MARCOS HEYSE PEREIRA

UMA PROPOSTA DE ENGENHARIA DE TRÁFEGO EM REDES DE SENSORES ZIGBEE BASEADA EM OUTAGE

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para a obtenção do título de Mestre em Informática Aplicada.

CURITIBA

2013

MARCOS HEYSE PEREIRA

UMA PROPOSTA DE ENGENHARIA DE TRÁFEGO EM REDES DE SENSORES ZIGBEE BASEADA EM OUTAGE

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para a obtenção do título de Mestre em Informática Aplicada.

Área de Concentração: *Redes de Computadores e Telecomunicações.*

Orientador: Prof. Dr. Edgard Jamhour

CURITIBA

2013

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central

P436p 2013

Pereira, Marcos Heyse
Uma proposta de engenharia de tráfego em redes de sensores Zigbee baseada em outage / Marcos Heyse Pereira ; orientador, Edgard Jamhour. – 2013.
xxiii, 110 p. : il. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2013
Bibliografia: f. [93]-100

1. Informática. 2. Engenharia de tráfego. 3. Redes de sensores sem fio. 4. Desempenho. I. Jamhour, Edgard. II. Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Informática Aplicada. III. Título.

CDD 20. ed. – 004

Pontifícia Universidade Católica do Paraná
Escola Politécnica
Programa de Pós-Graduação em Informática

PUCPR
GRUPO MARISTA

ATA DE DEFESA DE DISSERTAÇÃO DE MESTRADO
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

DEFESA DE DISSERTAÇÃO Nº 16/2013

Aos 06 dias do mês de Setembro de 2013 realizou-se a sessão pública de Defesa da Dissertação **"Uma Proposta de Engenharia de Tráfego em Redes de Sensores ZIGBEE Baseada em *Outage*"** apresentado pelo aluno **Marcos Heyse Pereira,** como requisito parcial para a obtenção do título de Mestre em Informática, perante uma Banca Examinadora composta pelos seguintes membros:

Prof. Dr. Edgard Jamhour PUCPR (Orientador)	Edgard Jamhour *(assinatura)*	APROVADO *(Aprov/Reprov)*
Prof. Dr. Marcelo Eduardo Pellenz PUCPR	 *(assinatura)*	APROVADO *(Aprov/Reprov)*
Prof. Dr. Richard Demo Souza UTFPR	Richard Demo *(assinatura)*	Aprovado *(Aprov/Reprov)*

Conforme as normas regimentais do PPGIa e da PUCPR, o trabalho apresentado foi considerado APROVADO (*aprovado/reprovado*), segundo avaliação da maioria dos membros desta Banca Examinadora. Este resultado está condicionado ao cumprimento integral das solicitações da Banca Examinadora registradas no Livro de Defesas do programa.

Prof. Dr. Mauro Sergio Pereira Fonseca
Diretor do Programa de Pós-Graduação em Informática

Programa de Pós-Graduação em ... PPGIa PUCPR

Rua Imaculada Conceição, 1155 Prado Velho CEP 80215 901 Curitiba Paraná Brasil
Tel.: (41) 3271 1669 Fax.: (41) 3271 2121 www.ppgia.pucpr.br

Aos meus pais, Paulo Maurício e Vilse, e a minha noiva Suelen.

Agradecimentos

À minha família, principalmente aos meus pais, por toda a orientação, dedicação e apoio durante toda minha vida, e a minha noiva Suelen, por todo amor, incentivo e compreensão.

Ao Prof. Dr. Edgard Jamhour pela confiança, paciência e orientação durante todo o processo de execução deste trabalho.

Ao Prof. Dr. Marcelo Eduardo Pellenz pela colaboração prestada durante o desenvolvimento da pesquisa.

Aos amigos conhecidos durante o mestrado, especialmente aos colegas da área de conhecimento de redes, e demais amigos que de alguma maneira colaboraram na realização desta dissertação.

Aos colegas e professores do Programa de Pós-Graduação em Informática Aplicada da PUC-PR que me acompanharam nestes anos.

Ao Instituto Federal de Santa Catarina, pelo apoio financeiro e o reconhecimento de que o investimento em conhecimento resulta em uma educação de maior qualidade.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Símbolos

r_{ij}	Quadro de dados recebido no nó de destino
P_i	Potência de transmissão do nó *i*
γ_{ij}	Perda de caminho/percurso no enlace *i – j*
h_{ij}	Unidade de variação Nakagami-m de desvanecimento quase-estático
n_{ij}	Vetor de ruído de sinal
N_0	Densidade espectral de potência de ruído térmico
α	Expoente de perda do caminho
G	Ganho total das antenas de transmissão e recepção
G_{tx}	Ganho total das antenas de transmissão
G_{rx}	Ganho total da antena de recepção
λ	Comprimento de onda
M_l	Margem do enlace *l*
N_f	Figura de ruído no receptor
$\overline{SNR_{ij}}$	Potência de ruído no link *i – j*
β	Limiar de sinal-ruído instantâneo
Δ	Eficiência espectral do sistema
B	Largura de banda do sistema
$\mathcal{O}_{ij}$	Probabilidade de Outage do enlace *i – j* de acordo com o modelo Nakagami-m
$\Gamma(a)$	Função Gamma completa
$\Psi(a, b)$	Função Gamma incompleta inferior
T_{ij}	Número médio de transmissões pelo nó *i* antes de ser aceito pelo nó *j*
x_i, y_i, z_i	Posição dos nós no plano cartesiano tridimensional
meo	Probabilidade de outage máxima aceitável
mtd	Distância máxima de transmissão

ID	Distância de Interferência
TM	Matrix de Tráfego com o conjunto de fluxos l_{ij}
l_{ij}	Demanda de tráfego requerida no enlace $i - j$
(v_i e v_j)	Conjunto dos nós de origem e destino que compõe um enlace E
G(V,E)	Grafo unidirecional que representa uma WMN
V	Conjunto de vértices do grafo
E	Conjunto de enlaces sem fio bidirecionais
|	Tal que / Tal como
∧	Símbolo matemática que significa "e"
ed_{ij}	Distância euclidiana entre os nós i e j
d_{ij}	Distância em função do outage
TEL_{xy}	A carga total de tráfego através de uma aresta
p_{ij}	Conjunto dos enlaces que formam o caminho do nó i para o nó j
$IDVS_i$	Domínio de interferência de um nó sensor i
CDS_{ij}	Domínio de colisão da comunicação entre os nós v_i e v_j
$TDES_i$	Conjunto de arestas que estão no mesmo domínio de transmissão de v_i
CDL_{ij}	Carga total de tráfego no domínio de colisão de uma aresta
$\sum$	Somatório
∀	Para todo
$\prod$	Produtório
l_{max}	Capacidade máxima de transmissão dos nós sensores
$\mathcal{O}_{ij}$	Probabilidade de outage do caminho p_{ij}
f_c	Faixa de frequência do canal
dx_{min}	Distância mínima dentro do intervalo para definir onde o nó será posicionado no grid
dx_{max}	Distância máxima dentro do intervalo para definir onde o nó será posicionado no grid

Lista de Abreviaturas

ACK	*Acknowledgment Packet*
AES	*Advanced Encryption Standard*
AODV	*Ad hoc On-Demand Distance Vector*
CAP	*Contension Access Period*
CBR	*Constant Bit Rate*
CCA	*Clear Channel Assessment*
CFP	*Contension Free Period*
CSMA-CA	*Carrier Sense Multiple Access with Collision Avoidance*
CTS	*Clear to Send*
ED	*Energy Detection*
FFD	*Full Function Device*
GPS	*Global Positioning System*
GTS	*Guaranteed Time Slots*
IEEE	*Institute of Electrical and Electronics Engineers*
ISM	*Industrial, Scientific and Medic*
LOS	*Line of Sight*
LQI	*Link Quality Indicator*
LR-WPAN	*Low Rate – Wireless Personal Area Networks*
MAC	*Medium Access Control*
MHR	*MAC Header*
MPDU	*MAC Protocol Data Unit*
NLOS	*Non-Line of Sight*
NS-2	*Network Simulator versão 2*
NWK	*Network Layer*
PER	*Packet Error Rate*

PHR	*PHY header*
PSDU	*PHY Service Data Unit*
QoS	*Quality of Service*
RERR	*Route Error*
RFD	*Reduced Function Device*
RFID	*Radio-Frequency Identification*
RRPL	*Route Request-Route Reply*
RRQ	*Route Request*
RSSF	*Redes de Sensores Sem Fio*
RTS	*Request to Send*
SFD	*Start of Frame Delimiter*
SHR	*Synchronization Header*
SNR	*Signal-to-Noise Ratio*
SOL	*Shortest path with respect to the number of hops under a maximum outage limit*
SOP	*Smallest Outage probability*
SWP	*Shortest Weighted Path*
TMT	*Theoretical Maximum Throughput*
Wi-Fi	*Wireless Fidelity*
WISENES	*Wireless Sensor Network Simulator*
WMN	*Wireless Mesh Networks*
WSN	*Wireless Sensor Networks*
SHR	*Synchronization Header*

Resumo

As redes Zigbee, baseadas no padrão IEEE 802.15.4, surgem como alternativa para fornecer infraestrutura de acesso a redes pessoais sem fio de baixa taxa de comunicação (LR-WPAN). Certas aplicações do ZigBee, como o uso em redes industriais de sensores, podem ser extremamente limitadas pela sua baixa taxa de dados. Por esta razão torna-se importante a busca de meios para se obter o máximo desempenho da rede durante a comunicação. Este trabalho apresenta um método de Engenharia de Tráfego para Redes de Sensores Sem-fio (RSSFs), visando a determinar a capacidade máxima de transmissão em redes mesh Zigbee. A análise da capacidade das RSSF é realizada considerando a contenção imposta pela camada de acesso ao meio e sob a restrição de uma probabilidade de falha (outage) associada a cada enlace sem fio. A probabilidade é baseada no modelo de desvanecimento (*fading*) Nakagami-m, que avalia as retransmissões devido ao efeito do outage, enquanto que o modelo de contenção é necessário para avaliar caminhos de múltiplos saltos em RSSFs. Por fim, propomos um método para o planejamento otimizado de rotas em redes mesh com ou sem restrições de outage. O proposto foi validado através de simulação no NS2 juntamente com o módulo de sensores 802.15.4.

Palavras-Chave: Zigbee, Desempenho, Engenharia de Tráfego, Outage.

Abstract

Zigbee networks, based on the IEEE 802.15.4, are an alternative to provide infrastructure for access to personal wireless networks with low communication rate (LR-WPAN). Certain applications of ZigBee, as the use of sensors in industrial networks, may be critically limited by its designation as a low data rate standard. For this reason it is important to find ways to get maximum performance from the network during the communication. This work presents a method of Traffic Engineering for Wireless Sensor Networks (WSN), in order to determine the maximum transmission in ZigBee mesh networks. A capacity analysis of WSN is performed considering the contention imposed by the medium access layer and under the constraint of an outage probability associated with each wireless link. The probability is based on the Nakagami-m fading model, which evaluates the retransmissions due to the effect of the outage, while the contention model is necessary to evaluate multi-hop paths in WSN. Finally, we propose a method to the optimal planning of routes in WSN mesh networks with or without restrictions outage. The proposed has been validated by simulation on NS2 with the 802.15.4 sensor module.

Keywords: ZigBee, Performance, Traffic Engineering, Outage.

Capítulo 1

Introdução

Os recentes avanços nas comunicações sem fio permitiram o desenvolvimento de redes de sensores de baixo custo. As redes de sensores podem ser utilizadas em várias áreas de aplicação, como saúde, militar e habitação. Nas redes pessoais wireless (WPANs), um dos principais padrões adotados foi o Bluetooth, amplamente utilizado em aparelhos móveis como telefones celulares. Outro padrão muito utilizado neste quesito é o Wi-Fi (*Wireless Fidelity*), entretanto, para alguns dispositivos estes padrões se tornaram inviáveis devido a problemas como o alto consumo de energia, surgindo a necessidade da criação de um novo padrão para redes de baixo consumo. A tecnologia ZigBee, definida pelo IEEE em conjunto com a ZigBee Alliance, foi criada com o intuito de disponibilizar uma rede com baixa potência de operação e baixo consumo de energia pelos dispositivos, estendendo autonomia de suas baterias, podendo as mesmas durarem anos.

Por se tratar de uma rede de baixa taxa de comunicação, certas aplicações podem ser extremamente limitadas em redes de grande porte ou em redes mal dimensionadas, tornando necessária a otimização do uso da taxa de comunicação da rede (Throughput). Por essas razões, o provisionamento da capacidade das redes de sensores sem fio, a implantação de mecanismos para fornecer a escolha dos melhores caminhos, constituem um tema com grande potencial de pesquisa e desenvolvimento.

1.1. Motivação

Dentro do contexto de abordagem das WPANs (*Wireless Personal Área Network*), os protocolos Zigbee e Bluetooth se destacam. As duas propostas divergem, sendo a primeira direcionada a aplicações de baixa potência, onde o baixo consumo é importante e a

necessidade de taxa de comunicação em geral é menor. Isso a torna ideal para aplicações em WSNs (*Wireless Sensor Networks*). Outra característica importante é o fator escalabilidade, que permite redes grandes, com muitos dispositivos. Já o Bluetooth é empregado em aplicações que exigem maior taxa de transmissão e redes mais compactas, como aplicativos de áudio. As desvantagens são: consumo elevado, maior complexidade de implementação, maior necessidade de recursos computacionais.

A tecnologia ZigBee foi desenvolvida com o objetivo de permitir a construção de redes WPAN de fácil escalabilidade, com um baixo consumo de potência e a um custo acessível. O padrão IEEE 802.15.4, no qual as redes ZigBee são baseadas, prevê funcionamento nas bandas de 868 MHz na Europa, 915 MHz na América do Norte e na banda global ISM 2.4 GHz (*Industrial, Scientific and Medic*), em taxas de comunicação de 20 Kbps, 40 Kbps e 250 Kbps, respectivamente. Na prática, o padrão mais amplamente divulgado é o de 2.4 GHz, pelo fato de ser licenciado mundialmente. As topologias mais empregadas são estrela, árvore em cluster e malha (mesh), sendo essa última a que permite o maior grau de escalabilidade. Em teoria, permite-se a alocação de até 65536 dispositivos ZigBee. Esta característica de permitir redes grandes, aliado à característica de ser uma tecnologia de baixa taxa de comunicação, pode provocar grandes limitações no desempenho das redes Zigbee, tornando necessária a otimização do uso da taxa de comunicação da rede (throughput).

Este trabalho, foca o estudo de redes Zigbee pré-concebidas, com pouca dinamicidade em sua estrutura. Se por um lado falta de mobilidade simplifica o problema de roteamento, por outro lado abre espaço para estudos mais aprofundados em termos de desenvolvimento de estratégias que possam ofertar serviços com garantia de qualidade de serviço e engenharia de tráfico. Para isso, diferentes cenários podem ser levados em consideração, como por exemplo: topologia da rede, quantidade de nós, configurações dos mecanismos de rede que serão utilizados na comunicação, entre outros. Este projeto de pesquisa insere-se no contexto da abordagem de otimização da taxa de transmissão nas Redes de Sensores Sem-fio, com aplicação especial nas redes Zigbee.

1.2. Proposta

Existem muitos trabalhos relacionados à pesquisa do desempenho de redes de sensores. [01] e [02] demonstram de forma detalhada como estimar a taxa de transmissão em redes de um salto (*single-hop*) sem o uso de beacons, enquanto [03] propõe um modelo para

redes com beacon ativo. Os resultados apresentados, porém, são inadequados às redes de múltiplos saltos (*multi-hop*) devido às suas particularidades.

Em [04] é proposto um modelo de engenharia de tráfego para prover qualidade de serviço (QoS – *Quality of Service*) em redes de sensores com múltiplos caminhos, buscando melhorar a confiabilidade e a entrega de pacotes mantendo baixos níveis de consumo de energia. O modelo se baseia em atraso (*delay*), confiabilidade e caminhos de energia limitada para determinar o roteamento na rede de sensores.

Outra solução é o *Autonomous Traffic Engineering* (ATE), descrito em [05]. Ele utiliza três sistemas de coordenação: um sistema de inferência de congestionamento, um sistema de estimativa da qualidade de link e um sistema dinâmico de desvio de tráfego, além de um algoritmo de roteamento baseada em localização geográfica e nos níveis de energia residuais dos nós.

A priorização de economia de energia pode não resultar no cálculo ideal da capacidade das redes sem fio, diminuindo o throughput máximo possível, o que em alguns casos torna-se uma desvantagem. Além disso, os modelos não levam em consideração os domínios de colisão dos nós e o efeito do outage presente nas comunicações sem fio, fatores importantes no cálculo da capacidade das redes sem fio.

Neste contexto, Jun e Sichitiu [06] resolveram o problema para o cálculo da capacidade das WMN (*Wireless Mesh Networks*), utilizando o conceito de domínio de colisão (ou contenção). Apesar de determinar a capacidade de uma WMN, o trabalho considera somente o domínio de colisão com a maior carga da rede e não leva em conta o reuso espacial dentro dos domínios de colisão, reduzindo a eficiência de utilização dos recursos da rede.

Aoun e Boutaba [07] estendem o método proposto por [06] considerando vários domínios de colisão e o reuso espacial, tornando a estimativa da capacidade mais próxima da real.

Fischer e Jamhour [08] formalizaram os modelos de [06] e [07], propondo um modelo simbólico de engenharia de tráfego em redes Mesh Wi-Fi para determinar a capacidade da rede, considerando a contenção do canal e o reuso espacial, além de uma abordagem de otimização, com uso de métodos heurísticos, para realizar a alocação de recursos e a identificação dos melhores caminhos da rede. O modelo foi adaptado para ser executado através do software Wolfram Matemática em forma de algoritmo.

O objetivo deste trabalho é propor um método para prover engenharia de tráfego e o cálculo da capacidade de uma WSN, levando em consideração os domínios de colisão e a probabilidade de falha (outage) associada a cada enlace sem fio. Formulamos um modelo analítico de capacidade baseado na formulação Nakagami-m de probabilidade de outage para estimar a distância máxima de comunicação entre os nós sensores em relação a um nível de outage aceitável.

O método proposto baseia-se nesta distância de transmissão dos nós para determinar a escolha dos melhores caminhos, visando oferecer o melhor provisionamento possível da rede sem exceder a capacidade máxima do canal.

O modelo se baseia nas premissas de que todos os nós operam no mesmo canal em 2.4 Ghz, considerando uma única interface de rádio por nó da rede, e que não existe mobilidade nos nós na topologia.

Os resultados do algoritmo foram ainda comparados com simulações no software ns-2, fazendo o uso do módulo de rede de sensores desenvolvido por [09], além de alterações para prover o descarte de pacotes relacionados ao efeito do outage.

1.3. Estrutura do Documento

Este trabalho está dividido em 6 capítulos. O Capítulo 2 descreve a tecnologia de redes de sensores sem fio com suas principais características, funcionalidades, sendo explorados os principais conceitos relacionados à pesquisa.

O Capítulo 3 apresenta o estado da arte, contendo os principais trabalhos relacionados à pesquisa da análise da capacidade das redes de sensores;

O Capítulo 4 apresenta em detalhes a proposta de engenharia de tráfego para redes de sensores Zigbee, contendo o modelo de canal sem fios baseado no modelo de desvanecimento Nakagami-m, o modelo de contenção para redes mesh de sensores, e os algoritmos necessários para utilizar o modelo no planejamento otimizado de rotas em RSSF mesh.

O Capítulo 5 descreve as simulações realizadas em cenários típicos e a análise dos resultados, comparando os dados teóricos obtidos com simulação via software.

O Capítulo 6 conclui o trabalho realizado e apresenta propostas para trabalhos futuros

Capítulo 2

Principais Conceitos Relacionados à Pesquisa

Neste capítulo são apresentados os principais conceitos relacionados ao tema de pesquisa e o padrão ZigBee. Primeiramente, são abordados os principais conceitos da tecnologia com uma apresentação inicial e suas características básicas. Em seguida, é demonstrada as principais características do padrão 802.15.4, que define as camadas físicas e de enlace do ZigBee. Além disso, o capítulo traz informações sobre as camadas superiores e a segurança em redes ZigBee, encerrando o assunto com as peculiaridades que podem ser utilizadas em pesquisas para se obter a maximização da taxa de comunicação de dados.

2.1. Redes ZigBee

Zigbee é um padrão que define um conjunto de protocolos de comunicação para redes sem fio de baixa taxa e curta distância. É classificado como tecnologia de rede pessoal sem fio de baixa taxa de comunicação (LR-WPAN) de baixo custo de implementação e baixo consumo de energia, direcionado principalmente a redes sem-fio de sensores (WSNs), sistemas de Rádio Frequência (RFID), automação residencial e predial, aplicações de monitoramento e controle industrial e médicas.

Com surgimento em 2004 através de uma aliança entre várias empresas (cerca de 200) - ZigBee Alliance, em parceria com o *Institute of Electrical and Electronics Engineers* (IEEE), a tecnologia tem por objetivos definir as camadas mais elevadas do modelo OSI (rede até aplicação), garantir a interoperabilidade entre os sistemas e promover a tecnologia dentro do mercado de aplicações sem-fio de baixa potência [10]. A Figura 2.1 demonstra as camadas do padrão ZigBee.

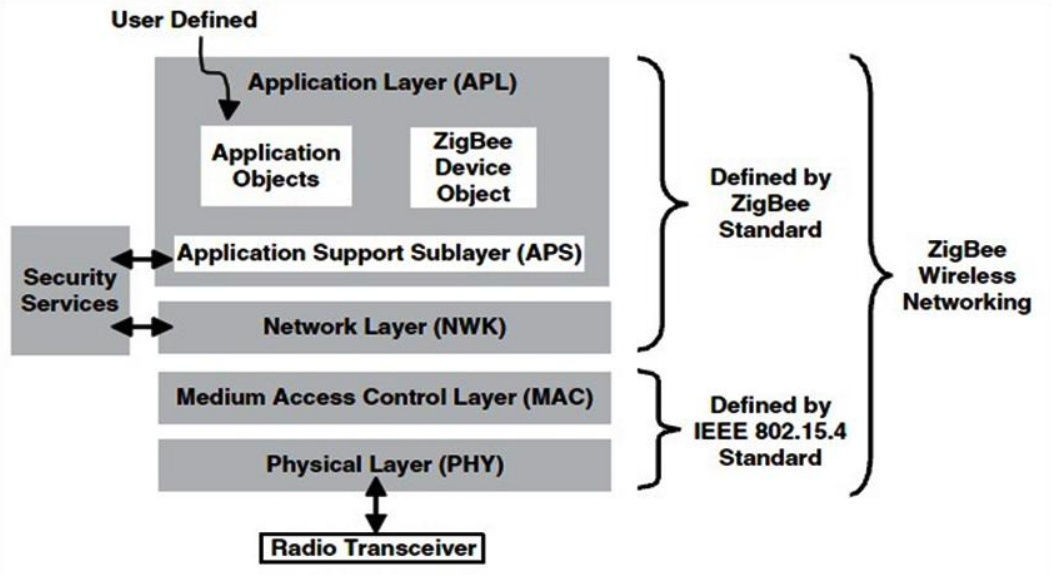

Figura 2.1: Camadas e Protocolos das Redes Sem-fio ZigBee [11]

2.1.1. Topologias

Existem diferentes topologias que podem variar de uma estrela centralizada (*Star*) ou uma arquitetura de cluster baseado em árvore (*Cluster Tree*) até a uma rede de malha completa (*Mesh*). As arquiteturas possíveis são mostradas na Figura 2.2.

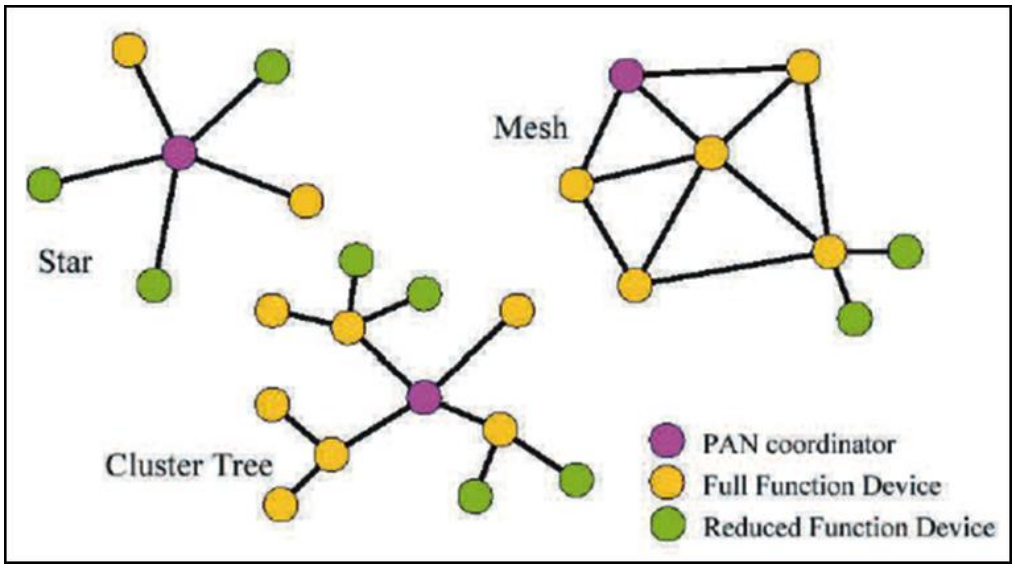

Figura 2.2: Topologias de Redes ZigBee [12]

Na topologia em estrela, cada dispositivo na rede pode se comunicar apenas com o coordenador ZigBee. Um cenário típico de uma formação de rede em estrela é que um FFD

(*Full Function Device* – conforme informações detalhadas disponíveis no Apêndice A.2), programado para ser um coordenador do PAN, é ativado e começa a estabelecer a sua rede. A primeira coisa que o coordenador faz é selecionar um identificador único que não é usado por qualquer outra rede na sua esfera de rádio na região ao redor do dispositivo, no qual seu rádio possa comunicar com êxito com outras rádios. Em outras palavras, ela garante que o identificador PAN não está sendo usado por qualquer outra rede nas proximidades.

