Um método para o diagnóstico do tipo de perda de pacotes em redes sem fio IEEE 802.11

Allysson Chagas Carapeços[1], **Diego Gimenez Passos**[1]

[1]Instituto de Computação – Universidade Federal Fluminense (UFF)
Av. Gal. Milton Tavares de Souza, São Domingos – 24.210-346 – Niterói – RJ – Brazil

allyssoncc@id.uff.br, dpassos@ic.uff.br

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 makes it possible to optimize the use of the medium. Thus, this work proposes a new method for identifying the type of packet losses 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. Our evaluation shows that the proposed method has good accuracy in identifying the type of packet loss, especially for higher data rates.*

Resumo. *Perdas de pacotes são uma ocorrência comum nas redes sem fio. Estas perdas podem ser ocasionadas por colisões ou simplesmente pelo baixo SNR 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. Assim, este trabalho propõe 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.*

1. Introdução

Nos últimos anos, o crescimento no número de dispositivos aptos a utilizar redes sem fio tem crescido. 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 delas utiliza as redes sem fio locais.

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*). No CSMA/CA, um nó só transmite quando julga que o canal está livre. Mesmo assim, o padrão supracitado é susceptível 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 et al. 2016]. No entanto, colisões não são a única possível razão para perda de pacotes. Pacotes podem ser perdidos também por conta de um baixo SNR 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 [Vutukuru et al. 2009] e [Sen 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. 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.

Neste sentido, 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 introduz bits de controle que são multiplexados juntamente aos bits de dados do pacote original. Como as subportadoras no OFDM pode ser moduladas e codificadas independentemente, os bits de controle são transmitidos utilizando combinações mais robustas de modulação e codificação. Conforme detalhado no decorrer do artigo, 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 nesse trabalho mostra que o método é capaz de apresentar boa acurácia na distinção da causa das perdas de pacotes.

Este artigo está dividido da seguinte maneira. Na Seção 2, são apresentadas as principais características dos trabalhos relacionados encontrados na literatura. Em seguida, na Seção 3, é feita uma fundamentação teórica. Na Seção 4, é apresentada a proposta da abordagem para identificar a causa da perda de pacotes. Posteriormente, na Seção 5, são apresentadas as metodologias para avaliação e os resultados obtidos. Ao final, na Seção 6, são apresentadas as considerações finais.

2. Trabalhos relacionados

Com o objetivo de distinguir as causas de perdas de pacotes em redes sem fio, algumas abordagens foram apresentadas na literatura nos últimos anos. Essas abordagens utilizam

vários tipos de técnicas diferentes para classificar a causa das perdas de pacotes e muitas vezes incluem também propostas de como tratá-las.

O SoftRate [Vutukuru et al. 2009] e o AccuRate [Sen et al. 2010] são mecanismos de adaptação automática da taxa de transmissão que utilizam a diferenciação da causa de perda de pacotes para tomar decisões distintas. Apesar de possuírem o mesmo propósito, suas abordagens são diferentes. Enquanto o SoftRate utiliza informações relacionadas ao BER, o AccuRate analisa a dispersão entre as posições dos símbolos transmitidos e recebidos no diagrama de constelação da modulação. No SoftRate, quando o pacote é recebido com sucesso, o receptor envia um ACK. Por outro lado, se o pacote é recebido com erros, tendo o preâmbulo ou postâmbulo íntegro, o receptor reponde com um NACK informando a BER do quadro. Neste caso, o SoftRate assume que a causa da perda foi SNR baixo, acionando um algoritmo de adaptação da taxa de transmissão altamente sensível a variações rápidas do canal.

Em [Aman and Sikdar 2012], apresenta-se um mecanismo baseado em EVM (*Error Vector Magnitude*) e árvores de classificação e regressão (CART). Um vetor de erro é a diferença entre os valores complexos da tensão de um símbolo ideal e do sinal efetivamente recebido. A proposta tenta encontrar um limiar para o EVM que permita a distinção entre SNR baixo e colisão. O limiar é encontrado por meio de CART através de uma fase preliminar de treinamento. Os autores apresentam resultados de simulações em Matlab que mostram uma precisão na detecção do tipo de perda entre 73% e 97%, dependendo do cenário proposto. No entanto, a necessidade de um treinamento prévio é um problema em ambientes dinâmicos com alta mobilidade.

