ilegítima. Uma variação é o Ataque do Homem no Meio (*Man-in-the-Middle*). Nesse caso, o nó malicioso intercepta uma comunicação entre dois nós legítimos e se passa por cada um deles, ficando no meio da comunicação. A autenticação de nós pode ser utilizada para evitar esse tipo de ataque [Bangash et al., 2017].

- **Ataques do tipo Negação de Serviço (DoS – *Denial of Service*)**: consiste em atacar a disponibilidade da rede visando interromper, subverter, destruir a rede ou diminuir a capacidade da rede de fornecer os serviços necessários [Al-Janabi et al., 2017]. Alguns exemplos desse tipo de ataque estão apresentados a seguir:

  - **Interferência (*Jamming*)**: é um tipo de ataque que consiste no uso de equipamentos que transmitem sinais com alta potência na mesma frequência de

rádio da rede, com o intuito de causar interferência ou interromper a comunicação legítima entre fonte e destino [Luong et al., 2017]. Uma fonte de interferência pode ser poderosa o suficiente para interromper toda a rede. Em aplicações WBAN, se esse ataque fosse feito para interromper a comunicação com o nó coordenador, os dados coletados pelos sensores não iriam chegar até seu destino final. Assim, os dados registrados na aplicação estariam desatualizados. As defesas típicas contra este ataque envolvem o uso de técnicas de espalhamento de sinal (*Spread Spectrum*), como a de Saltos em Frequência (*Frequency Hopping Spread Spectrum* - FHSS) [Sen e Jaydip, 2009]. Na técnica FHSS, a transmissão é realizada com alteração da frequência numa sequência pseudo-aleatória. Contudo, esses mecanismos exigem mais potência dos dispositivos, e em uma rede com limitação de potência, o custo dessas soluções deve ser levado em consideração [Luong et al., 2017]. Existem também soluções em que os nós identificam uma interferência e entram no modo suspensão por um período para economizar seus recursos [Raymond e Midkiff, 2008].

– **Colisão**: é uma variação do ataque de Interferência. Uma colisão ocorre quando dois ou mais nós tentam transmitir na mesma frequência e no mesmo instante de tempo. Quando os pacotes colidem, eles são descartados e precisam ser retransmitidos. As redes sem fio basicamente evitam a colisão escutando o canal antes de transmitir e durante sua transmissão. Nesse ataque, o invasor envia pacotes contínuos em todas as direções para colidir com os pacotes legítimos que estão sendo transmitidos e, portanto, a retransmissão ocorrerá para outros pacotes. A retransmissão causa atraso e drena a energia dos nós [Bangash et al., 2017]. No caso das aplicações WBAN, os nós sensores esgotariam sua energia e precisariam ser substituídos. Uma defesa típica contra ataques de colisão é o uso de códigos de correção de erros. No entanto, esses códigos também adicionam processamento e sobrecarga de comunicação. Além disso, é razoável supor que um invasor pode danificar uma quantidade de dados maior do que aquilo que pode ser corrigido [Sen e Jaydip, 2009].

– **Buraco Negro (*Black Hole*)**: esse ataque tenta destruir os serviços de rede, como roteamento ou encaminhamento de pacotes. Em um protocolo de roteamento típico, uma fonte transmite um pacote de solicitação de rota para todos os nós intermediários antes de enviar pacotes de dados para seu destino. Em seguida, os nós que estão na rota em direção ao destino respondem à origem com pacotes de resposta da rota. Pode existir um nó malicioso que afirma ter a rota mais curta para o destino e depois descarta pacotes recebidos em vez de encaminhá-los para o destino [Luong et al., 2017]. Nas aplicações de saúde, esse ataque pode causar atraso e desperdício de energia, pois os pacotes precisariam ser retransmitidos por outros caminhos. O gerenciamento adequado de chaves e a autenticação dos nós podem proteger o ataque do buraco negro, pois o nó do adversário não poderá se autenticar [Bangash et al., 2017]. Outro mecanismo de defesa é utilização de uma lista de observação que registra o mau comportamento dos sensores com o intuito de reconhecer

os sensores maliciosos e notificar os outros sensores para não se comunicarem com eles [Luong et al., 2017].

- **Ataque *Sybil***: um nó que pode assumir várias identidades de maneira ilegítima é introduzido na rede. O invasor pode usar as identidades dos outros nós para participar de algoritmos distribuídos, como a eleição. Um nó com várias identidades em momentos diferentes pode interromper o roteamento ou levar a resultados falsos pela inserção de dados falsos. Em WBAN, o nó malicioso pode usar identidades falsas para enviar informações falsas para o nó coordenador [Javadi e Razzaque, 2013]. É difícil identificar o nó legítimo [Bangash et al., 2017] sem o uso de técnicas de autenticação e métodos de criptografia [Malik et al., 2018]. Há também mecanismos que detectam identidades falsas e isolam o nó malicioso [Sen e Jaydip, 2009].
- **Ataques de Inundação de `HELLO`**: Muitos protocolos de roteamento em redes sem fio utilizam pacotes `HELLO` para definir o alcance de rádio entre um nó e seus vizinhos. Um invasor, com alto poder de transmissão, pode transmitir pacotes `HELLO` falsificados para convencer uma grande quantidade de nós de que são vizinhos do nó transmissor. Dessa forma, os nós inserem o invasor em suas tabelas de roteamento, e tentam enviar pacotes para ele. No entanto, o invasor está fora do alcance dos nós, e a rota é inalcançável. Nas redes WBAN, esse ataque pode causar atraso e desperdício de energia. Esse ataque pode ser evitado pela verificação da birecionalidade do enlace [Fernandes et al., 2006]. A utilização de algoritmo de criptografia também é uma solução para esse tipo de ataque [Malik et al., 2018].
- **Ataques de Inundação *(Flooding)***: O ataque de inundação é usado para esgotar os recursos de memória enviando um grande número de solicitações de configuração de conexão. Os sensores corporais sofrem com pouco espaço de memória, portanto, são vulneráveis a ataques de inundação. Em WBANs, o nó coordenador é um alvo muito atraente para inundações, pois é o coração do sistema. Se um invasor puder tornar o nó coordenador indisponível para a rede, todo o sistema pode ser bloqueado. Em muitos casos, o nó coordenador está conectado à Internet, o que permite ataques remotos, enquanto os atacantes não podem ter conectividade direta com os sensores corporais. Dessa forma, é necessário fornecer ao nó coordenador boa capacidade de energia, espaço de memória suficiente e mecanismos de segurança fortes, como autenticação, firewalls, constante monitoramento, dentre outros [Javadi e Razzaque, 2013].

As informações de saúde são confidenciais e devem ser protegidas e mantidas sempre em sigilo contra pessoas não autorizadas que possam usar os dados de forma prejudicial ao indivíduo. Diversas soluções de segurança foram desenvolvidas para proteger as redes de sensores sem fio desses fenômenos indesejados. As WBANs herdam a maioria dos desafios conhecidos de segurança das redes de sensores sem fio (WSN). No entanto, características típicas de WBANs, como restrições severas de recursos e condições físicas adversas, apresentam desafios únicos adicionais para suporte de segurança e privacidade [Javadi e Razzaque, 2013]. Os desafios de pesquisa envolvem minimizar o

consumo de bateria, assim como a utilização de protocolos que sejam seguros e ao mesmo tempo não sobrecarreguem os dispositivos em termos de processamento e memória [Ma et al., 2018], [Liang et al., 2012], [Bhangwar et al., 2017], [Selimis et al., 2011].

4.4.2. Gerenciamento dos Dados

Na área de saúde, os dados disponibilizados pelos sensores podem ser utilizados para realização de um diagnóstico ou até mesmo de um tratamento médico. Esses dados são abrangentes, diversificados, heterogêneos e devem proteger a privacidade dos indivíduos. Além disso, é necessário garantir a integridade e a veracidade desses dados, uma vez que uma informação imprecisa ou incorreta pode acarretar erro de diagnóstico ou tratamento médico inadequado para um paciente. Devido a essas características, o domínio de dados médicos é extremamente complexo de gerenciar e usar. Políticas de controle de acesso aos dados também devem ser estabelecidas para proteger a privacidade do indivíduo [Al-Janabi et al., 2017].

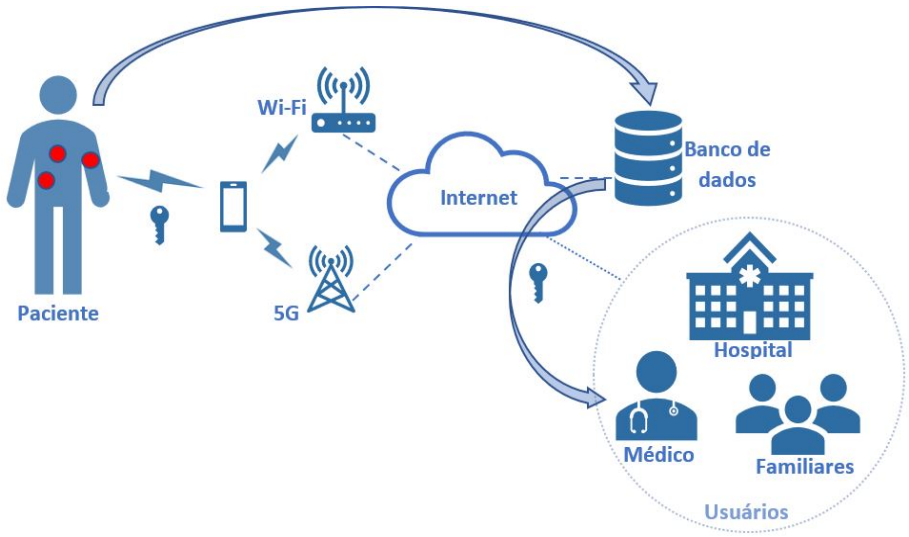

Figura 4.4. Transmissão e armazenamento seguro dos dados de WBAN na área de saúde.

A Figura 4.4 apresenta uma configuração típica de transmissão, armazenamento e coleta de dados em uma rede de sensores corporais sem fio aplicada à saúde. O paciente possui sensores que coletam e transmitem os dados por uma rede sem fio, e esses dados são, geralmente, armazenados em um banco de dados do fornecedor da aplicação do paciente. As informações são disponibilizadas para usuários do sistema de saúde, como médicos, e outros usuários autorizados pelo paciente. Para ter acesso aos dados, os usuários devem possuir uma chave. Nesse cenário, além da proteção dos dados durante a transmissão, é necessário garantir a segurança no armazenamento e na disponibilização da informação. Junto com o crescimento da utilização de ferramentas tecnológicas que facilitam o monitoramento e diagnóstico do paciente, cresce também a quantidade de registros de informações relacionadas à saúde e seu respectivo acesso. As informações médicas devem ser armazenadas com segurança em um prontuário eletrônico, para que as informações do paciente possam ser rastreadas quando transferidas de um médico para outro. Para garantir o armazenamento seguro e o gerenciamento de acesso, algumas

questões fundamentais de segurança devem ser resolvidas. Dentre elas estão a confidencialidade, o não-repúdio, o controle de acesso, a autenticação e a integridade dos dados.

A **confidencialidade** garante o sigilo das informações. Nas redes WBAN, os dados coletados pelos sensores são transmitidos por *smartphones* e podem passar por diversas redes antes de serem armazenadas. Além disso, os acessos aos dados que são feitos por médicos, pacientes e outros autorizados são realizados pelas mais diversas redes. A solução mais comum para garantia da confidencialidade é o uso de criptografia.

