

# CSMA Adaptativo para Redes LoRa

Leandro Jez<sup>1</sup>, Vinicius Pozzobon Borin<sup>1</sup>, Ana Cristina Kochem Vendramin<sup>2</sup>,  
Mauro Fonseca<sup>1</sup> e Anelise Munaretto<sup>1</sup>

<sup>1</sup>Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial (CPGEI)  
Universidade Tecnológica Federal do Paraná (UTFPR)  
Av. Sete de Setembro, 3165 – 80230-901 – Curitiba – PR – Brazil

<sup>2</sup>Programa de Pós-Graduação em Computação Aplicada (PPGCA)  
Universidade Tecnológica Federal do Paraná (UTFPR)  
Av. Sete de Setembro, 3165 – 80230-901 – Curitiba – PR – Brazil

leandrojez@gmail.com, {criskochem,maurofonseca,anelise}@utfpr.edu.br

**Resumo.** *LoRaWAN é um protocolo de acesso ao meio baseado na camada física LoRa (Long Range). Esta tecnologia utiliza Aloha puro, tamanho variável de pacote e espalhamento espectral adaptativo. O objetivo desse artigo é propor uma mudança no protocolo de acesso ao meio, substituindo o padrão Aloha por um CSMA (Carrier Sense Multiple Access) Adaptativo. O impacto dessa alteração é analisado em termos da taxa de entrega de mensagens, taxa de vazão da rede e eficiência energética. Com o CSMA Adaptativo, pode-se notar uma melhora na vazão da rede e na eficiência energética, tornando o protocolo mais confiável e capaz de suportar implementações que necessitem dessas características. Redes LoRa têm como uma das suas maiores preocupações uma grande autonomia de seus nós, assim uma melhora na eficiência energética, em termos de quantidade de bits enviados por Joule de energia, torna o método de acesso ao meio proposto ainda mais atrativo. Pode-se notar com as simulações realizadas que com uma grande ocupação da rede o CSMA Adaptativo obteve uma eficiência energética 173% maior que o CSMA e 62% maior que o Aloha.*

## 1. Introdução

A implantação da Internet das Coisas (*Internet of Things* - IoT) em um âmbito urbano visa melhorar a qualidade de vida da população, quando aplicada à uma grande área de cobertura (*Smart Cities*). Um dos benefícios desta implantação é, por exemplo, melhorar a administração pública, aprimorando a infraestrutura de comunicação que fornece acesso unificado, simples e econômico a uma infinidade de serviços públicos, desencadeando sinergias potenciais e aumentando a transparência dos cidadãos [Zanella et al. 2014].

Para implementar uma infraestrutura de comunicação é necessário criar uma rede que comporte milhares de dispositivos se comunicando, muitas vezes simultaneamente, e que consiga manter uma taxa aceitável de entrega de pacotes que por ela transitam. Espera-se ainda que os dispositivos não estejam ligados à uma rede de energia, fazendo com que estes necessitem de baterias próprias para seu funcionamento. Quanto maior o tempo de vida útil de um dispositivo, mais econômica será a manutenção da rede.

Tendo isto em vista, um dos maiores desafios de implementação de IoT é decidir a tecnologia de comunicação sem fio mais apropriada. Nos últimos anos, tecnologias conhecidas como LPWAN (*Low Power Wide Area Networks*) têm sido empregadas

[Margelis et al. 2015]. Redes LPWAN, em especial redes LoRaWAN (*Long Range Wide Area Network*), trazem consigo diversas vantagens que são necessárias para criar uma infraestrutura de comunicação sem fio em ambientes como Cidades Inteligentes, tais como: (i) Cobertura: LoRaWAN utiliza um modelo de infraestrutura que se baseia em um *gateway* central para cobrir uma ampla área. Em ambientes urbanos, o *gateway* cobre um raio de dois quilômetros, podendo chegar a quinze quilômetros em áreas abertas; (ii) Escalabilidade: as redes são utilizadas nos mais diversos cenários. Por exemplo, sensores podem ser utilizados por pequenos agricultores para monitorar suas plantações ou por prefeituras para tomada de decisões nas gestões dos recursos públicos; (iii) Custo: baixo custo na implementação da rede, sendo necessário um *gateway*, os nós transmissores e uma conexão com um servidor. Os nós transmissores normalmente possuem uma grande autonomia, assim diminuindo o custo de manutenção da rede.

Com o diferencial de oferecer simultaneamente uma grande cobertura, alta duração de bateria e uma grande capacidade de conexões, LoRa atua muito bem como uma rede de sensoriamento, quando há necessidade de conectar-se diversos nós sensores espalhados em uma grande área. Neste tipo de rede não costuma ser necessária a transmissão de um grande volume de dados, o que elimina uma das desvantagens do LoRa. E ainda, o baixo custo de implementação da rede e a economia em manutenção, decorrente da alta duração de bateria, vem para complementar e incentivar ainda mais sua utilização.

Trabalhos científicos acerca das limitações da tecnologia LoRaWAN vêm sendo conduzidos. Usualmente, são analisados parâmetros de rede como escalabilidade, confiabilidade de entrega de pacotes e vazão da rede. Pouco se tem investigado sobre o impacto na modificação do método de acesso ao meio empregado pelo LoRaWAN.

O objetivo principal deste trabalho é investigar um método de acesso aplicado à tecnologia LoRaWAN. Neste caso, o CSMA com tempos de sensoriamento do meio (*Carrier Sense - CS*) adaptativo. Diferentes tempos de sensoriamento do meio são testados para verificar o comportamento da rede em relação às métricas de vazão, taxa de entrega de pacotes e eficiência energética.

Este artigo encontra-se organizado em seis seções: a seção 2 descreve o protocolo LoRaWAN e os detalhes da especificação padrão. A seção 3 apresenta a revisão dos trabalhos relacionados sobre LoRa/LoRaWAN. Na seção 4 é realizada uma análise das limitações do modelo LoRaWAN padrão e as propostas de melhoria. A seção 5 apresenta os resultados obtidos através de simulações. A conclusão e os trabalhos futuros são apresentados na seção 6.

