UNIVERSIDADE FEDERAL FLUMINENSE

ALLYSSON CHAGAS CARAPEÇOS

# MECANISMOS DE DETECÇÃO DE COLISÃO EM REDES SEM FIO

NITERÓI 2022

#### ALLYSSON CHAGAS CARAPEÇOS

## MECANISMOS DE DETECÇÃO DE COLISÃO EM REDES SEM FIO

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Computação. Área de concentração: Ciência da Computação.

Orientador: DIEGO GIMENEZ PASSOS

> NITERÓI 2022

#### Ficha catalográfica automática - SDC/BEE Gerada com informações fornecidas pelo autor

C257m Carapeços, Allysson Chagas MECANISMOS DE DETECÇÃO DE COLISÃO EM REDES SEM FIO / Allysson Chagas Carapeços ; Diego Gimenez Passos, orientador. Niterói, 2022. 106 f. : il. Dissertação (mestrado)-Universidade Federal Fluminense, Niterói, 2022. DOI: http://dx.doi.org/10.22409/PGC.2022.m.01025375939 1. Perda de pacotes. 2. Detecção de colisão. 3. Reconhecimento de colisão. 4. Redes sem fio. 5. Produção intelectual. I. Passos, Diego Gimenez, orientador. II. Universidade Federal Fluminense. Instituto de Computação. III. Título. CDD -

Bibliotecário responsável: Debora do Nascimento - CRB7/6368

### ALLYSSON CHAGAS CARAPEÇOS

#### MECANISMOS DE DETECÇÃO DE COLISÃO EM REDES SEM FIO

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Computação. Área de concentração: Ciência da Computação.

Aprovada em março de 2022.

BANCA EXAMINADORA

Prof. Diego Gimenez Passos - Orientador, UFF

Cueso

Prof. Célio Vinicius Neves de Albuquerque, UFF

Juli, k

Prof. Rodrigo de Souza Couto, UFRJ

Este trabalho é dedicado ao meu pai, por ter sido um exemplo no empenho ao conciliar o estudo e trabalho, à minha mãe, por sempre me motivar a continuar estudando, até mesmo quando quis parar de estudar no primário, aos meus irmãos, pela paciência, dedicação e auxílio durante a educação primária e secundária, e por fim, à minha noiva pelo apoio e compreensão durante esta etapa.

## Agradecimentos

Agradeço a Deus e a Nossa Senhora Aparecida por terem proporcionado saúde para viver tudo que vivi, propiciando novos conhecimentos e oportunidades, fazendo novos colegas, levando amigos para vida toda.

Impossível deixar de agradecer meus pais, Airton Pereira Carapeços e Helena de Chagas Rodrigues, e meus irmãos, Deise Ane de Chagas Rodrigues Scalabrin e Elyzandro Carapeços, pelos ensinamentos, carinho, amor, dedicação, paciência, palavras de apoio e tudo que fizeram em prol de minha educação, o maior legado que eles podem me deixar.

À minha amiga, namorada e noiva, Tatiana Peiter, que compartilhou as angústias e conquistas, sendo sempre carinhosa, atenciosa e compreensiva, entendendo também cada um dos dias que estava cansado, devido horas, dias e semanas estudando e tentando transpor os desafios que o mestrado proporciona, e isso tudo sendo conciliado com minha agenda profissional.

Aos meus amigos e colegas que me apoiaram na realização desta formação e contribuíram para meu crescimento pessoal e profissional, em especial a Anselmo Luiz Éden Battisti, Davi Marcondes Rocha, Gustavo Rodrigues Vasconcelos, Odair Moreira de Souza, e aos Professores André Luiz Brun, Carlos José Maria Olguín e Guilherme Galante.

Aos gestores que tive na Dataprev, Bruno da Silva Passos, Bruno Manhães de Souza, Claudio Yuassa Tokoro, Giuliano Inácio Ferreira e Marcos de Jesus Vanzelli Arrais, que foram compreensivos para que eu pudesse conciliar o estudo e trabalho.

Por fim, agradeço todos os professores do IC-UFF que tive o prazer de conhecer. Em especial, tenho que agradecer dois que apostaram em minha dedicação e competência para conclusão do mestrado. Inicialmente o Professor Célio Vinicius Neves de Albuquerque, pelo direcionamento em um momento crítico, onde quase desisti deste sonho e objetivo, de concluir o Mestrado em Computação, em virtude de incompatibilidade com minha agenda profissional. Além disso, agradecê-lo por me apresentar o Professor Diego Gimenez Passos, que acreditou, incentivou, ensinou e me orientou, sendo sempre paciente e solícito, o que foi imprescindível na conclusão desta formação.

## Resumo

Perdas de pacotes são uma ocorrência comum nas redes sem fio. Estas perdas podem ser ocasionadas por colisões ou simplesmente pelo SNR baixo do canal, causando a redução da capacidade da rede e diminuição da vazão. A correta identificação do tipo de perda de pacotes possibilita a otimização do uso do meio. Por exemplo, é possível reduzir o overhead com o gasto desnecessário de energia para retransmissões de pacotes, utilizando uma aplicação adequada de acordo com o tipo de perda específico. Nos últimos anos, algumas abordagens surgiram com o objetivo de efetuar a distinção e diagnóstico do tipo de perda, fazendo uso de diferentes tipos de técnicas. No entanto, não há na literatura trabalhos que organizem estas abordagens. Desta maneira, inicialmente este trabalho propõe uma taxonomia que inclui análise das propostas, discussão dos métodos de avaliação utilizados pelos autores, viabilidade e eficiência das abordagens. Ademais, o objetivo principal deste trabalho é propor um novo método para identificação do tipo de perda de pacotes em redes sem fio IEEE 802.11. O método introduz bits de controle multiplexados juntamente aos bits de dados do pacote transmitido. No entanto, esses bits de controle são transmitidos de forma mais robusta — e.g., utilizando combinações mais robustas de modulação e codificação — em comparação aos bits de dados. Assim, em caso de perda do pacote, um algoritmo de decisão é executado no receptor. A avaliação realizada mostra que o método proposto possui boa acurácia na identificação do tipo de perda, principalmente para taxas de dados mais elevadas. Em particular, resultados comparativos indicam que o método pode ser usado de forma complementar a outros da literatura, apresentando bom desempenho em situações nas quais outros são menos eficientes.

**Palavras-chave**: Perda de pacotes — Detecção de colisão — Reconhecimento de colisão — Redes sem fio

## Abstract

Packet losses are a common occurrence on wireless networks. These packet losses can be caused by collisions or simply by the low SNR of the channel, causing a decrease in the network capacity and throughput. The correct identification of the type of packet loss enables the optimization of the use of the medium. For example, it is possible to reduce overhead and unnecessary energy consumed for retransmitting packets, using an appropriate application according to the specific type of packet loss. In recent years, some approaches have emerged with the aim of distinguishing and diagnosing the type of packet loss, using different techniques. However, there are no studies in the literature that organize these approaches. Thus, initially this work proposes a taxonomy that includes analysis of the proposals, discussion of the evaluation methods used by the authors, feasibility and efficiency of the approaches. Furthermore, the main objective of this work is to propose a new method for identifying the type of packet loss in IEEE 802.11 networks. The method introduces control bits that are multiplexed along with the transmitted frames. However, those control bits are sent in a more robust fashion - e.g., with more robust combinations of modulation and coding — in comparison to the data bits. Then, in case of loss, a decision algorithm is executed on the receiver. In particular, comparative results indicate that the method can be used in a complementary way to others in the literature, presenting good performance in situations in which others are less efficient.

Keywords: Packet loss — Collision detection — Collision recognition — Wireless LAN

# Lista de Figuras

1	Subportadoras OFDM para redes sem fio IEEE 802.11a (MAGLOGIAN- NIS, 2018)	34
2	Fluxograma do algoritmo para detecção e identificação da perda $\ .\ .\ .$	35
3	Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11g	40
4	Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 160 MHz	41
5	Sem colisões: taxa de efetividade do método para emenda IEEE 802.11 g. $% \left( {{{\rm{E}}} \right)_{\rm{e}}} \right)$	41
6	Sem colisões: taxa de efetividade do método para emenda IEEE 802.11ac @ 160 MHz	42
7	Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11g.	43
8	Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 160 MHz	44
9	Com colisões: taxa de efetividade do método para emenda IEEE $802.11\mathrm{g.}$ .	44
10	Com colisões: taxa de efetividade do método para emenda IEEE 802.11ac @ 160 MHz	45
11	Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11g.	47
12	Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 160 MHz	47
13	Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de efetividade do método para emenda IEEE 802.11g.	48

14	Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de efetividade do método para emenda IEEE 802.11ac @ 160 MHz	48
15	Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11g	50
16	Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11n @ 20 MHz	51
17	Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11n @ 40 MHz	52
18	Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac $@$ 20 MHz. $~.$	53
19	Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac $@$ 40 MHz. $\ .$ .	53
20	Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac $@$ 80 MHz. $\ .$ .	54
21	Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac $@$ 160 MHz. $% =$ .	55
22	Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac @ 160 MHz, comparando método proposto original e método proposto com duas subportadoras no cenário sem colisão	56
23	Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac @ 160 MHz, comparando método proposto original e método proposto com duas subportadoras no cenário com colisão	56
24	Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac @ 160 MHz, comparando método proposto original e método proposto com duas subportadoras no cenário com colisão e pacote colidente com potência mais baixa.	57

transmissão de 6 Mb/s na emenda IEEE 802.11<br/>g@20 MHz. . . . . . . . . 59

26	Árvore de classificação de valores de EVM - conjunto de dados para taxa de transmissão de 6 Mb/s na emenda IEEE 802.11g @ 20 MHz. $\ldots$ .	60
27	Árvore de classificação de valores de EVM - conjunto de dados para taxa de transmissão de 54 Mb/s na emenda IEEE 802.11g @ 20 MHz	61
28	Gráfico de dispersão de valores de EVM - conjunto de dados para taxa de transmissão de 54 Mb/s na emenda IEEE 802.11g @ 20 MHz. $\ldots$	61
29	Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário sem colisão para emenda IEEE 802.11g @ 20 MHz	62
30	Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário com colisão para emenda IEEE 802.11g @ 20 MHz	63
31	Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário com colisão com pacote colidente com potência mais baixa para emenda IEEE 802.11g @ 20 MHz	63
32	Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário sem colisão para emenda IEEE 802.11n @ 40 MHz	64
33	Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário com colisão para emenda IEEE 802.11n @ 40 MHz	64
34	Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário com colisão com pacote colidente com potência mais baixa para emenda IEEE 802.11n @ 40 MHz	65
35	Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário sem colisão para emenda IEEE 802.11ac @ 80 MHz.	66
36	Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário com colisão para emenda IEEE 802.11ac @ 80 MHz	66

37	Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário com colisão com pacote colidente com potência mais baixa para emenda IEEE 802.11ac @ 80 MHz	67
38	Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11n @ 20 MHz	78
39	Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11n @ 40 MHz	78
40	Sem colisões: taxa de efetividade do método para emenda IEEE 802.11n @ 20 MHz	79
41	Sem colisões: taxa de efetividade do método para emenda IEEE 802.11n @ 40 MHz	79
42	Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 20 MHz	80
43	Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 40 MHz	81
44	Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 80 MHz	81
45	Sem colisões: taxa de efetividade do método para emenda IEEE 802.11ac @ 20 MHz	82
46	Sem colisões: taxa de efetividade do método para emenda IEEE 802.11ac @ 40 MHz	82
47	Sem colisões: taxa de efetividade do método para emenda IEEE 802.11ac @ 80 MHz	83
48	Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11n @ 20 MHz	85
49	Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11n @ 40 MHz	85
50	Com colisões: taxa de efetividade do método para emenda IEEE 802.11n @ 20 MHz	86

51	Com colisões: taxa de efetividade do método para emenda IEEE 802.11n @ 40 MHz	86
52	Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 20 MHz	87
53	Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 40 MHz	88
54	Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 80 MHz	88
55	Com colisões: taxa de efetividade do método para emenda IEEE 802.11ac @ 20 MHz	89
56	Com colisões: taxa de efetividade do método para emenda IEEE 802.11ac @ 40 MHz	89
57	Com colisões: taxa de efetividade do método para emenda IEEE 802.11ac @ 80 MHz	90
58	Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11n @ 20 MHz	91
59	Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11n @ 40 MHz	92
60	Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de efetividade do método para emenda IEEE 802.11n @ 20 MHz	93
61	Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de efetividade do método para emenda IEEE 802.11n @ 40 MHz	93
62	Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 20 MHz	94

63	Com colisões quando a potência do pacote colidente é mais baixa que a do	
	pacote principal: taxa de entrega de pacotes de dados e bits de controle	
	para emenda IEEE 802.11ac @ 40 MHz	95
64	Com colisões quando a potência do pacote colidente é mais baixa que a do	
	pacote principal: taxa de entrega de pacotes de dados e bits de controle	
	para emenda IEEE 802.11ac @ 80 MHz	95
65	Com colisões quando a potência do pacote colidente é mais baixa que a	
	do pacote principal: taxa de efetividade do método para emenda IEEE	
	802.11ac @ 20 MHz	96
66	Com colisões quando a potência do pacote colidente é mais baixa que a	
	do pacote principal: taxa de efetividade do método para emenda IEEE	
	802.11ac @ 40 MHz	96
67	Com colisões quando a potência do pacote colidente é mais baixa que a	
	do pacote principal: taxa de efetividade do método para emenda IEEE	
	802.11ac @ 80 MHz	97

# Lista de Tabelas

1	Abordagens de acordo com a taxonomia	16
2	Identificação do valor de SNR a partir do qual cada taxa de transmissão resulta em uma probabilidade de entrega maior que 50% para a emenda IEEE 802.11g	37
3	Identificação do valor de SNR a partir do qual cada taxa de transmissão resulta em uma probabilidade de entrega maior que 50% para a emenda IEEE 802.11n	38
4	Identificação do valor de SNR a partir do qual cada taxa de transmissão resulta em uma probabilidade de entrega maior que 50% para a emenda IEEE 802.11ac	39
5	Melhores taxas para a porção de controle para cada taxa de dados na emenda IEEE 802.11g (Mb/s)	49
6	Melhores taxas para a porção de controle para cada taxa de dados na emenda IEEE 802.11n (Mb/s)	50
7	Melhores taxas para a porção de controle para cada taxa de dados na emenda IEEE 802.11ac (Mb/s). $\ldots$	50

## Lista de Abreviaturas e Siglas

AID Association ID

**ARF** Auto Rate Fallback

BEDR Bit Error Distribution Ratio

BER Bit Error Rate

CART Classification And Regression Tree

**CMT** Change of Mean Test

**COLLIE** Collision Inferencing Engine

**CRC** Cyclic Redundancy Check

**CRM-GD** Collision Recognition Mechanism Based on Generating Domains

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

CSMA/CN Carrier Sense Multiple Access with Collision Notification

CSMA/ECA Carrier Sense Multiple Access with Enhanced Collision Avoidance

CST The Chi-square Test of Independence

EVM Error Vector Magnitude

FFT Fast Fourier Transform

GD Generating Domains

**IEEE** Institute of Electrical and Electronics Engineers

IoT Internet of Things

iWWT Illinois Wireless Wind Tunnel

- LQI Link Quality Indicator
- MAC Media Access Control

MIMO Multiple Input Multiple Output

MWW Mann-Whitney-Wilcoxon Test

**OFDM** Orthogonal Frequency Division Multiplexing

PCC Packet Corruption Classifier

PLFC Packet-Level Failure Classifier

 $\mathbf{RSSI}$  Received Signal Strength Indicator

**SEDR** Symbol Error Distribution Ratio

**SNR** Signal-to-Noise Ratio

**USRP** Universal Software Radio Peripheral

Wi-Fi Wireless Fidelity

# Sumário

1	Intr	odução	12
	1.1	Motivação	12
	1.2	Principais contribuições	13
	1.3	Organização do texto	14
2	Tra	balhos Relacionados	15
	2.1	Taxonomia	15
		2.1.1 Calibração ou treinamento	15
		2.1.2 Feedback	16
		2.1.3 Overhead	17
		2.1.4 Detecção contínua de preâmbulo	17
	2.2	Calibração ou treinamento	17
	2.3	Feedback	22
	2.4	Overhead	26
	2.5	Detecção contínua de preâmbulo	26
	2.6	Tipos de aplicação	28
		2.6.1 Adaptação da taxa de transmissão	29
		2.6.2 Otimização do <i>backoff</i>	31
3	Proj	posta para o diagnóstico do tipo de perda em redes IEEE 802.11	32
	3.1	Fundamentação teórica	32
	3.2	Método para o diagnóstico do tipo de perda em redes IEEE 802.11	33

		3.2.1 Introdução de bits de controle	33
		3.2.2 Algoritmo de decisão no receptor	34
4	Aval	iação de Desempenho	<b>36</b>
	4.1	Cenário sem colisão	40
	4.2	Cenário com colisão entre pacotes de mesma potência	43
	4.3	Cenário com colisão com pacote colidente com potência mais baixa	46
	4.4	Melhor relação entre taxa de transmissão de pacotes de dados e bits de controle	49
	4.5	Adicionando subportadora para transmissão de bits de controle	54
	4.6	Comparação entre o método proposto e um mecanismo baseado em EVM .	57
5	Con	clusão	<b>68</b>
	5.1	Trabalhos futuros	70
RI	EFER	ÊNCIAS	71
Ap	pêndio	e A - SIMULADOR PERSONALIZADO	75
Aj	pêndic	e B - RESULTADOS COMPLEMENTARES	77
	B.1	Cenário sem colisão	77
	B.2	Cenário com colisão entre pacotes de mesma potência	84
	B.3	Cenário com colisão com pacote colidente com potência mais baixa	91

## 1 Introdução

Nos últimos anos, o número de dispositivos aptos a utilizar redes sem fio tem crescido acentuadamente. Estes dispositivos estão presentes em redes domésticas, comerciais e industriais. De acordo com a Cisco (CISCO, 2020), a quantidade pontos de acesso de redes sem fio Wi-Fi crescerá quatro vezes entre 2018 e 2023, podendo haver aproximadamente 628 milhões de pontos acessos ao final desse período. Há de se considerar também a franca expansão do mercado de IoT (*Internet of Things*), que pode chegar a aproximadamente 83 bilhões de dispositivos conectados em 2024 (JUNIPERRESEARCH, 2020), sendo que uma parte destes dispositivos utilizam as redes sem fio locais.

As redes sem fio são capazes de fazer transferências de pequenos e grandes volumes de dados, de acordo com as características do padrão adotado. Além do volume, é necessário levar em consideração a criticidade da informação a ser transmitida. Neste caso, informações referentes a medições de sensores, por exemplo, apesar de pequenas, podem ser de extrema importância.

### 1.1 Motivação

Em redes IEEE 802.11, o padrão de fato para redes locais sem fio, utiliza-se o protocolo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) (IEEE, 1997). No CSMA/CA, um nó só transmite quando julga que o canal está livre. Mesmo assim, o padrão supracitado é suscetível a colisões, seja pela sincronização das tentativas de transmissão de dois nós ou pela ocorrência de terminais ocultos. Quando níveis de colisão aumentam significativamente, há uma redução significativa da capacidade da rede e diminuição da vazão (BULHÕES; PASSOS; ALBUQUERQUE, 2016). No entanto, colisões não são a única possível razão para perda de pacotes. Pacotes podem ser perdidos também por conta de um SNR (*Signal-to-Noise Ratio*) baixo do canal de comunicação.