Já o PLFC (*Packet-Level Failure Classifier*) [Zhu and Sun 2015] utiliza o RSSI (*Received Signal Strength Indicator*) e o LQI (*Link Quality Indicator*) dos pacotes recebidos como atributos para classificar o tipo de perda. A proposta necessita de calibração de dois limiares, α e β, para as métricas RSSI e LQI, respectivamente. Ao medir taxa de classificação e atraso, o PLFC obteve 93,1% de acerto na classificação com 23 ms de atraso médio. Este atraso ocorre pois o método avalia o RSSI e LQI ao longo de todo o período de recepção do quadro, aplicando regras para a classificação de cada trecho. Ao final, as classificações dos trechos são usadas para determinar o tipo de perda. Usando esse método, os autores propõem um mecanismo de retransmissão. Na avaliação dos autores, os dois mecanismos combinados reduziram a taxa de retransmissão com o PLFC de 50% a 70%, dependendo do cenário, atenuando o desperdício de energia.

Uma proposta voltada a redes de sensores é apresentada em [Whitehouse et al. 2005]. As colisões são categorizadas em *stronger-first*, quando o rádio sincroniza com o pacote de sinal mais forte primeiro, e *stronger-last*, quando o rádio sincroniza com o pacote de sinal mais fraco primeiro, mas a recepção falha, pois o pacote de sinal mais forte captura e corrompe o sinal do primeiro pacote. A proposta consiste em procurar continuamente um novo preâmbulo, mesmo durante a recepção de um pacote, e ressincronizar com o novo pacote no cenário *stronger-last*. Após a finalização da transmissão do pacote de sinal mais forte, é possível que o pacote corrompido — o de sinal mais fraco — seja recuperado desde que as informações do cabeçalho tenham sido recebidas corretamente. 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.

Em [Wu et al. 2019], foi proposta uma abordagem denominada CRM-GD (*Collision Recognition Mechanism Based on Generating Domains*). Os autores argumentam 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. Em particular, em caso de colisão, os erros de símbolo são distribuídos, em geral, no final de um pacote corrompido. O CRM-GD é baseado em aprendizado de máquina. Ele insere blocos redundantes em um quadro de dados, conhecidos como GD (*Generating Domains*). Tais blocos podem ser aplicados para reconhecer efetivamente os pacotes corrompidos quando a causa for o efeito de terminal oculto. Resultados experimentais indicaram que o CRM-GD alcança precisão de reconhecimento entre 92,25% e 99,05%. Apesar dos bons resultados, o método requer calibração, o que o limita em cenários com modificações constantes.

O CSMA/CN (*Collision Notification*) [Sen et al. 2012] requer que o transmissor possua dois rádios operando no mesmo canal: um para transmissão e outro para a escuta de notificações. A colisão é identificada pelo receptor por meio de *hints* do SoftPHY. Quando há colisão, o receptor notifica imediatamente o transmissor que, por sua vez, interrompe sua transmissão, liberando o canal para outros transmissores nas proximidades. Neste esquema, há limitações relacionadas à tecnologia MIMO e ao cancelamento de ruído — necessário para o funcionamento do rádio de notificações —, que nem sempre funciona, podendo prejudicar o desempenho e reduzir a eficácia do método.

O PCC (*Packet Corruption Classifier*) [Zeng and Kumar 2008] analisa informações obtidas a partir do fluxo de entrada e saída do *slicer*. O *slicer* é um elemento do receptor que quantifica a amostra de sinal na forma de números complexos. Na avaliação conduzida pelos autores, a proposta obteve uma taxa de falha — perdas classificadas equivocadamente como sendo por baixo SNR — de 6% e taxa de falsos positivos — perdas erroneamente classificadas como colisões — de 5%, mesmo no cenário mais difícil avaliado.

Em [Peng et al. 2007], é apresentada uma proposta de protocolo MAC 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. Neste sentido, o protocolo proposto assume que cada nó possui habilidade para simultaneamente transmitir em dois canais, dados e controle.

