

ALLAN DA SILVA ESPINDOLA

**PROTOCOLO GEOGRÁFICO ORIENTADO
PARA QUALIDADE DE SERVIÇO PARA
REDES DE SENSORES AMBIENTAIS**

CURITIBA

2018

ALLAN DA SILVA ESPINDOLA

**PROTOCOLO GEOGRÁFICO ORIENTADO PARA
QUALIDADE DE SERVIÇO PARA REDES DE
SENSORES AMBIENTAIS**

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

Área de Concentração: Ciência da Computação

Orientador: Prof. Dr. Manoel Camillo de O. Penna

Coorientador: Prof. Dr. Marcelo Eduardo Pellenz

CURITIBA

2018

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central
Edilene de Oliveira dos Santos CRB 9 /1636

E77p
2018

Espindola, Allan da Silva
Protocolo geográfico orientado para qualidade de serviço para redes de sensores ambientais / Allan da Silva Espindola ; orientador, Manoel Camillo de O. Penna ; coorientador, Marcelo Eduardo Pellenz. -- 2018
69 f. : il. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2018
Bibliografia: f.67-69

1. Protocolo de aplicação sem fio (Protocolo de rede de computadores).
2. Roteadores (Redes de computação). 3. Redes de sensores sem fio.
I. Penna, Manoel Camillo de Oliveira. II. Pellenz, Marcelo Eduardo
III. Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Informática. IV. Título.

CDD 20. ed. – 004.62

ATA DE SESSÃO PÚBLICA

DEFESA DE DISSERTAÇÃO DE MESTRADO Nº 04/2018

**PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA – PPGIa
PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ - PUCPR**

Em sessão pública realizada às 14h00 de **05 de Abril de 2018**, no Auditório Guglielmo Marconi – Bloco 8, ocorreu a defesa da dissertação de mestrado intitulada “**Protocolo Geográfico Orientado para Qualidade de Serviço para Redes de Sensores Ambientais**” apresentada pelo aluno **Allan da Silva Espíndola**, como requisito parcial para a obtenção do título de **Mestre em Informática**, na área de concentração **Ciência da Computação**, perante a banca examinadora composta pelos seguintes membros:

Prof. Dr. Manoel Camillo de Oliveira Penna Neto (Orientador)- PUCPR

Prof. Dr. Marcelo Eduardo Pellenz – PUCPR

Prof. Dr. Edgard Jamhour – PUCPR

Prof. Dr. Eduardo Parente Ribeiro – UFPR



Após a apresentação da dissertação pelo aluno e correspondente arguição, a banca examinadora emitiu o seguinte parecer sobre a tese:

Membro	Parecer
Prof. Dr. Manoel Camillo de O. Penna Neto	<input checked="" type="checkbox"/> Aprovado () Reprovado
Prof. Dr. Marcelo Eduardo Pellenz	<input checked="" type="checkbox"/> Aprovado () Reprovado
Prof. Dr. Edgard Jamhour	<input checked="" type="checkbox"/> Aprovado () Reprovado
Prof. Dr. Eduardo Parente Ribeiro	<input checked="" type="checkbox"/> Aprovado () Reprovado

Portanto, conforme as normas regimentais do PPGIa e da PUCPR, a tese foi considerada:

APROVADO

(aprovação condicionada ao atendimento integral das correções e melhorias recomendadas pela banca examinadora, conforme anexo, dentro do prazo regimental)

() **REPROVADO**

E, para constar, lavrou-se a presente ata que vai assinada por todos os membros da banca examinadora. Curitiba, 05 de Abril de 2018.

Prof. Dr. Manoel Camillo de Oliveira Penna Neto

Prof. Dr. Marcelo Eduardo Pellenz

Prof. Dr. Edgard Jamhour

Prof. Dr. Eduardo Parente Ribeiro

Agradecimentos

Agradeço primeiramente a Deus por permitir que esse trabalho tenha sido desenvolvido. Agradeço aos professores Edgard Jamhour e Marcelo Pellenz pelas orientações e ao meu orientador Manoel Camillo que me deu a oportunidade de trabalhar com ele, com orientações precisas e valiosas e pela imensa paciência. Agradeço aos meus amigos que fiz durante essa fase da minha vida, especialmente Rosana Lachowski, Eduardo Viegas, Vilmar Abreu e meu professor de graduação Cleverton Vicentini. Agradecimento especial para a minha esposa Bruna Espindola meu pai Gilson Espindola e minha mãe Maria Natalícia que me deram condições, apoio e incentivo incondicional que me manteve focado neste trabalho.