Conhecer a razão para as perdas de pacote em um determinado enlace pode ser uma ferramenta valiosa para a otimização do funcionamento da rede. Por exemplo, em (VU-

TUKURU; BALAKRISHNAN; JAMIESON, 2009) e (SEN; SANTHAPURI et al., 2010) os autores propõem abordagens para determinar a taxa de transmissão mais adequada. Técnicas de adaptação de taxa são capazes de reduzir a ocorrência de perdas de pacotes causadas por SNR baixo. No entanto, se as perdas em um enlace são majoritariamente causadas por colisões, reduzir a taxa de transmissão resultará em maior gasto de energia e uma menor capacidade do canal, sem sanar a causa correta da perda de pacotes, e piorando devido a competição pelo meio de transmissão. Por outro lado, protocolos de acesso ao meio, como o CSMA/CA, tratam perdas de pacote por SNR baixo da mesma forma que colisões, acionando um *backoff* potencialmente desnecessário incapaz de resolver o problema que efetivamente levou à perda.

#### **1.2** Principais contribuições

Com o objetivo de distinguir as causas de perdas de pacotes em redes sem fio, algumas abordagens foram apresentadas nos últimos anos. Essas abordagens utilizam vários tipos de técnicas diferentes. Assim, este trabalho propõe uma taxonomia para organizá-las.

Além disso, este trabalho propõe um novo método com a finalidade de identificar a causa da perda de pacotes em redes sem fio IEEE 802.11. O método se vale do uso do OFDM (*Orthogonal Frequency Division Multiplexing*) por parte do IEEE 802.11 — o que ocorre desde as emendas a e g — para introduzir bits de controle que são multiplexados juntamente aos bits de dados do pacote original. Como as subportadoras no OFDM podem ser moduladas e codificadas independentemente, os bits de controle são transmitidos utilizando combinações mais robustas de modulação e codificação. Conforme detalhado no decorrer deste trabalho, em caso de corrupção dos bits de dados, a análise desses bits de controle — em particular, se também foram corrompidos ou não — permite que o receptor execute um simples algoritmo de decisão para discernir o tipo de perda. O método não exige qualquer modificação no formato do quadro na camada de enlace, porque as informações de controle são adicionadas no nível dos símbolos OFDM, evitando maiores problemas relacionados a compatibilidade. Além disso, a avaliação de desempenho conduzida neste trabalho mostra que o método é capaz de apresentar boa acurácia na distinção da causa das perdas de pacotes.

### 1.3 Organização do texto

Este trabalho está dividido da seguinte maneira. No Capítulo 2, é proposta uma taxonomia baseada nas principais características dos trabalhos encontrados na literatura. Em seguida, no Capítulo 3, é feita uma fundamentação teórica e também apresentada a proposta da abordagem para identificar a causa da perda de pacotes. Posteriormente, no Capítulo 4, são apresentadas as metodologias para avaliação e os resultados obtidos. Ao final, no Capítulo 5, são apresentadas as considerações finais e a discussão dos trabalhos futuros.

## 2 Trabalhos Relacionados

Devido à grande utilidade que a correta distinção das causas de perdas de pacotes em redes sem fio proporciona, é possível encontrar na literatura diversas abordagens propostas para esse fim. Essas abordagens utilizam vários tipos de técnicas diferentes. Neste sentido, este trabalho propõe uma taxonomia para organizá-las.

### 2.1 Taxonomia

É possível classificar os métodos de distinção de causa da perda de pacotes de diversas formas, incluindo: necessidade de calibração ou treinamento, se depende do *feedback* do receptor, se introduz *overhead* significativo, e se faz detecção contínua de preâmbulo. Esta taxonomia é apresentada na Tabela 1 e será discutida nas seguintes subseções. A Tabela 1 também mostra como diversas propostas encontradas na literatura são classificadas de acordo com esses critérios. Ao final, na linha destacada, é possível identificar o método proposto que será apresentado no Capítulo 3.

É importante salientar que a classificação não é mutuamente exclusiva. Na verdade, a taxonomia proposta não tem propriamente classes, mas atributos que podem ser usados para entender cada proposta. No decorrer do trabalho serão identificadas várias propostas que possuem atributos correspondentes a duas ou mais classificações.

#### 2.1.1 Calibração ou treinamento

Nesta categoria, é utilizado o conceito de calibração ou treinamento do método para distinguir a perda de pacotes e, em seguida, tratá-la. A ideia é analisar o ambiente previamente, juntando informações que auxiliem na distinção da causa da perda de pacotes.

As informações analisadas variam de acordo com a abordagem. Em (AMAN; SIK-DAR, 2012) é apresentado um mecanismo baseado em EVM (*Error Vector Magnitude*), onde é calculada a diferença entre o valor complexo da tensão entre um símbolo ideal e

Artigos	Calibração ou treinamento	Feedback	Overhead	Detecção contínua de preâmbulo
(AMAN; SIKDAR, 2012)	√	-	-	-
(AMAN; SIKDAR, 2012) (ZHU; SUN, 2015)	$\checkmark$	-	-	-
(AMAN; SIKDAR, 2012) (ZHU; SUN, 2015) (WHITEHOUSE et al., 2005)	✓ ✓ -	- - -	- - -	- - \
(AMAN; SIKDAR, 2012) (ZHU; SUN, 2015) (WHITEHOUSE et al., 2005) (WU et al., 2019)	✓ ✓ - ✓	- - -	- - -	- - -
(AMAN; SIKDAR, 2012) (ZHU; SUN, 2015) (WHITEHOUSE et al., 2005) (WU et al., 2019) (SEN; ROY CHOUDHURY; NELAKUDITI, 2012)	✓ ✓ ✓ – –	- - - -	- - - -	- - - - -
(AMAN; SIKDAR, 2012) (ZHU; SUN, 2015) (WHITEHOUSE et al., 2005) (WU et al., 2019) (SEN; ROY CHOUDHURY; NELAKUDITI, 2012) (ZENG; KUMAR, 2008)	✓ ✓ - ✓ - ✓	- - - - -	- - - - -	- - - - - -
(AMAN; SIKDAR, 2012) (ZHU; SUN, 2015) (WHITEHOUSE et al., 2005) (WU et al., 2019) (SEN; ROY CHOUDHURY; NELAKUDITI, 2012) (ZENG; KUMAR, 2008) (PENG; CHENG; SIKDAR, 2007)	✓ ✓ - ✓ - ✓ -	- - - - -	- - - - -	- - - - - - -
(AMAN; SIKDAR, 2012) (ZHU; SUN, 2015) (WHITEHOUSE et al., 2005) (WU et al., 2019) (SEN; ROY CHOUDHURY; NELAKUDITI, 2012) (ZENG; KUMAR, 2008) (PENG; CHENG; SIKDAR, 2007) (RAYANCHU et al., 2008)	✓ ✓ - ✓ - - - -	- - - - - - - - - - - - - -	- - - - - - - -	- - - - - - -
(AMAN; SIKDAR, 2012) (ZHU; SUN, 2015) (WHITEHOUSE et al., 2005) (WU et al., 2019) (SEN; ROY CHOUDHURY; NELAKUDITI, 2012) (ZENG; KUMAR, 2008) (PENG; CHENG; SIKDAR, 2007) (RAYANCHU et al., 2008) (JI-HOON YUN; SEUNG-WOO SEO, 2006)	✓ ✓ ✓ - ✓ - - - - -	- - - - - - - / / /	- - - - - - - - -	- - - - - - - - -

Tabela 1: Abordagens de acordo com a taxonomia

o sinal real recebido, e árvores de classificação e regressão são usadas para determinar a causa da perda de pacotes. Já em (ZHU; SUN, 2015), são coletadas informações acerca de indicadores da intensidade do sinal recebido pelos receptores e da qualidade do link no nível do pacote, avaliando a taxa de erro no preâmbulo, para posteriormente efetuar a calibração e definir limiares para as causas de perda de pacotes. A abordagem adotada em (WU et al., 2019) baseia-se em informações de erro no nível de bits e símbolos, posteriormente utilizadas para aprendizado de máquina. Em (ZENG; KUMAR, 2008) são analisadas informações da camada física no sistema OFDM a fim de fundamentar um classificador que identifica a causa de perda de pacotes. Mais detalhes acerca das abordagens propostas serão apresentadas na Seção 2.2.

#### 2.1.2 Feedback

A segunda categoria da taxonomia diz respeito a abordagens que fazem uso de *feedback* ou retroalimentação. Nesse contexto, *feedback* pode ser basicamente para comparação entre

o pacote enviado e recebido, mas também com o uso de técnicas, informações ou métricas para avaliar os resultados de uma transmissão.

#### 2.1.3 Overhead

Para a correta distinção das causas de perda de pacotes em redes sem fio, algumas abordagens utilizam técnicas que podem gerar *overhead*. Nesta categoria estão as abordagens onde são necessários pulsos, bits redundantes e até mesmo o uso exclusivo de subportadoras para bits de controle.

#### 2.1.4 Detecção contínua de preâmbulo

A fim de preparar o receptor para uma transmissão, o preâmbulo tem como objetivo auxiliar para que a interpretação do quadro recebido seja correta. Para isso, o preâmbulo possibilita que seja feita a escolha da antena com melhor sinal e a devida sincronização entre o transmissor e receptor. Nesta categoria, são apresentadas abordagens que usam detecção contínua de preâmbulo, porém com o objetivo de identificar colisões.

#### 2.2 Calibração ou treinamento

Dadas as características de cada categoria da taxonomia, nesta seção serão apresentadas em detalhes as propostas categorizadas como calibração ou treinamento.

Um exemplo de proposta na categoria calibração ou treinamento utiliza um mecanismo baseado em EVM e árvores de classificação e regressão para determinar a causa da perda de pacotes (AMAN; SIKDAR, 2012). Um vetor de erro é a diferença entre o valor complexo da tensão entre um símbolo ideal e o sinal real recebido.

A metodologia proposta tenta encontrar um limiar para EVM, possibilitando a distinção entre SNR baixo e colisão. O limiar é encontrado por meio de CART (*Classification And Regression Tree*). Este modelo foi usado para encontrar o valor limite  $\gamma$ , efetuando um treinamento com base em dados simulados e em um conjunto de regras.

Durante os testes executados pelos autores foram criados dois cenários simulados no Matlab. Inicialmente foi feito o treinamento do modelo CART, onde os transmissores são colocados a uma distância entre 3 e 40 metros do receptor. O primeiro cenário era composto por dois transmissores a uma mesma distância do receptor. Para esse cenário, o modelo obteve 97% de precisão na detecção do tipo de perda. No segundo cenário, um transmissor é colocado a 5 metros do receptor, e o outro a uma distância maior, obtendo entre 73% e 94% de precisão na detecção. Conforme a distância do segundo transmissor aumenta, a taxa de detecção errada (quando colisão é classificada erroneamente como SNR baixo) aumenta significativamente (AMAN; SIKDAR, 2012).

Em boa parte dos testes executados pelos autores, a abordagem utilizada apresentou números satisfatórios, porém há necessidade de um treinamento. Este treinamento deve ser executado frequentemente para que o limiar se adapte de acordo com as modificações do ambiente, aumentando assim o *overhead*. A frequência do treinamento irá depender das modificações do ambiente, pois um limiar pode ser válido para um dado ambiente, e não necessariamente para outro.

Uma segunda proposta, chamada PLFC (*Packet-Level Failure Classifier*) (ZHU; SUN, 2015), utiliza o RSSI (*Received Signal Strength Indicator*) e LQI (*Link Quality Indicator*) no nível de pacotes. Foram analisados dois mecanismos como motivação: a retransmissão baseada em colisões e retransmissão baseada em SNR baixo. Nos dois mecanismos há um limite de 10 retransmissões.

No mecanismo de retransmissão baseada em colisões, efetua-se *backoff* e até 5 retransmissões. Após as 5 retransmissões, caso a colisão persista, a potência de transmissão é aumentada para as próximas 5 retransmissões. A premissa é que, se somente após o aumento de potência o pacote for entregue, as perdas seriam causadas por SNR baixo, e não por colisões. Ao final, se o problema for classificado como de SNR baixo, as 5 primeiras retransmissões poderiam ter sido evitadas. No outro mecanismo de retransmissão, o baseado em SNR baixo, utiliza-se o procedimento inverso: aumenta-se a potência de transmissão para as primeiras 5 retransmissões. Caso as perdas persistam, o *backoff* é introduzido após a  $5^{a}$  retransmissão.

Para efetuar a classificação de perda e decidir qual dos dois mecanismos de retransmissão utilizar, os autores utilizam duas métricas, RSSI e LQI. RSSI é o indicador da intensidade do sinal de transmissão recebido pelos receptores de pacotes, enquanto LQI reflete a qualidade do link no nível do pacote, avaliando a taxa de erro no preâmbulo. Segundo os autores, pacotes corrompidos por colisão geralmente têm LQI melhor com relação aos corrompidos por SNR baixo, o que pode ser utilizado para diferenciar as causas das perdas (ZHU; SUN, 2015).

A proposta necessita de calibração de dois limitares  $\alpha$  e  $\beta$  para as métricas RSSI e LQI, respectivamente. São desenvolvidas 3 regras para a classificação: 1) quando o RSSI

ultrapassa o limiar  $\alpha$ , o pacote é rotulado como *Rise*; 2) quando o RSSI fica abaixo do limiar  $\alpha$ , o pacote é rotulado como *Fall* (se houver *Fall* enquanto o pacote estiver rotulado como *Rise*, ele é rotulado como *Peak*); e 3) se o pacote for rotulado como *Rise* ou *Fall*, e LQI for maior que  $\beta$ , o PLFC classifica que houve uma colisão (caso contrário é classificado como SNR baixo). Quando aplicados em diferentes ambientes internos,  $\alpha \in \beta$  podem ser configurados com base na potência de transmissão, distância entre o transmissor e receptor, e a condição do enlace. No entanto, os autores não apresentam uma solução para estimativa dos parâmetros, a não ser através da execução de testes preliminares.

Na avaliação conduzida pelos autores, utilizou-se  $\alpha$  de 3 dB e  $\beta$  de 95. Durante os testes, foram detectadas redes IEEE 802.11 que não estavam sob o controle dos autores, bem como movimentação aleatória de humanos no ambiente. Foram criados dois cenários: primeiro, utilizando um receptor fixo; e o segundo, com um receptor móvel. Nos dois cenários existiam 10 nós transmissores fixos. Ao medir taxa de classificação e atraso, o PLFC obteve 93,1% de acerto na classificação. A taxa de retransmissão da camada de enlace com o PLFC obteve redução de 50 a 70%, atenuando o desperdício de energia.

Em (WU et al., 2019), a identificação das falhas ocorre da seguinte maneira. Os autores assumem duas situações de colisões. A primeira ocorre quando múltiplos transmissores podem sentir um ao outro, e enviam pacotes ao mesmo tempo para um receptor, escolhendo a mesma janela de *backoff*. Na segunda situação, os múltiplos transmissores não conseguem sentir um ao outro e enviam pacotes ao mesmo tempo. Esta situação é mais frequente no IEEE 802.15.4, pois, segundo os autores, não há RTS/CTS, a fim de reduzir o consumo energético (IEEE, 2007).

De acordo com os autores, os resultados obtidos em análises revelam que existem diferenças óbvias entre os casos de colisão e não colisão em termos de distribuição de posição de erro no nível de bits e símbolos. Eles argumentam ainda que os bits de colisão e os erros de símbolo são distribuídos, em geral, no final de um pacote corrompido (WU et al., 2019).

Com base nessas observações foi proposta uma abordagem denominada CRM-GD (*Collision Recognition Mechanism Based on Generating Domains*). O CRM-GD é baseado em aprendizado de máquina, e objetiva identificar colisões causadas pelo efeito de terminal oculto em redes IEEE 802.15.4 de múltiplos saltos. Por ser baseada em aprendizado de máquina, esta proposta é categorizada como calibração ou treinamento.

O CRM-GD insere alguns blocos redundantes em um quadro de dados. Cada trans-

missor possui uma sequência de bits redundantes que são inseridos dentro de cada pacote por ele transmitido, conhecida como GD (*Generating Domains*). Como são padrões conhecidos de bits, os GDs podem ser usados para reconhecer efetivamente a distribuição dos bits corrompidos ao longo dos pacotes.

Para análise da proposta os autores realizaram testes com três cenários, L1, L2 e L3. O L1 é um estacionamento aberto que pode acomodar mais de 100 carros. O L2 fica em um bosque de árvores de cânfora. Por fim, o L3 fica no corredor de um prédio de escritórios, com Wi-Fi disponível 24h. Como métrica foram utilizados o BEDR (*Bit Error Distribution Ratio*) e SEDR (*Symbol Error Distribution Ratio*), que são a razão entre o número de erros em cada posição de bit/símbolo, sobre o total de pacotes com erros. Os resultados experimentais dos testes executados pelos autores da abordagem indicaram que o CRM-GD alcança precisão de reconhecimento de 99,05% em L1, 97,58% em L2 e 92,25% em L3, respectivamente (WU et al., 2019).

Em outra proposta, denominada PCC (*Packet Corruption Classifier*) (ZENG; KU-MAR, 2008), desenvolve-se um classificador que identifica a causa da perda de pacotes, analisando informações de interferência entre dois transmissores. Esta interferência também pode estar relacionada à sobreposição do espectro em algumas subportadoras. Com isso a retransmissão pode ser feita sem *backoff* e com a mesma taxa de transmissão, mas evitando as subportadoras interferidas.

Segundo os autores, os equipamentos de prateleira, ao utilizar OFDM, exportam apenas o fluxo de bits final na camada física (ZENG; KUMAR, 2008). A proposta se baseia na utilização de informações adicionais da camada física para ajudar a estimar a condição e a interferência do canal. As informações são obtidas a partir do fluxo de entrada e saída do *slicer*. O *slicer* é um elemento chave do receptor, que quantifica a amostra de sinal na forma de números complexos.

Na formulação do problema e projeto, os autores utilizam o conceito de teste de hipóteses, definindo hipóteses H0, H1 e H2. H0 corresponde ao pacote ter sido corrompido por SNR baixo. H1 corresponde ao pacote ter sido corrompido por colisão, que iniciaram antes da recepção e terminaram durante a recepção do pacote de interesse, ou que iniciaram durante a recepção e terminaram com o fim da recepção do pacote de interesse. H2 diz respeito a colisões que iniciaram e terminaram durante a recepção do pacote de interesse. O objetivo é confrontar H0 e H1 mais H2, a fim de descobrir a causa da perda.

Como métricas de avaliação da proposta, são utilizadas a taxa de falsos positivos e a taxa de falha. A taxa falsos positivos é a porcentagem de pacotes corrompidos que o teste identifica como colisão, mas na verdade foram pacotes corrompidos por SNR baixo. Já a taxa de falha é a porcentagem de pacotes corrompidos que o teste identifica como SNR baixo, mas foram corrompidos por colisão. Os autores aplicaram três testes estatísticos de classificação, CMT (*Change of Mean Test*), CST (*The Chi-square Test of Independence*) e MWW (*Mann-Whitney-Wilcoxon Test*), no PCC para avaliação.

Para avaliação do PCC foi utilizada a plataforma GNU radio com três nós (T1, T2 e R), onde cada nó é um PC comum conectado a um USRP (*Universal Software Radio Peripheral*) GNU Radio. T1 e T2 são transmissores que trabalham sobre a mesma banda espectral, porém com preâmbulos diferentes, para que R, o receptor, possa detectar apenas pacotes de T1. Os experimentos foram executados na iWWT (*Illinois Wireless Wind Tunnel*), uma câmara anecoica eletromagnética, no sentido de prevenir interferências externas. Foram criados dois cenários: SNR baixo e interferência.

No cenário de SNR baixo, T2 foi desligado e T1 foi posicionado a uma distância fixa de R. A potência de transmissão de T1 foi gradualmente alterada, a fim de descobrir o limite de não detecção de pacotes em R, denominado Pno, e o limite quando pacotes recebidos são corrompidos, denominado Pc. Neste cenário quando o BER (*Bit Error Rate*) é superior a 1%, assume-se que o pacote está corrompido. Após a descoberta dos limites, são executados experimentos com diferentes potências de T1 entre Pno e Pc.