O 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 de quadros em redes IEEE 802.11 [Rayanchu et al. 2008]. 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 de acordo com a classificação, possibilitando melhorias significativas na taxa de transmissão e capacidade para cenários de alto uso de mobilidade. 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). De acordo com observações feitas pelos autores, as métricas SER e EPS em conjunto possibilitariam distinguir a causa da perda de pacote, pois pacotes com erro por colisão possuiriam SER e EPS mais altas. É possível verificar que, para análise empírica, é obrigatório o *feedback* do receptor para o transmissor. Isso só é possível se o receptor conseguir decodificar corretamente o endereço MAC do transmissor do pacote com erro.

O CD-ET [Ji-Hoon Yun and Seung-Woo Seo 2006] utiliza a duração de energia de RF (Radiofrequência). Quando ocorre uma colisão entre duas estações, o AP (*Access Point*) vê a energia de RF mesclada causada pelos quadros colididos. Se os quadros transmitidos tiverem durações diferentes, a duração da energia de RF mesclada será maior que as durações dos quadros originais, exceto, talvez, para o quadro mais longo. Com base nisso, se as estações puderem conhecer a duração da energia de RF mesclada, poderão compará-la às durações de suas próprias transmissões. No entanto, as colisões são detectadas com algum atraso, o que resulta em melhoria sub-ótima do desempenho.

Em resumo, as propostas existentes possuem algumas limitações. Os métodos propostos em [Aman and Sikdar 2012], [Wu et al. 2019] e [Zhu and Sun 2015] exigem treinamento e calibração, o que é problemático em ambientes dinâmicos e com alta mobilidade. O método apresentado em [Sen et al. 2012] não pode ser usado em ambientes que utilizam a tecnologia MIMO. Já em [Whitehouse et al. 2005], a capacidade de detecção de colisões é reduzida à medida que cai a diferença entre os inícios das transmissões. Também há métodos que exigem a comparação entre o pacote enviado e recebido, o que adiciona atraso e *overhead*.

3. Fundamentação teórica

Para possibilitar melhor entendimento 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.

Uma portadora é uma onda eletromagnética 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 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. Números fracionários expressam qual a parte da mensagem redundante é realmente significava. Por exemplo, uma codificação com taxa de 2/3 produzirá a cada 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]. 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. Ele divide o canal em subcanais independentes, utilizando múltiplas sub-

portadoras 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.

4. Proposta

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.

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.

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%

Repare que 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.

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. 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 baixo SNR. Por outro lado, se houver perda por colisão, haverá uma alta probabili-

dade 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. A Seção 5 apresenta dados empíricos que permitem uma seleção adequada.

5. Avaliação de desempenho

Nessa seção, apresentamos resultados de simulação 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.

Para os propósitos dessa avaliação, foi utilizado um simulador personalizado escrito em Python 2. O simulador modela um sistema composto por um transmissor e um receptor 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 simulador um sistema de rádio IEEE 802.11g. Isso inclui as combinações de modulação e codificação utilizadas que correspondem àquelas utilizadas nas várias taxas de transmissão previstas no IEEE 802.11g.

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. A principal métrica de desempenho avaliada é a taxa de efetividade do método. Considera-se que a falha 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 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 um canal IEEE 802.11g tradicional — 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. Com isso, foi possível chegar ao mapeamento apresentado na Tabela 1, onde é possível identificar o valor de SNR a partir do qual cada taxa de transmissão deve ser usada.

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

Tabela 1. Identificação do valor de SNR a partir do qual cada taxa de transmissão resulta em uma probabilidade de entrega maior que 50%.

Taxa de dados	SNR	Taxa de entrega
6 Mbit/s	5 dB	54%
9 Mbit/s	8 dB	88%
12 Mbit/s	9 dB	92%
18 Mbit/s	10 dB	61%
24 Mbit/s	14 dB	62%
36 Mbit/s	17 dB	67%
48 Mbit/s	23 dB	91%
54 Mbit/s	24 dB	89%