## **2. LoRa**

LoRa é uma tecnologia de comunicação sem fio promovida pela LoRa Alliance. LoRa oferece soluções para problemas reais em comunicação sem fio, provendo longo alcance de transmissão, baixo consumo de energia e transmissão segura de dados.

Uma das características das redes LoRaWAN são as impossibilidades de comunicações dispositivo a dispositivo. As redes LoRaWAN são organizadas em uma topologia em estrela na qual os nós, dispositivos finais (por exemplo, sensores), transmitem pacotes a um *gateway* em um único salto, o qual repassa esses pacotes para um servidor [Semtech Corporation 2016]. Os *gateways* são conectados ao servidor de rede LoRa

através de uma conexão não LoRa (por exemplo, Ethernet). O servidor gerencia toda a rede, controlando dinamicamente seus parâmetros para adaptar o sistema às condições em constante mudança e estabelecendo conexões seguras. O servidor de rede garante a autenticidade de todos os sensores da rede e a integridade de todas as mensagens.

LoRa possui duas camadas distintas: uma camada física usando a técnica proprietária de modulação com espalhamento espectral derivada da tecnologia existente CSS (*Chirp Spread Spectrum*) e uma camada de acesso ao meio que utiliza o protocolo LoRaWAN. Essas camadas são detalhadas na próximas subseções.

## 2.1. Camada Física

Na modulação LoRa, a difusão do espectro é obtida gerando um sinal do tipo *chirp*, ou seja, um sinal que varia constantemente sua frequência. Uma vantagem desse método é que não existe diferença de tempo e frequência entre o transmissor e o receptor, reduzindo a complexidade no projeto do receptor [Augustin et al. 2016].

Um rádio LoRa tem quatro parâmetros de configuração principais: frequência da portadora, fator de espalhamento, largura de banda e taxa de codificação. A seleção desses parâmetros determina o consumo de energia, a faixa de transmissão e a resiliência da transmissão. A frequência da portadora é a frequência central utilizada para a banda de transmissão. A modulação LoRa tem um total de seis fatores de espalhamento (*Spreading Factor* - SF) ortogonais entre si, variando de SF7 a SF12. Quanto maior o fator de espalhamento usado, mais longe o sinal poderá viajar e ainda ser recebido sem erros pelo receptor. Cada aumento no SF reduz pela metade a taxa de transmissão e dobra a duração da transmissão, com isso aumentando também o consumo de energia. Pacotes que usam diferentes SF's são invisíveis uns para os outros e simplesmente aparecem como ruído. Isso se deve ao fato de diferentes SF's serem ortogonais entre si. Portanto, dois pacotes que chegam ao mesmo tempo no mesmo canal de recepção em diferentes fatores de espalhamento não irão colidir. No entanto, dois pacotes com o mesmo fator de espalhamento chegando ao mesmo tempo no mesmo canal podem resultar em uma colisão. A largura de banda corresponde à faixa de frequência ocupada pelo sinal modulado. Quanto mais alta for a largura de banda, maior será a taxa de dados. Porém, terá uma sensibilidade menor, devido à integração de ruído adicional. A taxa de codificação descreve a proporção entre os dados reais e os dados de correção de erros adicionados (*Forward Error Correction* - FEC) aos dados. Uma taxa de codificação mais alta não aumentará o alcance, mas tornará um enlace mais resiliente à interferência de pacotes [Semtech Corporation 2016].

Com a definição desses parâmetros, obtém-se a taxa de dados ( $R_b$ ) teórica através da Equação 1 [Semtech Corporation 2015].

$$R_b = SF * \frac{BW}{2^{SF}} * \frac{4}{4 + CR} \text{ bits/s}, \quad (1)$$

onde SF é o fator de espalhamento, BW é a largura de banda da modulação (Hz) e CR é a taxa de codificação, variando de (1..4). O CR é fixado em 4/5 para o protocolo LoRaWAN.

Nós de uma rede LoRa podem realizar otimizações adaptativas dos níveis de energia e taxas de dados. Por exemplo, um dispositivo final localizado próximo a um *gateway*

deve transmitir dados com um SF baixo, permitindo maiores taxas de dados. No entanto, um dispositivo final localizado a quilômetros de distância de um *gateway* precisa transmitir com um SF muito maior. Este SF mais alto fornece maior ganho de processamento e maior sensibilidade de recepção, porém com uma taxa de dados menor.

## 2.2. Camada de Acesso ao Meio

Na camada de acesso ao meio, o LoRaWAN define três tipos diferentes de arranjos: classe A, B e C. Somente a classe A obrigatoriamente deve estar implementada em todos os dispositivos finais. Dispositivos classe B precisam operar também como classe A e dispositivos classe C devem suportar todas as três classes. Por esse motivo, este artigo focará na classe A. Os dispositivos da classe A usam Aloha puro.

A recepção de pacotes é apenas permitida após uma transmissão bem-sucedida. Depois de cada transmissão, o dispositivo de classe A que originou a transmissão deve esperar duas janelas de recepção para receber novas transmissões. O valor recomendado para cada janela de recepção é de 1 e 2 segundos, respectivamente. Essas janelas são usadas para receber do servidor uma mensagem de reconhecimento da chegada do pacote ou mesmo alguns pacotes de dados. Uma transmissão *downlink* (ou seja, transmissão do servidor para o dispositivo final) deve passar por uma dessas janelas e nunca durante outro instante de tempo.

Algumas características importantes decorrentes do uso das janelas são: (i) caso o servidor tenha algum pacote para enviar a um nó, ele deve esperar até que uma das janelas se abra e jamais conseguirá se comunicar em outro momento; (ii) caso o nó receba uma mensagem na sua primeira janela de tempo ele não precisará abrir a segunda; (iii) os nós não podem enviar outros pacotes antes de receber qualquer resposta em uma de suas janelas ou antes dos dois tempos das janelas expirarem. Analisando essas características pode-se notar que não existem formas de uma aplicação acordar um dispositivo final. Então, a classe A não foi projetada para ser utilizada em uma rede de atuadores.

