UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Genilson Israel da Silva

Priorização de Alertas Médicos em Redes Sem Fio Definidas Por Software: Uma Perspectiva Experimental

Juiz de Fora

2021

Genilson Israel da Silva

Priorização de Alertas Médicos em Redes Sem Fio Definidas Por Software: Uma Perspectiva Experimental

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de Mestre em Ciência da Computação. Área de concentração: Ciência da Computação.

Orientador: Prof. Dr. Alex Borges Vieira

Coorientadora: Profa. Dra. Michele Nogueira Lima

Juiz de Fora

2021

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

da Silva, Genilson Israel.
Priorização de Alertas Médicos em Redes Sem Fio Definidas Por Software: Uma Perspectiva Experimental / Genilson Israel da Silva. – 2021.
75 f. : il.

Orientador: Alex Borges Vieira
Coorientadora: Michele Nogueira Lima
Dissertação (Mestrado) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Programa de Pós-Graduação em Ciência da Computação, 2021.

1. Redes corporais sem fio. 2. Redes sem fio definidas por software. 3. Sistemas de monitoramento de saúde. 4. Priorização de acesso ao meio. I. Vieira, Alex Borges, orient. II. Lima, Michele Nogueira, coorient. III. Título.

Genilson Israel da Silva

Priorização de Alertas Médicos em Redes Sem Fio Definidas Por Software: Uma Perspectiva Experimental

Dissertação apresentada ao Programa de Pós-graduação em Ciência da Computação da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de Mestre em Ciência da Computação. Área de concentração: Ciência da Computação.

Aprovada em 08 de dezembro de 2021.

BANCA EXAMINADORA

Prof. Dr. Alex Borges Vieira - Orientador
Universidade Federal de Juiz de Fora

Profª. Dra. Michele Nogueira Lima - Coorientadora
Universidade Federal de Minas Gerais

Prof. Dr. Edelberto Franco Silva
Universidade Federal de Juiz de Fora

Prof. Dr. José Augusto Miranda Nacif
Universidade Federal de Viçosa

Juiz de Fora, 18/04/2022.

Documento assinado eletronicamente por **Alex Borges Vieira**, **Coordenador(a) em exercício**, em 18/04/2022, às 14:21, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Edelberto Franco Silva**, **Professor(a)**, em 18/04/2022, às 14:27, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **José Augusto Miranda Nacif**, **Usuário Externo**, em 18/04/2022, às 15:03, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Michele Nogueira Lima**, **Usuário Externo**, em 18/04/2022, às 17:42, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no Portal do SEI-Ufjf (www2.ufjf.br/SEI) através do ícone Conferência de Documentos, informando o código verificador **0746483** e o código CRC **25AC2CB2**.

Ao meu pai Vicente (in memorian), meu herói

AGRADECIMENTOS

O desenvolvimento desta pesquisa foi um processo deveras desafiador. Mas apesar dos ocasionais tropeços e incertezas no decorrer do caminho, me sinto orgulhoso por tê-la realizado. Agradeço a Deus por ter me dado forças para chegar ao fim.

Agradeço à minha família pelo costumeiro apoio incondicional. Agradeço especialmente à minha irmã, Maria Jacqueline, por toda a ajuda nos momentos em que me encontrava atarefado. Obrigado por fazer de tudo para me ver bem.

À minha mãe, Luzia, e ao meu pai, Vicente (*in memorian*), por serem tão nobres e íntegros, e por terem me oferecido tanto, mesmo tendo tão pouco.

Aos meus orientadores, Alex e Michele, por toda a contribuição, e por terem me guiado por tanto tempo com paciência e sabedoria. Obrigado pelos vários ensinamentos.

Ao professores Edelberto e José Nacif, pelas valiosas contribuições no desenvolvimento desta pesquisa.

Aos amigos do *NetLab*, especialmente Mayara, Airton, Fred e Jorge, por tornarem a caminhada mais leve, e pela amizade que certamente levarei por toda a vida.

Aos meus amigos Breno, Maurício e Eliane, que acompanharam mais de perto essa etapa da minha vida, e me ajudaram muito, seja na pesquisa, ou apenas ouvindo meus desabafos.

Ao IF Sudeste MG - *Campus* Barbacena, pela oportunidade da licença capacitação, por ceder um laboratório para que eu pudesse finalizar a pesquisa, e por todo o apoio que me deram. Agradecimento especial ao Wagner, por ter me incentivado e assumido minhas tarefas, e aos demais amigos da Coordenação de Tecnologia da Informação, pela compreensão, e por terem "segurado as pontas".

Finalmente, agradeço à UFJF e aos profissionais do PPGCC por toda a estrutura, e pela oportunidade de evolução.

"All we have to decide is what to do with the time that is given to us."

Gandalf

RESUMO

Os avanços tecnológicos das Redes Corporais Sem Fio (WBANs) possibilitaram seu uso em diferentes cenários. Entre as áreas de aplicação possíveis, os sistemas de monitoramento de saúde são uma das mais notáveis, visto que essas redes possibilitam o monitoramento de pacientes em tempo real e o diagnóstico de muitas doenças fatais. Os dados sensíveis coletados servem de entrada para sistemas voltados à identificação antecipada de eventos críticos relacionados ao estado de saúde do paciente. Uma vez identificado um evento crítico, pacotes de alerta podem ser enviados com certa priorização para servidores médicos, viabilizando a rápida prestação de socorro e a redução dos riscos de morte ou sequelas graves para o paciente. Em um ambiente hospitalar, pacotes de alerta médico competem com diversos e variados fluxos de tráfego pelo uso dos recursos da rede local sem fio (WLAN), de modo que um dos maiores desafios nesse contexto encontra-se em reduzir latências e perdas para esses pacotes. Além disso, é desejável que a priorização de dados médicos cause o menor impacto possível no desempenho geral da rede, motivo pelo qual é importante que seja adotada uma abordagem sob demanda, que atue apenas quando são identificados fluxos de dados médicos, e apenas nos pontos de acesso (APs) participantes da comunicação. Nesse sentido, este trabalho propõe uma plataforma baseada em Redes Sem Fio Definidas por *Software* (SDWN) para priorização de acesso ao meio sem fio sob demanda para pacotes de alerta médico, com base na alteração programática de parâmetros da subcamada de acesso ao meio das redes sem fio IEEE 802.11. Esses parâmetros permitem definir, para cada uma das quatro categorias de tráfego WLAN, a quantidade de tempo que o canal sem fio deve ficar desocupado antes que uma transmissão de dados seja iniciada. Ao variar esses parâmetros entre as categorias, é possível dar a elas diferentes prioridades de acesso ao canal sem fio. A plataforma foi avaliada em um ambiente real de rede sem fio, com diferentes quantidades de clientes conectados. No cenário de maior densidade dentre os construídos para os testes, com 20 clientes sem fio, houve uma redução de 34,65% no atraso médio dos pacotes de alerta médico priorizados em relação aos não priorizados, além de uma redução de 58,62% na quantidade de pacotes perdidos.

Palavras-chave: Redes corporais sem fio. Redes sem fio definidas por software. Sistemas de monitoramento de saúde. Priorização de acesso ao meio.

ABSTRACT

Technological advances in Wireless Body Area Networks (WBAN) have enabled their use in different scenarios. Among their many possible areas of application, health monitoring systems are one of the most notable ones, as these networks make it possible to monitor patients in real time and diagnose many fatal diseases. The collected sensitive data can be fed to systems capable of early detection of critical events related to the patient's health status. Once a critical event is identified, medical alert packets can be sent with some level of prioritization to medical servers, enabling rapid relief provisioning and reducing the risk of death or serious sequelae for the patient. In a hospital environment, medical alert packets contend with multiple traffic flows, with varying characteristics, for the wireless local area network (WLAN) resources. Thus, one of the main challenges in this context is to ensure lower latencies and loss rates for medical data packets. Furthermore, it is desirable that the impact on the overall performance of the network be kept to a minimum, which is why it is important to adopt an on-demand approach, which acts only when medical data flows are identified, and only on the access points (APs) that participate in the communication. In this sense, this work proposes a platform based on Software Defined Wireless Networks (SDWN) for on-demand access prioritization to the wireless medium for medical alert packets, based on the programmatic configuration of medium access control sublayer parameters in IEEE 802.11 wireless networks. These parameters allow the definition, for each of the four WLAN traffic categories, of the amount of time that the wireless channel must be idle before a data transmission is initiated. By varying these parameters, it's possible to give traffic categories different wireless channel access priorities. The platform was evaluated in a real wireless network environment, with different quantities of wireless stations connected to the AP. In the highest density scenario among the ones built for the tests, with 20 wireless clients, there was a 34.65% reduction in the average delay of prioritized medical alert packets compared to non-prioritized ones, in addition to a reduction of 58.62% in the amount of packets lost.

Keywords: Wireless body area networks. Software defined wireless networks. Health monitoring systems. Medium access prioritization.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AC	*Access Category*
ACI	*Access Category Index*
AIFS	*Arbitration Interframe Space*
AIFSN	*Arbitration Interframe Space Number*
AP	*Access Point*
API	*Application Programming Interface*
BLE	*Bluetooth Low Energy*
BSA	*Basic Service Area*
BSS	*Basic Service Set*
CAP	*Contention Access Period*
CCA	*Clear Channel Assessment*
CFP	*Contention Free Period*
CP	*Contention Period*
CS	*Carrier Sense*
CSMA/CA	*Carrier Sense Multiple Access With Collision Avoidance*
CW	*Contention Window*
CWmax	*Maximum Contention Window*
CWmin	*Minimum Contention Window*
DCF	*Distributed Coordination Function*
DIFS	*DCF Interframe Space*
D-ITG	*Distributed Internet Traffic Generator*
DLL	*DataLink Layer*
DS	*Distribution System*
DSCP	*Differentiated Services Code Point*
DSSS	*Direct-Sequence Spread-Spectrum*
EDCA	*Enhanced Distributed Channel Access*
EIFS	*Extended Interframe Space*
ESS	*Extended Service Set*
FHSS	*Frequency-Hopping Spread Spectrum*
HCCA	*HCF Controlled Channel Access*
HCF	*Hybrid Coordination Function*
IBSS	*Independent Basic Service Set*
IDT	*nter Departure Time*
IFS	*Interframe Space*
LAN	*Local Area Network*
LLC	*Logical Link Control*
MAC	*Medium Access Control*
MEMS	*Microelectromechanical Systems*
MIB	*Management Information Base*
MIMO	*Multiple Input Multiple Output*

MPDU	*MAC Protocol Data Unit*
NAV	*Network Allocation Vector*
OFDM	*Orthogonal FrequencyDivision Multiplexing*
OSI	*Open System Interconnection*
OVSDB	*Open vSwitch Database Management Protocol*
PC	*Point Coordinator*
PCF	*Point Coordination Function*
PIFS	*PCF Interframe Space*
PHY	*Physical Layer*
QoE	*Quality of Experience*
QoS	*Quality of Service*
RL	*Reinforcement Learning*
SDN	*Software-Defined Networking*
SDWN	*Software Defined Wireless Network*
SIFS	*Short Interframe Space*
SSID	*Service Set Identifier*
SSL	*Secure Socket Layer, ouCamada de Soquete Seguro*
STA	*Station*
TCAM	*Ternary Content Addressable Memory*
TDMA	*Time Division Multiple Access*
TID	*Traffic Identifier*
TXOP	*Transmission Opportunity*
UP	*User Priority*
VAP	*Virtual Access Point*
WBAN	*Wireless Body Area Network*
WLAN	*Wireless Local Area Network*
WME	*Wireless Multimedia Extension*
WMM	*Wi-Fi Multimedia*
WSN	*Wireless Sensor Networks*

SUMÁRIO

1 INTRODUÇÃO

A taxa de envelhecimento da população mundial vem aumentando de forma significativa. De acordo com a OMS (Organização Mundial de Saúde), o número de pessoas com idade superior a 60 anos deverá subir para 2.1 bilhões em 2050 (28). Alguns problemas de saúde são mais frequentes em populações idosas (45), motivo pelo qual esse grupo demanda cuidados extras (2). Na ocorrência de um evento crítico de saúde, um atendimento rápido pode ser decisivo para salvar a vida do paciente, ou pelo menos reduzir as possíveis sequelas decorrentes do evento.

Os avanços recentes nas áreas de comunicação sem fio, tecnologia de sistemas microeletromecânicos e circuitos integrados, permitiram que fossem criados sensores miniaturizados derivados de micro e nanotecnologia, que podem ser utilizados interna ou externamente ao corpo humano (52). Esses sensores se comunicam formando as chamadas Redes Corporais Sem Fio , ou WBANs (*Wireless Body Area Networks*), que possibilitaram o desenvolvimento de sistemas de monitoramento de sinais vitais de pacientes hospitalares, tais como o *iCare* (35) e o *eCardio* (38). Os dados sensíveis coletados servem de entrada para sistemas capazes de identificar antecipadamente eventos críticos relacionados ao estado de saúde do paciente, e enviar pacotes de alerta para um servidor médico central, viabilizando a rápida prestação de socorro e a redução do risco de morte ou sequelas graves para o paciente. O SANTE (61), exemplo de um desses sistemas, é capaz de prever uma mudança brusca no estado de saúde do paciente, ao analisar indicadores tais como batimentos cardíacos e frequência respiratória. A combinação de WBANs e Redes Locais Sem Fio, ou WLANs (*Wireless Local Area Networks*), pode fornecer um sistema de comunicação local efetivo para transmissão ao servidor médico central de dados de saúde coletados pelas WBANs (52).

As WBANs se comunicam com o mundo externo através de outras tecnologias de redes sem fio, como redes celulares e WLANs. A WLAN de um hospital pode ser utilizada para transmitir dados médicos vindos de WBANs até o AP (*Access Point*, ou Ponto de Acesso) mais próximo (52), de onde seguem para o servidor médico central, normalmente por uma infraestrutura de rede cabeada. Além das WBANs, diversos outros dispositivos sem fio são conectados à WLAN do hospital, como computadores portáteis e *smartphones* usados pela equipe médica (53).

A competição entre fluxos de tráfego de diferentes características, como voz, vídeo e dados, pelo acesso ao canal de comunicação, é especialmente desafiadora em se tratando de meios de transmissão sem fio, devido à sua natureza propensa a erros e interferências (16). Além disso, um elevado número de usuários conectados à rede sem fio pode levar à saturação do canal de comunicação, resultando em maiores latências e perdas de pacotes. Se esses pacotes forem, por exemplo, alertas para a iminência de uma situação crítica de saúde, as

consequências podem ser desastrosas. Por esse motivo, os dois principais parâmetros a serem considerados para sistemas de monitoramento em tempo real de pacientes são a confiabilidade e o atraso (52, 45).

Desde seu surgimento, as WLANs seguem um processo contínuo de evolução. O padrão IEEE 802.11 especifica caraterísticas da subcamada de controle de acesso ao meio, ou subcamada MAC (*Medium Access Control*) e camada física (PHY) para redes locais sem fio (23) e, durante os últimos vinte anos, recebeu diversas revisões para incorporação de emendas, correções e melhorias. A constante evolução do padrão visa atender às crescentes demandas por maiores taxas de transferência e menores latências impostas pelas aplicações. Incorporado ao padrão IEEE 802.11 em 2007, o adendo IEEE 802.11e é um exemplo dessa evolução constante, e introduziu melhorias no esquema de acesso ao meio da camada de enlace, que permitiram o gerenciamento de Qualidade de Serviço, ou QoS (*Quality of Service*) em redes sem fio locais. O novo método de acesso pode ser empregado para reduzir atrasos e perdas para fluxos de pacotes de alerta médico.

As WLANs se popularizaram principalmente pela praticidade e conveniência que oferecem, aliadas ao crescimento da disponibilidade de dispositivos portáteis (46, 36). As redes baseadas no padrão IEEE 802.11 são uma das tecnologias sem fio de maior sucesso já inventadas (55) e, graças às constantes revisões do padrão, espera-se que em 2023 o número de pontos de acesso disponíveis seja quatro vezes maior do que em 2018 (11).

As tecnologias emergentes de rede sem fio de alta velocidade utilizam ondas de frequências mais altas (*e.g.* 802.11ad, que opera na frequência de 60GHz) e, portanto, de menor comprimento. Essas ondas têm maior dificuldade em atravessar obstáculos, o que resulta na densificação de APs (41) para atender uma mesma área, e aumenta a necessidade de um controle mais aprimorado dos dispositivos da rede. O gerenciamento centralizado de infraestruturas de rede sem fio é realizado por controladores capazes de gerenciar os APs existentes na rede, e efetuar ajustes de potência de sinal, seleção de canal, gerenciamento de associação e mobilidade de usuários, políticas de limitação de banda e segurança. Contudo, as arquiteturas de gerenciamento de redes sem fio atuais, em sua maioria, utilizam controladores proprietários, com código fechado, capazes de gerenciar apenas dispositivos compatíveis, geralmente fornecidos pelo mesmo fabricante do controlador. Essas soluções de rede sem fio, muitas vezes com custos proibitivos, levam a uma dependência de fornecedores, além de disponibilizarem um conjunto limitado de rotinas de configuração para o administrador (15), o que restringe sua capacidade de adequar o gerenciamento da rede às suas necessidades particulares. Devido a essa limitação, as abordagens atuais para gerenciamento de WLANs normalmente se resumem a configurações estáticas de parâmetros nos APs da rede ou na utilização de soluções proprietárias (41).

O paradigma de Redes Sem Fio Definidas por Software, ou SDWN (*Software*

Defined Wireless Network) propicia uma visão global da rede sem fio, e permite seu controle de forma programática a partir de um controlador logicamente centralizado (25). A programabilidade da rede dá ao administrador o poder de alterar o comportamento dos fluxos de dados conforme as necessidades das aplicações, e o controle centralizado mantém a consistência na configuração de parâmetros de rede entre os diversos APs. Um exemplo de arquitetura de redes definidas por software para redes sem fio IEEE 802.11 é o Ethanol (41), que possibilita não só o controle das características da rede sem fio nos APs, como também a manipulação dos fluxos de dados em comutadores de pacote compatíveis.

1.1 PROBLEMA

Os dois principais parâmetros a serem considerados para a comunicação de aplicações médicas de monitoramento de pacientes em tempo real, são a latência e a confiabilidade (52). Isso é especialmente desafiador em um ambiente hospitalar, onde a rede sem fio é utilizada não só por essas aplicações, mas também para a comunicação de diversos dispositivos sem fio, os quais geram múltiplos fluxos de dados concorrentes e de diferentes características, que competem com os dados das aplicações médicas pelo uso de recursos da rede. Os fluxos de dados médicos precisam ser priorizados em relação aos demais, mas essa priorização deve ser feita sob demanda, de forma a impactar o mínimo possível o desempenho geral da rede.

1.2 OBJETIVO

Este trabalho tem como principal objetivo, utilizar funcionalidades da subcamada MAC de redes sem fio IEEE 802.11, em conjunto com a abordagem SDWN, para priorizar dinamicamente o acesso ao meio para fluxos de pacotes de alerta médico em uma rede sem fio hospitalar, e com isso reduzir latências e perdas observados para esses pacotes. Para esse fim, estendemos as funcionalidades do Ethanol (41), e implementamos as funções que alteram nos APs os parâmetros de subcamada MAC definidos pelo adendo IEEE 802.11e para melhorias de QoS. Utilizamos a versão aprimorada do Ethanol para propor e avaliar, em um ambiente real de rede sem fio, uma plataforma baseada em SDWN para priorização de fluxos de pacotes de alerta médico. Essa plataforma é implementada como um módulo do controlador Ethanol, e configura sob demanda os parâmetros de QoS da subcamada MAC de redes sem fio IEEE 802.11. A solução apresentada busca reduzir os atrasos e perdas observados para esses pacotes ao trafegarem entre a WBAN e o AP, quando o canal de comunicação está saturado pelo tráfego gerado por outras estações sem fio.

1.3 CONTRIBUIÇÕES

Como contribuições do nosso trabalho, destacamos a proposta de uma plataforma para priorização dinâmica de pacotes de alerta médico em redes sem fio hospitalares, e a avaliação dessa proposta em um ambiente real de rede sem fio com a utilização de até 20 estações sem fio, ou STAs. De fato, estudos que avaliam a melhoria de QoS em WLANs usando IEEE 802.11e geralmente utilizam ambientes simulados, como em (61, 13, 62, 63, 7, 53), o que dificulta a avaliação dos efeitos das propriedades de propagação assimétricas e variáveis inerentes aos meios sem fio nos resultados obtidos. Uma outra contribuição decorrente deste estudo é o aprimoramento das funcionalidades do Ethanol quanto à sua capacidade de programabilidade da rede, com a inclusão de funções para gerenciamento dos parâmetros QoS da subcamada MAC de redes sem fio IEEE 802.11. Essa nova funcionalidade da ferramenta expande as possibilidades para a realização de novos estudos em ambientes reais de redes sem fio, utilizando diferentes abordagens como, por exemplo, o emprego de algoritmos de aprendizado de máquina para definição de valores otimizados para esses parâmetros, considerando diferentes aplicações de rede sem fio.

1.4 ORGANIZAÇÃO DO TEXTO

No restante desta dissertação, o Capítulo 2 apresenta os fundamentos teóricos necessários para compreensão do trabalho desenvolvido, como conceitos de redes locais sem fio, redes corporais sem fio, redes definidas por *software* e redes sem fio definidas por *software*. O Capítulo 3 discute trabalhos que têm relação com nosso estudo. No Capítulo 4 apresentamos a plataforma de priorização dinâmica de tráfego para pacotes de alerta médico baseada em redes sem fio definidas por *software* e as funções implementadas para gerenciamento de subcamada MAC. A avaliação experimental da plataforma em um ambiente real de rede sem fio e os resultados obtidos são apresentados no Capítulo 5. Por fim, o Capítulo 6 traz as conclusões do estudo e discute trabalhos futuros.

2 FUNDAMENTOS

Este capítulo apresenta os principais conceitos utilizados no desenvolvimento deste trabalho. A Seção 2.1 traz conceitos sobre as WLANs, discutindo seu funcionamento e apresentando os mecanismos disponíveis para gerenciamento de QoS nessas redes. A Seção 2.2 discute as WBANs e sua importância para o aprimoramento dos cuidados de saúde. A Seção 2.3 aborda o paradigma SDN, e discute seu papel na simplificação do gerenciamento e na evolução das redes de computadores. A Seção 2.4 trata sobre as vantagens do uso da abordagem SDN em redes sem fio, introduzindo o conceito de SDWN.

2.1 REDES LOCAIS SEM FIO IEEE 802.11 (WLANs)

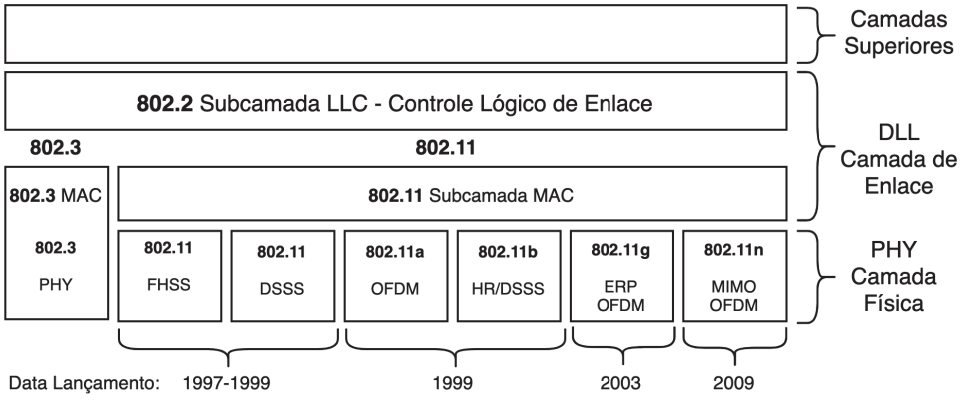
A família IEEE 802 compreende uma série de especificações para Redes Locais, ou LANs (*Local Area Networks*), focadas nas duas camadas mais inferiores do modelo de referência para Interconexão de Sistemas Abertos, ou OSI (*Open System Interconnection*), as quais englobam componentes de ligações física e de dados da comunicação de redes. Todas as redes IEEE 802 possuem uma camada física (PHY), responsável por lidar com a transmissão e recepção de sinais pelo meio de comunicação, e uma camada MAC, que estabelece as regras para acesso ao meio e envio de dados (16).