Já no cenário de interferência, T1 e T2 foram colocados a uma distância fixa e igual de R e configurados para usar potências P1 e P2, respectivamente. Foram executados 4 sub cenários: 1) sinal forte/interferência forte, quando P1  $\geq$  Ps (Ps é o limite de P1 onde mais de 98% dos pacotes recebidos tem BER zero), e P2  $\geq$  P1; 2) sinal forte/interferência fraca, quando P1  $\geq$  Ps e P2  $\leq$  P1, e a interferência é fraca ; 3) sinal *borderline*/interferência forte, quando P2  $\geq$  P1 = Pb, onde Pb é a potência *borderline*; e 4) sinal *borderline*/interferência fraca, quando P1 = Pb, e P2  $\leq$  P1.

A proposta obteve uma taxa de falha de 6% e taxa de falsos positivos de 5%, mesmo no cenário em que a interferência é mais difícil de ser detectada. Os testes foram conduzidos em um ambiente de teste real, possibilitando resultados mais autênticos.

Por fim, a última abordagem nesta categoria é o método proposto neste trabalho, que é apresentado no Capítulo 3. Para avaliação de desempenho, apresentada no Capítulo 4, foi necessário efetuar o mapeamento do valor do SNR para avaliar o meio de transmissão sem o método proposto. O mapeamento possibilita que o método proposto seja classificado como calibração ou treinamento. Além disso, há um trabalho para achar a taxa de transmissão mais adequada de controle baseada na taxa de transmissão de dados, que também faz parte do processo de calibração ou treinamento.

#### 2.3 Feedback

Em (PENG; CHENG; SIKDAR, 2007), é apresentada uma proposta de protocolo MAC (*Media Access Control*) que visa detectar colisões antes do final da transmissão. Este protocolo utiliza pulsos em um canal de controle de banda estreita com o objetivo de controlar o acesso a um canal compartilhado de dados. Estes pulsos são acompanhados de pausas de comprimento aleatório, que têm como objetivo dessincronizá-los entre diferentes transmissores. O canal de controle reserva o meio ao redor dos transmissores, enquanto os dados são enviados em um canal separado (PENG; CHENG; SIKDAR, 2007). Neste sentido, o protocolo proposto assume que cada nó possui habilidade para simultaneamente transmitir em dois canais, dados e controle.

Como exemplo, considere uma transmissão de um nó A para um nó B. Antes da transmissão, A escuta o canal de controle para garantir que o meio está ocioso. Se o canal de controle estiver ocioso por um período de tempo maior que a duração máxima da pausa de um pulso, então A inicia um *backoff* aleatório extraído da janela de contenção. Caso contrário, A continua monitorando o canal de controle.

Após o *backoff*, se não foram detectadas transmissões, A inicia a transmissão do pacote. Na transmissão, os dados seguem o canal de dados, enquanto no canal de controle são enviados pulsos. Após a transmissão do cabeçalho no canal de dados, espera-se que B responda com um pulso CTS no canal de controle, que deve ser enviado durante uma pausa nos pulsos enviados por A. Após o recebimento do pulso CTS enviado por B, A inicia a transmissão do pacote. Não fica claro como A garante que o CTS é de B (ou, mais especificamente, direcionado a A). Realmente, RTS/CTS geralmente tem endereços, mas se o CTS é só uma sequência de pulsos, ele não carrega essa informação.

A transmissão do pacote de A para B pode ser interrompida por dois motivos. O primeiro é o não recebimento do pulso CTS enviado por B. O segundo ocorre se A detectar um pulso de outro nó em uma de suas pausas de pulso. Dessa forma, os pulsos gerados pelos transmissores funcionam também como um *feedback* detectável durante o processo de recepção de que duas ou mais transmissões estão ocorrendo em paralelo. Nos dois casos, a janela de contenção é dobrada e A volta a monitorar o canal de controle. Este processo se encerra quando A atinge o limite de tentativas, ou com a confirmação do recebimento do pacote por B.

O protocolo proposto em (PENG; CHENG; SIKDAR, 2007) utiliza mecanismos similares (*e.g.*, *backoffs* aleatórios, RTS/CTS, ACKs) aos do CSMA/CA tradicional, considerando potencial colisão quando um nó detecta outro nó transmissor. O que diferencia as abordagens é que o protocolo proposto faz uso de um canal de controle específico para *handshake* e pulsos para reservar o meio. O uso de um canal de controle separado com sinalização através de pulsos com intervalos aleatórios permite que colisões sejam detectadas enquanto os pacotes de dados ainda estão sendo transmitidos (*i.e.*, quando, ao pausar seu pulso, um transmissor detecta outro pulso no canal de controle).

Para avaliar o desempenho do protocolo proposto, foi desenvolvido um modelo analítico da taxa de transmissão de saturação em redes de um salto. Ao final, foi feita a comparação com resultados utilizando o ns-2 (*Network Simulator 2*) (NS2, 2007). Os resultados mostraram forte correspondência entre os resultados do modelo analítico e a simulação.

COLLIE (*Collision Inferencing Engine*) é um estudo empírico baseado em RSSI, padrões de BER, e capturas de erros em nível de símbolo, para diagnóstico de perda em redes IEEE 802.11. A proposta se baseia na comparação entre o dado recebido e transmitido, e consiste de dois componentes básicos. O primeiro componente são algoritmos de classificação de perdas entre colisão e SNR baixo por meio de análise empírica após o ocorrido. O segundo é um protocolo que ajusta parâmetros na camada de enlace, possibilitando melhorias significativas na taxa de transmissão e capacidade para cenários de alto uso de mobilidade (RAYANCHU et al., 2008).

Os autores citam o ARF (*Auto Rate Fallback*), um algoritmo de adaptação da taxa baseado no histórico de taxas de erro de transmissão anteriores para selecionar de forma adaptativa as taxas de transmissão usadas em transmissões futuras. Após várias transmissões bem sucedidas consecutivas, o remetente tenta transmitir a uma taxa de transmissão mais alta. Se a entrega desse quadro não for bem sucedida, ele imediatamente retornará ao modo anteriormente suportado. Na proposta dos autores, o algoritmo ARF foi adaptado para torná-lo sensível a colisões.

Para determinar a causa de perda de pacote, o COLLIE realiza uma análise empírica após o ocorrido, com o *feedback* explícito obtido do receptor. O COLLIE realiza uma análise dos dados recebidos por meio de uma combinação de três métricas: RSSI, padrões de BER, e capturas de erros em nível de símbolo. Esta análise é feita por meio de um algoritmo de inferência que possibilita a distinção da causa.

De acordo com os autores, dada uma cópia do pacote originalmente transmitido e do

recebido com erros, é possível fazer uma inferência instruída sobre a causa da falha de transmissão com base nos padrões de bits de erro desse pacote único.

Segundo os autores, com base em testes, geralmente os pacotes que sofrem colisão possuem RSSI maior que os perdidos por SNR baixo (ambos analisados com mesma taxa de transmissão). Com relação a BER, os autores analisaram diferentes taxas de transmissão (24, 36 e 48 Mb/s) em uma função distribuição acumulada, e constataram que os valores de BER verificados em pacotes que sofreram colisão são muito mais diferentes (distribuição mais ampla) dos que não sofreram colisão.

Estudar os padrões de símbolos com erro, em vez de apenas os bits recebidos com erro, pode fornecer informações valiosas sobre a causa de uma perda de pacote (RAYANCHU et al., 2008). Neste sentido são avaliadas as capturas de erros em nível de símbolos, por meio de três métricas: SER (taxa de erro de símbolo), EPS (erro por símbolo) e S-Score (pontuação de erro do símbolo). Com a junção das métricas SER e EPS é possível distinguir a causa da perda de pacote, já que, de acordo com observações feitas pelos autores, pacotes com erro por colisão possuem SER e EPS mais altas

Para avaliação da posposta, foram criados quatro cenários de teste: estático, fontes adicionais de colisão, móvel e emulando uma chamada de voz. No cenário estático foi verificado que o COLLIE obteve até 52% de ganho de vazão, com ganho médio de 30%. Neste cenário com o aumento da distância entre o transmissor e receptor, a taxa de transmissão reduz, com e sem o COLLIE. Em um cenário com fontes adicionais de colisão, o experimento do cenário estático foi repetido, obtendo ganho de até 60% de vazão. No terceiro cenário, com mobilidade, observou-se que a melhoria de vazão varia cerca de 15% a 65%. No último cenário, os autores efetuaram uma chamada de 4 minutos de duração usando um telefone IP Netgear SPH101 VoWiFi com Skype. Esse cenário foi avaliado com a mobilidade nas velocidades lenta, média e alta, sendo que na maior taxa de mobilidade sem o COLLIE as perdas excederam 80%, sendo reduzidas para aproximadamente 55% com o COLLIE.

De acordo com os autores, a proposta difere das existentes no sentido de haver uma análise empírica do pacote originalmente transmitido e do recebido com erros, enquanto algumas simplesmente definem um limiar (RAYANCHU et al., 2008). É necessário salientar que a análise empírica é feita após a ocorrência da colisão. Também é possível verificar que para análise empírica, é obrigatório o *feedback* do receptor que só é possível se o AP conseguir decodificar corretamente o endereço MAC de origem do pacote com erro. Uma última proposta desta categoria, denominada CD-ET (JI-HOON YUN; SEUNG-WOO SEO, 2006), utiliza informações de *feedback* relacionadas à duração de energia de RF (Radiofrequência).

Mais detalhadamente, o CD-ET funciona da seguinte maneira. Quando as estações transmitem quadros simultaneamente, ocorre uma colisão e o AP vê a energia de RF mesclada causada pelos quadros colididos. Se os DTs (Tempos de Duração) dos quadros transmitidos forem diferentes entre si, a energia de RF mesclada do EDT (Tempo de Duração para Energia de RF) será maior que os DTs dos quadros originais, exceto, talvez, para o quadro mais longo. Com base nisso, se as estações puderem conhecer a energia de RF mesclada do EDT, poderão compará-lo ao DT de sua própria tentativa de transmissão. O mesmo ocorre quando os STs (Tempos de Início) dos quadros colididos são diferentes entre si.

Se os DTs de todos os quadros colididos forem iguais, o CD-ET não poderá detectar a colisão (todos os seus STs são considerados iguais). Isto é especialmente verdade quando todas as estações operam no modo RTS/CTS, podendo haver colisões de quadros RTS. Por esse motivo, os autores propõem usar o RBP (*Random Bit Padding*), no qual cada estação preenche um número aleatório de bits no final de um quadro de dados antes da transmissão. A quantidade de bits de *padding* é sorteada de uma janela RW: quanto maior RW, maior a probabilidade de diferentes tempos de transmissão dos quadros.

Os autores propõem um modelo analítico da capacidade de detecção do CD-ET. A fim de simplificar a análise, algumas suposições foram feitas pelos autores: 1) as estações geram quadros de dados de mesmo comprimento; 2) o AP do BSS não gera tráfego de dados; e 3) não há erros de canal. Além do modelo analítico, foram efetuadas simulações utilizando o ns-2. Nas simulações os autores investigaram o *overhead* em termos de largura de banda, capacidade de detecção e atraso de detecção. Também foi testado o desempenho do algoritmo ARF com CD-ET.

O modelo analítico e a simulação apresentaram resultados semelhantes. Nos testes foi possível verificar que quanto maior o tamanho de RW, maior é a probabilidade de detecção de colisão. Portanto, se faz necessário configurar o RW com cuidado para obter uma boa probabilidade de detecção com *overhead* moderado. O esquema proposto para melhorar o desempenho do ARF conseguiu atingir até 500% de melhora quando testado com 10 estações.

Os autores citam que com o CD-ET as colisões são detectadas com algum atraso, o que resulta em melhoria sub-ótima do desempenho, e que, quando erros de colisão e de canal ocorrem simultaneamente para um quadro, o esquema proposto pode detectar apenas a colisão.

### 2.4 Overhead

O primeiro exemplo nesta categoria é o CRM-GD (WU et al., 2019). O *overhead* ocorre com a inserção de alguns blocos redundantes em um quadro de dados. Estes blocos redundantes são compostos por uma sequência de bits redundantes inseridos dentro de cada pacote. Por se tratar de padrões conhecidos de bits, eles podem ser utilizados para reconhecer efetivamente a distribuição de bits corrompidos no pacote.

Em seguida, a proposta (PENG; CHENG; SIKDAR, 2007) utiliza pulsos RTS/CTS para distinção do tipo de perda. O uso de RTS/CTS pode resultar em um aumento significativo do *overhead* na rede sem fio. Não é recomendado que RTS/CTS seja utilizado de maneira indiscriminada em redes sem fio.

Outra abordagem nesta categoria é o método proposto neste trabalho. De maneira resumida, este método utiliza uma subportadora exclusiva para envio de bits de controle. Sendo assim, uma das subportadoras utilizadas para transmissão de dados deixa de ser utilizada para os dados, destinando-se na identificação do tipo de perda de pacotes. Como será demonstrado no Capítulo 3, esse *overhead* totaliza pouco mais de 2%.

#### 2.5 Detecção contínua de preâmbulo

Analisando a percepção e recuperação de colisões em redes de sensores, que utilizam rádios de baixa potência, uma proposta para detecção da colisão no receptor é apresentada em (WHITEHOUSE et al., 2005). Nesta proposta, as colisões são categorizadas em *stronger-first* e *stronger-last*. A colisão é *stronger-first* quando o rádio sincroniza com o pacote mais forte primeiro. Com isso o rádio não irá, nessa situação, tentar ressincronizar com o segundo pacote pelo fato dele ser mais fraco. No caso da *stronger-last*, o rádio sincroniza com o pacote mais forte primeiro, mas a recepção falha, pois o pacote mais forte captura e corrompe o sinal do primeiro pacote.

A técnica de detecção e recuperação de colisões utilizada é procurar continuamente um novo preâmbulo, mesmo durante a recepção de pacotes, e ressincronizar com o novo pacote no cenário *stronger-last*. Esta técnica não requer alteração no formato do pacote, nem na camada MAC, apenas na maneira como o receptor processa o recebimento de pacotes.

No processo de recebimento de um pacote, se, durante a recepção, um novo preâmbulo é encontrado, o método assume que houve uma colisão. Caso o receptor consiga parar de receber o primeiro pacote e ressincronizar adequadamente, poderá recuperar o segundo pacote. Para efetuar a recuperação do segundo pacote, é mandatório já ter recebido parcialmente o primeiro pacote, com informações do cabeçalho. Se estas informações puderem ser recuperadas, é possível identificar o transmissor do primeiro pacote (corrompido), e assim recuperá-lo. É importante notar que a capacidade de detectar colisões nesse método diminui à medida que a diferença de tempo entre as transmissões diminui. No caso extremo, se os sinais dos pacotes chegarem ao receptor exatamente ao mesmo tempo, a colisão não será detectada.

Outra proposta nessa categoria é um esquema chamado CSMA/CN (*Carrier Sense Multiple Access with Collision Notification*) (SEN; ROY CHOUDHURY; NELAKUDITI, 2012). Neste esquema, o transmissor possui duas antenas (no mesmo canal), uma para transmissão e outra dedicada a escuta de notificações. A colisão é identificada pelo receptor por meio de uma busca contínua de um novo preâmbulo, em conjunto com a inferência realizada por meio das *hints* do SoftPHY. Quando há colisão, o receptor no-tifica imediatamente o transmissor. Ao detectar a notificação, o transmissor interrompe sua transmissão, liberando o canal para outros transmissores nas proximidades. Nesse caso, quando o transmissor tiver uma nova oportunidade de acesso ao meio, irá transmitir apenas a porção do pacote ainda não recebida pelo receptor, isto é, a porção já recebida não será retransmitida.

Mesmo com duas antenas, uma para cada função, os autores citam dois desafios. Primeiro, como o receptor detecta uma colisão enquanto o pacote está sendo recebido. Segundo, como o transmissor detecta uma notificação de colisão durante sua própria transmissão.

Para lidar com esses aspectos o CSMA/CN utiliza a correlação de sinais para discernir um padrão de bits conhecido, mesmo na presença de uma forte interferência. Ao iniciarse a transmissão, o receptor efetua a detecção de colisão por meio de uma busca (por correlação de sinais) contínua de um novo preâmbulo. Além disso, o receptor utiliza *hints* do SoftPHY para inferir, durante a recepção, se o pacote será perdido. Com essa inferência, o CSMA/CN passa a pressupor que o pacote será perdido, e tendo um novo preâmbulo detectado durante a transmissão, assume-se que está havendo uma colisão. Desta maneira, é iniciada uma notificação de colisão para o transmissor. A notificação é uma assinatura curta exclusiva do receptor, também conhecida pelo transmissor. A antena dedicada para escuta do transmissor ouve continuamente a assinatura do receptor usando correlação.

A correlação é mais um desafio citado pelos autores, já que sinal da notificação é mais fraco que o da transmissão. Com isso é necessário o discernimento da notificação com uma alta taxa de acerto. Para isso, os autores propõem suprimir o sinal da antena de transmissão com o auxílio de técnicas de cancelamento de interferência.

Uma notificação de colisão é simplesmente uma assinatura sem nenhum preâmbulo. Portanto, uma notificação de colisão não causa notificações de colisão em cascata. O sinal de notificação pode interferir em transmissões ativas, porém isso pode ser reparado utilizando esquemas como PPR (JAMIESON; BALAKRISHNAN, 2007). O PPR evita a retransmissão de partes de pacotes que já foram recebidas, reduzindo o desperdício de recursos da rede. Além disso, informações da camada física são utilizadas para melhorar a resiliência a erros.

De maneira geral, o objetivo do CSMA/CN é utilizar as *hints* do SoftPHY para detectar uma colisão enquanto a transmissão está sendo feita, de forma a permitir que o receptor avise o transmissor e este possa abortar sua transmissão, a fim de economizar recursos do meio sem fio. O CSMA/CN é um método interessante, pois não apenas recupera os pacotes perdidos, mas também gera economia de tempo para essa recuperação. Entretanto, os autores destacam que o método tem uma integração complexa com a tecnologia MIMO (*Multiple Input Multiple Output*), requerendo alterações. Outra limitação é que o cancelamento de ruído nem sempre funciona, podendo prejudicar o desempenho e reduzir a eficácia do método.

### 2.6 Tipos de aplicação

No propósito de buscar soluções para adaptação da taxa ou abordagens para dispor acesso ao meio mais eficazes, existem propostas que contêm componentes para classificar as perdas. Quando detectado o tipo de perda de pacotes, existem basicamente duas práticas usualmente adotadas. Para propostas que buscam otimizar o mecanismo de acesso ao meio e sofrem colisão, pode ser utilizado o *backoff* aleatório, que basicamente evita a sincronização de dois transmissores que causaram colisão. No caso de propostas de mecanismos de adaptação automática de taxa de transmissão, quando o tipo da perda de pacotes é por SNR baixo, aciona-se a redução da taxa de transmissão para outra mais
robusta.

### 2.6.1 Adaptação da taxa de transmissão

Estimar a taxa de transmissão ideal é um problema que vem sendo estudado em redes sem fio (VUTUKURU; BALAKRISHNAN; JAMIESON, 2009) (SEN; SANTHAPURI et al., 2010) (BICKET, 2005) (MAGUOLO; LACAGE; TURLETTI, 2008). O controle da taxa é realizado na camada de enlace, sendo difícil a definição de uma taxa ideal devido à flutuação de qualidade do canal, que torna a taxa ideal obsoleta rapidamente.

A adaptação de taxa de transmissão deve ser ágil, a fim de responder de forma eficaz as variações do canal sem fio. Além disso, a eficácia está diretamente ligada à maneira como as colisões são detectadas e tratadas. Não se deve reduzir a taxa de transmissão em resposta a colisões, pois isso aumenta a duração para transmissão de pacotes e piora a contenção do canal.