Dispositivos da Classe A utilizam o protocolo Aloha para transmitir pacotes, sendo este um protocolo simples de acesso ao meio para comunicações sem fio e comumente usado em IoT. Os dados são enviados sem agendamentos prévios ou tempos pré-determinados. O protocolo não analisa o meio e as colisões são tratadas com o uso de um tempo de *backoff* aleatório para a retransmissão de pacotes. A eficiência máxima teórica do Aloha é de 18%. Maiores detalhes sobre o método Aloha estão descritos em [Adelantado et al. 2017].

## 3. Revisão do estado da arte

As primeiras pesquisas publicadas sobre a tecnologia LoRa são datadas do ano de 2015. Essas pesquisas buscam avaliar a cobertura em redes que utilizavam LoRa.

Em [Petajajarvi et al. 2015] é utilizado um dispositivo final, fixado em um carro e em um barco, a fim de verificar a distância máxima de transmissão em meios terrestre e marítimo. Segundo o estudo, para um nó operando na banda ISM (*Industrial, Scientific, and Medical*) de 868 MHz usando 14 dBm de potência de transmissão e com um SF máximo, observa-se um alcance máximo de comunicação de mais de 15 km no solo e perto de 30 km na água.

Em [Mikhaylov et al. 2016] são verificadas as limitações das redes LoRa. Inicialmente, os autores analisam a taxa e o tempo de transmissão de dados para um dispositivo final. Após essa análise, estima-se o número de nós suportados por um *gateway* com base na sua distribuição espacial. Por fim, é apresentada uma discussão das aplicações que podem ser utilizadas em uma rede LoRa e suas limitações.

Alguns parâmetros definidos em uma implementação LoRa trazem consigo características únicas. É o caso do espalhamento espectral ortogonal que possibilita transmissões concorrentes não destrutivas. A análise dessa característica é um dos pontos presentes em [Bor et al. 2016]. Outra peculiaridade dos dispositivos finais é a presença de um detector de portadora diferente do usado pela maioria dos outros transceptores, por detectar o preâmbulo das mensagens e não a real ocupação de um canal. No artigo também é registrada a precisão de tais detectores de portadora.

Em [Bankov et al. 2016] buscam-se as limitações da tecnologia LoRa com foco na Taxa de Erro de Pacote e na Relação de Perda de Pacote. Para os testes é utilizada uma rede com três canais e seis taxas de dados. Os autores concluem que o limite das redes que podem ser criadas com LoRaWAN são equivalentes ao tráfego gerado por 500 nós enviando duas mensagens por dia.

Embora uma das principais vantagens de redes LPWAN seja a possibilidade de prover comunicação em grandes distâncias, na ordem de quilômetros, existem diversas aplicações IoT para ambientes fechados. Em [Neumann et al. 2016] é verificado como o LoRaWAN se comporta nesses cenários. Inicialmente, são apresentadas as limitações da rede em termos de periodicidade e tamanho dos dados de transmissões. Em seguida, são testadas as transmissões através de diversas salas do prédio considerado. Constata-se que os obstáculos não causam muito impacto nas transmissões dos dados.

O protocolo LoRaWAN não usa nativamente o protocolo IP (*Internet Protocol*), o que segundo [Weber et al. 2016] tornam mais difíceis as integrações em um ambiente IoT com diversas tecnologias. Os autores propõem uma integração do protocolo IPv6 e concluem que o uso deste com LoRaWAN é possível na comunicação fim-a-fim, possibilitando uma completa integração no ambiente IoT.

Em [Petrić et al. 2016] é apresentado um novo tipo de rede baseado na tecnologia LoRa, conhecida como LoRa FABIAN. Também é analisada a qualidade de serviço (*Quality of Service* - QoS) das redes.

Com o aumento na popularidade das redes LoRa, se faz necessária uma estratégia para mitigar a interferência entre redes vizinhas colocadas em uma localidade próxima [Voigt et al. 2016]. São utilizadas duas estratégias: antenas direcionais e múltiplos *gateways*. Através de simulações, comprova-se um ganho para ambas as estratégias, mas o uso de múltiplos *gateways* traz um ganho muito superior.

Em [de Carvalho Silva et al. 2017] é realizado um estudo de caso para a tecnologia LoRaWAN, fazendo comparações com outras redes LPWAN largamente empregadas. Segundo os autores, LoRaWAN têm várias vantagens sobre outras tecnologias LPWAN, incluindo: melhor tempo no ar, melhor duração da bateria, comunicação bidirecional e ilimitada, criptografia nativa dos pacotes sendo capaz de criar redes públicas e/ou privadas e taxa de dados adaptável permitindo maior escalabilidade da rede.

Redes sem fios, por utilizarem um meio comum e de fácil acesso a várias pessoas, são vulneráveis a diversos tipos diferentes de ataques. Tendo isso em vista, em [Aras et al. 2017] é analisada a vulnerabilidade das redes LoRa contra diferentes tipos de ataques. Os autores concluem que os dispositivos presentes no mercado, na época, são passíveis de diferentes ataques.

Para alcançar sempre a melhor eficiência em cada transmissão, a tecnologia LoRa traz uma grande diversidade de configurações para seus vários parâmetros. Mas, configurar os parâmetros de forma ideal é um desafio. Em [Bor and Roedig 2017] relata-se que existem 6720 possíveis configurações dentro dessa tecnologia. Os autores criam um regime de testes para determinar as configurações suficientes para um determinado cenário. Com isso, são fornecidos os primeiros passos na busca de um sistema automático de ótima qualidade para configurações em uma rede.

Mais atualmente, pesquisadores vêm demonstrando interesse em aprimorar a tecnologia LoRaWAN para ambientes de cidades inteligentes. Em [To and Duda 2018] é proposto o uso de CSMA como método de acesso ao meio e realizada uma comparação com o método de acesso padrão Aloha. Os parâmetros avaliados são: taxa de entrega de pacotes, taxa de colisão e consumo de energia em cada nó. Os resultados constataam que o CSMA atinge uma maior taxa de entrega do que o protocolo Aloha convencional.