O padrão IEEE 802.11[1] é um membro da família IEEE 802, e desde seu surgimento segue um processo contínuo de evolução. Originalmente incluía a camada MAC e duas camadas físicas: FHSS (*Frequency-Hopping Spread Spectrum*, ou Espalhamento Espectral por Salto de Frequências) e DSSS (*Direct-Sequence Spread-Spectrum*, ou Espalhamento Espectral por Sequência Direta), ambas com taxas de transferência de 1 Mbps, e um modo opcional de 2 Mbps (36). Evoluções incorporadas ao padrão por emendas posteriores permitiram que se atingisse taxas de transferência muito maiores, sempre utilizando faixas de frequência não licenciadas, ou seja, a banda ISM (*Industrial Scientifc Medical*), que opera nas frequências 2,4 GHz e 5 GHz. A aplicação de técnicas de Multiplexação por Divisão de Frequências Ortogonais, ou OFDM (*Orthogonal Frequency Division Multiplexing*) permitiu a transição do padrão 802.11b para os 802.11a/g. A OFDM é ainda a tecnologia utilizada nas camadas físicas das redes sem fio em uso atualmente, como as 802.11n e 802.11ac. Mesmo o novo padrão para redes sem fio, o IEEE 802.11ax, utiliza uma versão aprimorada da OFDM, com mais subportadoras, chamada OFDMA (*Orthogonal Frequency-Division Multiple Access*, ou Acesso Múltiplo por Divisão de Frequência Ortogonal). No caso dessas redes, as maiores taxas de transferência são decorrentes da combinação de melhorias nas técnicas de modulação com o uso de múltiplas antenas, que multiplicam sua capacidade de transmissão, tecnologia conhecida como MIMO (*Multiple Input Multiple Output*, ou Múltiplas Entradas e Múltiplas Saídas) (17).

[1] https://standards.ieee.org/standard/802_11-2020.html

Após publicar a primeira versão do padrão 802.11, em 1997, o Grupo de Trabalho responsável recebeu algumas notificações de problemas de compatibilidade entre equipamentos de diferentes fabricantes. Foi fundada então a *Wi-Fi Alliance*, uma organização sem fins lucrativos, responsável pela criação do selo *Wi-Fi CERTIFIED*^{TM} [2] e pela popularização do termo Wi-Fi para designar redes sem fio baseadas no padrão IEEE 802.11. Recebem a certificação Wi-Fi, produtos que passam por testes específicos, para garantir que atendam aos padrões de interoperabilidade acordados pela indústria. A Figura 1 mostra a relação entre a família IEEE 802 e o modelo OSI. A subcamada LLC (*Logical Link Control*, ou Controle Lógico de Enlace) é especificada pelo padrão IEEE 802.2, e pode ser utilizada pelas camadas inferiores de qualquer tecnologia de rede local. As subcamadas MAC e LLC integram a camada de enlace do modelo OSI (DLL - *Data Link Layer*). A arquitetura de redes sem fio permite que estações sem fio sejam enxergadas pelas camadas superiores como se fossem estáticas. Essa abstração fornecida às camadas superiores, permite que protocolos TCP/IP existentes sejam executados em redes sem fio da mesma forma que em redes cabeadas (46).

Figura 1 – Família IEEE 802 e sua relação com o modelo OSI



Fonte: Adaptado de (16)

2.1.1 Arquitetura de redes sem fio IEEE 802.11

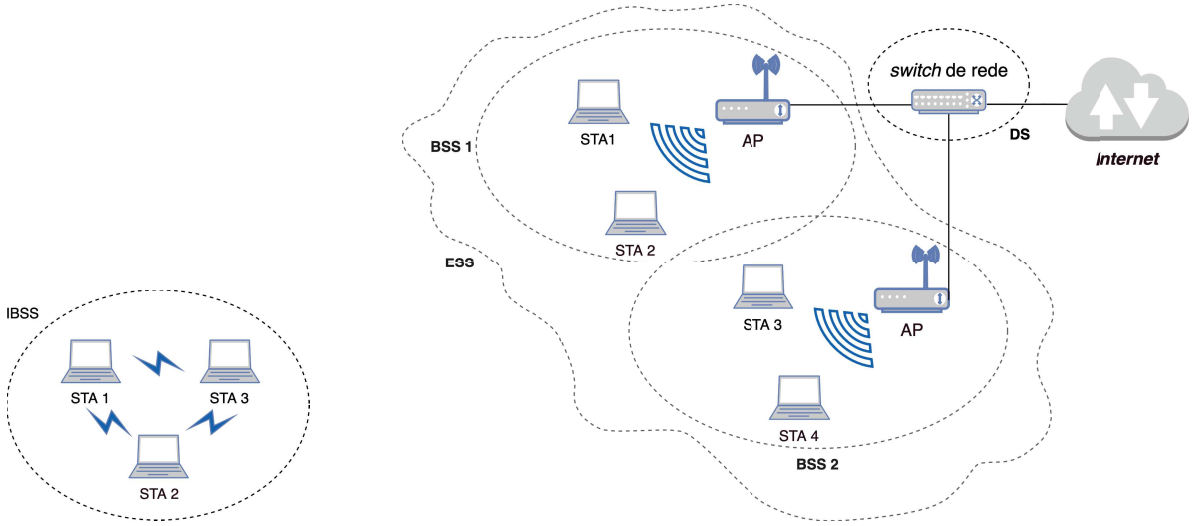
A arquitetura de redes IEEE 802.11 possui diferentes componentes que interagem entre si. O elemento fundamental de uma WLAN é o Conjunto Básico de Serviço, ou BSS (*Basic Service Set*). A área de cobertura de um BSS é chamada Área Básica de Serviço, ou BSA (*Basic Service Area*). Há dois modos de configuração para redes 802.11: *ad hoc* e infraestrutura. No modo *ad hoc*, as estações sem fio dentro de uma mesma BSA se comunicam diretamente, sem um controle central, formando um BSS Independente, ou IBSS (*Independent BSS*), que não se conecta a outras redes. Esse modo de configuração

[2] https://www.wi-fi.org/certification

é mostrado na Figura 2(a). No modo infraestrutura, as STAs se comunicam com a rede cabeada através de uma *bridge* (ou ponte) provida por um AP (46). Como pode ser observado na Figura 2(b), dois ou mais APs podem se conectar através de um Sistema de Distribuição, ou DS (*Distribution System*), unindo seus BSSs em um Conjunto Estendido de Serviço, ou ESS (*Extended Service Set*), o que amplia a área de cobertura da rede. O DS não faz parte do ESS. A infraestrutura do DS é comumente cabeada, mas também pode ser sem fio, já que o padrão não estabelece essa limitação (22).

Quando o AP está presente, a BSA é definida pela área de cobertura do AP, e toda a comunicação passa por ele, seja entre as STAs do mesmo BSS ou a partir das STAs para a rede externa. Apesar de mais custosa do que uma transmissão direta entre STAs, a transmissão com dois saltos adiciona menos complexidade à camada física, já que as STAs de um BSS não precisam manter registro das localizações das STAs vizinhas, e não precisam estar ao alcance umas das outras, desde que estejam ao alcance do AP (16). As áreas de cobertura de dois ou mais BSSs podem se sobrepor parcialmente, para prover cobertura contínua dentro de um espaço físico. Isso permite que as STAs possam se mover de forma transparente entre BSSs, processo conhecido como *handoff*.

Figura 2 – Arquitetura de redes IEEE 802.11 WLAN



(a) Rede *ad hoc* (b) Rede infraestruturada

Fonte: Elaborado pelo autor (2021)

Em redes 802.11 configuradas no modo infraestrutura, cada STA precisa se associar a um AP antes de iniciar uma comunicação de rede (31). Após associada, a STA só enviará quadros de dados para a rede através do AP, e quadros de dados destinados à STA serão entregues a ela pelo AP. O BSS é identificado pelo AP através de um Identificador de Conjunto de Serviço, ou SSID (*Service Set Identifier*), e possui um canal sem fio definido para comunicação. No caso de redes 802.11g, como a utilizada em nosso experimento, 11 canais parcialmente sobrepostos estão disponíveis. O AP envia quadros de sinalização

(*beacon frames*) periodicamente, informando o endereço MAC do AP (BSSID) e o SSID da rede, além de outras informações. Para escolher um AP para se associar, a STA varre os canais sem fio em busca de quadros *beacon*, ou envia quadros de investigação (*Probe Request*) aos APs. Os APs respondem quadros de investigação com quadros *Probe Response*. A STA define a qual AP deseja se associar e envia um pedido de associação (*Association Request*), recebendo como resposta do AP um quadro (*Association Response*). Quadros de pedido e resposta de reassociação (*Reassociation Request* e *Reassociation Response*), são utilizados quando uma STA retorna à uma BSA de um BSS onde já tenha se associado anteriormente, ou quando esta se move entre BSSs de um mesmo ESS.

2.1.2 Subcamada de Controle de Acesso ao Meio (MAC)

O uso de ondas de rádio como meio de comunicação, torna as camadas físicas do padrão IEEE 802.11 muito mais complexas do que as de meios guiados (16). Isso se deve às características inerentes à comunicação sem fio, que possui propriedades de propagação assimétricas e variáveis. Não existem delimitações físicas absolutas para cobertura de sinal, a topologia da rede pode mudar a qualquer momento, e além disso o canal de comunicação está sujeito à interferência de outros sinais sem fio (22). Essas características tornam impossível assumir que todos os quadros transmitidos foram de fato entregues, motivo pelo qual cada quadro enviado deve ser confirmado (63).

Um dos grandes desafios encontrados nesse contexto, é permitir que múltiplas STAs possam acessar um canal de difusão compartilhado (31). Os rádios normalmente são *half-duplex*, o que significa que não conseguem fazer transmissões e recepções simultaneamente. O sinal recebido, mais fraco do que o transmitido, acaba não sendo detectado (19). Essa característica impede que eventuais colisões possam ser detectadas durante a transmissão, que uma vez iniciada, não é interrompida, o que resulta em desperdício de tempo de uso do canal e prejudica o desempenho da rede.

O acesso ao meio sem fio deve ser coordenado, para que não seja feito simultaneamente por múltiplos transmissores e receptores. Essa coordenação pode ser centralizada ou distribuída. O método básico de acesso utilizado pela subcamada MAC do padrão IEEE 802.11, desde seu lançamento, é uma Função de Coordenação Distribuída, ou DCF (*Distributed Coordination Function*) (22), onde cada STA atua de modo independente, sem um controle central, mas de forma coordenada com as demais. A DCF utiliza a abordagem "ouça antes de falar", implementando para isso o protocolo de Acesso Múltiplo com Detecção de Portadora com Prevenção de Colisão, ou CSMA/CA (*Carrier-Sense Multiple Access With Collision Avoidance*), e é obrigatória para todas as STAs de uma rede sem fio, seja no modo infraestrutura ou *ad hoc*. O padrão inclui também uma Função de Coordenação de Ponto, ou PCF (*Point Coordination Function*), construída sobre a DCF, que permite acesso sem contenção por um período limitado de tempo ao

canal de comunicação. A PCF é opcional e exclusiva para redes infraestruturadas. Seu funcionamento é baseado em um controle centralizado realizado pelo AP, que exerce a função de Coordenador de Ponto, ou PC (*Point Coordinator*), e determina quais estações podem utilizar o meio durante o período sem contenção, ou CFP (*Contention Free Period*).

As redes baseadas no padrão IEEE 802.11 WLAN não eram originalmente adequadas para provisionamento de QoS, visto que a subcamada de acesso ao meio (MAC) não possuía funções para esse fim, e a camada física (PHY) é instável e suscetível a erros e interferências (46). Projetadas para entrega de tráfego a altas taxas, as WLANs podem ser ineficientes quando empregadas no uso de aplicações sensíveis ao atraso (29). Os protocolos originais de camada MAC não diferenciavam quadros com diferentes prioridades, e a probabilidade de ganhar acesso ao canal era a mesma para todas as STAs (10).

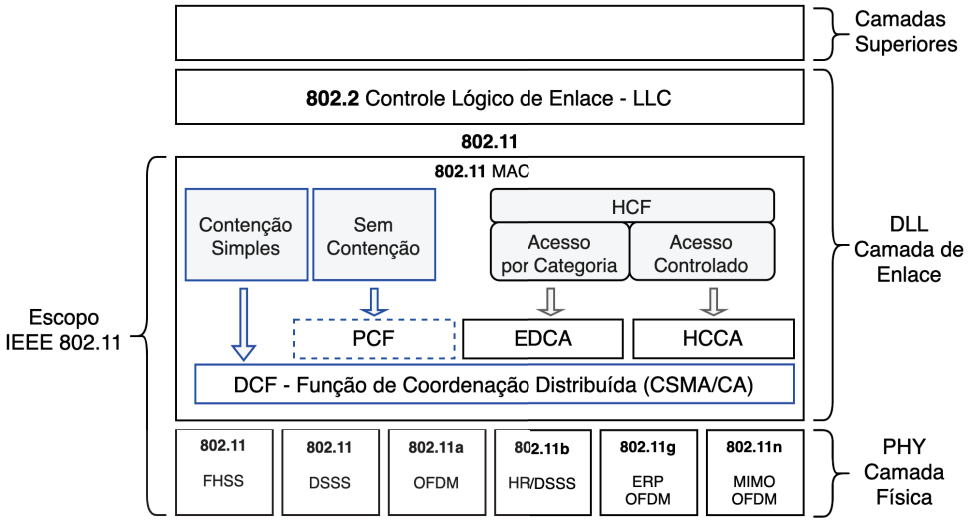
Com a finalidade de introduzir especificações de subcamada MAC para atender às aplicações com requisitos de QoS em redes sem fio, o adendo IEEE 802.11e-2005[3], incorporado ao padrão IEEE 802.11-2007[4], incluiu um novo esquema de acesso ao meio, chamado Função de Coordenação Híbrida, ou HCF (*Hybrid Coordination Function*). A HCF combina funções da DCF e PCF com mecanismos aprimorados específicos e subtipos de quadros para utilização em transmissões com requisitos de QoS (22), implementando para isso dois métodos de acesso: o Acesso ao Canal Distribuído Aprimorado, ou EDCA (*Enhanced Distributed Channel Access*), baseado em contenção, e o Acesso Controlado do Canal, ou HCCA (*HCF Controlled Channel Access*), sem contenção. O HCCA é uma versão melhorada da PCF, e também utiliza um coordenador central para gerenciar o acesso ao meio. O EDCA aprimorou o esquema básico de contenção utilizado pela DCF, permitindo a segregação do tráfego de rede em diferentes categorias, com diferentes prioridades de acesso ao meio.

A Figura 3 ilustra o relacionamento entre os protocolos definidos pela subcamada MAC, destacando-a na arquitetura IEEE 802.11. Os métodos de acesso legados do padrão, ainda suportados, estão destacadas em azul. Como pode ser observado, todos os métodos de acesso ao meio são construídos sobre a DCF. A falta de robustez da PCF contra nós ocultos resultou em uma adoção pífia pelos fabricantes, e o HCCA não é implementado em dispositivos comerciais (21), motivo pelo qual essas duas abordagens centralizadas de controle de acesso não serão discutidas mais a fundo.

Para o desenvolvimento deste trabalho, utilizamos o método de acesso EDCA, que permite priorizar o tráfego por categoria de acesso, ou AC (*Access Category*). O EDCA é implementado sobre a DCF e, portanto, esses dois métodos serão apresentados mais detalhadamente nas próximas duas sessões.

[3] https://standards.ieee.org/standard/802_11e-2005.html
[4] https://standards.ieee.org/standard/802_11-2007.html

Figura 3 – Funções de coordenação de acesso ao meio da subcamada MAC do padrão IEEE 802.11



Fonte: Adaptado de (22, 16)

2.1.3 Função de Coordenação Distribuída (DCF)

Como mencionado na Subseção **2.1.2**, a DCF é o método básico de acesso ao meio utilizado desde o lançamento do padrão 802.11. A DCF é uma função de coordenação distribuída, ou seja, não há um controle central. As STAs concordam em utilizar as mesmas regras para acessar o canal de comunicação, agindo individualmente, mas de forma coordenada. Para isso, a DCF implementa CSMA/CA como protocolo de acesso ao meio, seguindo a abordagem "ouça antes de falar", conforme os passos abaixo (22):

1. A STA verifica se o canal está livre ou ocupado. Para isso, utiliza o mecanismo de verificação de portadora, ou CS (*Carrier Sense*), que geralmente utiliza um processo de verificação físico e outro virtual. O processo físico é chamado de Verificação de Canal Livre, ou CCA (*Clear Channel Assessment*), e é utilizado para detectar ruído no meio de comunicação. O processo virtual, chamado de Vetor de Alocação de Rede, ou NAV (*Network Allocation Vector*), utiliza o campo de duração no cabeçalho MAC dos pacotes para prever se o meio está ocupado. Se a verificação determinar o canal como livre, a STA pode prosseguir.

2. Se a condição do passo 1 for satisfeita, ou seja, se o meio estiver livre, a STA aguarda por um Intervalo Entre Quadros, ou IFS (*Interframe Space*). O IFS varia de acordo com o protocolo utilizado, e será detalhado mais adiante.

3. Se o durante o passo 2 o meio continuar livre, a STA seleciona um valor aleatório chamado *backoff* (período de recuo), que deve estar no intervalo $[0, CW]$, onde CW é a Janela de Contenção, ou *Contention Window*.

4. A cada *slot* de tempo transcorrido durante o período em que o meio está livre, a STA decrementa em 1 o valor de *backoff*. A duração dos *slots* de tempo é fixada pela camada física em uso, e tem relação com os atrasos de propagação para envio e recepção de quadros na rede. Aguardar por um intervalo aleatório antes de inciar uma transmissão é importante para evitar colisões, dado que a probabilidade de colisão aumenta quando é tentado um acesso imediatamente após o canal ficar livre.

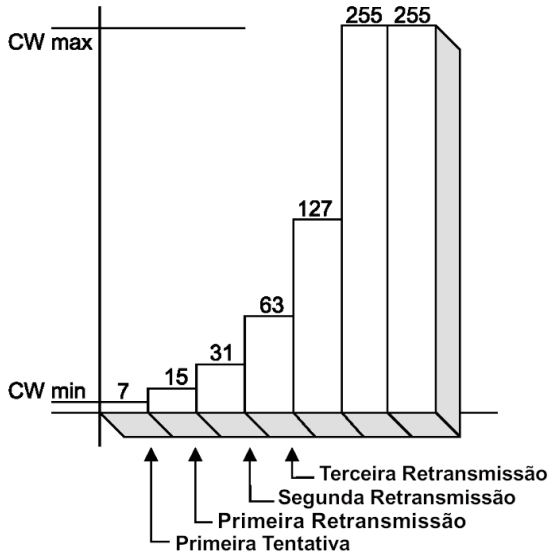
5. Se o meio sem fio for ocupado por uma transmissão concorrente durante a execução do passo 4, a STA pausa o decremento de *backoff*, executa novamente os passos 1 e 2, e então volta a decrementar o *backoff* de onde parou.

6. Quando o valor de *backoff* chega a zero, se o canal sem fio ainda estiver livre (condição do passo 1), a STA pode finalmente transmitir.

A principal característica do protocolo CSMA/CA, é a realização de *backoff* antes de uma tentativa de transmissão, reduzindo a possibilidade de que mais de uma STA ganhe acesso ao canal simultaneamente. Embora seja bastante eficiente na tarefa de evitar colisões, as complexidades inerentes ao meio sem fio não permitem que o CSMA/CA seja infalível. Quando os quadros enviados não são confirmados, supõe-se ter havido colisão no destino. Quando isso acontece, é empregado o mecanismo de *backoff* exponencial binário, onde o intervalo da janela de contenção (CW) é dobrado a cada nova tentativa de transmissão. O valor do *backoff* a ser decrementado pela STA é aleatoriamente escolhido dentre os valores do intervalo $[0, CW]$, onde CW é limitado pelos parâmetros $CWmin$ e $CWmax$, com $CWmin <= CW <= CWmax$. Esses parâmetros são especificados como potência de 2, tal que $2^n - 1$, onde n é o valor configurado para cada parâmetro. Um novo valor de *backoff* não é gerado se o valor atual for diferente de zero. Inicialmente, o valor de $CW = CWmin$, e *backoff* é um valor aleatório pertencente ao intervalo $[0, 2^{CW} - 1]$. Havendo nova falha na transmissão, o valor de CW é incrementado em 1.

A Figura 4 ilustra o processo de *backoff* exponencial binário. Inicialmente $CW = 3$ (valor de $CWmin$), então o intervalo possível para *backoff* é $[0, 2^3 - 1]$. Havendo nova tentativa de retransmissão, CW é incrementado para 4, e o novo intervalo passa a ser $[0, 2^4 - 1]$. Esse processo é repetido para cada tentativa de transmissão sem sucesso, até que CW seja igual a $CWmax$, onde se manterá até que a transmissão tenha sucesso, ou até que seja atingido o número máximo de tentativas, quando então CW é redefinido para $CWmin$ (22). É importante notar a natureza probabilística do método de acesso baseado em contenção. Apesar de CW crescer exponencialmente a cada tentativa falha de transmissão, o intervalo de possíveis valores para *backoff* será sempre um valor pertencente ao intervalo $[0, CW]$. Isso significa que, apesar de um valor maior de CW aumentar estatisticamente a possibilidade de seleção de um valor de *backoff* também maior, não impede que um *backoff* mínimo seja selecionado.

Figura 4 – Crescimento exponencial da janela de contenção (CW)



Fonte: Adaptado de (22)

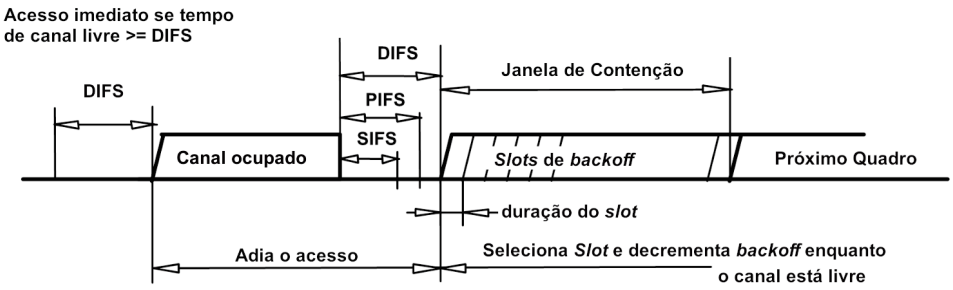
Como visto anteriormente, o intervalo entre os envios de quadros é chamado IFS, e varia conforme o método de acesso utilizado. Comum a todas as funções de coordenação, o SIFS (*Short Interframe Space*, ou Intervalo Curto Entre Quadros), é o menor entre os intervalos entre quadros, sendo usado entre quadros de controle, como ACK e CTS, assim como entre quadros MPDU de rajadas de fragmentos. O PIFS (*PCF Interframe Space*, ou Intervalo Entre Quadros PCF) é utilizado pela PCF e o DIFS (*DCF Interframe Space*, ou Intervalo Entre Quadros DCF) é utilizado pela DCF. Há ainda o EIFS (*Extended Interframe Space*, ou Espaço Estendido Entre Quadros), utilizado no lugar do DIFS após um erro de transmissão. A Figura 5 mostra o funcionamento do método básico de acesso ao meio baseado em contenção da DCF. O acesso é imediato se o canal estiver livre por um tempo superior ao IFS da DCF, ou DIFS (*DCF Interframe Space*). Se outra STA começar a utilizar o canal, o acesso é adiado, até que fique livre novamente por pelo menos um intervalo DIFS, quando a STA pode calcular um valor de *backoff* e começar a decrementá-lo.

2.1.4 IEEE 802.11e MAC

A Qualidade de Serviço, ou QoS (*Quality of Service*), se refere às garantias de desempenho estatístico que uma rede de computadores pode dar em relação a perda, atraso, *jitter* (variação do atraso) e vazão (12).