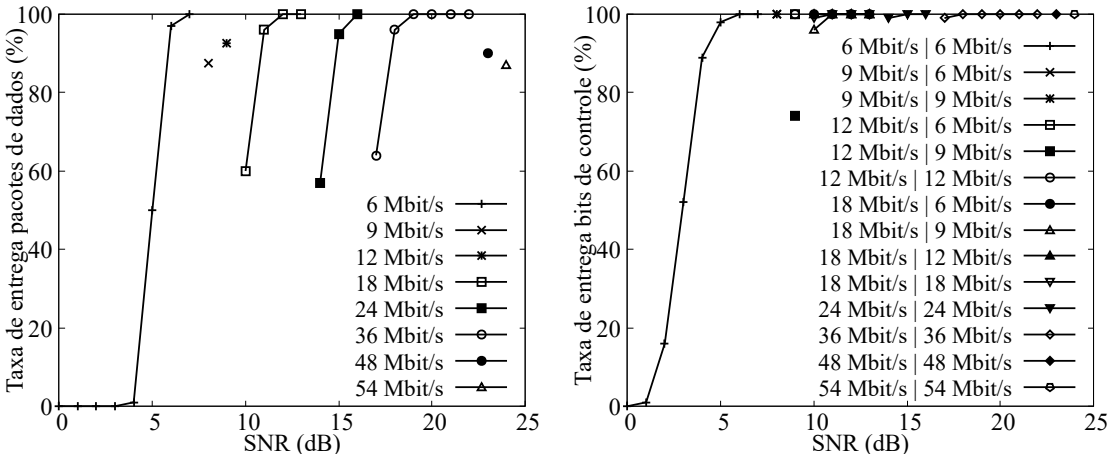
simulações com o método proposto utilizando-se vários valores de SNR. As taxas utilizadas para a subportadora de controle foram variadas entre todas as taxas disponíveis no IEEE 802.11g que resultariam em uma transmissão mais robusta que a da porção de dados. Essas simulações foram divididas em três 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.

5.1. Cenário sem colisão

Os resultados do primeiro cenário são apresentados nas Figuras 1 e 2. A Figura 1(a) mostra 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 a Figura 1(b) mostra a taxa de entrega de bits de controle. 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 às taxas mais baixas para a porção de controle.

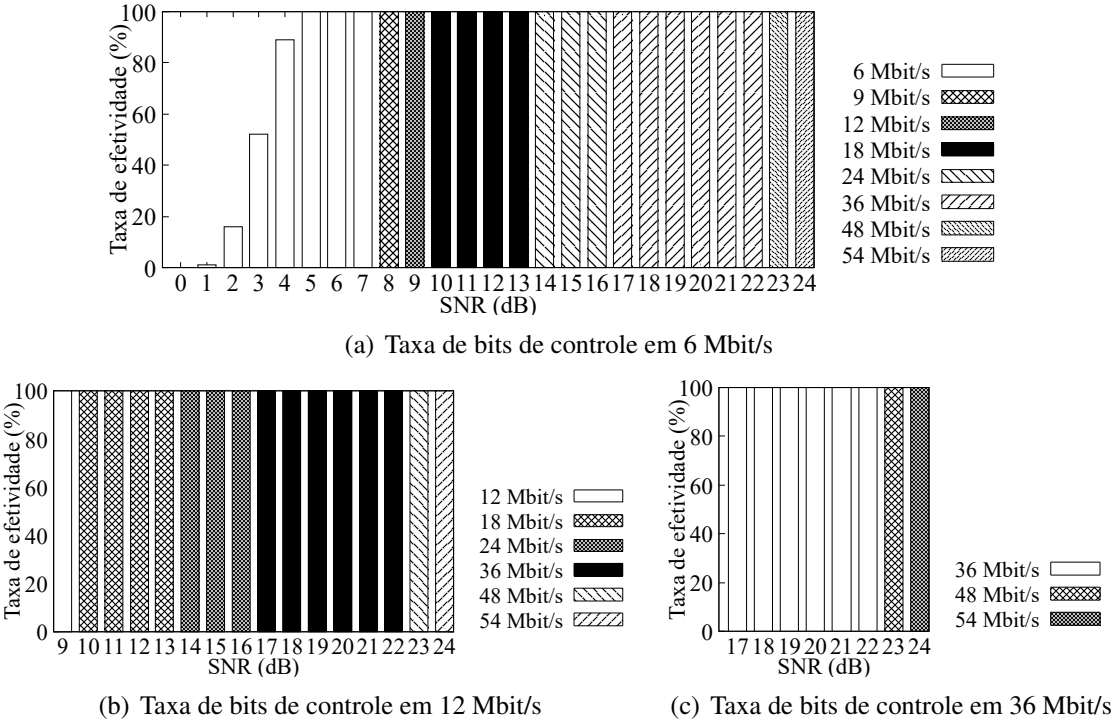
A taxa de efetividade para esse cenário é apresentada na Figura 2. Devido às restrições de espaço, a Figura exibe os dados apenas para os casos em que a taxa de transmissão da porção de controle é 6, 12 ou 36 Mbit/s. Em cada gráfico, o eixo vertical mostra a taxa de efetividade do método como uma função 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 Mbit/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 1(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 Mbits/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 Mbits/s são usadas para a subportadora de controle (Figuras 2(b) e 2(c)), o método