Não-repúdio é garantir que um usuário não negue o registro ou a alteração dele no sistema. Os dados médicos podem ser utilizados para tomada de decisões médicas ou em tratamentos, assim, esses dados precisam estar registrados, com a fonte autenticada e não deve ser possível apagar esses dados ou alterá-los.

A política de **controle de acesso** é tipicamente baseada no privilégio e direito de cada usuário autorizado. Em uma WBAN típica, diferentes médicos, equipe de assistência médica e agentes da companhia de seguros médicos são os principais usuários, mas o acesso a todas as informações médicas de um paciente específico pode não ser necessário para todos os tipos de usuários. Por exemplo, um médico em questão pode recuperar os dados de seu paciente, mas nenhuma outra informação do paciente [Chatterjee et al., 2014].

A **autenticação** é a verificação da identidade do usuário, o que é essencial antes de revelar qualquer tipo de informação sigilosa armazenada ou realizar alguma transação. Já a **integridade** é garantia de que a informação recebida não foi modificada. Um componente vital da integridade é garantir que os dados de assistência médica estejam totalmente protegidos contra ameaças ou perigos de segurança razoavelmente previstos e que todo o seu ciclo de vida seja totalmente auditável. Algumas soluções conhecidas têm sido utilizadas para controle de acesso e autenticação, sendo as mais comuns a validação por senha; a utilização de *token*; e o uso de chaves criptográficas. O uso de biometria como autenticação do usuário também vem sendo amplamente utilizado, pois os *smartphones* já possuem o sensor biométrico instalado. Em um sistema de saúde, as informações de saúde oferecidas pelos provedores e as identidades dos consumidores devem ser verificadas na entrada de cada acesso.

Em relação à garantia de integridade, a função resumo criptográfico (*hash*) é um dos mecanismos utilizados, e consiste em criar um resumo por meio de um algoritmo que faz o mapeamento dos dados. É considerada uma função unidirecional, ou seja, de difícil reversão, e por isso é bastante utilizada para assinaturas digitais, nas quais faz-se um resumo da mensagem antes da assinatura digital pela chave criptográfica. A assinatura digital, por sua vez, garante também a autenticidade da informação, ou seja, que ela foi produzida realmente por quem é de direito.

Uma tecnologia mais recente que pode ser empregada na segurança dos dados na área de saúde é a cadeia de blocos (*blockchain*). Essa tecnologia é bastante popular no setor de criptomoedas. A cadeia de blocos pode ser empregada para armazenar os dados do usuário da WBAN, evitando a violação dos dados devido às características intrínsecas da cadeia de blocos [Ren et al., 2019]. A cadeia de blocos é capaz de garantir as propriedades fundamentais da segurança da informação, como integridade, autenticidade e

não-repúdio, devido ao uso de resumos criptográficos (*hash*) encadeados entre os blocos da cadeia de blocos. Além disso, as estruturas de dados da cadeia de blocos também são adequadas para coletar dados de sensores e aplicativos móveis, aprimorando a análise dos riscos versus os benefícios dos tratamentos, bem como dos resultados relatados pelos pacientes. Portanto, essa tecnologia é vista como uma solução promissora para futuros serviços de saúde [de Oliveira et al., 2019] e sua integração com as últimas pesquisas sobre segurança é crucial para a implementação de uma arquitetura de saúde segura que suporte serviços médicos avançados [Mucchi et al., 2019].

4.4.3. Privacidade e a Lei Geral de Proteção de Dados

A palavra privacidade teve origem do latim, *privatus*, que significa "privado, particular, próprio". O vocábulo *privacy*, do direito inglês, deu significado ao termo *right to privacy*, definido pelo *Cambridge Advanced Learner's Dictionary* como "*direito de alguém manter seus assuntos e relacionamentos pessoais secretos*". Na legislação dos EUA, o termo "*healthcare information privacy*" ou "privacidade das informações de saúde" é definido como: *o direito de um indivíduo controlar a aquisição, o uso ou a divulgação de seus dados de saúde identificáveis* [HIMSS, 2010]. No Brasil, a divulgação de informações da vida privada é considerada violação ao direito fundamental da privacidade, e isto inclui os dados médicos de uma pessoa. Visando proteger essas informações privadas de uma pessoa, inclusive por meios digitais, foi criada a LGPD - Lei Geral de Proteção de Dados.

O texto da LGPD foi sancionado pela Lei nº 13.709, de 14 de agosto de 2018, e entraria em vigor após 24 meses da sua publicação, com exceção dos artigos referentes a criação da Autoridade Nacional de Proteção de Dados (ANPD), que estão em vigor desde 28 de dezembro de 2018. Contudo, o texto da Lei foi modificado em abril de 2020, e a LGPD entrará em vigor somente a partir de maio de 2021. Essa alteração foi realizada com a justificativa de que a pandemia do COVID-19 prejudicou a adequação das empresas à LGPD. Na Europa, existe legislação similar em vigor desde maio de 2018, a *General Data Protection Regulation* (GDPR), e de acordo com relatório da *GLA Piper* – escritório de advocacia multinacional – , já foram aplicadas pelas autoridades europeias multas que ultrapassam o valor 100 milhões de euros a empresas que descumpriram as regras da GDPR. Na legislação brasileira, as multas previstas podem atingir até 2% do faturamento da empresa, limitada a 50 milhões de reais por infração [Brasil., 2018].

O artigo primeiro da LGPD diz que seu objetivo é dispor sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, para proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A privacidade é considerada um direito fundamental pela LGPD, e está de acordo com a Constituição Federal Brasileira de 1988, que prevê a inviolabilidade da privacidade por meio dos termos intimidade e vida privada, e ainda assegura direito a indenização em caso de violação.

Dessa forma, no Brasil, a divulgação de dados pessoais é considerada violação ao direito fundamental da privacidade. A LGPD traz algumas definições importantes sobre os dados pessoais: primeiro, dado pessoal é a informação relacionada a pessoa natural identificada ou identificável; segundo, dado pessoal sensível inclui dado referente à saúde

ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; e, terceiro, dado anonimizado é dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Assim, está explícito que dado referente à saúde de uma pessoa é classificado como dado pessoal sensível, sendo o tratamento desse dado restrito a hipóteses específicas previstas no artigo onze. Sobre a definição de dado anonimizado, para a área de saúde, significa dizer que, se as informações médicas forem reveladas sem a possibilidade de identificação do paciente, essas podem ser classificadas como anonimizadas. Na prática, um médico poderia diagnosticar uma paciente sem conhecer sua identidade, apenas analisando seus dados médicos.

Portanto, em uma rede de sensores corporais sem fio, os dados privados dos pacientes devem ser protegidos desde a sua medição até o seu armazenamento e durante todo o tempo em que estiverem armazenados. Com o objetivo de minimizar ameaças à privacidade dos indivíduos, os detentores de dados têm realizado a supressão de dados de identificadores únicos no momento de sua apresentação. Dados como nome e número de documentos pessoais não são divulgados, e, assim, acreditam que o anonimato está garantido, pois os dados resultantes geram um olhar anônimo. Entretanto, este conjunto de dados teoricamente anonimizados pode ser combinado com outras bases de dados, ameaçando a privacidade do indivíduo [El Emam e Dankar, 2008]. Desse modo, é de suma importância que as informações relativas à saúde sejam preservadas, e para isso, algumas questões relacionadas à privacidade devem ser consideradas: (i) Quem pode ter permissão para possuir os dados; (ii) que tipo de dados médicos, quanto e onde os dados devem ser coletados; (iii) quem pode ter permissão para inspecionar os dados médicos; e (iv) a quem os dados médicos devem ser revelados sem o consentimento do paciente [Kumar e Lee, 2011].

4.5. Processamento em Nuvem para Dados de Sensores de Assistência Médica

A computação em nuvem representa um avanço técnico importante para o desenvolvimento de aplicativos que realizam o processamento de grandes volumes de dados com alto desempenho e facilitam o gerenciamento das diferentes ferramentas no ambiente médico [Pino e Salvo, 2013]. A computação em nuvem permite que os usuários usem infraestrutura, plataformas e software fornecidos pelos provedores de nuvem sob a forma de serviços. Consequentemente, a computação em nuvem reduz a necessidade do usuário final investir em infraestrutura física de computação, o que incorre em custos de capital para a instalação (CAPEX – *CAPital EXpenditure*) e custos operacionais para a manutenção do serviço funcional (OPEX - *OPerational EXpenditure*). Assim, a computação em nuvem é amplamente apontada como a infraestrutura de computação da próxima geração. Outro ponto importante que diferencia a computação em nuvem de outras abordagens de computação paralela e distribuída, como as grades computacionais, é que os usuários utilizam elasticamente os recursos sob demanda. Como resultado, os aplicativos móveis podem ser rapidamente provisionados e liberados com o mínimo esforço de gerenciamento ou as iterações do provedor de serviços [Dinh et al., 2013].

O uso da tecnologia de computação em nuvem no ambiente de saúde tornou-se crucial para sustentar os requisitos das estruturas médicas e de saúde. Os requisitos se distinguem em dois aspectos principais dessa comunidade. O primeiro está relacionado

aos aspectos gerenciais e administrativos. O segundo está relacionado ao médico ou pesquisador que precisa da infraestrutura para processar, armazenar, gerenciar dados do paciente, realizar análises, diagnósticos e assim por diante. As estruturas modernas de saúde devem, portanto, ter arquiteturas que garantam a maior velocidade no gerenciamento de operações de TI, configuração, reconfiguração de infraestrutura, aplicativos e serviços, assim como a automação de tarefas específicas simples e repetitivas de saúde, reduzindo o número de erros e recursos, durante o uso de cada aplicativo de saúde específico.

As soluções existentes na nuvem para o ambiente de saúde envolvem diferentes aspectos. Uma categorização sobre soluções que usam a computação em nuvem no ambiente de saúde pode ser feita definindo quais os requisitos cada aplicação deve prover. As infraestruturas de computação e aplicações de saúde devem garantir a prestação de serviços que atendam a requisitos específicos [Elhoseny et al., 2017]:

- autoatendimento, em que o usuário, por exemplo, um médico, deve ser capaz de solicitar os serviços de computação, como aumento da largura de banda, poder de computação, disponibilização de aplicativos, por conta própria, sem a intervenção dos gerentes de infraestrutura;
- acessibilidade global; em que os serviços devem estar acessíveis a partir de vários dispositivos, de forma ubíqua, e garantir a privacidade e a criptografia de dados sensíveis;
- elasticidade, em que os recursos devem poder ser ajustados para cima ou para baixo rapidamente e, em alguns casos, automaticamente.