Uma das grandes preocupações ao lidar com redes para IoT é a capacidade de escalonamento das redes. Vindo de uma necessidade de diversas aplicações comunicarem-se com múltiplos dispositivos finais, em [Georgiou and Raza 2017] e [Bor et al. 2016] verifica-se a capacidade de redes LoRa escalonarem.

Em uma análise inicial pode-se comparar a utilização de tempos diferentes de DIFS (*Distributed Inter Frame Spacing*) proposta nesse trabalho com a que é realizada no protocolo IEEE 802.11e [Mangold et al. 2002]. Porém, deve-se notar que o protocolo aqui proposto não tem a intenção de providenciar qualquer tipo de QoS na rede, diferente do que se busca com a implementação do 802.11e.

#### 4. LoRaWAN com CSMA Adaptativo

O protocolo CSMA no seu modo padrão exige que um nó que tenha um pacote para transmitir monitore o canal por um período de tempo chamado DIFS. Se durante o período de DIFS, o meio estiver desocupado, o nó está liberado para enviar sua mensagem. Entretanto, se durante a verificação for detectada a utilização do meio, o nó deve aguardar um tempo aleatório de *Backoff*. Após aguardar o tempo de *backoff*, o nó deve iniciar a verificação do meio novamente.

O CSMA Adaptativo proposto neste artigo utiliza um valor de DIFS adaptável. Quando os nós estiverem em redes desocupadas eles terão um comportamento mais semelhante ao Aloha padrão e quando eles sentirem que a rede está bastante ocupada seu comportamento se assemelherá ao CSMA padrão. O protocolo proposto iniciará com um menor tempo de DIFS esperando que a rede esteja livre e, caso encontre a rede ocupada, aumentará o DIFS até um valor máximo definido.

A Figura 1 apresenta o fluxograma de execução do CSMA Adaptativo. A adaptação do DIFS se deve aos seguintes motivos: (i) em cenários com menos de 1000 nós, um nó poucas vezes realizava *backoff* durante o sensoriamento do meio; (ii) a

implementação do protocolo CSMA traz um aumento no consumo energético se comparado ao protocolo padrão Aloha. Com o CSMA adaptativo, espera-se que ao diminuir o tempo DIFS diminua também o consumo da energia dos nós para se manter no estado de sensoriamento do meio. Uma diminuição de alguns milissegundos por transmissão pode parecer que não causará muito impacto visto que os dispositivos LoRaWAN são projetados para terem bateria por 8~10 anos. Porém, ao se acumularem pequenos ganhos, é esperado um grande impacto na duração da bateria dos dispositivos.

## 5. Resultados

Essa seção descreve as simulações conduzidas utilizando o simulador NS-3 [ns3 2021] para comparar o desempenho do CSMA Adaptativo com os protocolos Aloha e CSMA padrão. Os resultados apresentados são médias de 10 execuções. Utilizou-se o código da tecnologia LoRa/LoRaWAN Classe A implementado em [Magrin, D. and Capuzzo, M. and Romagnolo, S. and Luvisotto, M. 2018]. O módulo LoRaWAN adotado é capaz de operar com o módulo de energia padrão, sendo possível realizar medições de consumo e monitoramento de energia dos nós sensores. Parâmetros de energia, como corrente e tensão adotados, são extraídos do transceptor Semtech série SX1276 [Semtech Corporation 2019]. Os parâmetros utilizados para o cálculo energético são: tensão de 3,3 V, estado transmitindo 112 mA, estado recebendo 28 mA, estado desocupado 1,4 mA, estado dormindo 1,5  $\mu$ A. O módulo utilizado usa SF's aleatórios para cada mensagem transmitida, utilizando SF's entre 7-12.

Para avaliar o desempenho dos protocolos de acesso ao meio, três métricas de desempenho são consideradas:

- **Taxa de entrega:** representa o percentual de mensagens criadas ( $M_{criadas}$ ) que são entregues ( $M_{entregues}$ ) ao destino (ver equação 2).

$$Taxa\ de\ Entrega = \frac{M_{entregues}}{M_{criadas}} \quad (2)$$

- **Vazão da rede:** representa a quantidade de bits que estão sendo efetivamente enviados pela rede levando em conta o tamanho dos pacotes enviados ( $M_{tamanho}$ ). Como se deseja obter uma vazão em bits por segundo deve-se normalizar o valor pelo tempo de simulação ( $T_{simulação}$ ). A equação 3 demonstra como é realizado o cálculo da vazão da rede.