Outra forma é a topologia de árvore (*Cluster-tree*). Neste caso, um coordenador ZigBee (coordenador PAN), estabelece a rede inicial. Roteadores ZigBee formam os galhos e retransmitem as mensagens. Dispositivos ZigBee finais atuam como folhas da árvore e não participam nas mensagens de encaminhamento. Roteadores ZigBee podem crescer a rede para além da rede inicial estabelecida pelo coordenador ZigBee [11].

Já as redes Mesh (conhecida também como topologia *peer-to-peer*), permitem aumentar o alcance, confiabilidade (auto-reparo da rede) e a formação de redes ad-hoc onde todos os caminhos redundantes são fornecidos. Cada dispositivo pode se comunicar diretamente com qualquer outro dispositivo, se os aparelhos são colocados próximos o suficiente para estabelecer um elo de comunicação bem-sucedida [13].

Qualquer FFD pode desempenhar o papel do coordenador do PAN. Uma maneira de decidir qual dispositivo será o coordenador é escolher o primeiro dispositivo FFD que iniciar a comunicação como coordenador.

Em uma rede mesh, todos os dispositivos que participam da transmissão das mensagens são FFDs, pois RFDs (*Reduced Fuction Devices*) não são capazes de transmitir as mensagens. No entanto, um RFD pode ser parte da rede e se comunicar apenas com um dispositivo em particular (o coordenador ou um roteador) na rede.

2.1.2. Camada de Enlace – MAC e o CSMA-CA

A camada de enlace definida pelo padrão IEEE 802.15.4 é onde o acesso ao canal e a transmissão de quadros acontecem. Oferece suporte à transmissão confiável com retransmissão de pacotes, correção de erros, envio de quadros de confirmação, associação entre os dispositivos e gerenciamento dos slots de transmissão.

O *MAC Protocol Data Unit* (MPDU) é detalhado na Figura 2.3. Dentro do quadro MAC, o cabeçalho (MHR – *MAC Header*) é composto pelo controle de quadro (*Frame Control*) que indica o tipo de quadro, o formato do endereço e controla o envio do quadro

opcional de confirmação ACK (*Acknowledgment*), o número de sequência, que ordena os quadros durante o envio de uma transmissão e o endereço, que carrega os endereços MAC e lógico. A carga útil (*payload*) é de tamanho variável. Ao final do quadro, o campo de checagem de quadro (*Frame Check Sequence*) valida os dados recebidos pela estação destino.

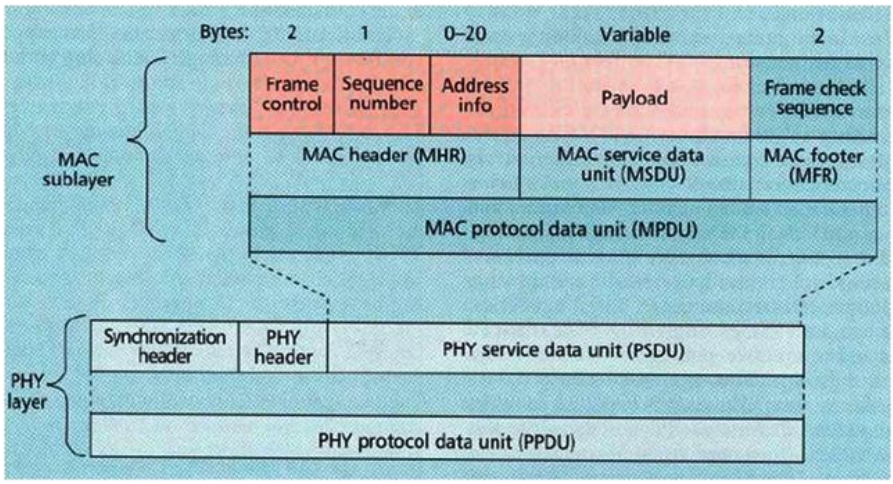

Figura 2.3: Estrutura do Quadro MAC IEEE 802.15.4 [12]

Com relação ao método de acesso ao canal, o IEEE 802.15.4 faz uso do protocolo *Carrier Sense Multiple Access with Collision Avoidance* (CSMA-CA), nas versões slotted e unslotted. No CSMA-CA, a qualquer hora que o dispositivo quiser transmitir, é realizado um *Clear Channel Assessment* (CCA), que compara o nível de energia do canal com um limiar de transmissão para assegurar que o canal não está em uso por outro dispositivo. Então o dispositivo inicia transmitindo seu próprio sinal. A decisão de declarar se um canal está vazio ou não pode ser baseado na medição da energia spectral no canal de freqüência de interesse ou detectando o tipo de ocupação de sinal.

Através do mecanismo de detecção de energia (ED – *Energy Detection*), o módulo estima a potência do sinal recebido dentro da faixa do canal de transmissão. No ED, o módulo não tenta decodificar o sinal, mas somente a potência é estimada. Se existe sinal na faixa de interesse, o ED não determina se é ou não um sinal IEEE 802.15.4 [14].

Uma forma alternativa de declarar se um canal de frequência está livre ou ocupado é o *carrier sense* (CS). No CS, em contraste com ED, o tipo de sinal de ocupação é determinado e, se este sinal é um sinal IEEE 802.15.4, então o dispositivo pode decidir considerar o canal ocupado, mesmo se o nível do sinal é inferior ao definido.

Se o canal não está livre, o dispositivo se afasta por um período de tempo aleatório e tenta novamente. Este procedimento se repete até que o canal se torna livre ou o dispositivo atinge o número máximo de tentativas definido.

2.1.3 Modos Beaconing e Non-Beaconing

Conforme dito anteriormente, existem dois métodos para acesso ao canal: baseado em contenção (*unslotted*) e ou livre de contenção (*slotted*). Em canal de acesso baseado em contenção, todos os dispositivos que pretendem transmitir no mesmo canal de frequência usam o mecanismo CSMA-CA, e a primeira que encontra o canal livre começa a transmitir. Assim, o canal deve ser monitorado o tempo todo pelas estações, deixando a rede sempre ativa.

Já o método de contenção livre, também conhecido por modo *beaconing* ou *beacon enabled mode*, o coordenador do PAN dedica um horário específico para um determinado dispositivo. Isto é chamado um intervalo de tempo garantido (GTS - *Guaranteed Time Slots*). O modo utiliza o formato de *superframes* periódicos, dividido em 16 GTS que podem ser alocados para até sete aplicações distintas. Essa estrutura tem o objetivo de prover banda livre em algumas situações e de proporcionar baixa latência nas transmissões.

O *superframe* é limitado por *beacons* a cada período de tempo pré-determinado, podendo ser esse período entre 15ms e 252s. O acesso ao canal no interior de cada *slot* será livre de contenções. Beacon é uma mensagem com formato específico que é utilizado para sincronizar os relógios dos nós da rede.

Como ilustrado na Figura 2.4, após o beacon, existe os tempos de acesso CAP (*Contension Access Period*), onde todos os dispositivos competem entre si utilizando CSMA-CA e o CFP (*Contension Free Period*) que garante *slots* de tempo para cada dispositivo. Após isso, o dispositivo entra em modo inativo e guarda energia [15].

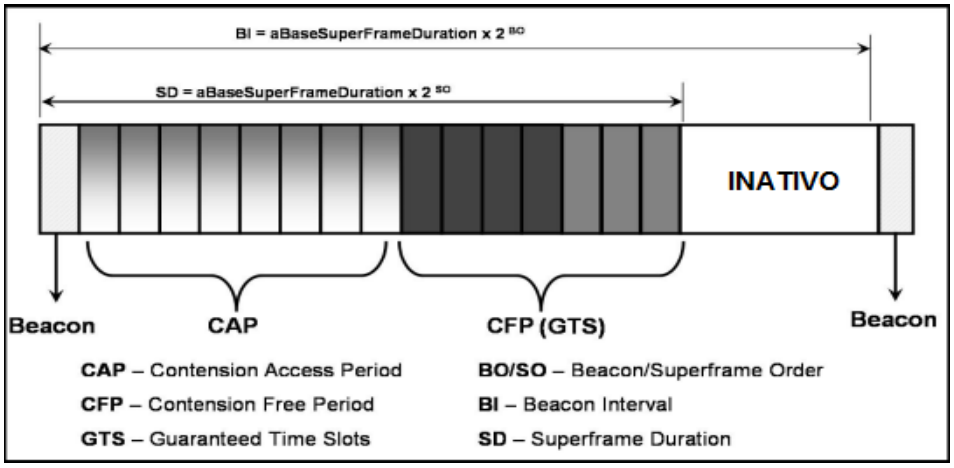

Figura 2.4: Estrutura do Superframe [15]

A desvantagem do uso de Beacons é que todos os dispositivos na rede devem acordar regularmente, escutar o beacon, sincronizar os relógios, e voltar a dormir. Isso significa que muitos dos dispositivos da rede podem acordar somente para sincronização e não realizar qualquer outra tarefa enquanto estão ativos. Portanto, a duração da bateria de um dispositivo em uma rede beacon-ativo é normalmente inferior a uma rede sem beacon porque neste último caso os dispositivos precisam acordar com menos frequência. [11].

2.1.4 Camada de Rede

A camada NWK (*Network Layer*) proporciona interfaces entre as camadas MAC e de Aplicação e é responsável pelo gerenciamento da formação e roteamento da rede. A camada NWK de um coordenador ZigBee é responsável por estabelecer uma nova rede e selecionar a topologia (estrela, árvore ou malha). O coordenador também atribui os endereços de rede para os dispositivos em sua rede.

O algoritmo de roteamento padrão definido pela Zigbee Alliance é o AODV (*Ad hoc On-Demand Distance Vector*), com a diferença de que as estações são heterogêneas quanto à capacidade de roteamento. Quando se deseja realizar uma transmissão para um destinatário desconhecido, mensagens de requisição de rota (RRQ – *Route Request*) são enviadas por broadcast para a rede. As rotas são atualizadas com base na resposta dos roteadores (RRPL - *Route Request-Route Reply*), e caso a rota não possa ser encontrada, uma mensagem de erro (RERR – *Route Error*) é gerada. Quando isso acontece, é acionado um mecanismo para detectar um novo caminho para o destinatário da mensagem e avisar os módulos vizinhos sobre a alteração da topologia. A grande vantagem desse modelo de roteamento é a

inexistência da necessidade de atualização periódica das tabelas de roteamento, o que reduz significativamente o tráfego de controle [10].

Outra forma de implementação é a de roteamento hierárquico em árvore. Este modelo tira proveito das associações da camada MAC para implementar o roteamento. As tabelas de roteamento são formadas a partir da árvore hierárquica de nós, criada no momento das associações.

Além de diminuir a quantidade de pacotes de transmitidos, este modelo torna-se interessante na topologia em árvore, pois se trata de um modelo hierárquico. Por outro lado, sua aplicabilidade torna-se reduzida em redes Mesh, onde todos os nós podem se tornar roteadores, sendo o protocolo AODV mais indicado neste caso.

2.2. Características Específicas para Maximização do Throughput

O padrão Zigbee possui uma série de peculiaridades que foram exploradas nos artigos estudados, relacionados à análise da capacidade das redes de sensores. Uma das características abordadas é o uso do CSMA-CA no tráfego, devido a seus modos com ou sem Beacon. No modo Beacon-ativo, o sistema trabalha com transmissões de Beacons periódicos para sincronia dos nós da rede e fará o uso de *slots* de tempo garantidos na transmissão que poderão garantir *QoS* em alguns casos. O modo sem Beacon trabalha de maneira parecida com a tradicional, utilizada no padrão IEEE 802.11, com todos os nós que querem transmitir disputando o canal e utilizando tempos de *backoff* exponencial.

O consumo de energia é levado em conta por boa parte dos autores, sendo que nesse caso muitas vezes para se obter um consumo menor de energia, poderá ser necessário abrir mão da maximização de desempenho.

Outro fator importante é a topologia escolhida. Trabalhos relacionados às redes estrela são mais simples de se desenvolver, uma vez que se trata de redes de único salto. Estudos em topologias de múltiplos saltos requerem soluções robustas que servirão normalmente para redes de maior tamanho.

Por fim, observou-se que as redes Zigbee possuem em sua especificação opções restritas de roteamento, o que pode acarretar em problemas de desempenho e consumo de energia devido à grande quantidade de cenários de rede possíveis, tornando o provisionamento da capacidade das redes sem fio, a implantação de mecanismos para fornecer a escolha dos melhores caminhos, temas importantes de estudo.

2.3. Conclusão

Com o crescente uso das redes sem-fio em todas as áreas, e o aumento de uso das redes pessoais sem-fio e especialmente o Bluetooth, notou-se a necessidade da criação de um novo padrão para redes pessoais sem fio com baixo consumo de energia.

As redes Zigbee, surgiram como alternativa para fornecer infraestrutura de acesso a redes pessoais sem fio de baixa taxa de comunicação (LR-WPAN), sendo que este protocolo aparece como opção às redes Bluetooth, uma vez que oferece maior alcance e grande poder de duração da bateria nos dispositivos.

Por fim, as redes Zigbee devem continuar em uso e desenvolvimento, uma vez que já é muito utilizada na indústria e na área médica e continua com um grupo cada vez maior de colaboradores em seu desenvolvimento.

Informações mais detalhadas sobre as redes Zigbee estão constadas no Apêndice A, onde são demonstradas as principais características, a classificação e detalhes do padrão 802.15.4, no qual o Zigbee foi baseado.

Capítulo 3

Trabalhos Relacionados com a Pesquisa

3.1. Introdução

As soluções existentes para o cálculo da capacidade e maximização do desempenho em redes de sensores estão atualmente relacionadas a dois grandes focos de pesquisa: 1) baseado em análises de desempenho e 2) baseado em engenharia de tráfego. O primeiro é empregado através da descrição de um modelo teórico de tráfego a fim de se obter qual a capacidade máxima das WSNs, considerando diferentes situações de uso da rede, como topologias, uso do modo beacon-ativo, CSMA-CA, eficiência energética, entre outros, e/ou através também da realização de simulações reais ou via software.

Já o segundo foco de pesquisa é em soluções efetivas que visam não só determinar a capacidade das redes de sensores sem fio em diferentes cenários, mas da busca de mecanismos para se alcançar a melhoria do throughput e do roteamento na rede, através do planejamento otimizado, procurando determinar os melhores caminhos, o balanceamento do trafego entre roteadores, menor atraso (*delay*) na comunicação, entre outros conceitos abordados. Em soluções de engenharia de tráfego, os autores também podem levar em consideração modelos teóricos de tráfego a fim de se obter um desempenho otimizado.

Desta forma, torna-se relevante a utilização de um modelo que leve em consideração as características de utilização da rede. Outro favor importante é determinar a forma como efetuar os testes e apresentar a solução. Muitos trabalhos utilizam a simulação como ferramenta, embora outros optem pela obtenção de dados analíticos.

Neste capítulo são apresentados de maneira detalhada os diferentes cenários de uso das redes de sensores sem fio, relacionando pesquisas relevantes em acordo com as várias características peculiares, classificadas segundo o seguinte critério:

- De acordo com a topologia: *single-hop* (estrela) ou *multi-hop* (*cluster-tree* e *mesh*);
- De acordo com o protocolo de roteamento utilizado;
- De acordo com utilização ou não do modo de pacotes de confirmação (ACK);
- De acordo com o uso do modo Beacon e sem Beacon.

Além disso, será debatida a metodologia utilizada pelos pesquisadores para a obtenção e comparação dos resultados, conforme o seguinte critério de classificação:

- Resultados gerados através de simulação;
- Resultados gerados através de dados teóricos analíticos.

Por fim, serão descritos os principais trabalhos relacionados aos dois grandes focos de pesquisa:

- Soluções baseadas em análises de desempenho;
- Soluções baseadas em engenharia de tráfego.

3.2. Topologias

Ao desenvolver-se um trabalho de pesquisa onde um cenário de rede é proposto, uma das primeiras características a serem levadas em consideração é a topologia que será escolhida. Modelos teóricos para redes *single-hop* e *multi-hop* são diferentes, o que poderá acarretar em resultados insatisfatórios caso adotado o modelo incorreto para uma determinada proposta. Por esta razão, é corriqueiro aos autores adotarem uma topologia específica em seus trabalhos.

Existem vários trabalhos desenvolvidos em redes com topologia estrela (*single-hop*), onde cenários simplistas são levados em consideração. [16], [17] e [01] são exemplos de trabalhos que utilizam redes em estrela com poucos nós, para obtenção do throughput.

Já as pesquisas em redes de múltiplos saltos, embora apresentem uma quantidade menor de trabalhos publicados, apresentam-se como um tema de grande número de possibilidades de pesquisa. As redes também conhecidas como *peer-to-peer*, são descritas nos cenários *cluster-tree* ([18] e [19]) e Mesh, onde diferentes modelos são detalhados em [20],

[21] e [22]. Na topologia *cluster-tree*, é possível economizar energia, pois cada nó mantém a sincronização apenas com seu coordenador-mãe. Entretanto, uma desvantagem é que uma falha de um coordenador pode causar uma grande quantidade de nós filho e nós neto órfãos e com isso o aumento da demanda de tráfego e consumo de energia nas re-associações. Isto torna a topologia Mesh mais flexível e tolerante a falhas.

Como são topologias semelhantes, alguns autores descrevem soluções onde a princípio seriam aplicáveis nos dois cenários. Os modelos de engenharia de tráfego [04] e [05] são dois exemplos de solução para cenários de múltiplos caminhos e múltiplos saltos.

3.3. Protocolos de Roteamento

Conforme descrito na seção 2.1.4, a tecnologia Zigbee possui em sua especificação opções restritas de roteamento que deverão ser utilizadas independentes das demais configurações de rede, o que pode acarretar em problemas de desempenho e consumo de energia devido à grande quantidade de cenários de rede possíveis.

Além disso, para redes mesh, o protocolo AODV proposto é bastante simples, fornecendo espaço para possibilidades de melhorias em seu protocolo ou até mesmo para propostas de novos protocolos de roteamento. Um exemplo disso são os protocolos de roteamento baseados em localização geográfica, como o *Energy-Balanced Multipath Geografic Forwarding* (EBMGF), descrito em [05], onde a localização e roteamento dos nós são realizadas por GPS (*Global Positioning System*) ou outra técnica similar. Já em [23] é proposto o *Enhanced Hierarchical Routing Protocol* (EHRP), a fim de determinar os melhores caminhos no roteamento em árvore hierárquica e outras melhorias. [24] e [25] fazem o uso do protocolo AODV Junior em redes Zigbee, por este se tratar de um protocolo compatível e mais leve de acordo com os autores. Por fim, outros autores propõem melhorias no próprio AODV, como em [26].

Para fornecer uma maior flexibilidade e o roteamento otimizado das redes, uma opção interessante é a do próprio administrador da rede definir por quais caminhos o tráfego deverá passar. Isto se justifica principalmente em redes onde a ocorrência de colisão e retransmissão de pacotes possa ser grande, como em uma rede mesh, por exemplo. Ao contrário das redes *ad-hoc*, em redes mesh a topologia não muda constantemente, o que justifica o não uso de um protocolo de roteamento padrão. Em outras palavras, uma rede mesh apresenta topologia estável, exceto para eventuais falhas e adição de novos nós [07].

Desta forma, é possível implementar soluções de engenharia de tráfego e promover a escolha dos melhores caminhos em redes Zigbee, como será apresentado neste trabalho.

3.4. Modos ACK e sem ACK

Por se tratar de uma tecnologia de baixa taxa de transmissão, as redes de sensores IEEE 802.15.4 oferecem um modo opcional de confirmação de recebimento na transmissão de pacotes entre o nó e o coordenador. Esta confirmação é realizada através do envio de um pacote do tipo ACK (*Acknowledgment Packet*) pelo receptor. Este recurso garante que os dados transmitidos cheguem ao seu destino, entretanto, a taxa efetiva fim-a-fim dependerá da sobrecarga da transmissão do pacote ACK [21]. Assim, ao realizar o uso de pacotes ACK, a capacidade total da rede poderá ser reduzida, principalmente em redes *multi-hop*, pois além do aumento no número de pacotes, aumentará também a ocorrência de colisão de pacotes. Por outro lado, a utilização deste mecanismo promove uma maior confiabilidade da rede, e a taxa efetiva da rede poderá ser maior, devido às retransmissões dos pacotes que não chegaram ao destino inicialmente.

Existem vários trabalhos que realizam a análise de desempenho com a utilização das duas abordagens. Alguns consideram modo ACK ativo como em [27]. Já em [28] os pacotes de reconhecimento são desconsiderados. Por fim, ainda existem trabalhos que especificamente realizam a análise e comparação dos dois modos em um cenário específico de rede. Os trabalhos [17] e [29] descrevem esta situação.

3.5. Modos Beacon e sem Beacon

Outro fator importante na definição das características da rede a ser proposta é o uso do modo Beaconing, descrito no capítulo 2. O uso de Beacons reduz o consumo de energia, tornando-se uma boa solução em redes pequenas e principalmente nas com topologia estrela. No entanto, de acordo com [30], o uso de *slots* de tempo (GTS) é pobre em redes mesh e cluster-tree, pois o QoS é realizado apenas em um salto (coordenador PAN e os nós diretamente conectados a ele). Além disso, o uso de slots de tempo limita o throughput em redes descongestionadas. Deste modo, é preferível não utilizar beacons em redes de múltiplos saltos, como em redes Mesh.

O trabalho descrito em [22] propõe melhorias no modo Beacon em redes *multi-hop*, porém, ainda assim seus resultados ficam abaixo das taxas da rede sem beacons. Em [31]

também é realizado a análise de desempenho entre os dois modos. Por fim, outros trabalhos como [29] e [32] levam em consideração um dos modos em seus cenários.

3.6. Domínios de Colisão e Nós Escondidos

Segundo [08], o domínio de colisão de um enlace sem fio "*x*" é composto pelo conjunto de enlaces vizinhos a "*x*", que compartilham seu canal local, e consequentemente interferem em sua transmissão. Pode-se dizer que um domínio de colisão representa o conjunto de nós que devem estar inativos para que um enlace possa transmitir com sucesso. Devido a isto, a capacidade efetiva diminui quando existe mais de um nó no domínio de colisão, uma vez que somente um nó pode transmitir a cada tempo.

Além disso, como identificado em [33], o raio de alcance da interferência é normalmente maior que o alcance da transmissão, aumentando a probabilidade de colisão. Desta forma, deve se considerar no domínio de colisão todos os nós que estão dentro da distância de interferência do transmissor. [21] considera em seu modelo que uma rede *multi-hop* pode obter 1/4 do Throughput de uma rede *single-hop*. A Figura 3.1 demonstra um cenário envolvendo duas transmissões, onde a circulo sólido mostra o alcance de transmissão e o círculo pontilhado representa o alcance da interferência [32]. A Figura 3.2 mostra um cenário típico de um domínio de colisão, envolvendo o par de nós 4 e 3, mostrando que a carga total deste enlace deve também levar em consideração as transmissões vizinhas que interferem na transmissão. Cada fluxo de transmissão é computado como uma unidade de tráfego *U*.