O SoftRate (VUTUKURU; BALAKRISHNAN; JAMIESON, 2009) é um protocolo de adaptação da taxa de transmissão. A abordagem utiliza a BER do canal livre de interferências como informação para tomada de decisão. Esta estimativa é calculada usando o nível de confiança no valor decodificado de cada bit exportado da camada física, conhecidas como *hints* do SoftPHY. No PPR (JAMIESON; BALAKRISHNAN, 2007), as *hints* do SoftPHY são usadas para o protocolo Zigbee, sendo que o SoftRate foi generalizado para qualquer PHY.

O receptor SoftRate utiliza uma heurística para separar os erros causados por interferência fortes. O transmissor SoftRate usa a BER reportada pelo receptor (*feedback*) após uma transmissão sem interferências. Essa BER condiz a uma taxa de transmissão inicial, que é usada para os primeiros pacotes transmitidos. Posteriormente, o SoftRate estima a BER em outras taxas de transmissão, a fim de escolher uma taxa que minimize o tempo de transmissão, mantendo a entrega.

Analisando a BER ao longo da recepção de um pacote é possível identificar quando ocorre a interferência. Se a interferência ocorrer após o início da transmissão ela se manifestará como um pico na BER. No caso do sinal do transmissor iniciar-se após o receptor sincronizar com o quadro interferente, o quadro do transmissor não será detectado. Neste caso, o receptor não enviará o *feedback* ao transmissor.

Quando o transmissor não recebe o *feedback* do receptor, ele não consegue identificar se a perda ocorreu por colisão ou SNR baixo. A fim de evitar este problema é inserido um postâmbulo em cada quadro enviado, aumentando assim a probabilidade de detecção de parte do quadro. Se o postâmbulo é usado, ou seja, quando ou preâmbulo sofrer interferência, o transmissor pode assumir que houve perda por SNR baixo, reduzindo assim a taxa de transmissão. Os autores citam que a lógica de detecção do postâmbulo não foi implementada na prática.

Outra abordagem, nomeada como AccuRate (SEN; SANTHAPURI et al., 2010), está localizada no limite da camada física e MAC. O AccuRate analisa a dispersão entre as posições dos símbolos transmitidos e recebidos. Quando há pequenas dispersões, indicase que o enlace dispõe uma boa qualidade, sugerindo possibilidade de suporte a taxas de dados mais altas. Até mesmo se houver corrupções, o AccuRate consegue extrair a parte recebida com sucesso do pacote, para estimar a taxa de transmissão apropriada. O fato dele extrair parte do pacote deve-se ao uso do PPR. A taxa estimada é utilizada pela próxima transmissão, porém pode haver oscilações da taxa de transmissão ideal de acordo com as condições do enlace.

Mais detalhadamente, o funcionamento do AccuRate é feito com a concatenação de cada pacote e um postâmbulo. O receptor AccuRate efetua as seguintes verificações. Se o pacote for recebido corretamente, o AccuRate estima a taxa de transmissão e a envia junto ao ACK. No entanto, se o pacote for recebido incorretamente, o AccuRate dispara uma operação de detecção de interferência. Segundo os autores, um pacote recebido incorretamente significa que o preâmbulo foi decodificado, mas a verificação CRC falhou. Durante a operação de detecção de interferência, o AccuRate pode estimar a taxa de transmissão analisando apenas o preâmbulo e postâmbulo, dependendo de qual exibe menor dispersão de símbolos, e a envia junto ao NACK. Se o transmissor não receber nenhum ACK/NACK, o pacote será retransmitido conforme as especificações IEEE 802.11.

Segundo os autores, a principal vantagem do AccuRate sobre o SoftRate é a de não haver necessidade de mais de uma transmissão para obter a taxa de transmissão ideal. Esta taxa pode ser obtida com a transmissão de um pacote, desde que o mesmo seja recebido corretamente ou identificado o preâmbulo ou postâmbulo, reduzindo o tempo de convergência. Eles também citam que o AccuRate consegue fazer melhor distinção entre desvanecimento e colisões. É necessário ratificar que a utilização de postâmbulo aumenta o *overhead*.

## 2.6.2 Otimização do backoff

Uma das possíveis aplicações da detecção do tipo de perda é o *backoff* aleatório. O *backoff* aleatório tem como objetivo evitar a sincronização entre estações que causaram colisão (PASSOS; BALBI; CARRANO, 2016). Em redes IEEE 802.11, se a quantidade de estações concorrentes fosse conhecida, o mecanismo de *backoff* poderia ser ajustado para obter um desempenho ideal do CSMA/CA. No entanto, estimar o número de estações concorrentes não é trivial. Também existem trabalhos para modificar o modo como a janela de contenção diminui ou aumenta (CHONGGANG WANG; BO LI; LEMIN LI, 2004; JAEHYUK CHOI et al., 2005). Além disso, a utilização de um *backoff* não aleatório também é sugerido em (JAEHYUK CHOI et al., 2005), porém nesta proposta as estações devem estar cientes dos valores de *backoff* de seus concorrentes. Neste contexto, é proposto ainda o CSMA/ECA (*Carrier Sense Multiple Access with Enhanced Collision Avoidance*) (BARCELO et al., 2009), que utiliza um *backoff* determinístico e igual para todas as estações, após uma transmissão com sucesso. Essa abordagem reduz consideravelmente as colisões, e, em alguns casos, chega a extingui-las.

Alguns trabalhos na literatura citados na taxonomia proposta fazem uso do *backoff* aleatório, tanto para auxílio na detecção, mas também como possível solução de colisão identificada. Em (ZHU; SUN, 2015), é utilizado um mecanismo de retransmissão baseada em colisões, onde é acionado o *backoff* aleatório em 5 retransmissões, a fim de identificar e solucionar a colisão. Já em (PENG; CHENG; SIKDAR, 2007) e (WU et al., 2019), o *backoff* aleatório é essencial, pois os autores o utilizam como ferramenta para considerar potencial colisão, onde um nó detecta outro nó transmissor.

# **3** Proposta para o diagnóstico do tipo de perda em redes IEEE **802.11**

Para possibilitar melhor compreensão acerca do método proposto, é necessário entender alguns conceitos prévios. Serão contextualizados, de maneira sucinta, a função e características dos conceitos de portadora, codificação, modulação e OFDM. Em seguida o método proposto será descrito em detalhes.

## 3.1 Fundamentação teórica

Uma portadora é uma onda que tem como objetivo o transporte do sinal através do meio físico. Frequentemente, utiliza-se um sinal em forma senoidal caracterizado pela sua frequência, amplitude e fase. A modulação é a ação de alterar as características da portadora para representar a informação a ser transmitida. O sinal pode ser modulado através da frequência, da amplitude, da fase, ou de uma combinação dessas. No IEEE 802.11g, as modulações utilizadas são BPSK, QPSK, 16QAM e 64QAM (IEEE, 2003). A emenda IEEE 802.11ax, aprovada em fevereiro de 2021, utiliza também as modulações 256QAM e 1024QAM (IEEE, 2021). A codificação é usada a fim de permitir detecção e, em alguns casos, a correção de eventuais erros na transmissão. Isso é alcançado através da inserção de bits redundantes. Frações expressam qual a parte da mensagem redundante é realmente significava. Por exemplo, uma codificação com taxa de 2/3 produzirá 3 bits transmitidos para cada dois bits de dados originais. Em redes IEEE 802.11g, são usadas as codificações 1/2, 2/3 e 3/4 (IEEE, 2003). Em emendas mais atuais, por exemplo 802.11ax, há codificações de 5/6 (IEEE, 2021). A codificação e a modulação têm influência direta na taxa de transmissão. Combinações mais agressivas resultam em taxas mais altas, mas menos robustas.

Introduzido pela primeira vez em redes IEEE 802.11 na emenda IEEE 802.11a, o OFDM é uma técnica de espalhamento espectral que alcança maior robustez contra interferências e maior eficiência espectral. Ele divide o canal em subcanais independentes, utilizando múltiplas subportadoras ortogonais. Os bits do pacote a ser transmitido são multiplexados nas várias portadoras e cada portadora pode usar modulações e codificações diferentes. No IEEE 802.11a, por exemplo, canais de 20 MHz são divididos em 52 suportadoras, sendo 48 dedicadas à transmissão de dados — as outras 4 são usadas como piloto auxiliando na estimativa do canal.

## 3.2 Método para o diagnóstico do tipo de perda em redes IEEE 802.11

O método proposto nesse trabalho explora o *tradeoff* entre robustez e taxa de transmissão utilizada. Este método está dividido em duas partes: introdução de bits de controle no processo de transmissão e a execução de um algoritmo de decisão no receptor em caso de perda.

#### 3.2.1 Introdução de bits de controle

Durante o processo de multiplexação dos bits do pacote pelas subportadoras OFDM, o transmissor adiciona um conjunto de bits de controle contendo seu AID (Association ID). Além desse identificador, o transmissor também adiciona um CRC (Cyclic Redundancy Check) de 4 bits computado exclusivamente sobre os bits de controle. Um CRC com poucos bits é eficaz na detecção de erro, considerando que a informação de controle é também pequena. Além disso, essa quantidade de bits para o CRC torna o método aplicável para pacotes de dados pequenos e/ou com taxa de transmissão muito altas.

Uma das subportadoras disponíveis é dedicada a transportar esse conjunto de bits adicionais. Enquanto as subportadoras de dados utilizam uma combinação de modulação e codificação especificada pelo usuário ou por um algoritmo de adaptação de taxa tradicional, a subportadora dedicada aos bits de controle utiliza uma combinação que resulte em uma transmissão mais robusta.

A hipótese básica desse trabalho é que a interferência causada por uma colisão é muito mais severa que o ruído de fundo do canal. Assim, ao tornar a transmissão dos bits de controle mais robusta, espera-se que, em ausência de colisão, esses sejam recebidos corretamente independentemente do que ocorra com os bits de dados. Por outro lado, caso ocorra uma colisão, essa deve afetar também a capacidade de recepção correta dos bits de controle. O método proposto introduz um *overhead* no processo de transmissão, já que efetivamente reduz o número de subportadoras disponíveis para dados. No entanto, esse *overhead* é relativamente baixo. No caso específico do IEEE 802.11a, por exemplo, as 48 subportadora de dados são reduzidas para 47 resultando em um *overhead* de 1/48, ou pouco mais de 2%.

A visualização fica mais clara na Figura 1, onde é possível ver os 64 pontos da FFT (*Fast Fourier Transform*) da emenda IEEE 802.11a. Nas extremidades existem 12 subportadoras de guarda, sendo 6 subportadoras em cada lado. Em azul são visualizadas as 4 subportadoras piloto, que auxiliam na estimativa do canal. Por fim, em vermelho é possível verificar 48 subportadoras de dados, onde 1 delas será utilizada para inclusão dos bits de controle.



Figura 1: Subportadoras OFDM para redes sem fio IEEE 802.11a (MAGLOGIANNIS, 2018)

O número de símbolos OFDM transmitidos em um pacote depende do número de bits e da combinação de modulação e codificação utilizada para a porção de dados. Dessa forma, é possível que os 12 bits do AID concatenados aos bits de CRC não sejam suficientes para preencher o número de símbolos OFDM necessários para os dados. Para evitar esse descasamento, os bits do AID são repetidos ciclicamente o número de vezes necessário para que os bits de controle preencham a portadora de controle em todos os símbolos OFDM.

## 3.2.2 Algoritmo de decisão no receptor

Do lado do receptor, um algoritmo de decisão é executado caso a porção de dados do pacote seja perdida — *i.e.*, caso o CRC da porção de dados do pacote aponte corrupção.



Um fluxograma que representa o algoritmo é apresentado na Figura 2.

Figura 2: Fluxograma do algoritmo para detecção e identificação da perda

Se houver perda sem colisão, ou seja por SNR baixo, a subportadora de controle será afetada com uma probabilidade menor. Com isso, o receptor pode extrair o identificador do transmissor e enviar um NACK explicitamente avisando-o sobre a perda por SNR baixo. O NACK deve utilizar uma robustez igual ou similar a utilizada pela subportadora de controle, a fim de que ele chegue com sucesso ao transmissor. Por outro lado, se houver perda por colisão, haverá uma alta probabilidade de perda também da porção de controle. Nesse caso, o receptor não enviará qualquer reconhecimento ao transmissor, que poderá interpretar que houve uma perda por colisão.

Note que uma decisão importante é qual combinação de modulação e codificação usar na subportadora de controle. Idealmente, deve-se escolher uma combinação suficientemente robusta para que a porção de controle nunca sofra corrupções em ausência de colisões, mas não tão robusta a ponto dos bits de controle não sofrerem corrupção em caso de colisão. Na prática, essa combinação ideal depende da qualidade do enlace. O Capítulo 4 apresenta dados empíricos que permitem uma seleção adequada.

## 4 Avaliação de Desempenho

Nesse capítulo, são apresentados resultados de simulações utilizando o método proposto. Essas simulações têm dois objetivos distintos. Em primeiro lugar, elas foram utilizadas para determinar quais são as combinações de modulação e codificação ideais para a subportadora de controle de acordo com a qualidade do enlace sem fio. Além disso, elas permitem também a validação e verificação da efetividade do método proposto.

Devido a falta de modelagem da camada física em simuladores conhecidos e utilizados pela literatura (e.g., ns-2 (NS2, 2007) e ns-3 (NS3, 2008)), e para os propósitos dessa avaliação, foi utilizado um simulador personalizado<sup>1</sup> escrito em Python 2.7. O simulador modela um sistema composto por um transmissor e um receptor (em certos cenários, é possível incluir também um segundo transmissor interferente) conectados através de um enlace sem fio modelado como um canal com múltiplos percursos e ruído gaussiano branco. As transmissões utilizam OFDM como método de espalhamento espectral. Todos os parâmetros do sistema foram escolhidos para simular um sistema de rádio IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac. Isso inclui as combinações de modulação e codificação utilizadas que correspondem àquelas utilizadas nas várias taxas de transmissão previstas em IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac. Mais detalhes acerca do simulador podem ser consultados no Apêndice A.

Todos os resultados reportados nessa seção correspondem a médias — ou percentuais — baseados em 1000 repetições do simulador para cada conjunto de parâmetros avaliados. Cada repetição diz respeito à transmissão de um pacote de 12000 bits (1500 bytes). A principal métrica de desempenho avaliada é a taxa de efetividade do método. Considerase que uma falha do método acontece em casos diferentes a depender se o cenário é de colisão ou não. Se há colisão, o método falha quando a porção de dados do pacote é perdida, mas os bits de controle não — diante disso, o método declararia, erroneamente, que a perda foi por SNR baixo. Se não há colisão, considera-se uma falha do método quando ambas as porções de dados e controle são perdidas simultaneamente — neste caso

 $<sup>^{1}</sup> Disponível \ em \ https://github.com/allyssonccuff/SimOFDM.$ 

o método considera, de maneira equivocada, que houve colisão.

Enlaces IEEE 802.11 comumente utilizam algum tipo de mecanismo de adaptação da taxa de transmissão. Assim, como um primeiro experimento, foram executadas simulações preliminares sem o método proposto — *i.e.*, simulando canais IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac tradicionais — com o objetivo de mapear cada valor de SNR usado nas simulações a uma taxa de transmissão adequada para os dados. Para cada valor de SNR utilizado nessa avaliação, foram realizadas simulações com diferentes taxas de transmissão de forma a determinar a taxa mais alta que resultasse em menos que 50% de perda em ausência de colisões<sup>2</sup>. Com isso, foi possível chegar ao mapeamento apresentado nas Tabelas 2, 3 e 4, onde é possível identificar o valor de SNR a partir do qual cada taxa de transmissão deve ser usada para cada emenda e largura de banda.

Tabela 2: Identificação do valor de SNR a partir do qual cada taxa de transmissão resulta em uma probabilidade de entrega maior que 50% para a emenda IEEE 802.11g.

Emenda	Frequência	Taxa de dados	$\mathbf{SNR}$	Taxa de entrega
		$6 { m Mb/s}$	5  dB	52%
00		9  Mb/s	8  dB	86%
.11		$12 \mathrm{~Mb/s}$	9  dB	94%
IEEE 802	20 MHz	$18 \mathrm{~Mb/s}$	10  dB	63%
	20 101112	$24 \mathrm{~Mb/s}$	14  dB	58%
		$36 \mathrm{~Mb/s}$	17  dB	66%
		$48 \mathrm{~Mb/s}$	23  dB	91%
				$54 \mathrm{~Mb/s}$

Uma vez definidas as taxas de transmissão da porção de dados para cada SNR, prosseguiu-se para a avaliação do método proposto. Para isso, foram executadas simulações com o método proposto utilizando-se vários valores de SNR. As taxas utilizadas para a subportadora de controle<sup>3</sup> foram variadas entre todas as taxas disponíveis no IEEE 802.11g, no IEEE 802.11n e no IEEE 802.11ac, que resultariam em uma transmissão mais robusta que a da porção de dados. Essas simulações foram divididas em três cenários: (1) sem colisão; (2) com colisão, onde os sinais transmitido e colidente possuem a mesma potência; e (3) com colisão, mas com o sinal transmitido com potência 3 dB mais alta que o colidente. Para os cenários que envolvem colisão, o pacote que colide com a transmissão principal tem também 12000 bits. É importante ratificar que por terem sido criados

<sup>&</sup>lt;sup>2</sup>Note que, por padrão, o IEEE 802.11 retransmite quadros "grandes" — *i.e.*, acima do limiar de RTS/CTS — até 4 vezes. Para uma taxa de perda de pacotes de menos de 50%, ao considerar até 4 tentativas de retransmissão independentes, a probabilidade de sucesso é maior que  $1 - 0.5^4 = 93.75\%$ .

<sup>&</sup>lt;sup>3</sup>Serão utilizadas taxas originais das emendas avaliadas (*e.g.*, 48 Mb/s) para denotar o uso de um esquema de codificação e modulação, embora a taxa efetivamente alcançada é mais baixa por conta de usar apenas uma subportadora.

Emenda	Frequência	Taxa de dados	SNR	Taxa de entrega
		$6,5~{ m Mb/s}$	6 dB	94%
ц		$13 \mathrm{~Mb/s}$	9  dB	85%
.11		$19,5 \mathrm{~Mb/s}$	11 dB	92%
802	20 MHz	$26 \mathrm{~Mb/s}$	14 dB	93%
E E	20 101112	$39 \mathrm{~Mb/s}$	17  dB	57%
니 도		$52 \mathrm{~Mb/s}$	52 Mb/s 23 dB	85%
		$58,5 \mathrm{~Mb/s}$	24  dB	81%
		$65 \mathrm{~Mb/s}$	25  dB	61%
		$13,5 \mathrm{~Mb/s}$	5  dB	77%
ц		$27 \mathrm{~Mb/s}$	Mb/s 9 dB	86%
		$40,5 \mathrm{~Mb/s}$	11 dB	92%
802	40 MHz	54  Mb/s	14 dB	78%
EEE	40 MIIZ	HZ 81 Mb/s 17 dB	81%	
		$108 \mathrm{~Mb/s}$	22  dB	73%
	121	121,5  Mb/s	23  dB	65%
		135  Mb/s	25  dB	89%

Tabela 3: Identificação do valor de SNR a partir do qual cada taxa de transmissão resulta em uma probabilidade de entrega maior que 50% para a emenda IEEE 802.11n.

três cenários divididos, os testes podem não refletir um cenário mais realístico, onde há uma mistura dos cenários avaliados. Além disso, nos cenários com colisão o simulador transmite tanto o pacote que colide quanto o pacote principal simultaneamente.

Apesar das simulações terem sido executadas com todas as combinações de modulação e codificação das emendas IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac, neste capítulo serão apresentadas apenas os resultados das emendas IEEE 802.11g (com largura de banda de 20 MHz) e IEEE 802.11ac (exclusivamente para largura de banda de 160 MHz). Isso será feito pois os resultados das demais combinações são muito similares. Caso o leitor entenda serem pertinentes, os resultados das demais combinações estão disponíveis no Apêndice B.