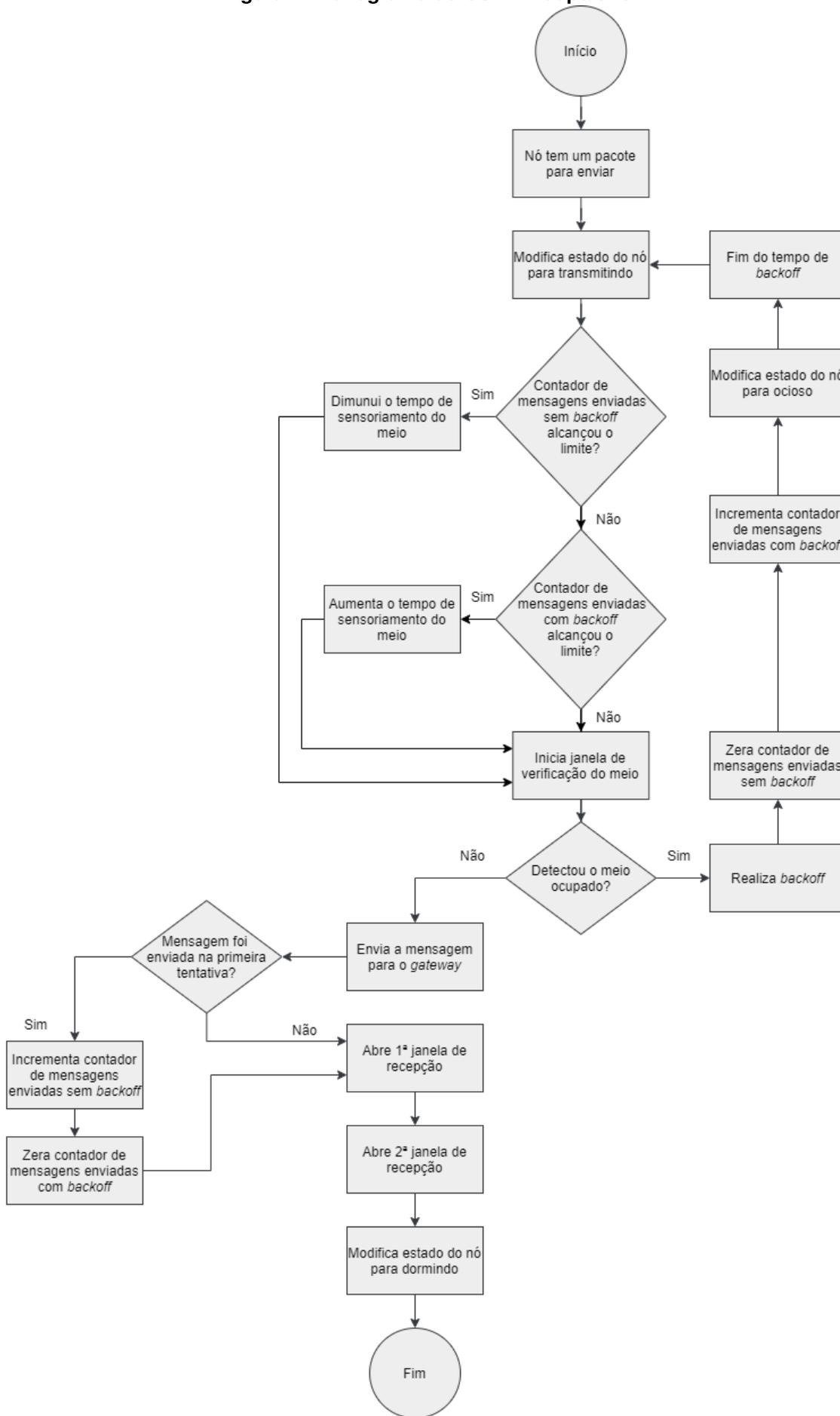
$$Vazão\ da\ rede = \frac{M_{entregues} * M_{tamanho}}{T_{simulação}} \quad (3)$$

- **Eficiência energética:** representa a quantidade de bits que é possível enviar pela rede gastando um Joule de energia. É analisada a quantidade total de energia gasta ( $E_{gasta}$ ) por cada nó da rede e a quantidade de bits que cada nó conseguiu enviar. A equação 4 demonstra como é realizado o cálculo da eficiência energética.

$$Eficiência\ energética = \frac{M_{entregues} * M_{tamanho}}{E_{gasta}} \quad (4)$$

Para uma comparação mais justa, os parâmetros adotados na simulação estão de acordo com os utilizados por [To and Duda 2018] e estes são apresentados na Tabela 1.

Figura 1. Fluxograma do CSMA Adaptativo



**Tabela 1. Parâmetros dos cenários de simulação**

Parâmetro	Valores
Número de nós	10 até 10,000
Tamanho dos pacotes	50 bytes
DIFS	10 ms (CSMA) Adaptativo com DIFS máximo de 10 ms (CSMA Adaptativo)
Tempo de simulação	20.000 s
Número de simulações	10
Limite dos contadores	33
Tempo entre mensagens	600 s
SF's utilizados (aleatório)	7 ao 12

### 5.1. Análise de Desempenho

Após vários cenários de teste notou-se que quanto menor a ocupação do canal, menos se faz necessário um prévio sensoriamento do meio. Porém, as vantagens de analisar previamente o meio aumenta muito a capacidade de acomodar um tráfego maior de mensagens na rede. Sendo assim, foi proposto um novo método de acesso ao meio, onde em redes pouco ocupadas se faria o menor sensoriamento prévio possível e, se observada uma maior ocupação da rede, aumentaria automaticamente o tempo de sensoriamento.

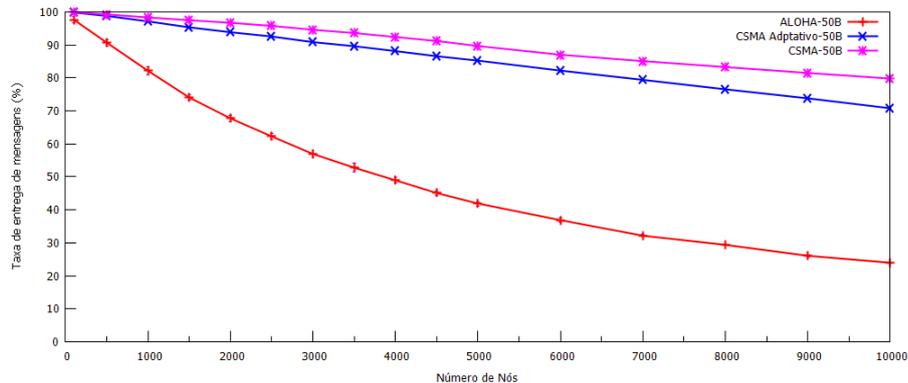
O objetivo dessas alterações é obter uma diminuição no consumo de energia dos nós e uma melhora na vazão da rede se comparado ao método de acesso CSMA e, principalmente, melhorar a eficiência energética da rede. Espera-se ter uma rede com uma eficiência energética igual ao de redes Aloha, mas com as vantagens do CSMA inclusas.

Após as modificações necessárias, detalhadas na Figura 1, implementou-se o novo modelo de acesso ao meio chamado de CSMA Adaptativo. As Figuras 2, 3, 4 e 5 apresentam o desempenho dos três protocolos de acesso ao meio (Aloha, CSMA e CSMA Adaptativo) em relação à taxa de entrega de mensagens, vazão da rede, consumo de energia e eficiência energética, respectivamente, variando o número de nós na rede e considerando um tempo entre mensagens de 600s.