As melhorias trazidas pelo adendo 802.11e são coletivamente referenciadas no padrão como *QoS Facility*, e incluem primitivas de serviço, formatos de quadro, regras

Figura 5 – Método básico de acesso



Fonte: Adaptado de (22)

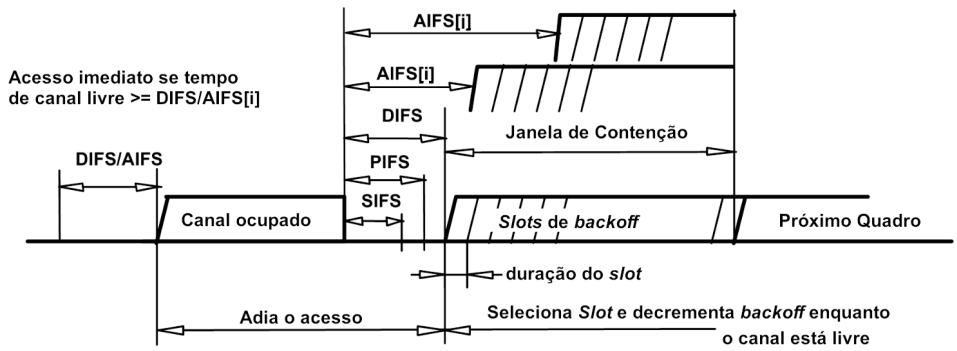
para trocas de quadros, funções de coordenação e algumas funções de gerenciamento (22). O esquema básico de contenção utilizado em redes 802.11 foi aprimorado, e em cima da DCF surgiu a EDCA, que permite segregar o tráfego de rede em quatro diferentes categorias de acesso, ou AC (*Access Category*) e, para cada categoria, definir diferentes janelas de contenção e IFS, que na EDCA são chamados AIFS (*Arbitrate Interframe Space*, ou Intervalo Arbitrário Entre Quadros). Ao definir diferentes IFS para cada AC, a EDCA melhora estatisticamente as chances de uma categoria priorizada conseguir acesso ao meio de comunicação antes das demais (21).

O mecanismo de diferenciação de tráfego utilizado pelo EDCA se baseia na variação de três fatores (53, 22): i) quantidade de tempo que um canal deve ficar livre antes que uma STA inicie procedimento de *backoff* ou transmissão; ii) o intervalo de valores possíveis para definição do recuo (janela de contenção) após erros de transmissão, ou antes de iniciar uma transmissão; iii) o tempo que uma STA pode transmitir após conseguir acesso ao canal de comunicação. A Figura 6 mostra a relação entre os IFS depois da atualização introduzida do IEEE 802.11e, em comparação com os IFS mostrados na Figura 5. O AIFS corresponde a $AIFSN[AC] \times aSlotTime + aSIFSTime$. Assim, uma fila com valor $AIFS = 2$ deverá aguardar 2 *slots* de tempo após um intervalo SIFS antes de iniciar o processo de *backoff* ou transmissão.

Para diferenciar o tráfego, a EDCA mapeia 8 UPs (*User Priorities*, ou prioridades de usuários) para 4 ACs: AC_VO (voz), AC_VI (vídeo), AC_BE (melhor esforço) e AC_BK (tráfego de fundo). As 8 UPs, com valores de 0 a 7, são idênticas às definidas no padrão 802.1D, e correspondem aos 3 primeiros bits (precedência IP) do campo DSCP (*Differentiated Services Code Point*) do cabeçalho IP (12). O mapeamento entre UPs e ACs é mostrado na Tabela 1. Importante notar que a UP 0 é mapeada para AC_BE por questões de compatibilidade, garantindo que quadros com marcações antigas sejam entregues por melhor esforço.

Cada AC mantém uma fila própria para o tráfego associado a ela, e executa sua própria função EDCA, com diferentes parâmetros para acesso ao meio. Possíveis colisões

Figura 6 – Relação entre os IFS



Fonte: Adaptado de (22)

Tabela 1 – Mapeamento UP para AC

Prioridade	UP (mesmas do 802.1D)	Designação 802.1D	AC	Categoria
Menor ↓ Maior	1	BK	AC_BK	Tráfego de Fundo
	2	–	AC_BK	Tráfego de Fundo
	0	BE	AC_BE	Melhor esforço
	3	EE	AC_BE	Melhor esforço
	4	CL	AC_VI	Vídeo
	5	VI	AC_VI	Vídeo
	6	VO	AC_VO	Voz
	7	NC	AC_VO	Voz

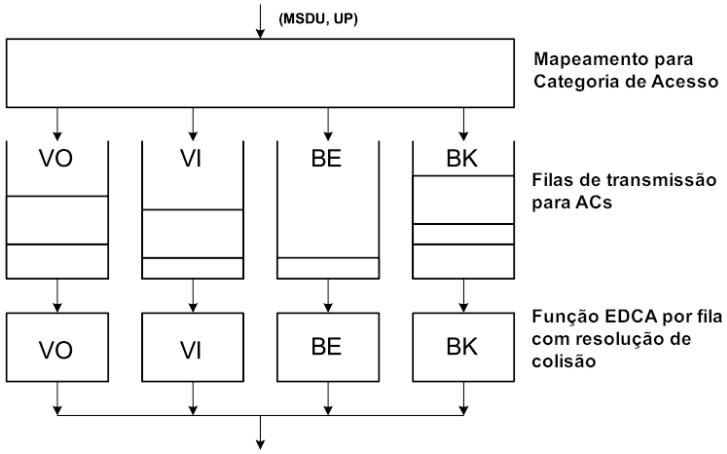
Fonte: Adaptado de (22)

entre as filas são tratadas internamente, ou seja, caso o *backoff* de duas filas chegue a zero ao mesmo tempo, ganha acesso ao meio a fila da categoria mais prioritária. A Figura 7 mostra o funcionamento do acesso diferenciado por ACs.

A Tabela 2 apresenta os parâmetros EDCA utilizados por padrão em cada AC. O campo TXOP (*Transmission Opportunity*, ou Oportunidade de Transmissão) é expresso em milissegundos, em valores múltiplos de 32 μs. Os valores padrões para aCWmin e aCWmax em redes 802.11g são, respectivamente, 15 e 1023, ou, em forma exponencial, 4 e 10.

Para atualizar os parâmetros EDCA nas STAs, o AP envia um elemento de conjunto de parâmetros EDCA (EDCA *parameter set element*) em quadros de sinalização (*beacons*) e em todos os quadros de resposta de investigação (*Probe Response*) e resposta a pedido de associação (*Association Response*) e reassociação (*Reassociation Response*). A Subseção **2.1.1** descreve o papel desses quadros no processo de associação entre STAs e APs em uma rede sem fio configurada no modo infraestrutura. Ao receber um elemento

Figura 7 – Categorias de acesso EDCA



Fonte: Adaptado de (22)

Tabela 2 – Valores padrões para parâmetros EDCA

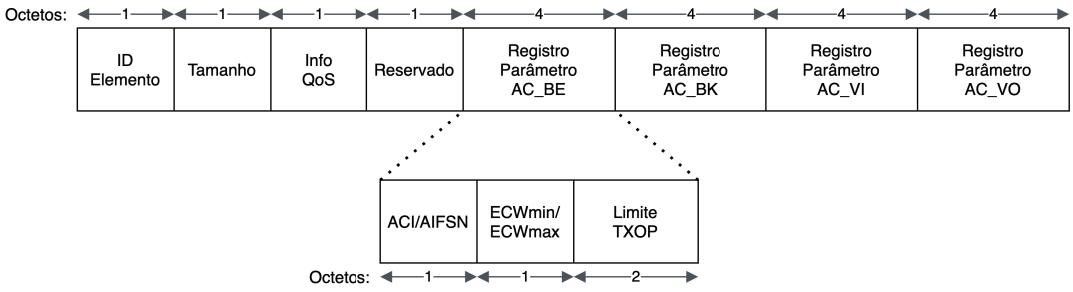
AC	**CWmin**	**CWmax**	**AIFSN**	**TXOP**
AC_BK	aCWmin	aCWmax	7	0
AC_BE	aCWmin	aCWmax	3	0
AC_VI	(aCWmin+1)/2 – 1	aCWmin	2	3008 ms
AC_VO	(aCWmin+1)/4 – 1	(aCWmin+1)/2 – 1	2	1504 ms

Fonte: (22)

EDCA a STA atualiza os parâmetros em sua MIB (*Management Information Base*, ou Base de Informações de Gerenciamento). A Figura 8 mostra o formato do elemento EDCA. O campo Info QoS mantém, dentre outras informações, um contador de atualizações de parâmetros EDCA. As STAs utilizam esse contador para determinar se seus parâmetros estão atualizados, comparando-o com um contador de atualizações próprio. Os parâmetros de cada AC são informados em um campo de 32 bits, onde o primeiro octeto informa o índice da categoria de acesso (ACI) e seu valor AIFS. O segundo octeto armazena o valor no formato exponencial de CWmin nos 4 primeiros bits e o de CWmax nos 4 últimos. O terceiro e o quarto octetos são destinados ao tempo que a AC poderá utilizar o meio após conseguir o acesso (oportunidade de transmissão).

Ainda antes da retificação do padrão 802.11e, a pressão pela adoção de QoS em redes sem fio levou a *Wi-Fi Alliance* a padronizar e introduzir para o mercado uma variação do EDCA chamada WMM (*Wi-Fi Multimedia*) (21, 59), ou WME (*Wireless Multimedia Extensions*). No WMM, o valor UP é deduzido a partir dos valores de 0 a 7 do campo TID (*Traffic Identier*, ou Identificador de Tráfego). Valores entre 8 e 15 especificam requisitos de tempo de transmissão (TXOP). A Figura 9 mostra um *beacon* capturado com

Figura 8 – Elemento de conjunto de parâmetros EDCA



Fonte: Adaptado de (22)

o Wireshark[5] na rede utilizada no experimento, destacando as informações para AC_VO no *WMM Parameter Element*.

Figura 9 – Elemento de conjunto de parâmetros WMM

```
IEEE 802.11 wireless LAN
  Fixed parameters (12 bytes)
  Tagged parameters (176 bytes)
    Tag: SSID parameter set: SDWN
    Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
      Tag Number: Vendor Specific (221)
      Tag length: 24
      OUI: 00:50:f2 (Microsoft Corp.)
      Vendor Specific OUI Type: 2
      Type: WMM/WME (0x02)
      WME Subtype: Parameter Element (1)
      WME Version: 1
      WME QoS Info: 0x00
      Reserved: 00
      Ac Parameters ACI 0 (Best Effort), ACM no, AIFSN 3, ECWmin/max 4/10 (CWmin/max 15/1023), TXOP 0
      Ac Parameters ACI 1 (Background), ACM no, AIFSN 7, ECWmin/max 4/10 (CWmin/max 15/1023), TXOP 0
      Ac Parameters ACI 2 (Video), ACM no, AIFSN 2, ECWmin/max 3/4 (CWmin/max 7/15), TXOP 94
      Ac Parameters ACI 3 (Voice), ACM no, AIFSN 1, ECWmin/max 0/1 (CWmin/max 0/1), TXOP 47
```

Fonte: Elaborado pelo autor (2021)

2.2 REDES DE ÁREA CORPORAL SEM FIO (WBANs)

O aumento da expectativa de vida em muitos países desenvolvidos leva ao envelhecimento da população, o que resulta na sobrecarga dos sistemas de saúde e afeta a qualidade de vida das pessoas. Além disso, o crescente aumento nos gastos desses países com saúde representa uma ameaça para suas economias (44), evidenciando a necessidade de se aperfeiçoar os sistemas de saúde atuais para que se tornem mais escaláveis e acessíveis.

Sensores miniaturizados, que podem ser utilizados interna ou externamente ao corpo humano (52), são capazes de monitorar sinais vitais e enviar os dados coletados a um centro médico para processamento e análise. Sistemas de monitoramento de sinais vitais, como (38), (18) e (35), podem alertar para alterações bruscas no estado de saúde

[5] https://www.wireshark.org/

do paciente, notificando familiares, médicos e o serviço de emergência. Os dados coletados pelos sensores podem ser analisados por sistemas capazes de prever a proximidade de um evento crítico, como é feito em (61), possibilitando um socorro mais imediato e a redução do risco de morte ou sequelas graves para o paciente.

As Redes Corporais Sem Fio, ou WBANs (*Wireless Body Area Networks*), são um ramo das Redes de Sensores Sem Fio, ou WSNs (*Wireless Sensor Networks*), e são compostas por sensores e atuadores sem fio miniaturizados, de curto alcance e baixo consumo energético, que podem ser invasivos ou não invasivos (9). Publicado em 2012, o padrão IEEE 802.15.6[6] foi projetado especificamente para comunicação sem fio de curto alcance internamente ao nas proximidades do corpo humano, mas não limitado a humanos (24). Além do IEEE 802.15.6, outras soluções de comunicação utilizadas como referência em redes de sensores sem fio são o IEEE 802.15.4 (Zigbee) e BLE (*Bluetooh Low Energy*, ou Bluetooh de baixo consumo) (9).

2.2.1 Aplicações de WBANs

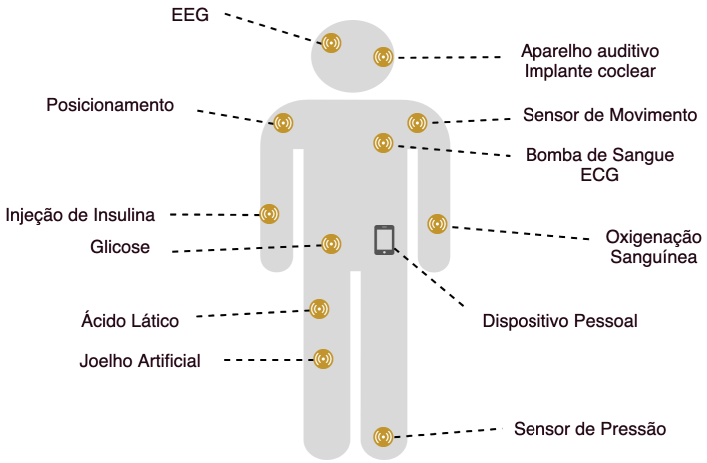
Como WBANs são capazes de prover interconexão entre vários dispositivos implantados no corpo ou montados em sua superfície, suas aplicações incluem acompanhamento pós-tratamento, pesquisas farmacêuticas, tratamento de traumas, pesquisas sobre doenças crônicas, etc. O padrão IEEE 802.15.6 categoriza as aplicações WBANs apenas em médicas e não médicas, sendo a melhoria da qualidade de vida do usuário a principal característica comum a todas elas. São vários os possíveis usos em diferentes áreas além da médica, como entretenimento, emergência não médica (e.g. detecção de incêndio, vazamento de gás), entre outros. A Figura 10 apresenta exemplos de sensores sem fio vestíveis e implantáveis tipicamente utilizados para o monitoramento de pacientes, e a Figura 11 mostra algumas aplicações para WBANs subdivididas em médicas e não médicas.

Todo ano muitas pessoas morrem de câncer, doenças cardiovasculares, asma, mal de Parkinson, obesidade, diabetes, etc. Um problema comum à essas doenças fatais é que muitas pessoas só experienciam sintomas e obtém um diagnóstico quando já é tarde. Pesquisas mostram que muitas doenças podem ser evitada se forem detectadas nos estágios iniciais (44, 28), caso em que sistemas de monitoramento de saúde em tempo real podem ser de grande ajuda.

Sensores implantáveis ou vestíveis são utilizados para medir e reportar sinais vitais do paciente, como frequência de batimentos cardíacos, temperatura corporal, pressão sanguínea, nível de glicose no sangue, nível de oxigenação, etc. Variações bruscas nessas medições podem ser respondidas com intervenção médica imediata. Além disso, a análise do histórico desses indicadores pode ajudar a identificar doenças em estágios iniciais. Um exemplo de aplicação médica é o tratamento para pessoas com diabetes, uma doença que

[6] https://standards.ieee.org/standard/802_15_6-2012.html

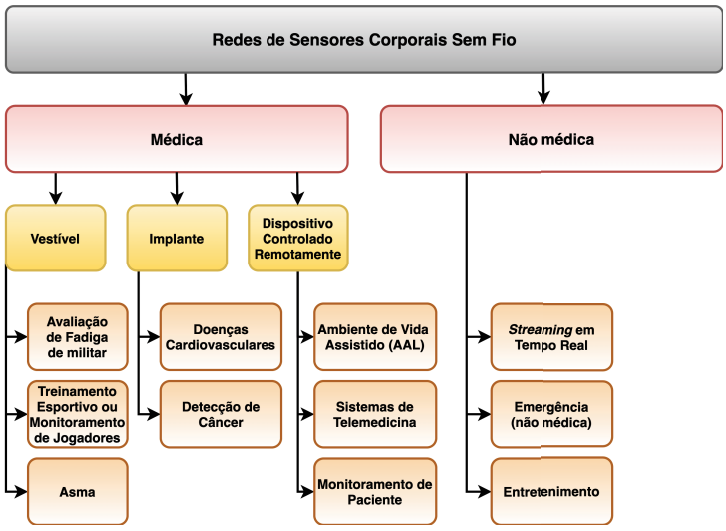
Figura 10 – Exemplo de sensores biomédicos em uma WBAN.



Fonte: Adaptado de (32).

afeta mais de 246 milhões de pessoas no mundo. A atuação conjunta de um nó sensor e um nó atuador para o monitoramento constante do nível de glicose, e a administração da dose correta de insulina, reduzem riscos de desmaios, cegueira na vida adulta, perda de circulação e outras complicações (32).

Figura 11 – Aplicações WBAN



Fonte: Adaptado de (28)

Alguns desafios são comuns às WBANs utilizadas em contexto médico, devido à proximidade com o corpo humano. O tecido corporal absorve radiação quando exposto aos campos eletromagnéticos gerados pelas ondas de radiofrequência emitidas pelos nós da WBAN, podendo inclusive sofrer danos devido ao calor resultante. Por isso, os efeitos de aquecimento localizado (regiões onde há maior exposição à radiação) e absorção de radiação, são os tópicos mais importantes a serem analisados em relação à comunicação

sem fio dentro do corpo ou ao seu redor (44). A quantidade de energia absorvida pelo tecido é expressa em termos da Taxa de Absorção Específica, ou SAR (*Specific Absorption Rate*), medida em watts por kilograma (W/kg), e deve cumprir restrições estabelecidas por regulamentos internacionais ou regionais (9). Além da redução de calor gerado, a necessidade de menor consumo de energia pelos nós da WBAN se deve também à limitação da fonte de energia que eles possuem, devido ao tamanho miniaturizado das baterias utilizadas. Não é viável recarregar ou substituir sensores WBANs, especialmente se forem implantados (44), caso em que é necessário procedimento cirúrgico. Por isso, protocolos de roteamento, segurança e transmissão de dados, precisam ser especialmente pensados para atingirem melhor eficiência energética (28).

2.2.2 Estrutura WBANs

Os nós em uma WBAN são classificados de acordo com sua funcionalidade, implementação e função na rede. Quanto à funcionalidade, a classificação se dá em (32, 44):

- **Dispositivo Pessoal**: Também conhecido como *hub*, *gateway*, servidor pessoal (*personal server*), nó coletor (*sink*) ou unidade de controle corporal (*Body Control Unit - BCU*), esse dispositivo junta todas as informações obtidas pelos sensores e atuadores e informa ao usuário via um *gateway* externo, atuador, ou visor/LED. É composto por uma unidade de energia, processador (maior), memória e transceptor. Em algumas aplicações, um *smartphone* pode ser utilizado.

- **Nó sensor**: Pode ser interno ou externo ao corpo. Monitora e responde a estímulos físicos, reportando os dados por um canal sem fio. Estes sensores podem ser fisiológicos, de ambiente ou biocinéticos. Esse dispositivo consiste em um *hardware* sensor, uma unidade de energia, um processador, memória e um transmissor ou transceptor.

- **Nó atuador**: Age com base nos dados recebidos dos sensores, ou em alguma interação do usuário. Os componentes dos nós atuadores são parecidos com os dos nós sensores, com a alteração do *hardware* sensor pelo *hardware* atuador. Esse *hardware* pode ter a finalidade, por exemplo, de injetar a dosagem correta de medicamento no corpo, e para isso possui um reservatório para armazenamento de medicamento.

Quanto à implementação, a classificação dos nós proposta pelo IEEE 802.15.6 se dá em (1):

- **Nó implantado (*in-body*)**: Inserido no corpo humano, seja imediatamente sob a pele ou dentro do tecido corporal.

- **Nó de superfície corporal (*on-body*)**: Montado na superfície do corpo humano, ou a 2 centímetros de distância dele.

- **Nó externo (*off-body*)**: Não tem contato com o corpo humano, podendo estar a uma distância entre alguns centímetros e 5 metros dele.

A classificação dos nós quanto à sua função na rede se dá em (44):

- **Coordenador (*coordinator*)**: Nó através do qual os demais nós se comunicam, atuando como um *gateway* para o mundo externo.

- **Nó final (*end node*)**: Nó limitado a executar sua aplicação embarcada. Não retransmite informações de outros nós, comunicando-se apenas com o nó coordenador.

- **Nó retransmissor (*relay node*):** Um nó retransmissor fica entre um nó final e o coordenador, ou seja, é um nó intermediário, capaz de retransmitir informações. Pode atuar também como sensor.

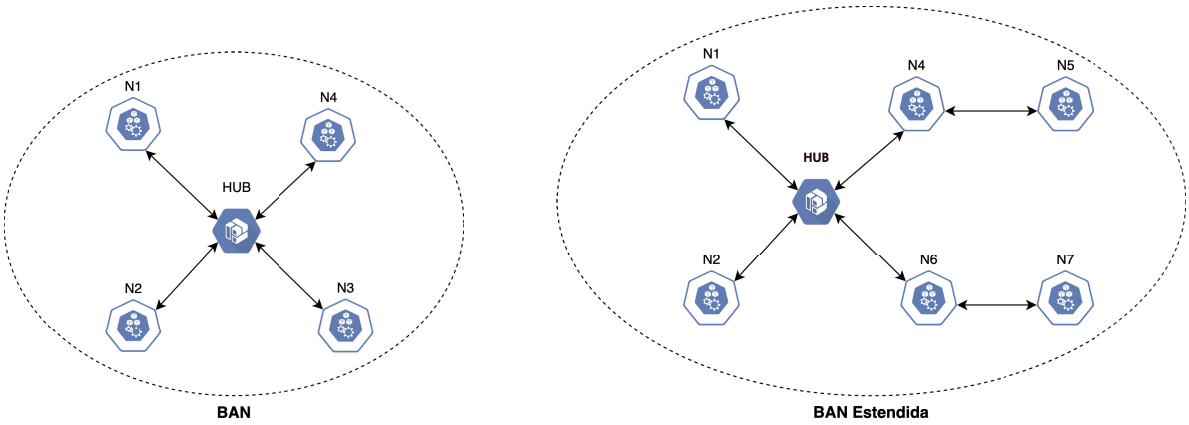
2.2.3 Topologia WBAN

Uma WBAN pode operar em uma topologia estrela de um ou dois saltos (24). Múltiplos saltos causam *overhead* na rede e aumentam sua complexidade. Sistemas proprietários podem utilizar mais de dois saltos, mas com isso incorrem em problemas de interoperabilidade, por fugirem às definições do padrão (44). Todos os nós são coordenados por um único nó central, responsável por gerenciar o acesso ao meio e o consumo de energia (24). Na topologia de um salto, mostrada na Figura 12(a), não há nós retransmissores (ou *relays*), e todos os nós se comunicam diretamente com o nó coordenador, o que reduz o *overhead* da rede e o atraso de transmissão. Contudo, caso o nó esteja mais distante do coordenador, maiores potências de transmissão precisarão ser utilizadas, o que resultará em um maior gasto de energia e maior acúmulo de calor ao redor do nó transmissor. Na topologia estendida de dois saltos, mostrada na Figura 12(b), há um nó intermediário entre o nó final e o nó coordenador. Menores potências de transmissão são empregadas, e há uma melhor distribuição do calor gerado ao redor do nó transmissor. Em contrapartida, o atraso observado é maior (44).