É possível verificar que algumas combinações de taxa de transmissão da porção de dados e de bits de controle não foram avaliados. Nestes casos é entendido que não faz sentido a avaliação de uma taxa de transmissão para porção de dados mais robusta que os bits de controle.

Além disso, quando apresentado a taxa de efetividade do método proposto, note que as taxas de transmissão da porção de controle são apresentadas para certos valores de SNR. Isto se deve ao mapeamento de valores de SNR efetuado anteriormente. Este comportamento é repetido em todos os cenários e emendas avaliados. Tabela 4: Identificação do valor de SNR a partir do qual cada taxa de transmissão resulta em uma probabilidade de entrega maior que 50% para a emenda IEEE 802.11ac.

Emenda	Frequência	Taxa de dados	SNR	Taxa de entrega
		$6,5~{ m Mb/s}$	6 dB	94%
0		$13 { m ~Mb/s}$	9  dB	85%
1ac		$19,5 \mathrm{~Mb/s}$	11 dB	92%
2.1		$26 { m ~Mb/s}$	14 dB	93%
80	$20 \mathrm{~MHz}$	$39 \mathrm{~Mb/s}$	17 dB	57%
년 G		$52 \mathrm{~Mb/s}$	23  dB	85%
		$58,5 \mathrm{~Mb/s}$	24  dB	81%
		$65 { m ~Mb/s}$	25  dB	61%
		$78 { m ~Mb/s}$	30  dB	79%
		$13,5 \mathrm{~Mb/s}$	5  dB	77%
		$27 \mathrm{~Mb/s}$	9 dB	86%
ac		$40,5~{ m Mb/s}$	11 dB	92%
		$54 \mathrm{~Mb/s}$	14 dB	78%
302	40 MHz	$81 \mathrm{~Mb/s}$	17 dB	81%
	40 101112	$108 { m ~Mb/s}$	22  dB	73%
		$121,5 \mathrm{~Mb/s}$	23  dB	65%
		$135 \ \mathrm{Mb/s}$	25  dB	89%
		$162 \mathrm{~Mb/s}$	29  dB	66%
		$180 { m ~Mb/s}$	31  dB	83%
		$29{,}3~{\rm Mb/s}$	5  dB	96%
		$58,5 \mathrm{~Mb/s}$	9 dB	85%
ac		$87,8 \mathrm{~Mb/s}$	10 dB	51%
802.11		$117 \mathrm{~Mb/s}$	13 dB	55%
	80 MHz	20 MHz 175,5 Mb/s 16 c	16 dB	68%
の 1 1 1 1 1 1 1 1 1 1 1 1 1	00 WIIIZ	$234 \mathrm{~Mb/s}$	21 dB	51%
		$263,3 \mathrm{~Mb/s}$	22  dB	53%
		$292,5~{\rm Mb/s}$	24  dB	85%
		$351~{ m Mb/s}$	28  dB	58%
		$390~{ m Mb/s}$	30  dB	77%
		$58,5 \mathrm{~Mb/s}$	5  dB	95%
		117  Mb/s	9 dB	63%
ac		$175,5~{ m Mb/s}$	11 dB	84%
11		$234 \mathrm{~Mb/s}$	13  dB	54%
02.	160 MHz	$351~{ m Mb/s}$	16 dB	65%
		$468 \mathrm{~Mb/s}$	21 dB	67%
		$526,5~{\rm Mb/s}$	23  dB	92%
		$585 { m ~Mb/s}$	24 dB	74%
		$702 { m ~Mb/s}$	28 dB	67%
		$780 \mathrm{~Mb/s}$	30 dB	76%

## 4.1 Cenário sem colisão

Os resultados do primeiro cenário para a emenda IEEE 802.11g e IEEE 802.11ac com canais de 160 MHz, são apresentados nas Figuras 3-6. As Figuras 3(a) e 4(a) mostram a taxa de entrega de pacotes de dados, representada no eixo vertical, como função do SNR do canal. As várias curvas diferentes se referem às possíveis taxas de transmissão usadas nas subportadoras de dados. Já as Figuras 3(b) e 4(b) mostram a taxa de entrega de bits de controle — quando esses são adicionados aos pacotes. Nesse caso, as curvas representam a combinação das taxas utilizadas para as subportadoras de controle e de dados. Como esperado, a porção de controle possui maior robustez que os dados para todos os valores de SNR devido ao uso de taxas sempre iguais ou mais baixas para a porção de controle, aliado ao menor comprimento da informação de controle em comparação ao tamanho total dos pacotes.



Figura 3: Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11g.

A taxa de efetividade para esse cenário nas emendas IEEE 802.11g e IEEE 802.11ac @ 160 MHz, são apresentadas nas Figuras 5 e 6, respectivamente. A Figura 5 exibe os dados apenas para os casos em que a taxa de transmissão da porção de controle é 6, 12 ou 36 Mb/s. Já na Figura 6, são exibidos os dados onde a taxa de transmissão da porção de controle é 58,5, 526,5 e 702 Mb/s. Em cada gráfico, o eixo vertical mostra a taxa de efetividade do método como uma função do SNR do canal. Os padrões das barras associam esses valores de SNR às taxas de transmissão usadas para a porção de dados.

Com a taxa de transmissão de 6 Mb/s para dados e controle, o algoritmo frequentemente classificou erroneamente perdas como sendo por colisão para valores de SNR



Figura 4: Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 160 MHz.



Figura 5: Sem colisões: taxa de efetividade do método para emenda IEEE 802.11g.

menores que 5 dB. É importante destacar, no entanto, que, segundo os resultados da Figura 3(a), a porção de dados raramente chega ao receptor sem corrupções para esta faixa de valores de SNR. Isso indica que uma taxa mais robusta que os 6 Mb/s — algo não disponível no IEEE 802.11g — deveria ser utilizada nesses casos. A partir do SNR de 5 dB, a taxa de efetividade se manteve em 100%, independente da taxa de transmissão

de pacotes de dados adotada e SNR. Por outro lado, quando as taxas de transmissão de 12 e 36 Mb/s são usadas para a subportadora de controle (Figuras 5(b) e 5(c)), o método obteve sempre uma taxa de efetividade de 100%.



Figura 6: Sem colisões: taxa de efetividade do método para emenda IEEE 802.11ac @ 160 MHz.

As mais altas taxas de transmissão da porção de controle foram avaliadas na emenda IEEE 802.11ac @ 160 MHz. Com uma taxa de transmissão de 58,5 Mb/s para dados e controle, o algoritmo frequentemente classificou erroneamente perdas como sendo por colisão para valores com SNR menores que 3 dB, conforme pode ser visto na Figura 6(a). Já nas taxas de transmissão da porção de controle de 526,5 e 702 Mb/s, apresentadas nas Figuras 6(b) e 6(c), o método obteve sempre a mais alta taxa de efetividade, para todas as taxa de dados utilizada.

O método proposto apresentou um bom desempenho geral para o cenário sem colisão. Para a maioria das combinações de taxas de transmissão e valores de SNR avaliados, o método proposto obteve a taxa de efetividade de 100%. A exceção ocorre para os menores valores de SNR avaliados, abaixo de 5 dB para a emenda IEEE 802.11g, e abaixo de 3 dB para a emenda IEEE 802.11ac @ 160 MHz. Este comportamento se mantém para as demais combinações avaliadas.

## 4.2 Cenário com colisão entre pacotes de mesma potência

Nesse cenário, em toda tentativa de transmissão, há uma colisão e as potências dos sinais colidentes no receptor são iguais. Note que todos os resultados reportados aqui foram calculados com base nos resultados das transmissões do transmissor principal, sem levar em conta o que ocorreu com o sinal colidente. Utilizando a emenda IEEE 802.11g, na Figura 7(a), é possível verificar que a taxa de entrega de pacotes de dados se mantém em 0%, independente da taxa de transmissão ou SNR. Quase sempre há perda da porção de dados para todos os valores de SNR na emenda IEEE 802.11ac @ 160 MHz, apresentada na Figura 8(a). Na Figura 7(b), um comportamento semelhante é verificado para a porção de controle na emenda IEEE 802.11g, embora, nesse caso, algumas vezes não houve corrupção dos bits de controle. Ao utilizar taxas de transmissão maiores, com a emenda IEEE 802.11ac @ 160 MHz apresentada na Figura 8(b), é possível verificar que houve corrupção dos bits de controle em menor quantidade, principalmente para SNR menor ou igual a 15 dB.



Figura 7: Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11g.

Avaliando as taxas da emenda IEEE 802.11g, as Figuras 9(a), 9(b) e 9(c) mostram a taxa de efetividade da proposta para 6, 12 e 36 Mb/s, respectivamente. Assim como no caso anterior, nesse cenário o método proposto classifica de maneira correta a causa na maioria dos casos. As exceções ocorreram quando a taxa de 6 Mb/s foi usada para a porção de controle em canais com alto SNR. Nesses cenários, devido ao uso de uma taxa bastante robusta, algumas vezes o receptor foi capaz de recuperar a porção de controle corretamente devido à porção de controle ter menos bits que a de dados. Com isso, o



Figura 8: Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 160 MHz.

receptor erroneamente classificou as perdas das porções de dados como sendo devidas a SNR baixo. Por outro lado, para a faixa de valores de SNR nos quais esses erros de classificação ocorreram, nota-se que o uso das taxas de 12 e 36 Mb/s foi suficiente para classificar corretamente as perdas em 100% dos casos.



Figura 9: Com colisões: taxa de efetividade do método para emenda IEEE 802.11g.

Já na emenda IEEE 802.11ac @ 160 MHz, com uma taxa de transmissão de 58,5

Mb/s para dados e controle, o algoritmo frequentemente classificou erroneamente perdas como sendo por SNR baixo, conforme pode ser visto na Figura 10(a). Já nas taxas de transmissão da porção de controle de 526,5 e 702 Mb/s, apresentadas nas Figuras 10(b) e 10(c), o método obteve sempre a mais alta taxa de efetividade, para todas as taxa de dados utilizada.



Figura 10: Com colisões: taxa de efetividade do método para emenda IEEE 802.11ac @ 160 MHz.

No cenário com colisão, para todas as combinações avaliadas, a taxa de entrega de pacotes de dados quase sempre se mantém em 0%. Já a taxa de entrega de bits de controle variou a medida que a taxa de transmissão avaliada aumenta. As variações ocorreram nos valores menores de SNR, onde não houve corrupção dos bits de controle. Além disso, a utilização de taxas de transmissão de bits de controle menores proporciona uma transmissão tão robusta que possibilita a entrega da porção de controle para valores maiores de SNR. Sendo assim, para maior efetividade do método proposto, não é indicado o uso da menor taxa de transmissão disponível em cada emenda para os bits de controle.

## 4.3 Cenário com colisão com pacote colidente com potência mais baixa

No cenário anterior, avaliou-se o caso da colisão entre pacotes que chegam ao receptor com exatamente a mesma potência. Na prática, devido a diversos fatores, o mais comum é que o sinal de um dos pacotes chegue ao receptor com uma potência mais alta. Conforme os resultados anteriores mostram, quando as potências são iguais, muito provavelmente ambas as porções de controle e dados chegam corrompidas no receptor. Assim, um cenário mais desafiador para o método proposto é aquele de uma colisão em que o pacote principal chega ao receptor com uma potência superior à do pacote colidente. Assim como cenário anterior, os resultados reportados neste cenário foram calculados com base nos resultados das transmissões do transmissor principal, sem levar em conta o que ocorreu com o sinal colidente.

Nas Figuras 11 e 12, são apresentados os resultados obtidos nesse cenário para as emendas IEEE 802.11g e IEEE 802.11ac @ 160 MHz, respectivamente. Para essas simulações, considerou-se que o pacote colidente chega ao receptor com uma potência 3 dB mais baixa que a do pacote principal. Nota-se, na Figura 11(a), que quase sempre há perda da porção de dados para todos os valores de SNR. Por outro lado, dependendo do SNR e da taxa de transmissão de porção de controle, essa é entregue com sucesso com probabilidade relativamente alta, conforme mostrado na Figura 11(b). Já na Figura 12(a) é possível verificar que houve perda da porção de dados na maioria dos valores de SNR, com exceção entre 6 e 8 dB. Em contrapartida, a taxa de entrega de bits de controle é consideravelmente alta para a maioria dos valores de SNR, conforme apresentado na Figura 12(b).

As Figuras 13 e 14 mostram a taxa de efetividade do método para a emenda IEEE 802.11g e IEEE 802.11ac @ 160 MHz nesse cenário, respectivamente. Como esperado, esse cenário se mostra bem mais desafiador que os anteriores. O método proposto exibe falhas na classificação da causa da perda para várias combinações de SNR e taxa de transmissão da porção de controle. Em particular, na Figura 13(a) nota-se que a taxa de 6 Mb/s tem baixa efetividade para valores de SNR acima de 5 dB porque, a partir desse valor, ela se torna robusta o suficiente para que frequentemente a porção de controle seja recebida corretamente. Por outro lado, na Figura 13(c) a taxa de 36 Mb/s resultou em 100% de efetividade para todos os valores de SNR avaliados. Ao utilizar a taxa de 58,5 Mb/s da emenda IEEE 802.11ac, há baixa taxa de efetividade para a maioria dos valores de SNR, conforme a Figura 14(a). As demais taxas de bits de controle avaliadas para esta emenda,



Figura 11: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11g.



Figura 12: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 160 MHz.

apresentaram quase sempre a taxa máxima de efetividade.

Diferentemente do cenário onde o pacote principal e colidente chegam com a mesma potência, quando o pacote colidente têm potência mais baixa é onde há maiores variações da taxa de efetividade do método proposto. A taxa de entrega de pacotes de dados quase sempre é igual a 0%. A exceção ocorre nas emendas IEEE 802.11n (resultados estão disponíveis no Apêndice B) e IEEE 802.11ac, onde há um aumento na taxa de entrega de pacotes de dados, principalmente com taxas de transmissão mais baixas e entre 6 e 8



Figura 13: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de efetividade do método para emenda IEEE 802.11g.



Figura 14: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de efetividade do método para emenda IEEE 802.11ac @ 160 MHz.

dB de SNR. Por outro lado a taxa de entrega de bits de controle sofre grandes variações, para maioria das combinações avaliadas, independentemente da emenda. Apesar de ser o cenário mais desafiador, o método proposto obteve bons resultados relacionados a taxa de efetividade em taxas maiores para a transmissão dos bits de controle. Ao utilizar taxas mais baixas para essa porção, o método tende a diminuir a efetividade.

## 4.4 Melhor relação entre taxa de transmissão de pacotes de dados e bits de controle

Com base nos cenários apresentados, foi identificada a taxa de transmissão ideal para a porção de controle associada a cada taxa usada para a porção de dados. O processo de seleção foi efetuado da seguinte maneira. Para cada taxa de transmissão da porção de dados, computou-se a taxa de efetividade média de cada taxa de controle ao longo de todos os valores de SNR associados àquela taxa de dados.

A Tabela 5 mostra os resultados para a emenda IEEE 802.11g. Os dados são apresentados da seguinte maneira: a largura de banda utilizada (MHz), a porção e as taxas em Mb/s. É interessante notar que, para a maioria das taxas da porção de dados, a melhor opção para a porção de controle foi a mesma taxa. A exceção ocorre com a porção de dados de 12 Mb/s, onde a melhor taxa para a porção de controle é 9 Mb/s.

Nas Tabelas 6 e 7 são apresentados os resultados para as emendas IEEE 802.11n e IEEE 802.11ac, respectivamente. A apresentação dos dados é da mesma maneira explicada anteriormente. Nestas emendas, para todas as taxas da porção de dados, a melhor opção para a porção de controle foi exatamente a mesma taxa. Isso se deve à diferença de comprimento das duas porções: por ser mais curta, a porção de controle se torna mais robusta mesmo utilizando a mesma taxa da porção de dados.

Tabela 5: Melhores taxas para a porção de controle para cada taxa de dados na emenda IEEE 802.11g (Mb/s).

20	Dados	6	9	12	18	24	36	48	54
	Controle	6	9	9	18	24	36	48	54

Utilizando o mapeamento apresentado na Tabela 5, a Figura 15 resume a taxa de efetividade do método proposto nos três cenários avaliados para a emenda IEEE 802.11g. Nota-se que o método obteve bom desempenho em geral nos cenários com e sem colisão — nesse último, principalmente para valores de SNR acima de 5 dB. O cenário do pacote colidente com potência mais baixa é particularmente desafiador, especialmente para en-

Tabela 6: Melhores taxas para a porção de controle para cada taxa de dados na emenda IEEE 802.11n (Mb/s).

20	Dados	6,5	13	19,5	26	39	52	58,5	65
	Controle	6,5	13	19,5	26	39	52	58,5	65
40	Dados	13,5	27	40,5	54	81	108	121,5	135
	Controle	$13,\!5$	27	40,5	54	81	108	121,5	135

Tabela 7: Melhores taxas para a porção de controle para cada taxa de dados na emenda IEEE 802.11ac (Mb/s).

20	Dados	6,5	13	19,5	26	39	52	58,5	65	78	
	Controle	6,5	13	19,5	26	39	52	58,5	65	78	
40	Dados	13,5	27	40,5	54	81	108	121,5	135	162	180
	Controle	13,5	27	40,5	54	81	108	121,5	135	162	180
80	Dados	29,3	58,5	87,8	117	175,5	234	263,3	292,5	351	390
	Controle	29,3	$58,\!5$	87,8	117	175,5	234	263,3	292,5	351	390
160	Dados	58,5	117	175,5	234	351	468	526,5	585	702	780
	Controle	58,5	117	175,5	234	351	468	526,5	585	702	780

laces com SNR menor ou igual a 8 dB. Entretanto, para enlaces de maior qualidade, o método tem sempre mais que 88% (taxas de dados e controle de 18 Mb/s) de efetividade mesmo nesse cenário.



Figura 15: Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11g.

Seguindo a mesma abordagem, mas considerando a Tabela 6 referente à emenda IEEE 802.11n, as Figuras 16 e 17 resumem a taxa de efetividade do método proposto nos três cenários avaliados, utilizando as larguras de banda de 20 e 40 MHz, respectivamente.

O método obteve bom desempenho em geral nos cenários com e sem colisão na emenda

IEEE.11n @ 20 MHz, apresentada na Figura 16. As curvas representadas por estes cenários, comparando com a emenda IEEE 802.11g, são bastante similares. É possível identificar que no cenário sem colisão e valores de SNR acima de 5 dB obtiveram desempenho máximo. O cenário do pacote colidente com potência mais baixa sofreu maiores variações, principalmente para enlaces de menor qualidade. Nos enlaces de maior qualidade o método obteve sempre mais de 76% (taxas de dados e controle de 13 Mb/s, com SNR acima de 10 dB) de efetividade mesmo nesse cenário.



Figura 16: Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11n @ 20 MHz.

Ao utilizar a largura de banda de 40 MHz, obtendo assim maiores taxas para as porções de dados e controle, o método resulta em menor efetividade, conforme a Figura 17. No cenário sem colisão os resultados foram similares aos obtidos para a largura de banda de 20 MHz, onde obteve-se desempenho máximo para valores de SNR acima de 5 dB. Diferente das taxas avaliadas anteriormente, a emenda IEEE 802.11n @ 40 MHz mostrou variações no cenário com colisão. Mesmo com as variações o método proposto obteve sempre mais de 80% (taxas de dados e controle de 13,5 Mb/s, com SNR acima de 8 dB) de efetividade. As maiores variações ocorrem no cenário do pacote colidente com potência mais baixa, obtendo um desempenho bom principalmente para valores de SNR acima de 9 dB. A partir deste valor de SNR, o método sempre obteve mais de 60% (taxas de dados e controle de 27 Mb/s, com SNR maior que 10 dB) de efetividade.

As taxas de efetividade do método proposto nos três cenários avaliados para a emenda IEEE 802.11ac, última emenda analisada, são apresentadas nas Figuras 18, 19, 20 e 21, nas larguras de banda de 20, 40, 80 e 160 MHz, respectivamente. As figuras foram elaboradas considerando as taxas da Tabela 7.