(a) Taxa de entrega de pacotes de dados (b) Taxa de entrega de bits de controle

Figura 1. Sem colisões: taxa de entrega de pacotes de dados e bits de controle



(a) Taxa de bits de controle em 6 Mbit/s

(b) Taxa de bits de controle em 12 Mbit/s (c) Taxa de bits de controle em 36 Mbit/s

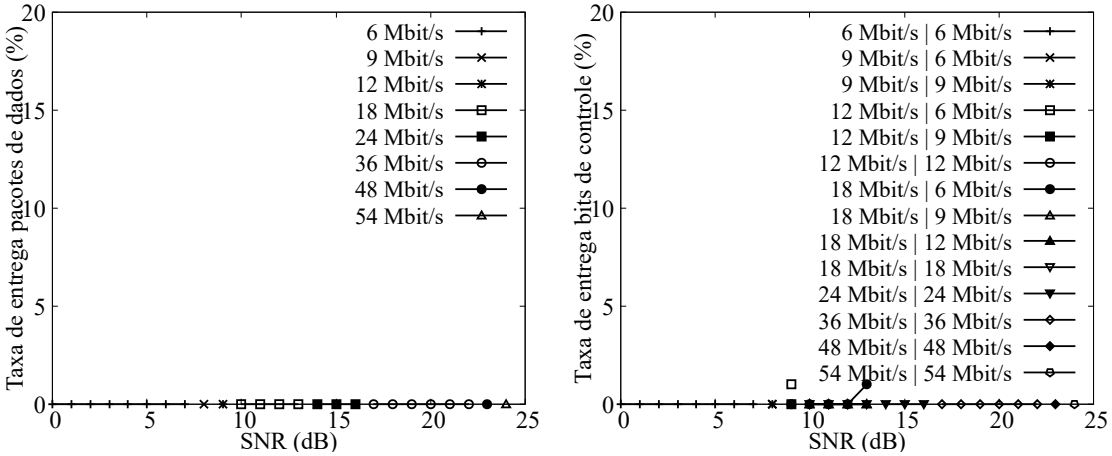
Figura 2. Sem colisões: taxa de efetividade do método

obteve sempre uma taxa de efetividade de 100%.

5.2. 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.Na Figura 3(a), é possível verificar que a taxa de entrega de pacotes de dados se mantém em 0%, independente da taxa de transmissão ou SNR. Na Figura 3(b), um comportamento semelhante é verificado para a porção de controle, embora, nesse caso, algumas vezes não houve corrupção dos bits de controle.

As Figuras 4(a), 4(b) e 4(c) mostram a taxa de efetividade da proposta para 6, 12