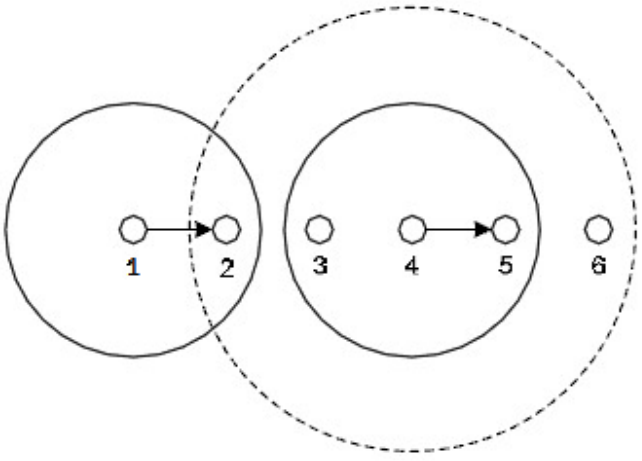

Figura 3.1: Domínios de Transmissão e Interferência

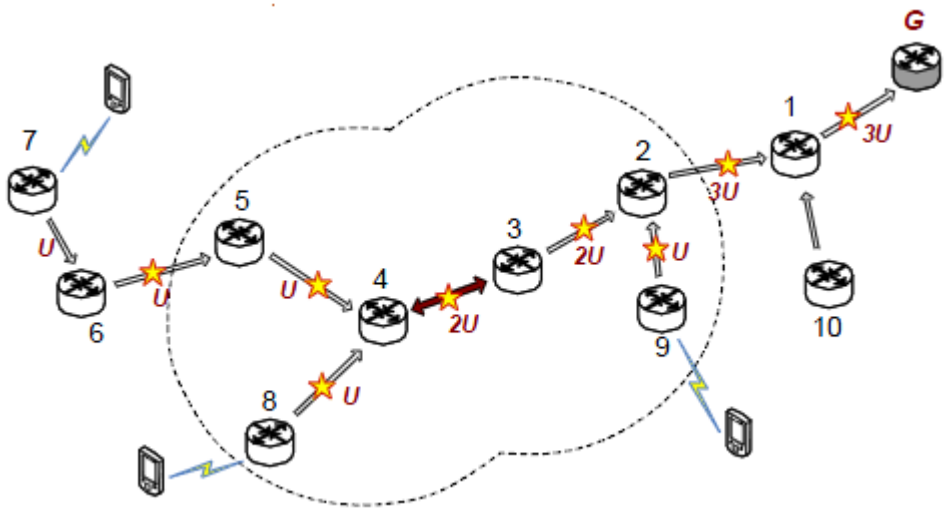

Figura 3.2: Domínio de Colisão 4⟶3 [07]

A capacidade de transmissão ainda é afetada pelo conhecido problema do terminal oculto, ou nó escondido. Conforme demonstrado na Figura 3.2, considerando que:

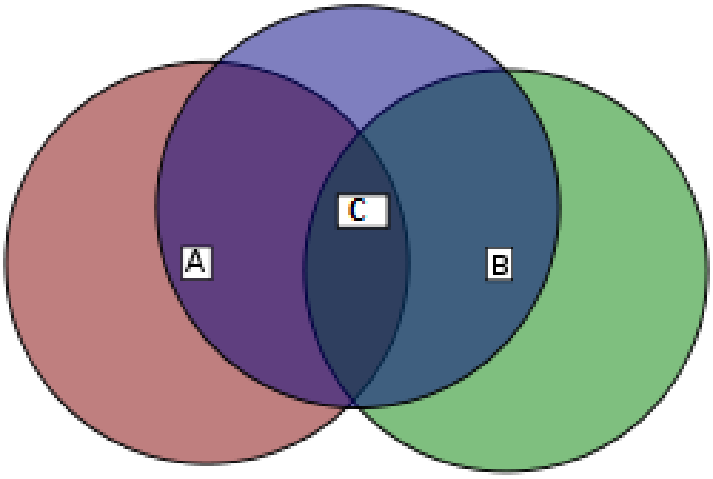

Figura 3.3: Exemplo do Problema do Nó Escondido [34]

- o nó A está enviando dados para o nó C;
- o nó B também deseja transmitir para C;
- o nó B está fora da área de transmissão de A.

O terminal B acha que o meio está livre e envia seus dados o nó C, o que resulta em uma colisão em C, porque este recebe dados de A e B simultaneamente. Neste caso, dizemos que A e B são terminais ocultos em relação a C.

O mecanismo RTS/CTS (*Request to Send / Clear to Send*), presente no padrão IEEE 802.11, previne o problema do nó escondido. Devido ao padrão IEEE 802.15.4 usualmente trafegar pacotes de tamanho pequeno, o custo da utilização do mecanismo RTS/CTS é grande, tornando-se inviável em muitos casos, sendo este recurso indisponível nas redes IEEE 802.15.4 por padrão. Assim, o problema do nó escondido é ainda mais presente nas redes de sensores sem fio, sendo mais uma questão que pode ser levada em consideração no cálculo da capacidade das RSSF.

Dentre os trabalhos que abordam o problema, em [35] estima que a probabilidade de dois nós no alcance do coordenador estarem escondidos um do outro é de 41%. O problema desta abordagem é que em redes mesh a topologia e a quantidade de nós poderão mudar esta probabilidade, uma vez que vários caminhos poderão ser usados para um mesmo destino. [20] propõe a adoção do mecanismo de RTS/CTS com algumas alterações para redes de sensores a fim de reduzir o problema do nó escondido. Por fim, [21] propõe superar o efeito dos terminais ocultos através do uso de “trens” de pacotes consecutivos, onde cada trem consiste de um grupo de nós por onde percorrerá um trafego, dando a ideia de que cada trem é um fluxo continuo. O tamanho do trem dependerá do raio de interferência e de transmissão da tecnologia em questão.

3.7. Abordagem Analítica e Abordagem Simulada

No desenvolvimento de um trabalho de pesquisa, é importante a busca de uma metodologia para validar e demonstrar os resultados do que foi proposto. Para isso, algumas estratégias podem ser tomadas, a fim de garantir um resultado satisfatório. Dentre as abordagens mais utilizadas nas pesquisas de capacidade de redes de sensores estão a analítica e a simulada.

Na abordagem analítica, os resultados são gerados matematicamente, com a implementação dos cenários propostos através de cálculos, probabilidades, e outras definições matemáticas. Um exemplo seria agrupar os domínios de colisão da topologia utilizando a teoria de conjuntos, sendo cada subconjunto um domínio de colisão da rede. Para considerar os nós escondidos, poderia se utilizar uma probabilidade “*x*” de ocorrência deste fenômeno. A topologia poderá ser mapeada através de grafos de conectividade. Por fim, os parâmetros da rede poderiam ser considerados com valores pré-determinados. A vantagem desta abordagem é que vários cenários podem ser montados de forma mais rápida, incluindo cenários

complexos e redes grandes, onde a simulação se tornaria muito custosa. A desvantagem é que dados matemáticos teoricamente são menos realísticos que dados simulados e muitas vezes não preverem todas as situações do mundo real.

Já a simulação pode ser realizada de duas maneiras, via software específico de simulação ou com simulação de hardware. No primeiro, o cenário proposto e os parâmetros como nós, rotas e configurações da rede são definidos inicialmente em arquivos de configuração. Em seguida, o cenário é colocado em execução, disparando pacotes na rede, e ao final, dados de desempenho, atraso, entre outros são obtidos. No segundo caso, uma simulação real é feita, com equipamentos reais ou protótipos. A grande vantagem deste modelo é que o uso de equipamentos reais torna os resultados mais realistas, porém, com alto custo de implementação e alto grau de complexidade para gerar cenários complexos. Além disso, a abordagem de simulação real necessita de maior tempo para sua implementação devido à maior complexidade.

Vários são os trabalhos que abordam os dois casos. Nos trabalhos baseados em análise de desempenho, onde somente um modelo teórico é levado em consideração, a maior parte dos trabalhos utiliza a simulação como ferramenta de comparação e geração dos resultados. [01] realizou um estudo através da comparação analítica e simulada via software com os resultados da simulação real via hardware em uma rede Zigbee. O Throughput simulado por software foi realizado através do simulador NS-2, equipado com o módulo IEEE 802.15.4 desenvolvido por Zheng and Lee [09].

Já [30] realiza a análise matemática e simulada do desempenho e do consumo de energia em uma rede Zigbee de larga escala com 1560 nós. Esta é uma prática muito comum de validar os resultados, onde ao final, os dados teóricos analíticos são comparados com os valores simulados. Neste trabalho, foi utilizado o *WIreless SEnsor NEtwork Simulator* (WISENES). Segundo o autor, o WISENES possui alto nível de abstração e possui como principal objetivo o uso em simulações de larga escala.

Em [32], os testes foram realizados com hardware Crossbow's 2.4 GHz MICAz motes, hardware específico que permite a programação diretamente no hardware, e o uso do sistema operacional de sensores.

Por outro lado, a muitas das soluções baseadas em Engenharia de Tráfego utiliza somente a abordagem analítica. Nos trabalhos [04], [18] e [08], por exemplo, os resultados são gerados através de dados teóricos matemáticos. Isto se deve à complexidade deste tipo de

solução e dos cenários e topologias utilizadas, o que dificulta a simulação de software e praticamente inviabiliza a simulação de hardware em topologias com muitos nós.

3.8. Soluções para a Capacidade das RSSF

Abaixo, serão descritos com uma riqueza maior de detalhes os trabalhos relacionados aos dois grandes grupos de soluções relacionados à capacidade das redes de sensores sem fio. As baseadas na Análise de Desempenho e as baseadas em Engenharia de Tráfego.

3.8.1. Soluções Baseadas na Análise de Desempenho

Existem vários estudos que exploram diferentes situações em redes Zigbee quanto à estimativa da capacidade das WSN. [01] e [02] demonstram de forma detalhada como estimar a taxa de transmissão em cada salto (*single-hop*) em uma rede *non-beaconing*. No caso de [01], os resultados são comparados ainda com uma simulação real em hardware. Neste estudo, a estimativa prática de taxa de transferência em uma rede ZigBee foi regida pelas seguintes hipóteses:

- Não há erros de transmissão resultando em pacotes corrompidos ou perdidos.
- Cada pacote de dados pede a confirmação quando da recepção.
- A estrutura de pacotes e tamanhos de campo em análise são as definidas de acordo com cada camada IEEE 802.15.4. Especificamente, o payload da camada de aplicação, *AppPayload*, é igual a 101 bytes.
- O nó de destino é do tipo único salto (*single-hop*); as tabelas de roteamento são pré-compiladas.
- Tempo é modelado a partir da perspectiva do rádio em símbolos, que podem ser convertidos em segundos dividindo-os pela taxa simbólica de 62,500 símbolos por segundo.

Para o cálculo do throughput, primeiramente é estimado o tempo médio necessário para executar o CSMA-CA, em seguida, calculado o tempo necessário para completar as quatro etapas restantes do processo de transmissão (TX) de um pacote de determinado tamanho. O maior tamanho de pacote permitido dentro 802.15.4 proporcionará maior capacidade para a razão de sobrecarga. Desta forma, cada pacote de dados é assumido para conter 101 bytes de dados do aplicativo mais 32 bytes de overhead (133 bytes).

Para o cálculo do tempo do CSMA-CA *unslotted* (sem beacon), o artigo considera um número máximo de *backoffs*, com probabilidade de falha de acesso segundo uma cadeia de Markov. O tempo médio é calculado utilizando variáveis como duração do *backoff* e a duração do mecanismo CCA. O tempo total necessário para executar o processo de transmissão é a soma de seus componentes:

- TX de dados
- TX de tempo de resposta (*ACKTurnaround*)
- TX de tempo de reconhecimento (TX ACK)
- TX de tempo de espaçamento de *InterFrames* (LIFTS)

Já o *Throughput* simulado foi realizado através do simulador NS-2, equipado com o módulo IEEE 802.15.4 desenvolvido por Zheng and Lee [09], considerando adicionalmente os tempos de *delay* IFS entre as sucessivas transmissões. A comunicação *single-hop* entre dois nós é realizado com um coordenador PAN em modo sem beacon e um tráfego constante (CBR – *Constant Bit Rate*). O *throughput* foi obtido através da eliminação de pacotes perdidos e do payload da camada de aplicação de cada pacote.

Kohvakka e.t AL. em [30] realiza a análise matemática e simulada do desempenho e do consumo de energia em uma rede zigbee de larga escala de 1560 nós. Contrariando o primeiro estudo, as estimativas são realizadas com modo beacon ativado.

Outra diferença é que a topologia escolhida é a cluster-tree, que embora também seja considerada *peer-to-peer*, possui peculiaridades em relação às redes mesh. O artigo cita que redes *peer-to-peer* são importantes em grandes redes como, por exemplo, as industriais, porém, cita como problemas o aumento de latência da rede devido às várias mensagens de retransmissão entre os nós.

Devido ao uso do modo beacon ativado, foram levadas em consideração as características que compõem o superframe do modo beacon como o intervalo de Beacon, o tempo de duração do superframe ativo, e os períodos de acesso com contenção (CAP) e livre de contenção (CFP).

O artigo descreve de forma detalhada os cálculos da probabilidade de sucesso do CCA e os tempos de *backoff* do CSMA. O tempo médio de *Backoff* e energia no CSMA foram modelados através da quantidade de transmissões durante o CAP. Como foi utilizada uma estrutura de *cluster-tree* uniforme, o número de nós é calculado de acordo com a profundidade da árvore em relação ao coordenador. O algoritmo leva em consideração também a

probabilidade de colisão quando houver dois nós com mesmo *backoff* ou na existência de nós escondidos, o que afeta significativamente o desempenho do CCA. Por fim, a probabilidade de retransmissão é levada em conta no cálculo, para que sejam definidos os intervalos de cada beacon.

Com base nos cálculos acima e na configuração da rede, elaborada na tabela de parâmetros sumarizada a partir do trabalho em [36], o estudo faz a análise do consumo de energia do coordenador e demais dispositivos e do *Goodput*, além da probabilidade de sucesso na transmissão.

As simulações foram feitas com o WIreless SEnsor NEtwork Simulator (WISENES). Segundo o autor, o WISENES possui alto nível de abstração e possui como principal objetivo o uso em simulações de larga escala. Foram considerados diferentes tamanhos de CAP a fim de avaliar o consumo de energia e o *Goodput*.

Outro estudo é realizado por Lee [31] que traz a análise em uma rede estrela *single-hop* dos efeitos provocados em quatro tipos de experimentos:

- Transmissão direta (do dispositivo para o coordenador) e indireta (do coordenador para o dispositivo) de dados
- Uso do CSMA-CA
- Diferentes Tamanhos de *Payload* (tamanho do pacote de dados)
- Com e sem Modo Beacon-Ativo

Os resultados mostraram as características que a sobrecarga do protocolo reduz o *throughput* possível: adicionar mais nós de contenção em um meio com CSMA-CA aumenta a probabilidade de colisão e diminui o *throughput*; aumentar o tamanho do payload reduz a sobrecarga (overhead) por quadro e aumenta o *throughput*; transmitir mais beacons reduz o *throughput* útil.

Por fim, os trabalhos de [32] e [21] trazem o SenProbe: uma abordagem para mensurar a capacidade em redes *multi-hop* sem beacon. A ferramenta faz a estimativa da capacidade dos caminhos, levando em consideração os domínios de colisão e nós escondidos, através das distâncias de interferência e de transmissão.

A capacidade teórica de transmissão é dada pelas expressões:

$$C = \frac{Tpacket}{Tpacket + Tack + Theader + Twait} \times Cp \qquad 3.1$$

$$Tpacket = \frac{Spacket}{Cp}, \quad Tack = \frac{Sack}{Cp} \tag{3.2}$$

$$Theader = \frac{Snetwork + Smac + Sphy}{Cp} \tag{3.3}$$

Onde:

Tpacket: tempo de transmissão do *payload*

Tack: tempo de transmissão do pacote ACK (se utilizar)

Theader: tempo de transmissão do pacote header

Twait: tempo mínimo de espera do radio para enviar outro pacote

Spacket: tamanho do *payload overhead* (sobrecarga)

Snetwork: tamanho de *overhead* da camada de rede

Smac e *Sphy*: tamanhos de *overhead* das camadas física e MAC.

Sack: tamanho do pacote ACK

Cp: Capacidade do enlace na camada física (250 kbps)

Ao invés de considerar pares de pacotes consecutivos, são considerados "trens" de pacotes consecutivos, que são calculados através das distâncias de interferência e transmissão:

$$Ntrain = \left\lfloor \frac{InterferenceRange}{TransmissionRange} \right\rfloor + 2 \tag{3.4}$$

A capacidade total é obtida através da soma de todos os trens de pacotes obtidos. Neste artigo, os testes foram realizados com hardware Crossbow's MICAz motes, a 2.4 GHz e o uso do sistema operacional de sensores.

Há ainda outros estudos proposta, principalmente com foco em topologia estrela, como em [37], mas possuem foco na eficiência do consumo de energia, o que não é o foco deste trabalho

3.8.2. Soluções Baseadas na Engenharia de Tráfego

Existe uma quantidade menor de estudos que abordam soluções para a melhora do *throughput* em redes de sensores através da engenharia de tráfego. [04] propõe um modelo de engenharia de tráfego para prover qualidade de serviço (QoS) em redes de sensores com múltiplos caminhos, buscando melhorar a confiabilidade e a entrega de pacotes mantendo baixos níveis de consumo de energia. O modelo se baseia em atraso (*delay*), confiabilidade e caminhos de energia limitada para determinar o roteamento na rede de sensores.

Uma vez que múltiplos caminhos são considerados, o modelo proposto atende a todas as topologias, inclusive Mesh. Por isso, é considerada nos cálculos a soma dos valores (atraso, energia, etc) para os conjuntos de caminhos possíveis (*Path Set*), tais como:

- Atraso: soma do atraso entre os nós de origem e destino para cada caminho;
- Energia: energia consumida entre os caminhos;
- Confiabilidade: define-se assumindo que os enlaces de um caminho são independentes;

O algoritmo de roteamento para energia limitada é o *Energy Constrained Multipath Routing* (ECMP), descrito em [38]. Para justificar o uso deste algoritmo, o autor fez a comparação do ECMP com outras soluções já propostas. O ECMP define a qualidade dos caminhos através do tamanho do caminho, o seu uso (frequência de reuso dos mesmos caminhos) e o número de caminhos utilizados para enviar dados para a estação base. Estes valores fornecem uma indicação de confiabilidade e estabilidade deste algoritmo.

Os parâmetros de desempenho considerados nos experimentos incluem o consumo médio de energia, a taxa de entrega de pacotes, o atraso médio de entrega de dados e a qualidade dos caminhos utilizados pelos algoritmos.

Outra proposta de engenharia de tráfego é o *Autonomous Traffic Engineering* (ATE), descrito em [05]. Ele utiliza três sistemas de coordenação: um sistema de inferência de congestionamento, um sistema de estimativa da qualidade de link e um sistema dinâmico de desvio de tráfego. ATE busca minimizar o descarte de pacotes devido ao congestionamento, através do controle dinâmico e adaptativo do tráfego de dados em nós congestionados e/ou em links de baixa qualidade, e pelo aproveitamento oportunista de nós subutilizados para desvio de tráfego, minimizando a estimativa e medição de sobrecarga. Procura também fornecer alta fidelidade de aplicação na rede e sistemas leves e distribuídos da qualidade de link e congestionamento para melhorar a eficiência energética.

O algoritmo de roteamento é o *Energy-Balanced Multipath Geografic Forwarding (*EBMGF), algoritmo de exploração normalizada do progresso geográfico e dos níveis de energia residuais dos nós, também desenvolvido pelos autores. É assumido que os nós estão conscientes das suas informações de localização geográfica, seja através de GPS ou de outra técnica de determinação de localização. A divulgação das posições dos nós e sua energia residual são divulgadas por mensagens Beacon em *broadcast*.

Para prover melhorias no tráfego, ATE faz a divisão do tráfego entre dois nós a partir do sensor de origem, diminuindo o congestionamento e fazendo balanceamento de carga, melhorando o *throughput*. Para isso, é levada em consideração a qualidade do link estimada, melhorando ainda mais a eficiência da comunicação. A medição de congestionamento leva em consideração o nível de ocupação (número de pacotes) do buffer e o grau de contenção (atividade do canal) do nó. As simulações foram realizadas no NS-2 e foram comparadas as soluções CODA [39] e TARA [40], obtendo êxitos em todos os quesitos.

Já o trabalho realizado em [18] propõe uma metodologia diferente. O trabalho visa, através de um modelo de tráfego, determinar o pior caso aceitável em redes de sensores sem fio usando topologia *cluster-tree*. A abordagem torna-se interessante, uma vez que também determina até onde e de que maneira pode ser construída uma rede, mantendo-a em funcionamento e evitando gargalos.

O modelo é caracterizado pela profundidade de nós na topologia, máximo número de roteadores filho e o número máximo de nós filho para cada roteador pai. Através do uso do software *Network Calculus*, foram derivadas expressões para obter o atraso fim a fim, buffer e largura de banda necessária e demais características de especificação de tráfego. Por fim, o artigo demonstra a aplicação e resultados no dimensionamento de uma rede Zigbee.

Ao contrário da maioria dos modelos propostos até agora, este não se preocupa com o consumo de energia dos equipamentos. O seu foco é no dimensionamento para evitar perda de rendimento da rede. Os autores pretendem caracterizar a quantidade mínima de recursos necessária em cada roteador (largura de banda, tamanho do buffer de entrada) e o atraso máximo permitido.

Por fim, [08] propõem um modelo simbólico de engenharia de tráfego em redes Mesh sem fio IEEE 802.11 para determinar a capacidade da rede, considerando a contenção do canal, além de efetuar a escolha das melhores rotas através da abordagem de otimização com métodos heurísticos. O modelo foi adaptado para ser executado através do programa Wolfram

Matemática em forma de algoritmo e possui características aplicáveis e semelhantes quando comparadas a uma rede zigbee no modo *unslotted* (sem beacon).

O método determina a capacidade máxima de transmissão de uma rede mesh usando os conceitos de domínio de colisão, o reuso espacial dos nós e a capacidade teórica do canal. Como a capacidade máxima de transmissão é afetada pela quantidade de tráfego e caminho utilizado na rede, este trabalho propõe o uso de métodos de otimização para escolha dos melhores caminhos a serem utilizados pelas demandas de tráfego para oferecer o melhor provisionamento da rede sem exceder a capacidade máxima do canal.

3.9. Conclusão

Este capítulo apresentou soluções atualmente propostas a respeito da analise e maximização da taxa de dados (Throughput) em redes Zigbee, através de análises, simulações e engenharia de tráfego. O padrão possui uma série de peculiaridades que foram exploradas nos trabalhos estudados, tais como: consumo de energia, utilização do CSMA-CA, modo beacon-ativo, entre outros.

Soluções baseadas em análise de desempenho demonstram os resultados teóricos e simulados em determinadas situações específicas de rede. A principal vantagem dessa abordagem é a riqueza de detalhes expostos com relação aos cálculos e simulações realizadas. Por outro lado, soluções específicas podem gerar resultados muito diferentes do simulado em situações reais de uso da rede sem fio.

Soluções baseadas em engenharia de tráfego visam à melhoria do *throughput* e do roteamento na rede, procurando determinar os melhores caminhos, o balanceamento do trafego entre roteadores, menor atraso, entre outros conceitos. Sua aplicabilidade é normalmente utilizada em redes de múltiplos saltos, mas sem a necessidade de utilizar situações tão específicas, sendo um modelo mais genérico. A desvantagem desta abordagem é a complexidade necessária para desenvolver este tipo de solução.

É possível verificar nos trabalhos existentes a influência do CSMA-CA no tráfego devido a seus modos com ou sem Beacon. O modo Beacon ativo, normalmente é utilizado em soluções que buscam a economia de energia devido à sua transmissão com GTS e para garantir QoS em alguns casos. Por outro lado, seu uso implica em redução significativa do Throughput, principalmente em redes pequenas, onde *slots* de tempo são desperdiçados em comunicações ociosas.

O consumo de energia é levado em conta pela maioria dos autores, porém, é possível verificar que existem trabalhos com foco exclusivo no desempenho da rede, assim como outras buscam melhorias tanto no desempenho como na eficiência energética.

Outro fator importante é a topologia escolhida. Embora existam vários trabalhos relacionados a redes estrela, alguns autores já desenvolveram estudos nas topologias *peer-to-peer*, sendo estas, soluções robustas para redes de maior tamanho.

Por fim, a engenharia de tráfego se mostrou uma solução eficaz para redes de sensores em *cluster-tree* ou *mesh*, sendo esta uma área com bastantes opções para novas pesquisas. Outra opção é explorar soluções de análise de desempenho em situações ainda não previstas, ou até mesmo em cima de uma situação mais generalista.

Capítulo 4

Proposta do Projeto

4.1. Introdução

Conforme apresentado anteriormente, um modelo para estimar a capacidade das redes sem fios organizados segundo uma topologia mesh, assumindo um canal comum para todos os nós de transmissão, é dado por [06], [07] e formalizado em [08]. Nestes trabalhos, o alcance da transmissão é fixado, e considerado uma entrada para o problema. No entanto, na prática, o alcance de transmissão dos nós sensores sem fio é uma relação entre a distância e a taxa de perda de pacotes aceitável (outage). Se um elevado outage é tolerado, os nós podem ser assumidos como sendo capazes de comunicar em distâncias mais longas. Este capítulo apresenta um algoritmo para prover engenharia de tráfego e o cálculo da capacidade de uma WSN, sendo proposto um modelo analítico de capacidade baseado na formulação Nakagami-m de probabilidade de falha (outage) para estimar a distância máxima de comunicação entre os nós sensores em relação a um nível de outage aceitável.

O modelo propõe ainda um método para o planejamento otimizado das rotas, onde as mesmas são otimizadas no que diz respeito à capacidade geral da rede (isto é, a largura de banda disponível para cada nó sensor). O outage máximo aceitável para qualquer caminho que conecta o nó sensor e o gateway também pode ser definido.

Dada uma determinada topologia, o gateway de destino (opcional, pois a escolha do gateway pode ser automática também), também chamado de Coordenador PAN/Zigbee, os nós que transmitem ao gateway, as distâncias de transmissão (calculada de acordo com o outage máximo informado) e de interferência, e o conjunto das demandas de tráfego requeridas, o algoritmo efetua a construção de um grafo de conectividade dos nós, o cálculo da probabilidade de descarte de pacotes pelo efeito do outage em cada enlace, a identificação

dos caminhos, dos domínios de colisão, e por fim a definição das cargas efetivas dos domínios de colisão, e do cálculo da capacidade da rede para evitar que as cargas admitidas na rede excedam a capacidade máxima dos enlaces sem fio. O algoritmo ainda possui funções de para efetuar engenharia de tráfego através de uma abordagem de otimização com métodos heurísticos para a escolha dos melhores caminhos, porém, este não é foco deste trabalho e não será utilizado.