Essas são características típicas da computação em nuvem e, por isso, na área da saúde, o uso da computação em nuvem tem sido proposto como um meio para manter registros de saúde, monitorar pacientes, gerenciar doenças e cuidar de maneira mais eficiente e eficaz, ou colaborar com colegas e realizar a análise de dados. Algumas dessas propostas relacionam-se a diagnóstico de doenças e à privacidade dos dados dos pacientes. Alguns exemplos de aplicativos de assistência médica baseados na computação em nuvem são a integração de dispositivos de Internet das Coisas (IoT) e a nuvem para o monitoramento de doenças; o uso da computação em nuvem como infraestrutura de base para sistemas de suporte à decisão para rastrear o câncer e outras doenças; métodos para melhorar o autocuidado e o controle glicêmico de pacientes; métodos para melhorar o diagnóstico de doenças de pele usando redes neurais; diagnóstico de diabetes executado usando o sistema especialista no Google App Engine; antecipação do diagnóstico de doenças cardíacas usando algoritmos de aprendizado de máquina; método para proteger sistemas de saúde com base em análises de *big data*; método introduzido para manter a privacidade na exibição de imagens médicas; soluções de segurança para a assistência médica em termos de transferência de dados, armazenamento de dados e intercâmbio de dados no ambiente em nuvem.

Contudo, as soluções atuais voltadas para as aplicações de saúde apresentam vários desafios associados à automação nesse ambiente, devido à heterogeneidade de dispositivos, de protocolos e de interfaces de programação. Além disso, há a dificuldade no

requisito de implantação flexível e sem impacto de novos recursos e aplicativos. Dessa maneira, o paradigma de computação em nuvem é, também, uma interface de integração entre diferentes sistemas. A computação em nuvem é um paradigma para estruturar recursos de TI que redefine a maneira de gerenciar nossos sistemas computacionais. Os modelos dos serviços fornecidos são:

- Software como Serviço (SaaS – *Software as a Service*), o software é entregue como serviço executado na nuvem, ou seja, a interface entre o usuário e a nuvem é o próprio software entregue pelo provedor de nuvem;
- Plataforma como Serviço (PaaS – *Platform as a Service*), o provedor de nuvem fornece serviços que permitem desenvolver, testar e implantar um aplicativo ou software;
- Infraestrutura como Serviço (IaaS – *Infrastructure as a Service*), o provedor de nuvem fornece a infraestrutura de TI: processadores, armazenamento, serviços de rede. Contudo, a execução da plataforma e do software são de responsabilidade do cliente que contrata o provedor de nuvem.

Diferentes empresas desenvolvem software para criar e gerenciar a arquitetura em nuvem. Os padrões de distribuição de serviço em nuvem são providos por nuvens públicas, nuvens privadas ou nuvens híbridas. Nuvem pública se refere ao modelo de provisão de serviços em que os serviços de computação em nuvem são entregues pela Internet a partir de um provedor de serviços para diferentes clientes. Nuvem privada se refere ao modelo em que os serviços de computação em nuvem são fornecidos em uma intranet ou na Internet através de redes privadas virtuais (VPN – *Virtual Private Networks*) da empresa para suas diversas unidades. Vale destacar que, nesse modelo, a infraestrutura da nuvem fica restrita à rede privada, mesmo que passe pela Internet, pois o tráfego é criptografado e isolado. Nuvem híbrida se refere ao modelo em que os serviços são construídos em infraestrutura híbrida, que usa o modelo privado para certos aspectos, como o armazenamento de dados, e o modelo público para outros, por exemplo, as interfaces de acesso.

4.5.1. Aplicações de Computação em Nuvem na Saúde

Alguns dos principais serviços de saúde suportados pela computação em nuvem são o gerenciamento de dados, a telemedicina, os sistemas de informações gerenciais e os sistemas de apoio à decisão [Zafar et al., 2014, Elhoseny et al., 2017].

O gerenciamento de dados é um problema primordial no setor de saúde. Os dados de assistência médica contêm informações pessoais e confidenciais que podem ser atraentes para os ataques de criminosos cibernéticos, como por exemplo, os que buscam por se beneficiar financeiramente do roubo de tais dados. Nesse caso, podem vender os dados a um fornecedor terceirizado, que pode realizar uma análise de dados para identificar indivíduos não seguráveis devido ao seu histórico médico ou desordem genética. Além disso, para privacidade e integridade dos serviços de saúde, os dados devem ser protegidos não apenas contra invasores externos, mas também contra tentativas de acesso não autorizado de dentro da rede ou do ecossistema, como um funcionário do provedor

de serviços de saúde ou provedor de serviços em nuvem. Os comportamentos maliciosos podem ser intencionais ou não intencionais, e as organizações podem ser penalizadas ou responsabilizadas criminalmente por tais incidentes. As abordagens para a armazenagem segura incluem o uso de primitivas criptográficas, como as baseadas em infraestrutura de chave pública e nuvens públicas para garantir a confidencialidade e a privacidade dos dados. No entanto, isso limita a capacidade de pesquisa sobre os dados, no sentido de que os profissionais de saúde precisam descriptografar os dados potencialmente grandes antes de realizar consultas sobre os dados, resultando em aumentos de tempo e custos para a recuperação de dados e atraso no diagnóstico [Esposito et al., 2018]. Nesse sentido, a computação em nuvem desponta como uma solução escalável para o armazenamento de grandes volumes de dados e, também, escalável quanto ao processamento para realizar a criptografia e descriptografia quando necessário. Vale ainda destacar que um problema crucial em saúde diz respeito ao gerenciamento de emergências. Durante o gerenciamento de casos de emergência, o acesso imediato a partes dos dados anteriores do paciente e aos dados de atendimento pré-hospitalar permite diagnóstico e tratamento adequados, elimina o risco de erros médicos e de medicamentos e simplifica o processo de assistência médica de emergência. Koufi *et al.* descrevem uma arquitetura orientada a serviços (SOA) baseada na computação em nuvem para a implementação de um sistema eletrônico de registro de pacientes de emergência que fornece funcionalidades para gerenciar, recuperar, transformar, trocar e armazenar informações de casos de emergência e informações médicas críticas do paciente de maneira distribuída e ubíqua [Koufi et al., 2010]. Por sua vez, Oliveira *et al.* propõem um protocolo de criptografia baseada em atributos de política do texto cifrado para acessar registros médicos na nuvem. Embora o registro médico eletrônico (EMR – *Eletronic Medical Record*) deva manter a privacidade do paciente, o registro deve estar prontamente disponível para os profissionais de saúde em caso de emergência. Assim, a proposta consiste em um protocolo de criptografia baseada em atributos para fornecer acesso ao EMR criptografado do paciente durante o tratamento de emergência. A proposta garante autorização para acessar os dados do paciente apenas para o período de emergência [de Oliveira et al., 2020].

A telemedicina se apoia em tecnologias de informação e comunicação que fornecem serviços de atendimento ao paciente além dos centros médicos. As tecnologias de telemedicina, como telecirurgia, conferência de áudio e vídeo e telerradiologia, trazem um novo modelo de colaboração e comunicação entre várias partes interessadas na área da saúde. Armazenamento de bancos de dados em nuvem, registros médicos eletrônicos, aprendizado de máquina e cuidados de longo prazo são os desafios e tecnologias mais comuns para a telemedicina e o teleatendimento que podem ser suportados pela computação em nuvem [Hsu, 2017].

O setor de saúde iniciou o uso de sistemas de gerenciamento de informação (MIS – *Management Information System*) para organizar o fluxo de dados dentro e fora da empresa. Os médicos usam o sistema para fornecer melhor atendimento aos pacientes. Os pacientes o utilizam para consultar serviços, enquanto os administradores usam para gerenciar os recursos humanos, cobrança e finanças. A direção dos serviços de saúde usa o sistema para fins de tomada de decisão e previsão. O desenvolvimento desses sistemas enfrenta desafios que incluem pressões e gerenciamento de várias partes interessadas para a prestação de serviços. O uso da tecnologia de computação na nuvem tem o potencial

de reduzir custos e melhorar os resultados do serviço. A computação em nuvem promove serviços que estão disponíveis o tempo todo e de todos os locais e, assim, é um novo mecanismo de entrega de recursos de computação [Ali et al., 2018].

Um sistema de apoio à decisão clínica é um sistema especialista que emula o conhecimento e o comportamento de um especialista médico para gerar conselhos na análise do prontuário do paciente, com base em dados de saúde previamente coletados. Médicos e pacientes podem usar esses sistemas para fins de diagnóstico e medicação. A capacidade da mente humana é atualmente insuficiente para se estabelecer decisões ideais com o grande volume de dados e com a complexidade de requisitos analíticos. Além do apoio à decisão clínica, o suporte à decisão também deve ser considerado para decisões de negócio. A implementação de sistemas de suporte à decisão em organizações de saúde pode assumir diferentes níveis estratégicos, como abordar algumas perguntas sobre a dimensão operacional; ajudar passivamente na criação de relatórios para execução de procedimento; apoiar a modificação de estratégias; ou tratar os sistemas de apoio à decisão como recursos estratégicos na tomada de decisão [Sousa et al., 2019].

4.5.2. Integração entre Internet das Coisas e a Computação em Nuvem

Dispositivos de Internet das Coisas (IoT), os sensores ou objetos inteligentes, são fundamentais na estrutura de assistência médica amparada por Tecnologias Informação de Comunicação (TICs). Esses dispositivos possibilitam que os aplicativos de assistência médica utilizem dados coletados em tempo real, ou quase real, e permitem a integração com a computação em nuvem para o processamento e a geração de relatórios e resultados [Botta et al., 2016]. Cada componente cumpre uma função específica na estrutura de assistência médica da IoT. Os dados coletados são geralmente transmitidos a servidores remotos, hospedados na nuvem, para análise, e os resultados são exibidos em tempo real. Os servidores podem executar em nuvens IaaS, como máquinas virtuais dedicadas a um serviço de IoT, ou executam como serviço nas plataformas de nuvem, abordagem comum em soluções comerciais como as da Google e da Amazon.

Quando se trata da implementação de um novo sistema de assistência médica baseado em IoT e computação em nuvem, é necessário elencar todas as atividades e casos de uso associados ao sistema, pois diferentes enfermidades requerem procedimentos distintos de tratamento. Nesse sentido, dois fatores transversais são a facilidade de uso e o custo reduzido obtido por usuários e fornecedores de aplicativos e serviços. A nuvem facilita o fluxo entre a coleta de dados dos sensores e o processamento desses dados, além de permitir a rápida configuração e integração de novas funcionalidades, mantendo baixos os custos de implantação e processamento de dados. Consequentemente, análises de complexidade sem precedentes e algoritmos de tomada de decisão e previsão baseados em dados podem ser empregados com baixo custo, fornecendo meios para aumentar as receitas e reduzir os riscos. Nesse contexto, o processamento oportuno de enormes dados de sensores em fluxo contínuo, sujeito a restrições e incertezas de energia e rede, foi identificado como o principal desafio. A nuvem oferece novas oportunidades na agregação de dados dos sensores e na exploração dos agregados para maior cobertura e relevância, mas ao mesmo tempo afeta a privacidade e a segurança.

A integração do dispositivo de IoT e as aplicações que executam na nuvem reque-

rem algum software de adaptação e encaminhamento dos dados, chamados de *drivers*. A maioria dos *drivers* de interconexão entre dispositivos de IoT e a nuvem se enquadra nas categorias de comunicação, armazenamento ou computação, enquanto outros, mais básicos, têm implicações em todas essas categorias.