(a) Taxa de entrega de pacotes de dados (b) Taxa de entrega de bits de controle

Figura 3. Com colisões: taxa de entrega de pacotes de dados e bits de controle

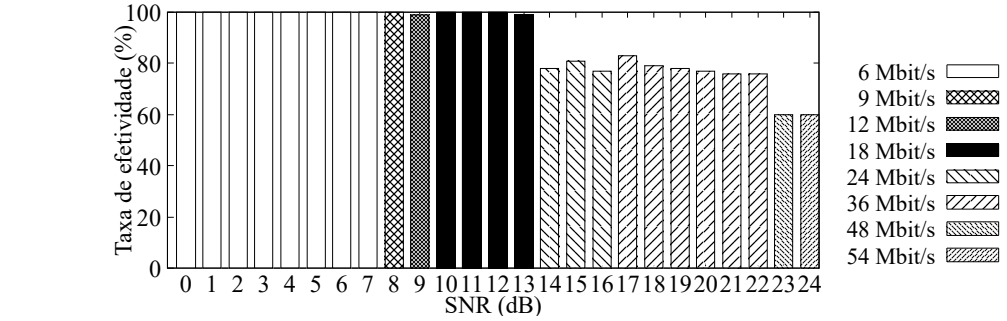
e 36 Mbit/s, respectivamente. Assim como no caso anterior, nesse cenário o método proposto classifica de maneira correta a causa na maioria dos casos. As exceções ocorreram quando a taxa de 6 Mbit/s foi usada para a porção de controle em canais com alto SNR. Nesses cenários, devido ao uso de uma taxa 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 receptor erroneamente classificou as perdas das porções de dados como sendo devidas a baixo SNR. 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.

5.3. Cenário com colisão com pacote colidente com potência mais baixa

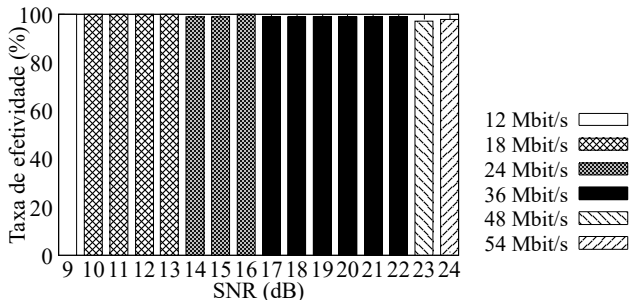
No cenário anterior, avaliou-se o caso da colisão entre pacotes que chegam ao receptor com exatamente a mesma potência. Na prática, devido a diversos fatores, o mais comum é que o sinal de um dos pacotes chegue ao receptor com uma potência mais alta. Conforme os resultados anteriores mostram, quando 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.

Nas Figuras 5(a) e 5(b), são apresentados os resultados obtidos nesse cenário referentes às taxas de entrega das porções de dados e controle, 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 5(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 5(b).

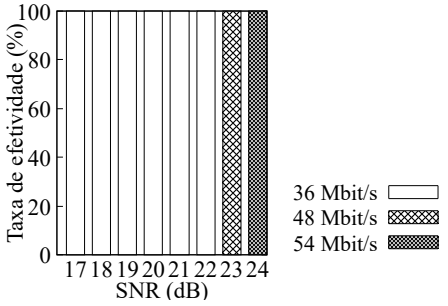
A Figura 6 mostra a taxa de efetividade do método para esse cenário. Como esperado, esse cenário se mostra bem mais desafiador que os anteriores. O método proposto exibe falhas na classificação da causa da perda para várias combinações de SNR e taxa de transmissão da porção de controle. Em particular, nota-se que a taxa de 6 Mbit/s tem baixa efetividade para valores de SNR acima de 5 dB porque, a partir desse valor, ela