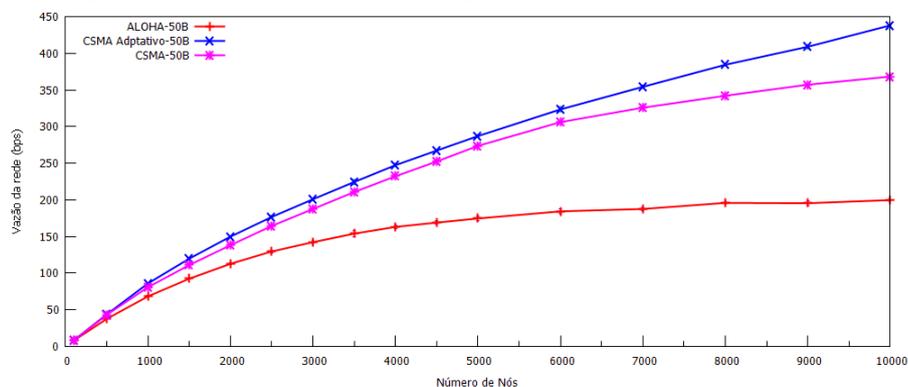
Como citado na Tabela 1, o limite dos contadores para adaptação é de 33 mensagens perdidas em sequência. Esse número representa 1% das mensagens totais enviadas no cenário com menos nós na rede, assim dando a todos os cenários chances de realizarem a adaptação, caso necessário.

Na Figura 2 pode ser visto que assim como a versão original do CSMA, o CSMA Adaptativo consegue manter uma alta taxa de entrega de mensagens. Apesar de entregar menos mensagens do que o CSMA, essa perda é de no máximo 12,8%, pior caso ocorrido com uma rede de 10000 nós. Em relação ao Aloha original, o CSMA Adaptativo obtém uma taxa de entrega bem superior. Quanto maior o número de nós na rede, maior é essa diferença de desempenho. Para uma rede com 10000 nós, por exemplo, o CSMA Adaptativo obtém um ganho em relação à taxa de entrega de mensagens de 207% se comparado ao Aloha. Em cenários com uma rede menos congestionada, entre 1 e 2000 nós, a diferença em relação à taxa de mensagens entregues entre o CSMA e o CSMA Adaptativo é muito pequena. Por exemplo, em um cenário com 1000 nós, o CSMA Adaptativo apresentou uma taxa de entrega de mensagens de 97,15% em comparação

**Figura 2. Taxa de entrega de mensagens em relação ao número de nós na rede**



**Figura 3. Vazão da rede em relação ao número de nós na rede**



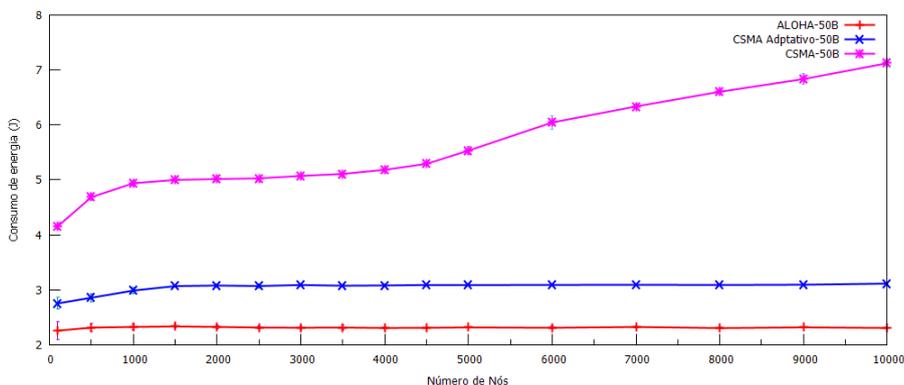
com 98,36% de mensagens entregues no CSMA e 82,16% no Aloha. Já no cenário com 10000 nós o CSMA Adaptativo apresentou uma taxa de entrega de mensagens de 70,82% em comparação com 79,83% de mensagens entregues no CSMA e 23,98% no Aloha.

Com uma verificação mais rápida do meio executada pelo CSMA Adaptativo, um fluxo maior de mensagens trafega pela rede. Na Figura 3 pode-se ver a vazão da rede. Inicialmente, a vazão da rede é muito próxima para os três protocolos. Mas, com o aumento no número de nós na rede, aumenta-se a ocupação do meio e a diferença no desempenho dos protocolos aumenta. A partir de 1000 nós na rede pode ser visto que o CSMA Adaptativo começa a apresentar um melhor desempenho em relação à vazão da rede se comparado ao Aloha e CSMA. No cenário com 1000 nós, por exemplo, o CSMA Adaptativo, o CSMA e o Aloha apresentam uma vazão de 86, 81 e 68, respectivamente. Isso representa para o CSMA Adaptativo um ganho na vazão de rede de aproximadamente 6% em relação ao CSMA e 26% em relação ao Aloha. No cenário com 10000 nós, por exemplo, o CSMA Adaptativo, o CSMA e o Aloha apresentam uma vazão de 438, 368 e 200, respectivamente. Isso representa para o CSMA Adaptativo um ganho na vazão da rede de 19% em relação ao CSMA e 119% em relação ao Aloha.