Aplicações de IoT em saúde se caracterizam por uma heterogeneidade muito alta de dispositivos, tecnologias e protocolos. Assim, a interoperabilidade é um requisito importante. A interoperabilidade consiste na capacidade de equipamentos e sistemas de diferentes fornecedores operarem juntos. A interoperabilidade é mandatória, já que sensores e dispositivos inteligentes, como *smartwatch* e sensores corporais, emergem como uma tecnologia de larga escala. A interoperabilidade é essencial tanto entre dispositivos inteligentes de diferentes fabricantes quanto entre os dispositivos e as diversas infraestruturas de nuvens existentes. Dispositivos inteligentes devem interoperar da camada física até a camada de aplicação ou integração. A interoperabilidade da camada física ocorre quando equipamentos de diferentes fornecedores se comunicam fisicamente entre si. Na camada física, os dispositivos inteligentes devem concordar em configurações como as frequências físicas nas quais a comunicação ocorre, que tipo de modulação os sinais físicos devem utilizar e a taxa na qual as informações são transferidas. Na camada da rede, os dispositivos devem concordar quanto ao formato das informações enviadas e recebidas pelo canal físico e como os dispositivos são endereçados, além de como as mensagens devem ser transportadas através de uma rede para a Internet das Coisas. Na camada de aplicação, os dispositivos inteligentes devem compartilhar uma visão comum sobre como os dados devem ser inseridos ou extraídos de uma rede de Internet das Coisas, bem como como os dispositivos inteligentes devem ser alcançados a partir de sistemas externos ou na nuvem [Vasseur e Dunkels, 2010].

4.6. Desafios e Tendências

4.6.1. Desafios da Interoperabilidade entre Dispositivos e Sistemas de Saúde

A disponibilidade de informações da saúde dos pacientes de forma contínua, sustentável e confiável não tem se mostrado uma tarefa trivial, principalmente devido a alguns fatores: falta de registro, registro inadequado e incompleto, falta de padronização na aplicação de vocabulário médico, mudanças constantes nas rotinas administrativas e nas diretrizes clínicas aplicadas às unidades de saúde municipais, estatuais e federais [Araujo et al., 2014].

A interoperabilidade é a capacidade de sistemas de domínios diferentes compartilharem e trocarem informações. Os sistemas de informação em saúde atuam no processamento de informações de fontes de dados bastante heterogêneas, automatizando de forma integral ou parcial, processos de agendamento, atendimento, triagem, diagnóstico e tratamento de pacientes. Os dados da saúde perpassam diversos domínios, incluindo os administrativos, clínicos e demográficos, distribuídos em diferentes sistemas de informação, elevando o grau de heterogeneidade e complexidade presente no domínio da saúde [Iroju et al., 2013].

Sistemas de informação em saúde dependem da interoperabilidade para obter e compartilhar dados. São vários os benefícios da definição de um modelo de interoperabilidade. Por exemplo, os sistemas de informação laboratoriais podem fornecer resultados

críticos de testes clínicos que podem salvar vidas se chegarem ao lugar certo em tempo hábil. Os sistemas de informação usados em farmácias podem detectar pedidos de medicamentos inapropriados ou em dosagens inapropriadas para aquele paciente, avisando profissionais e até os pacientes na identificação de um problema potencial [Frisse, 2017].

A multiplicidade dos sistemas de informação em saúde comerciais e o desejo dos sistemas de saúde de controlar e usar estrategicamente os dados do paciente são alguns dos principais impedimentos à interoperabilidade [Benson e Grieve, 2016]. Bilhões de dólares já foram investidos no desenvolvimento de modelos de interoperabilidade para que sistemas de informação em saúde consigam atender aos objetivos da interoperabilidade [Edmunds et al., 2016]. Nos EUA, a questão da interoperabilidade se tornou política de governo federal. Um exemplo é a HIMSS (*Healthcare Information and Management System Society*), organização sem fins lucrativos que ajuda no desenvolvimento de políticas públicas, no desenvolvimento de força de trabalho e na definição das melhores práticas para o ecossistema da saúde digital [Furukawa e Pollack, 2020].

Uma abordagem considera a interoperabilidade em pelo menos três níveis de complexidade. A forma mais simples e usual é a interoperabilidade de transporte simples de dados entre os sistemas. Como em qualquer comunicação, deve haver um padrão de empacotamento e transporte das informações implementado pelos sistemas de envio e recebimento. Nesse nível, o mecanismo de transporte não possui qualquer conhecimento ou entendimento do significado dos dados [Di Martino et al., 2018].

O segundo nível é a interoperabilidade estruturada. Os dados são empacotados em um ambiente pré-definido, de maneira que a identidade e a localização de cada elemento dentro da estrutura seja entendida por todos os sistemas. Isso permite que os dados sejam analisados quando recebidos e armazenados nos locais apropriados no sistema de recebimento. Um padrão para isso deve identificar os valores permitidos de cada elemento de dados para garantir que o remetente e os sistemas de recebimento estejam trocando informações válidas.

O terceiro nível é o da interoperabilidade semântica, o que requer que os dados sejam suficientemente padronizados para que seu significado fique claro para os sistemas de envio e recebimento. Um exemplo do que isso implica seria que os dados clínicos coletados de um registro eletrônico de saúde *A* possam ser usados com segurança por um sistema de apoio à decisão *B* depois de receber esses dados [del Carmen Legaz-García et al., 2016].

Atualmente, as interoperabilidades de transporte e estruturada são amplamente utilizadas. Para a interoperabilidade semântica, há especificações de domínio público disponibilizadas por renomadas instituições que se propõem ser utilizadas como padrão de interoperabilidade. Contudo, na prática, poucas encontram-se efetivamente implementadas, mais por questões políticas do que tecnológicas [Benson e Grieve, 2016]. A Política Nacional de Informação e Informática em Saúde (PNIIS) cita, entre as diretrizes relacionadas a estratégia de saúde digital para o Brasil, a necessidade do estabelecimento de um padrão que permita a construção do Registro Eletrônico de Saúde (RES) do cidadão por meio da identificação unívoca de usuários e protocolos de interoperabilidade eletrônica e/ou digital entre os equipamentos e sistemas.

O OpenEHR é uma comunidade virtual internacional que atua na elaboração e governança de especificações que permitam aos sistemas de informação em saúde apresentar interoperabilidade com segurança. O OpenEHR também fornece uma série de ferramentas de autoria para serem usadas por médicos e especialistas do domínio na descrição de conceitos aplicados a área de saúde. A abordagem do OpenEHR ocorre em dois níveis, onde os modelos de domínio e o modelo de referência são elaborados por perfis de profissionais distintos. O modelo de referência é desenvolvido por profissionais de tecnologia da informação e comunicação, seguindo uma estrutura lógica do Registro Eletrônico de Saúde (RES). O modelo de domínio é especificado por especialistas do domínio, médicos, enfermeiros, farmacêuticos, nutricionistas e demais profissionais da saúde, que elaboram a descrição da informação clínica, seguindo a estrutura lógica descrita no modelo de referência, denominando esse artefato como arquétipo. O OpenEHR disponibiliza uma biblioteca de cerca de 500 arquétipos e 6500 elementos de dados, denominada CKM (*Clinical Knowledge Manager*), facilitando o conhecimento clínico e eliminando a demanda de modelagem de um mesmo elemento mais de uma vez. Um ponto de dificuldade é que o OpenEHR se baseia em uma modelo de governança centralizado. Antes de ser utilizado pelo sistema de informação em saúde, o arquétipo precisa do aceite de toda a comunidade que governa o CKM, o que torna o processo de implantação de novos arquétipos moroso e bastante custoso [Iroju et al., 2013]. Ainda assim, a Portaria do SUS n^o. 2073 de 31 de agosto de 2011 cita o OpenEHR como modelo de referência para os dados de saúde do Ministério da Saúde. Contudo, poucos resultados práticos são encontrados no Brasil.

O HL7 é outro padrão de interoperabilidade de dados em saúde. Ele fornece uma estrutura e padrões relacionados para o intercâmbio, integração, compartilhamento e recuperação de informações eletrônicas de saúde. Esses padrões definem como as informação são empacotadas e comunicadas de uma parte para outra, definindo a estrutura e os tipos de dados necessários para uma integração entre sistemas. Além disso, os padrões HL7 suportam diretrizes clínicas, e a avaliação de serviços de saúde. As versões mais usadas do HL7 são a versão 2 e a versão 3. A versão 2 é mais utilizada no intercâmbio de resultados dos testes laboratoriais, com um foco maior na interoperabilidade estrutural, aplicando a tecnologia EDI/X12, já considerada antiga. A versão 3 usa XML, o que torna as mensagens HL7 mais legíveis [Weber-Jahnke et al., 2012]. Inspirado no OpenEHR descrito anteriormente, o HL7 agrupa as definições em duas categorias de referência. A primeira é denominada modelo de informação de referência, ou RIM (*Reference Information Model*), onde são definidos padrões de tipos primários usados nos sistemas de informação em saúde, bem como a arquitetura de documentação clínica, perfis de gerenciamento de registros eletrônicos de saúde, e a representação do conhecimento clínico, o que facilita o desenvolvimento de sistemas de apoio à decisão. Da mesma forma que o OpenEHR, o HL7 conta com um modelo de governança centralizado, ou seja, as decisões quanto a definição de uma nova informação clínica são tomadas por 100% do consenso da comunidade participante da definição, antes da sua liberação para o uso.

Uma arquitetura centralizada e compartilhada está sempre suscetível a influências políticas e governamentais e, portanto, o seu nível de confiança é baixo. Um modelo de interoperabilidade de informações de saúde em ambiente federado ajuda bastante a resolver essas preocupações. Em um ambiente federado, os dados originais permanecem na fonte. Os participantes devem, então, converter seus dados em algum formato padrão de

resposta, ou devem mapear suas informações em um modelo de dados padrão geralmente armazenado em um servidor separado, que serve para manipular consultas e respostas. O exemplo mais bem sucedido atualmente é o OHDSI (*Observational Health Data Sciences and Informatics*), e seu modelo de dados OMOP (*Observational Medical Outcomes Partnership*). OHDSI foi criado para permitir a vigilância ativa da segurança de medicamentos com apoio do governo e da indústria farmacêutica, usando dados observacionais coletados durante o atendimento ao paciente [Park, 2017].

Em 2011, Grahame Grieve propôs uma nova abordagem de interoperabilidade chamada Recursos para Saúde (RFH - *Resources for Health*). Essa iniciativa, mais tarde, foi denominada FHIR (*Fast Healthcare Information Resources*). O FHIR introduz o conceito de modelo de dados simplificado para cuidados de saúde. Esse modelo consiste em recursos de conteúdo intencionalmente limitados, acordados por 80% ou mais dos participantes do esforço de definição, priorizando a usabilidade e algumas diretrizes operacionais, com segurança e consistência da informação. O FHIR usa uma arquitetura orientada a serviços web, com funções de busca de recursos e de CRUD (acrônimo para Criar, Ler, Atualizar e Excluir) dos registros clínicos de saúde. As especificações do FHIR abrangem uma lista de 13 módulos: 1. infraestrutura básica de definição, 2. suporte ao desenvolvedor, 3. segurança e privacidade, 4. conformidade, 5. terminologia, 6. RDF e ontologias, 7. administração, 8. conteúdo clínico, 9. medicamento, 10. diagnóstico, 11. fluxo de trabalho, 12. financeiro, 13. raciocínio clínico. Os módulos somam mais de 150 recursos para saúde [Braunstein, 2018].