Figura 17: Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11n @ 40 MHz.

Na emenda IEEE 802.11ac @ 20 MHz, o método obteve bom desempenho em geral nos cenários com e sem colisão. Conforme apresentado na Figura 18, as curvas representadas por estes cenários, comparando com as emendas IEEE 802.11g e IEEE 802.11n, são bastante similares. No cenário sem colisão e valores de SNR acima de 5 dB, é possível identificar que obtiveram desempenho máximo. Considerando o cenário com colisão há um excelente desempenho para todas as taxas de transmissão e valores de SNR avaliados. As maiores variações ocorreram no cenário do pacote colidente com potência mais baixa, principalmente para enlaces de menor qualidade. Considerando enlaces de maior qualidade, o método obteve sempre mais de 75% (taxas de dados e controle de 13 Mb/s, com SNR acima de 10 dB) de efetividade mesmo nesse cenário.

Em seguida, na avaliação com a largura de banda de 40 MHz, o método experimentou algumas reduções em sua efetividade, conforme a Figura 19. No cenário sem colisão, os resultados foram similares àqueles quando utilizada a largura de banda de 20 MHz na mesma emenda, onde obteve-se desempenho máximo para valores de SNR acima de 4 dB. Considerando o cenário com colisão, houve algumas variações da taxa de efetividade, porém mesmo com as variações o método proposto obteve sempre mais de 82% (taxas de dados e controle de 13,5 Mb/s, com SNR acima de 8 dB) de efetividade. As maiores variações ocorrem no cenário do pacote colidente com potência mais baixa, obtendo um desempenho bom principalmente para valores de SNR acima de 9 dB. A partir deste valor de SNR, o método sempre obteve mais de 60% (taxas de dados e controle de 27 Mb/s, com SNR maior ou igual a 10 dB) de efetividade.



Figura 18: Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac @ 20 MHz.



Figura 19: Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac @ 40 MHz.

A queda de desempenho foi maior na taxa de efetividade do método com a largura de banda de 80 MHz da emenda IEEE 802.11ac, conforme a Figura 20. O cenário sem colisões obteve desempenho máximo para valores de SNR acima de 3 dB. Para os cenários com colisão, os resultados não foram tão bons. Mesmo assim, no cenário com colisão, o método proposto obteve sempre mais de 97% (taxas de dados e controle de 58,5 Mb/s, com SNR maior ou igual a 9 dB) de efetividade. Os maiores desafios ocorrem no cenário do pacote colidente com potência mais baixa, que obteve um bom desempenho geral, principalmente para valores de SNR acima de 10 dB. A partir deste valor de SNR, o método sempre obteve mais de 66% (taxas de dados e controle de 87,8 Mb/s, com SNR maior ou igual a 12 dB) de efetividade.



Figura 20: Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac @ 80 MHz.

Na emenda IEEE 802.11ac @ 160 MHz de largura de banda, são avaliadas as mais altas taxas de transmissão das porções de dados e controle. Com o aumento das taxas de transmissão, também houve as maiores quedas na taxa de efetividade do método, conforme a Figura 21. O cenário sem colisões obteve desempenho máximo para valores de SNR acima de 3 dB. No cenário com colisão, o método proposto obteve sempre mais de 83% (taxas de dados e controle de 117 Mb/s, com SNR maior ou igual a 9 dB) de efetividade. Os maiores desafios ocorrem no cenário do pacote colidente com potência mais baixa, que obteve um bom desempenho geral, principalmente para valores de SNR acima de 15 dB. A partir deste valor de SNR, o método sempre obteve mais de 92% (taxas de dados e controle de 351 Mb/s, com SNR maior ou igual a 19 dB) de efetividade.

## 4.5 Adicionando subportadora para transmissão de bits de controle

O uso de uma única subportadora pode levar ao entendimento que há um ponto único de falha. Uma solução é a adoção de mais de uma subportadora para transmissão da porção de bits de controle. Com este objetivo, o método proposto foi modificado com a finalidade de avaliar a eficácia neste tipo de abordagem. Para avaliação, foram utilizadas as melhores relações entre taxa de transmissão de pacotes de dados e bits de controle da emenda IEEE 802.11ac com canais de 160 MHz. Esta emenda foi escolhida por definir as taxas de transmissão onde houve as maiores variações das taxas de efetividade.



Figura 21: Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac @ 160 MHz.

Inicialmente, foi efetuada a transmissão utilizando duas subportadoras para transmissão dos bits de controle, onde os bits são divididos igualmente entre as duas subportadoras. Havendo a divisão igualmente entre as duas subportadoras, há dependência entre as subportadoras. Desta maneira, se apenas bits de uma das duas subportadoras chegam corrompidos, isso ainda assim corrompe toda a parte de controle.

Em seguida outra avaliação foi efetuada. Neste caso, são utilizadas duas porções independentes de controle, uma para cada subportadora. Nesta abordagem, considera-se que a informação de controle foi perdida apenas se ambas as porções independentes forem recebidas corrompidas. Assim, só nesse caso o método considera que a perda ocorreu por colisão. Se ao menos uma das porções de controle chega íntegra, o método classifica a perda como sendo por SNR baixo.

Os resultados do método proposto, original e utilizando duas subportadoras para transmissão dos bits de controle, estão separados por cenários. No cenário sem colisão, apresentado na Figura 22, o método proposto original é mais eficiente comparado ao que utiliza duas subportadoras dependentes. Por outro lado, ao utilizar duas subportadoras independentes a eficiência é superior com relação ao método proposto original.

Outro cenário avaliado é o com colisão, apresentado na Figura 23. Neste cenário o método proposto com duas subportadoras dependentes obtém as melhores taxas de efetividade. Em seguida, o método proposto original é o mais eficaz. Ao utilizar duas subportadoras independentes as menores taxas de efetividade são observadas. Com SNR maior ou igual a 11 dB, todos os métodos apresentaram resultados próximos.



Figura 22: Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac @ 160 MHz, comparando método proposto original e método proposto com duas subportadoras no cenário sem colisão.



Figura 23: Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac @ 160 MHz, comparando método proposto original e método proposto com duas subportadoras no cenário com colisão.

Por fim, é avaliado o cenário com colisão e pacote colidente com potência mais baixa, apresentado na Figura 24. Assim como no cenário com colisão onde o pacote principal e colidente possuem a mesma potência, o método proposto com duas subportadoras dependentes obteve as melhores taxas de efetividade. Com duas subportadoras independentes foram obtidos as piores taxas de efetividade entre os métodos avaliados. O método proposto original obteve um desempenho intermediário, comparado com os métodos com duas subportadoras.



Figura 24: Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados para emenda IEEE 802.11ac @ 160 MHz, comparando método proposto original e método proposto com duas subportadoras no cenário com colisão e pacote colidente com potência mais baixa.

De modo geral é possível verificar que o método proposto com duas subportadoras dependentes é uma abordagem que torna a porção de controle efetivamente menos robusta, pelo fato de haver o dobro de chance de ao menos um bit chegar errado ao final da decodificação. Nesse caso, o método classifica a perda como colisão. A adoção desta abordagem proporcionou piores resultados em cenários sem colisão. Em contrapartida, nos cenários com colisão essa abordagem se destacou com as melhores taxas de efetividade.

A outra abordagem com duas subportadoras, porém de maneira independente, se mostra mais robusta, aprimorando o desempenho para o cenário sem colisão e reduzindo para os cenários com colisão. Essa abordagem tornou o método proposto ainda mais robusto, e com isso dificultou a identificação de colisão nos cenários onde havia colisão.

## 4.6 Comparação entre o método proposto e um mecanismo baseado em EVM

A fim de avaliar o método proposto em relação a outro da literatura, foi efetuada a implementação de um mecanismo baseado em EVM. O mecanismo baseado em EVM (AMAN; SIKDAR, 2012) escolhido para comparação foi apresentado no Capítulo 2 na taxonomia proposta, e está presente na categoria de calibração ou treinamento.

Inicialmente, foi efetuada a implementação do mecanismo no mesmo simulador personalizado escrito em Python 2.7. O objetivo é utilizar o mesmo simulador possibilitando uma comparação mais fiel, pois utiliza as mesmas condições de avaliação de desempenho do método proposto. Para isso, foi utilizada a Equação 4.1, onde T é o número de símbolos recebidos e N é o número de subportadoras. Já  $e_{n,k} = r_{n,k} - i_{n,k}$  representa a distância entre o símbolo recebido  $r_{n,k}$  e a posição ideal do símbolo decodificado  $i_{n,k}$ . Por fim,  $P_0$  é a média da potência de todos os símbolos para a subportadora utilizada.

A implementação deste mecanismo no simulador foi efetuada exatamente como apresentada pelos autores. Desta maneira, o receptor não têm certeza de qual símbolo foi enviado, porém ele sabe qual é o símbolo decodificado, sendo este certo ou não. O símbolo decodificado possui uma posição ideal, que não necessariamente corresponde à posição do símbolo recebido. O mecanismo baseado em EVM calcula a distância entre o símbolo recebido e símbolo ideal decodificado, sendo que este que pode ter sido interpretado errado.

$$EVM = \sqrt{\frac{\sum_{n=0}^{T-1} \sum_{k=0}^{N-1} |e_{n,k}|^2}{T.N.P_0}}$$
(4.1)

Durante as simulações para avaliação de desempenho do método proposto, também foi efetuado o cálculo do EVM de cada pacote. Desta maneira, foram considerandos os mesmos parâmetros como: SNR, tamanho do pacote, modulação e codificação. Para cada repetição — baseados em 1000 repetições do simulador para cada conjunto de parâmetros avaliados — o valor de EVM para a porção de dados foi calculado. Além disso, os cenários avaliados foram os mesmos do método proposto: sem colisão, com colisão e com colisão com pacote colidente com potência mais baixa.

Considerando os EVM calculados, é necessário o limiar único  $\gamma$  para cada taxa de transmissão, e indiferente do cenário avaliado. Aqui, há o primeiro grande desafio, que é obter um valor limite único que funcione bem em todos os cenários.

Com o propósito seguir de forma mais fiel possível a metodologia proposta pelos autores, foi utilizado CART. Para tal fim, foi gerado um conjunto de dados com instâncias de perda por colisão e por SNR baixo. O conjunto de dados foi gerado da seguinte maneira: para cada taxa de transmissão, tendo em conta simulações com e sem colisões e o EVM de cada pacote transmitido, foram selecionados os pacotes que foram perdidos. Levando em conta cada pacote perdido, foi criada uma tupla da forma (tipo de perda, EVM). Ao final, com o conjunto dessas tuplas para uma dada taxa de transmissão, foi utilizado CART.

O CART foi executado com auxílio do Weka 3.8.5. O Weka possui uma coleção de algoritmos de aprendizado de máquina para tarefas de mineração de dados. Ele contém ferramentas para preparação de dados, classificação, regressão, clusterização, mineração de regras de associação e visualização (WITTEN et al., 2016). O algoritmo utilizado para CART do mecanismo baseado em EVM foi o *Decision stump*.

Na Figura 25, é apresentado um gráfico de dispersão de valores EVM. Este gráfico foi criado com base no conjunto de dados para a taxa de transmissão de 6 Mb/s na emenda IEEE 802.11g. Em vermelho estão destacados os pacotes perdidos nas simulações sem colisão. Por outro lado, em azul estão os pacotes perdidos nas simulações com colisão.



Instâncias de Simulação

Figura 25: Gráfico de dispersão de valores de EVM - conjunto de dados para taxa de transmissão de 6 Mb/s na emenda IEEE 802.11g @ 20 MHz.

É possível verificar que os valores de EVM dos casos com colisão são tipicamente mais altos, mas os valores de EVM dos casos sem colisão estão na mesma faixa de muitos casos em que houve colisão, o que dificulta muito encontrar o valor limite  $\gamma$  de separação. Isso se torna mais evidente quando, ao utilizar o algoritmo *Decision stump* no Weka, o mesmo até traçou um valor limite  $\gamma$ , porém atribui a causa de perda como colisão em ambos os casos (acima e abaixo do limiar). A árvore de classificação para taxa de transmissão de 6 Mb/s na emenda IEEE 802.11g @ 20 MHz é apresentada na Figura 26.



Figura 26: Árvore de classificação de valores de EVM - conjunto de dados para taxa de transmissão de 6 Mb/s na emenda IEEE 802.11g @ 20 MHz.

No geral, independente da emenda adotada, com taxas de transmissão menores, os casos de colisão e SNR baixo não são facilmente separáveis apenas com a informação do EVM. Conforme aumenta-se a taxa de transmissão, a diferença do valor de EVM entre instâncias de perda por SNR baixo e por colisão se torna cada vez maior. Isso permite obter um valor limite  $\gamma$  mais assertivo, não havendo problema para classificar.

Além disso, faz mais sentido que uma perda por SNR baixo esteja associada a valores de EVM mais altos para 6 Mb/s do que para taxas de transmissão maiores, já que, por ter menos símbolos, a taxa de transmissão de 6 Mb/s precisa que erros maiores sejam introduzidos no sinal para que dois símbolos sejam confundidos no receptor. Desta maneira, é razoável assumir que os valores de EVM para SNR baixo no caso de 6 Mb/s sejam próximos aos dos casos de colisão para essa taxa.

Na Figura 27, é apresentada a árvore de classificação para a taxa de transmissão de 54 Mb/s na emenda IEEE 802.11g @ 20 MHz. É possível verificar que o algoritmo *Decision* stump no Weka conseguiu identificar um valor limite  $\gamma$  que permite a distinção do tipo de perda.

Ainda, no gráfico de dispersão apresentado na Figura 28, nota-se a maior diferença entre os valores de EVM típicos para as instâncias de perda por SNR baixo e por colisão. Devido a esta diferença, se torna mais fácil a separação apenas com a informação do EVM.



Figura 27: Árvore de classificação de valores de EVM - conjunto de dados para taxa de transmissão de 54 Mb/s na emenda IEEE 802.11g @ 20 MHz.

Em vermelho estão destacados os pacotes perdidos nas simulações sem colisão. Por outro lado, em azul estão os pacotes perdidos nas simulações com colisão.



Instâncias de Simulação

Figura 28: Gráfico de dispersão de valores de EVM - conjunto de dados para taxa de transmissão de 54 Mb/s na emenda IEEE 802.11g @ 20 MHz.

Este comportamento é repetido independentemente da emenda adotada. Com taxas de transmissão menores, o mecanismo baseado em EVM apresenta maior dificuldade para classificação do tipo de perda. Para as demais taxas de transmissão, as perdas são mais facilmente classificadas por meio do algoritmo *Decision stump*.

Após a obtenção do valor limite  $\gamma$  para cada taxa de transmissão de cada emenda, prosseguiu-se com a avaliação do EVM em cada um dos três cenários. Para isso, foi verificado o EVM de cada pacote transmitido e comparado com o limiar da taxa de transmissão/emenda utilizada, com o objetivo de identificar a perda de pacote (SNR baixo ou colisão). Posteriormente, foi computada a taxa de efetividade do mecanismo baseado em EVM.

Na comparação entre o método proposto e o mecanismo baseado em EVM, foram avaliadas três emendas: IEEE 802.11g, IEEE 802.11n com largura de banda de 40 MHz, e IEEE 802.11ac com largura de banda de de 80 MHz. Para cada emenda avaliada, foram considerados os três cenários de maneira separada, seguindo a mesma metodologia da avaliação da proposta.

Os resultados para a primeira emenda avaliada, IEEE 802.11g, são apresentados nas Figuras 29, 30 e 31. Cada figura representa um cenário avaliado: sem colisão, com colisão e com colisão com pacote colidente com potência mais baixa, respectivamente. Cada gráfico apresenta curvas de efetividade para a proposta e para o mecanismo baseado em EVM, com o objetivo de facilitar a comparação.



Figura 29: Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário sem colisão para emenda IEEE 802.11g @ 20 MHz.



Figura 30: Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário com colisão para emenda IEEE 802.11g@20 MHz.



Figura 31: Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário com colisão com pacote colidente com potência mais baixa para emenda IEEE 802.11g @ 20 MHz.

É possível verificar que o mecanismo baseado em EVM possui excelentes resultados no cenário sem colisão, como pode ser visto na Figura 29. Neste cenário, o método proposto apresentou taxas de efetividade inferiores com relação ao mecanismo baseado em EVM, considerando valores de SNR menores que 5 dB. Em contrapartida, o mecanismo baseado em EVM possui dificuldades consideráveis nos cenário com colisão e com colisão com pacote colidente com potência mais baixa, principalmente para valores de SNR inferiores a 7 dB, de acordo com as Figuras 30 e 31. Nestes últimos dois cenários, o método proposto apresentou melhores taxas de efetividade com relação ao mecanismo baseado em EVM.

A próxima emenda avaliada, IEEE 802.11n com canais de 40 MHz, é apresentada nas Figuras 32, 33 e 34, cada uma correspondendo a um dos três cenários avaliados.



Figura 32: Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário sem colisão para emenda IEEE 802.11n @ 40 MHz.



Figura 33: Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário com colisão para emenda IEEE 802.11n @ 40 MHz.

O comportamento relacionado à taxa de efetividade no cenário sem colisão se mantém mais favorável ao mecanismo baseado em EVM para a emenda IEEE 802.11n e largura de banda de 40 MHz, como pode ser visto na Figura 32. No cenário com colisão, apresentado na Figura 33, o método proposto se sobressai ao mecanismo baseado em EVM, mesmo nos valores de SNR menores. Ao final, no cenário com colisão com pacote colidente com


Figura 34: Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário com colisão com pacote colidente com potência mais baixa para emenda IEEE 802.11n @ 40 MHz.

potência mais baixa, apresentado na Figura 34, o método proposto apresenta resultados melhores para SNR menores que 6 dB, porém o mecanismo baseado em EVM consegue destaque entre os valores 9 e 14 dB de SNR. Para os demais valores de SNR as abordagens possuem excelentes resultados.

Por fim, é avaliada a emenda IEEE 802.11ac e com canais de 80 MHz, apresentada nas Figuras 35, 36 e 37, cada uma correspondendo a um dos três cenários avaliados.

No cenário sem colisão, apresentado na Figura 35, o método proposto possui menores taxas de efetividade com relação ao mecanismo baseado em EVM, para menores valores de SNR. A taxa de efetividade do método proposto e do mecanismo baseado em EVM são bastante similares no cenário com colisão, conforme pode ser visualizado na Figura 36. No cenário com colisão com pacote colidente com potência mais baixa, o último avaliado e apresentado na 37, o método proposto apresenta melhores resultados para valores até 6 dB. Já o mecanismo baseado em EVM sobrepuja o método proposto entre os valores 9 e 15 dB de SNR. Nos demais valores, as duas abordagens apresentaram resultados similares.

No geral, é possível constatar que tanto o método proposto como o mecanismo baseado em EVM possuem melhores taxas de efetividade para valores mais altos de SNR. Considerando o cenário sem colisão e SNR baixo, o mecanismo baseado em EVM é excelente, e o método proposto possui taxa de efetividade que cai com a redução do SNR. Por outro lado, o método proposto é muito bom para o cenário com colisão e SNR baixo. Neste cenário o desempenho do mecanismo baseado em EVM não é ruim, mas significa-



Figura 35: Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário sem colisão para emenda IEEE 802.11ac @ 80 MHz.



Figura 36: Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário com colisão para emenda IEEE 802.11ac @ 80 MHz.

tivamente pior dependendo da emenda utilizada. Além disso, o mecanismo baseado em EVM possui baixíssima efetividade em valores menores de SNR no cenário com colisão com pacote colidente com potência mais baixa. Neste mesmo cenário, o método proposto também possui problemas com a efetividade, mas ainda assim é, em geral, melhor.