As próximas seções apresentam o modelo de canal sem fios utilizado nesta proposta com base no modelo de desvanecimento Nakagami-m, o modelo de contenção para redes mesh de sensores, que também leva em conta o outage e, por fim, os algoritmos necessários para utilizar o modelo no planejamento otimizado de rotas em RSSF mesh.

4.2. Modelo de Canal

O modelo de canal sem fios presente neste trabalho é realizado sob a restrição de uma probabilidade de falha (outage) associada a cada enlace. A probabilidade de outage dá uma boa previsão para a taxa de erro de pacote (PER - *Packet Error Rate*) em sistemas de códigos práticos (*practical codes*) [41]. Isso significa que o desempenho de um sistema real de transmissão sem fios empregando códigos práticos, com blocos de tamanhos relativamente pequenos, pode ser bem previsto utilizando o modelo de probabilidade de outage [42].

A distribuição Nakagami-m [43] é utilizada para modelar os efeitos de desvanecimento (*fading*) de múltiplos caminhos em ambiente de propagação sem fios. Este modelo permite ajustar a severidade da atenuação através do parâmetro *m*. Menores valores de *m* ($0.5 \leq m \leq 1$) modelam um canal com propagação sem linha de visão direta entre os nós (*non-line-of-sight* - NLOS). Por outro lado, valores mais elevados de *m* ($m > 1$), representam situações com pelo menos alguma linha de visão (*line-of-sight* - LOS).

Neste trabalho, foi considerado o valor de $m = 2$ e também foi assumido que o canal está em desvanecimento quase-estático (*quasi-static fading)*, o que significa que suas características variam muito lentamente em relação à transmissão e o canal está fortemente correlacionado com o tempo, mantendo-se constante durante a transmissão do bloco de dados. Além disso, assumimos que as transmissões são ortogonais no tempo e que os nós são *half-duplex*.

Conforme a expressão apresentada em [44], para um quadro *s* transmitido a partir do nó *i* para nó *j*, o quadro recebido r_{ij} no nó de destino *j* é dado pela equação 4.1. Na expressão,

P_i é a potência de transmissão, γ_{ij} representa a perda de caminho/percurso (*path loss*) no enlace *i* - *j*, h_{ij} é um escalar que representa a unidade de variação Nakagami-m de desvanecimento quase-estático e n_{ij} representa o vetor de ruído de sinal. O ruído é Aditivo Branco Gaussiano (AWGN - *Additive White Gaussian Noise*) com variância $N_0/2$ por dimensão, onde N_0 é a densidade espectral de potência de ruído térmico em Watts / Hertz.

$$r_{ij} = \sqrt{P_i \gamma_{ij}}\, h_{ij}\, s + n_{ij} \tag{4.1}$$

O ruído térmico tem uma distribuição de amplitude gaussiana no tempo e o comportamento de um ruído branco no domínio da frequência. Como o ruído branco apresenta componentes em todo o espectro de frequência, a densidade espectral de potência desse ruído é independente da frequência e, portanto, tem intensidade muito parecida em todas as frequências.

A perda de percurso/caminho entre *i* e *j*, é dada pela expressão 4.2 (ver [45]), em que d_{ij} é a distância em metros entre os nós *i* e *j*, α é o expoente de perda de percurso, $G = G_{tx}G_{rx}$ é o ganho total das antenas de transmissão e recepção, λ é o comprimento de onda, M_l é a margem do enlace e N_f é a figura de ruído no receptor.

$$\gamma_{ij} = \frac{G\lambda^2}{(4\pi)^2 d_{ij}^{\alpha} M_l N_f} \tag{4.2}$$

A perda de percurso é a relação entre a potência recebida e a potência transmitida para um dado caminho de propagação e é função da distância de propagação. Visto que as perdas por percurso diminuem a relação sinal ruído (SNR), consequentemente a taxa de dados e o alcance do sinal de um determinado sistema de comunicação são limitados. O expoente de perda de percurso determina o quão rápido o sinal decresce com o aumento da distância, logo canais sem fio com menores expoentes de perda de percurso terão áreas de cobertura maior que aqueles com maiores expoentes de perda de percurso. Da mesma forma, a figura de ruído é outra métrica de degradação da relação sinal ruído.

A relação sinal-ruído instantânea (SNR - *Signal-to-Noise Ratio*) no link *i* - *j* é definida de acordo com a equação 4.2, onde $\overline{SNR_{ij}} = (\gamma_{ij} P_i)/N$ e $N = N_0 \cdot B$ é a potência do ruído:

$$SNR_{ij} = \left|h_{ij}\right|^2 \cdot \overline{SNR_{ij}} \quad (4.3)$$

Uma falha (outage) ocorre quando o SNR no nó *j* cai abaixo de um limiar $\beta = 2^{\Delta} - 1$ que permite a decodificação livre de erros [45]. O parâmetro $\Delta = R_b/B$ é a eficiência espectral do sistema e *B* é a largura de banda do sistema em Hertz. No modelo Nakagami-m a probabilidade de outage do enlace *i* - *j* é demonstrada pela expressão 4.4 (ver [46]), sendo Γ(a) e Ψ (a, b) são as funções Gamma completa e incompleta inferior, respectivamente.

$$\mathcal{O}_{ij} = Pr\left[SNR_{ij} < \beta\right] = \frac{\Psi\left(m \cdot \frac{mN\beta}{\gamma_{ij}P_i}\right)}{\Gamma(m)} \quad (4.4)$$

A capacidade do canal sem fio é uma função das deficiências do canal de rádio, como a perda de caminho, desvanecimento/atenuação em pequena escala, sombreamento e ruído térmico. Estes efeitos são bem capturados pelo modelo de probabilidade de falha de canal (outage). Muitos protocolos sem fio suportam o uso de transmissões com confiabilidade. Neste caso, o outage resulta em retransmissão de pacotes, reduzindo ainda mais a capacidade efetiva do canal sem fios. Assumindo um desvanecimento quase-estático, onde o ganho do canal mantém-se aproximadamente constante durante a transmissão de um pacote e muda apenas de uma transmissão para o outra, o número de retransmissões pode ser estimada diretamente a partir da probabilidade de outage. Partindo deste pressuposto, o número médio de vezes, T_{ij}, que um pacote deve ser transmitido pelo nó *i* antes de ser aceito pelo nó *j*, é (ver [47]):

$$T_{ij} = \frac{1}{1 - \mathcal{O}_{ij}} \quad (4.5)$$

4.3. Modelo de Capacidade Baseado em Outage

Nesta seção, apresentamos o modelo de capacidade para RSSFs que utilizam a topologia mesh. O modelo baseia-se nas ideias apresentadas em [07], [08], e aprimorado com o conceito de outage. A solução desenvolvida em [07], consiste em avaliar a capacidade de

rede sem fios em termos de domínios de contenção. Em uma rede com fios, a carga de tráfego de um enlace é simplesmente a soma de todos os fluxos de tráfego cujos caminhos passam pelo enlace. Numa rede sem fios, no entanto, o tráfego transmitido através de um canal sem fio depende do tráfego sendo transportado pelos seus vizinhos que estão no mesmo domínio de contenção. As ideias apresentadas em [07], foram desenvolvidas para o caso particular onde todos os fluxos transportam a mesma quantidade de tráfego. O mesmo conceito foi explorado em [08], porém, este foi generalizado para o caso onde os fluxos pudessem transportar diferentes quantidades de tráfego, e até mesmo ser dividido entre múltiplos caminhos, a fim de proporcionar balanço de carga. O modelo desenvolvido em [08] permite a construção de um modelo de capacidade da rede mesh sem fios como um conjunto de equações. As equações são usadas para formular as restrições de problemas de otimização que determinam a carga máxima de tráfego que pode ser transportada por cada fluxo de acordo com diferentes critérios de otimização.

Semelhante a [07] e [08], o modelo apresentado nesta seção fornece uma estimativa assintótica da capacidade média de transmissão dos nós sem fio. A estimativa fornecida espera aproximar a capacidade média real, se a rede for observada por um longo período. A fim de utilizar o modelo, os seguintes parâmetros de entrada devem ser conhecidos a priori:

- A posição dos nós sensores (x_i, y_i, z_i), definida no plano cartesiano tridimensional, em metros;
- A probabilidade de outage máxima aceitável (*meo – maximum edge outage*) entre nós sensores adjacentes. Esta informação é usada para calcular a distância de transmissão máxima entre nós adjacentes (*mtd – maximum transmission distance*);
- Distância de Interferência (*ID*), definida como a distância máxima a qual uma transmissão de um nó sensor provoca contenção em outros nós, em metros;
- A matriz de tráfego, $TM = \{l_{ij}\}$, definida como um conjunto de fluxos (demanda de tráfego requerida, l_{ij}) entre os nós sensores de origem e o destino, v_i e v_j.

O modelo de capacidade é utilizado de acordo com as 5 etapas definidas na Figura 4.1. Os passos 1 e 2 correspondem à fase de planejamento, e consistem em determinar as rotas (isto é, caminhos), dos fluxos de tráfego transmitidos pelos nós de sensores. O modelo de capacidade é utilizado na fase de validação, de forma a determinar se o planejamento das

rotas é viável. Para o caso particular em que todos os nós sensores transmitem a mesma quantidade de tráfego, é possível utilizar a informação da fase de validação para determinar analiticamente a máxima largura de banda disponível para os nós de sensores, fazendo o uso da abordagem apresentada em [07]. No caso dos nós tiverem requisitos de transmissão distintos, o planejamento e validação devem ser repetidos iterativamente utilizando um algoritmo de otimização, até que uma solução viável seja encontrada, como foi proposto em [08].

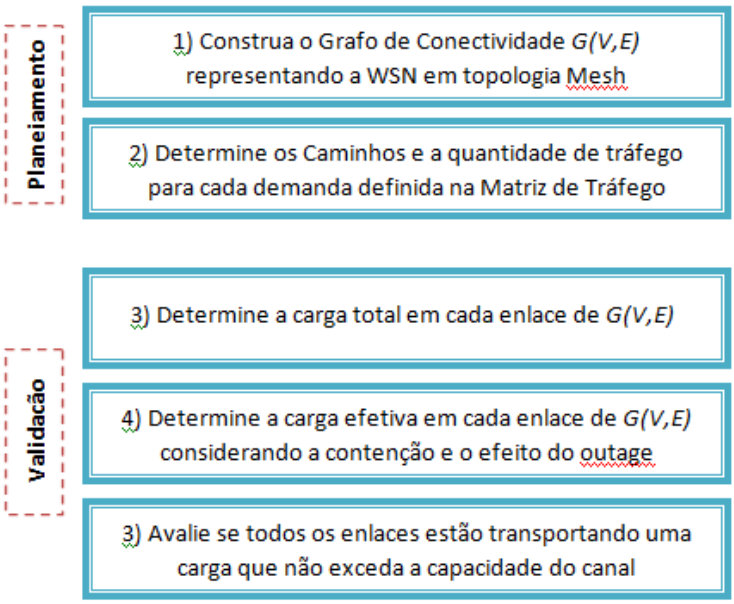

Figura 4.1: Principais etapas do algoritmo de capacidade das WSN

Na etapa 1, o grafo de conectividade *G (V, E)* é representado por um dado conjunto de nós *V* e um conjunto calculado de arestas *E*. O conjunto de arestas (*E*) consiste de todos os pares de nós que possuem valor de distância Euclidiana tridimensional inferior ou igual à distância de transmissão (*mtd*), conforme definido pela equação 4.6. Para o leitor não familiarizado com a sintaxe utilizada, a expressão é interpretada da seguinte forma: O conjunto *E* é formado por um conjunto de pares (v_i e v_j), "tal que" (símbolo "|") cada elemento do par é um vértice "e" (símbolo "∧") as distâncias euclidianas ed_{ij} entre os nós é menor do que *mtd*. O termo *mtd* é uma distância de transmissão d_{ij} obtida através da imposição de um outage máximo $\mathcal{O}_{ij}$ para as equações 4.2 e 4.4, definidas na seção 4.2. O

termo d_{ij} só pode ser determinado numericamente através de um método de pesquisa, pois não pode ser analiticamente isolado nas expressões 4.2 e 4.4.

$$E = \{ (v_i, v_j) \mid v_i, v_j \in V \wedge ed_{ij} \leq mtd \} \quad 4.6$$

onde: $ed_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (z_i - z_j)^2}$

Na etapa 2, são determinados os caminhos que ligam os nós de origem e de destino usando o gráfico *G (V, E)*. Várias estratégias são possíveis para determinar as rotas, de acordo com os limites e critérios de desempenho para as RSSF. Os algoritmos para o planejamento de rotas serão apresentados na seção 4.4. No passo 3, é determinada a carga total de tráfego que atravessa cada aresta (canal sem fio) na WSN. A carga total de tráfego através de uma aresta (v_x, v_y) (TEL_{xy}) é a soma das cargas de todas as demandas que usam este enlace. Assumindo que cada demanda l_{ij} na matriz de tráfego *TM* é atribuída a um caminho $p_{ij} = \{(v_i, v_{\dots}), \dots, (v_{\dots}, v_j)\}$ entre os nós v_i e v_j, então TEL_{xy} pode ser definida por:

$$TEL_{xy} = \sum_{l_{ij} \in TM \wedge (v_x, v_y) \in p_{ij}} l_{ij} \quad 4.7$$

A parte mais importante do algoritmo é realizada na etapa 4. A largura do canal sem fio de uma aresta (v_i, v_j) não é apenas consumida pela carga de tráfego TEL_{ij}, mas também por qualquer outra comunicação realizada no mesmo domínio de interferência. O domínio de interferência $IDVS_i$ de um sensor v_i nó é definido como o conjunto de nós (sensores) que competem pelo mesmo canal de fio, em acordo com o definido na expressão 4.8. É mais usual expressar a competição de um mesmo canal sem fios em termos de arestas (pares de nós / enlaces), ao em vez de nós. Essa é a ideia do conceito de domínio de colisão. Conforme definido por [07] e [06], um domínio de colisão é o conjunto dos nós que devem estar inativos para permitir que um dado nó possa transmitir com êxito. Para identificar o domínio de colisão da comunicação entre os nós v_i e v_j (CDS_{ij}), é necessário identificar primeiramente o conjunto de arestas que estão no mesmo domínio de transmissão de v_i, $(TDES_i)$, de acordo com a expressão 4.9. O *TDES* identifica todas as transmissões possíveis de um nó sensor na WSN. O CDS_{ij} de uma aresta (v_i, v_j) é data pela equação 4.10.

$$IDVS_i = \{ v_j \mid v_j \in V \wedge ed_{ij} \leq ID \} \quad 4.8$$

$$TDES_i = \{ (v_i, v_j) \mid (v_i, v_j) \in E \} \quad 4.9$$

$$CDS_{ij} = \{ TDES_x \mid v_x \in IDV\ S_i \cup IDV\ S_j \} \quad 4.10$$

A carga de tráfego efetiva através de uma aresta (v_i, v_j) deve levar em conta todas as transmissões dentro do mesmo domínio de colisão, e o efeito do outage. Assim, a carga total de tráfego no domínio de colisão de uma aresta (CDL_{ij}) é definida de acordo com a equação 4.11. O CDL_{ij} representa o resultado final do modelo. Na expressão, $\mathcal{O}_{xy}$ representa o outage presente no canal sem fios, entre os nós v_x e v_y. Observe que o uso do outage na expressão é válido somente se a transmissão em cada salto é realizada com confirmação de pacotes (por exemplo, modo ACK habilitado na comunicação Zigbee). Este trabalho sempre considerará esta hipótese.

$$CDL_{ij} = \sum_{(v_i, v_j) \in CDS_{xy}} \frac{TEL_{xy}}{1 - \mathcal{O}_{xy}} \quad 4.11$$

O passo 5 do algoritmo define as condições que permitem determinar se um dado cenário de tráfego é viável. Estas condições podem ser utilizadas como restrições de um problema de otimização, a fim de estimar a capacidade máxima de uma RSSF. As restrições são expressas de acordo com a equação 4.12, onde, *TMT* representa o throughput máximo teórico da tecnologia de sensores, para todos (∀) os enlaces. O *TMT* para a tecnologia Zigbee pode ser considerado com a sobrecarga introduzida pelo protocolo. Há várias referências na literatura que propõe estimativas de *TMT* para o Zigbee (conforme capítulo 3 deste trabalho). Por exemplo, considerando uma WSN ZigBee operando em modo sem beacon, o *TMT* de o canal sem fios pode ser estimado em cerca de 140kbits / s (ver [48]).

$$CDL_{ij} \leq TMT, \forall (v_i, v_j) \in E \quad 4.12$$

4.4. Proposta de Planejamento de Rotas Baseado em Outage

O modelo de capacidade apresentado nesta Seção é genérico, porque nós sensores podem transmitir para qualquer destino, e a quantidade de tráfego transmitida por cada nó pode ser diferente. Nesta seção, vamos assumir hipóteses mais específicas, a fim de simplificar a apresentação dos algoritmos de seleção de rotas e o método para calcular a capacidade máxima de transmissão disponível para os nós sensores. As premissas estão listadas a seguir:

- Todos nós sensores na RSSF transmitem para o mesmo nó de destino, conhecido como Gateway ou Coordenador PAN/Zigbee;
- Um caminho (rota) único e fixo é utilizado para transmitir todo o tráfego entre um nó e o Gateway (isto é, o balanceamento de carga entre múltiplos caminhos não são considerados);
- Todos os nós podem receber a mesma largura de banda para transmitir o tráfego para o Gateway;
- Qualquer nó na WSN pode atuar como um roteador (ou seja, é um dispositivo *Full Function Device* – ver Apêndice A.2) para outros nós;

Como já mencionado anteriormente, se a capacidade de transmissão de todos os nós de sensores é assumida como sendo o mesmo, é possível determinar a esta capacidade analiticamente, uma vez que todos os caminhos interligando os nós a um gateway são conhecidos. Por exemplo, se todas as demandas na matriz de tráfego *TM* forem iguais a uma unidade, isto é, l_{ij} = 1, então a carga de tráfego total de uma aresta, CDL_{ij}, definida na expressão 4.11 da seção 4.3 será determinada numericamente, e a capacidade máxima de transmissão dos nós sensores, l_{max}, poderá ser obtido por:

$$l_{max} = \frac{TMT}{\max\limits_{\forall(v_i,v_j)\in E} CDL_{ij}} \qquad 4.13$$

Na Seção anterior, *mtd* é definida como a distância máxima entre os sensores que podem se comunicar diretamente, sem o auxílio de outro nó agindo como um retransmissor

(ou seja, um roteador). O *mtd* é computado através da imposição de uma probabilidade máxima outage (*meo*) para o grafo de conectividade. A probabilidade de outage de um caminho $p_{ij} = \{(v_i, v_{\dots}), \dots, (v_{\dots}, v_j)\}$, a partir de um nó de origem v_i para o gateway v_j é definida pela expressão 4.14:

$$\mathcal{O}_{ij} = 1 - \prod_{(v_x, v_y) \in p_{ij}} (1 - \mathcal{O}_{xy}) \qquad 4.14$$

Observe que a probabilidade de outage do caminho $\mathcal{O}_{ij}$ pode ser menor do que a probabilidade de outage máximo da aresta (*meo*), pois alguns enlaces do grafo de conectividade podem estar a uma distância mais próxima do que *mtd*. Portanto, o algoritmo de planejamento de roteamento pode controlar o outage do caminho pela seleção de caminhos onde a distância entre os nós adjacentes é pequena. Assim, impondo um pequeno outage de caminho levará a caminhos mais longos em número de saltos e, provavelmente, a uma capacidade de transmissão da rede menor do que seria obtido por uma abordagem de caminho mais curto (*shortest path*). Assim, dependendo dos objetivos de desempenho da aplicação suportada pela WSN, definimos três principais estratégias de planejamento de roteamento, para a escolha do caminho entre um nó sensor e o gateway:

1) Caminho mais curto ponderado (SWP – *Shortest Weighted Path*);

2) Caminho com menor probabilidade de outage (SOP – *Smallest Outage probability Path*);

3) Caminho mais curto em relação ao número de saltos sob um limite máximo de outage (SOL - *Shortest path with respect to the number of hops under a maximum outage limit*).

A estratégia de roteamento SWP consiste em atribuir um peso para as arestas do grafo de conectividade, como uma função da distância dos nós que compõe o enlace, e executar um algoritmo padrão de caminho mais curto (*Shortest Path*) para determinar a melhor rota. Neste método, os pesos das arestas são dimensionados com valor entre 1,0 (aresta com distância mais curta no grafo) e 1,1 (aresta com maior distância no grafo). Usando essa estratégia, a

métrica predominante para determinar o caminho mais curto é o número de saltos. A distância do enlace será usada principalmente como um critério de desempate entre os caminhos com o mesmo número de saltos.

As estratégias de planejamento SOP e SOL são baseados na classificação dos k-menores caminhos candidatos. Para ambos os métodos, primeiramente são determinados os k-caminhos mais curtos no que diz respeito ao número de saltos. Em seguida, a probabilidade de outage do caminho é calculada para cada caminho candidato utilizando a expressão 4.14. Para o método de SOP, o caminho com o menor outage é selecionado. Para o método SOL, todos os caminhos cuja probabilidade de outage ultrapassar um determinado limite são eliminados, e o caminho mais curto remanescente é selecionado.

4.5. Conclusão

Este capítulo apresentou de forma detalhada a estrutura do algoritmo proposto para realizar engenharia de tráfego em redes de sensores mesh sem fio, padrão IEEE 802.15.4. O capítulo descreve de forma genérica e formal o modelo de canal sem fios utilizado em nossa proposta, baseado no modelo de desvanecimento Nakagami-m, Da mesma forma, é apresentado o modelo de contenção para redes mesh de sensores, que também leva em conta o outage. Por fim, são demonstrados os algoritmos necessários para utilizar o modelo no planejamento otimizado de rotas em RSSF mesh, além de propor diferentes estratégias de roteamento, a fim de prever a solução para diferentes situações e cenários de rede.

Capítulo 5

Simulação e Resultados

5.1. Introdução

Neste capítulo, avaliamos a capacidade de RSSF redes mesh, com base no padrão IEEE 802.15.4 [14]. Este capítulo apresenta os resultados teóricos obtidos com o algoritmo proposto no Capítulo 4 e as simulações realizadas com software específico de simulação. Cada etapa proposta para a execução do algoritmo é demonstrada através de um exemplo com um cenário típico, onde é possível demonstrar o efeito do outage na engenharia de tráfico das redes mesh de sensores sem fio para determinar a distribuição das cargas na rede, a identificação dos domínios de colisão, a definição das rotas escolhidas e, por fim o cálculo da capacidade das RSSF.

Primeiramente foram comparadas as estratégias de planejamento de roteamento SWP, SOP e SOL. Em seguida, foram obtidos os resultados em 3 cenários distintos. No primeiro, utilizou-se um cenário de redes mesh, onde todos os nós praticamente participam do mesmo domínio de colisão. O segundo cenário envolve um grid 5x5 gerado aleatoriamente com 25 nós. Por fim, é proposto um grid maior, resultando em vários domínios de colisão e rotas possíveis ao gateway de destino. Nos cenários utilizados, todos os nós da topologia fazem transmissões ao Coordenador PAN que fica em posição mais centralizada.

Os resultados obtidos pelo algoritmo de engenharia de tráfego foram comparados com a simulação, visando identificar se o modelo atende a situações reais, além de tornar possível a verificação de fatores que possam resultar em divergências entre o modelo teórico e a simulação.

5.2. Parâmetros Gerais

A implementação e testes do algoritmo foram realizados com o auxílio do software Wolfram Mathematica 9.0 [49], originalmente concebido por Stephen Wolfram, que disponibiliza diversas bibliotecas prontas, auxiliando na redução dos tempos de implementação. As execuções foram realizadas em uma máquina com Windows 7 32 Bits, 4GB de RAM e processador Intel Core 2 Duo de 2.66GHz.

Os testes foram efetuados com base na norma IEEE 802.15.4. Mais precisamente, os parâmetros do modelo de probabilidade de outage foram ajustados assumindo módulos de rádio 2.4 GHz XBee-Pro DigiMesh [50].

Os parâmetros necessários para calcular a probabilidade de outage, conforme definido no capítulo 4, foram assumidos com os seguintes valores: M_l = 0 dB, N_f = 11.5 dB, G = 4.2 dBi (G_{tx} = G_{rx} = 2.1 dBi), f_c = 2.410 GHz (canal 12); N_0 = -174 dBm/Hz e α = 3. A potência de transmissão dos módulos de rádio é P_i = +10dBm e o limiar de potência de recepção é igual a -100dBm para uma taxa de erro de pacote recebido (PER – *Packet Error Rate*) de 1%. A eficiência espectral do sistema é $\triangle$ = 2 bits/s/Hz.