Resumo

As Redes de Sensores Ambientais (*RSA*) são formadas por um conjunto de sensores que suportam as aplicações de gestão do meio ambiente. Têm como finalidade coletar dados sobre o ambiente onde os sensores estão implantados. As *RSA* são muito importantes para compreensão de fenômenos naturais e principalmente os fenômenos que antes não era possível o acompanhamento devido ocorrerem em locais de difícil acesso ou permanência de seres humanos, como exemplo áreas vulcânicas, florestas, geleiras, montanhas entre outros. Os protocolos geográficos aparecem como uma opção importante de roteamento, onde as mensagens são encaminhadas para um destino com base na localização geográfica não para uma identificação ou um endereço lógico, e não precisa guardar informações de topologia para encaminhar os pacotes, a única informação que deve ser guardada pelos nós da rede é a dos vizinhos diretos. Esta dissertação de mestrado apresenta uma alternativa de encaminhamento que utiliza o paradigma geográfico que é capaz de suportar consultas combinando técnicas de roteamento como: métricas de qualidade de enlace e técnicas de busca de múltiplos caminhos que não provoquem um tráfego excessivo de mensagens de controle, proporcionando para as aplicações um protocolo resiliente com caminhos de boa qualidade de transmissão. Os experimentos apresentam que o protocolo proposto é capaz de fornecer consultas e respostas com taxas de perda de mensagens consideravelmente menores, e caminhos de comunicação de melhor qualidade, inclusive em cenários em que a qualidade dos links é afetada pelas condições ambientais. Os resultados obtidos demonstram que a proposta deste trabalho fornece um alto grau de resiliência quando comparado com um protocolo geográfico clássico.

Palavras-chave: Roteamento Geográfico, Redes de Sensores Ambientais, Redes de Sensores Sem Fios, Qualidade de Serviço.

Abstract

The Environmental Sensors Networks (ESN) are formed by a set of sensors that support the applications of environmental management. They aim to collect data on the environment where sensors are implanted. The ESN are very important for understanding natural phenomena and especially phenomena that were previously not possible due to their occurrence in places of difficult access or permanence of human beings, for example volcanic areas, forests, glaciers, mountains and others. Geographic protocols appear as an important routing option, where messages are routed to a destination based on geographic location not for an identification or a logical address, and do not need to store topology information to route the packets, the only information that should be stored by the nodes of the network is that of the direct neighbors. This master dissertation presents a routing alternative that uses the geographical paradigm that is able to support queries by combining routing techniques such as link quality metrics and multipath search techniques that do not provoke excessive control message traffic by providing for applications a resilient protocol with good transmission paths. The experiments show that the proposed protocol is able to provide queries and responses with considerably lower message loss rates and better quality communication paths, even in scenarios where the quality of the links is affected by the environmental conditions. The results obtained demonstrate that the proposal of this work provides a high degree of resilience when compared with a classic geographic protocol.

Keywords: Geographic Routing, Environmental Sensor Networks, Wireless Sensor Networks, Quality of Service.

Lista de ilustrações

Figura 1 – Característica das redes sem fio.	26
Figura 2 – Consulta <i>RCD</i>	27
Figura 3 – Falha encaminhamento guloso, local máximo.	29
Figura 4 – Encaminhamento de face.	30
Figura 5 – Cálculo <i>ETX</i>	33
Figura 6 – Controle de caminhos com 3 <i>bits</i>	35
Figura 7 – Encaminhamento Guloso.	39
Figura 8 – A) Grafo não planar - B) Grafo planar.	39
Figura 9 – GEAR modo encaminhamento de face.	40
Figura 10 – Aprendendo rotas em volta do buraco.	42
Figura 11 – Encaminhamento Geográfico Recursivo.	43
Figura 12 – Parâmetro da região	47
Figura 13 – Controle de réplicas e cálculo do custo dos caminhos.	48
Figura 14 – A: Topologia com 20 nós. B: Topologia com 120 nós.	54
Figura 15 – A: <i>PMIRS</i> . B: <i>PMRRS</i> . C: <i>ETX-Path</i> . D: Contagem de Saltos	57
Figura 16 – Proporção de Mensagens de Interesse recebidas com sucesso.	60
Figura 17 – Média <i>ETX-Path</i>	61
Figura 18 – Proporção de Mensagens de Interesse recebidas com sucesso.	62
Figura 19 – Proporção de Mensagens de Resposta recebidas com sucesso.	63
Figura 20 – Média <i>ETX-Path</i>	64
Figura 21 – Média de Contagem de Saltos.	65