2.2.4 Arquitetura de comunicação das WBANs

A arquitetura de comunicação das WBAN pode ser separada em três diferentes níveis (44, 2, 28). O nível **Intra-BAN** compreende os sensores e atuadores, e engloba questões relacionadas ao projeto desses dispositivos, além da confiabilidade, QoS, eficiência energética, etc., na comunicação entre eles e o dispositivo pessoal. Este nível é também chamado de “Sensores”. O nível **Inter-BAN** compreende as funcionalidades do dispositivo

Figura 12 – Topologia WBAN



(a) Topologia estrela de um salto

(b) Topologia estrela estendida de dois saltos

Fonte: Adaptado de (24)

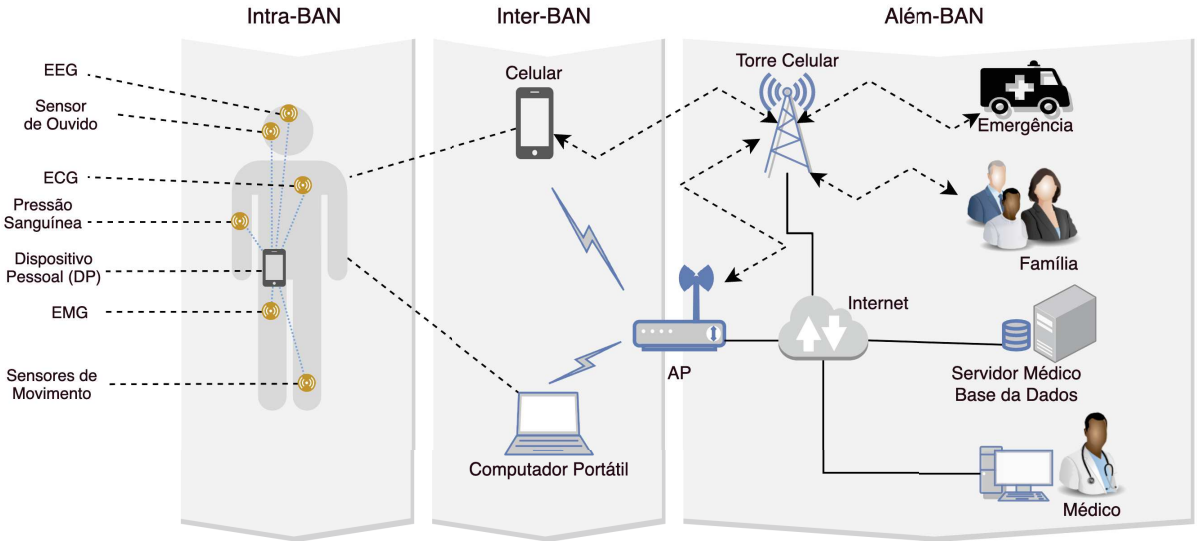
pessoal, responsável por coletar, processar, agregar e comunicar informações recebidas dos sensores (7). Este nível engloba questões relacionadas à comunicação da WBAN com outras redes (inclusive outras WBANs) através de diferentes tecnologias de rede sem fio, como WLANs e redes celulares. É, por isso, também chamado de *"Gateway"*. O nível **Além-BAN** foi projetado para comunicação em redes metropolitanas (28, 44), e seu principal componente é a base de dados. Também chamado de "Servidor", este nível é dependente da aplicação, e no caso de aplicações médicas, compreende o Servidor Médico Central, cuja base de dados inclui o histórico médico e perfil dos pacientes.

A comunicação entre **Intra-BAN** e **Além-BAN** também depende da aplicação. Por exemplo, em aplicações médicas, o dispositivo pessoal pode se comunicar com o servidor médico central através de um AP, ou pode usar diretamente a rede celular para notificar a família do paciente e o serviço de emergência sobre ocorrência de alguma situação grave. A Figura 13 mostra os níveis da arquitetura de comunicação de WBANs em sistemas médicos, bem como o relacionamento entre eles.

2.3 REDES DEFINIDAS POR SOFTWARE

Tradicionalmente, as redes de computadores são compostas por diversos elementos de rede fabricados por diferentes fornecedores, com diferentes capacidades de transmissão e processamento (12). Um comutador de pacotes recebe um pacote em uma de suas portas e o direciona a uma de suas outras portas, seguindo para isso uma tabela que associa cada porta do comutador ao endereço MAC do dispositivo a ela conectado. Essa tabela é conhecida como CAM (*Content Addressable Memory*), tabela de encaminhamento de camada 2, ou simplesmente tabela de endereços MAC, e fica armazenada em memória RAM, o que torna sua consulta bastante rápida. Quando não há uma entrada correspondente na

Figura 13 – Camadas de comunicação WBAN



Fonte: Adaptado de (44, 52)

tabela MAC o comutador faz uma difusão do pacote, enviando-o para todas as portas, exceto para a de origem. O *host* de destino responde, e então o comutador grava na tabela MAC o endereço de origem do pacote de resposta, de forma que da próxima vez saiba exatamente para qual porta encaminhar um pacote com o mesmo endereço MAC de destino. O comutador pode, ainda, classificar o quadro de acordo com políticas pré-definidas como, por exemplo, associando uma porta a uma VLAN definida pelo administrador.

Conceitualmente, é possível identificar duas partes em um dispositivo de rede: o **plano de controle**, onde são configuradas as políticas para classificação de pacotes, e o **plano de dados**, onde os pacotes são comutados, ou encaminhados, segundo essas políticas (12). A fabricação tradicional de equipamentos de rede segue uma abordagem vertical, que integra fortemente os planos de controle e dados, de forma que o mesmo dispositivo é responsável por classificar e encaminhar pacotes, dificultando uma administração global e centralizada da rede.

Parte crítica da infraestrutura de empresas, casas e escolas, redes de computadores são atualmente uma enorme base instalada de equipamentos e protocolos, e por isso são comumente complexas e heterogêneas (37), compostas por equipamentos fornecidos por diversos fabricantes. Uma estrutura como essa tem alto custo administrativo, dado que exige pessoal treinado para mantê-la. Muitas vezes, novas configurações e políticas precisam ser aplicadas individualmente, exigindo familiaridade com uma *interface* de gerenciamento própria do equipamento.

Erros de configuração são muito comuns nas redes atuais. A partir de um único roteador mal configurado, muitos problemas podem surgir, como perdas de pacotes, *loops*

de encaminhamento, rotas de rede indesejáveis, entre outras coisas. De fato, apesar de raro, um único roteador mal configurado pode ser responsável por comprometer o funcionamento da Internet por horas (30).

Essas características tornam as redes IP tradicionais, além de difíceis de gerenciar, pouco flexíveis. Isso dificulta o estudo e desenvolvimento de novos protocolos de rede, visto que há uma relutância em realizar experimentos com tráfego de produção (58). Assim, novas ideias da comunidade científica muitas vezes não podem ser experimentadas em ambientes suficientemente realistas, com tráfego real. Para tentar solucionar esse problema, a comunidade de redes começou a trabalhar no desenvolvimento de topologias de redes virtualizadas, que visavam utilizar *switches* e roteadores programáveis que empregam virtualização para processar separadamente pacotes de múltiplos experimentos. Contudo, considerando o alto custo e tempo de implementação esperado para a disponibilização desse tipo de infraestrutura, surgiu a necessidade de pensar em uma forma de utilizar a infraestrutura existente em um campus universitário para realizar esses experimentos (37).

2.3.1 Definição de SDN

Originado em 2008 como um experimento acadêmico, o padrão *OpenFlow* foi especificado com o objetivo de possibilitar aos pesquisadores executarem protocolos de rede experimentais em redes de produção (37). O interesse da comunidade de redes pelo *OpenFlow* levou ao desenvolvimento de novas pesquisas e trabalhos, dando origem mais tarde ao termo SDN (30). A abordagem SDN simplifica a arquitetura de rede, quebrando a integração vertical entre os planos de dados e controle. A mudança fundamental introduzida pelo paradigma SDN foi a de conceder ao administrador de rede o controle sobre dispositivos de encaminhamento, antes exercido exclusivamente pelos fabricantes, permitindo ao administrador programar sua própria rede (50). A indústria muitas vezes se refere a qualquer arquitetura de rede que contenha software como SDN, mas uma definição menos ambígua é dada por Kreutz et al., onde SDN é uma arquitetura de rede com quatro pilares (30):

1. Os planos de dado e controle são separados, e a lógica de controle é retirada do comutador, que passa a funcionar como um simples dispositivo para encaminhamento de pacotes.

2. Regras de encaminhamento são baseadas em fluxos, e não em destinos de pacotes. Cada fluxo é resultado da filtragem de uma combinação de valores de campos dos pacotes, e é associado a um conjunto de ações a serem executadas para pacote que case com o filtro. Um pacote que não case com as regras de filtragem de nenhum fluxo pode ser descartado ou enviado ao controlador para análise. Ao receber o pacote, o controlador pode aplicar alguma lógica específica da aplicação para definir como

tratar futuros pacotes que pertençam ao mesmo fluxo, instalando uma nova regra no comutador. A abstração em fluxos permite tratar de forma única os dispositivos subjacentes da rede, sejam eles *switches*, roteadores, *firewalls* ou *middleboxes*[7]. A programação de fluxos traz muita flexibilidade ao gerenciamento da rede, limitando-se apenas à capacidade das tabelas de fluxos implementadas.

3. Como o dispositivo passa apenas a encaminhar pacotes com base em sua tabela de fluxos, a lógica de controle é movida para uma entidade externa, o controlador SDN, também conhecido como Sistema Operacional de Rede, ou NOS (*Network Operating System*). O controlador utiliza um canal seguro de comunicação para consultar e alterar configurações dos comutadores de rede, reunindo os recursos e abstrações necessários para programaticamente controlar os comutadores de pacotes com base em uma visão logicamente centralizada, abstrata e global da rede.

4. A rede é programável através do uso de aplicações que são executadas no controlador, que por sua vez interage com os dispositivos subjacentes, modificando seu comportamento. Essa é a principal característica da SDN. Comutadores de rede antes configurados de forma estática e limitada, podem então ser programados de forma dinâmica, respondendo ao estado da rede. O controle logicamente centralizado e com visão global da rede, além de reduzir a possibilidade de erros ao permitir a modificação de políticas de rede através de componentes de software e linguagens de alto nível, possibilita o desenvolvimento de serviços, funções de rede e aplicações mais sofisticados.

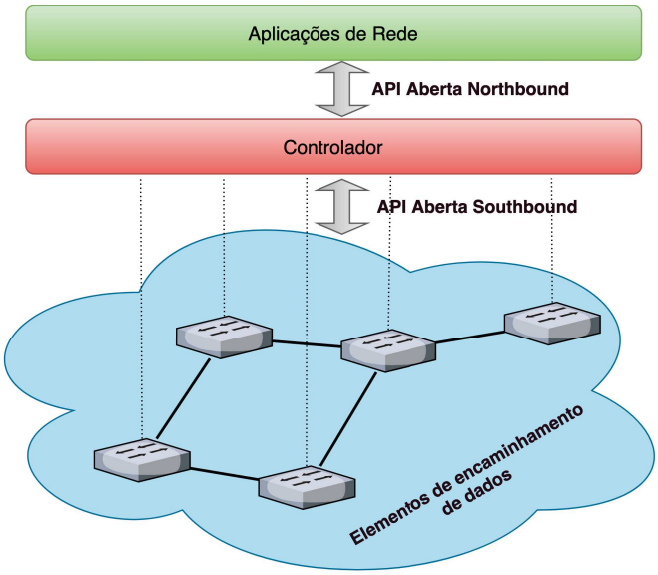
2.3.2 Arquitetura SDN

A Figura 14 apresenta uma visão simplificada da arquitetura SDN. O plano de dados é toda a infraestrutura de equipamentos de rede responsáveis por encaminhar pacotes. O plano de controle é centralizado no controlador de rede, responsável por configurar em cada comutador os encaminhamentos de pacotes de acordo com políticas de rede definidas. O controlador gerencia os comutadores de pacotes por meio de uma Interface de Programação de Aplicações, ou API (*Application Programming Interface*). Na Figura 14, essa API é descrita como *Open southbound API*, cujo exemplo mais notório é o *OpenFlow*. As aplicações de rede utilizam os serviços disponibilizados pela *Open Northbound API*, provida pelo controlador, para alterar configurações dos elementos do plano de dados e modificar o estado da rede.

A Figura 15 apresenta uma comparação entre redes tracionais e redes SDN. Enquanto em redes tradicionais os *middleboxes* precisam ser instalados e configurados indi-

[7] Um *middlebox* é um dispositivo de rede que executa outras funções que não o encaminhamento de pacotes. Exemplos de *middleboxes* são os *firewalls*, tradutores de endereços de rede (NAT), balanceamento de carga e caixas de inspeção profunda de pacotes (DPI).

Figura 14 – Visão simplificada da arquitetura SDN



Fonte: Adaptado de (30)

vidualmente, na abordagem SDN eles podem ser implantados como aplicações de rede. Essas aplicações utilizam a API disponibilizada pelo controlador SDN para programar os elementos de encaminhamento de rede, para que reproduzam o comportamento desejado, podendo atuar como roteador, *firewall*, *switch*, etc.

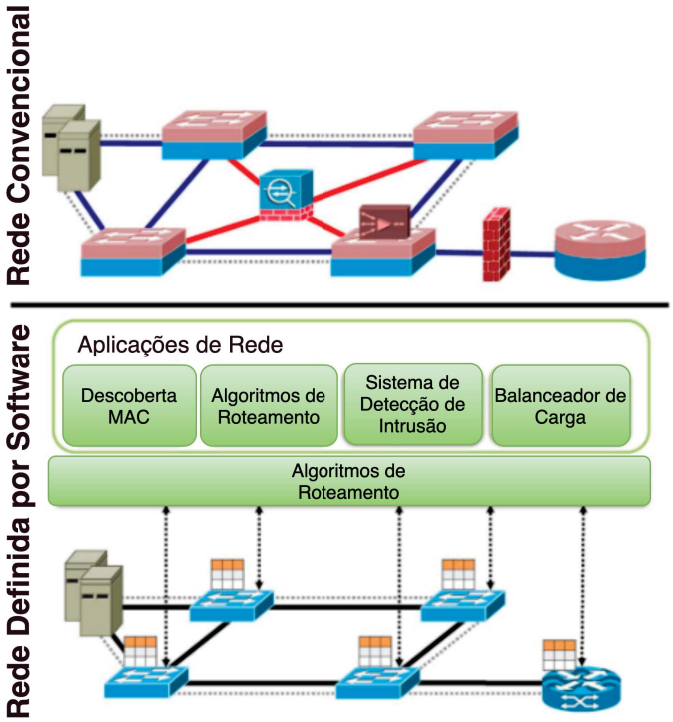
2.3.3 O Protocolo *OpenFlow*

O padrão *OpenFlow* especifica um protocolo para encaminhamento de decisões de controle aos dispositivos do plano de dados, através do qual o controlador manipula as tabelas de fluxos existentes nos comutadores de pacotes (30). Exemplo mais notável de API *Southbound* para SDN, o *OpenFlow* esconde as complexidades de *hardware* de rede subjacente e expõe um conjunto de funções para programação de *switches*.

Muitos *switches* e roteadores Ethernet atuais possuem tabelas de fluxos construídas a partir da TCAM (*Ternary Content Addressable Memory*, ou Memória Ternária de Conteúdo Endereçável). Apesar da implementação da tabela de fluxos variar conforme o fornecedor, a maioria dos *switches* comerciais possui um conjunto comum de funções básicas, o que foi um ponto-chave para a criação do *OpenFlow* (37).

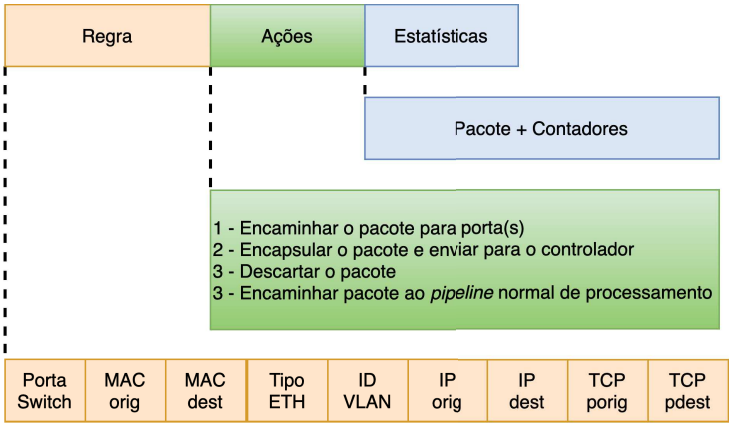
Cada entrada da tabela de fluxos possui três partes, conforme ilustrado na Figura 16: 1) regras para filtragem de pacotes; 2) ações a serem executadas para pacotes que casarem com as regras; 3) contadores para manter estatísticas para pacotes que casem com as regras. As regras são construídas com base nos campos do cabeçalho do pacote, e as ações definem se o pacote deverá ser enviado a alguma porta específica do comutador, encaminhado ao controlador, encaminhado ao fluxo normal de processamento ou descartado (30).

Figura 15 – Comparação entre rede tradicional e SDN



Fonte: Adaptado de (30)

Figura 16 – Uma entrada da tabela de fluxo de um *switch OpenFlow*



Fonte: Adaptado de (30)

Grandes fabricantes, como HP, IBM, Juniper, Huawey, Extreme e CISCO oferecem *switches* e roteadores compatíveis com *OpenFlow* (26, 30), e além disso *switches OpenFlow* podem coexistir com *switches* tradicionais, facilitando uma adoção gradual. Além disso, existem também comutadores em *software* com suporte a *OpenFlow*, sendo o *Open vSwitch* (49) o exemplo mais notório. O *Open vSwitch* possibilita automação da rede por meio de extensões programáveis, além de suportar protocolos e *interfaces* de gerenciamento

padrões.

2.4 REDES SEM FIO DEFINIDAS POR SOFTWARE (SDWN)

A separação do plano de dados do plano de controle, a centralização lógica (embora fisicamente distribuída) do plano de controle e a visão global da rede oferecidas pela abordagem SDN, facilitam a introdução de inovações de rede. Muitos são os trabalhos desenvolvidos nessa área (8, 37, 58, 48). Inicialmente pensada para aplicação em comutadores de pacotes de redes cabeadas, a ideia de desacoplar o plano de controle do plano de dados e utilizar controladores de rede programáveis para ajustar os parâmetros de operação da rede sem fio deu origem ao conceito de SDWN (*Software Defined Wireless Networks*, ou Redes Sem Fio Definidas por Software) (36). O plano de dados em SDWN é composto por dispositivos de qualquer tipo de rede sem fio, como WLANs (que são o foco deste trabalho), redes celulares, redes *mesh* ou redes de sensores sem fio (54).

Muitos são os benefícios de se adotar a abordagem SDN para redes sem fio. O controlador SDWN possui uma visão global da rede, e permite que o administrador a programe a partir de um ponto central para alterar o comportamento dos fluxos de dados conforme as necessidades das aplicações, ao mesmo tempo que mantém a configuração de parâmetros de rede consistente entre os diversos APs. Além disso, o desenvolvimento de software para controladores não depende de dispositivos específicos, o que resulta em independência de fabricantes e permite heterogeneidade entre os dispositivos de rede sem fio. Essas características trazem diversas vantagens, como o gerenciamento eficiente da rede, possibilidade de aplicar técnicas de engenharia de tráfego, melhor alocação de recursos, facilidade de monitoramento, redução de problemas de interferência, integração de infraestruturas heterogêneas, etc. (54).

As especificidades das redes sem fio 802.11 WLAN, como características variáveis do meio de comunicação, mobilidade dos nós, dificuldades de se garantir QoS e segurança, dificultam que sejam adotados para elas conceitos propostos pelo paradigma SDN e pelo *OpenFlow*. (42). Os padrões de tráfego variam rapidamente, exigindo que o controlador se adapte à essas mudanças, o que aumenta o *overhead* na rede. No intuito de resolver muitas dessas questões, algumas arquiteturas SDWN foram propostas pela comunidade científica (5, 34, 33, 41).

3 TRABALHOS RELACIONADOS

As diversas possibilidades de aplicação para as WBANs despertaram o interesse da comunidade científica para o desenvolvimento de estudos que buscam solucionar problemas inerentes à essas redes (44). O potencial das WBANs de revolucionar os serviços de saúde faz com que as aplicações médicas sejam um tópico bastante promissor, mas com alguns desafios importantes a serem superados. A otimização dos sensores sem fio, alta variabilidade de taxas de transmissão, necessidade de uso eficiente de fontes limitadas de energia, necessidade de satisfazer requisitos de QoS para aplicações de tempo real, privacidade e segurança dos dados sensíveis que trafegam por essas redes, interferência de sinais sem fio propagados por redes próximas e problemas de roteamento são alguns desses desafios (1, 32, 44).

A arquitetura de comunicação das WBANs compreende três níveis. O nível Intra-BAN abrange questões relacionadas aos sensores sem fio e à comunicação entre eles e o coordenador WBAN, ou dispositivo pessoal. O nível Inter-BAN abrange questões relacionadas ao processamentos dos dados da WBANs pelo dispositivo pessoal, bem como a comunicação com outras redes, sejam elas outras WBANs, WLANs, redes celulares, etc. O nível Além-BAN tem como principal componente a base de dados do sistema e, em aplicações médicas, o Servidor Médico Central. Os autores em (2) relacionam os estudos desenvolvidos na área de WBAN com esses três níveis, dividindo-os em: i) baseados em sensor; ii) baseados em *gateway*; iii) baseados em servidor médico central.

Alguns trabalhos propõem sistemas de monitoramento e suporte à saúde completos, que atuam nos três níveis de comunicação. Esses sistemas monitoram sinais vitais de pacientes através de sensores corporais, processam esses dados no dispositivo pessoal, e os enviam ao servidor médico central para armazenamento e análise. Também emitem alertas quando uma situação crítica de saúde é detectada, podendo contactar serviços de emergência, equipe médica, familiares, ou uma combinação destes.

O *eCardio*, proposto por (38), tem foco em pessoas idosas, e sua arquitetura é composta por um celular (*eCardio Terminal*), um sensor cardíaco (*eCardioMeter*) e um servidor médico remoto. O *eCardio Terminal* requisita informações de medições do *eCardio Meter* por uma conexão BLE (*Blueetooth Low Energy*, Ou Bluetooth de Baixo Consumo) e as envia para o servidor médico. Uma aplicação executada no servidor médio alerta a equipe caso os indicadores observados fiquem fora dos limites pré-definidos. Tais limites levam em consideração características do paciente, como doenças pré-existentes, uso de medicações e idade. Além de não se preocupar com o envio prioritário dos dados coletados, o sistema não detecta um evento crítico em andamento, já que o *eCardio Meter* só envia dados ao *eCardio Terminal* quando solicitado. Os autores consideram 3 consultas por hora ao sensor em seus experimentos.

As propostas de (18) e (35) possuem arquiteturas e características semelhantes. A primeira é focada em pacientes com problemas cardíacos, e a segunda em pacientes idosos. Ambos utilizam *Bluetooth* como tecnologia de comunicação Intra-BAN, e sensores corporais de superfície para monitoramento de sinais vitais de pacientes. O dispositivo pessoal analisa esses dados e, caso ultrapassem limiares definidos pelo médico, a equipe médica, o serviço de emergência, e os familiares, são avisados por mensagem de texto, que informa também a localização do paciente. Por ser voltado a pacientes com problemas cardíacos, o sistema proposto por (18) usa um algoritmo classificador de batimentos cardíacos para identificar eventos de arritmia. Já o sistema de (35) possui várias funções acessórias, como dicas para o paciente (*e.g.*, "exercite-se mais"), funções de lembrete para eventos médicos, consulta ao histórico de eventos de risco, recomendações médicas, botões para contactar o serviço de emergência, etc. Os autores classificam os dados da WBAN em "limiares", "recomendação médica" e "dados fisiológicos", mas essas categorias servem apenas para indicar qual módulo do sistema deverá ser inicializado. Nem o *eCardio* de (38), nem as propostas de (18) e (35), se preocupam com questões relacionadas à classificação ou priorização dos dados médicos, focando-se apenas nas funcionalidades dos sistemas.

Doenças cardiovasculares são a maior causa de todas as mortes registradas no mundo (28, 44, 2). Outras doenças como câncer, diabetes e asma são crônicas, e com frequência podem ser fatais. O monitoramento constante de pacientes tem papel fundamental na redução de fatores de risco de doenças que ameaçam a vida, alertando a equipe médica antecipadamente sobre a iminência de uma situação crítica, para que possa haver uma intervenção imediata (52). O monitoramento dos sinais vitais do paciente permite identificar a ocorrência de um evento crítico que ameace sua vida como, por exemplo, uma parada cardíaca ou parada respiratória. Diferente dos trabalhos anteriores, que no máximo reportam um evento crítico em andamento, o sistema SANTE, proposto por (61), é capaz de identificar um evento crítico antes que ele aconteça.

Para identificar a iminência de uma situação crítica, o SANTE toma como base um conjunto de indicadores estatísticos genéricos. Ao processar os dados de sinais vitais coletados pelos sensores corporais de um paciente, o sistema analisa o histórico dos indicadores e busca identificar um conjunto de tendências específicas. Com base nessas análises, o SANTE prediz a iminência de uma transição crítica, e possibilita que a equipe médica seja alertada e possa prestar socorro a tempo de salvar a vida do paciente. Ao identificar a iminência de um evento crítico, o SANTE envia ao servidor médico do hospital um pacote de alerta marcado com a categoria mais prioritária do padrão IEEE 802.11e. Os autores validam o sistema proposto no simulador NS3[8], onde configuram os APs da rede para trabalharem com valores mínimos de contenção para a categoria mais prioritária. Contudo, por não considerar um ambiente de rede sem fio programável, o SANTE não é capaz de configurar sob demanda os APs da rede. Inspirada no SANTE, nossa proposta

[8] https://www.nsnam.org/

utiliza as funções de programabilidade de subcamada MAC implementadas no Ethanol, em conjunto com a visão global da rede provida pelo paradigma SDWN, para identificar automaticamente pacotes de alerta emitidos pelo SANTE, e configurar sob demanda o AP correspondente para promover acesso ao meio prioritário para esses pacotes.