4.6.2. Desafios do Processamento em Fluxo

As aplicações médicas geram um volume massivo de dados heterogêneos provenientes de textos clínicos, imagens biomédicas, registros médicos eletrônicos, dados genéticos, sinais biomédicos e redes sociais. O processamento de dados em fluxo permite que esses dados sejam coletados, integrados, analisados e visualizados em tempo real, isto é, enquanto os dados estão sendo produzidos por sensores. O objetivo das soluções de processamento em tempo real dos dados é permitir o processamento de fluxos de dados contínuos e não limitados, integrados a partir de fontes *online* e históricas, de forma rápida e escalável. Assim, as soluções de processamento de dados em fluxo são projetadas para dar suporte à análise de grandes volumes de dados em tempo real mantendo elevada escalabilidade, disponibilidade e tolerância a falhas. Nas aplicações médicas, existe uma necessidade cada vez maior de obter informações em tempo real, a partir da análise de um volume de dados massivo a fim de aumentar a qualidade dos resultados produzidos.

Os desafios existentes no processamento de dados em fluxo se relacionam a diversos aspectos da análise de dados. Primeiramente, os desafios se relacionam com os três principais V's da análise de grandes volumes de dados, a volatilidade, a velocidade e volume [Krempl et al., 2014]. O volume e a velocidade exigem que um grande volume de dados seja processado em um intervalo de tempo limitado. A volatilidade tem relação com o tempo de validade de um determinado dado. Devido à dinâmica do ambiente, os padrões podem mudar constantemente, de forma que dados antigos podem ter pouca utilidade. A volatilidade pode afetar os modelos de análise, modificando o alvo, as características disponíveis e provocando desvios de conceito [Medeiros et al., 2019]. O desvio de conceito nada mais é do que a mudança na distribuição condicional da saída,

dado o vetor de características de entrada, que pode ter sua distribuição inalterada. Para lidar com a velocidade e o volume, é necessário desenvolver abordagens que analisam os dados de forma incremental à medida que eles chegam. Também existem desafios que se relacionam às diversas etapas da análise de grandes volumes de dados [Cortés et al., 2015] e outros que são impostos tanto pelas características do cenário de aplicação como pelas características inerentes ao tipo de dado coletado em aplicações de sensoriamento em saúde.

Os dados obtidos de sensores em aplicações de saúde se caracterizam pela alta dimensionalidade, irregularidades, informações faltantes, esparsidade, ruído e enviesamento, dificultando a análise dos dados [Lee et al., 2017]. A elevada dimensionalidade é proveniente da existência de inúmeras características (*features*) nos dados coletados por múltiplas fontes. A elevada dimensionalidade é desafiadora porque introduz mais parâmetros no modelo, aumentando sua complexidade. A irregularidade é causada pelo fato de os dados serem capturados com um padrão de tempo irregular, seja porque os sensores não funcionam de forma contínua, seja porque ocorre falha na transmissão dos dados. Dados faltantes e esparsos são recorrentes no cenário da saúde e isso pode ser causado tanto pela coleta de dados insuficiente como por falta de documentação. No caso da coleta insuficiente, o sistema que monitora o paciente não verifica uma determinada característica, provocando a falta da informação nos dados. Já no problema da documentação, apesar de o sistema de monitoramento verificar todas as características necessárias, o valor obtido não é armazenado, seja devido a um erro humano ou de transmissão. Uma consequência imediata da falta de dados e da irregularidade é a obtenção de um conjunto de dados esparso. Esses dados podem, ainda, ser ruidosos devido a diversas razões, como codificação imprecisa ou uma convenção de nomes inconsistente. O enviesamento dos dados ocorre quando o registro armazenado depende do julgamento do médico em relação ao paciente. Pode ocorrer enviesamento também porque, em geral, são coletados mais dados sobre pacientes doentes do que sobre pacientes sãos. Ademais, os dados analisados são sensíveis, uma vez que são coletados de dispositivos pessoais e envolvem informações sobre o estado de saúde do indivíduo. Dessa forma, acrescentam-se ainda desafios de privacidade e confidencialidade.

Durante a aquisição e a exploração dos dados, deve-se coletar e filtrar um fluxo de dados de entrada massivo gerado por inúmeras fontes heterogêneas, com uma determinada frequência definida pela aplicação. Um desafio crítico nesse momento é a filtragem em tempo real para descartar dados redundantes sem a perda de informação útil. Os filtros podem ser definidos diretamente na fonte, ou em uma camada superior da arquitetura de processamento. Outro desafio dessa etapa é suportar um número variável de fontes conectadas simultaneamente, de forma a evitar picos que sobrecarreguem o sistema. Antes de alimentarem modelos, os dados devem ser pré-processados. Diversas etapas fazem parte dessa fase da análise de dados. Em sistemas de processamento em tempo real, o pré-processamento dos dados deve ser implementado de forma automatizada, com modelos que sejam capazes de otimizar seus próprios parâmetros e de operar de forma autônoma. Os modelos devem se autoatualizar e devem estar sincronizados com os modelos preditivos utilizados nas outras etapas, uma vez que a representação dos dados pode mudar, inutilizando o modelo preditivo anterior [Krempl et al., 2014]. Normalmente, assume-se que as informações atuais são completas e estão disponíveis imediatamente para o sis-

tema. Essas considerações, contudo, podem não ser verdadeiras em aplicações de saúde que utilizam sensores para monitorar os pacientes. Os dados obtidos não são completos, uma vez que os valores verdadeiros de todas as variáveis não são eventualmente conhecidos pelo algoritmo usado, e não estão disponíveis de forma imediata, já que o resultado da avaliação atual não está disponível para realimentar o modelo e melhorar a avaliação imediatamente subsequente. O resultado está disponível apenas para avaliações muito posteriores, podendo perder o significado até lá.

Em uma das etapas do pré-processamento, a limpeza dos dados, o sistema deve lidar com a incerteza e o erro nos dados. As principais causas desses problemas são o tempo de vida da bateria dos sensores usados no sistema, a imprecisão desses mesmos sensores e falhas na transmissão dos dados coletados [Cortés et al., 2015]. Esses problemas são especialmente desafiadores no processamento em fluxo devido à natureza igualmente desafiadora dos dados, que são continuamente recebidos. Dessa forma, não se sabe com antecedência qual informação os dados futuros trarão, impossibilitando a enumeração determinística de possíveis ações a serem tomadas. Deve-se sempre considerar as propriedades espaço-temporais dos dados [Chen et al., 2015]. Ressalta-se que os desafios inerentes ao caráter desafiador dos próprios dados estão presentes em todas as etapas do pré-processamento e da análise dos dados. Na etapa que geralmente prossegue a limpeza, por exemplo, busca-se uma representação comum para os dados a fim de habilitar a agregação de fluxos heterogêneos. Além disso, é possível que diversos fluxos de diversos sensores, ou mesmo diversos pacientes, tenham que ser agregados para formar as respectivas visões globais sobre o paciente ou sobre uma doença, por exemplo. Os fluxos, sejam eles de sensores do mesmo indivíduo, ou de indivíduos diferentes, surgem em momentos diferentes no tempo e devem ser relacionados de alguma forma. A agregação desses fluxos deve levar em consideração como lidar com a diferença de velocidade entre os fluxos individuais, ou qual informação de cada fluxo deve ser armazenada [Krempl et al., 2014]. A dinamicidade e a incerteza sobre os dados devem ser levadas em consideração na criação de modelos analíticos. Isso pode ser feito através de abordagens que usam processos estocásticos na modelagem [Wang et al., 2015].

Os sistemas de processamento em tempo real devem se preocupar, ainda, com a privacidade e a confidencialidade dos dados [Cortés et al., 2015]. Tipicamente, a presença de informações que violam a privacidade e a confidencialidade é evitada através de uma distorção controlada dos dados sensíveis, modificando valores ou adicionando ruído. A garantia de privacidade e confidencialidade em sistemas de processamento em fluxo é desafiadora, porque os modelos não têm acesso aos dados completos, uma vez que chegam continuamente. Assim, o modelo de preservação de privacidade e confidencialidade nunca é o modelo final, sendo difícil julgar a eficiência da preservação sem ter acesso aos dados completos. O desvio de conceito [Medeiros et al., 2019] potencial em cenários de processamento em tempo real também afeta os modelos de privacidade, uma vez que em um determinado momento o modelo usado pode preservar a privacidade e a confidencialidade, mas se houver um desvio de conceito é possível que o mesmo modelo não seja mais aplicável. Dessa forma, é necessário o desenvolvimento de mecanismos de preservação de privacidade e confidencialidade adaptativos.

Os sistemas de processamento em fluxo precisam lidar com esses desafios, além de manter a ordenação dos dados, a consistência e habilitar o acesso rápido aos dados.

Ainda, é necessário decidir a durabilidade dos dados, isto é, por quanto tempo esses dados devem permanecer armazenados após serem processados. A escalabilidade e a tolerância a falhas também devem ser garantidas. Assim, o processamento em fluxo em tempo real do grande volume de dados gerado não pode ser implementado usando soluções tradicionais de processamento, porque elas não escalam para esse tipo de abordagem. Essas soluções costumam ser centralizadas. O requisito temporal imposto pela necessidade do processamento online requer a implementação de sistemas distribuídos capazes de agregar a visão local dos dados em cada nó de processamento em uma visão global dos resultados com uma latência mínima de comunicação entre os nós. Devido a essa necessidade, ferramentas como *Apache Spark Streaming*, *Apache Storm* e *Apache Kafka* [Medeiros et al., 2019] estão se popularizando no cenário da saúde. Essas ferramentas permitem o processamento distribuído de dados em fluxo. O *Apache Kafka* suporta uma grande variedade de cenários, com elevada vazão e confiabilidade. O *Apache Storm* é útil para processar dados com alta velocidade. O *Apache Spark Streaming* permite o processamento de dados em memória e inclui APIs para execução eficiente do processamento e permitir uso de SQL (*Structured Query Language*) para acessar os dados. No *Apache Storm*, cada nó é responsável por receber os dados e atualizar o estado interno. Esse modelo de funcionamento cria diversos desafios no ambiente da nuvem em termos de tolerância a falhas, consistência e fusão com o processamento em lotes. O *Apache Spark Streaming* implementa fluxos discretizados, chamados *D-Streams*, que facilitam a fusão com o processamento em lotes.

4.6.3. Projetos de pesquisa

Diversos projetos vêm sendo desenvolvidos para prover assistência e cuidados médicos através do monitoramento remoto. Isso é consequência da integração entre a tecnologia da informação e comunicação e as aplicações médicas. O monitoramento remoto dos pacientes pode ser feito com diversos objetivos, como prevenção de doenças e reabilitação, conforto e segurança, e o monitoramento de doenças crônicas. Este minicurso apresenta projetos europeus[15] que podem ser classificados nesses grupos. Existem ainda projetos que se preocupam com o desenvolvimento de dispositivos biomédicos para monitoramento, como o projeto FABIMED[16].

Prevenção de doenças e reabilitação

O projeto **RedStroke**[17] desenvolve uma solução inteligente, precisa e econômica para a triagem de fibrilação atrial (FA), com o objetivo de prevenir o Acidente Vascular Cerebral (AVC). Os pacientes monitorados que apresentam suspeita de FA são encaminhados para um cardiologista para confirmação do diagnóstico e início do tratamento. A aplicação desenvolvida no contexto do projeto monitora a frequência cardíaca do paciente através unicamente da câmera do celular. Os pacientes devem realizar medições regulares para formar um histórico de medidas, a partir do qual são realizadas análises pelo aplicativo para detectar a fibrilação atrial. A detecção é feita através da presença de batimentos

[15]Projetos financiados por um dos seguintes programas: Horizon 2020, EU Structural Funds e AAL Europe Programme

[16]Disponível em `http://www.fabimed.eu/`, último acesso em 09/05/2020

[17]Duração de 2018 a 2020. Disponível em `https://en.preventicus.com/en/briefly-explained/`, último acesso em 09/05/2020.

extras ou de arritmia.