(a) Taxa de bits de controle em 6 Mbit/s

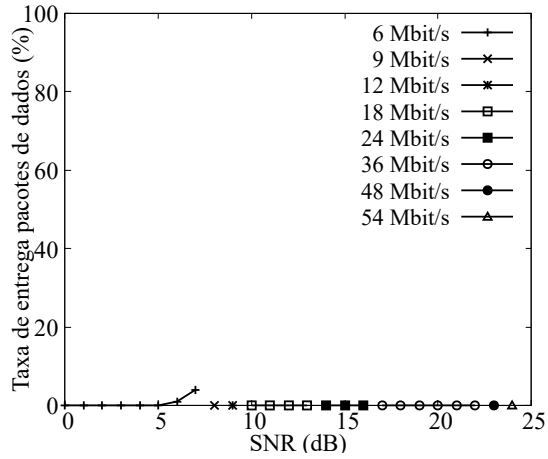


(b) Taxa de bits de controle em 12 Mbit/s

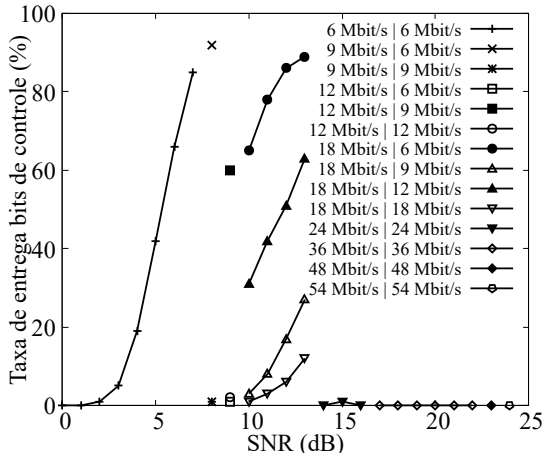


(c) Taxa de bits de controle em 36 Mbit/s

Figura 4. Com colisões: taxa de efetividade do método



(a) Taxa de entrega de pacotes de dados



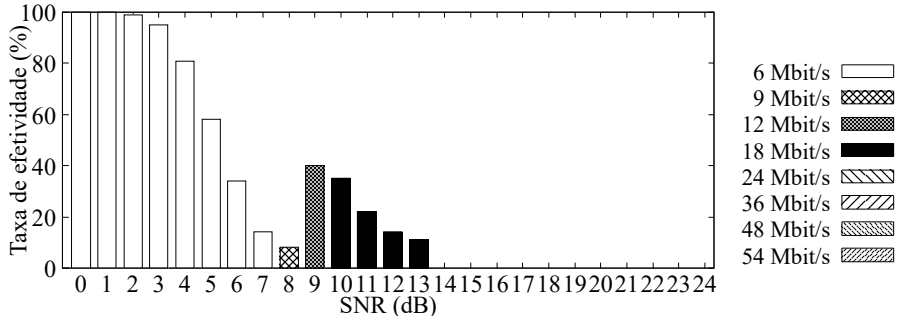
(b) Taxa de entrega de bits de controle

Figura 5. 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

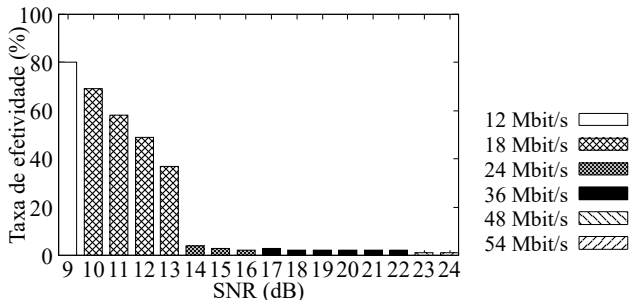
se torna robusta o suficiente para que frequentemente a porção de controle seja recebida corretamente. Por outro lado, a taxa de 36 Mbit/s resultou em 100% de efetividade para todos os valores de SNR avaliados.

5.4. Melhor relação entre taxa de transmissão de pacotes de dados e bits de controle

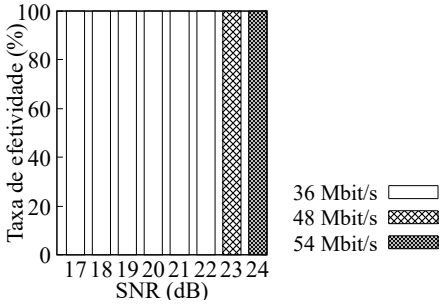
Com base nos cenários apresentados, foi identificada a taxa de transmissão ideal para a porção de controle associada à cada taxa usada para a porção de dados. O processo de



(a) Taxa de bits de controle em 6 Mbit/s



(b) Taxa de bits de controle em 12 Mbit/s



(c) Taxa de bits de controle em 36 Mbit/s

Figura 6. Com colisões quando a potência do pacote colidente é mais baixa que a do pacote principal: taxa de efetividade do método

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 2 mostra os resultados. 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. 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 2. Melhores taxas para a porção de controle para cada taxa de dados.

Taxa da porção de dados (Mbit/s)	6	9	12	18	24	36	48	54
Taxa da porção de controle (Mbit/s)	6	9	9	18	24	36	48	54

Utilizando esse mapeamento, a Figura 7 resume a taxa de efetividade do método proposto nos três cenários avaliados. 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 enlaces 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 Mbit/s) de efetividade mesmo nesse cenário.