Assim como a proposta de (61), os trabalhos de (7) e (53) consideram a interação entre os dois primeiros níveis da arquitetura de comunicação WBAN, buscando satisfazer requisitos de QoS para melhorar o desempenho geral de sistemas de saúde. Ambos propuseram o mapeamento de prioridades de quadros WBAN para categorias de acesso da WLAN, e consideraram respectivamente os protocolos IEEE 802.15.6 e IEEE 802.11e como tecnologias de comunicação para essas redes.

No primeiro trabalho, os autores propõem a classificação de pacotes WBAN em três categorias de prioridade: OD (*On Demand*, ou Sob Demanda), EM (*Emergency*, ou Emergência) e NR (Normal). Essas categorias são mapeadas para diferentes ACs WLAN, e alocadas em três filas gerenciadas por escalonadores de pacotes. A classificação é realizada com base em 3 dos valores de prioridade UP dos pacotes provenientes da WBAN. São propostos, ainda, dois mecanismos de escalonamento que consideram o tempo de espera do pacote na fila, visando evitar que pacotes menos prioritários sejam preteridos indefinidamente. Os dois escalonadores se diferem unicamente pela agregação ou não de múltiplos pacotes WBAN em um mesmo quadro WLAN, mapeado para a AC relacionada à maior prioridade UP entre os pacotes agregados. Os parâmetros de contenção utilizados são os definidos pelo padrão IEEE 802.11e para as ACs. A proposta é validada por meio de simulações, onde pacotes WBAN das três diferentes categorias são gerados, classificados e priorizados, mas não são considerados ambientes de rede densos, com múltiplas STAS disputando o meio de comunicação.

No segundo trabalho, os autores dão foco à interconexão de WBANs de pacientes à rede do hospital, e investigam os impactos de fatores como quantidade de pacientes, quantidade de dispositivos na WLAN, qualidade do sinal e a variação de parâmetros de subcamada MAC no desempenho da rede. A diferenciação de tráfego na WLAN foi realizada exclusivamente pelo valor AIFS definido individualmente para cada AC, e todas as ACs utilizaram valores mínimo e máximo de contenção idênticos. Foram realizados testes com valores de TXOP de $0\mu s$ e $5000\mu s$ para todas as categorias. As 7 prioridades UP dos quadros WBANs são mapeadas para as 4 ACs WLAN, e dois cenários são considerados. No primeiro, cada 4 quadros WBAN destinados à mesma AC são agregados em um único quadro WLAN, e no segundo, cada quadro da WBAN é enviado individualmente para a WLAN. Apesar de utilizados valores diferentes dos definidos pelo padrão para os parâmetros de contenção, estes são utilizados em todo o experimento. Além disso, ao definir valores idênticos para janelas de contenção de todas as ACs, os autores limitam um dos três fatores utilizados pela EDCA para diferenciação de tráfego, que é o tamanho da janela para contenção.

Ainda com relação ao tratamento prioritário para dados médicos, vários estudos avaliam a priorização de dados em WBANs, mas limitam-se à comunicação Intra-BAN, ou seja, entre os nós WBAN e o dispositivo pessoal. Em (20), os autores classificam o tráfego WBAN em 3 níveis: emergência, sob-demanda e normal. Essa classificação é relacionada ao tipo de sensor em uso, e os nós sensores acessam o meio sem fio por divisão de tempo - TDMA (*Time Division Multiple Access*). Um período é dividido em 10 *slots* de tempo, e os nós de emergência, sob-demanda e normal utilizam, respectivamente, o primeiro, segundo e terceiro *slots* de um período para enviar dados. O nó coordenador recebe os dados e implementa uma fila de prioridade não preemptiva M/G/1 para transmiti-los.

Já os autores em (39), propõem um algoritmo para alocação prioritária de *slots* de tempo utilizando uma extensão da teoria dos jogos evolutivos. O ajuste do modelo é feito com base em características do nó, como criticidade dos dados transmitidos, fator de dissipação de energia e tempo de inatividade. Uma estratégia justa ajuda esses nós a terem prioridade de transmissão.

Um protocolo MAC adaptativo baseado em prioridades é proposto por (6). Os autores utilizam a capacidade de troca rápida de canal do padrão IEEE 802.15.4 para criar dois canais de comunicação, um dedicado ao tráfego de quadros de controle e outro para tráfego de dados. O tráfego é dividido em 4 categorias e, dependendo da quantidade de nós em cada categoria, os autores dividem dinamicamente o CAP (*Contention Access Period*, ou Período de Acesso por Contenção) do CSMA/CA em 4 fases. *Slots* de tempo são alocados dinamicamente, com base na prioridade do tráfego. O IEEE 802.15.4 é um padrão para redes pessoais sem fio com baixas taxas de transferência, o qual é base para o ZigBee.

Ainda no contexto de QoS em redes sem fio IEEE 802.11, é válido mencionar o trabalho de (43), embora este não tenha relação direta com aplicações médicas. Os autores utilizam técnicas de Aprendizado Reforçado, ou RL (*Reinforcement Learning*) para gerenciar automaticamente a Qualidade de Experiência, ou QoE (*Quality of Experience*) do usuário para navegação WEB em redes sem fio. Contudo, apenas características de camada física (PHY) são ajustadas, mais especificamente, potência de sinal e canal sem fio utilizado para transmissão. Essas alterações podem resultar em melhoria da qualidade geral do canal de comunicação, mas não permitem priorizar fluxos de dados específicos.

Diferente da nossa proposta, dentre os trabalhos citados, os que abordam o tratamento prioritário de dados médicos no nível Inter-BAN (entre o dispositivo pessoal e o AP) utilizam simulações para validar suas propostas, e não consideram ambientes reais de rede. Além disso, esses trabalhos não identificam fluxos de pacotes específicos na rede, e com isso não podem aplicar programaticamente uma política de priorização sob demanda como é feito pela plataforma proposta nesta dissertação. Os trabalhos que alteram as configurações de contenção da rede o fazem manualmente, em cada AP. No melhor do

nosso conhecimento, não há estudos que utilizem a abordagem de redes programáveis para, de forma centralizada, identificar e priorizar dinamicamente fluxos de pacotes de alerta médico em redes sem fio IEEE 802.11 hospitalares. A Tabela 3 sumariza os trabalhos relacionados no contexto de aplicações médicas.

Tabela 3 – Tabela comparativa de trabalhos relacionados

Trabalho	**Escopo**	**Priorização Camada 2**	**Program. de Camada 2**	**Sensível ao contexto**	**Validação**
(38)	Intra-BAN Inter-BAN Além-BAN	Não	Não	Não	Protótipo
(18)	Intra-BAN Inter-BAN Além-BAN	Não	Não	Não	Protótipo
(35)	Intra-BAN Inter-BAN Além-BAN	Não	Não	Não	Protótipo
(61)	Intra-BAN Inter-BAN	Sim	Não	Não	Ambiente simulado
(7)	Intra-BAN Inter-BAN	Não	Não	Não	Ambiente simulado
(53)	Intra-BAN Inter-BAN	Sim	Não	Não	Ambiente simulado
(20)	Intra-BAN	Sim	Não	Não	Ambiente simulado
(39)	Intra-BAN	Sim	Não	Não	Ambiente simulado
(6)	Intra-BAN	Sim	Não	Não	Ambiente simulado
Nossa proposta	Inter-BAN	Sim	Sim	Sim	Ambiente Real

Fonte: Elaborado pelo autor (2021)

4 PLATAFORMA PARA PRIORIZAÇÃO DINÂMICA DE PACOTES DE ALERTA MÉDICOS EM REDES SEM FIO DEFINIDAS POR SOFTWARE

Neste capítulo, apresentamos a plataforma proposta para priorização de acesso ao meio sob demanda para pacotes de alerta médico em redes sem fio hospitalares. Inicialmente discutimos o Ethanol (41), arquitetura SDN para redes sem fio utilizada pela plataforma, bem como as funções de sua API que implementamos para gerenciamento de parâmetros da subcamada MAC das redes sem fio IEEE 802.11.

A visão global da rede, propiciada pelo paradigma SDWN, permite que a plataforma possa identificar um fluxo de pacotes de alerta médico em determinado AP, e então configurá-lo programaticamente para priorizar em seu BSS o acesso ao meio para esses pacotes. Isso é feito através da alteração dos parâmetros QoS da subcamada MAC, melhorando estatisticamente as chances dos pacotes de alerta médico serem transmitidos antes de outros tipos de tráfego presentes na rede sem fio. Com isso, buscamos reduzir as perdas e os atrasos na entrega desses pacotes através da WLAN. A atuação sob demanda da plataforma permite reduzir o impacto da priorização mais agressiva dos pacotes de alerta médico no funcionamento normal da rede. A plataforma foi implementada como um módulo do Ethanol.

4.0.1 Ethanol: uma arquitetura SDN para redes IEEE 802.11

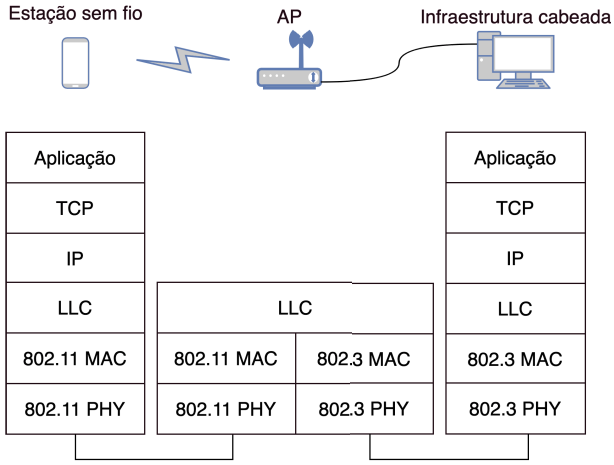
O Ethanol refatora as funcionalidades do plano de controle entre os APs e o controlador, permitindo que sejam criadas aplicações que consumam os serviços providos por sua API aberta. Esses serviços possibilitam ao programador obter informações do estado da rede, especificar o comportamento desejado mediante regras implementadas pelo controlador, e disseminar novas configurações para elementos de rede. O controlador Ethanol foi desenvolvido como um módulo do POX, um controlador SDN com suporte a *OpenFlow*, e com isso é capaz de controlar não só as características da rede sem fio nos APs, mas também comutadores de pacote compatíveis com *OpenFlow*. O AP Ethanol foi implementado sobre o `hostapd`[9], uma aplicação de espaço do usuário compatível com Linux e FreeBSD para implementação de pontos de acesso IEEE 802.11. O Ethanol, assim como o controlador POX, é implementado em Python, e o `hostapd` é implementado em C. A comunicação entre controlador e AP se dá pela troca de mensagens realizada por uma conexão segura SSL (*Secure Socket Layer*, ou Camada de Soquete Seguro).

O controlador utiliza a *interface southbound* Ethanol para controlar as *interfaces* sem fio do AP. Contudo, um AP é um dispositivo híbrido, que faz uma ponte entre redes IEEE 802.3 (Ethernet) e IEEE 802.11 (Sem fio), conforme mostra a Figura 17. A instalação

[9] https://w1.fi/hostapd/

do *Open vSwitch*[10] no AP é opcional, mas permite que além das *interfaces* sem fio, o controlador consiga também manipular os fluxos do comutador de pacotes do AP utilizando *OpenFlow* e OVSDB (*Open vSwitch Database Management Protocol*, ou Protocolo Aberto de Gerenciamento de Banco de Dados vSwitch) (51). Essa funcionalidade é indispensável para que nossa proposta seja capaz de identificar novos fluxos de dados médicos na rede.

Figura 17 – *Bridge* IEEE 802.11/IEEE 802.3



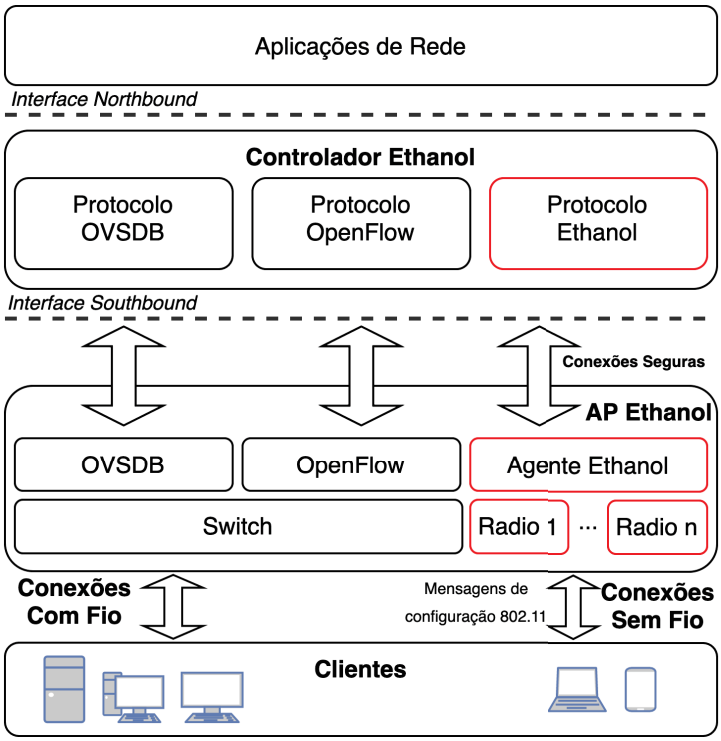
Fonte: Adaptado de (56)

A Figura 18 apresenta a arquitetura do Ethanol, e destaca em vermelho os blocos de gerenciamento de rede sem fio. As aplicações de rede podem utilizar OVSDB, *OpenFlow* ou Ethanol, de forma conjunta ou separadamente, para controlar comutadores de rede compatíveis com *OpenFlow* e pontos de acesso sem fio compatíveis com Ethanol. O protocolo Ethanol utiliza um canal de comunicação separado, tornando-o independente do *OpenFlow*, caso seja utilizado apenas para controlar as funções sem fio do AP. Apenas mensagens de gerenciamento definidas no padrão IEEE 802.11 são utilizadas para controlar características das estações sem fio, portanto nenhuma modificação nessas estações é necessária. A capacidade do Ethanol de conjuntamente programar fluxos no comutador do AP e controlar suas *interfaces* sem fio foi decisiva para sua utilização pela plataforma proposta nesse trabalho, visto que pacotes de alerta médico que cheguem pela *interface* sem fio do AP com destino à rede cabeada geram uma notificação ao controlador através de eventos *PacketIn OpenFlow*.

Como visto na Subseção 2.3, o controlador SDN é responsável por programar os comutadores de rede, instalando neles regras para encaminhamento de fluxos de pacotes. Já um controlador SDWN pode, além de controlar o encaminhamento de pacotes, gerenciar diversas outras configurações de rede, como potência de sinal dos APs, canal de comunicação sem fio utilizado, autenticação de usuários, mobilidade de nós, parâmetros de subcamada MAC, etc.

[10] http://openvswitch.org/

Figura 18 – Arquitetura do Ethanol



Fonte: Adaptado de (41)

O Ethanol provê uma API de controle aberta, que dá ao administrador o poder de controlar um grande número de parâmetros da rede. A API, apresentada na Figura 19, foi desenvolvida utilizando a abordagem de orientação a objetos, onde as entidades de rede podem ser objetos físicos ou virtuais, que manipulam eventos e possuem atributos e métodos. Uma entidade AP e uma entidade VAP (*Virtual Access Point*, ou Ponto de Acesso Virtual) são exemplos respectivamente de objetos físicos e virtuais. Um sinal de menos (-) indica um atributo somente leitura. Métodos com prefixo "*ev*" são eventos gerenciáveis pelo controlador. A notação *crow's foot* (pé de galinha) representa a cardinalidade. Por exemplo, um *Access Point* pode ter ao mesmo tempo vários *VAPs*. O losango preenchido indica uma dependência forte, onde uma classe não pode existir sem a classe da qual depende, tocada pelo losango. Por exemplo, um VAP não pode existir sem um *AccessPoint*. Os métodos *get* e *set* das entidades não foram incluídos na figura para melhor visibilidade. As principais funções de cada entidade são:

- Entidade *Access Point*: Representa um dispositivo físico, que pode ter um ou mais rádios físicos e um ou mais VAPs.

- Entidade *Radio*: Configura as *interfaces* sem fio físicas, e tem atributos como canal, taxas de transferência suportadas, potência de transmissão, além de coletar informações e estatísticas do sinal sem fio.

- Entidade *Device*: Implementa funções para configurar e coletar informações do dispositivo, tais como endereço IP, endereço MAC e suporte a QoS, além de características da conexão entre a estação sem fio e o AP.

- Entidade *VAP*: Um VAP pode ser configurado e mantido desativado, para uso futuro. Estações se conectam a um VAP, e um grupo de VAPs forma uma *Network* (ou rede) em um dispositivo físico, e vários usuários podem se conectar a um VAP. Dentre outros parâmetros de transmissão MAC, o VAP expõe os parâmetros de contenção IEEE 802.11e (valores mínimo e máximo para janela de contenção, AIFS, tempo de transmissão e controle de admissão).

- Entidade *Network*: Pode conter vários VAPs, e representa a rede e seu SSID. Provê métodos para associação e desassociação de APs na rede e um método para solicitar transição de usuário.

- Entidade *Station*: Representa uma estação sem fio, e herda métodos e propriedades da entidade *Device*. Essa entidade retorna medições coletadas utilizando IEEE 802.11k (*Radio Resource Management*, ou Gestão de Recursos de Rádio), como relatórios de estado do canal e lista de APs ao alcance, além de métricas da rede sem fio, como *bytes* enviados e recebidos.

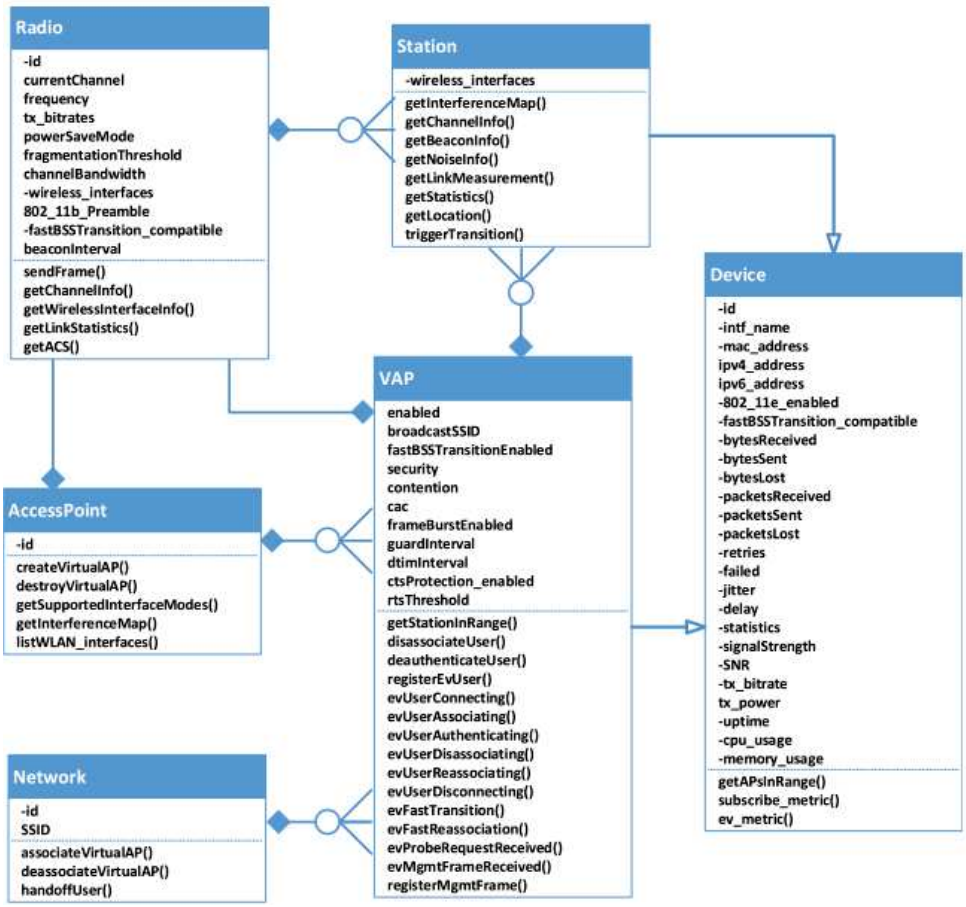
4.0.2 Funções de programabilidade de subcamada MAC implementadas no Ethanol

Os autores implementaram um protótipo do Ethanol, e disponibilizaram-no sob a Licença Pública Geral, ou GPL (*General Public License*). Contudo, algumas das funções descritas na API não foram incluídas no protótipo. Mais especificamente, as funções para consulta e alteração de parâmetros de contenção na subcamada MAC (AIFS, CWmin, CWMax, TxOP e controle de admissão) não foram implementadas, visto que não foram necessárias para as aplicações que os autores desenvolveram como prova de conceito em seu trabalho. Importante lembrar que a versão do padrão IEEE 802.11e adotada pelo mercado, e padronizada pela *Wi-FI Alliance*, é chamada WMM. Com isso, para que a plataforma de priorização proposta neste trabalho pudesse alterar de forma programática tais parâmetros no AP, estendemos as funcionalidades do Ethanol, e implementamos as trocas de mensagens e as funções para consulta e alteração dos parâmetros mencionados. As funções implementadas no controlador[11] foram:

- **`is_802_11e_enabled(server, id, intf_name, ssid)`**: Verifica se o WMM está ou não ativo em um AP. O parâmetro *server* é uma tupla com endereço IP e porta do AP a ser consultado. *id* é o identificador da mensagem. *intf_name* é o nome da

[11] https://github.com/genilson/ethanol_controller

Figura 19 – API Ethanol



Fonte: (41)

interface sem fio a ser consultada, e *ssid* é o nome da rede. Uma *interface* de rede com mais de um SSID pode ter o WMM ativado ou não para cada SSID.

- **`get_wmm_params(server, id, intf_name, ac)`**: Consulta parâmetros WMM de um AP. Apesar de a diferenciação por categorias de acesso poder estar ou não ativa para cada SSID, os valores dos parâmetros são os mesmos para todos os SSIDs que utilizam uma mesma *interface* de rádio. O parâmetro *server* é uma tupla com endereço IP e porta do AP a ser consultado. *id* é o identificador da mensagem. *intf_name* é o nome da interface sem fio a ser consultada, e *ac* é a categoria de acesso a ser consultada (0, 1, 2 ou 3). Se ac = –1, retorna os parâmetros das 4 ACs em uma única consulta.

- **`set_wmm_params(server, id, intf_name, ac, aifs, cwmin, cwmax, txop_limit, admission_control_mandatory)`**: Altera os parâmetros WMM em um AP. Os valores são validados antes do envio, evitando *overhead* desnecessário na rede. O parâmetro *server* é uma tupla com endereço IP e porta do AP a ser configurado. *id* é o identificador da mensagem. *intf_name* é o nome da interface sem

fio a ser configurada. *ac* é a categoria que deverá ser alterada. *aifs*, *cwmin*, *cwmax*, *txop_limit* e *admission_control_mandatory* (0 para desativado e 1 para ativado) são os valores dos parâmetros a serem alterados. Parâmetros com valor = –1 não são alterados no AP, permitindo que seja feita alteração individual de um parâmetro.

O controlador utiliza essas funções para enviar mensagens de consulta e alteração ao AP, e o servidor de mensagens Ethanol existente no AP decodifica as mensagens e executa o que é solicitado. Ao ser iniciado, o `hostapd` lê os parâmetros a partir de um arquivo de configuração, mantendo esses valores em uma estrutura de dados interna. As funções abaixo foram implementadas no `hostapd`[12] para consultar e alterar esses dados em tempo de execução:

- `struct hostapd_wmm_ac_params *get_wmm_ac_params(char *intf_name)`: consulta os parâmetros atualmente em uso, armazenados na estrutura interna de dados do `hostapd`.
- `void set_wmm_ac_params(char *intf_name, int ac, struct hostapd_wmm_ac_params *ac_params)`: Modifica os valores na estrutura interna de dados do `hostapd`, atualizando em seguida o *beacon* de rede para refletir as alterações.

As funções implementadas podem ser utilizadas por algoritmos de controle desenvolvidos pelo administrador de rede, a fim de gerenciar os parâmetros de contenção (QoS) da subcamada MAC em redes IEEE 802.11.