Lista de tabelas

Tabela 1 – Estrutura de dados para armazenar informações sobre os vizinhos de um nó	46
Tabela 2 – Parâmetros de Mensagem de Interesse	46
Tabela 3 – Exemplo de Mensagem de Interesse	49
Tabela 4 – Exemplo de Mensagem de Resposta	49
Tabela 5 – Entrada da tabela de interesse	50
Tabela 6 – Características de topologia	54
Tabela 7 – Grau médio de nó	55
Tabela 8 – Parâmetros de protocolo	55

Lista de abreviaturas e siglas

DODAG	Destination Oriented Directed Acyclic Graph
ETT	Expected Transmission Time
ETX	Expected Transmission Count
GAF	Geographic Adaptative Fidelity
GEAR	Geographical and Energy Aware Routing
GG	Gabriel Graph
GPS	Global Position System
GPSR	Greedy Perimeter Stateless Routing
LOCALMOR	LOCALized Multiobjectives Routing
MANET	Mobile Ad Hoc Network
MIE	Mensagens de Interesse enviadas
MIR	Mensagens de Interesse recebidas
MRE	Mensagens de Resposta esperadas
MRR	Mensagens de Resposta recebidas
PMIRS	Proporção de Mensagens de Interesse recebidas com sucesso
PMRRS	Proporção de Mensagens de Resposta recebidas com sucesso
QoS	Quality of Service
RCC	Rede Centrada em Conteúdo
RCD	Rede Centrada em Dado
RCI	Rede Centrada em Informação
RGPOP	Resilient Geographic Protocol Oriented to Path Quality
RNG	Relative Neighborhood Graph
RPL	Routing Protocol for Low-Power and Lossy Networks

RSA	Redes de Sensores Ambientais
RSSF	Redes de Sensores Sem Fio
TORA	Temporally Ordered Routing Algorithm
VANET	Vehicular Ad Hoc Network
WMN	Wireless Mesh Network
WSN	Wireless Sensor Network

Sumário

1	INTRODUÇÃO	19
1.1	Motivação	20
1.2	Objetivo	21
1.3	Estrutura do documento	22
2	REVISÃO DA LITERATURA	23
2.1	Rede de Sensores Ambientais	23
2.2	Rede de Sensores <i>Ad Hoc</i>	24
2.3	Rede Centrada em Dados	27
2.4	Rede baseada em Localização	28
2.4.1	Temas de pesquisa relacionados à protocolos geográficos	31
2.5	Métricas de qualidade de <i>link</i>	32
2.5.1	<i>Expected Transmission Count</i>	32
2.5.2	<i>Expected Transmission Time</i>	33
2.6	Controle de caminhos	34
3	TRABALHOS RELACIONADOS	37
3.1	<i>Greedy Perimeter Stateless Routing</i>	38
3.2	<i>Geographical and Energy Aware Routing</i>	40
3.3	Conclusão	43
4	<i>RESILIENT GEOGRAPHIC PROTOCOL ORIENTED TO PATH QUALITY</i>	45
4.1	Conceito e arquitetura	45
4.2	Especificação do protocolo	51
5	MÉTODO	53
5.1	Cenários	53
5.2	Modelo de tráfego	55
5.3	Métricas	56
5.4	Experimentos	57
6	RESULTADOS	59
6.1	Quantidade de réplicas do <i>RGPOP</i>	59
6.2	Proporção de Mensagens de Interesse recebidas	60
6.3	Proporção de Mensagens de Resposta recebidas com sucesso	61
6.4	Média <i>ETX-Path</i>	62

6.5	Média de Contagem de Saltos	62
6.6	Discussão	63
7	CONCLUSÃO	67
7.1	Publicação	68
	REFERÊNCIAS	69

1 Introdução

É notório o avanço industrial ininterrupto na área de microprocessadores e comunicação sem fio. Isso motivou o desenvolvimento e uso de sensores “inteligentes” que podem ser aplicados para monitoramento, gerenciamento e processamento para os mais variados contextos. Quando existe a necessidade do emprego de mais de um sensor para suprir uma determinada demanda, formam-se as chamadas redes de sensores sem fios (*RSSF*). As *RSSFs* apresentam variadas vantagens, dentre elas: baixo custo de implantação e ausência de infraestrutura, além disso a literatura apresenta um crescente número de pesquisas nesta área.

Os sensores (também denominados de nós sensores ou simplesmente nós) são pequenos dispositivos com capacidade de processamento e armazenamento reduzidas, tipicamente a fonte de energia deles é uma bateria finita. Devido a característica dos sensores terem a sua vida útil limitada à quantidade de energia residual, ao decorrer do tempo os nós desconectam-se da rede, causando descontinuidade afetando a comunicação dos nós.