A Figura 5.1 mostra a probabilidade de falha (outage) esperada para esta configuração. A figura também mostra a distância de interferência (ID), utilizada para determinar o domínio de colisão definido no capítulo 4. Tipicamente, ID é definido como sendo entre duas e três vezes o da distância de transmissão de referência [06], [51]. A distância de transmissão de referência geralmente é calculada com base no limiar de potência recepção do transceptor de rádio (isto é, -100dBm para um 1% PER). Para os parâmetros de canal sem fio assumidos, utilizando o modelo de perda de caminho (*path loss*), estimamos um alcance de transmissão de referência de cerca de 300 m para o rádio XBee-Pro DigiMesh. Na Figura 5.1, a distância de interferência (ID) foi assumida como sendo o dobro do alcance da transmissão de referência (cerca de 600m). Consideramos a distância de interferência como um "limite rígido" para a distância máxima de transmissão (*mtd*). Neste exemplo então, a probabilidade de outage do enlace está limitado a cerca de 25% (como indicado na figura), apesar de ser possível considerar a comunicação a maiores distâncias e altos outages. Em nossos testes consideramos a distância de interferência como sendo o dobro ou o triplo da distância de transmissão, dependendo do cenário.

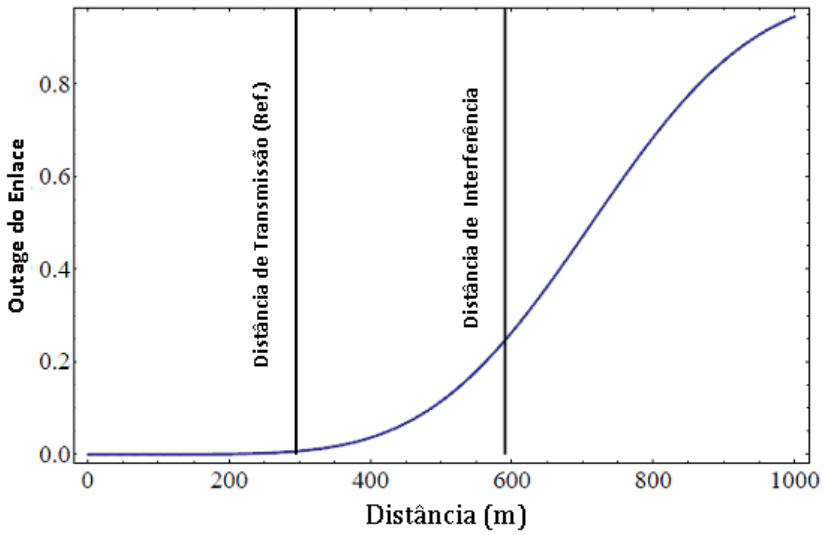

Figura 5.1: Outage em relação à distância entre os nós

As simulações foram realizadas através do software *Network Simulator* versão 2 (*ns-2*) [52], que a partir da versão 2.28 já possui o módulo de sensores 802.15.4 desenvolvido por Zheng e Lee [09]. Além disso, para permitir a escolha dos caminhos definidos pelo algoritmo de engenharia de tráfego, e para aprimorar os resultados, diminuindo tempos de comunicação inicial entre os nós, foram utilizadas rotas estáticas, através do uso do módulo FIXRT, descrito em [53]. No ns-2, as rotas foram definidas manualmente para cada nó, de acordo com as rotas escolhidas e exportadas pelo algoritmo de engenharia de tráfego. O algoritmo define a rota a ser utilizada para cada nó de origem, sendo que desta forma, cada nó de origem possui apenas uma rota a ser seguida.

Outra alteração realizada no simulador foi a implementação do descarte de pacotes devido ao efeito do outage presente em cada enlace. A alteração consiste na leitura de um arquivo contendo uma tabela com as distâncias de cada enlace e suas respectivas probabilidades de descarte devido ao efeito do outage. Esta tabela, assim como com as rotas, também é gerada na execução do algoritmo e exportada em arquivo texto para leitura no ns-2. Desta forma, para cada transmissão que ocorre, o simulador verifica a distância euclidiana entre os nós de origem e destino do enlace e procura no arquivo/tabela qual a probabilidade de outage correspondente a esta distância. A verificação de descarte então é realizada através de um sorteio com distribuição de Bernoulli com probabilidade igual ao outage obtido. Caso o valor do sorteio seja verdadeiro, o pacote então é descartado. Desta forma, quanto maior a probabilidade de outage, maior o número de pacotes descartados devido ao efeito do outage.

O modelo de propagação utilizado é o *TwoRayGround*, considerando todos os nós posicionados em uma área plana. Os parâmetros de ganho e altura das antenas e exponencial de perda de percurso não foram modificados, uma vez que não influenciam diretamente no resultado das simulações aplicadas neste trabalho. Os parâmetros que definem se uma transmissão ocorrerá no ns-2 são os limiares *RXThresh*, *CSThresh* e *CPThresh*, descritos como componentes do *Capture Threshold Model* em [54]. O Receiver Threshold define a distância máxima (na verdade a relação sinal ruído mínima) necessária para que uma recepção de pacote possa ocorrer com sucesso. Neste caso, o *RXThresh* é um limiar de *SNR* calculado a partir da distância dos nós envolvidos na transmissão e de parâmetros de modulação e codificação, seguindo um modelo de propagação definido. O cálculo leva em conta a potência, o ganho das antenas, além de parâmetros de perda de sinal. Desta forma, uma recepção de pacote de um enlace qualquer a uma taxa de transmissão específica é realizada com sucesso se a relação sinal ruído entre o nó transmissor e o receptor for maior ou igual ao definido pelo limiar *RXThresh*, sendo este previamente calculado para uma distância máxima de transmissão desejada. Já o *Carrier Sense Threshold* é um limiar relacionado à distância de interferência, pois indica até onde um nó sente a transmissão de outro, permitindo identificar se o canal está ocupado por atividade em outro nó. Por fim, o *Capture Threshold* é utilizado para determinar colisões de pacote, sendo possível ajustar o quão sensível o receptor será na detecção de colisão e descarte de pacotes, através da comparação do nível do sinal recebido com o limiar máximo permitido. Caso a diferença do sinal de duas transmissões que chegaram ao destino seja menor que o *CPThresh*, uma colisão é identificada e o pacote é descartado. As colisões são tratadas nas simulações de redes 802.15.4 como descarte por *LQI* (*Link Quality Indicator*), ou descarte por baixa qualidade de sinal de transmissão.

Deste modo, os parâmetros *RXThresh* e *CSThresh* foram ajustados de acordo com os valores de distância de transmissão e de interferência, previamente calculados pelo algoritmo executado no Wolfram Mathematica. Já o valor de *CPThresh* foi mantido em 10 dB, sendo este um valor amplamente aceito, porém, é possível ajustar este valor, para que os nós aceitem um número maior ou menor de pacotes, ou até mesmo, aceitar todos os pacotes, simulando uma situação de camada MAC perfeita, sem colisões, o que não é tão factível com situações reais.

Os scripts TCL utilizados foram baseados nos próprios arquivos de exemplo do módulo de sensores 802.15.4, disponíveis por Zheng e Lee. Para fins dos testes e cálculos do

Throughput, foram considerados pacotes com tamanho de 127 Bytes (tamanho máximo permitido no ns-2). Os pacotes de confirmação (ACK) foram utilizados, possibilitando assim a retransmissão de pacotes, limitados ao valor definido no parâmetro *aMaxFrameRetries*, que por padrão é 3 (três) e não foi alterado. Para considerar um número maior de retransmissões, seria necessário ainda alterar parâmetros relacionados ao CSMA, como o número máximo de *backoffs* por exemplo. Os cenários consideram uma rede sem a utilização de Beacons (*non-beacon enable*). Por fim, o modelo de geração de tráfego utilizado é o Poisson, por ser menos determinístico para redes non-mobile [55], o que naturalmente pode provocar colisões por transmissões poderem ocorrer simultaneamente.

Os resultados gerados nos arquivos de *trace* (log da simulação) do ns-2 foram extraídos através de scripts awk. As simulações foram realizadas em uma máquina com Debian 7 Wheezy, 4GB de RAM e processador Intel Core i5-2410M de 2.30GHz.

5.3. Comparação dos Métodos SWP, SOP e SOL

Nesta seção, iremos explorar as três estratégias de planejamento de escolha das rotas, com o intuito de determinar o método mais indicado para cada cenário pretendido. Para estes testes não foi feito o uso de simulação, sendo os resultados gerados apenas através do algoritmo de engenharia de tráfego. A fim de se obter um resultado mais generalista, criamos um gerador de topologia aleatório, onde as posições dos nós sensores foram dispostas em aproximadamente em forma de uma grade (grid). As distâncias verticais e horizontais entre os nós são distribuídas uniformemente entre um intervalo (dx_{min}, dx_{max}). A Figura 5.2 mostra a ilustração de uma topologia gerada com os nós espaçados a uma distância entre 250 e 375 metros. Os nós estão interligados por arestas (enlaces) quando eles estão dentro da distância de transmissão. O círculo ilustra a distância de interferência do nó 45 (um candidato a ser gateway), considerando a distância de interferência como sendo o dobro da distância de transmissão de referência, valor que será considerado para os testes desta seção.

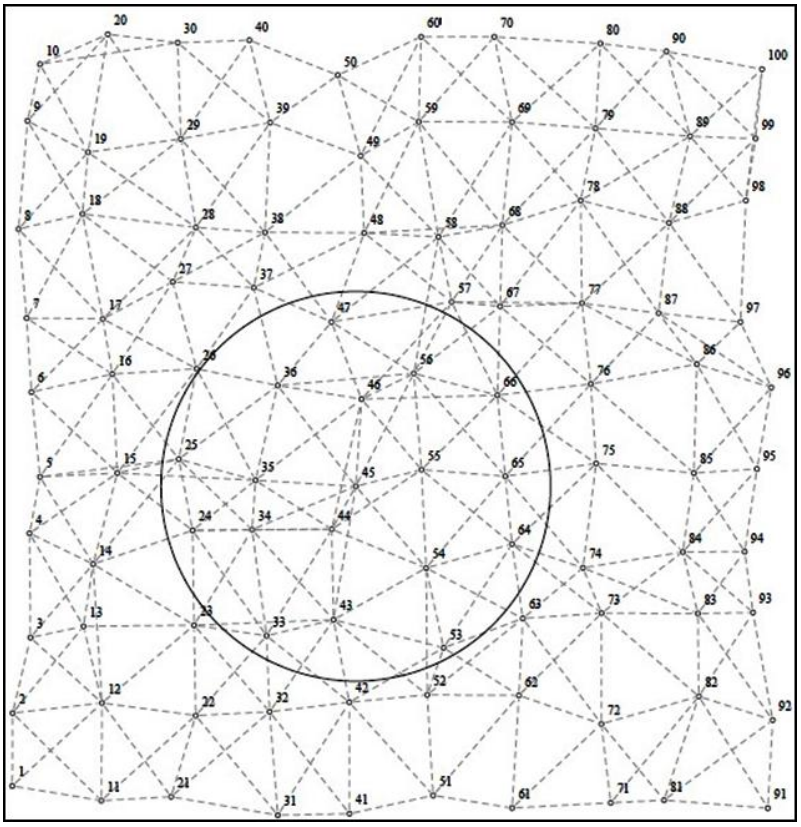

Figura 5.2: Grafo de conectividade com 5% de probabilidade de outage.

Para o cenário de grid, as Figuras 5.3 a 5.5 mostram o desempenho da rede obtido pelos métodos SWP, SOP e SOL, respectivamente. A linha contínua nas figuras representa o valor médio obtido com 30 topologias aleatórias de grid, e as linhas verticais representam o intervalo de confiança de 95% para esses resultados. As topologias aleatórias de grade têm 100 nós sensores, e o nó 45 foi escolhido como gateway, tal como indicado na Figura 5.2. Os gráficos de cima nas Figuras representam uma "capacidade normalizada", que indica a capacidade obtida com um outage maior em relação à obtida usando a distância de transmissão de referência (cerca de 1% de PER), como indicado pelo fabricante. Os gráficos inferiores nas figuras representam o outage de caminho médio de todos nós sensores.

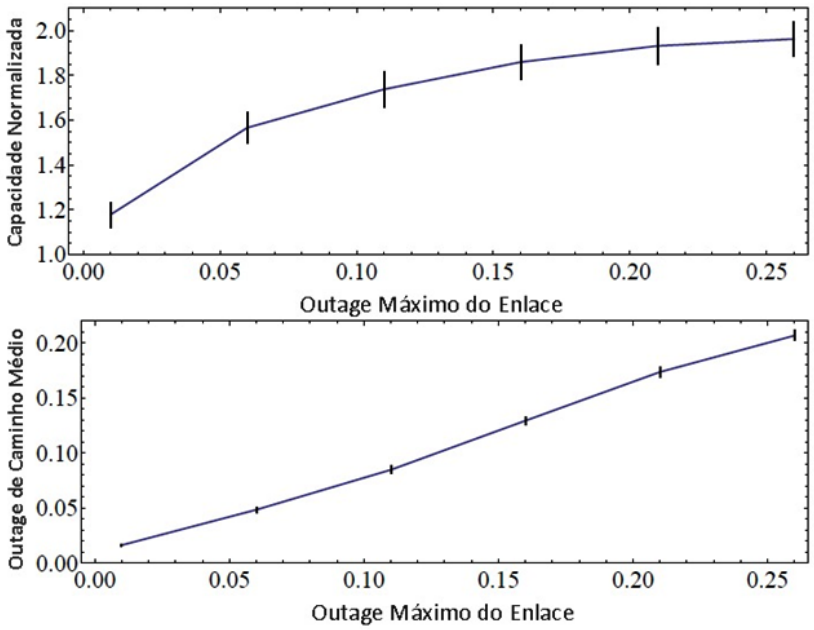

Figura 5.3: Resultados obtidos com o método SWP

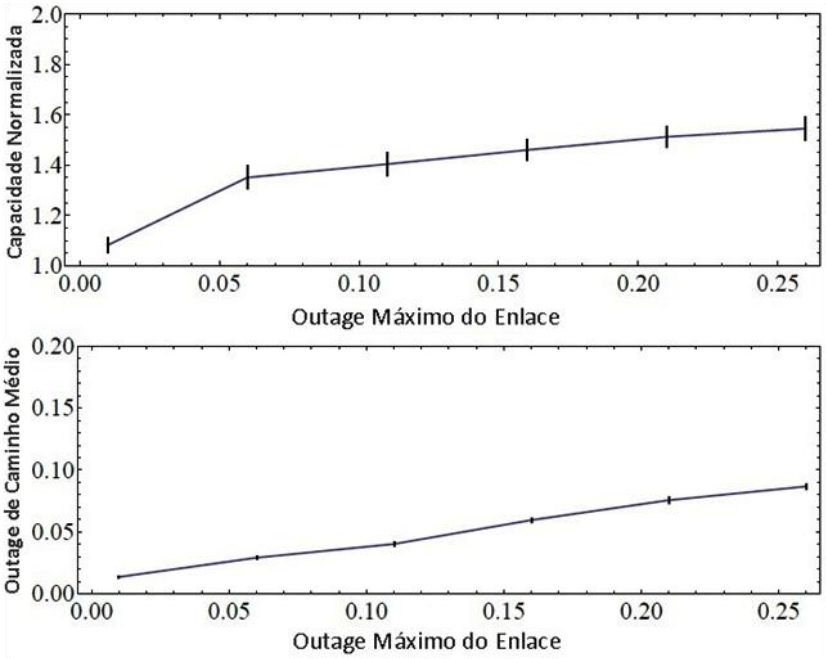

Figura 5.4: Resultados obtidos com o método SOP

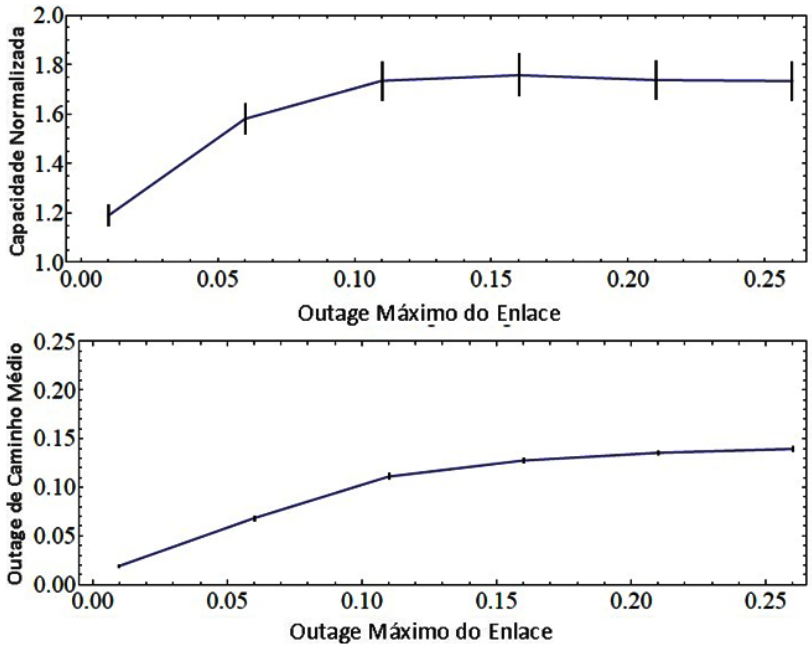

Figura 5.5: Resultados obtidos com o método SOL

A capacidade mais alta foi obtida com o método SWP, podendo atingir quase o dobro da capacidade obtida através do planejamento de rotas limitada pela distância de transmissão de referência. Neste caso, a probabilidade média de outage dos caminhos é também muito elevada. Isto indica que se o atraso imposto pelo alto PER não é um problema, reduzir o número de vezes que um pacote é repetido pelas rotas melhora a capacidade geral da rede. Utilizando o método SOP, o outage de caminho é limitado a 5% no pior cenário, mas o ganho de capacidade em relação à distância de transmissão de referência é de aproximadamente 40%. Finalmente, o método SOL apresenta um resultado intermediário, obtido pela imposição de uma probabilidade de outage de caminho inferior a 15% para todos os caminhos.

As próximas seções deste capítulo contém os resultados teórico e simulado em 3 cenários distintos. Considerando os resultados acima apresentados, os próximos testes foram realizados considerando o método SWP, sendo que os resultados teóricos obtidos foram comparados com os resultados alcançados através de simulação com o ns-2.

5.4. Avaliações com Simulação - Cenário 1

O primeiro cenário é composto por 18 nós, sendo o nó 8 definido como Sink/Coordenador PAN e os demais como roteadores que além de encaminhar pacotes, também efetuam transmissões ao Coordenador.

5.4.1. Execução do Algoritmo de Engenharia de Tráfego

Nos resultados obtidos neste cenário, os seguintes parâmetros de entrada do algoritmo foram utilizados, conforme Tabela 5.1.

Parâmetro	Valor
Gateway/Sink/Coordenador	{8}
Outage Máximo Permitido	0.02, 0.05, 0.08, 0.11, 0.14, 0.17, 0.21, 0.24, 0.27 e 0.30 (2%, 5%, 8%, 11%, 14%, 17%, 21%, 24%, 27% e 30%)
Distância de Interferência	3 * distância de transmissão
Vértices (posição dos nós em metros)	{{435, 845}, {406, 598}, {539, 390}, {779, 322}, {630,1000}, {855, 900}, {1000, 1090}, {1000, 750}, {1200,1100}, {1200, 700}, {1300, 900}, {1440, 1000}, {1545,820}, {1425, 610}, {870, 552}, {1029, 366}, {1272,310}, {1490, 410}}

Tabela 5.1: Parâmetros de entrada

A execução do algoritmo, além de exibir os resultados teóricos de desempenho da rede para o experimento, fornece também os parâmetros necessários para a simulação, tais como: distância de transmissão e interferência, rotas utilizadas de acordo com o nível de outage máximo permitido por enlace, e o percentual de outage calculado para cada enlace, de acordo com a sua distância. A distância de transmissão é calculada pelo algoritmo baseado no outage passado como parâmetro. Utilizou-se a distância de interferência 3 (três) vezes maior que a distância de transmissão, valor aceito para redes sem fio e suficiente para deixar quase todos os nós dentro do mesmo domínio de colisão, um dos objetivos deste cenário.

Para cada outage máximo escolhido, o algoritmo determina a distância de transmissão e quais os enlaces possíveis dentro da topologia. A partir destes enlaces, é gerada a tabela que relaciona cada enlace, a distância entre o par de nós e seu percentual de outage. A Tabela 5.2 representa esta situação esta situação para os nós 1 e 2, considerando o outage máximo de 30% por enlace, situação que gera enlaces entre uma boa parte dos nós da topologia. A tabela completa é apresentada no Apêndice B, Tabela B.1.

Enlace	Distância / Outage
1-2	{248.697,0.00240556}
1-3	{466.734,0.08108}
1-5	{249.098,0.00242841}

1-6	{423.586,0.0488942}
1-7	{615.833,0.293029}
1-8	{572.931,0.215942}
1-15	{524.475,0.14411}
2-3	{246.887,0.00230475}
2-4	{464.01,0.0786917}
2-5	{460.196,0.0754328}
2-6	{541.115,0.166835}
2-8	{613.139,0.28786}
2-15	{466.275,0.0806734}

Tabela 5.2: Percentual de outage em função da distância dos enlaces

Quanto maior o nível de outage permitido, maior é a conectividade entre enlaces distantes. Desta forma, para níveis de outage mais baixos que 30%, esta mesma tabela poderá ser utilizada, uma vez que o número de enlaces será menor ou igual ao atual e todos os enlaces já existirão na tabela acima. O mesmo não acontece quando o outage for maior, pois novos enlaces poderão ser descobertos e os mesmos não constarão na tabela acima.

O algoritmo fornece ainda as rotas escolhidas para cada nó de origem. As Tabelas 5.3 e 5.4 demonstram as rotas escolhidas de acordo com o nível máximo de outage escolhido:

Outage 2%	Outage 5%	Outage 8%	Outage 11%	Outage 14%
{1-5,5-6,6-8}	{1-6,6-8}	{1-5,5-8}	{1-5,5-8}	{1-5,5-8}
{2-1,1-5,5-6,6-8}	{2-1,1-6,6-8}	{2-5,5-8}	{2-4,4-8}	{2-4,4-8}
{3-4,4-15,15-8}	{3-15,15-8}	{3-15,15-8}	{3-4,4-8}	{3-4,4-8}
{4-15,15-8}	{4-15,15-8}	{4-15,15-8}	{4-8}	{4-8}
{5-6,6-8}	{5-6,6-8}	{5-8}	{5-8}	{5-8}
{6-8}	{6-8}	{6-8}	{6-8}	{6-8}
{7-8}	{7-8}	{7-8}	{7-8}	{7-8}
{9-7,7-8}	{9-8}	{9-8}	{9-8}	{9-8}
{10-8}	{10-8}	{10-8}	{10-8}	{10-8}
{11-8}	{11-8}	{11-8}	{11-8}	{11-8}
{12-11,11-8}	{12-9,9-8}	{12-7,7-8}	{12-7,7-8}	{12-8}
{13-11,11-8}	{13-10,10-8}	{13-9,9-8}	{13-9,9-8}	{13-9,9-8}
{14-10,10-8}	{14-10,10-8}	{14-8}	{14-8}	{14-8}
{15-8}	{15-8}	{15-8}	{15-8}	{15-8}
{16-15,15-8}	{16-8}	{16-8}	{16-8}	{16-8}
{17-14,14-10,10-8}	{17-10,10-8}	{17-10,10-8}	{17-4,4-8}	{17-8}
{18-14,14-10,10-8}	{18-10,10-8}	{18-10,10-8}	{18-10,10-8}	{18-10,10-8}

Tabela 5.3: Rotas escolhidas em função do percentual de outage

Outage 17%	Outage 21%	Outage 24%	Outage 27%	Outage 30%
{1-5,5-8}	{1-5,5-8}	{1-8}	{1-8}	{1-8}
{2-4,4-8}	{2-4,4-8}	{2-1,1-8}	{2-1,1-8}	{2-8}
{3-4,4-8}	{3-4,4-8}	{3-8}	{3-8}	{3-8}
{4-8}	{4-8}	{4-8}	{4-8}	{4-8}
{5-8}	{5-8}	{5-8}	{5-8}	{5-8}
{6-8}	{6-8}	{6-8}	{6-8}	{6-8}
{7-8}	{7-8}	{7-8}	{7-8}	{7-8}
{9-8}	{9-8}	{9-8}	{9-8}	{9-8}
{10-8}	{10-8}	{10-8}	{10-8}	{10-8}
{11-8}	{11-8}	{11-8}	{11-8}	{11-8}
{12-8}	{12-8}	{12-8}	{12-8}	{12-8}
{13-9,9-8}	{13-8}	{13-8}	{13-8}	{13-8}
{14-8}	{14-8}	{14-8}	{14-8}	{14-8}
{15-8}	{15-8}	{15-8}	{15-8}	{15-8}
{16-8}	{16-8}	{16-8}	{16-8}	{16-8}
{17-8}	{17-8}	{17-8}	{17-8}	{17-8}
{18-10,10-8}	{18-10,10-8}	{18-10,10-8}	{18-8}	{18-8}

Tabela 5.4: Rotas escolhidas em função do percentual de outage

É possível claramente verificar que quanto maior o nível de outage aceitável, menos saltos ocorrem entre os nós de origem e o gateway. Isto por que ao aceitar um outage maior, a distância de transmissão também será maior, resultado na comunicação direta entre nós distantes, antes inalcançáveis. As Figuras 5.6 e 5.7 demonstram a topologia deste cenário com todos os enlaces possíveis (linhas tracejadas e linhas coloridas), além das rotas escolhidas (linhas coloridas apenas), considerando um outage máximo de 2% e de 30% respectivamente.