Outros projetos focam na reabilitação de pacientes que sofrem com doenças crônicas. O projeto **ReHub**[18], por exemplo, usa sensores biomecânicos para monitorar pacientes de distúrbios musculoesqueléticos crônicos. Com base nas medições dos sensores sobre a força muscular e o movimento das articulações, os fisioterapeutas podem criar programas de reabilitação mais objetivos e monitorar o progresso dos pacientes remotamente.

Conforto e segurança

O projeto **selfBACK**[19] foca no suporte a pacientes que sofrem com dores na coluna. O paciente utiliza apenas o celular e uma pulseira inteligente (*smart wristband*) que possui um acelerômetro para coletar dados usados para reconhecimento de atividades. A aplicação também conta com um questionário que ajuda a criar o perfil do paciente. As informações disponíveis são usadas para treinar um sistema preditivo que fornece recomendações personalizadas para auxiliar o paciente a gerenciar sua própria dor.

Os projetos SMART-BEAR[20], WorkingAge[21], Bionic[22], e Dem@Care[23] focam no uso de sensores heterogêneos para monitorar o paciente e o ambiente no qual está imerso, visando melhorar a vida cotidiana dos pacientes. O projeto **SMART-BEAR** foca nos idosos e usa os dados coletados para oferecer recomendações personalizadas para promover a saúde do idoso e sua independência. A plataforma a ser desenvolvida também deve se conectar aos hospitais e outros sistemas de saúde para obter dados do paciente, como seu registro médico, para auxiliar o sistema de tomada de decisão.

Já o projeto **WorkingAge** tem como foco o monitoramento do estado emocional e cognitivo da força de trabalho para identificar ações apropriadas que melhorem o estilo de vida e o trabalho do indivíduo, promovendo interações mais eficientes e a organização no ambiente de trabalho, além de hábitos mais saudáveis.

O projeto **Bionic** foca no envelhecimento saudável da força de trabalho. O projeto tem como objetivo o desenvolvimento de uma plataforma que analisa os dados de movimento. Os resultados da análise permitem o desenvolvimento de estratégias para promover a adaptação do local de trabalho para as necessidades e níveis de condicionamento físico da força de trabalho em envelhecimento.

Por fim, o projeto **Dem@Care** tem como foco os pacientes com demência. A partir da análise de dados coletados por sensores vestíveis e locais, o perfil do paciente

[18]Duração de 2018 a 2020. Disponível em `https://www.dycare.com/rehub/`, último acesso em 09/05/2020.

[19]Duração de 2016 a 2020. Disponível em `https://www.selfback.eu/about-the-project.html`, último acesso em 09/05/2020.

[20]Duração de 2019 a 2023. Disponível em `https://www.smart-bear.eu/`, último acesso em 09/05/2020.

[21]Duração de 2019 a 2022. Disponível em `https://www.workingage.eu/project/`, último acesso em 09/05/2020.

[22]Duração de 2019 a 2021. Disponível em `https://bionic-h2020.eu/about/`, último acesso em 09/05/2020.

[23]Duração de 2011 a 2015. Disponível em `http://www.demcare.eu/`, último acesso em 09/05/2020.

é criado levando em consideração o contexto, a fim de garantir cuidados reativos e proativos, além de *feedback* personalizado. Os dados podem ser acessados por médicos e cuidadores para avaliar o progresso do paciente e a efetividade da medicação, e recomendar tratamento preventivo e ajuste do tratamento.

Monitoramento de doenças crônicas

O projeto **SERAS**[24] monitora pacientes que sofrem de epilepsia. O monitoramento é feito através de um dispositivo vestível a fim de prever convulsões epilépticas antes que elas ocorram. O dispositivo é como um aparelho auditivo que monitora os sinais cerebrais gerando um eletroencefalograma. O eletroencefalograma é armazenado em uma aplicação que executa no celular. A aplicação se conecta com a nuvem, onde um algoritmo de inteligência artificial analisa os dados armazenados para alertar o usuário e os serviços médicos um minuto antes de a convulsão acontecer.

O projeto **BigO**[25] tem como foco o monitoramento da obesidade infantil. A ideia é medir de forma objetiva comportamentos obesogênicos de crianças e adolescentes, levando em consideração o ambiente local. Para tanto, utilizam-se informações fornecidas pelos pacientes ou seus responsáveis e dados obtidos de sensores do celular e de relógios inteligentes (*smartwatches*). O cruzamento das informações permite que a aplicação forneça modelos com a matriz de dependência de prevalência da obesidade. Com isso, é possível predizer a efetividade de políticas específicas para a comunidade e o monitoramento em tempo real da resposta da população.

Os projetos **myAirCoach**[26] e **HEARTEN**[27] focam no monitoramento de pacientes asmáticos e cardíacos, respectivamente. No projeto **myAirCoach**, o objetivo é auxiliar o paciente a gerenciar a própria doença através de ferramentas que aumentam a sua consciência sobre o seu estado clínico e sua aderência ao tratamento, bem como sobre a efetividade desse tratamento. Para tanto, os pacientes usam um inalador com sensor embarcado que envia informações para o celular do paciente. Além disso, diversos fatores fisiológicos, comportamentais e ambientais são monitorados pelos sensores do myAirCoach. A análise de todas essas informações permite a disponibilização de uma imagem geral das condições do paciente. Os profissionais de saúde podem usar as informações obtidas pela aplicação para supervisionar os pacientes e ajustar o tratamento. Além disso, as informações podem ser usadas para auxiliar no entendimento dos mecanismos que atuam na progressão da doença.

Já o projeto **HEARTEN** não somente monitora os pacientes como também desenvolve os sensores usados para o monitoramento. Os sensores desenvolvidos detectam e quantificam biomarcadores de insuficiência cardíaca presentes na respiração e na saliva. A partir da análise desses biomarcadores, é possível identificar as condições de saúde do

[24]Duração de 2019 a 2021. Disponível em `https://d-lab.tech/mjn/`, último acesso em 09/05/2018.

[25]Duração de 2016 a 2020. Disponível em `https://bigoprogram.eu/big-data-against-childhood-obesity/`, último acesso em 09/05/2018.

[26]Duração de 2015 a 2018. Disponível em `http://www.myaircoach.eu/content/what-myaircoach-project`, último acesso em 09/05/2018.

[27]Duração de 2015 a 2018. Disponível em `http://www.hearten.eu/` último acesso em 09/05/2018.

paciente e identificar se o paciente está aderindo ao tratamento. O sensor biomédico de respiração é integrado ao celular do paciente, enquanto o de saliva é integrado a um copo do paciente. Sensores adicionais são usados para monitorar eletrocardiograma, a pressão sanguínea e a atividade física do paciente. Os dados são complementados com informações nutricionais, ganho de peso, perfil do paciente e outras informações fornecidas pelos cuidadores e pelos profissionais de saúde. Com isso, a aplicação fornece alertas, orientações, tendências e predições sobre a saúde do paciente, a fim de melhorar a aderência do paciente ao tratamento e permitir a antecipação de incidentes.

4.7. Considerações Finais

As redes de sensores para dados de saúde podem ter diferentes arquiteturas, utilizar diferentes tecnologias de hardware e diferentes tecnologias de transmissão de dados. A possibilidade de aplicações é muito vasta e, cada vez mais, está se popularizando no meio médico. A popularização dos *smartphones* e *smart devices*, assim como das redes móveis, mudou a forma como a sociedade lida e aceita os sensores médicos. Mais do que isso, sensores pensados com finalidades distintas, como acelerômetros, câmeras, microfones, entre outros, passaram a servir como fonte de dados para avaliar a condição de saúde dos indivíduos. Assim, a associação das redes de sensores, sejam elas de pequeno, médio ou grande porte, com a telemedicina está causando uma revolução na assistência básica em saúde em nível mundial.

Este capítulo apresentou os conceitos básicos sobre redes de sensores e suas principais aplicações na saúde. Além disso, discutiu temas desafiadores, como a segurança, a gerência, a interoperabilidade, o armazenamento em nuvens e o processamento de dados em fluxo, os quais, se não forem bem definidos, levarão ao fracasso da aplicação da rede de sensores.

Foram apresentados, também, alguns dos principais projetos de grande porte para a criação de aplicações de monitoramento de saúde baseado em sensores sem fio. Observa-se que existem diversas iniciativas na Europa, usualmente, focadas no monitoramento de casos de doenças graves. Apesar disso, cabe observar que a maioria dos aplicativos existentes e amplamente utilizados foca na monitoração da saúde de pessoas enquanto ainda estão saudáveis, pelo acompanhamento de peso, batimento cardíaco, fluxo respiratório, qualidade do sono, quantidade de exercícios realizados, entre diversos outros. É fato que, hoje em dia, existe uma verdadeira coleção de dados que são coletados de forma transparente ao usuário, mas que podem dizer muitas informações sobre a sua saúde. A evolução dos algoritmos de processamento de dados baseados em aprendizado de máquina e compartilhamento de informações tornará mais viável o amplo uso dessas informações para detecção prematura de problemas em larga escala.

No contexto das pandemias, toda forma para coleta e disponibilização segura de dados para profissionais de saúde é de grande interesse e relevância. De fato, a possibilidade de monitorar pacientes sem que esses saiam de suas residências, ou ainda, monitorar pacientes em hospitais que são portadores de doenças altamente contagiosas é um fator que revoluciona a forma como a sociedade atual lida com as doenças, melhorando a qualidade de vida do paciente e reduzindo os riscos de contaminação para as equipes médicas. Por essas razões, as redes de sensores sem fio para aplicações médicas são hoje tema de

pesquisa para curto, médio e longo prazo, com impactos estratégicos na gestão de saúde da população.

Referências

[Aileni, 2015] Aileni, R. M. (2015). Mobile application for tracking data from humidity and temperature wearable sensors. *2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*.

[Al Ameen et al., 2012] Al Ameen, M., Liu, J. e Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems*, 36:93 – 101.

[Al-Janabi et al., 2017] Al-Janabi, S., Al-Shourbaji, I., Shojafar, M. e Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal*, 18(2):113 – 122.

[Alemdar e Ersoy, 2010] Alemdar, H. e Ersoy, C. (2010). Wireless sensor networks for healthcare: A survey. *Computer networks*, 54(15):2688–2710.

[Ali et al., 2018] Ali, O., Shrestha, A., Soar, J. e Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, 43:146–158.

[Altuwaiyan et al., 2018] Altuwaiyan, T., Hadian, M. e Liang, X. (2018). EPIC: Efficient privacy-preserving contact tracing for infection detection. *2018 IEEE International Conference on Communications (ICC)*.

[Araujo et al., 2014] Araujo, T. V., Pires, S. R. e Bandiera-Paiva, P. (2014). Adoção de padrões para registro eletrônico em saúde no brasil. *Revista Eletrônica de Comunicação, Informação e Inovação em Saúde*, 8(4).