Levando em consideração a taxa de efetividade das abordagens em diferentes emendas e cenários avaliados, é possível identificar que ambas possuem resultados bons e ruins, dependendo da situação. Sendo assim, pode haver espaço para um classificador que



Figura 37: Comparação entre taxa de efetividade do método proposto com relação ao mecanismo baseado em EVM, no cenário com colisão com pacote colidente com potência mais baixa para emenda IEEE 802.11ac @ 80 MHz.

combine o método proposto e o mecanismo baseado em EVM, a fim de tentar melhorar a acurácia da predição.

### 5 Conclusão

Neste trabalho, foi apresentado um novo método para detecção e identificação da causa de perda de pacotes em redes IEEE 802.11. A distinção entre os tipos de perda de pacotes permite otimizar o uso do meio sem fio, diminuindo gastos desnecessários de tempo e energia com retransmissões de pacotes, que causam a redução da capacidade da rede e, consequentemente, a diminuição da vazão.

O método proposto inclui bits de controle em uma subportadora específica do símbolo OFDM no transmissor. Essa portadora específica dos bits de controle é transmitida usando uma taxa de transmissão que a torna mais robusta que a a porção de dados. Esses bits de controle são processados no receptor para identificar a causa da perda quando a porção de dados sofre corrupção.

Através de uma avaliação em um ambiente simulado, demonstramos a seleção ideal da taxa de transmissão para a portadora de controle. Além disso, mostramos que usando essa seleção ideal de taxas o método proposto alcança alta efetividade na classificação da causa da perda em cenários sem e com colisão.

Em ambientes sem colisão, o mecanismo apresentou resultados satisfatórios na maioria das transmissões. Contudo, houve equívocos na identificação da causa de perda de pacotes, quando as taxas de transmissão de pacotes de dados e controle eram mais baixas. Por exemplo, quando a taxa de transmissão da porção de controle estava fixada em 6 Mb/s, o método classificou a perda como colisão, sendo que a causa real era SNR baixo.

Ao avaliar cenários com colisão, o método obteve excelentes resultados na detecção e identificação da causa de perda. Quando a potência do sinal transmitido e colidente são iguais, o método se comportou como esperado, classificando de maneira correta a causa de perda. O mesmo ocorreu quando a potência do sinal colidente é maior em relação ao sinal transmitido. Todavia, quando a potência do sinal transmitido é maior em relação ao sinal colidente, o mecanismo classificou o tipo de perda de maneira imprecisa. Isso se deve ao fato de os bits de controle terem sido entregues com sucesso, mesmo quando o pacote de dados foi perdido. Neste caso, o método classificou a perda como SNR baixo, ao invés de colisão.

O método proposto foi modificado a fim de avaliar o uso de mais de uma subportadora para a transmissão dos bits de controle. Foram avaliadas duas abordagens: subportadoras dependentes, onde os bits de controle são espalhados entre as subportadoras, e subportadoras independentes, onde os bits de controle são duplicados entre as subportadoras. No cenário sem colisão, o método proposto com duas subportadoras independentes obteve melhor desempenho, porém na avaliação com colisão essa abordagem obteve o pior desempenho. Por outro lado, o método proposto com duas subportadoras dependentes se destaca no cenário com colisão, embora, no cenário sem colisão, tenha uma redução considerável na taxa de efetividade. Essa variação da taxa de efetividade dependendo do cenário avaliado se deve a robustez proporcionada por cada abordagem. O método proposto original obteve um bom desempenho geral, independente do cenário avaliado.

Além disso, o método proposto foi comparado com um método da literatura. O método da literatura escolhido foi um mecanismo baseado em EVM. Para um comparativo mais fiel, foram adotados o mesmo simulador e cenários utilizados na avaliação do método proposto, proporcionando cenários homogêneos para de fato verificar a taxa de efetividade de cada método. O método proposto possui melhor desempenho geral em cenários com colisão e SNR baixo. No entanto, o mecanismo baseado em EVM é excelente para o cenário sem colisão e SNR baixo.

Ademais, foi efetuado um estudo do estado da arte das abordagens de distinção dos tipos de perda de pacotes. Foram categorizados e definidos os dois principais tipos de perdas de pacotes, colisão e SNR baixo. Considerando as características destas abordagens de distinção dos tipos de perda de pacotes, foi proposta uma taxonomia, onde as abordagens foram classificadas de maneira não mutuamente exclusiva. As classificações aplicadas se diferenciam com relação a: necessidade de calibração ou treinamento, dependência de *feedback* do receptor, adição de *overhead* representativo, uso detecção contínua de preâmbulo e os tipos de aplicação para a causa de perda de pacote. Durante a descrição das abordagens foram apresentados seus pontos fortes e fracos, destacando problemas identificados que estão em aberto.

#### 5.1 Trabalhos futuros

Como trabalho futuro, uma aplicação possível para o método é dar suporte a mecanismos como acesso ao meio ou a adaptação da taxa de transmissão. Além destas aplicações, é possível explorar melhorias no método. Durante a comparação com o mecanismo baseado em EVM, foi possível identificar que ambos possuem resultados bons e ruins, dependendo da situação avaliada. Desta maneira, há possibilidade de elaboração de um classificador que combine método proposto e o mecanismo baseado em EVM. A combinação destes métodos pode melhorar a acurácia da predição.

Por fim, também é possível investigar o uso de um algoritmo *Round-Robin* nos símbolos de controle de forma a espalhá-los por várias das subportadoras do canal ao longo da transmissão do pacote. Isso tornaria o método mais resiliente a efeitos de desvanecimento seletivo.

# REFERÊNCIAS

AMAN, M. N.; SIKDAR, B. Distinguishing between channel errors and collisions in IEEE 802.11. In: 2012 46th Annual Conference on Information Sciences and Systems (CISS). [S. l.: s. n.], 2012. p. 1–6.

BARCELO, J. et al. CSMA with Enhanced Collision Avoidance: A Performance Assessment. In: VTC Spring 2009 - IEEE 69th Vehicular Technology Conference.[S. l.: s. n.], 2009. p. 1–5.

BICKET, John C. Bit-rate selection in wireless networks. 2005. Tese (Doutorado)Master's Thesis, MIT.

BULHÕES, R. P.; PASSOS, D.; ALBUQUERQUE, C. V. N. Collision probability estimation in wireless networks. In: 2016 8th IEEE Latin-American Conference on Communications (LATINCOM). [S. l.: s. n.], 2016. p. 1–6. DOI: 10.1109/LATINCOM.2016.7811595.

CHONGGANG WANG; BO LI; LEMIN LI. A new collision resolution mechanism to enhance the performance of IEEE 802.11 DCF. **IEEE Transactions on Vehicular Technology**, v. 53, n. 4, p. 1235–1246, 2004.

CISCO. Cisco Annual Internet Report (2018–2023) White Paper. [S. l.]: Cisco, mar. 2020. Disponível em:

<https://www.cisco.com/c/en/us/solutions/collateral/executiveperspectives/annual-internet-report/white-paper-c11-741490.html>.

JI-HOON YUN; SEUNG-WOO SEO. Collision Detection based on RE Energy Duration in IEEE 802.11 Wireless LAN. In: 2006 1st International Conference on Communication Systems Software Middleware. [S. l.: s. n.], 2006. p. 1–6.

IEEE. IEEE Standard for Information Technology – Local and metropolitan area networks – Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs): Amendment 1: Add Alternate PHYs. **IEEE Std 802.15.4a-2007** (Amendment to **IEEE Std 802.15.4-2006**), p. 1–210, 2007. DOI: 10.1109/IEEESTD.2007.4299496. IEEE. IEEE Standard for Information Technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band. IEEE Std 802.11g-2003 (Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003) as amended by IEEE Stds 802.11a-1999, 802.11b-1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001), p. 1–104, 2003. DOI: 10.1109/IEEESTD.2003.94282.

\_\_\_\_\_\_. 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 Amendment 1: Enhancements for High-Efficiency WLAN. **IEEE Std 802.11ax-2021 (Amendment to IEEE Std 802.11-2020)**, p. 1–767, 2021. DOI: 10.1109/IEEESTD.2021.9442429.

\_\_\_\_\_. IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. **IEEE Std 802.11-1997**, p. 1–445, 1997. DOI: 10.1109/IEEESTD.1997.85951.

JAEHYUK CHOI et al. EBA: an enhancement of the IEEE 802.11 DCF via distributed reservation. **IEEE Transactions on Mobile Computing**, v. 4, n. 4, p. 378–390, 2005.

JAMIESON, Kyle; BALAKRISHNAN, Hari. PPR: Partial Packet Recovery for Wireless Networks. **SIGCOMM Comput. Commun. Rev.**, Association for Computing Machinery, New York, NY, USA, v. 37, n. 4, p. 409–420, ago. 2007. ISSN 0146-4833. DOI: 10.1145/1282427.1282426. Disponível em:

<https://doi.org/10.1145/1282427.1282426>.

JUNIPERRESEARCH. IoT The Internet of Transformation 2020. [S. l.: s. n.], 2020. Disponível em: <a href="https://www.juniperresearch.com/document-library/white-papers/iot-the-internet-of-transformation-2020">https://www.juniperresearch.com/document-library/white-papers/iot-the-internet-of-transformation-2020</a>>.

MAGLOGIANNIS, Vasilis. Innovative Methods for Fair Coexistence between LTE and Wi-Fi in Unlicensed Spectrum. Jan. 2018. Tese (Doutorado).

MAGUOLO, F.; LACAGE, M.; TURLETTI, T. Efficient collision detection for auto rate fallback algorithm. In: 2008 IEEE Symposium on Computers and Communications. [S. l.: s. n.], 2008. p. 25–30.

NS2. The Network Simulator – ns-2. [S. l.: s. n.], 2007. Disponível em: <a href="http://www.isi.edu/nsnam/ns/">http://www.isi.edu/nsnam/ns/</a>>.

NS3. The Network Simulator – ns-3. [S. l.: s. n.], 2008. Disponível em: <a href="https://www.nsnam.org/">https://www.nsnam.org/></a>.

PASSOS, Diego.; BALBI, Helga D.; CARRANO, Ricardo C. **Tecnologias de Redes Sem Fio**. Rio de Janeiro, RJ, Brasil: Escola Superior de Redes, 2016. ISBN 978-85-63630-54-4.

PENG, J.; CHENG, L.; SIKDAR, B. A Wireless MAC Protocol with Collision Detection. **IEEE Transactions on Mobile Computing**, v. 6, n. 12, p. 1357–1369, 2007.

RAYANCHU, S. et al. Diagnosing Wireless Packet Losses in 802.11: Separating Collision from Weak Signal. In: IEEE INFOCOM 2008 - The 27th Conference on Computer Communications. [S. l.: s. n.], 2008. p. 735–743.

SEN, S.; ROY CHOUDHURY, R.; NELAKUDITI, S. CSMA/CN: Carrier Sense Multiple Access With Collision Notification. **IEEE/ACM Transactions on Networking**, v. 20, n. 2, p. 544–556, 2012.

SEN, Souvik; SANTHAPURI, Naveen et al. AccuRate: Constellation Based Rate Estimation in Wireless Networks. In: 7TH USENIX Symposium on Networked Systems Design and Implementation (NSDI 10). San Jose, CA: USENIX Association, abr. 2010. Disponível em: <a href="https://www.usenix.org/conference/nsdi10-0/accurate-constellation-based-rate-estimation-wireless-networks">https://www.usenix.org/conference/nsdi10-0/accurate-constellation-based-rate-estimation-wireless-networks</a>.

VUTUKURU, Mythili; BALAKRISHNAN, Hari; JAMIESON, Kyle. Cross-Layer Wireless Bit Rate Adaptation. **SIGCOMM Comput. Commun. Rev.**, Association for Computing Machinery, New York, NY, USA, v. 39, n. 4, p. 3–14, ago. 2009. ISSN 0146-4833. DOI: 10.1145/1594977.1592571. Disponível em: <https://doi.org/10.1145/1594977.1592571>.

WHITEHOUSE, K. et al. Exploiting the capture effect for collision detection and recovery. In: THE Second IEEE Workshop on Embedded Networked Sensors, 2005. EmNetS-II. [S. l.: s. n.], 2005. p. 45–52.

WITTEN, Ian H. et al. Data Mining, Fourth Edition: Practical Machine Learning Tools and Techniques. 4th. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2016. ISBN 0128042915.

WU, M. et al. Collision Recognition in Multihop IEEE 802.15.4-Compliant Wireless Sensor Networks. **IEEE Internet of Things Journal**, v. 6, n. 5, p. 8542–8552, 2019.

ZENG, Zheng; KUMAR, P. R. Towards Optimally Exploiting Physical Layer Information in OFDM Wireless Networks. In: PROCEEDINGS of the 4th Annual International Conference on Wireless Internet. Maui, Hawaii, USA: ICST (Institute for Computer Sciences, Social-Informatics e Telecommunications Engineering), 2008. (WICON '08). ISBN 9789639799363.

ZHU, Y.; SUN, Y. Packet-Level Failure Classification by Characterizing Failure Patterns in Wireless Sensor Networks. In: 2015 IEEE Global Communications Conference (GLOBECOM). [S. l.: s. n.], 2015. p. 1–6.

# APÊNDICE A - SIMULADOR PERSONALIZADO

Devido a falta de modelagem da camada física em simuladores conhecidos, um simulador personalizado foi utilizado para avaliação de desempenho. Este simulador é escrito em Python 2.7, e possibilita a parametrização de vários atributos. O simulador é composto por um transmissor, que envia o sinal principal, e um receptor. Também é possível adicionar um outro transmissor, que irá enviar um sinal colidente.

Durante a simulação é gerado um sinal do pacote principal a ser transmitido. Para isso são gerados bits aleatórios para a porção de dados, e em seguida efetuado um CRC32 para verificação de integridade dos bits da porção de dados. Com o conjunto dos bits de dados e o CRC32 é realizada a codificação dos bits, que serão agrupados de acordo com a modulação utilizada pela porção de dados. Em seguida é efetuada a tradução dos bits de dados em uma sequência de símbolos.

Um processo semelhante é executado para a porção de controle. Assim como a porção de dados, os bits de controle são gerados aleatoriamente. Diferentemente da porção de dados, o transmissor adiciona um CRC de 4 bits que é computado exclusivamente sobre os bits de controle. Com os bits e o CRC, é efetuada a codificação dos bits de controle, em seguida o agrupamento de acordo com a modulação utilizada, e ao final a tradução dos bits de controle em uma sequência de símbolos.

Considerando a sequência de símbolos de dados e controle, são gerados os símbolos OFDM. Sobre cada símbolo OFDM são calculadas as amostras de tempo. Por fim, é anexado o prefixo cíclico a cada amostra de tempo OFDM. Todo este processo de geração de um sinal do pacote principal e bits de controle, é repetido para o pacote colidente, se houver outro transmissor, aplicando o respectivo ganho de colisão.

Com os símbolos OFDM obtidos no processo de geração do sinal, durante a transmissão destes símbolos são introduzidas modificações no canal (e.g., ruído e distorções). Já o processo de interpretação do sinal recebido, incluindo a porção de dados e bits de controle, funciona da seguinte maneira. Inicialmente é dividido o sinal recebido em sequências de amostras de tempo, para cada símbolo OFDM com prefixo cíclico. Em seguida são removidos os prefixos cíclicos.

O próximo passo é computar a lista de símbolos OFDM no domínio da frequência. Sendo assim, é estimado os parâmetros do canal para equalização, aplicado a equalização. Considerando os símbolos OFDM equalizados, é executada a demultiplexação da porção de dados e bits de controle. Com os símbolos demultiplexados é efetuada a concatenação deles em listas completas de símbolos, uma para a porção de dados e outra para os bits de controle.

Com as listas completas de símbolos, são demoduladas a porção de dados e os bits de controle. Após a demodulação são executadas as linearizações da porção de dados e bits de controle.

O processo de análise da transmissão é iniciado com a verificação do BER da porção de dados codificada e decodificada, além do CRC dela. Este mesmo processo é executado para os bits de controle. Se a porção de dados ou bits de controle possuírem BER maior que zero, o simulador identifica que houve perda da porção específica.

# APÊNDICE B - RESULTADOS COMPLEMENTARES

Os resultados das emendas IEEE 802.11n e IEEE 802.11ac são similares aos da emenda IEEE 802.11g, apresentados no Capítulo 4. Desta maneira, eles foram separados neste Apêndice para análise e consulta, caso o leitor entenda ser pertinente.

#### **B.1** Cenário sem colisão

Para obtenção de todas as taxas de transmissão da emenda IEEE 802.11n, os testes foram efetuados com as larguras de banda de 20 e 40 MHz, conforme as Figuras 38-41. Seguindo as mesmas características explicadas no Capítulo 4, a Figura 38(a) mostra a taxa de entrega de pacotes de dados, representada no eixo vertical, como função do SNR do canal. É possível identificar várias curvas diferentes referentes às possíveis taxas de transmissão usadas nas subportadoras de dados. Ao lado, na Figura 38(b), há a taxa de entrega de bits de controle, onde as curvas representam a combinação das taxas utilizadas para as subportadoras de controle e de dados, respectivamente. Assim como na emenda IEEE 802.11g, a porção de controle possui maior robustez que os dados para todos os valores. Nas Figuras 39(a) e 39(b), utilizando a emenda IEEE 802.11n porém com a largura de banda de 40 MHz, o comportamento foi semelhante ao com a largura de banda de 20 MHz.

Ainda acerca da emenda IEEE 802.11n, a taxa de efetividade para o cenário sem colisões é apresentada nas Figuras 40 e 41. Na Figura 40 são exibidos os dados apenas para os casos em que a taxa de transmissão da porção de controle é 6,5, 19,5 ou 52 Mb/s. Já na Figura 41 as taxas de transmissão da porção de controle são apresentadas em 27, 40,5 ou 108 Mb/s. Em cada gráfico, o eixo vertical mostra a taxa de efetividade do método como uma função do SNR do canal. Os padrões das barras associam esses valores de SNR às taxas de transmissão usadas para a porção de dados.



Figura 38: Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11n @ 20 MHz.



Figura 39: Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11n @ 40 MHz.

Com a taxa de transmissão de 6,5 Mb/s para dados e controle, o algoritmo frequentemente classificou erroneamente perdas como sendo por colisão para valores de SNR menores que 5 dB. É importante destacar, no entanto, que, segundo os resultados da Figura 38(a), a porção de dados raramente chega ao receptor sem corrupções para esta faixa de valores de SNR. Isso indica que uma taxa mais robusta que os 6,5 Mb/s — algo não disponível no IEEE 802.11n @ 20 MHz — deveria ser utilizada nesses casos. A partir do SNR de 5 dB, a taxa de efetividade se manteve em 100%, independente da taxa de transmissão de pacotes de dados adotada e SNR. Por outro lado, quando as taxas de transmissão de 19,5 e 52 Mb/s são usadas para a subportadora de controle (Figuras 40(b)



Figura 40: Sem colisões: taxa de efetividade do método para emenda IEEE 802.11<br/>n@20 MHz.



Figura 41: Sem colisões: taxa de efetividade do método para emenda IEEE 802.11<br/>n@40 MHz.

e 40(c)), o método obteve sempre uma taxa de efetividade de 100%.

Utilizando a largura de banda de 40 MHz na emenda IEEE 802.11n, com todas as taxas de transmissão da porção de controle avaliadas, o método obteve sempre a mais alta taxa de efetividade. Apesar de não ter sido avaliada a taxa de transmissão da porção de controle em 13,5 Mb/s, levando em consideração a Figura 39(a), é possível supor que o algoritmo irá classificar erroneamente perdas como sendo por colisão para valores de SNR menores que 5 dB. Isto se deve ao fato de a porção de dados raramente chegar ao receptor sem corrupções entre os SNRs de 0 e 4 dB.