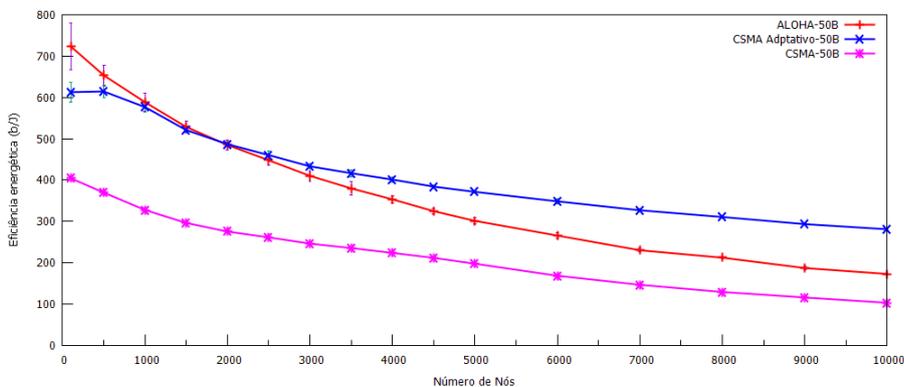
Vale lembrar que apenas o ganho obtido na vazão da rede não garante uma eficiência energética como a obtida pelo protocolo Aloha. Para isso é necessário analisar como se dá o consumo de energia dos nós ao utilizar cada um dos protocolos avaliados. A Figura 4 apresenta esses dados. Pode-se verificar que o objetivo principal de diminuir

o consumo de energia foi alcançado. Assim como o método Aloha, o CSMA Adaptativo apresenta um gasto constante de energia. Como era esperado, o CSMA Adaptativo apresenta um maior consumo de energia em relação ao Aloha, pois mesmo utilizando um DIFS reduzido, o sensoriamento do meio faz com que o dispositivo se coloque em um modo energético mais custoso. Ao considerar um cenário com 1000 nós, o consumo de energia no CSMA Adaptativo foi 28,40% maior que o Aloha e 39,51% menor do que o CSMA. No cenário com 10000 nós, o consumo de energia foi 34,94% maior que o Aloha e 56,28% menor do que o CSMA.

**Figura 4. Consumo de energia em relação ao número de nós na rede**

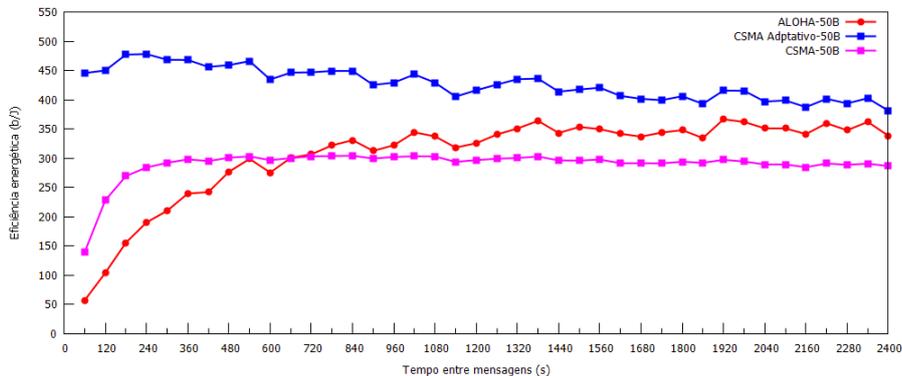


**Figura 5. Eficiência energética em relação ao número de nós na rede**



Espera-se que com uma maior vazão da rede, o CSMA Adaptativo consiga compensar o consumo extra de energia com uma maior eficiência energética. A Figura 5 apresenta essa confirmação. Como nos cenários com até 500 nós, o CSMA Adaptativo ainda não apresentava uma maior vazão se comparada ao Aloha, a eficiência do CSMA Adaptativo nesses cenários ainda é menor se comparado ao Aloha. Em cenários com um número de nós variando entre 1000 e 2000, tem-se uma aproximação grande na eficiência energética dos protocolos Aloha e CSMA Adaptativo. No cenário com 1000 nós, a eficiência energética do CSMA Adaptativo foi apenas 2% menor que o Aloha e 75% maior que o CSMA. Com uma maior vazão da rede, o CSMA Adaptativo consegue um desempenho melhor. Por exemplo, em um cenário com 10000 nós, o CSMA Adaptativo, o CSMA e o Aloha apresentam uma eficiência energética de 281 bits/J, 103 bits/J e 173 bits/J, respectivamente. Isso representa que o CSMA Adaptativo obteve uma eficiência 173% maior que o CSMA e 62% maior que o Aloha.

**Figura 6. Eficiência energética em relação ao tempo entre mensagens**



Na sequência, foi analisada a eficiência energética dos protocolos variando a ocupação da rede através do tempo entre mensagens. Assim, quanto menor o tempo entre mensagens, maior a ocupação da rede. A Figura 6 apresenta os resultados obtidos, considerando 1000 nós na rede. Nos cenários com maior ocupação da rede, mais especificamente com um tempo entre mensagens menor do que 360s, o protocolo CSMA com tempo fixo de sensoriamento obteve um melhor desempenho se comparado ao protocolo Aloha. Com um tempo entre mensagens maior do que 360s, onde se tem uma diminuição na ocupação da rede, a eficiência entre os protocolos CSMA e Aloha se invertem. Em relação ao CSMA Adaptativo, para todos os tempos entre mensagens o protocolo proposto obteve o melhor desempenho. Por exemplo, em um cenário com tempo entre mensagens de 360s, o CSMA Adaptativo obteve uma eficiência energética 95,29% maior que o Aloha e 57,02% maior que o CSMA.

## 6. Conclusões e trabalhos futuros

Este artigo apresentou um novo protocolo de acesso ao meio aplicado à tecnologia LoRaWAN. Esse protocolo chamado de CSMA Adaptativo propõe variar o tempo de sensoriamento do meio de acordo com a ocupação da rede. Inicialmente, o protocolo utilizará um menor tempo de sensoriamento, esperando que a rede esteja livre e, caso encontre a rede ocupada, esse tempo será aumentado. Assim, quando os nós estiverem em redes desocupadas eles terão um comportamento mais semelhante ao Aloha padrão e quando eles sentirem que a rede está bastante ocupada seu comportamento se assemelherá ao CSMA padrão.