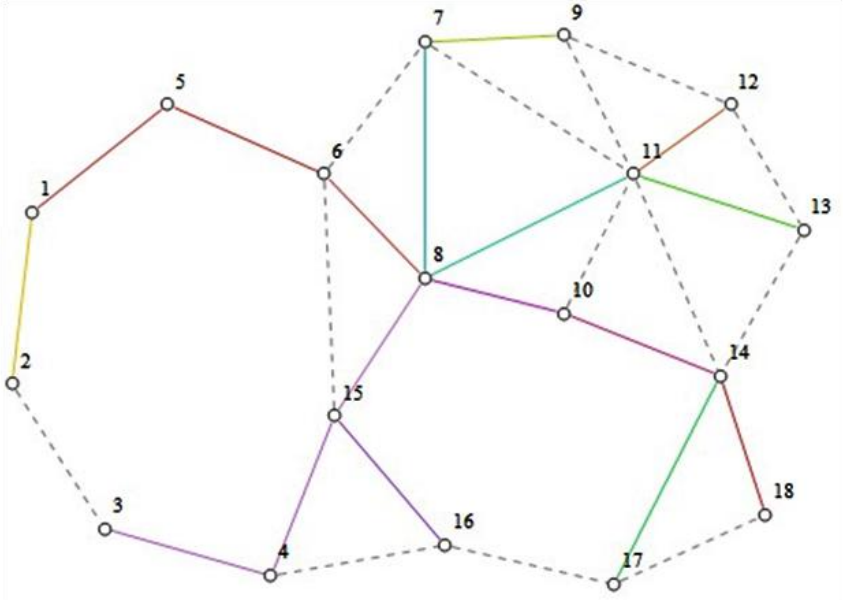

Figura 5.6: Enlaces e rotas escolhidas – Outage 2%

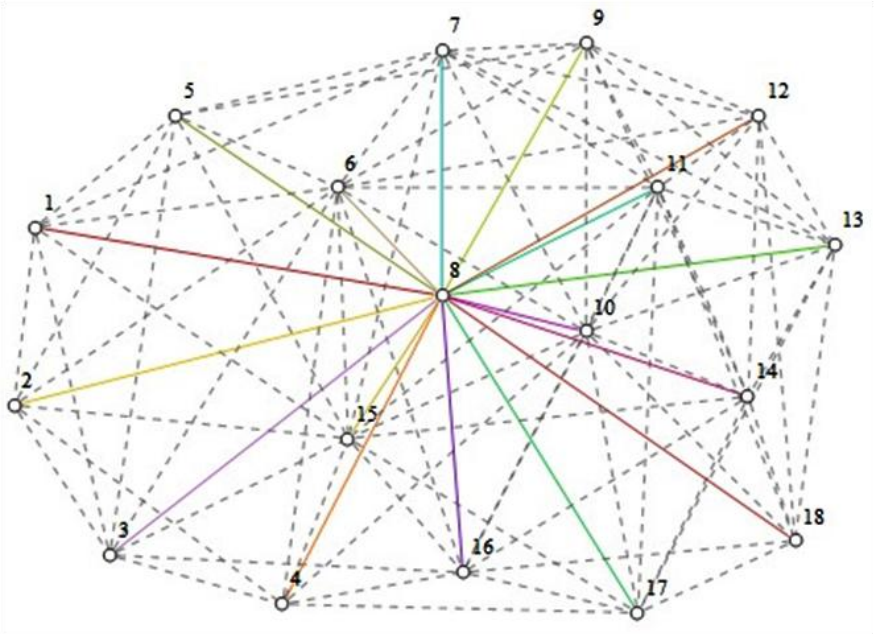

Figura 5.7: Enlaces e rotas escolhidas – Outage 30%

É possível constatar, portanto, que a quantidade de enlaces e caminhos possíveis aumenta consideravelmente de acordo com o perceitual de outage máximo aceito na rede para o cenário proposto. Para um outage máximo de 2%, o nó 2 precisa efetuar 4 saltos para chegar ao gateway de destino, enquanto que com um outage de 30%, todos os nós, inclusive o 2, efetuam a transmissão direta ao gateway com um salto apenas.

Através das informações disponibilizadas é possível efetuar as simulações para o mesmo cenário.

5.4.2. Simulação

Com as informações detalhadas no item anterior, juntamente com as distâncias de transmissão calculadas para cada caso e a definição dos intervalos entre pacotes (taxa de pacotes por segundo) com distribuição Poisson, é possível realizar simulações no ns-2 para determinar o desempenho das redes zigbee. As rotas foram fixadas de acordo com as Tabelas 5.3 e 5.4. Já o arquivo com níveis de outage em função da distância foi gerado extraindo as informações de distância e outage da Tabela 5.2. Os nós foram posicionados com as mesmas coordenadas X e Y da Tabela 5.1. Por fim, os demais parâmetros foram definidos em consonância com a Tabela 5.5 abaixo.

Parâmetros (Outage: 0.02)	**Valor**
RXThresh_ (359,602m)	8.5325e-011
Intervalo entre Pacotes (Algoritmo)	0,285561708
Intervalo entre Pacotes (Max)	0,13
Parâmetros (Outage: 0.05)	**Valor**
RXThresh_ (425,372m)	4.35802e-011
Intervalo entre Pacotes (Algoritmo)	0,230742
Intervalo entre Pacotes (Max)	0,11
Parâmetros (Outage: 0.08)	**Valor**
RXThresh_ (465,509m)	3.03845e-011
Intervalo entre Pacotes (Algoritmo)	0,209505092
Intervalo entre Pacotes (Max)	0,1
Parâmetros (Outage: 0.11)	**Valor**
RXThresh_ (496m)	2.35743e-011
Intervalo entre Pacotes (Algoritmo)	0,204623
Intervalo entre Pacotes (Max)	0,11
Parâmetros (Outage: 0.14)	**Valor**
RXThresh_ (521,293m)	1.93213e-011
Intervalo entre Pacotes (Algoritmo)	0,188231
Intervalo entre Pacotes (Max)	0,1
Parâmetros (Outage: 0.17)	**Valor**
RXThresh_ (543,319m)	1.63736e-011
Intervalo entre Pacotes (Algoritmo)	0,188231
Intervalo entre Pacotes (Max)	0,09

Parâmetros (Outage: 0.21)	**Valor**
RXThresh_ (569,317m)	1.35815e-011
Intervalo entre Pacotes (Algoritmo)	0,181013
Intervalo entre Pacotes (Max)	0,08
Parâmetros (Outage: 0.24)	**Valor**
RXThresh_ (587,043m)	1.20139e-011
Intervalo entre Pacotes (Algoritmo)	0,168765
Intervalo entre Pacotes (Max)	0,08
Parâmetros (Outage: 0.27)	**Valor**
RXThresh_ (603,662m)	1.07446e-011
Intervalo entre Pacotes (Algoritmo)	0,163089
Intervalo entre Pacotes (Max)	0,1
Parâmetros (Outage: 0.30)	**Valor**
RXThresh_ (619,432m)	9.69148e-012
Intervalo entre Pacotes (Algoritmo)	0,155988276
Intervalo entre Pacotes (Max)	0,08

Tabela 5.5: Parâmetros da simulação

Os limiares RXThresh e CSThresh foram obtidos com ajuda do programa threshold, disponível no próprio suíte de aplicativos do ns-2, acessível em indep-utils → propagation, onde são passados como parâmetros o modelo de propagação, a potência e a distância. O limiar RXThresh foi definido de acordo com a distância de transmissão calculada pelo algoritmo, enquanto CSThresh foi configurado em acordo com a distância de interferência.

É possível ainda verificar a presença de 2 intervalos, utilizados para definir a taxa de pacotes enviados por segundo em cada nó da simulação. O primeiro intervalo de pacotes Poisson define a taxa de pacotes por segundo em acordo com o nosso modelo proposto, calculado em função do throughput obtido pela execução do algoritmo, convertido para o formato de intervalo entre pacotes por segundo. O segundo é o ajuste deste intervalo, a fim de se obter o máximo throughput possível na simulação. Para isto, tentou-se tanto aumentar o intervalo (diminuindo a taxa de pacotes, ou seja, injetando menos pacotes na rede, tornando-a menos congestionada e com menos colisões) como diminuí-lo, aumentando a média Poisson de pacotes. Em todos os casos, a diminuição do intervalo mostrou-se mais eficaz, o que demonstra que mesmo com o aumento da saturação, tornando a rede mais congestionada e

com maior descarte de pacotes, o aproveitamento de todos os espaços de tempo foi o fator que contribuiu para o maior throughput da rede.

5.4.3. Resultados

Os testes contemplam a obtenção do desempenho teórico estimado da rede, e o desempenho simulado através do ns-2, dentro dos diferentes níveis de outage considerados. O throughput teórico é calculado pelo algoritmo de engenharia de tráfego, conforme apresentado no capítulo 4. Já o throughput simulado é obtido através da leitura do arquivo de trace (log de simulação) do ns-2, com a extração pacotes transmitidos pelos nós de origem e pelos pacotes recebidos pelo gateway de destino. O throughput total da rede nada mais é que a soma de todos os pacotes recebidos, multiplicado pelo seu tamanho (127 bytes, ou 1016 bits) e dividido pelo tempo total da simulação, considerando o momento da primeira transmissão de um pacote de dados como tempo inicial da simulação.

A Figura 5.8 mostra o throughput obtido por nó, em função do outage. A linha vermelha demonstra o throughput obtido pelo modelo teórico de engenharia de tráfego proposto neste trabalho. A linha azul representa o throughput médio por nó obtido na simulação, enquanto a linha verde representa o throughput máximo simulado, após testes de execução com diferentes taxas de envio de pacotes (*packet rate*). Os melhores resultados foram sempre obtidos aumentando a taxa de pacotes. A Figura 5.9 mostra o mesmo gráfico, porém com o throughput total da rede.

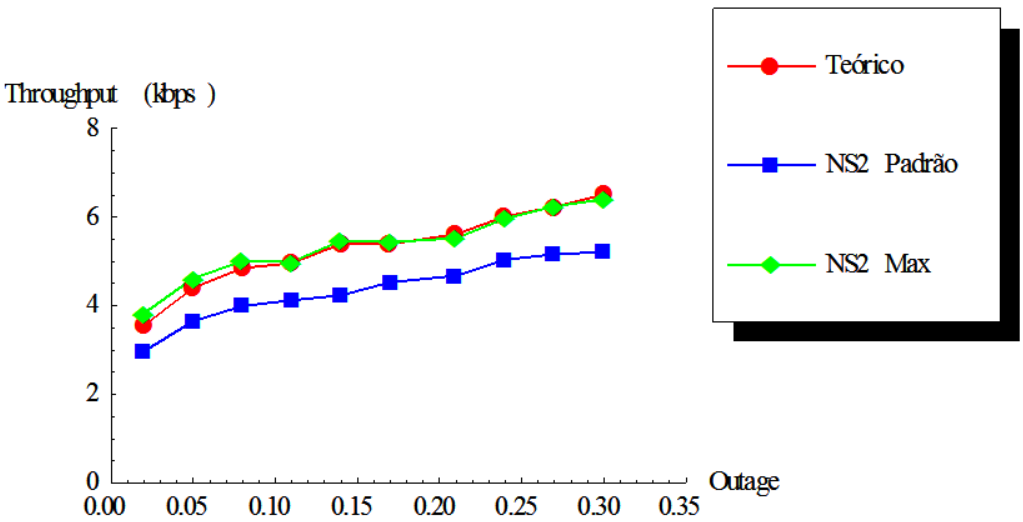

Figura 5.8: Throughput (nó) em função do outage

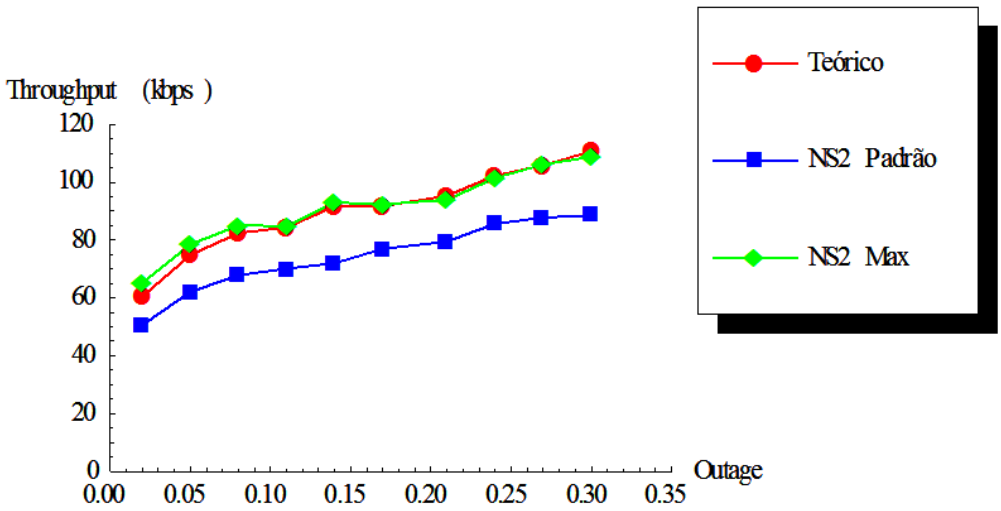

Figura 5.9: Throughput (Total) em função do outage

Os gráficos do cenário 1 mostram que mesmo com níveis altos de outage (24%, 27% e 30%), o throughput foi maior que o obtido com outages menores (2%, 5%, 8%). Isto significa que apesar da maior quantidade de descartes devido ao efeito do outage, ainda assim esta situação torna-se vantajosa, devido à possibilidade de transmissões com menos saltos entres os nós de origem e o gateway de destino.

Além disso, os valores teóricos e simuladores foram muito próximos, especialmente se considerar o throughput máximo simulado, o que valida o modelo para o cenário proposto. A melhor situação encontrada foi onde todos os nós transmitiam diretamente ao gateway em um único salto (30% de outage máximo permitido na rede).

Constata-se ainda uma diferença aceitável entre os valores simulados com taxa de pacotes definido conforme o modelo teórico e os valores máximos atingidos na simulação (Max), mostrando que a taxa de pacotes calculada pelo modelo teórico mostrou-se adequada para ser utilizada nos outros testes. É importante frisar que os valores máximos foram atingidos com menores intervalos entre pacotes, acarretando na injeção excessiva de pacotes, onde embora seja atingido um throughput maior, também resultou em uma baixa taxa de entrega de pacotes ao destino (*packet ratio*), conforme é possível verificar no gráfico da Figura 5.10, não sendo ideal para muitas situações reais.

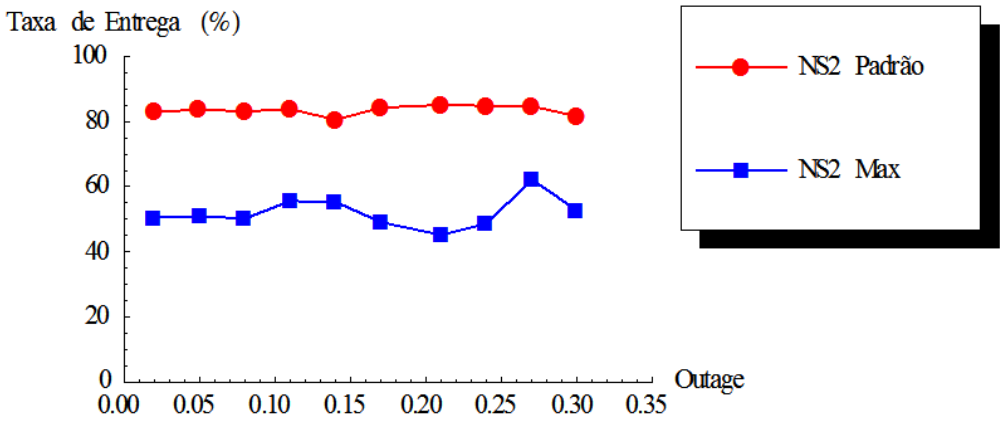

Figura 5.10: Taxa de entrega em função do outage

5.5. Avaliações com Simulação - Cenário 2

O segundo cenário é composto por um grid (5x5) de 25 nós, sendo o nó 13 definido como Sink/Coordenador PAN. Utilizou-se neste caso uma distância média de 600 metros entre nós vizinhos, para uma distância de interferência de 3 vezes a distância de transmissão, a fim de se obter em cenário com alguns domínios de colisão e a obrigatoriedade de um alto nível de outage para que a haja comunicação por parte de todos os nós que compõe o grid. A Figura 5.11 mostra a topologia e os nós que compõe o domínio de colisão (12 → 13), enquanto a Figura 5.12 mostra as rotas definidas pelo algoritmo de engenharia de tráfego, ambas para um outage máximo de 50%.

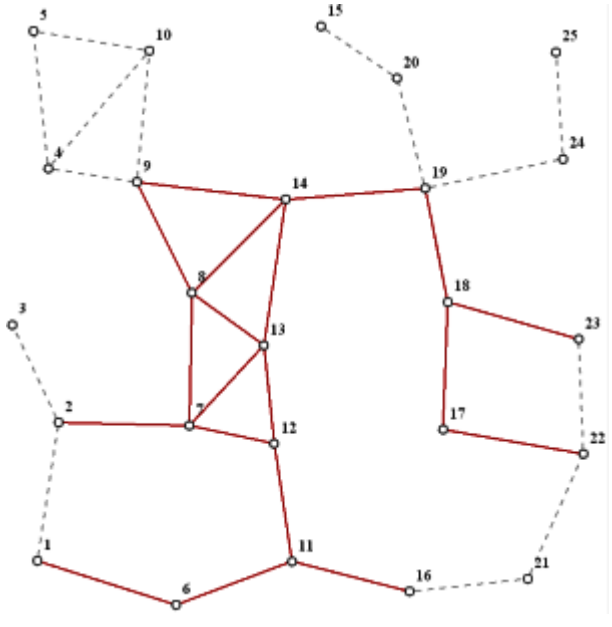

Figura 5.11: Topologia e domínio de colisão

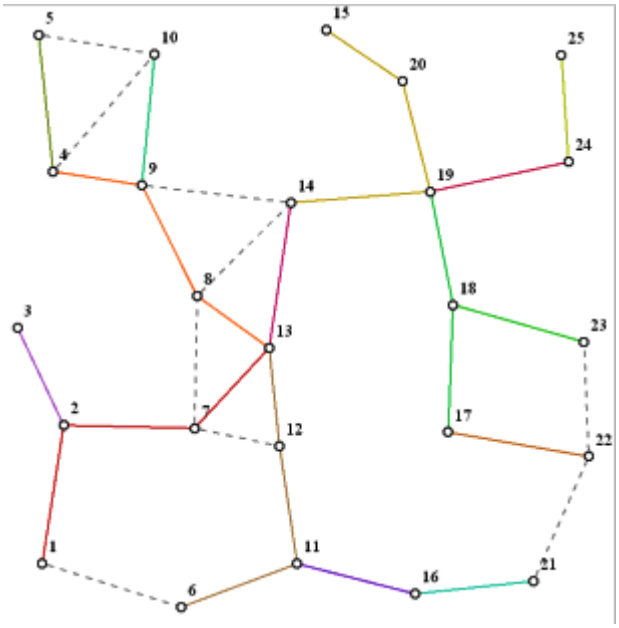

Figura 5.12: Rotas escolhidas (algoritmo)

Devido à maior distância entre os nós vizinhos, a utilização de um alto nível de outage não foi suficiente para se obtiver vários caminhos, como no cenário anterior. Desta forma, espera-se menor diferença no throughput final da rede em função do outage, uma vez que a quantidade de enlaces muda menos neste cenário.

5.5.1. Execução do Algoritmo de Engenharia de Tráfego

Os seguintes parâmetros de entrada do algoritmo foram definidos conforme a Tabela 5.6. Do mesmo modo que no cenário 1, foram geradas informações com as rotas e percentuais de outage de cada enlace para uso no simulador.

Parâmetro	Valor
Gateway/Sink/Coordenador	{13}
Outage Máximo Permitido	0.35, 0.40, 0.45, 0.50, 0.60
Distância de Interferência (metros)	3 * distância de transmissão
Vértices (posição dos nós em metros)	{{186.215,270.398},{283.222,897.271}, {73.017,1340.97},{235.758,2049.2}, {169.199,2670.8},{816.745,71.3142}, {878.035,883.654},{889.56,1483.8}, {638.339,1986.7},{696.354,2582.03}, {1344.06,268.572},{1263.93,802.362}, {1216.76,1248.1},{1315.58,1907.68}, {1475.44,2691.94},{1879.02,131.787},

	{2030.17,865.878},{2051.88,1444.31}, {1949.6,1958.14},{1822.16,2458.11}, {2417.,189.466},{2668.29,755.339}, {2647.16,1275.65},{2576.84,2092.4}, {2544.44,2576.64}}

Tabela 5.6: Parâmetros de entrada

5.5.2. Simulação e Resultados

Em virtude da maior distância entre os nós, níveis maiores de outage são necessários para que aja conectividade de todos os nós do grid, permitindo assim um nível de potência de transmissão dos nós mais alto também. Para fins desta simulação, o limiar RXThresh_ foi ajustado para os seguintes valores, de acordo com o outage: 644.327, 668.03, 691.02 e 713.684 metros. Todos são valores relativamente próximos da distância de interferência, de aproximadamente 900 metros, valor este definido para o limiar CSThresh_.

A Tabela 5.7 demonstra os níveis totais de outage em cada caminho (soma das probabilidades de outage de todos os enlaces que compõe o caminho) para um outage máximo de 50% por enlace. É possível verificar um grande impacto do outage neste caso, chegando a até quase 83% de probabilidade de descarte dos pacotes, o que reduz drasticamente o throughput a ser provisionado neste cenário pelo modelo teórico.

{1-2,2-7,7-13}	**0.555784**
{2-7,7-13}	**0.337409**
{3-2,2-7,7-13}	**0.406715**
{4-9,9-8,8-13}	**0.259211**
{5-4,4-9,9-8,8-13}	**0.489761**
{6-11,11-12,12-13}	**0.375791**
{7-13}	**0.111702**
{8-13}	**0.0375522**
{9-8,8-13}	**0.228596**
{10-9,9-8,8-13}	**0.429051**
{11-12,12-13}	**0.219897**
{12-13}	**0.0658308**
{14-13}	**0.397664**
{15-20,20-19,19-14,14-13}	**0.667689**

{16-11,11-12,12-13}	0.36271
{17-18,18-19,19-14,14-13}	0.733572
{18-19,19-14,14-13}	0.655845
{19-14,14-13}	0.598242
{20-19,19-14,14-13}	0.651786
{21-16,16-11,11-12,12-13}	0.468986
{22-17,17-18,18-19,19-14,14-13}	0.828642
{23-18,18-19,19-14,14-13}	0.758609
{24-19,19-14,14-13}	0.736476
{25-24,24-19,19-14,14-13}	0.762497

Tabela 5.7: Outage total das rotas

Os resultados são apresentados na Figura 5.13 e na Tabela 5.8. O throughput simulado médio, utilizando a taxa de pacotes prevista pelo modelo teórico, foi aproximadamente 30% menor que o throughput teórico calculado pelo nosso modelo, com uma taxa de entrega de 70%. Análises no arquivo de trace levaram à conclusão de que a razão para este resultado está principalmente devido a dois fatores: 1) o descarte devido ao efeito do outage; 2) na colisão de pacotes devido ao uso da geração de tráfego com distribuição de Poisson, que naturalmente provoca transmissões aleatórias muito próximas, resultando na colisão.

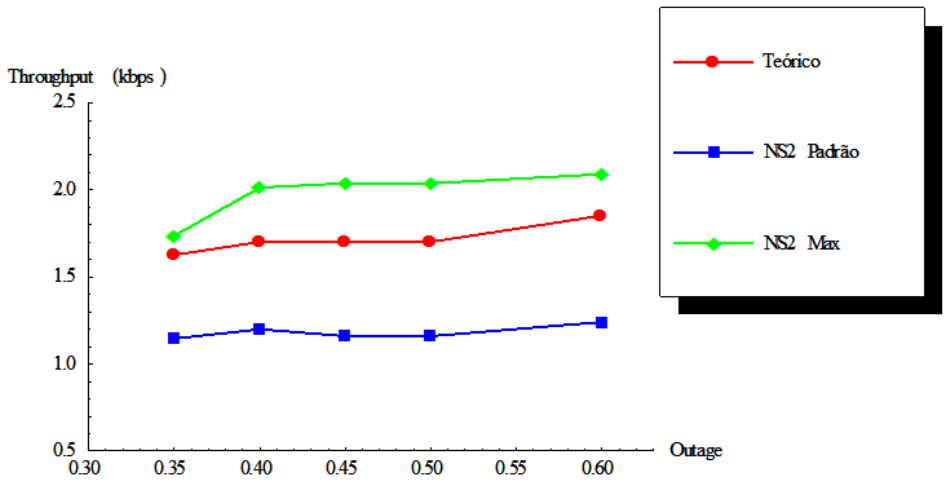

Figura 5.13: Resultados teórico e simulado

Métrica	Outage 35%	Outage 40%	Outage 45%	Outage 50%	Outage 60%
Throughput Máximo Teórico	39,05 kbps	40,84 kbps	40,84 kbps	40,84 kbps	44,49 kbps
Throughput Simulado	27,51 kbps	28,68 kbps	27,85 kbps	28,85 kbps	29,80 kbps
Throughput Simulado (Max)	40,45 kbps	48,33 kbps	48,92 kbps	48,92 kbps	50,20 kbps

Tabela 5.8: Resultados teórico e simulado (Total)

Chamou a atenção também o fato de que foi possível novamente obter um throughput até mesmo superior ao teórico, ao diminuir consideravelmente o intervalo entre pacotes Poisson, o que indica que para alguns casos, a capacidade da rede em uma situação com uma camada MAC perfeita e sem colisões é maior que o previsto pelo nosso modelo. Mais uma vez é possível concluir que este ganho é muito custoso e impraticável em situações reais, devido à baixa taxa de entrega de pacotes (chegando a apenas 21%), como mostra a Figura 5.14, ou seja, uma rede com uma grande quantidade de pacotes descartados e pouco efetiva, onde quanto mais nós a rede tiver, menor a taxa de entrega e maior a probabilidade de colisões. Por outro lado, a taxa de entrega foi aceitável ao se utilizar a taxa de pacotes sugerida pelo algoritmo.