[Badidi e Moumane, 2019] Badidi, E. e Moumane, K. (2019). Enhancing the processing of healthcare data streams using fog computing. *2019 IEEE Symposium on Computers and Communications (ISCC)*.

[Bangash et al., 2017] Bangash, Y. A., Abid, Q. u. D., Alshreef, A. A. e Al-Salhi, Y. E. A. (2017). Security issues and challenges in wireless sensor networks: A survey. *IAENG International Journal of Computer Science*, 44(2):94 – 108.

[Benson e Grieve, 2016] Benson, T. e Grieve, G. (2016). Why interoperability is hard. Em *Principles of Health Interoperability*, p. 19–35. Springer.

[Bhangwar et al., 2017] Bhangwar, A. R., Kumar, P., Ahmed, A. e Channa, M. I. (2017). Trust and thermal aware routing protocol (TTRP) for wireless body area networks. *Wireless Personal Communications*, 97(1):349–364.

[Botta et al., 2016] Botta, A., de Donato, W., Persico, V. e Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems*, 56:684 – 700.

[Brasil., 2018] Brasil. (2018). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Acessado em 12 fev 2020.

[Braunstein, 2018] Braunstein, M. L. (2018). Healthcare in the age of interoperability: The promise of fast healthcare interoperability resources. *IEEE Pulse*, 9(6):24–27.

[Cabra et al., 2017] Cabra, J., Castro, D., Colorado, J., Mendez, D. e Trujillo, L. (2017). An IoT approach for wireless sensor networks applied to e-health environmental monitoring. Em *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, p. 578–583.

[Callejon et al., 2013] Callejon, M. A., Naranjo-Hernandez, D., Reina-Tosina, J. e Roa, L. M. (2013). A comprehensive study into intrabody communication measurements. *IEEE Transactions on Instrumentation and Measurement*, 62(9):2446–2455.

[Cao et al., 2009] Cao, H., Leung, V., Chow, C. e Chan, H. (2009). Enabling technologies for wireless body area networks: A survey and outlook. *IEEE Communications Magazine*, 47(12):84–93.

[Cavallari et al., 2014] Cavallari, R., Martelli, F., Rosini, R., Buratti, C. e Verdone, R. (2014). A survey on wireless body area networks: Technologies and design challenges. *IEEE Communications Surveys & Tutorials*, 16(3):1635–1657.

[Chatterjee et al., 2014] Chatterjee, S., Das, A. K. e Sing, J. K. (2014). A novel and efficient user access control scheme for wireless body area sensor networks. *Journal of King Saud University - Computer and Information Sciences*, 26(2):181 – 201.

[Chen et al., 2015] Chen, P., Yang, S. e McCann, J. A. (2015). Distributed real-time anomaly detection in networked industrial sensing systems. *IEEE Transactions on Industrial Electronics*, 62(6):3832–3842.

[Cortés et al., 2015] Cortés, R., Bonnaire, X., Marin, O. e Sens, P. (2015). Stream processing of healthcare sensor data: Studying user traces to identify challenges from a big data perspective. *Procedia Computer Science*, 52:1004 – 1009. The 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015).

[D. Ovalle e Montoya, 2010] D. Ovalle, D. R. e Montoya, A. (2010). Artificial intelligence for wireless sensor networks enhancement. *Smart Wireless Sensor Networks InTech*.

[de Oliveira et al., 2020] de Oliveira, M. T., Bakas, A., Frimpong, E., Groot, A. E. D., Marquering, H. A., Michalas, A. e Olabarriaga, S. D. (2020). A break-glass protocol based on ciphertext-policy attribute-based encryption to access medical records in the cloud. *Annals of Telecommunications*, 75(3):103–119.

[de Oliveira et al., 2019] de Oliveira, M. T., Reis, L. H. A., Carrano, R. C., Seixas, F. L., Saade, D. C. M., Albuquerque, C. V., Fernandes, N. C., Olabarriaga, S. D., Medeiros,

D. S. V. e Mattos, D. M. F. (2019). Towards a blockchain-based secure electronic medical record for healthcare applications. Em *Proceedings of the International Conference on Communications (ICC)*, p. 1–6.

[del Carmen Legaz-García et al., 2016] del Carmen Legaz-García, M., Martínez-Costa, C., Menárguez-Tortosa, M. e Fernández-Breis, J. T. (2016). A semantic web based framework for the interoperability and exploitation of clinical models and ehr data. *Knowledge-Based Systems*, 105:175–189.

[Demirors et al., 2016] Demirors, E., Alba, G., Santagati, G. E. e Melodia, T. (2016). High data rate ultrasonic communications for wireless intra-body networks. Em *2016 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, p. 1–6. IEEE.

[Dhillon et al., 2018] Dhillon, A., Majumdar, S., St-Hilaire, M. e El-Haraki, A. (2018). MCEP: A mobile device based complex event processing system for remote healthcare. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, p. 203–210.

[Di Martino et al., 2018] Di Martino, B., Rak, M., Ficco, M., Esposito, A., Maisto, S. A. e Nacchia, S. (2018). Internet of things reference architectures, security and interoperability: A survey. *Internet of Things*, 1:99–112.

[Dinh et al., 2013] Dinh, H. T., Lee, C., Niyato, D. e Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless Communications and Mobile Computing*, 13(18):1587–1611.

[Edmunds et al., 2016] Edmunds, M., Peddicord, D. e Frisse, M. E. (2016). Ten reasons why interoperability is difficult. Em *Healthcare Information Management Systems*, p. 127–137. Springer.

[El Emam e Dankar, 2008] El Emam, K. e Dankar, F. K. (2008). Protecting Privacy Using k-Anonymity. *Journal of the American Medical Informatics Association*, 15(5):627–637.

[Elhoseny et al., 2017] Elhoseny, M., Salama, A. S., Abdelaziz, A. e Riad, A. (2017). Intelligent systems based on loud computing for healthcare services: a survey. *International Journal of Computational Intelligence*, 6(2/3):157–188.

[English et al., 2017] English, P. B., Olmedo, L., Bejarano, E., Lugo, H., Murillo, E., Seto, E., Wong, M., King, G., Wilkie, A., Meltzer, D., Carvlin, G., Jerrett, M. e Northcross, A. (2017). The imperial county community air monitoring network: A model for community-based environmental monitoring for public health action. *Environmental Health Perspectives*, 125(7):074501.

[Esposito et al., 2018] Esposito, C., De Santis, A., Tortora, G., Chang, H. e Choo, K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing*, 5(1):31–37.

[Fernandes et al., 2006] Fernandes, N. C., Moreira, M. D. D., Velloso, P. B., Costa, L. H. M. K. e Duarte, O. C. M. B. (2006). Ataques e mecanismos de segurança em redes ad hoc. *Minicursos do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG 2006)*, p. 49—-102.

[Ferreira et al., 2018] Ferreira, V., Caballero, E., Lima, R., Balbi, H., Seixas, F., Albuquerque, C. d. e Muchaluat-Saade, D. (2018). Redes corporais sem fio e suas aplicações em saúde. *Livro da 37a. Jornada de Atualizaç ao em Informática*, 1(1):1–53.

[Frisse, 2017] Frisse, M. E. (2017). Interoperability. Em *key advances in clinical informatics*, p. 69–77. Elsevier.

[Furukawa e Pollack, 2020] Furukawa, M. e Pollack, E. (2020). Achieving HIMSS Stage 7 designation for EMR adoption. *Nursing Management*, 51(1):10–12.

[G. Fortino, 2015] G. Fortino, R. G. (2015). Fall-MobileGuard: A smart real-time fall detection system. *Proc. 10th EAI Int'l. Conf. Body Area Networks*, p. 44–50.

[Gama e Gaber, 2007] Gama, J. e Gaber, M. M. (2007). *Learning from data streams: processing techniques in sensor networks*. Springer.

[Haddad e Khalighi, 2019] Haddad, O. e Khalighi, M. A. (2019). Enabling communication technologies for medical wireless body-area networks. Em *2019 Global LIFI Congress (GLC)*, p. 1–5. IEEE.

[HIMSS, 2010] HIMSS (2010). *HIMSS dictionary of healthcare information technology terms, acronyms and organizations*, chapter Appendix A - Acronym List. Healthcare Information and Management Systems Society, Chicago.

[Hsu, 2017] Hsu, W.-Y. (2017). Clustering-based compression connected to cloud databases in telemedicine and long-term care applications. *Telematics and Informatics*, 34(1):299 – 310.

[Iroju et al., 2013] Iroju, O., Soriyan, A., Gambo, I. e Olaleke, J. (2013). Interoperability in healthcare: benefits, challenges and resolutions. *International Journal of Innovation and Applied Studies*, 3(1):262–270.

[Javadi e Razzaque, 2013] Javadi, S. S. e Razzaque, M. A. (2013). Security and privacy in wireless body area networks for health care applications. Em Khan, S. e Khan Pathan, A.-S., editors, *Wireless Networks and Security: Issues, Challenges and Research Trends*, p. 165–187, Berlin, Heidelberg. Springer Berlin Heidelberg.

[Kim et al., 2016] Kim, M., Lee, J. Y. e Kim, H. (2016). Warning and detection system for epidemic disease. *2016 International Conference on Information and Communication Technology Convergence (ICTC)*.

[Koufi et al., 2010] Koufi, V., Malamateniou, F. e Vassilacopoulos, G. (2010). Ubiquitous access to cloud emergency medical services. Em *Proceedings of the 10th IEEE International Conference on Information Technology and Applications in Biomedicine*, p. 1–4.

[Krempl et al., 2014] Krempl, G., Žliobaite, I., Brzeziundefinedski, D., Hüllermeier, E., Last, M., Lemaire, V., Noack, T., Shaker, A., Sievi, S., Spiliopoulou, M. e Stefanowski, J. (2014). Open challenges for data stream mining research. *SIGKDD Explor. Newsl.*, 16(1):1–10.

[Kumar e Lee, 2011] Kumar, P. e Lee, H.-J. (2011). Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors*, 12(1):55–91.

[Lee et al., 2017] Lee, C., Luo, Z., Ngiam, K. Y., Zhang, M., Zheng, K., Chen, G., Ooi, B. C. e Yip, W. L. J. (2017). Big healthcare data analytics: Challenges and applications. Em Khan, S. U., Zomaya, A. Y. e Abbas, A., editors, *Handbook of Large-Scale Distributed Computing in Smart Healthcare*, p. 11–41. Springer International Publishing.

[Liang et al., 2012] Liang, X., Li, X., Qinghua Shen, Lu, R., Lin, X., Shen, X. e Weihua Zhuang (2012). Exploiting prediction to enable secure and reliable routing in wireless body area networks. Em *2012 Proceedings IEEE INFOCOM*, p. 388–396.

[Liu et al., 2012] Liu, T., Bihr, U., Anis, S. M. e Ortmanns, M. (2012). Optical transcutaneous link for low power, high data rate telemetry. Em *2012 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, p. 3535–3538. IEEE.

[Luong et al., 2017] Luong, N. C., Hoang, D. T., Wang, P., Niyato, D. e Han, Z. (2017). Applications of economic and pricing models for wireless network security: A survey. *IEEE Communications Surveys Tutorials*, 19(4):2735–2767.

[Ma et al., 2018] Ma, Y., Luo, Z., Steiger, C., Traverso, G. e Adib, F. (2018). Enabling deep-tissue networking for miniature medical devices. Em *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, SIGCOMM '18, p. 417–431, New York, NY, USA. Association for Computing Machinery.