O desempenho dos protocolos rede foi analisado em relação às métricas de taxa de entrega de pacotes, vazão de rede e eficiência energética. De acordo com os resultados obtidos, quanto menos congestionada estiver a rede, mais próximo será o desempenho dos protocolos em relação à taxa de entrega de mensagens e vazão da rede. Conforme aumenta-se o número de nós na rede, maior será a diferença de desempenho entre os protocolos. Por exemplo, em uma rede com 10000 nós, o CSMA Adaptativo apresentou uma taxa de entrega de mensagens de 70,82% em comparação com 79,83% de mensagens entregues no CSMA e 23,98% no Aloha. Isso representou para o CSMA Adaptativo um aumento em relação ao número de mensagens entregues de 195% se comparado ao Aloha e uma perda de 11,29% se comparado ao CSMA. No mesmo cenário, o CSMA Adaptativo, o CSMA e o Aloha apresentam uma vazão de 438 bps, 368 bps e 200 bps,

respectivamente. Isso representa para o CSMA Adaptativo um ganho na vazão de rede de 19% em relação ao CSMA e 119% em relação ao Aloha. Em relação ao consumo de energia dos nós, o Aloha é o protocolo que consome menos energia dos nós, seguido pelo CSMA Adaptativo e CSMA. Devido ao uso do DIFS adaptável, o CSMA Adaptativo foi capaz de reduzir o consumo em energia dos nós em 56,28% se comparado ao CSMA, com um aumento de 34,94% se comparado ao Aloha. Porém, com uma maior vazão da rede, o CSMA Adaptativo conseguiu compensar o consumo extra de energia em relação ao Aloha e prover uma maior eficiência energética. Nesse mesmo cenário com 10000 nós, o CSMA Adaptativo obteve uma eficiência 173% maior (281 bits/J) que o CSMA (103 bits/J) e 62% maior que o Aloha (173 bits/J).

Como trabalhos futuros, pretende-se analisar o impacto da utilização de protocolos de acesso ao meio TDMA (*Time Division Multiple Access*). Estes protocolos podem trazer um maior grau de confiança na entrega de mensagens eliminando esta deficiência das redes LoRaWAN.

## Referências

- Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia-Segui, J., and Watteyne, T. (2017). Understanding the limits of lorawan. *IEEE Communications magazine*, 55(9):34–40.
- Aras, E., Ramachandran, G. S., Lawrence, P., and Hughes, D. (2017). Exploring the security vulnerabilities of lora. In *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*, pages 1–6. IEEE.
- Augustin, A., Yi, J., Clausen, T., and Townsley, W. M. (2016). A study of lora: Long range & low power networks for the internet of things. *Sensors*, 16(9):1466.
- Bankov, D., Khorov, E., and Lyakhov, A. (2016). On the limits of lorawan channel access. In *2016 International Conference on Engineering and Telecommunication (EnT)*, pages 10–14. IEEE.
- Bor, M. and Roedig, U. (2017). Lora transmission parameter selection. In *2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pages 27–34. IEEE.
- Bor, M. C., Roedig, U., Voigt, T., and Alonso, J. M. (2016). Do lora low-power wide-area networks scale? In *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pages 59–67.
- de Carvalho Silva, J., Rodrigues, J. J., Alberti, A. M., Solic, P., and Aquino, A. L. (2017). Lorawan—a low power wan protocol for internet of things: A review and opportunities. In *2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, pages 1–6. IEEE.
- Georgiou, O. and Raza, U. (2017). Low power wide area network analysis: Can lora scale? *IEEE Wireless Communications Letters*, 6(2):162–165.
- Magrin, D. and Capuzzo, M. and Romagnolo, S. and Luvisotto, M. (2018). Lorawan class a implementation for ns-3. <https://github.com/signetlabdei/lorawan>. [Online; acessado em 18-Junho-2021].

- Mangold, S., Choi, S., May, P., Klein, O., Hiertz, G., and Stibor, L. (2002). Ieee 802.11 e wireless lan for quality of service. In *Proc. European Wireless*, volume 2, pages 32–39. sn.
- Margelis, G., Piechocki, R., Kaleshi, D., and Thomas, P. (2015). Low throughput networks for the iot: Lessons learned from industrial implementations. In *2015 IEEE 2nd world forum on internet of things (WF-IoT)*, pages 181–186. IEEE.
- Mikhaylov, K., Petaejaevaervi, J., and Haenninen, T. (2016). Analysis of capacity and scalability of the lora low power wide area network technology. In *European Wireless 2016; 22th European Wireless Conference*, pages 1–6. VDE.
- Neumann, P., Montavont, J., and Noël, T. (2016). Indoor deployment of low-power wide area networks (lpwan): A lorawan case study. In *2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 1–8. IEEE.
- ns3 (2011-2021). A discrete-event network simulator for internet systems. <https://www.nsnam.org/>. [Online; acessado em 18-Junho-2021].
- Petajarvi, J., Mikhaylov, K., Roivainen, A., Hanninen, T., and Pettissalo, M. (2015). On the coverage of lpwans: range evaluation and channel attenuation model for lora technology. In *2015 14th International Conference on ITS Telecommunications (ITST)*, pages 55–59. IEEE.
- Petrić, T., Goessens, M., Nuaymi, L., Toutain, L., and Pelov, A. (2016). Measurements, performance and analysis of lora fabian, a real-world implementation of lpwan. In *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pages 1–7. IEEE.
- Semtech Corporation (2015). AN1200.22: LoRa Modulation Basics. Rev. 2. <http://wiki.lahoud.fr/lib/exe/fetch.php?media=an1200.22.pdf>. [Online; acessado em 18-Junho-2021].
- Semtech Corporation (2016). LoRa® and LoRaWAN®. <https://lora-developers.semtech.com/library/tech-papers-and-guides/lora-and-lorawan/>. [Online; acessado em 18-Junho-2021].
- Semtech Corporation (2019). Wireless RF LoRa Transceivers: SX1276; Rev. 6. <https://semtech.my.salesforce.com>. [Online; acessado em 18-Junho-2021].
- To, T. and Duda, A. (2018). Simulation of lora in ns-3: Improving lora performance with csma. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–7.
- Voigt, T., Bor, M., Roedig, U., and Alonso, J. (2016). Mitigating inter-network interference in lora networks. *arXiv preprint arXiv:1611.00688*.
- Weber, P., Jäckle, D., Rahusen, D., and Sikora, A. (2016). Ipv6 over lorawan™. In *2016 3rd International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, pages 75–79. IEEE.
- Zanella, A., Bui, N., Castellani, A., Vangelista, L., and Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things journal*, 1(1):22–32.