A plataforma de priorização de pacotes de alerta médico é implementada como um módulo SDWN, ou seja, é uma aplicação de rede que roda no controlador Ethanol. Ao detectar um novo AP, o módulo instala nele uma regra para detectar fluxos de pacotes de alerta médico e, ao ser informado de um novo pacote desse tipo ingressante na rede, verifica se os parâmetros de contenção do AP estão diferentes dos valores definidos na política de priorização. Em caso positivo, o módulo armazena os dados atuais, para que mais tarde possa retornar a rede ao seu estado original, e configura os parâmetros com os novos valores definidos na política. Um contador *check_idle_timeout* é iniciado, e sempre que um novo pacote de alerta médico é identificado na rede, tem seu valor redefinido para 0. Ao atingir um período de inatividade igual a *idle_timeout*, definido pelo administrador, o módulo retorna a rede à sua configuração original.

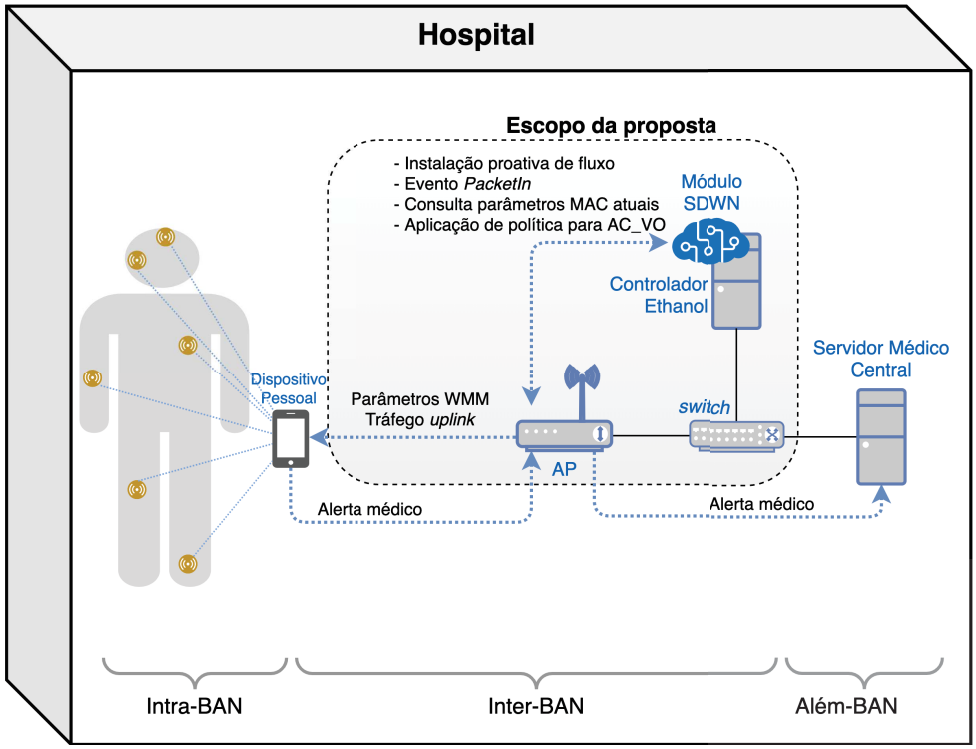
4.0.3 Escopo e funcionamento da plataforma proposta

A Figura 20 detalha o escopo de atuação da plataforma no cenário considerado. O controlador Ethanol possui um canal de comunicação seguro com o AP, através do qual

[12] https://github.com/genilson/ethanol_hostapd

instala regras de encaminhamento, recebe notificação de eventos, consulta informações de estado da rede e consulta e altera parâmetros de rede, dentre eles os parâmetros de contenção da subcamada MAC. Essas ações são orquestradas pelo módulo SDWN, aplicação de rede executada no controlador. O dispositivo pessoal se comunica com o AP via WLAN. Os parâmetros de contenção utilizados em cada AC (AIFS, janela de contenção e TXOP) para comunicação *uplink*, ou seja, no sentido do dispositivo pessoal para o AP, são informados periodicamente pelo AP à todas as STAs do BSS, conforme explicado na Subseção **2.1.4**. A coleta de dados Intra-BAN, a análise para detecção de eventos críticos, a geração de pacotes de alerta médico pelo dispositivo pessoal e a entrega ao destino final através da rede cabeada do hospital não fazem parte do escopo da proposta.

Figura 20 – Escopo de atuação da plataforma de priorização

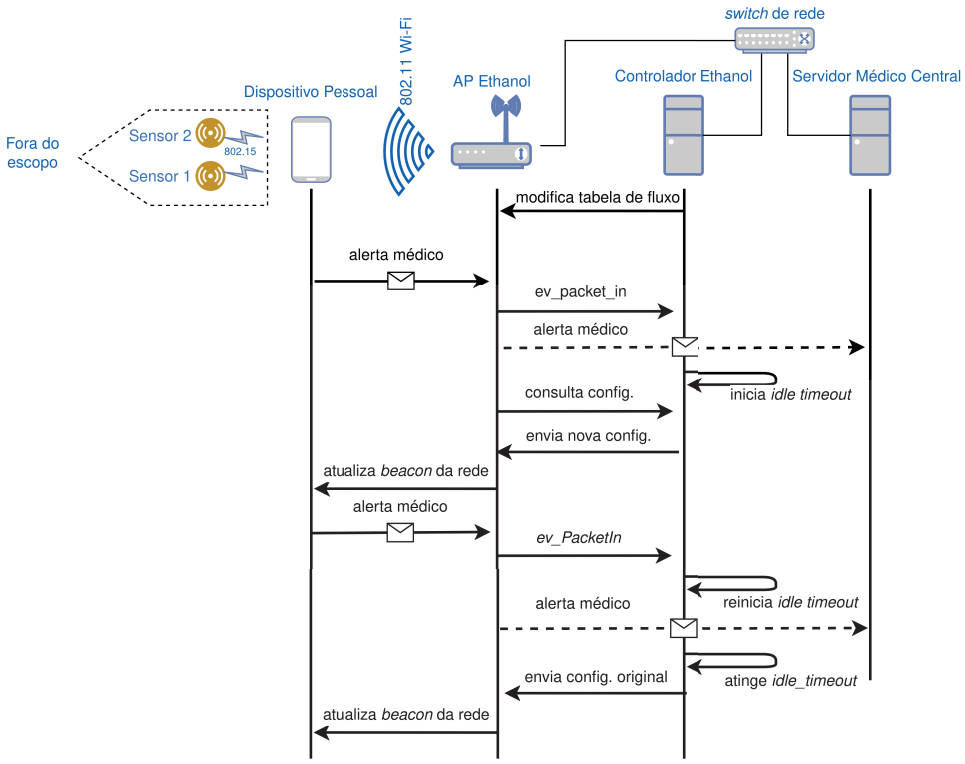


Fonte: Elaborado pelo autor (2021)

Ao ser iniciada, a plataforma instala uma regra na tabela de fluxos no comutador de pacotes presente nos APs detectados, instruindo-os a encaminhar ao controlador pacotes de alerta médico que chegarem até eles. Isso é possível, porque além de controlar as *interfaces* sem fio do AP, o Ethanol também é capaz de programar a tabela de fluxos do comutador de pacotes presente nele. Quando o dispositivo pessoal envia o primeiro pacote de alerta médico, é gerado no AP um evento *PacketIn*, responsável por notificar o controlador de que um novo fluxo de pacotes de alerta médico foi iniciado. Ao ser notificado, o módulo SDWN armazena os valores atuais dos parâmetros AIFS (*Arbitration Interframe Space*, ou Intervalo Arbitrário entre Quadros), janela de contenção mínima (CWmin) e janela

de contenção máxima (CWmax) desse AP, alterando-os para os valores configurados pelo administrador caso sejam diferentes. A nova configuração é mantida enquanto pacotes de alerta continuarem ingressando na rede. Após um período de inatividade, chamado *idle timeout*, a configuração da rede é retornada ao estado anterior. O *idle timeout* é configurável pelo administrador, e tem valor pré-definido de 5 minutos. Os passos seguidos pela plataforma para priorização do fluxo de pacotes de alerta médico são representados no diagrama de sequência da Figura 21, e são detalhados a seguir:

Figura 21 – Diagrama de sequência para priorização de pacotes de alerta médico



Fonte: Elaborado pelo autor (2021)

1. Inicialmente o controlador atua de forma proativa, incluindo uma regra na tabela de fluxos do AP. Essa regra associa os pacotes de alerta médico a duas ações: (1) encaminhar o pacote ao controlador, e (2) encaminhar o pacote à porta associada ao Servidor Médico Central. Os campos de cabeçalho utilizados para filtrar o fluxo de pacotes de alerta são *IP de destino*, *porta de destino* e *valor do campo DSCP*. Por exemplo, um pacote com *DSCP* igual a 192, destinado ao Servidor Médico Central, especificamente na porta definida para pacotes de alerta médico, casa com as regras definidas para o fluxo.

2. Como os sensores corporais enviam constantemente dados de sinais vitais do paciente para o dispositivo pessoal, esses dados históricos podem ser analisados por um modelo de detecção antecipada de evento crítico, como o criado por (61) que, ao

identificar a iminência de um evento crítico, envia ao Servidor Médico Central um pacote de alerta médico. Como ainda não há uma política diferenciada definida para a categoria de acesso (AC) à qual pertence esse fluxo, o primeiro pacote de alerta enviado utiliza a configuração padrão da rede sem fio para chegar ao AP (tráfego *uplink*, ou *upstream*).

3. Ao receber o pacote com destino à rede cabeada, o comutador compara as informações com a entrada configurada na tabela de fluxos e executa as ações associadas, encaminhando o pacote à porta de saída para ao Servidor Médico Central, e encapsulando uma cópia desse pacote em uma mensagem *PacketIn*, enviada ao controlador Ethanol.

4. O controlador trata o evento *PacketIn* e mantém uma contagem de tempo para gerir o *idle timeout* configurado, ou seja, o período de tempo em que a priorização do fluxo de pacotes de alerta médico deverá permanecer ativa após a última notificação de entrada de pacote de alerta na rede.

5. O controlador envia ao AP que originou o evento uma mensagem de consulta aos parâmetros QoS em uso.

6. Se os parâmetros atuais não forem os definidos pelo administrador para pacotes de alerta médico, o controlador os armazena localmente e envia ao AP que originou o evento uma mensagem de alteração com os novos valores dos parâmetros a serem configurados.

7. O AP aplica as configurações de contenção e atualiza o *beacon* de rede.

8. Um novo pacote de alerta médico é emitido pelo dispositivo pessoal. Agora as novas configurações de contenção já são utilizadas para chegada do pacote ao AP. O controlador trata o evento *PacketIn* apenas reiniciando a contagem de tempo de inatividade para o fluxo de pacotes de alerta.

9. Nenhuma nova notificação de pacote de alerta chega ao controlador durante o período de tempo configurado para *idle timeout*.

10. O controlador envia ao AP uma mensagem de alteração para configuração dos valores anteriormente em uso para os parâmetros QoS da subcamada MAC.

Ao ser enviado pelo dispositivo pessoal, o pacote precisa primeiro transitar pelo meio sem fio para então chegar ao AP. Esse primeiro passo é mais desafiador, devido à natureza propensa a erros e interferências do meio sem fio (16), o que reforça a relevância da nossa proposta. A partir do AP, o pacote usualmente segue por uma infraestrutura cabeada, onde podem ser aplicadas outras políticas de QoS para garantir melhores níveis de latência e perda no restante do caminho.

5 AVALIAÇÃO EXPERIMENTAL

Neste capítulo, avaliamos a viabilidade do uso da plataforma proposta para priorização de acesso ao meio sob demanda para fluxos de pacotes de alerta médico. Para isso, utilizamos um ambiente real de rede sem fio e variamos o número de STAs conectadas à rede, de modo a experimentar com diferentes cenários de densidade. Foram realizados experimentos em três diferentes cenários. No primeiro, conectamos 5 STAs à rede. Chamaremos este cenário de **densidade baixa**. No segundo cenário, que chamaremos de **densidade média**, 10 STAs foram conectadas no total e, no terceiro cenário, que chamaremos de **densidade alta**, aumentamos para 20 o número de STAs conectadas.

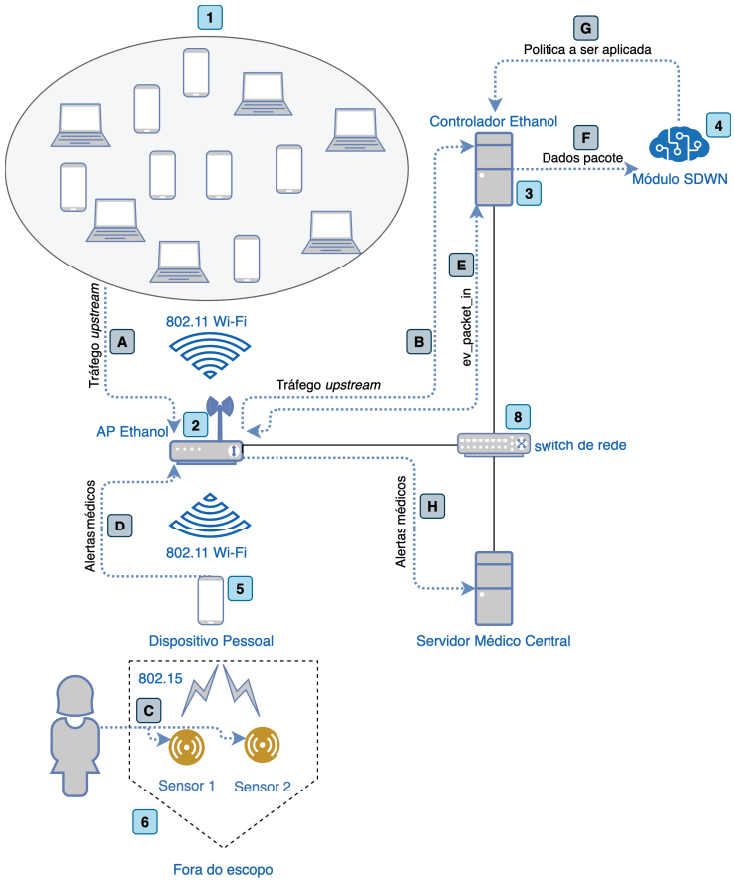
A Seção 5.1 apresenta a arquitetura do ambiente de testes utilizado, o fluxo de dados do experimento e o método utilizado para a mensuração de atrasos e perdas de pacotes. A Seção 5.2 apresenta o método experimental utilizado para avaliar as melhorias estatísticas obtidas com o uso da plataforma para os atrasos e perdas de pacotes de alerta médico. Finalmente, a Seção 5.3 apresenta e discute os resultados alcançados.

5.1 AMBIENTE DE TESTES UTILIZADO

A Figura 22 apresenta mais detalhadamente o ambiente de testes, onde fluxos de dados e trocas de mensagens são referenciados por marcadores com letras em fundo cinza e os equipamentos utilizados são referenciados por marcadores com números em fundo azul. O ambiente é composto por estações sem fio (STAs) (1), um ponto de acesso sem fio (2), ou AP, com o Ethanol habilitado, um controlador de Redes Sem Fio Definidas por Software, ou SDWN (*Software Defined Wireless Networks*) (3), um módulo SDWN (4), um dispositivo pessoal (5), uma rede corporal sem fio (6), um Servidor Médico Central (7), e um *switch* de rede (8).

As STAs são interligadas à rede através de uma conexão sem fio IEEE 802.11 WLAN, provida pelo AP Ethanol. O controlador executa o módulo SDWN para configuração de parâmetros de QoS da subcamada MAC no AP. A comunicação entre os sensores sem fio, envio de sinais vitais ao dispositivo pessoal e detecção de evento crítico fogem ao escopo deste trabalho, de forma que abstraímos essa parte em nossos experimentos. O dispositivo pessoal apenas envia pacotes de alerta médico para o servidor médico central. A quantidade de pacotes a serem enviados e o intervalo entre envios são configuráveis, mas utilizamos valores fixos para controlar a duração dos experimentos. O Servidor Médico Central recebe os pacotes de alerta médico e mensura os atrasos e perdas para cada pacote. O *switch* de rede utilizado neste experimento é um roteador sem fio com a função de ponto de acesso desativada, de modo a atuar como simples comutador de pacotes para interligar por meio de uma rede cabeada o AP Ethanol, o controlador SDWN e o Servidor Médico Central.

Figura 22 – Ambiente de testes utilizado



Fonte: Elaborado pelo autor (2021)

Em uma WLAN, STAs podem ser celulares, *laptops*, PDAs, *desktops* equipados com placa de rede sem fio, ou qualquer outro dispositivo capaz de se comunicar utilizando o protocolo WLAN IEEE 802.11. Todas as STAs conectadas participantes de um mesmo BSS utilizam o mesmo canal de comunicação sem fio, e competem entre si pela oportunidade de transmitir dados por esse canal.

Utilizamos 21 STAs em nosso ambiente de testes, todas elas *desktops* rodando o sistema operacional Ubuntu 14.04, equipados com placa de rede sem fio modelo WPN 200, com *chip* Atheros AR9227 e antena com 2 dbi de ganho. Um desses *desktops* atua como dispositivo pessoal, e envia apenas pacotes de alerta médico para o Servidor Médico Central. O dispositivo pessoal funciona como *gateway* entre os sensores sem fio da WBAN e a rede sem fio externa. Os outros 20 *desktops* atuam como clientes da rede, STAs comuns, e são responsáveis por gerar três fluxos de tráfego de diferentes categorias no sentido *upstream*, reproduzindo uma situação de utilização máxima do canal de comunicação em uma rede sem fio densa. Por questões práticas, no decorrer deste texto nos referiremos a esses *desktops* simplesmente como STAs.

Para a execução dos contêineres Docker do controlador e AP Ethanol, ambos

utilizando Ubuntu 14.04, utilizamos *desktops* com o sistema operacional Arch Linux[13] *rolling release*, kernel 5.11.16-arch1-1. O Servidor Médico Central também utilizou um *desktop* com essa configuração. A placa de rede sem fio instalada no AP Ethanol foi equipada com uma antena de 7 dbi de ganho, objetivando uma maior potência de transmissão para aumentar a área de cobertura, abrangendo todo o laboratório. O controlador Ethanol executa o módulo de configuração dos APs.

5.1.1 Fluxo de dados do Experimento

A Figura 22 descreve também os fluxos de dados do experimento. A geração do tráfego para saturação do canal de rede é feita a partir das STAs (1) para um computador da rede cabeada (sentido *upstream*) (A e B), que neste caso é o mesmo *desktop* utilizado para executar o controlador Ethanol (3). Das STAs até o AP, o tráfego é enviado pelo meio sem fio (A), e do AP até o servidor de geração de tráfego, o trajeto é por uma infraestrutura cabeada (B). Durante o período de geração de tráfego, o dispositivo pessoal (5) envia pacotes de alerta médico (D) para a unidade central médica (7). Da mesma forma que o tráfego sintético, os pacotes de alerta inicialmente trafegam pelo meio sem fio (D) e, a partir do ponto de acesso sem fio, seguem pela rede cabeada (H) até o servidor médico. O canal de comunicação entre o controlador Ethanol e o AP (E) é por onde o controlador recebe as mensagens *PacketIn* e envia mensagens de configuração ao AP.

5.1.2 Mensuração das perdas e atrasos fim-a-fim de pacotes de alerta médico

Utilizamos o protocolo UDP no intuito de que os pacotes de alerta médico tivessem o menor tamanho possível e gerassem o mínimo de *overhead* na rede. O UDP é um protocolo de transporte simplificado, leve e minimalista, sem confirmação de entrega ou apresentação antes de iniciar o envio de mensagens (31). Ele ocupa apenas 8 *bytes* no cabeçalho do pacote, enquanto o TCP ocupa no mínimo 20, podendo chegar a 60, já que possui 40 *bytes* opcionais para funções. O pacote de alerta médico possui 42 bytes, correspondentes à 14 *bytes* do cabeçalho Ethernet, 20 do IP e 8 do UDP. Isso é menor que o tamanho mínimo do quadro Ethernet, que é de 64 *bytes*.

A mensuração de atrasos fim-a-fim é complexa, uma vez que exige sincronização entre os relógios da origem e do destino, e qualquer erro de sincronização afetará as medições dos atrasos (3). De fato, mesmo utilizando o serviço NTP [14] (*Network Time Protocol*, ou Protocolo de Tempo para Redes) para sincronização entre os relógios do dispositivo pessoal e do Servidor Médico Central, obtivemos em alguns casos atrasos negativos ou nulos. Para reduzir ao máximo as incertezas quando às medições de atraso fim-a-fim com granularidade de microssegundos, e considerando que não nos interessava

[13] https://archlinux.org/
[14] https://www.ntp.org/

a hora exata de saída e chegada do pacote, mas sim o tempo transcorrido entre os dois eventos, optamos por implementar um contador de tempo em hardware[15], utilizando placas de prototipagem eletrônica modelo Arduíno Uno Atmega328p.

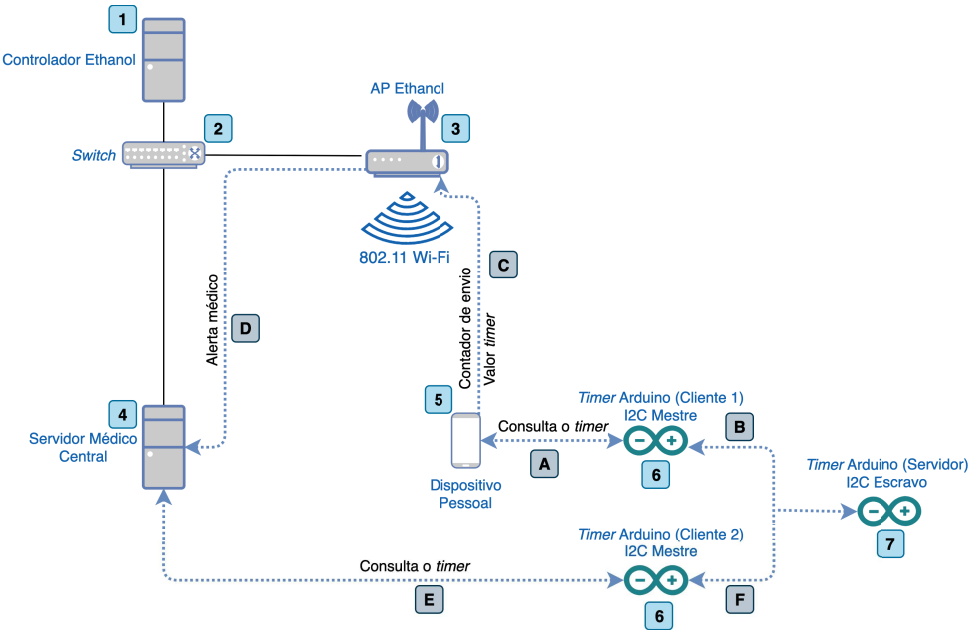
Os dois protocolos mais utilizados para comunicação síncrona entre circuitos integrados são o I^2C (*Inter-Integrated Circuit*, ou Circuito Inter-Integrado) e o SPI (*Serial Peripheral Interface*, ou Interface Periférica Serial). Em ambos é utilizada uma arquitetura mestre/escravo, onde o mestre controla a comunicação e o escravo transmite apenas quando solicitado pelo mestre. Cada um possui vantagens e desvantagens em relação ao outro, e são indicados para tipos de aplicações específicas (57, 40). Apesar de mais rápido, o protocolo SPI não permite a utilização de um esquema multi-mestres, sendo ideal para quando um microcontrolador precisa gerenciar vários dispositivos ao mesmo tempo (sensores, atuadores, periféricos). Por esse motivo, não nos aprofundaremos nos detalhes desse protocolo.

Como precisamos que os clientes solicitem o valor do contador sob demanda, eles precisam atuar como mestres no barramento, ao passo que o contador, que apenas responde às solicitações com o valor da variável de contagem, atua como escravo. Por isso, utilizamos o I^2C, um protocolo de comunicação síncrona e um verdadeiro barramento multi-mestres. O I^2C inclui detecção de colisão e arbitragem, a fim de evitar corrompimento dos dados se dois ou mais mestres iniciarem transferência simultaneamente (57). Os dispositivos conectados ao barramento I^2C utilizam dois fios para se comunicarem, sendo um para dados (*serial data - SDA*) e um para *clock* (*serial clock - SCL*), responsável por sincronizar a comunicação. Dispositivos que atuam como escravos possuem um endereço, utilizado pelo(s) mestre(s) para enviar ou requisitar dados. Esse barramento comporta até 128 dispositivos e a comunicação é *half-duplex*, ou seja, os dados são enviados nos dois sentidos mas não de forma simultânea.