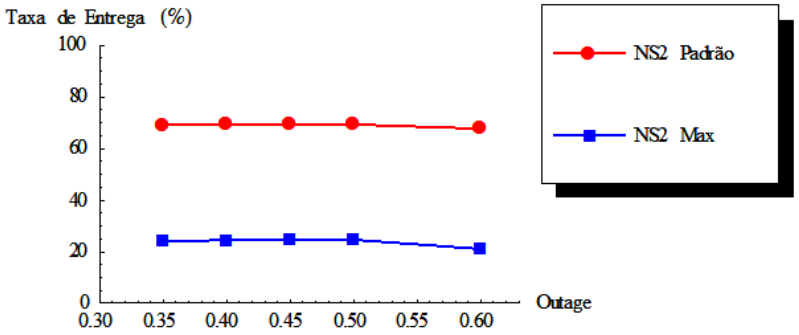

Figura 5.14: Taxa de Entrega (*Packet Ratio*)

5.6. Avaliações com Simulação - Cenário 3

Neste cenário, propomos um grid com 100 nós (10x10) de acordo com a Figura 5.15, sendo o nó 55 do gateway da topologia. Na geração aleatória do grid, considerou-se uma distância média entre os nós de 350 metros, com até 50% de deslocado randômico do nó em relação à sua posição de origem. Neste cenário, o tempo de convergência de execução do algoritmo e da simulação é muito maior. Deste modo, foram definidos 4 pontos de coleta

(outages máximos de 10%, 15%, 23% e 30%) A distância de interferência é o triplo da distância de transmissão, resultado ainda assim, vários domínios de colisão para este cenário.

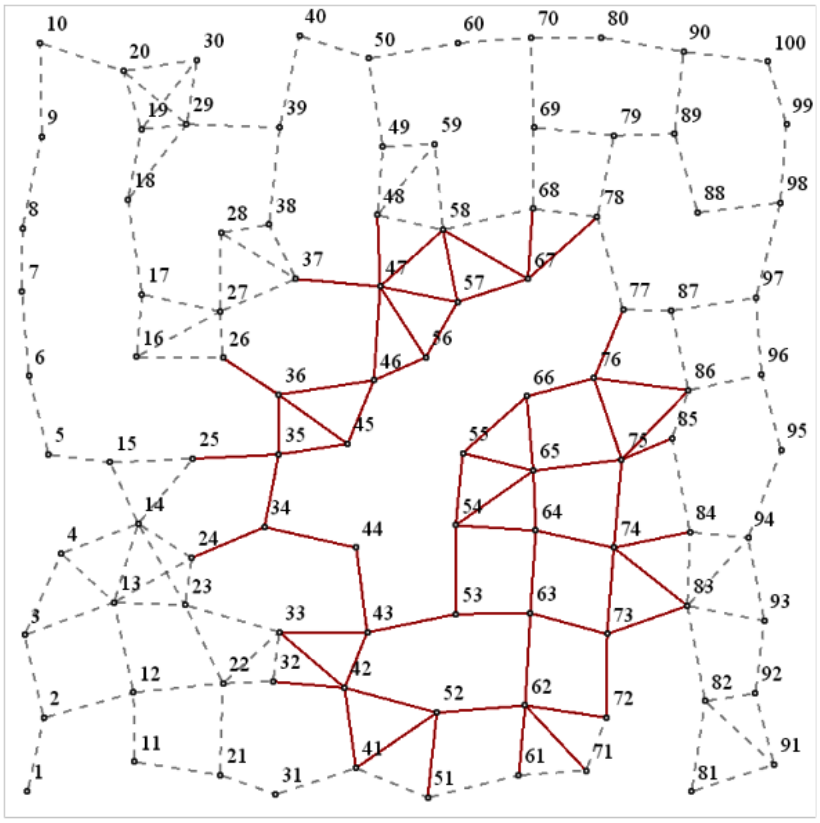

Figura 5.15: Topologia com Domínio de Colisão (54 → 55)

5.6.1. Simulação e Resultados

O principal objetivo deste cenário é obter o desempenho em uma rede com um nível de saturação maior, onde 99 nós transmitem em direção a um único Gateway de destino. Além disso, o cenário proposto leva em consideração vários domínios de colisão, além de possibilitar uma quantidade maior de diferentes efeitos na rede. Os resultados são demonstrados nos gráficos das Figuras 5.16 e 5.17.

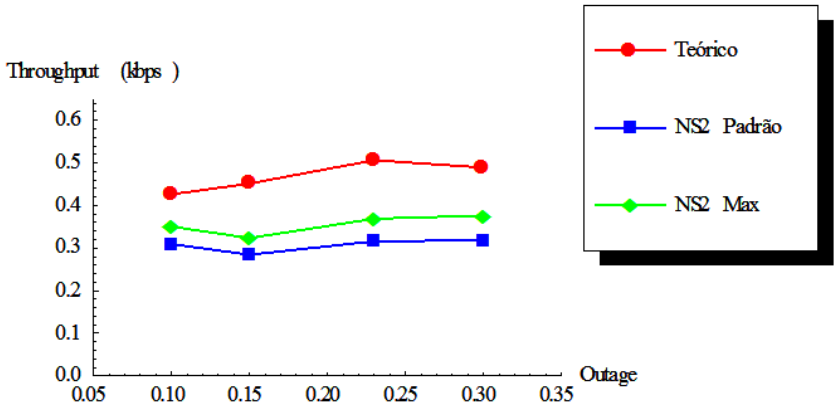

Figura 5.16: Throughput médio dos nós em função do outage

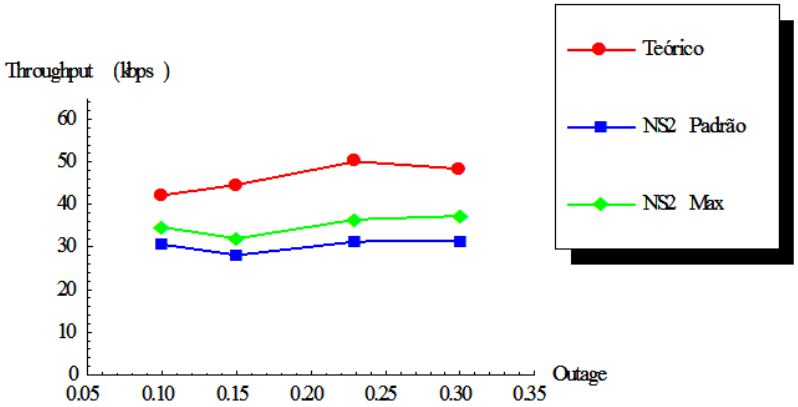

Figura 5.17: Throughput total da rede em função do outage

Levando-se em conta que a colisão de pacotes para este cenário certamente é maior, utilizou-se para os resultados de NS2 Max, os valores máximos obtidos, considerando uma taxa de entrega de pacotes mínima de 30%, a fim de medir a capacidade máxima da rede dentro de um limiar mínimo de qualidade e confiabilidade.

Diferentemente dos outros cenários, é possível verificar uma redução no throughput previsto em dois casos. O throughput simulado com outage de 15% foi menor que o obtido com 10% de probabilidade máxima de outage, indicando que as rotas escolhidas para este caso geraram mais colisões ou gargalos na rede. Outra hipótese é a de que os ganhos obtidos com o roteamento foram menores que as perdas (descartes) devido efeito do outage para esta situação. Por fim, o reuso espacial dos nós, presente em cenários com muitos saltos, pode também ter impactado o resultado, favorecendo neste caso, cenários com baixos níveis de outage. O segundo caso se encontra nos resultados teóricos, onde o algoritmo revela que com

um outage de 30% o ganho com rotas menores se mostrou menor que a perda proporcionada pelo outage na rede para esta topologia.

Outro ponto constatado foi a distribuição injusta do tráfego, como mostram as figuras 18 e 19. A Figura 18 mostra o throughput individual dos nós, considerando a taxa de pacotes sugerida pelo algoritmo (NS2 Padrão). É possível verificar diferenças acima de 100% entre os nós que obtiveram pior desempenho (nó 89 por exemplo obteve um throughput de 0,19 kbps) com os nós com desempenho mais alto (0,56 kbps para o nó 71 por exemplo). O contraste é ainda maior quando se injeta uma quantidade maior de pacotes na rede (NS2 Max), sendo que em geral, nós mais próximos ao gateway obtiveram um desempenho superior a nós distantes, devido à menor quantidade de saltos, como demonstra a Figura 19.

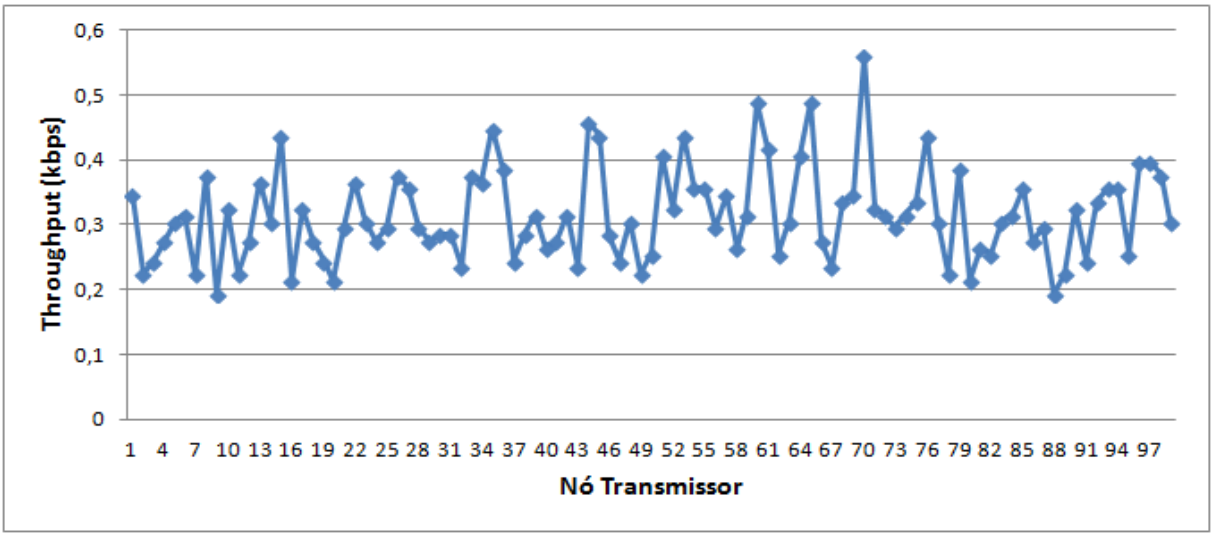

Figura 5.18: Throughput em cada nó transmissor (NS Padrão)

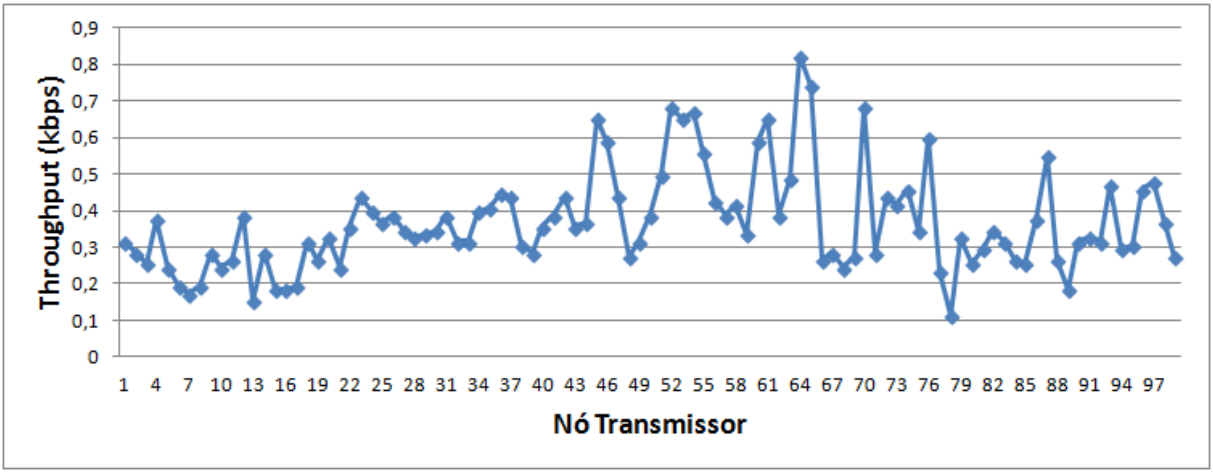

Figura 5.19: Throughput em cada nó transmissor (NS Max)

É possível verificar ainda que os resultados de NS2 e NS2 Max foram muito próximos, o que sugere que a taxa de pacotes sugerida pelo algoritmo está próxima do ideal. Mais uma vez, houve diferença no throughput teórico e simulado, principalmente devido à quantidade de descarte de pacotes de outage e de colisão, sendo o segundo não considerado pelo presente modelo teórico. Além disso, o limite de retransmissões imposto pelo NS-2 (*aMaxFrameRetries* e demais parâmetros de CSMA) em sua parametrização padrão provoca o descarte precoce de pacotes, contrário ao proposto no modelo teórico.

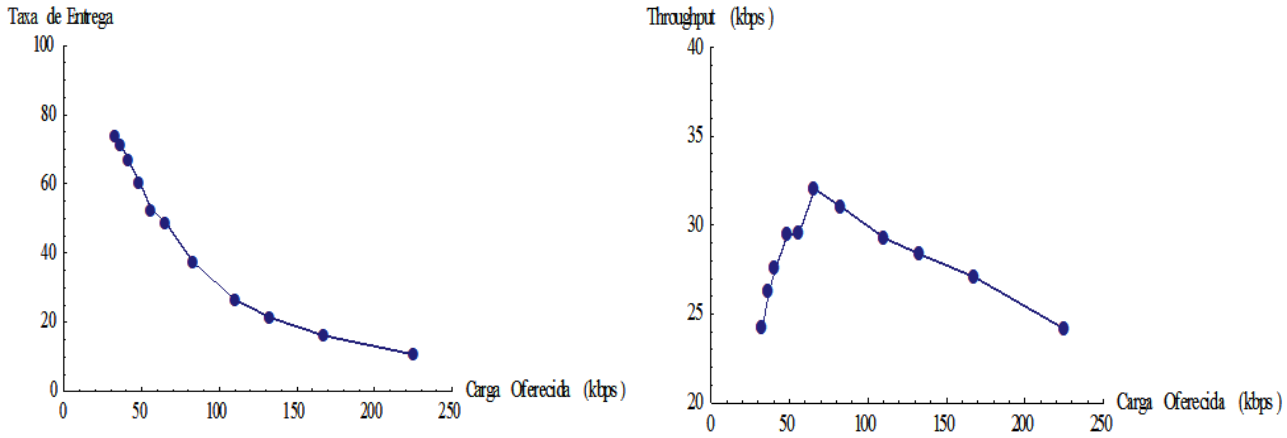

Figura 5.20: Taxa de Entrega e Throughput em função da Carga Oferecida

Os gráficos da Figura 5.20 demonstram a metodologia utilizada para a obtenção dos valores de "NS Max". Os gráficos mostram a taxa de entrega e o throughput obtido em função das diferentes cargas de tráfego oferecidas testadas no NS-2, para um outage máximo de 15%. O maior valor obtido de throughput foi considerado como "NS2 Max". No exemplo, a simulação executada com intervalo Poisson de 1.5 segundos para cada transmissão realizada por nó, resultou em uma carga oferecida de aproximadamente 60 kbps e um throughput aproximado de 33 kbps. É possível assim comparar o throughput e a taxa de entrega para cada carga oferecida, sendo que mesmo com a taxa de entrega diminuindo constantemente, a capacidade da rede não necessariamente acompanha esta trajetória, como é possível verificar na figura.

Capítulo 6

Conclusão e Trabalhos Futuros

Neste estudo, apresentamos uma nova abordagem para o planejamento de rotas e o cálculo da capacidade das redes mesh de sensores sem fio, com base no padrão IEEE 802.15.4. O algoritmo proposto visa determinar a capacidade máxima de transmissão, considerando a contenção imposta pela camada de acesso ao meio e o efeito do outage associado a cada enlace sem fio, além de fornecer um método para o planejamento otimizado de rotas.

Demonstramos através de simulações e comparações que o método é capaz de realizar engenharia de tráfego para as RSSF respeitando a capacidade máxima do canal e os níveis de outage presentes nos caminhos. Dentre as estratégias de planejamento de rotas analisadas, o método SWP atingiu o melhor desempenho em relação aos métodos SOP e SOL, sendo indicado em casos onde o atraso imposto pelo alto PER (e alto outage) não seja um problema.

Através ainda das comparações analítica e simulada é possível perceber o efeito do outage em todos os cenários propostos, e de que forma este efeito afeta a capacidade das WSN. O nosso estudo mostra que aceitar uma taxa maior de perda de pacotes permite em geral reduzir significativamente o tamanho de todos os caminhos, e aumenta a capacidade geral da rede, até um certo limite, apesar do aumento do número de retransmissões.

Foi possível verificar também outros efeitos que impactaram no resultado final. A colisão de pacotes introduzida no modelo de geração de tráfego (Poisson) influencia de forma significativa o desempenho da rede, e deve ser contemplado em futuras melhorias do modelo proposto neste trabalho. Além disso, a limitação do número máximo de retransmissões de um pacote no software de simulação também influenciou o resultado final, principalmente em cenários com altos níveis de outage e de colisões.

Como trabalhos futuros pretende-se desenvolver um modelo probabilístico para definir a distância de interferência. Neste trabalho, a distância de interferência foi assumida como sendo um valor constante, e os nós vizinhos dentro da distância de interferência de um dado nó provocam 100% de contenção, independentemente da distância em relação ao dado nó. Seguindo a estimativa de distância de transmissão baseada em outage proposta no presente documento, um modelo semelhante poderia ser desenvolvido para a distância de interferência, e os nós vizinhos poderiam apresentar uma possibilidade probabilística de interferir com a transmissão, definida como uma função da distância em relação a um dado nó. Também pretendemos investigar o efeito de diferentes sistemas de retransmissão e levar em conta o impacto de energia causada por trabalhar com probabilidades altas de interrupção.

Referências Bibliográficas

[01] BURCHFIELD, T. R.; VENKATESAN; S. & WEINER, D., "Maximizing Throughput in ZigBee Wireless Networks through Analysis, Simulations and Implementations", International Workshop on Localized Algorithms and Protocols for Wireless Sensor Networks Santa Fe, New Mexico, 2007. LOCALGOS 2007, located with Distributed Computing in Sensor Systems (DCOSS), 2007. CTI Press, Athens, p. 15-29.

[02] LATRÉ, B.; MIL, P. D.; MOERMAN, I.; DHOEDT, B. & DEMEESTER, P., "Throughput and Delay Analysis of Unslotted IEEE 802.15.4", Journal of Networks, 2006. p. 20-28.

[03] P. HAO, W. QIU AND R. EVANS, "Performance Evaluation of IEEE 802.15.4 MAC in Beacon-enabled Tree-topology Wireless Sensor Networks", Fifth International Conference on Systems and Networks Communications, 2010, pp. 58-63

[04] [BAG10] BAGULA, A. B., "Modelling and Implementation of QoS in Wireless Sensor Networks - A Multiconstrained Traffic Engineering Model", EURASIP Journal on Wireless Communications and Networking Volume 2010, Article ID 468737, 2010.

[05] RAZZAQUE, A.; HONG, C. S. & LEE, S., "Autonomous Traffic Engineering for Boosting Application Fidelity in Wireless Sensor Networks", IEICE Trans. Commun., Vol. E93-B, No.11, 2010. p. 2990-3003.

[06] JUN, J.; SICHITIU, M. L. "The Nominal Capacity of Wireless Mesh Networks" IEEE Wireless Communications 2003.

[07] AOUN, B.; BOUTABA, R., "Max-Min Fair Capacity of Wireless Mesh Networks", IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS), Jun 2006.

[08] JAMHOUR, E.; FISHER, A. “A symbolic model to traffic engineering in wireless mesh networks,” in Proceedings of the 44th Annual Simulation Symposium, ser. ANSS ’11. San Diego, CA, USA: Society for Computer Simulation International, 2011, pp. 32–38. Disponível em: http://dl.acm.org/citation.cfm?id=2048370.2048375

[09] ZHENG, J.; LEE, M. J., “Low rate wireless personal area networks (LR-WPANs), NS2 simulation platform”, 2001, Disponível em: <http://ees2cy.engr.ccny.cuny.edu/zheng/pub/>. Acesso em: mar. 2011.

[10] ZIGBEE ALLIANCE. “ZigBee Specification 053474r17”. Disponível em: <http://www.zigbee.org.> Acesso em: maio. 2011.

[11] FARAHANI, F. “ZigBee Wireless Networks and Transceivers”**.** Editora Elsevier, 2008.

[12] KLUES, K. “802.15.4 and ZigBee”, Department of Computer Science and Engineering, Washington University in St. Louis. Disponível em: <sing.stanford.edu/klueska/Black_Site/Publications_files/802_15_4.ppt>. Acesso em: jun. 2011.

[13] HOSSAIN, E.; LEUNG, K. “Wireless Mesh Networks”, Editora Springer, 2008.

[14] 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),” IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003), pp. 1–320, 2006.

[15] VASQUES, B., COUTINHO, I., LIMA, M.; CARNEVA, V. “Zigbee”. Universidade Federal do Rio de Janeiro, 2010. Disponível em: <http://www.gta.ufrj.br/grad/10_1/zigbee/introducao.html>. Acesso em: fev. 2011.

[16] SHRESTHA, B., HOSSAIN, E. & CAMORLINGA, S., “A Markov model for IEEE 802.15.4 MAC with GTS transmissions and heterogeneous traffic in non-saturation mode”, Communication Systems (ICCS), 2010 IEEE International Conference, Nov. 2010, p. 56-61.

[17] WIJETUNGE, S., GUNAWARDANA, U. & LIYANAPATHIRANA R., “Performance Analysis of IEEE 802.15.4 MAC Protocol for WSNs with ACK Frame Transmission Under Unsaturated Traffic Conditions”, Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2010 Sixth International Conference, Dec. 2010, p. 55-60.

[18] KOUBAA, A.; ALVES, M. & TOVAR, E., “Modeling and Worst-Case Dimensioning of Cluster-Tree Wireless Sensor Networks”, RTSS '06 Proceedings of the 27th IEEE International Real-Time Systems Symposium, IEEE Computer Society Washington, DC, USA, 2006.

[19] KUMAR, V.; RAGHUVANSI, A.S.; TIWARI, S., “Performance study of beacon-enabled IEEE 802.15.4 standard in WSNs with clustering”, Power, Control and Embedded Systems (ICPCES), 2010 International Conference, Dec. 2010, p. 1-5.

[20] MAOHENG S., KAIJIAN S., YOUMIN Z., “Analysis and Improvement for 802.15.4 Multi-hop Network”, Communications and Mobile Computing, 2009. CMC '09. WRI International Conference, 2009, p. 52-56.

[21] SUN, T., et al. “Senprobe: Path Capacity Estimation in Wireless Sensor Networks”, in: SenMetrics, 2005.

[22] YOU-MIN Z., MAO-HENG S., PENG R., ”An Enhanced Scheme for the IEEE 802.15.4 Multi-hop Network”, Wireless Communications, Networking and Mobile Computing, 2006. WiCOM 2006.International Conference, Sept. 2006, p. 1-4.

[23] JAE Y. H.; Hong S. P.; Sunghyun C. & Wook H. K., “EHRP: Enhanced hierarchical routing protocol for zigbee mesh networks”, Communications Letters, IEEE, dec. 2007, p. 1028-1030.

[24] SHANG T.; Wu W.; Liu X. & Liu J., “AODVjr routing protocol with multiple feedback policy for ZigBee network”, IEEE 13th International Symposium on Consumer Electronics, 2009. ISCE '09, May 2009. p. 483-487.

[25] TAO S.; Jianwei L., “Security enhancement of AODVjr routing protocol for ZigBee network”, 2010 5th International ICST Conference on Communications and Networking in China (CHINACOM), Aug. 2010, p. 1-5.