Uma das aplicações importantes das *RSSF* são as redes de sensores ambientais (*RSA*). A *RSA* permite a conexão de uma grande variedade de dispositivos de monitoramento ambiental, enterrados no solo, posicionados na superfície ou imersos em rios e lagos (HART; MARTINEZ, 2006), (HAMILTON et al., 2007). O monitoramento ambiental é um conjunto de processos e atividades necessários para caracterizar e monitorar a qualidade do meio ambiente.

A *RSA* vem melhorando o monitoramento natural abrindo possibilidades de sensoriamentos de locais onde anteriormente era impossível. Esses sistemas permitem o estudo de processos fundamentais no meio ambiente, além de fornecer avisos de perigo vital por exemplo, alertas de inundação. Isto é particularmente importante em ambientes remotos ou perigosos onde muitos processos essenciais raramente foram estudados devido à sua inacessibilidade (HART; MARTINEZ, 2006).

Redes de sensores ambientais podem ser aplicadas para auxiliar em diversas pesquisas, coletando dados de ambientes que são de difícil acesso ou permanência aos seres humanos, alguns exemplos dessas aplicações são: Projeto *Volcán Tungurahua* e o projeto *GlacsWeb*. O primeiro projeto utilizou os sensores para monitorar atividades vulcânica através da utilização de microfones capazes de captar baixas frequências acústicas que é liberado durante a erupção. O segundo projeto utilizou sensores para compreensão dos processos subglaciais, embutindo os sensores na geleira coletando: pressão da água subglacial, temperatura, ângulo de inclinação e resistividade (HART; MARTINEZ, 2006).

1.1 Motivação

Como instrumento de coleta de dados no mundo natural, a *RSA* deve atender a um conjunto de requisitos, em particular, integração de sistemas e confiabilidade (CORKE et al., 2010). A integração do sistema significa a capacidade de fornecer dados aos usuários interessados, o que significa que a *RSA* é apenas parte de um sistema complexo que inclui links para servidores e bancos de dados. A *RSA* deve, portanto, suportar consultas para obter dados de sensores ambientais, periodicamente ou sob demanda.

A consulta é uma pergunta que contém alguns atributos específicos ao contexto aplicado, e pode ser respondida pelos nós da rede com os dados solicitados (ver exemplo de consulta na figura 2). Geralmente as consultas de *RSSF* são geográficas o que evita inundações, característica que contribui para economia de energia dos nós (YU; GOVINDAN; ESTRIN, 2001).

Embora a consulta seja uma característica importante para as *RSA* nem todos os protocolos propostos para as *RSSF* atendem esse requisito. Um dos motivos que dificulta o atendimento desse requisito é o paradigma de encaminhamento, que normalmente não suporta consulta (ver capítulo 2 sobre paradigmas de encaminhamento).

Como parte dos sensores das *RSA* podem ser introduzidos na rede de forma não sistematizada, por exemplo, lançados em uma região geográfica por um veículo aéreo, a abordagem de roteamento geográfico apresenta características adequadas para as *RSA*. Nessa abordagem, o roteamento de pacotes ocorre através das coordenadas dos nós, possibilitando a redução das mensagens de controle de topologia, assim reduzindo o consumo energético de cada nó. Os protocolos geográficos aparecem como uma abordagem de roteamento promissora para as redes de sensores ambientais, na qual os pacotes são encaminhados para o destino com base em sua posição geográfica e não em sua identidade ou endereço. Os protocolos geográficos são particularmente úteis para a *RSA* porque permitem que as consultas sejam encaminhadas para regiões em vez de um nó específico identificado pelo seu endereço.

O roteamento geográfico comumente utiliza duas técnicas para envio de dados: o encaminhamento guloso e o encaminhamento de face (CADGER et al., 2013). O encaminhamento guloso envia os dados sempre para o nó vizinho que está mais próximo do destino do que si mesmo. Devido aos nós sempre encaminharem os pacotes para os vizinhos mais próximos do destino, essa técnica pode falhar em redes que tenham baixa densidade. Isso é comum em *RSSF* não estruturadas, onde pode não ser possível recarregar as baterias dos nós (como nas *RSA*), ocasionando a perda de determinados nós da rede, formando assim o que na literatura é chamado de buraco, o que pode originar o problema do local máximo. O local máximo ocorre em um nó onde não existe nenhum vizinho mais próximo do destino do que si mesmo. A outra técnica é o encaminhamento de face, essa técnica é

aplicada em um grafo planar onde as arestas não se cruzam e realiza o encaminhamento pelas áreas poligonais formadas no sentido anti-horário até que a mensagem chegue ao destino. A principal limitação do encaminhamento é o alto custo computacional para transformação do grafo de comunicação da *RSSF* em um grafo planar (CADGER et al., 2013) o que contribui para que o encaminhamento de face tenha um custo computacional muito alto.