O esquema implementado é o apresentado na Figura 23, onde equipamentos utilizados no experimento são referenciados por marcadores com números em fundo azul e mensagens de requisição e respostas são referenciadas por letras em fundo cinza. São utilizados 3 microcontroladores (6 e 7) que se comunicam por meio de cabos *jumpers* macho-macho (B e F) conectados à uma *protoboard* com 830 furos. Um dos microcontroladores atua como servidor (7) e mantém uma variável para contagem de tempo, incrementada a cada 20 microssegundos. Os outros dois microcontroladores (6) atuam como clientes, e consultam o servidor para obter o valor atual do contador. O microcontrolador que atua como servidor utiliza a porta USB apenas para alimentação elétrica. Os microcontroladores clientes 1 e 2 utilizam a conexão USB para comunicação, respectivamente, com o dispositivo pessoal e o Servidor Médico Central, que passam a ter uma fonte única e compartilhada de consulta de tempo.

[15] https://github.com/genilson/arduino_timer

Figura 23 – Esquema de mensuração de atrasos fim-a-fim com temporizador implementado em microcontroladores Arduíno



Fonte: Elaborado pelo autor (2021)

Para criar, enviar e capturar os pacotes de alerta médico, assim como mensurar os atrasos e as perdas desses pacotes, criamos uma aplicação cliente/servidor, à qual chamamos *Alerts*, e utilizamos as bibliotecas do Scapy[16], um programa Python interativo que permite manipular pacotes de diferentes protocolos de rede. Os pacotes são enviados a partir do dispositivo pessoal, passam pelo AP e são recebidos pelo Servidor Médico Central. Ao iniciar o envio, o cliente informa ao servidor a quantidade de pacotes a serem enviados, e a função de captura é configurada com base nessa informação. Para cada pacote de alerta enviado, o cliente consulta e armazena em memória o valor atual do contador de tempo, associando-o ao *id* do pacote.

O servidor realiza a captura dos pacotes na porta definida para os alertas médicos, e cada pacote capturado dispara uma função de *callback* para consulta ao valor do contador, que também é armazenado em memória em conjunto com o *id* do pacote recebido. Quando termina de enviar a quantidade de pacotes configurada, o cliente envia ao servidor os dados coletados para cada pacote. O servidor processa esses dados, e subtrai o valor do contador armazenado no momento em que o pacote saiu do dispositivo pessoal, do valor armazenado no momento em que chegou ao Servidor Médico Central. O resultado obtido é multiplicado por 20 (o contador retorna unidades de tempo de 20 μs), e resulta no tempo transcorrido em microssegundos para o envio de cada pacote.

O *overhead* para consulta ao temporizador foi medido com a utilização do módulo

[16] https://scapy.net/

Python *timeit*[17], configurado para realizar 1000 execuções e 10 repetições. Foram calculadas então a média e o desvio padrão das médias amostrais. A média obtida para execução no Servidor Médico Central foi de 4,99 milissegundos, com desvio padrão de $2,08 \times 10^{-7}$, ao passo em que no dispositivo pessoal a média foi de 4,09 milissegundos, com desvio padrão de $2,85 \times 10^{-7}$. Podemos observar que nos dois casos o desvio padrão é muito baixo, o que indica a quase inexistência de variação no *overhead* para consulta ao contador. Como não é possível requisitar o valor do contador apenas quando o pacote é enviado a partir da camada física, devemos considerar também o tempo de execução da função `send` do Scapy individualmente para cada pacote. Esse *overhead*, pode ser mensurado como a diferença entre o tempo inicial, quando é chamada a função `send`, e o tempo final, quando o *Scapy* reporta de fato o envio do pacote. Para realizar essa mensuração, realizamos o envio de 10 mil pacotes, e obtivemos um *overhead* médio de 18,76 ms, com desvio padrão de 3,48 ms. Esse *overhead* não influencia na análise estatística realizada, dado que é o mesmo para todos os pacotes.

5.2 METODOLOGIA DE AVALIAÇÃO

Os experimentos foram conduzidos em três diferentes cenários, aos quais chamamos de **densidade baixa**, **densidade média** e **densidade alta**. As quantidades de STAs conectadas à rede sem fio em cada cenário foram, respectivamente, 5, 10 e 20. Devido às limitações impostas pela utilização de um ambiente real de testes, em todos os cenários foi utilizado apenas um AP. Uma maior quantidade de APs incorreria na necessidade de aumentar o número de STAs para densificar a rede sem fio. O AP foi configurado para trabalhar com uma rede sem fio IEEE 802.11g[18] na frequência de 2.4GHz e SSID "SDWN".

Conforme discutido na Subseção **2.1.4**, ao reduzir a faixa de possíveis valores para a janela de contenção configurada para a classe de acesso à qual pertence um fluxo a ser priorizado, os pacotes desse fluxo precisarão aguardar estatisticamente menos tempo do que os demais para acessar o canal, reduzindo o atraso médio desses pacotes. Por esse motivo, a saturação do canal é necessária para melhor avaliar a efetividade da priorização dos fluxos de pacotes de alerta médico em ambientes de rede sem fio congestionados, com muitas estações sem fio conectadas disputando acesso ao meio de comunicação. Uma janela de contenção tão pequena pode acarretar em um maior número de colisões. Procuramos mitigar esse problema criando pacotes de alerta com o menor tamanho possível, e utilizando um intervalo de 10ms entre cada envio.

O canal sem fio foi saturado com tráfego sintético gerado pelo D-ITG (*Distributed Internet Traffic Generator*, ou Gerador de Tráfego de Internet Distribuído) (4). O tráfego gerado tem como origem as STAs, onde são executados os clientes D-ITG, e como destino o

[17] https://docs.python.org/3/library/timeit.html
[18] https://standards.ieee.org/standard/802_11g-2003.html

servidor D-ITG, executado em um computador conectado ao AP através da rede cabeada. Para definir a quantidade de tráfego a ser gerada a fim de saturar o canal sem fio, medimos a taxa de transferência da rede a partir de duas STAs aleatórias, uma de cada vez, em direção ao computador responsável por executar o servidor D-ITG. Para essa medição utilizamos a ferramenta iPerf3[19]. A taxa de transferência apresentou uma pequena variação à cada nova execução, porém os resultados obtidos ficaram sempre entre 35 Mbps e 40 Mbps, motivo pelo qual definimos como 40 Mbps a taxa de transferência total para os clientes do gerador de tráfego.

Como visto na Subseção **2.1.4**, em redes IEEE 802.11e a categoria de voz, ou AC_VO, é a mais prioritária dentre as quatro categorias definidas pelo padrão. Então, os fluxos associados à essa categoria já são naturalmente priorizados em relação aos demais, mesmo com a utilização de valores de contenção padrão. Contudo, inspirados pelo trabalho de (61), definimos como política de priorização para nossos experimentos, valores mínimos de AIFS, CWmin e CWmax para a AC_VO. Para efeitos práticos, as expressões "com priorização" e "sem priorização" serão usadas para indicar quando os valores de contenção utilizados para a categoria AC_VO foram, respectivamente, os mínimos ou os definidos pelo padrão. A Tabela 4 mostra os valores utilizados nos dois casos. Da mesma forma, chamaremos os fluxos com priorização e sem priorização de, respectivamente, "fluxo priorizado" e "fluxo não priorizado".

Tabela 4 – Parâmetros WMM para AC_VO usados no experimento

	AIFS	CWmin	CWmax	TXOP Limit
Sem priorização	2	3	7	1504
Com priorização	1	0	1	1504

Fonte: Elaborado pelo autor (2021)

Foram realizados 20 testes em cada cenário de densidade, alternando entre a aplicação ou não da política de priorização definida. Os passos básicos seguidos em cada um dos testes foram os seguintes:

(i) configuração de parâmetros de contenção;

(ii) geração de tráfego sintético pelas STAs para saturação do canal sem fio;

(iii) envio de pacotes de alerta e mensuração dos atrasos e perdas desses pacotes;

- Para cada cenário, no passo (i), a plataforma foi configurada para alternar as configurações dos valores de contenção no AP entre "com priorização" e "sem priorização" em cada teste. Utilizamos a ferramenta Linux `iw`[20] para verificar se os parâmetros configurados pela plataforma estavam de fato sendo propagados pelo AP.

[19] https://iperf.fr/
[20] https://wireless.wiki.kernel.org/en/users/documentation/iw

- Como a quantidade de STAs participantes no experimento variou em cada cenário de densidade, no passo (ii) configuramos os clientes DIT-G executados nas STAs participantes para gerar, somados, 40 Mbps de tráfego. Cada um foi configurado para gerar três fluxos de dados com diferentes marcações de classes de serviço no campo DSCP (*Differentiated Service Code Point*) do protocolo IP. Os parâmetros utilizados na geração de cada fluxo em cada um dos três cenários são apresentados na Tabela 5, um por coluna, sendo eles o tempo de execução em milissegundos, a quantidade de pacotes por segundo a serem gerados (PPS), a quantidade de *bytes* por pacote, o valor do campo DSCP do cabeçalho IP, o protocolo de camada de transporte utilizado (TCP ou UDP) e a taxa de dados gerada em cada fluxo. Apenas o número de pacotes por segundo do fluxo 1 (AC_BE) foi modificado para variar a quantidade de tráfego gerado. Criamos um agendamento no serviço `cron`[21] de cada STA participante, para que iniciassem os clientes do gerador de tráfego no mesmo horário. Um minuto antes do horário agendado para que a geração de tráfego fosse iniciada, iniciamos o servidor D-ITG na máquina conectada à rede cabeada.

- No passo 3, um minuto após o início programado para a geração de tráfego, iniciamos o servidor da aplicação *Alerts* no Servidor Médico Central e, em seguida, iniciamos o cliente *Alerts* no dispositivo pessoal, configurado para enviar 7558 pacotes de alerta médico com IDT (*Inter Departure Time*, ou Tempo Entre Partida) de 10 milissegundos. Essa quantidade de pacotes foi escolhida por resultar em um tempo total de envio de $\approx$ 5 minutos, de forma que não extrapolasse a janela de tempo de geração de tráfego pelo D-ITG. Medimos o tempo gasto no processo, a fim de garantir que todos os pacotes de alerta médico fossem enviados durante os 7 minutos de geração de tráfego e saturação da rede.

Tabela 5 – Parâmetros utilizados para geração de fluxos de tráfego sintético

STAs	Fluxo	Tempo (ms)	PPS	Bytes	DSCP	Protocolo	Taxa de dados
5	1	420000	725	1448	0	TCP	8,0 Mbps
	2	420000	38	1316	128	UDP	390,6 Kbps
	3	420000	128	64	184	UDP	64 Kbps
10	1	420000	362	1448	0	TCP	3,99 Mbps
	2	420000	38	1316	128	UDP	390,6 Kbps
	3	420000	128	64	184	UDP	64 Kbps
20	1	420000	181	1448	0	TCP	1,99 Mbps
	2	420000	38	1316	128	UDP	390,6 Kbps
	3	420000	128	64	184	UDP	64 Kbps

Fonte: Elaborado pelo autor (2021)

Os experimentos produziram 453.480 dados de atrasos de pacotes que foram analisados de acordo com o seguinte método:

[21] http://manpages.ubuntu.com/manpages/bionic/man8/cron.8.html

(i) preprocessamento dos dados;

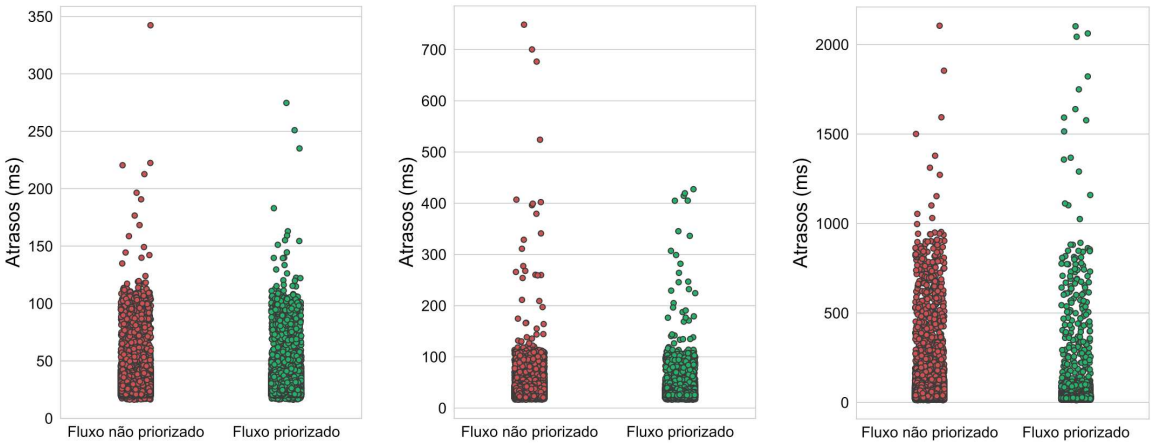
(ii) identificação da presença de *outliers*;

(iii) remoção dos *outliers*;

(iv) análises estatísticas;

No pré-processamento (i), foi gerado um *dataset* com os atrasos por pacote (em microssegundos) coletados no experimento, identificados por cenário de densidade e aplicação ou não de política de priorização. Um atraso nulo corresponde um pacote perdido. Os atrasos foram convertidos para milissegundos para facilitar a análise. Na fase de identificação de *outliers* (ii), verificamos uma alta dispersão dos dados, com alguns valores muito discrepantes, conforme pode ser observado na Figura 24. Considerando a alta variação na amplitude dos dados em cada cenário, a identificação de *outliers* foi realizada para cada um deles separadamente.

Figura 24 – Dispersão dos atrasos nos diferentes cenários de densidade



(a) Densidade baixa (b) Densidade média (c) Densidade alta

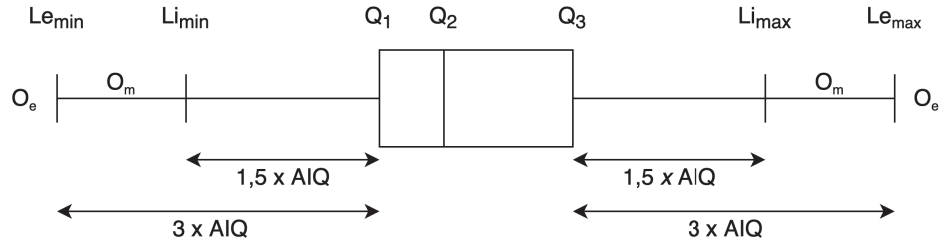
Fonte: Elaborado pelo autor (2021)

Um método bastante utilizado para identificar *outliers* em uma amostra foi apresentado por (60), quando popularizou o conceito de *box-and-whiskers*, também conhecido como diagrama de caixas, ou *boxplot*. Este método consiste em dividir as observações de uma amostra em quatro partes iguais, ou quartis, onde cada parte contém 25% dos dados. O primeiro quartil, Q_1, ou 0,25 percentil, é o valor até o qual se encontram 25% dos dados. O segundo quartil, Q_2, ou 0,5 percentil, é a mediana dos dados. O terceiro quartil, Q_3, ou 0,75 percentil, é o valor da amostra até onde se encontram 75% dos dados, e a partir do qual estão os 25% maiores valores da amostra. Entre Q_1 e Q_3 estão localizados 50% dos dados, e a diferença entre eles representa a amplitude interquartil, ou AIQ. Depois de calculados os valores dos quartis, são definidos os limites mínimo e máximo da amostra.

Esses valores correspondem a até 1,5 vezes a AIQ abaixo de Q_1 ($Q_1 - 1,5 \times AIQ$) e acima de Q_3 ($Q_3 + 1,5 \times AIQ$). Valores inferiores ao valor mínimo e superiores ao valor máximo são discrepantes e, portanto, são considerados "externos", ou simplesmente *outliers*.

Para amostras com alta dispersão dos dados, (60) propôs ainda a criação de limites extras, mais abrangentes. Além dos limites mínimo e máximo, que passam a ser **limites internos** mínimo e máximo, passam a existir também os **limites externos** mínimo e máximo. Esses valores correspondem a até 3 vezes a AIQ abaixo de Q_1 ($Q_1 - 3 \times AIQ$) e acima de Q_3 ($Q_3 + 3 \times AIQ$). Os *outliers* situados entre os limites internos e externos são chamados "externos". Já os situados fora dos limites externos são chamados "distantes". Os *outliers* "externos" e os "distantes" são comumente referenciados na literatura, respectivamente, como *outliers* "moderados" e "extremos", como pode ser visto em (47), sendo essa a terminologia utilizada também neste texto. Esse método é ilustrado na Figura 25, onde os *outliers* moderados (O_m) estão entre o limite inferior mínimo (Li_{min}) e o limite exterior mínimo (Le_{min}) e entre o limite interior máximo (Li_{max}) e o limite exterior máximo (Le_{max}). Valores menores que Le_{min} ou maiores Le_{max} são *outliers* extremos (O_e).

Figura 25 – *Boxplot* com limites interno e externo



Fonte: Adaptado de (60, 27)

A camada física de redes sem fio 802.11 possui muito ruído e características variáveis (46), uma vez que o sinal sem fio está sujeito a diversas interferências do meio. Por isso, é esperada uma considerável variação dos atrasos de alguns dos pacotes, que apesar de discrepantes em relação ao restante da amostra, são importantes na descrição de uma situação real de uso.

Em nossa amostra, alguns poucos atrasos se distanciam drasticamente dos demais. No cenário com 20 STAs sem priorização, houve atrasos entre 12,38 ms e 2.105,06 ms, mas dos 75.551 pacotes recebidos (29 foram perdidos), apenas 11 tiveram atrasos superiores a 1.000 ms. Esses valores muito discrepantes são *outliers* naturais, ou seja, não são frutos de medições incorretas ou erro de gravação dos dados, mas sim de flutuações das condições do sinal sem fio do ambiente testado. Conforme discutido por (14), se o analista de dados pretende amostrar a população livre de contaminações, ele deve ou remover os itens contaminantes ou aplicar procedimentos estatísticos para minimizar o efeito das

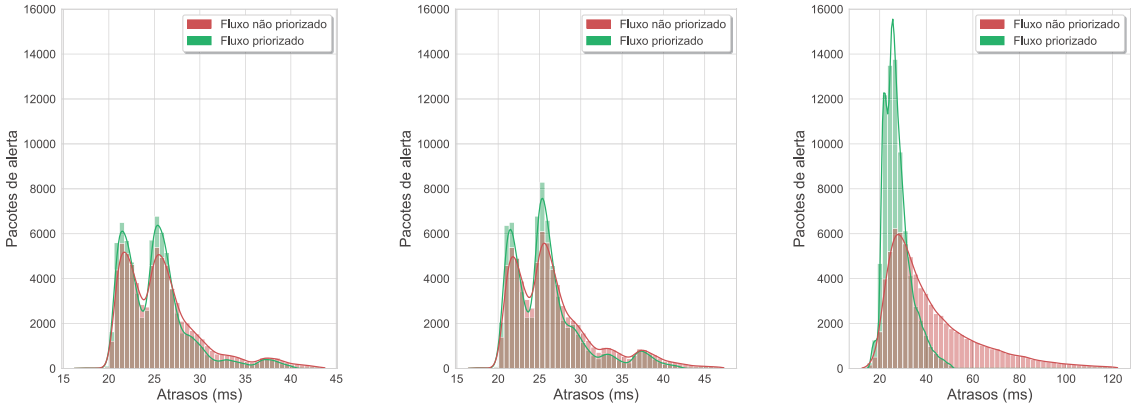
contaminações nas estimativas da população. Com isso, a fim de não descartar atrasos que podem ser importantes para descrever o comportamento geral da população, e ao mesmo tempo não prejudicar as análises estatísticas com valores muito discrepantes, optamos por manter os *outliers* moderados e remover apenas os *outliers* extremos, ou seja, aqueles que se distanciem mais do que três vezes a amplitude interquartil abaixo do primeiro quartil ou acima do terceiro quartil da amostra. Após removidos os *outliers* extremos, o *dataset* final manteve 98,45% dos dados.

Na fase de análise de dados (iv) avaliamos a distribuição dos atrasos obtidos em todos os cenários, assim como os efeitos da priorização dos pacotes de alerta médico na redução estatística dos atrasos e perdas desses pacotes.

5.3 RESULTADOS

A Figura 26 compara as distribuições dos atrasos nos três diferentes cenários de densidade. Como o intervalo de atrasos mensurados no cenário de densidade alta, ilustrado na Figura 26(c), foi consideravelmente maior, utilizamos escalas diferentes nos eixos das abscissas, que representam os atrasos, a fim de facilitar a visualização da imagem.

Figura 26 – Distribuição dos atrasos nos três cenários de densidade



(a) Densidade baixa (b) Densidade média (c) Densidade alta

Fonte: Elaborado pelo autor (2021)

No cenário representado na Figura 26(a), com densidade baixa, o atraso médio passou de 25,93 ms sem priorização, para 25,14 ms com priorização, uma redução de 3,06%. Uma redução igualmente pouco significativa foi observada no cenário da Figura 26(b), com densidade média, onde a média de atraso passou de 26,82 ms para 25,79 ms, uma redução de 3,81%. Já no cenário da Figura 26(c), com densidade alta, são observadas reduções consideráveis nos atrasos dos pacotes priorizados em comparação com os não priorizados, passando de 42,02 ms para 27,46 ms, uma redução de 34,65%.

A Tabela 6 apresenta os dados estatísticos obtidos a partir dos experimentos realizados nos três cenários. Importante observar que, sem a política de priorização, o atraso médio e o desvio padrão no cenário mais denso aumentaram muito em comparação com os demais cenários. Contudo, quando aplicada a priorização, esses valores ficaram bem próximos dos dados estatísticos observados nos cenários menos densos, demonstrando a redução do efeito da densificação da rede para pacotes de alerta médico quando aplicada a política de priorização. Além disso, com mais STAs disputando acesso ao meio, e consequente aumento no número de colisões, o número de pacotes perdidos é bastante superior no cenário com densidade alta. Porém, ao realizar a priorização desses pacotes, há uma redução de 58,62% das perdas observadas.

Tabela 6 – Latência e perda de pacotes por cenário de densidade com e sem priorização

Densidade	Priorizado	Pacotes Perdidos	Latência (ms)				
			Min.	Max.	Média	Mediana	Desvio Padrão
Baixa	Não	2	16,24	43,74	25,93	25,24	4,42
	Sim	1	16,20	40,32	25,14	24,92	3,74
Média	Não	0	16,38	47,32	26,82	25,72	5,12
	Sim	0	16,50	42,16	25,79	25,22	4,33
Alta	Não	29	12,38	122,14	42,02	35,82	19,28
	Sim	12	12,94	51,04	27,46	26,30	5,71

Fonte: Elaborado pelo autor (2021)

A Tabela 7 apresenta a redução percentual dos dados estatísticos quando é realizada a priorização do tráfego. Como pode ser observado, a redução do atraso médio no cenário de densidade alta foi de 34,65% e o desvio padrão teve redução de 70,40%, indicando significativa diminuição da dispersão dos atrasos observados.