[26] YU-DOO K.; Il-Young M., “Improved AODV routing protocol for wireless sensor network based on ZigBee”, 11th International Conference on Advanced Communication Technology, ICACT 2009, feb 2009. p. 859-862.

[27] MISIC, J., SHAFI, S. & MISIC V. B., “Performance of a beacon enabled IEEE 802.15.4 cluster with downlink and uplink traffic”, IEEE Trans. Parallel and Distributed Syst., vol. 17, no. 4, 2006, p. 361-376.

[28] MARTALO, M., FERRARI, G. & BUSANELLI S., “Markov Chain-Based Performance Evaluation of IEEE 802.15.4 Multihop Wireless Sensor Networks”, Communications, Control and Signal Processing, 2008. ISCCSP 2008. 3rd International Symposium, 2008, p. 461-466.

[29] JING, H., AIDA, H., “An Analytical Approach to Optimization of Throughput for IEEE 802.15.4 Slotted CSMA/CA Networks”, Consumer Communications and Networking Conference (CCNC), IEEE, 2011, p. 1021-1025.

[30] KOHVAKKA, M.; KUORILEHTO, M.; HÄNNIKÄINEN, M. & HÄMÄLÄINEN, T. D., “Performance Analysis of IEEE 802.15.4 and ZigBee for Large-Scale Wireless Sensor Network Applications”, in Proceedings of the 3rd ACM international workshop

on Performance evaluation of wireless ad hoc, sensor and ubiquitous networks, Terromolinos, Spain, 2006.

[31] LEE, J., “Performance Evaluation of IEEE 802.15.4 for Low-Rate Wireless Personal Area Networks”, IEEE Transactions on Consumer Electronics, Vol. 52, No. 3, 2006. p. 742-749.

[32] SUN, T., et al., “Measuring Effective Capacity of IEEE 802.15.4 Beaconless Mode”, Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE, p.493-498.

[33] HEIDEMANN, Ye, W., ESTRIN J. D., “An energy efficient MAC protocol for wireless sensor networks”, In Proceedings Infocom 2002, New York, June 2002.

[34] WIKIPEDIA. “Hidden node problem”. Disponível em: http://en.wikipedia.org/wiki/Hidden_node_problem. Acesso em 01/11/2011

[35] TSENG, Y. C., NI, S.Y., SHIH, E.Y., “Adaptive approaches to relieving broadcast storms in a wireless multihop mobile adhoc network”, IEEE Trans. on Computers, 52, 5 May. 2003, p. 545-557.

[36] TIMMONS, N.F.; SCANLON, W.G., “Analysis of the performance of IEEE 802.15.4 for medical sensor body area networking”, in Proceedings of the 1st IEEE international conference. On Sensor and ad hoc communications and networks (SECON’04) (Santa Clara, CA, USA, 2004. p.16-24.

[37] LU, G.; KRISHNAMACHARI, B. & RAGHAVENDRA, C. S., “Performance Evaluation of the IEEE 802.15.4 MAC for Low-Rate Low-Power Wireless Networks”, Performance, Computing, and Communications, 2004 IEEE International Conference, 2004. p. 701-706.

[38] BAGULA, A. B.; MAZANDU, K. G., “Energy constrained multipath routing in wireless sensor networks”, in Proceedings of the 5th International Conference on Ubiquitous Intelligence and Computing (UIC ’08), vol. 5061 of Lecture Notes in Computer Science, Oslo, Norway, 2008. p. 453-467.

[39] WAN, C.; WISENMAN, S. & CAMPBELL, A., “CODA: congestion detection and avoidance in sensor networks”, Proceedings of 1st International Conference on Embedded Networked Sensor Systems (ACM SenSys'03), Los Angeles, California, USA, Nov. 2003. p. 266-279.

[40] KANG, J.; ZHANG, Y. & NATH, B., “TARA: Topology-aware resource adaptation to alleviate congestion in sensor networks”, IEEE Transactions on Parallel and Distributed Systems, vol.18, no.7, 2007. p. 919-931.

[41] M. KAKITANI, G. BRANTE, R. DEMO SOUZA, AND A. MUNARETTO, “Comparing the energy efficiency of single-hop, multi-hop and incremental decodeand-forward in multi-relay wireless sensor networks,” in Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium on, 2011, pp. 970–974

[42] E. MALKAMAKI AND H. LEIB, “Coded diversity on block-fading channels,” Information Theory, IEEE Transactions on, vol. 45, no. 2, pp. 771–781, 1999.

[43] M. K. SIMON AND M.-S. ALOUINI, “Digital Communication over Fading Channel”s. Wiley Interscience, 2004.

[44] G. DE OLIVEIRA BRANTE, M. KAKITANI, AND R. DEMO SOUZA, “Energy efficiency analysis of some cooperative and non-cooperative transmission schemes in wireless sensor networks,” Communications, IEEE Transactions on, vol. 59, no. 10, pp. 2671–2677, 2011.

[45] A. GOLDSMITH, “Wireless Communications”, 1st ed. Cambridge University Press, 2005.

[46] Z. WANG AND G. GIANNAKIS, “A simple and general parameterization quantifying performance in fading channels,” IEEE Trans. on Communications, vol. 51, no. 8, pp. 1389 – 1398, aug. 2003.

[47] S. B. WICKER, “Error control systems for digital communication and storage”. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1995.

[48] T. SUN, L.-J. CHEN, C.-C. HAN, G. Y. 0001, AND M. GERLA, “Measuring effective capacity of ieee 802.15.4 beaconless mode.” in WCNC, 2006, pp. 493–498.

[49] WOLFRAM. “Wolfram Mathematica 9.0”, Disponível em: http://www.wolfram.com/. Acesso em 13/01/2013.

[50] DIGI, “Datasheet,” Jul. 2013. Disponível em: http://www.digi.com/

[51] R. PEREIRA, R. DEMO SOUZA, AND M. PELLENZ, “Multiple concurrent transmissions in wireless mesh networks employing superposition and dirty paper coding,” Vehicular Technology, IEEE Transactions on, vol. 58, no. 9, pp. 5115–5123, 2009.

[52] "The Network Simulator - ns-2", Disponível em: http://www.isi.edu/nsnam/ns/. Acesso em 12/05/2012.

[53] Z. WU, "Implement a routing agent with manually configured routing table (Static Routing)", Disponível em: http://www.winlab.rutgers.edu/~zhibinwu/html/Routing_Agent.html. Acesso em: 23/06/2012

[54] A. IYER, C. ROSENBERG AND A. KARNIK, "What is the Right Model for Wireless Channel Interference?", Wireless Communications, IEEE Transactions on (Volume:8 , Issue: 5), May 2009, pp. 2662-2671

[55] J. ZHENG AND M. J. LEE, "A comprehensive performance study of IEEE 802.15.4," Sensor Network Operations, IEEE Press, Wiley Interscience, ISBN 0-471-71976-5, Chapter 4, pp. 218-237, 2006.

[56] ONISHI. D.; ONISHI, F.; COELHO, L.G., "Localizador sem-fio de Equipamentos Médicos", Universidade Tecnológica Federal Do Paraná (UTFPR), Curitiba, 2008.

[57] FARAHANI, F., "ZigBee Wireless Networks and Transceivers**".** Editora Elsevier, 2008.

[58] SCHWETLICK, H., et al. "PSSS-Parallel Sequence Spread Spectrum: A Physical Layer for RF Communication", IEEE International Symposium on Consumer Electronics, 2004.

[59] LABIOD, H.; AFIFI, H.; SANTIS, C. "Wi-Fi, Bluetooth, ZigBee and WiMax", Editora Springer, 2007.

Apêndice A

Conceitos Básicos das Redes Zigbee

Neste apêndice, são descritas as principais funcionalidades das redes Zigbee, que não foram detalhadas no capítulo 2. São demonstradas as principais características, a classificação e detalhes do padrão 802.15.4, no qual o Zigbee foi baseado.

A.1. Características

ZigBee oferece serviços como segurança, descoberta, criação de perfis, entre outras características. Os dispositivos operam na faixa ISM (*Industrial, Scientific and Medical radio band*), isto é, não requer licença para funcionamento. Estes operam nas faixas de 2,4 GHz (Global), 915 MHz (Estados Unidos) e 868 MHz (Europa) e com taxas de transferências de dados de 250 Kbps em 2,4 GHz, 40 Kbps em 915 MHz e 20 Kbps em 868 MHz.

Além disso, o padrão oferece:

- Suporte a diferentes topologias como estrela e mesh;
- Endereçamento curto de 16 bits ou MAC normal (64 bits);
- Potência máxima de transmissão de 0dbm, com alcance médio de 30 a 100 metros;
- Suporte de acesso e repartição simples, com garantias,
- Transferência de dados reconhecida, e opcional modo Beacon;
- Detecção de Energia (ED)
- Indicação de qualidade de Link (LQI)

Nos equipamentos Zigbee, o tempo total que o dispositivo sem fio está envolvido em qualquer tipo de atividade é muito limitado, passando a maior parte de seu tempo em um

modo de economia de energia, também conhecido como modo de hibernação. Como resultado, os dispositivos Zigbee são capazes de permanecerem operacionais durante vários anos antes de suas baterias precisarem ser substituídas.

A.2. Classificação

O padrão ZigBee especifica duas classes de dispositivos físicos. *Full Function Devices* e *Reduced Function Devices*:

• *Full Function Device* (FFD): são dispositivos de maior capacidade de memória e processamento, geralmente alimentados eletricamente via USB ou rede AC. Tem capacidade de inicializar uma nova rede e se comunicar diretamente com outros dispositivos ou em topologias (estrela, árvore ou malha). Possuem maior infraestrutura devido a sua atividade mais intensa. Os FDD são subdivididos em:

- Coordenador ZigBee (PAN Coordinator): é o tipo de dispositivo mais completo. Pode atuar como coordenador de uma rede assim como também servir de ligação a outras redes, sendo o módulo central da topologia. Existe exatamente um coordenador em cada rede, em que este é o nó que a começa. Pode armazenar informação sobre a rede e atuar como coordenador na distribuição de chaves cifradas. É o dispositivo que inicializa a rede, configurando todos os parâmetros iniciais, como por exemplo, canal utilizado, identificador da rede, emprego de criptografia e permissões de acesso [56]. Pode ser conectado a um PC para permitir o monitoramento da rede, servindo como fonte de dados para esse processo. A única diferença entre o coordenador e os roteadores é que somente o primeiro pode inicializar uma rede, e tal é a semelhança que depois da configuração dos parâmetros, ele se transforma em um roteador comum [56].

- Roteadores (*Routers*): são os responsáveis pela área de cobertura do sistema, encaminhando as mensagens aos seus destinatários, efetuando a conexão dos módulos terminais à rede. São usados em topologias em malha (mesh) e cluster para dar maior robustez à rede. Eles possuem tabelas de roteamento alimentadas através de algoritmos de roteamento e, por serem FFD, permitem encontrar o menor caminho para se chegar ao destino [15]. Caso o roteador não possua o endereço de destino requisitado, este fará o broadcast de uma requisição de rota (*route request*) e receberá do destino a rota mais eficaz atualizando sua tabela. Este mecanismo dá à rede a característica de auto-regeneração caso ocorra a queda das funcionalidades de outros nós roteadores na rede.

• *Reduced Function Device* (RFD): São os dispositivos finais (Endpoints) que enviam dados periodicamente para a rede. Apresentam implementação física simplificada e normalmente são alimentados por baterias ao invés da rede AC, podendo somente se comunicar diretamente com dispositivos FFD. Devido à característica de tornarem-se ativos em períodos específicos, apresentam a capacidade de desligar seus transmissores durante os intervalos de medição e ativá-los novamente em apenas 15ms, permitindo uma redução no consumo de energia [10].

A.3. Padrão IEEE 802.15.4

O IEEE 802.15.4, padrão estabelecido em 2006 e direcionado à especificação de protocolos de LR-WPANs, é o alicerce das redes Zigbee e responsável pela especificação das camadas física e de enlace do modelo OSI.

A.3.1. Camada Física – PHY

As principais características de funcionamento da tecnologia ZigBee se encontram na camada física. Dentre os recursos gerenciados estão a ativação e desativação do transceptor de rádio, detecção de energia (ED), indicação da qualidade do enlace (LQI), seleção do canal, verificação de canal livre, além da transmissão e recepção de dados.

O padrão prevê operação em 27 canais nas bandas (ISM) conforme já comentado previamente. Na prática, encontram-se disponíveis no mercado apenas dispositivos de operação na faixa global não-licenciada de 2.4GHz de 16 canais e taxa de transmissão de 250kbps. A modulação empregada é a de Chaveamento por Deslocamento de Fase Ortogonal (O-QPSK) com banda de 2 MHz, espaçamento de 5 MHz entre os canais e espalhamento espectral por sequência direta (DSSS) com taxa de 32 chips por símbolo [56]. A Tabela A.1 mostra as características em todas as faixas de frequência:

	Frequency (MHz)	Number of Channels	Modulation	Chip Rate (Kchip/s)	Bit Rate (Kb/s)	Symbol Rate (Ksymbol/s)	Spreading Method
	868–868.6	1	BPSK	300	20	20	Binary DSSS
	902–928	10	BPSK	600	40	40	Binary DSSS
Optional	868–868.6	1	ASK	400	250	12.5	20-bit PSSS
	902–928	10	ASK	1600	250	50	5-bit PSSS
Optional	868–868.6	1	O-QPSK	400	100	25	16-array orthogonal
	902–928	10	O-QPSK	1000	250	62.5	16-array orthogonal
	2400–2483.5	16	O-QPSK	2000	250	62.5	16-array orthogonal

Tabela A.1: Faixas e velocidades de transmissão [57]

Existem três tipos de modulação no padrão IEEE 802.15.4: chaveamento por deslocamento de fase de binária (BPSK), chaveamento de amplitude (ASK), e o deslocamento de fase em quadratura (O-QPSK). Em BPSK e QPSK-O, os dados digitais são na fase do sinal. Em ASK, em contrapartida, os dados digitais são na amplitude do sinal.

Todos os métodos de comunicação sem fio no padrão IEEE 802.15.4 tiram proveito das técnicas de espalhamento espectral de propagação por sequencia direta (DSSS) ou espalhamento espectral de propagação por seqüência em paralelo (PSSS). DSSS e PSSS ajudam a melhorar o desempenho dos receptores em ambientes de múltiplos caminhos [58]. Para evitar problemas com outras tecnologias que utilizam a mesma faixa de frequência, o padrão estabelece um recurso de seleção do canal através de detecção de energia. Na inicialização da rede pelo coordenador, ele procura o canal com menor ruído possível para então estabelecer o canal.

Através do mecanismo de detecção de energia (ED), o módulo estima a potência do sinal recebido dentro da faixa do canal de transmissão. Tal informação é empregada pelo mecanismo de LQI, que caracteriza a qualidade da conexão e o nível de ruído do ambiente, e também pelo mecanismo de Clear Channel Assessment (CCA), que compara o nível de energia do canal com um limiar de transmissão para avaliar o estado de ocupação do mesmo [10].

Os dados e os comandos são transmitidos entre vários dispositivos na forma de pacotes. A estrutura geral de um pacote é mostrada na Figura A.1. O pacote PHY consiste em

três componentes: o cabeçalho de sincronização (*Synchronization Header* - SHR), o cabeçalho PHY (*PHY header* - PHR), e os dados PHY (*PHY Payload*).

Octets: 4	1	1		variable
Preamble	SFD	Frame length (7 bits)	Reserved (1 bit)	PSDU
SHR		PHR		PHY payload

Figura A.1: Estrutura do Pacote PHY IEEE 802.15.4 [59]

O tamanho máximo do *PHY Service Data Unit* (PSDU) é de 128 bytes com a carga útil máxima de 104 bytes. O SHR é composto pelo preâmbulo, responsável pela a sincronia e bloqueio do fluxo de bits entre transmissor e receptor, e o delimitador de Início do quadro (*Start of Frame Delimiter* - SFD), que sinaliza o início do quadro. O PHR guarda informações do tamanho do quadro de dados. Por fim, o PSDU é fornecido pelas camadas superiores e incluem dados ou comandos para o dispositivo receptor. Possui a carga útil repassada pela camada de enlace e o cabeçalho MAC.

A.4. Camada de Aplicação

A camada de aplicação é a camada mais elevada no protocolo de rede sem fio ZigBee e hospeda os objetos da aplicação. Fabricantes desenvolvem os objetos da aplicação para customizar um dispositivo para aplicações diversas. Objetos de aplicativo controlam e gerenciam as camadas de protocolo em um dispositivo ZigBee. Pode haver até 240 objetos de aplicativo em um único dispositivo. O padrão ZigBee oferece a opção de usar perfis de aplicação no desenvolvimento de um aplicativo. Um perfil de aplicação é um conjunto de acordos sobre os formatos de mensagens e ações de processamento [57]. A utilização de um perfil de aplicação permite ainda interoperabilidade entre os produtos desenvolvidos por fornecedores diferentes para uma aplicação específica.

A.5. Segurança

Em uma rede sem fio, as mensagens transmitidas podem ser recebidas por qualquer dispositivo nas proximidades, incluindo um intruso. As duas principais preocupações de segurança em uma rede sem fio são a confidencialidade e a integridade dos dados. O padrão

IEEE 802.15.4 suporta a utilização do *Advanced Encryption Standard* (AES) para criptografar suas mensagens enviadas, sendo esta uma solução à confidencialidade. Já para garantir a integridade dos dados transmitidos, é incluindo um código de integridade da mensagem (MIC) em cada quadro de saída, que vai permitir ao destinatário de saber se a mensagem foi alterada em trânsito. Esse processo é conhecido como autenticação de dados.

Na camada de rede, o padrão ZigBee oferece um mecanismo de autenticação por meio de uma chave de rede (*network key*), que impede o acesso de estações intrusas ao sistema. A vantagem em relação ao emprego da autenticação de enlace é a menor exigência de memória, porém por ser empregada em diversos nós simultaneamente oferece menor proteção, e por esse motivo não é recomendável para aplicações industriais [10].

Um dos principais obstáculos na implementação de funcionalidades de segurança em uma rede ZigBee Wireless são os limitados recursos. Como já dito, os nós são essencialmente alimentados por bateria e têm poder computacional e de memória limitado. ZigBee é direcionado para aplicações de baixo custo e o hardware nos nós pode não ser inviolável. Se um intruso adquire um nó de uma rede operacional que não tem resistência à adulteração, a chave atual poderia ser obtida simplesmente a partir da memória do dispositivo. Um nó inviolável pode apagar as informações sensíveis, incluindo as chaves de segurança, se for detectada adulteração.

A.6. Comparativo entre as Redes Sem-Fio

Dentre as tecnologias de comunicações sem-fio disponíveis atualmente, pode-se citar como principais concorrentes ao padrão ZigBee IEEE 802.15.4, o Bluetooth IEEE 802.15.1 e o Wi-Fi IEEE 802.11. A Tabela A.2 a seguir apresenta um comparativo entre as três tecnologias citadas:

	ZigBee 802.15.4	Bluetooth 802.15.1	Wi-Fi 802.11b
Foco de aplicação	Monitoramento e Controle	Substituição de cabos	Email, Vídeo, Internet
Recursos do Sistema	4KB -32 KB	250KB+	1MB+
Duração da bateria (dias)	100-1000+	1-7	1-5
Nós por rede	255/65K+	7	30
Largura de Banda (kb3ps)	20-250 kbps	1 Mbps+	11 Mbps+
Alcance (m)	1-100+	1-10+	1-100

	ZigBee 802.15.4	Bluetooth 802.15.1	Wi-Fi 802.11b
Atributos principais	Confiabilidade, baixo consumo, custo-benefício	Custo, conveniência	Velocidade, flexibilidade

Tabela A.2: Comparativo entre tecnologias sem-fio [56]

Comparando o padrão ZigBee com Bluetooth e IEEE 802.11 WLAN ajuda-nos a compreender como ZigBee diferencia-se a partir de padrões estabelecidos. Considerando os fatores consumo, taxa de transmissão, escalabilidade, simplicidade e custo-benefício, cada um dos fatores apresenta características distintas.

IEEE 802.11 é uma família de normas. IEEE 802.11b foi selecionado aqui, pois opera na banda de 2,4 GHz, que é comum ao Bluetooth e ZigBee. IEEE 802.11b tem uma alta taxa de dados (até 11 Mbps), mas com suporte a poucos nós por rede e consumo elevado de energia. Proporcionar uma conexão sem fio à Internet é uma das suas aplicações típicas. A faixa interior (indoor) do IEEE 802.11b é geralmente entre 30 e 100 metros. Por outro lado, o Bluetooth tem uma taxa de dados mais baixa e seu alcance interno é tipicamente 2-10 metros. Além disso, suporta poucos dispositivos e tem um alto consumo de energia. Uma aplicação popular do Bluetooth é em fones de ouvido sem fio, Bluetooth, onde fornece os meios para a comunicação entre um telefone móvel e um fone de ouvido, deixando as mãos-livres. ZigBee tem a menor taxa de dados e complexidade entre esses três padrões e proporciona uma vida de bateria mais longa.

A taxa de dados muito baixa do padrão ZigBee significa que não é a melhor escolha para a implementação em Internet sem fio ou um fone de ouvido sem fio com qualidade de CD, onde mais de 1 Mbps é desejado. No entanto, se o objetivo da comunicação sem fio é transmitir e receber comandos simples e/ou recolher informação dos sensores, como sensores de temperatura ou umidade, ZigBee oferece mais poder, apresentando melhor dimensionamento de taxas de transmissão, escalabilidade, alcance, consumo, e principalmente, custo-benefício, tornando-se a solução mais rentável em comparação às tecnologias Bluetooth e IEEE 802.11b.

Apêndice B

Tabelas de Relação Enlace, Distância e Outage

Enlace	Distância / Outage
1-2	{248.697,0.00240556}
1-3	{466.734,0.08108}
1-5	{249.098,0.00242841}
1-6	{423.586,0.0488942}
1-7	{615.833,0.293029}
1-8	{572.931,0.215942}
1-15	{524.475,0.14411}
2-3	{246.887,0.00230475}
2-4	{464.01,0.0786917}
2-5	{460.196,0.0754328}
2-6	{541.115,0.166835}
2-8	{613.139,0.28786}
2-15	{466.275,0.0806734}
3-4	{249.447,0.00244841}
3-5	{616.75,0.294799}
3-6	{599.963,0.263173}
3-8	{584.911,0.23628}
3-15	{368.517,0.0229189}
3-16	{490.587,0.104191}
4-6	{582.975,0.232928}
4-8	{481.69,0.0951003}
4-10	{565.796,0.204298}
4-15	{247.348,0.00233011}
4-16	{253.842,0.00271198}
4-17	{493.146,0.10691}
5-6	{246.221,0.00226859}
5-7	{380.789,0.0274653}
5-8	{446.542,0.0645537}
5-9	{578.705,0.225623}
5-15	{508.236,0.123921}
6-7	{239.008,0.00190534}
6-8	{208.626,0.000854666}
6-9	{398.779,0.0353483}
6-10	{398.779,0.0353483}
6-11	{445.,0.0634004}
6-12	{593.485,0.251422}
6-15	{348.323,0.0167325}
6-16	{561.633,0.197671}
7-8	{340.,0.0146026}
7-9	{200.25,0.000670521}
7-10	{438.292,0.0585575}
7-11	{355.106,0.0186425}
7-12	{449.11,0.0665076}
7-13	{608.215,0.278513}
7-15	{553.484,0.185056}
8-9	{403.113,0.0374808}
8-10	{206.155,0.000796474}
8-11	{335.41,0.0135233}
8-12	{506.063,0.121369}
8-13	{549.477,0.179031}
8-14	{447.465,0.065251}
8-15	{236.863,0.00180701}
8-16	{385.093,0.0292147}
8-17	{517.285,0.134929}
8-18	{596.406,0.256688}
9-10	{400.,0.0359394}
9-11	{223.607,0.00128734}
9-12	{260.,0.00311977}
9-13	{444.325,0.0629006}
9-14	{539.189,0.1641}
10-11	{223.607,0.00128734}
10-12	{384.187,0.0288396}
10-13	{365.274,0.0218211}
10-14	{242.332,0.00206631}
10-15	{361.668,0.0206491}
10-16	{375.229,0.0253268}
10-17	{396.59,0.0343068}
10-18	{410.122,0.0411341}
11-12	{172.047,0.000272127}
11-13	{257.73,0.00296403}
11-14	{315.793,0.00959993}
11-15	{553.176,0.18459}
11-16	{598.83,0.261098}
11-17	{590.664,0.246387}
11-18	{525.547,0.145512}
12-13	{208.387,0.00084887}
12-14	{390.288,0.0314383}

12-18	{592.115,0.24897}	14-16	{465.137,0.0796733}	16-17	{249.369,0.00244392}
13-14	{241.868,0.00204316}	14-17	{336.763,0.0138345}	16-18	{463.095,0.0779013}
13-17	{578.471,0.225226}	14-18	{210.297,0.000895964}	17-18	{239.842,0.00194469}
13-18	{413.673,0.0430839}	15-16	{244.698,0.00218749}		
14-15	{558.022,0.192023}	15-17	{469.221,0.0833034}		

Tabela B.1: Percentual de outage em função da distância dos enlaces