Por fim, foram avaliadas todas as taxas de transmissão da emenda IEEE 802.11ac. Para isso, os testes foram efetuados com as larguras de banda de 20, 40 e 80, conforme as Figuras 42-47. Seguindo as mesmas características explicadas no Capítulo 4, as Figuras 42(a), 43(a) e 44(a) mostram a taxa de entrega de pacotes de dados, representada no eixo vertical, como função do SNR do canal. É possível identificar várias curvas diferentes referentes às possíveis taxas de transmissão usadas nas subportadoras de dados. Ao lado, nas Figuras 42(b), 43(b) e 44(b), há a taxa de entrega de bits de controle, onde as curvas representam a combinação das taxas utilizadas para as subportadoras de controle e de dados, respectivamente. Nas Figuras 43 e 44, utilizando a emenda IEEE 802.11ac, porém com as larguras de banda de 40 e 80 MHz, respectivamente, o comportamento foi semelhante ao com a largura de banda de 20 MHz (Figura 42). Assim como nas emendas IEEE 802.11g e IEEE 802.11n, a porção de controle possui maior robustez que os dados para todos os valores.



Figura 42: Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 20 MHz.

Com relação a emenda IEEE 802.11ac, a taxa de efetividade para o cenário sem



Figura 43: Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 40 MHz.



Figura 44: Sem colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 80 MHz.

colisões é apresentada nas Figuras 45, 46 e 47. Na Figura 45 são exibidos os dados apenas para os casos em que a taxa de transmissão da porção de controle é 6,5, 19,5 ou 65 Mb/s. Já na Figura 46 as taxas de transmissão da porção de controle são apresentadas em 13,5, 40,5 ou 135 Mb/s. A Figura 47 apresenta as taxas de transmissão da porção de controle de 29,3, 175,5 ou 292,5 Mb/s. Em cada gráfico, o eixo vertical mostra a taxa de efetividade do método como uma função do SNR do canal. Os padrões das barras associam esses valores de SNR às taxas de transmissão usadas para a porção de dados.

Avaliando a taxa de transmissão de 6,5 Mb/s para dados e controle, o algoritmo repetidamente classificou de maneira errada perdas como sendo por colisão para valores de



Figura 45: Sem colisões: taxa de efetividade do método para emenda IEEE 802.11ac@ 20 MHz.



Figura 46: Sem colisões: taxa de efetividade do método para emenda IEEE 802.11ac@40 MHz.



Figura 47: Sem colisões: taxa de efetividade do método para emenda IEEE 802.11ac @ 80 MHz.

SNR menores que 5 dB. Para essa faixa de valores de SNR, a porção de dados dificilmente chega ao receptor sem corrupções, conforme é apresentado na Figura 42(a). Isso indica que uma taxa mais robusta que os 6,5 Mb/s — algo não disponível no IEEE 802.11ac @ 20 MHz — deveria ser utilizada nesses casos. A partir do SNR de 5 dB, a taxa de efetividade se manteve em 100%, independente da taxa de transmissão de pacotes de dados adotada e SNR. Essa taxa de efetividade de 100% também é visualizada quando utilizado as taxas de transmissão de 19,5 e 65 Mb/s para a subportadora de controle, segundo as Figuras 45(b) e 45(c).

Na largura de banda de 40 MHz da emenda IEEE 802.11ac, foram avaliadas as taxas de transmissão da porção de controle de 13,5, 40,5 e 135 Mb/s. Na Figura 46(a) o algoritmo classificou de maneira errada perdas como sendo por colisão para valores de SNR menores que 4 dB. A razão da falha se deve ao mesmo motivo quando utilizado a largura de banda de 20 MHz, onde a porção de dados raramente chega ao receptor sem corrupções para esta faixa de valores de SNR. Para as demais taxas de transmissão da porção de controle, apresentadas nas Figuras 46(b) e 46(c), o método obteve sempre a mais alta taxa de efetividade.

Seguindo para a próxima largura de banda, de 80 MHz, da emenda IEEE 802.11ac,

foram avaliadas as taxas de transmissão da porção de controle de 29,3, 175,5 e 292,5 Mb/s. Mantendo as características das taxas mais baixas previamente avaliadas, na Figura 47(a) o algoritmo classificou de maneira errada perdas como sendo por colisão para valores de SNR menores que 3 dB, onde a taxa de transmissão para dados e controle é de 29,3 Mb/s. Nas taxas de transmissão da porção de controle de 175,5 e 292,5 Mb/s, apresentadas nas Figuras 47(b) e 47(c), o método obteve sempre a mais alta taxa de efetividade, independente da taxa de dados utilizada.

#### **B.2** Cenário com colisão entre pacotes de mesma potência

Assim como no cenário anterior, para obtenção de todas as taxas de transmissão da emenda IEEE 802.11n, os testes foram efetuados com as larguras de banda de 20 e 40 MHz, conforme as Figuras 48-51. A Figura 48(a) mostra a taxa de entrega de pacotes de dados, representada no eixo vertical, como função do SNR do canal. É possível identificar que a taxa de entrega de pacotes de dados se manteve em 0%, independente da taxa de dados e SNR utilizados. Ao lado, na Figura 48(b), há a taxa de entrega de bits de controle, onde há a combinação das taxas utilizadas para as subportadoras de controle e de dados. A taxa de entrega de bits de controle se manteve em 0% na maioria das combinações avaliadas, conforme esperado por se tratar de um cenário com colisão.

Na Figura 49(a), utilizando a emenda IEEE 802.11n porém com a largura de banda de 40 MHz, o comportamento relacionado a taxa de entrega de pacotes de dados foi semelhante ao com a largura de banda de 20 MHz. Já com relação a taxa de entrega de bits de controle, apresentada na Figura 49(b), foi possível identificar uma elevação ao utilizar a combinação de 13,5 Mb/s para pacotes de dados e bits de controle. A medida que o valor de SNR aumenta, a taxa de entrega de bits de controle cresce. Este comportamento se deve a maior robustez da porção de controle, com relação a porção de dados.

A taxa de efetividade para o cenário sem colisões da emenda IEEE 802.11n é apresentada nas Figuras 50 e 51. Na Figura 50 são exibidos os dados apenas para os casos em que a taxa de transmissão da porção de controle é 6,5, 19,5 ou 52 Mb/s. Já na Figura 51 as taxas de transmissão da porção de controle são apresentadas em 27, 40,5 ou 108 Mb/s. Em cada gráfico, o eixo vertical mostra a taxa de efetividade do método como uma função do SNR do canal. Os padrões das barras associam esses valores de SNR às taxas de transmissão usadas para a porção de dados.



Figura 48: Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11n @ 20 MHz.



Figura 49: Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11n @ 40 MHz.

O algoritmo classificou corretamente os tipos de perdas na maioria dos casos ao utilizar a taxa de transmissão de 6,5 Mb/s para dados e controle, conforme a Figura 50(a). As exceções ocorreram em canais com alto SNR. Nesses cenários, devido ao uso de uma taxa bastante robusta, algumas vezes o receptor foi capaz de recuperar a porção de controle, classificando de maneira equivocada as perdas como sendo SNR baixo. Nesta mesma faixa onde houve falha na classificação, ao utilizar taxas de bits de controle maiores a taxa de efetividade se manteve em 100%. Isso é apresentado nas Figuras 50(b) e 50(c).

Com a largura de banda de 40 MHz na emenda IEEE 802.11n, considerando todas as taxas de transmissão da porção de controle avaliadas, o método obteve alta taxa de efetivi-



Figura 50: Com colisões: taxa de efetividade do método para emenda IEEE 802.11<br/>n@ 20 MHz.



Figura 51: Com colisões: taxa de efetividade do método para emenda IEEE 802.11<br/>n@40 MHz.

dade no geral. Com a taxa de bits de controle em 27 Mb/s, apresentada na Figura 51(a), à medida que canais com alto SNR são utilizados a taxa de efetividade reduz vagarosamente. Nas demais taxas de bits de controle avaliadas, o algoritmo frequentemente classificou corretamente os tipos de perdas na maioria dos casos, conforme apresentado nas Figuras 51(b) e 51(c).

Também foram avaliadas todas as taxas de transmissão da emenda IEEE 802.11ac. Para isso, os testes foram efetuados com as larguras de banda de 20, 40 e 80 MHz, conforme as Figuras 52-57. Seguindo as mesmas características explicadas no Capítulo 4, as Figuras 52(a), 53(a) e 54(a) mostram a taxa de entrega de pacotes de dados, representada no eixo vertical, como função do SNR do canal. Ao lado, nas Figuras 52(b), 53(b) e 54(b), há a taxa de entrega de bits de controle.

Tendo em vistas o aumento da taxa da porção de dados, a taxa de entrega de pacotes de dados se manteve igual a 0%, conforme apresentado nas Figuras 53(a) e 54(a), com larguras de banda de 40 e 80 MHz, respectivamente. Assim como nas emendas IEEE 802.11g e IEEE 802.11n, a porção de controle possui maior robustez que os dados para todos os valores. A robustez é visualizada nas Figuras 53(b) e 54(b), onde algumas vezes o receptor foi capaz de recuperar a porção de controle, classificando de maneira equivocada as perdas como sendo SNR baixo.



Figura 52: Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 20 MHz.

Para a emenda IEEE 802.11ac, a taxa de efetividade para o cenário com colisões é apresentada nas Figuras 55, 56 e 57. Na Figura 55 são exibidos os dados apenas para os casos em que a taxa de transmissão da porção de controle é 6,5, 19,5 ou 65 Mb/s. Já na Figura 56 as taxas de transmissão da porção de controle são apresentadas em 13,5, 40,5



Figura 53: Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 40 MHz.



Figura 54: Com colisões: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 80 MHz.

ou 135 Mb/s. A Figura 57 apresenta as taxas de transmissão da porção de controle de 29,3, 175,5 ou 292,5 Mb/s. Em cada gráfico, o eixo vertical mostra a taxa de efetividade do método como uma função do SNR do canal. Os padrões das barras associam esses valores de SNR às taxas de transmissão usadas para a porção de dados.

Com a taxa de transmissão de 6,5 Mb/s para dados e controle, o algoritmo frequentemente classificou corretamente perdas como sendo por colisão. As exceções ocorrem para valores de SNR maiores que 14 dB. A partir do SNR de 14 dB, a taxa de efetividade varia devido a alta robustez da porção de controle. A variação ocorre pois o receptor consegue recuperar a porção de controle, classificando erroneamente o tipo de perda como SNR



Figura 55: Com colisões: taxa de efetividade do método para emenda IEEE 802.11ac@ 20 MHz.



Figura 56: Com colisões: taxa de efetividade do método para emenda IEEE 802.11ac@40 MHz.



Figura 57: Com colisões: taxa de efetividade do método para emenda IEEE 802.11ac@ 80 MHz.

baixo. Por outro lado, quando as taxas de transmissão de 19,5 e 65 Mb/s são usadas para a subportadora de controle (Figuras 55(b) e 55(c)), o método obteve sempre uma taxa de efetividade de 100%.

Na largura de banda de 40 MHz da emenda IEEE 802.11ac, foram avaliadas as taxas de transmissão da porção de controle de 13,5, 40,5 e 135 Mb/s. Na Figura 56(a) o algoritmo classificou erroneamente perdas como sendo por SNR baixo para valores de SNR maiores que 4 dB. A razão da falha se deve ao mesmo motivo quando utilizado a largura de banda de 20 MHz, onde a porção de dados esporadicamente chega ao receptor sem corrupções para esta faixa de valores de SNR. Para as demais taxas de transmissão da porção de controle, apresentadas nas Figuras 56(b) e 56(c), o método obteve sempre a mais alta taxa de efetividade.

Para a próxima largura de banda, de 80 MHz, da emenda IEEE 802.11ac, foram avaliadas as taxas de transmissão da porção de controle de 29,3, 175,5 e 292,5 Mb/s. Mantendo as características das taxas mais baixas previamente avaliadas, na Figura 57(a) o algoritmo classificou erroneamente perdas como sendo por SNR baixo para valores de SNR maiores que 1 dB, onde a taxa de transmissão para dados e controle é de 29,3 Mb/s. Nas taxas de transmissão da porção de controle de 175,5 e 292,5 Mb/s, apresentadas nas

Figuras 57(b) e 57(c), o método obteve altas taxas de efetividade, independente da taxa de dados utilizada.

### B.3 Cenário com colisão com pacote colidente com potência mais baixa

Para obtenção de todas as taxas de transmissão da emenda IEEE 802.11n, os testes foram efetuados com as larguras de banda de 20 e 40 MHz, conforme as Figuras 58-61. A Figura 58(a) mostra a taxa de entrega de pacotes de dados, representada no eixo vertical, como função do SNR do canal. É possível identificar que a taxa de entrega de pacotes de dados se manteve em 0% na maioria das taxas de dados e SNR avaliados, com exceção do intervalo entre 5 e 8 dB de SNR. Ao lado, na Figura 58(b), há a taxa de entrega de bits de controle, onde há a combinação das taxas utilizadas para as subportadoras de controle e de dados. Dependendo do SNR e da taxa de transmissão de porção de controle, é possível identificar que a porção é entregue com sucesso.

Na Figura 59(a), utilizando a emenda IEEE 802.11n porém com a largura de banda de 40 MHz, o comportamento relacionado a taxa de entrega de pacotes de dados foi semelhante ao com a largura de banda de 20 MHz. O mesmo ocorre comparando a taxa de entrega de bits de controle com as larguras de banda de 20 e 40 MHz, apresentado na Figura 59(b), onde os comportamentos são similares.



Figura 58: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11n @ 20 MHz.

Acerca da emenda IEEE 802.11n, a taxa de efetividade para o cenário com colisões



Figura 59: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11n @ 40 MHz.

quando a potência do pacote colidente é mais baixa que a do pacote principal é apresentada nas Figuras 60 e 61. Na Figura 60 são exibidos os dados apenas para os casos em que a taxa de transmissão da porção de controle é 6,5, 19,5 ou 52 Mb/s. Já na Figura 61 as taxas de transmissão da porção de controle são apresentadas em 27, 40,5 ou 108 Mb/s. Em cada gráfico, o eixo vertical mostra a taxa de efetividade do método como uma função do SNR do canal. Os padrões das barras associam esses valores de SNR às taxas de transmissão usadas para a porção de dados.

A menor taxa de transmissão avaliada para as porções de dados e controle, de 6,5 Mb/s, apresentada na Figura 60(a), o algoritmo classificou erroneamente para SNR acima de 5 dB. Nesses cenários, devido ao uso de uma taxa bastante robusta, algumas vezes o receptor foi capaz de recuperar a porção de controle, classificando de maneira equivocada as perdas como sendo SNR baixo. Com o uso de taxa de bits de controle de 52 Mb/s, a taxa de efetividade do método é de 100%, conforme a Figura 60(c).

Com a largura de banda de 40 MHz na emenda IEEE 802.11n, com todas as taxas de transmissão da porção de controle avaliadas, o método obteve resultados similares aos da utilização da largura de banda de 20 MHz. Com a taxa de bits de controle em 27 Mb/s, apresentada na Figura 61(a), à medida que canais com alto SNR são utilizados a taxa de efetividade reduz. Já ao utilizar a taxa de bits de controle de 108 Mb/s, a taxa de efetividade do método é de 100%, conforme a Figura 61(c).

Enfim, foram avaliadas todas as taxas de transmissão da emenda IEEE 802.11ac. Para



Figura 60: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de efetividade do método para emenda IEEE 802.11n @ 20 MHz.



Figura 61: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de efetividade do método para emenda IEEE 802.11n @ 40 MHz.

isso, os testes foram efetuados com as larguras de banda de 20, 40 e 80 MHz, conforme as Figuras 62-67.

A Figura 62(a) mostra a taxa de entrega de pacotes de dados, representada no eixo vertical, como função do SNR do canal. É possível identificar que a taxa de entrega de pacotes de dados se manteve em 0% na maioria das taxas de dados e SNR avaliados, com exceção do intervalo entre 6 e 8 dB de SNR. Ao lado, na Figura 62(b), há a taxa de entrega de bits de controle, onde há a combinação das taxas utilizadas para as subportadoras de controle e de dados. Dependendo do SNR e da taxa de transmissão de porção de controle, é possível identificar que a porção é entregue com sucesso. A razão para que a porção de controle seja entregue com sucesso se deve a robustez da mesma.

Mesmo aumentando a largura de banda e, consequentemente, a taxa de transmissão, a taxa de entrega de pacotes de dados manteve um comportamento semelhante a avaliação feita com a largura de banda de 20 MHz. Isso pode ser visualizado nas Figuras 63(a) e 64(a), com larguras de banda de 40 e 80 MHz, respectivamente. Assim como nas emendas IEEE 802.11g e IEEE 802.11n, a porção de controle possui maior robustez que os dados para todos os valores. A robustez é visualizada nas Figuras 63(b) e 64(b), onde algumas vezes o receptor foi capaz de recuperar a porção de controle, classificando de maneira equivocada as perdas como sendo por SNR baixo.



Figura 62: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 20 MHz.

Com relação à emenda IEEE 802.11ac, a taxa de efetividade para o cenário com colisões é apresentada nas Figuras 65, 66 e 67. Na Figura 65 são exibidos os dados apenas para os casos em que a taxa de transmissão da porção de controle é 6,5, 19,5 ou 65 Mb/s.



Figura 63: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 40 MHz.



Figura 64: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de entrega de pacotes de dados e bits de controle para emenda IEEE 802.11ac @ 80 MHz.

Já na Figura 66 as taxas de transmissão da porção de controle são apresentadas em 13,5, 40,5 ou 135 Mb/s. A Figura 67 apresenta as taxas de transmissão da porção de controle de 29,3, 175,5 ou 292,5 Mb/s. Em cada gráfico, o eixo vertical mostra a taxa de efetividade do método como uma função do SNR do canal. Os padrões das barras associam esses valores de SNR às taxas de transmissão usadas para a porção de dados.

Na taxa de transmissão de 6,5 Mb/s para dados e controle, apresentada na Figura 65(a), o algoritmo classificou corretamente os tipos de perdas na maioria dos casos. As exceções ocorreram em canais com alto SNR. Nesses cenários, devido ao uso de



Figura 65: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de efetividade do método para emenda IEEE 802.11ac @ 20 MHz.



Figura 66: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de efetividade do método para emenda IEEE 802.11ac @ 40 MHz.



Figura 67: Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de efetividade do método para emenda IEEE 802.11ac @ 80 MHz.

uma taxa bastante robusta, algumas vezes o receptor foi capaz de recuperar a porção de controle, classificando de maneira equivocada as perdas como sendo SNR baixo. Nesta mesma faixa onde houve falha na classificação, ao utilizar taxas de bits de controle maiores a taxa de efetividade se manteve em 100%. Isso é apresentado na Figura 65(c).

Com a largura de banda de 40 MHz da emenda IEEE 802.11ac, foram avaliadas as taxas de transmissão da porção de controle de 13,5, 40,5 e 135 Mb/s. Na Figura 66(a) o algoritmo classificou erroneamente perdas como sendo por SNR baixo para valores de SNR maiores que 4 dB. A razão da falha se deve ao mesmo motivo quando utilizado a largura de banda de 20 MHz, onde a porção de dados chega ao receptor sem corrupções para esta faixa de valores de SNR. Para a maior taxa de transmissão avaliada nesta largura de banda, apresentada na Figura 66(c), o método obteve sempre a mais alta taxa de efetividade.

Já utilizando a largura de banda de 80 MHz, foram avaliadas as taxas de transmissão da porção de controle de 29,3, 175,5 e 292,5 Mb/s. Mantendo as características das taxas mais baixas previamente avaliadas, na Figura 67(a) o algoritmo classificou erroneamente perdas como sendo por SNR baixo para maioria dos valores de SNR avaliados, onde a taxa de transmissão para dados e controle é de 29,3 Mb/s. Nas taxas de transmissão da porção de controle de 175,5 e 292,5 Mb/s, apresentadas nas Figuras 67(b) e 67(c), o método obteve altas taxas de efetividade, independente da taxa de dados utilizada.