Tabela 7 – Variação percentual das perdas e dos dados estatísticos de latência de pacotes de alerta médico ao se aplicar priorização de tráfego

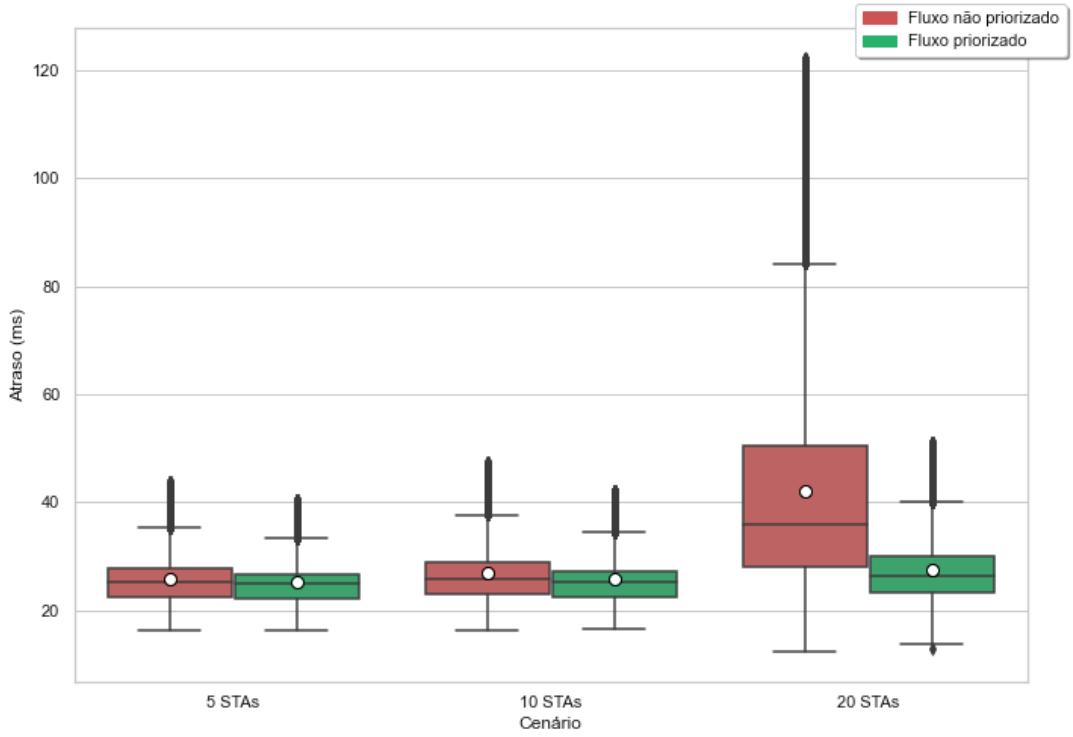
Densidade	Pacotes Perdidos	Latência (ms)				
		Min.	Max.	Média	Mediana	Desvio Padrão
Baixa	-50,00 %	-0,25 %	-7,82 %	-3,06 %	-1,27 %	-15,39 %
Média	0,00 %	0,73 %	-10,90 %	-3,81 %	-1,94 %	-15,46 %
Alta	-58,62 %	4,52 %	-58,21 %	-34,65 %	-26,58 %	-70,40 %

Fonte: Elaborado pelo autor (2021)

A redução na dispersão dos atrasos do cenário de densidade alta pode ser confirmada ao se observar a Figura 27, que apresenta um *boxblot* com as distribuições quantitativas dos atrasos observados em cada cenário de densidade. O eixo das ordenadas mostra os atrasos em milissegundos, e o eixo das abscissas mostra os três diferentes cenários

com e sem priorização do tráfego de pacotes de alerta médico. A média dos dados é apontada pelos marcadores brancos. Com um maior número de STAs conectadas, e maior competição pelo meio de comunicação sem fio, há uma maior dispersão dos atrasos de pacotes não priorizados, o que é evidenciado pelo *boxplot* do cenário de densidade alta, onde a amplitude interquartil dos dados não priorizados é muito maior do que a dos dados dos pacotes priorizados. A priorização do tráfego no cenário de densidade alta tornou possível manter os atrasos mais próximos aos dos cenários menos densos (os *boxplots* dos fluxos priorizados não diferem muito entre si), o que evidencia uma redução considerável dos efeitos da densificação da rede nesses atrasos.

Figura 27 – Variação dos atrasos dos pacotes de alerta médico por cenário de densidade



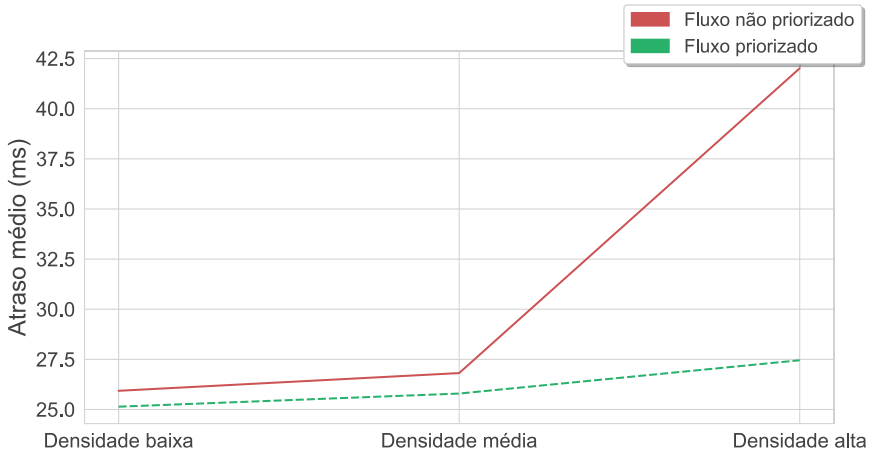
Fonte: Elaborado pelo autor (2021)

Ainda sobre o cenário de densidade alta na Figura 27, o limite máximo dos atrasos dos pacotes priorizados ficou abaixo da média dos atrasos quando não é feita priorização, e os valores de mais de 50% dos dados observados quando é feita a priorização de tráfego foram menores que a mediana dos dados observados quando não há priorização (0,5 percentil). Há uma assimetria positiva mais acentuada na distribuição dos atrasos dos pacotes sem priorização, com dados mais afastados da média, além de uma maior variabilidade de atrasos observados, com mais dados localizados entre o terceiro e o quarto quartis e uma média consideravelmente maior do que a mediana. Isso resultou em um alongamento da calda da distribuição para a direita, se estendendo por valores de atrasos maiores. Este comportamento pode ser observado no histograma da Figura 26(c). A

distribuição dos atrasos do fluxo priorizado é mais concentrada em torno da média e, em sua grande maioria, entre 20 e 40 milissegundos.

A Figura 28 mostra o atraso médio obtido em cada um dos cenários, com e sem priorização do tráfego de pacotes de alerta médico. Nos dois casos há uma suave tendência de subida na curva de atrasos médios, partindo do cenário de densidade baixa para o de densidade média. Já no cenário de densidade alta, a tendência de subida aumenta significativamente quando não é aplicada política de priorização, mantendo-se suave quando a política é aplicada. O aumento da quantidade de STAs conectadas disputando acesso ao canal de comunicação, reduz as chances que o dispositivo pessoal tem de transmitir dados. Essas chances são melhoradas estatisticamente com a aplicação da política de priorização.

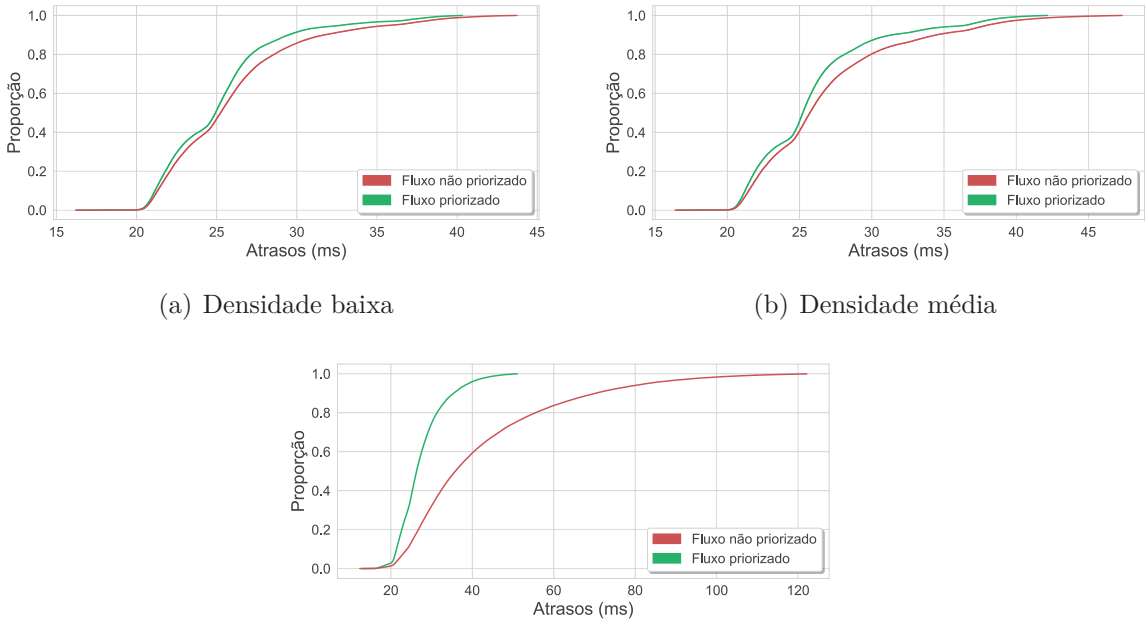
Figura 28 – Atraso médio dos pacotes de alerta médico por cenário de densidade



Fonte: Elaborado pelo autor (2021)

A Figura 29 mostra as ECDF (*Empirical Cumulative Distribution Functions*, ou Funções de Distribuição Acumulada Empíricas) dos atrasos observados com e sem priorização dos dados, em todos os cenários. O cenário da Figura 29(c), de densidade alta, é onde pode-se notar os melhores ganhos. Quando priorizados, 95,97% dos pacotes tiveram atrasos inferiores a 40 milissegundos. Sem priorização, o percentual de pacotes com atrasos inferiores a 40 ms cai para 59,34%. A curva dos dados empíricos também demonstra a similaridade no comportamento dos cenários das Figuras 29(a) e 29(b), respectivamente, cenários com densidades baixa e média.

Figura 29 – Função de distribuição acumulada empírica dos atrasos



(a) Densidade baixa

(b) Densidade média

(c) Densidade alta

Fonte: Elaborado pelo autor (2021)

6 CONCLUSÕES

Nesta dissertação, apresentamos uma plataforma baseada em Redes Sem Fio Definidas por Software (SDWN) para priorização de acesso ao meio para pacotes de alerta médico em redes sem fio hospitalares densas. A plataforma tem como propósito reduzir os atrasos e perdas de pacotes de alerta médico, priorizando dinamicamente o acesso desses pacotes ao canal de comunicação sem fio, a fim de dar suporte a aplicações críticas de monitoramento de saúde em hospitais. Para isso utilizamos o Ethanol, uma arquitetura SDWN para redes IEEE 802.11 WLAN. Implementamos funções para programabilidade de subcamada MAC de redes sem fio, que permitem manipular os parâmetros de QoS introduzidos pelo adendo IEEE 802.11e-2005. Avaliamos a plataforma em um ambiente real de rede sem fio, variando o número de STAs conectadas ao AP com o Ethanol ativado. Chamamos esses cenários de "densidade baixa", "densidade média" e "densidade alta", e conectamos em cada um, respectivamente, 5, 10 e 20 STAs. Os resultados demonstraram que a programabilidade dos parâmetros de QoS da subcamada MAC pelo Ethanol, possibilitou a priorização de acesso ao meio para pacotes de alerta médico, e reduziu o atraso médio desses pacotes em 3,06% no cenário de densidade baixa, 3,81% no cenário com densidade média, e 34.65% no cenário com densidade alta. Neste último cenário, a redução na quantidade de pacotes de alerta perdidos foi de 58.62%. É possível concluir, então, que a plataforma alcançou melhorias significativas de latência e perda para pacotes de alerta médico, importantes requisitos de QoS para aplicações críticas para monitoramento de saúde.

Como trabalhos futuros, destacamos a possibilidade de empregar algoritmos de aprendizado de máquina para definir parâmetros de contenção que melhorem o desempenho da plataforma, ao invés de configurar valores pré-definidos. Para isso, as funções de gerenciamento providas pelo Ethanol podem ser utilizadas para obter informações do estado da rede, como qualidade e potência do sinal sem fio, atrasos e perdas de pacotes, etc. Combinadas com os indicadores mensurados pela própria plataforma (como atraso e perda de pacotes de alerta médico), essas informações podem ser utilizadas para treinar modelos de aprendizagem de máquina, ou servir como *feedback* para algoritmos de aprendizado reforçado, ou RL (*Reinforcement Learning*). Com RL, nenhum conhecimento prévio da rede é necessário, e o resultado das alterações realizadas pelo módulo nos parâmetros de rede é utilizado pelo modelo para identificar quais conjuntos de configurações trazem melhores recompensas. No longo prazo, o módulo pode aprender a definir quais parâmetros trazem os melhores resultados para o desempenho da plataforma e da rede como um todo, realizando automaticamente as configurações necessárias.

REFERÊNCIAS

1 Abidi, B., Jilbab, A., and Mohamed, E. (2020). Wireless body area networks: a comprehensive survey. *Journal of Medical Engineering & Technology*, 44:1–11.

2 Albahri, O., Zaidan, A., Bahaa, B., Hashim, M., Albahri, A., and Alsalem, M. (2018). Real-Time Remote Health-Monitoring Systems in a Medical Centre: A Review of the Provision of Healthcare Services-Based Body Sensor Information, Open Challenges and Methodological Aspects. *Journal of Medical Systems*, 42.

3 Almes, G., Kalidindi, S., Zekauskas, M. J., and Morton, A. (2016). A One-Way Delay Metric for IP Performance Metrics (IPPM). `https://rfc-editor.org/rfc/rfc7679.txt`. Acesso em: 15 ago. 2021.

4 Avallone, S., Guadagno, S., Emma, D., Pescape, A., and Ventre, G. (2004). D-ITG distributed Internet traffic generator. In *First International Conference on the Quantitative Evaluation of Systems, 2004. QEST 2004. Proceedings.*, pages 316–317.

5 Bernardos, C. J., De La Oliva, A., Serrano, P., Banchs, A., Contreras, L. M., Jin, H., and Zúñiga, J. C. (2014). An architecture for software defined wireless networking. *IEEE Wireless Communications*, 21(3):52–61.

6 Bhandari, S. and Moh, S. (2016). A Priority-Based Adaptive MAC Protocol for Wireless Body Area Networks. *Sensors*, 16(3).

7 Bradai, N., Chaari Fourati, L., and Kamoun, L. (2015). WBAN Data Scheduling and Aggregation under WBAN/WLAN Healthcare Network. *Ad Hoc Netw.*, 25(PA):251–262.

8 Casado, M., Freedman, M. J., Pettit, J., Luo, J., McKeown, N., and Shenker, S. (2007). Ethane: Taking Control of the Enterprise. *SIGCOMM Comput. Commun. Rev.*, 37(4):1–12.

9 Cavallari, R., Martelli, F., Rosini, R., Buratti, C., and Verdone, R. (2014). A Survey on Wireless Body Area Networks: Technologies and Design Challenges. *IEEE Communications Surveys Tutorials*, 16(3):1635–1657.

10 Choi, S., del Prado, J., N, S. S., and Mangold, S. (2003). IEEE 802.11 e contention-based channel access (EDCF) performance evaluation. In *IEEE International Conference on Communications, 2003. ICC '03.*, volume 2, pages 1151–1156 vol.2.

11 Cisco (2020). Cisco Annual Internet Report (2018–2023). `https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf`. Acesso em: 3 nov. 2021.

12 Comer, D. E. (2015). *Interligação de redes com TCP/IP*, volume 1, page 900. Elsevier Editora Ltda., Rio de Janeiro, RJ, 6a edition.

13 da Silva, R. A., Santos, A., Nogueira, M., Boussetta, K., and Achir, N. (2016). Avoiding Collisions by Time Slot Reduction Supporting Voice and Video in 802.11 Networks. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6.

14 Dixon, W. J. (1950). Analysis of Extreme Values. *The Annals of Mathematical Statistics*, 21(4):488–506.

15 Fontes, R. R., Afzal, S., Brito, S. H. B., Santos, M. A. S., and Rothenberg, C. E. (2015). Mininet-WiFi: Emulating software-defined wireless networks. In *2015 11th International Conference on Network and Service Management (CNSM)*, pages 384–389.

16 Gast, M. (2005). *802.11 Wireless Networks: The Definitive Guide*. A Nutshell handbook. O'Reilly Media, Sebastopol, CA, 2 edition.

17 Gast, M. (2013). *802.11ac: A Survival Guide*. A Nutshell handbook. O'Reilly Media, Sebastopol, CA, first edition.

18 Gay, V. and Leijdekkers, P. (2007). A Health Monitoring System Using Smart Phones and Wearable Sensors. *International Journal of ARM*, 8(2):29 – 36.

19 Gummalla, A. C. V. and Limb, J. O. (2000). Wireless medium access control protocols. *IEEE Communications Surveys Tutorials*, 3(2):2–15.

20 Gündo, K. and Çalhan, A. (2016). An Implementation of Wireless Body Area Networks for Improving Priority Data Transmission Delay. *Journal of Medical Systems*, pages 1–7.

21 Hiertz, G. R., Denteneer, D., Stibor, L., Zang, Y., Costa, X. P., and Walke, B. (2010). The IEEE 802.11 universe. *IEEE Communications Magazine*, 48(1):62–70.

22 IEEE 802.11-2007 (2007). IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

23 IEEE 802.11-2020 (2020). IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

24 IEEE 802.15.6-2012 (2012). IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks.

25 Jagadeesan, N. A. and Krishnamachari, B. (2014). Software-Defined Networking Paradigms in Wireless Networks: A Survey. *ACM Comput. Surv.*, 47(2).

26 Jammal, M., Singh, T., Shami, A., Asal, R., and Li, Y. (2014). Software defined networking: State of the art and research challenges. *Computer Networks*, 72:74–98.

27 Jordanova, P. K. and Petkova, M. P. (2017). Measuring heavy-tailedness of distributions. *AIP Conference Proceedings*, 1910(1).

28 Khan, R. A. and Pathan, A.-S. K. (2018). The state-of-the-art wireless body area sensor networks: A survey. *International Journal of Distributed Sensor Networks*, 14(4).

29 Koprivica, M., Ilić, M., Nešković, A., Nešković, N., and Krajnović, N. (2011). Experimental evaluation of IEEE 802.11e EDCA QoS mechanism for voice over WLAN. In *2011 IEEE EUROCON - International Conference on Computer as a Tool*, pages 1–4.

30 Kreutz, D., Ramos, F. M. V., Veríssimo, P. E., Rothenberg, C. E., Azodolmolky, S., and Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE*, 103(1):14–76.

31 Kurose, J. F. and Ross, K. W. (2013). *Redes de computadores e a internet: uma abordagem top-dow*, pages 330–332. Pearson Education do Brasil, São Paulo, SP, 6 edition.

32 Latré, B., Braem, B., Moerman, I., Blondia, C., and Demeester, P. (2011). A Survey on Wireless Body Area Networks. *Wirel. Netw.*, 17(1):1–18.

33 Lee, J., Uddin, M., Tourrilhes, J., Sen, S., Banerjee, S., Arndt, M., Kim, K.-H., and Nadeem, T. (2014). MeSDN: Mobile Extension of SDN. In *Proceedings of the Fifth International Workshop on Mobile Cloud Computing & Services*, MCS '14, page 7–14, New York, NY, USA. Association for Computing Machinery.

34 Lei, T., Lu, Z., Wen, X., Zhao, X., and Wang, L. (2014). SWAN: An SDN based campus WLAN framework. In *2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE)*, pages 1–5.

35 Lv, Z., Xia, F., Wu, G., Yao, L., and Chen, Z. (2010). iCare: A Mobile Health Monitoring System for the Elderly. In *2010 IEEE/ACM Int'l Conference on Green Computing and Communications Int'l Conference on Cyber, Physical and Social Computing*, pages 699–705.

36 Malik, A., Qadir, J., Ahmad, B., Alvin Yau, K.-L., and Ullah, U. (2015). QoS in IEEE 802.11-based wireless networks: A contemporary review. *Journal of Network and Computer Applications*, 55:24–46.

37 McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., and Turner, J. (2008). OpenFlow: Enabling Innovation in Campus Networks. *SIGCOMM Comput. Commun. Rev.*, 38(2):69–74.

38 Mendes, J., Simões, H., Rosa, P., Costa, N., Rabadão, C., and Pereira, A. (2014). Secure Low-cost Solution for Elder's eCardio Surveillance. *Procedia Computer Science*, 27:46–56.

39 Misra, S. and Sarkar, S. (2015). Priority-Based Time-Slot Allocation in Wireless Body Area Networks During Medical Emergency Situations: An Evolutionary Game-Theoretic Perspective. *IEEE Journal of Biomedical and Health Informatics*, 19(2):541–548.

40 Motorola, I. (2004). *KeyStone Architecture Serial Peripheral Interface (SPI) User Guide*. V04.01.

41 Moura, H., Alves, A. R., Borges, J. R., Macedo, D. F., and Vieira, M. A. (2020). Ethanol: A Software-Defined Wireless Networking architecture for IEEE 802.11 networks. *Computer Communications*, 149:176 – 188.

42 Moura, H., Bessa, G. V. C., Vieira, M. A. M., and Macedo, D. F. (2015). Ethanol: Software defined networking for 802.11 Wireless Networks. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pages 388–396.

43 Moura, H. D., Fernandes Macedo, D., and Vieira, M. A. M. (2019). Automatic Quality of Experience Management for WLAN Networks using Multi-Armed Bandit. In *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pages 279–288.

44 Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., and Jamalipour, A. (2014). Wireless Body Area Networks: A Survey. *IEEE Communications Surveys Tutorials*, 16(3):1658–1686.

45 Napi, N., Zaidan, A., Bahaa, B., Albahri, O., Alsalem, M., and Albahri, A. (2019). Medical emergency triage and patient prioritisation in a telemedicine environment: a systematic review. *Health and Technology*, 9.

46 Ni, Q., Romdhani, L., and Turletti, T. (2004). A Survey of QoS Enhancements for IEEE 802.11 Wireless LAN: Research Articles. *Wirel. Commun. Mob. Comput.*, 4(5):547–566.

47 NIST/SEMATECH (2003). NIST/SEMATECH e-Handbook of Statistical Methods. `https://www.itl.nist.gov/div898/handbook/prc/section1/prc16.htm`. Acesso em: 18 ago. 2021.

48 Oliveira, A. T., Martins, B. J. C. A., Moreno, M. F., Gomes, A. T. A., Ziviani, A., and Borges Vieira, A. (2021). SDN-based architecture for providing quality of service to high-performance distributed applications. *International Journal of Network Management*, 31(5).

49 openvswitch (2021). Production Quality, Multilayer Open Virtual Switch. `https://www.openvswitch.org`. Acesso em: 3 nov. 2021.

50 Parulkar, G. (2020). SDN fundamentals: motivation, architecture, and benefits. *CSI Transactions on ICT*, 8:7–9.

51 Pfaff, B. and Davie, B. (2013). The Open vSwitch Database Management Protocol. RFC 7047.

52 Pramanik, P. K. D., Nayyar, A., and Pareek, G. (2019). Chapter 7 - WBAN: Driving e-healthcare Beyond Telemedicine to Remote Health Monitoring: Architecture and Protocols. In D. Jude, H. and Balas, V. E., editors, *Telemedicine Technologies*, pages 89–119. Academic Press.

53 Rashwand, S. and Misic, J. V. (2015). Bridging Between IEEE 802.15.6 and IEEE 802.11e for Wireless Healthcare Networks. *Ad Hoc Sens. Wirel. Networks*, 26:303–337.

54 Rawat, D. B. and Reddy, S. (2016). Recent advances on Software Defined Wireless Networking. In *SoutheastCon 2016*, pages 1–8.

55 Restuccia, F. (2021). IEEE 802.11bf: Toward Ubiquitous Wi-Fi Sensing. *ArXiv*, abs/2103.14918.

56 Schiller, J. (2003). *Mobile Communications*. Addison Wesley, Edinburgh Gate, Harlow, 2nd edition.

57 Semiconductors, N. (2014). *I2C-bus specification and user manual*. Rev. 6.

58 Sherwood, R., Gibb, G., Yap, K.-K., Appenzeller, G., Casado, M., McKeown, N., and Parulkar, G. (2010). Can the Production Network Be the Testbed? In *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation*, page 365–378, USA. USENIX Association.

59 Smith, G., Venkatesan, G., Reuss, E., Aboul-Magd, O., Ashley, A., Naveen, K., and Hart, B. (2008). 802.11 QoS Tutorial. `https://www.ieee802.org/1/files/public/docs2008/avb-gs-802-11-qos-tutorial-1108.pdf`. Acesso em: 6 nov. 2021.

60 Tukey, J. W. (1977). *Exploratory Data Analysis*. Addison-Wesley series in behavioral science. Addison-Wesley Publishing Company, Reading, Massachusetts.

61 Vergutz, A., da Silva, R., Vieira, A. B., and Nogueira, M. (2017). Um Sistema de Identificação Antecipada e Transmissão Prioritária de Alertas Médicos sobre WBAN e WLAN. In *Anais do XXXV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, Porto Alegre, RS, Brasil. SBC.

62 Vijay, B. and Malarkodi, B. (2016). Improved QoS in WLAN Using IEEE 802.11e. *Procedia Computer Science*, 89:17–26.

63 Xiao, Y. (2004). IEEE 802.11e: QoS provisioning at the MAC layer. *IEEE Wireless Communications*, 11(3):72–79.