6. Conclusão

Neste artigo, 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

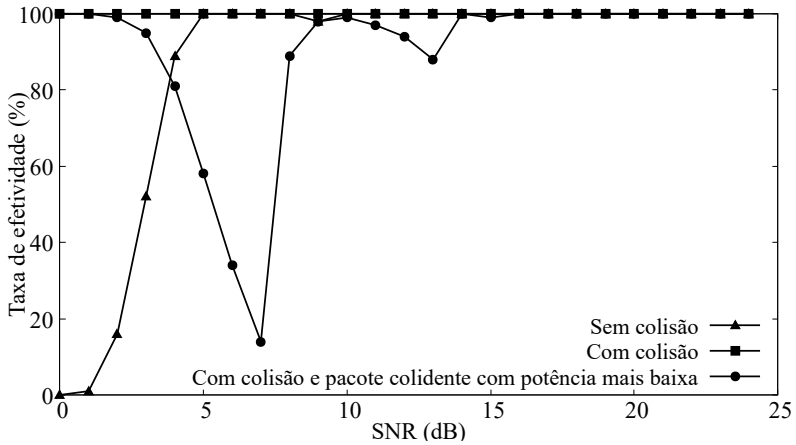


Figura 7. Taxa de efetividade utilizando seleção ideal da taxa de bits de controle para cada taxa de pacotes de dados

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 mais robusta que a usada para 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 com e sem colisão.

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 desta aplicação, é possível explorar melhorias no método. A primeira opção é duplicar a informação de bits de controle. Com a duplicação, a porção de controle se tornaria mais robusta, o que pode ser benéfico para enlaces de baixo SNR. Por fim, também pretendemos 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. and Sikdar, B. (2012). Distinguishing between channel errors and collisions in ieee 802.11. In *2012 46th Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6.

Bulhões, R. P., Passos, D., and Albuquerque, C. V. N. (2016). Collision probability estimation in wireless networks. In *2016 8th IEEE Latin-American Conference on Communications (LATINCOM)*, pages 1–6.

Cisco (2020). Cisco annual internet report (2018–2023) white paper.

IEEE (2003). Ieee 802.11g-2003 - 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 (2021). Ieee 802.11ax-2021 – ieee approved draft 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.

Ji-Hoon Yun and Seung-Woo Seo (2006). Collision detection based on re energy duration in ieee 802.11 wireless lan. In *2006 1st International Conference on Communication Systems Software Middleware*, pages 1–6.

JuniperResearch (2020). Iot the internet of transformation 2020.

Peng, J., Cheng, L., and Sikdar, B. (2007). A wireless mac protocol with collision detection. *IEEE Transactions on Mobile Computing*, 6(12):1357–1369.

Rayanchu, S., Mishra, A., Agrawal, D., Saha, S., and Banerjee, S. (2008). Diagnosing wireless packet losses in 802.11: Separating collision from weak signal. In *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, pages 735–743.

Sen, S., Roy Choudhury, R., and Nelakuditi, S. (2012). Csma/cn: Carrier sense multiple access with collision notification. *IEEE/ACM Transactions on Networking*, 20(2):544–556.

Sen, S., Santhapuri, N., Choudhury, R. R., and Nelakuditi, S. (2010). 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.

Vutukuru, M., Balakrishnan, H., and Jamieson, K. (2009). Cross-layer wireless bit rate adaptation. *SIGCOMM Comput. Commun. Rev.*, 39(4):3–14.

Whitehouse, K., Woo, A., Jiang, F., Polastre, J., and Culler, D. (2005). Exploiting the capture effect for collision detection and recovery. In *The Second IEEE Workshop on Embedded Networked Sensors, 2005. EmNetS-II.*, pages 45–52.

Wu, M., Hu, X., Zhang, R., and Yang, L. (2019). Collision recognition in multihop ieee 802.15.4-compliant wireless sensor networks. *IEEE Internet of Things Journal*, 6(5):8542–8552.

Zeng, Z. and Kumar, P. R. (2008). Towards optimally exploiting physical layer information in ofdm wireless networks. In *Proceedings of the 4th Annual International Conference on Wireless Internet*, WICON '08, Brussels, BEL. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Zhu, Y. and Sun, Y. (2015). Packet-level failure classification by characterizing failure patterns in wireless sensor networks. In *2015 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6.