[Malik et al., 2018] Malik, M., Abdullah, T., Kousar, N., Nigar, M. e Awais, M. (2018). Wireless body area network security and privacy issue in e-healthcare. *International Journal of Advanced Computer Science and Applications*, 9:209–215.

[Mano et al., 2016a] Mano, L., Funes, M., Volpato, T. e Neto, J. (2016a). Explorando tecnologias de iot no contexto de health smart home: uma abordagem para detecção de quedas em pessoas idosas. *Journal on Advances in Theoretical and Applied Informatics*, 2(1):46–57.

[Mano, 2018] Mano, L. Y. (2018). Emotional condition in the health smart homes environment: emotion recognition using ensemble of classifiers. Em *2018 Innovations in Intelligent Systems and Applications (INISTA)*, p. 1–8.

[Mano et al., 2016b] Mano, L. Y., Faiçal, B. S., Nakamura, L. H., Gomes, P. H., Libralon, G. L., Meneguete, R. I., Filho, G. P., Giancristofaro, G. T., Pessin, G., Krishnamachari, B. e Ueyama, J. (2016b). Exploiting IoT technologies for enhancing health smart homes through patient identification and emotion recognition. *Computer Communications*, 89-90:178 – 190. Internet of Things Research challenges and Solutions.

[Mao et al., 2017] Mao, A., Ma, X., He, Y. e Luo, J. (2017). Highly portable, sensor-based system for human fall monitoring. *Sensors*, 17(9):2096.

[Matthew Pike e Brusic, 2019] Matthew Pike, Nasser M. Mustafa, D. T. e Brusic, V. (2019). Sensor networks and data management in healthcare: Emerging technologies and new challenges. *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*.

[Mattos et al., 2018] Mattos, D. M. F., Velloso, P. B. e Duarte, O. C. M. B. (2018). Uma infraestrutura ágil e efetiva de virtualização de funções de rede para a internet das coisas. Em *XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - SBRC'2018*.

[McKee, 2008] McKee, M. G. (2008). Biofeedback: an overview in the context of heart-brain medicine. *Cleveland Clinic journal of medicine*, 75:S31–S34.

[Medeiros et al., 2019] Medeiros, D. S. V., Neto, C., H. N., Andreoni Lopez, M., Magalhaes, L. C. S., Silva, E. F., Vieira, A. B., Fernandes, N. C. e Mattos, D. M. F. (2019). Análise de dados em redes sem fio de grande porte: Processamento em fluxo em tempo real, tendências e desafios. *Minicursos do XXXVII SBRC'2019*, p. 142–195.

[Medjahed et al., 2011] Medjahed, H., Istrate, D., Boudy, J., Baldinger, J.-L. e Dorizzi, B. (2011). A pervasive multi-sensor data fusion for smart home healthcare monitoring. *2011 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE 2011)*.

[Montoya et al., 2010] Montoya, A., Restrepo, D. C. e Ovalle, D. A. (2010). Artificial intelligence for wireless sensor networks enhancement. *Smart Wireless Sensor Networks*, p. 73–81.

[Mshali et al., 2018] Mshali, H., Lemlouma, T. e Magoni, D. (2018). Adaptive monitoring system for e-health smart homes. *Pervasive and Mobile Computing*, 43:1 – 19.

[Mucchi et al., 2019] Mucchi, L., Jayousi, S., Martinelli, A., Caputo, S. e Marcocci, P. (2019). An overview of security threats, solutions and challenges in wbans for healthcare. Em *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, p. 1–6.

[Negra et al., 2016] Negra, R., Jemili, I. e Belghith, A. (2016). Wireless body area networks: Applications and technologies. *Procedia Computer Science*, 83:1274–1281.

[Noury et al., 2000] Noury, N., Herve, T., Rialle, V., Virone, G., Mercier, E., Morey, G., Moro, A. e Porcheron, T. (2000). Monitoring behavior in home using a smart fall sensor and position sensors. Em *1st Annual International IEEE-EMBS Special Topic Conference on Microtechnologies in Medicine and Biology. Proceedings (Cat. No.00EX451)*, p. 607–610.

[Pannurat et al., 2014] Pannurat, N., Thiemjarus, S. e Nantajeewarawat, E. (2014). Automatic fall monitoring: A review. *Sensors*, 14(7):12900–12936.

[Paoli et al., 2012] Paoli, R., Fernández-Luque, F. J., Doménech, G., Martínez, F., Zapata, J. e Ruiz, R. (2012). A system for ubiquitous fall monitoring at home via a wireless sensor network and a wearable mote. *Expert Systems with Applications*, 39(5):5566 – 5575.

[Park e Mercier, 2015] Park, J. e Mercier, P. P. (2015). Magnetic human body communication. Em *2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, p. 1841–1844. IEEE.

[Park, 2017] Park, R. W. (2017). Sharing clinical big data while protecting confidentiality and security: observational health data sciences and informatics. *Healthcare informatics research*, 23(1):1–3.

[Parmentier et al., 2008] Parmentier, S., Fontaine, R. e Roy, Y. (2008). Laser diode used in 16 mb/s, 10 mw optical transcutaneous telemetry system. Em *2008 IEEE Biomedical Circuits and Systems Conference*, p. 377–380. IEEE.

[Patil et al., 2018] Patil, K., Laad, M., Kamble, A. e Laad, S. (2018). A consumer-based smart home and health monitoring system. *International Journal of Computer Applications in Technology*, 58(1).

[Pike et al., 2019] Pike, M., Mustafa, N. M., Towey, D. e Brusic, V. (2019). Sensor networks and data management in healthcare: Emerging technologies and new challenges. Em *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, volume 1, p. 834–839. IEEE.

[Pino e Salvo, 2013] Pino, C. e Salvo, R. D. (2013). A survey of cloud computing architecture and applications in health. Em *Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering*. Atlantis Press.

[Qathrady et al., 2016] Qathrady, M. A., Helmy, A. e Almuzaini, K. (2016). Infection tracing in smart hospitals. *2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*.

[Ramos e Filho, 2015] Ramos, A. e Filho, R. (2015). Sensor data security level estimation scheme for wireless sensor networks. *Sensors*, 15:2104 – 2136.

[Raymond e Midkiff, 2008] Raymond, D. R. e Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*, 7(1):74–81.

[Ren et al., 2019] Ren, Y., Leng, Y., Zhu, F., Wang, J. e Kim, H.-J. (2019). Data storage mechanism based on blockchain with privacy protection in wireless body area network. *Sensors*, 19(10):2395.

[Santagati e Melodia, 2016] Santagati, G. E. e Melodia, T. (2016). Experimental evaluation of impulsive ultrasonic intra-body communications for implantable biomedical devices. *IEEE Transactions on Mobile Computing*, 16(2):367–380.

[Sareen et al., 2018] Sareen, S., Sood, S. K. e Gupta, S. K. (2018). IoT-based cloud framework to control ebola virus outbreak. *Journal of Ambient Intelligence and Humanized Computing*, 9:459–476.

[Selimis et al., 2011] Selimis, G., Huang, L., Massé, F., Tsekoura, I., Ashouei, M., Catthoor, F., Huisken, J., Stuyt, J., Dolmans, G., Penders, J. e De Groot, H. (2011). A lightweight security scheme for wireless body area networks: Design, energy evaluation and proposed microprocessor design. *Journal of Medical Systems*, 35(5):1289–1298.

[Sen e Jaydip, 2009] Sen e Jaydip (2009). A survey on wireless sensor network security. *International Journal of Communication Networks and Information Security*, 1:59 – 82.

[Shivnath Babu, 2001] Shivnath Babu, J. W. (2001). Continuous queries over data streams. *ACM Sigmod Record*, 30(3):109–120.

[Sousa et al., 2019] Sousa, M. J., Pesqueira, A. M., Lemos, C., Sousa, M. e Rocha, Á. (2019). Decision-making based on big data analytics for people management in healthcare organizations. *Journal of Medical Systems*, 43(9):290.

[Sposaro e Tyson, 2009] Sposaro, F. e Tyson, G. (2009). iFall: An android application for fall monitoring and response. Em *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, p. 6119–6122.

[Sun et al., 2015] Sun, X., Lu, Z., Zhang, X., Salathé, M. e Cao, G. (2015). Targeted vaccination based on a wireless sensor system. *2015 IEEE International Conference on Pervasive Computing and Communications (PerCom)*.

[Sureshkumar et al., 2019] Sureshkumar, V., Amin, R., Vijaykumar, V. e Sekar, S. R. (2019). Robust secure communication protocol for smart healthcare system with FPGA implementation. *Future Generation Computer Systems*, 100:938 – 951.

[Taha et al., 2018] Taha, M. S., Rahim, M. S. M., Hashim, M. M. e Johi, F. A. (2018). Wireless body area network revisited. *International Journal of Engineering & Technology*, 7(4):3494–3504.

[Todd e Skelton, 2004] Todd, C. e Skelton, D. (2004). What are the main risk factors for falls amongst older people and what are the most effective interventions to prevent these falls? Relatório técnico, World Health Organization Regional Office for Europe, Copenhagen, Denmark.

[Tomlinson et al., 2018] Tomlinson, W. J., Banou, S., Yu, C., Stojanovic, M. e Chowdhury, K. R. (2018). Comprehensive survey of galvanic coupling and alternative intra-body communication technologies. *IEEE Communications Surveys & Tutorials*, 21(2):1145–1164.

[Trevlakis et al., 2019] Trevlakis, S. E., Boulogeorgos, A.-A. A., Sofotasios, P. C., Muhaidat, S. e Karagiannidis, G. K. (2019). Optical wireless cochlear implants. *Biomedical optics express*, 10(2):707–730.

[Vasseur e Dunkels, 2010] Vasseur, J.-P. e Dunkels, A. (2010). Chapter 1 - what are smart objects? Em *Interconnecting Smart Objects with IP*, p. 3–20. Morgan Kaufmann, Boston.

[Wang et al., 2015] Wang, S., Urgaonkar, R., Zafer, M., He, T., Chan, K. e Leung, K. K. (2015). Dynamic service migration in mobile edge-clouds. Em *Proceedings of the IFIP Networking Conference (IFIP Networking)*, p. 1–9.

[Weber-Jahnke et al., 2012] Weber-Jahnke, J., Peyton, L. e Topaloglou, T. (2012). e-Health system interoperability. *Information Systems Frontiers*, 14(1):1–3.

[Yassine et al., 2017] Yassine, A., Singh, S. e Alamri, A. (2017). Mining human activity patterns from smart home big data for health care applications. *IEEE Access*, 5:13131–13141.

[Zafar et al., 2014] Zafar, Z., Islam, S., Aslam, M. S. e Sohaib, M. (2014). Cloud computing services for the healthcare industry. *Int J Multidiscip Sci Eng*, 5:25–29.

[Zhang et al., 2013a] Zhang, R., Zhang, J., Zhang, Y., Sun, J. e Yan, G. (2013a). Privacy-preserving profile matching for proximity-based mobile social networking. *IEEE Journal on Selected Areas in Communications*, 31:656 – 668.

[Zhang et al., 2013b] Zhang, Z., Wang, H., Lin, X., Fang, H. e Xuan, D. (2013b). Effective epidemic control and source tracing through mobile social sensing over wbans. *2013 Proceedings IEEE INFOCOM*.