Um fator muito importante para o funcionamento das *RSSFs* é a capacidade dos nós se auto organizarem superando as falhas através da criação de caminhos alternativos para alcançar o destino. Essa capacidade contribui para a resiliência da rede, já que com a utilização de múltiplos caminhos, se ocorrer falha no caminho principal o protocolo pode realizar o encaminhamento por caminhos alternativos evitando que afete na recepção de dados.

Os nós em uma *RSSF* colaboram uns com os outros para realizar a transmissão de dados, durante esse processo a transmissão está sujeita a erro causados por ruídos, sombreamento e interferências, gerando perda de pacotes. Por se tratar de uma rede muito dinâmica é importante que seja levada em consideração a qualidade dos enlaces. Uma forma de medir a qualidade do enlace é por meio da métrica *ETX*, o qual estima a quantidade de transmissões e retransmissões necessárias para enviar um pacote por um enlace. Desta forma é possível evitar os enlaces mais afetados, transmitindo por enlaces de boa qualidade.

Na literatura foram encontradas diversas propostas com objetivos para resolver um ou mais dos requisitos aqui apresentados, e que foram enunciados pelos autores (CORKE et al., 2010). Porém nenhuma delas consideram a utilização das seguintes características ao mesmo tempo: capacidade de realizar consultas, criação de múltiplos caminhos, qualidade de caminhos e independência de identidade ou endereço para entrega de pacotes. Essas características contribuem para que seja atendido o conjunto de requisitos para as *RSA*.

1.2 Objetivo

Considerando os problemas apresentado anteriormente, esta pesquisa pretende responder a seguinte questão: **é vantajoso desenvolver protocolos de roteamento geográfico para *RSA* que levem em conta múltiplos caminhos e a qualidade dos enlaces de comunicação em *RSSF*?** E para responder esta questão o objetivo geral desta dissertação é: **a idealização e implementação de um protocolo de roteamento geográfico capaz de encontrar caminhos resilientes e com boa qualidade para as *RSA*.** O protocolo proposto deverá suportar consultas e combinar técnicas de roteamento como: métricas de qualidade de enlace e técnicas de busca de múltiplos caminhos que não provoquem um tráfego excessivo de mensagens de controle. Essas aplicadas sobre o

paradigma de roteamento geográfico, que é imprescindível em muitas aplicações de *RSA*, e por utilizar poucas mensagens para manter a topologia da rede, apresenta baixa sobrecarga. O intuito é transmitir uma maior quantidade de dados, assim melhorando a experiência do usuário final, através de caminhos de boa qualidade.

Para atender ao objetivo principal da pesquisa, são apresentados os seguintes objetivos específicos a serem atingidos:

- Levantamento bibliográfico;
- Especificação do protocolo;
- Implementação do protocolo;
- Implementação do protocolo de comparação;
- Planejamento e validação dos experimentos;

1.3 Estrutura do documento

O capítulo 1 apresentou o contexto no qual esse trabalho está inserido, ainda definiu a motivação, questão de pesquisa e os objetivos para responder à questão de pesquisa.

O capítulo 2 apresenta os conceitos relacionados as redes de sensores *Ad Hoc*, paradigmas de roteamento, além de apresentar alguns temas relacionados aos protocolos geográficos, incluído métricas de qualidade de enlace e a técnicas de busca e controle de múltiplos caminhos.

O capítulo 3 apresenta alguns trabalhos relacionados ao tema de pesquisa, descrevendo com mais detalhes os trabalhos que foram utilizados para avaliar o protocolo proposto.

O capítulo 4 apresenta a proposta deste trabalho, organizado da seguinte forma: conceito, arquitetura e a especificação do protocolo.

O capítulo 5 apresenta os resultados, bem como descreve a forma que foram conduzidos os experimentos, detalhando os cenários, parâmetros de configuração e as métricas utilizadas para avaliação.

Por final o capítulo 6 apresenta a conclusão desta dissertação, ressaltando as características que favorecem a proposta deste trabalho alcançar melhores resultados em *RSA* quando comparado aos protocolos tradicionais de *RSSF*.

2 Revisão da Literatura

Nesse capítulo é realizada uma revisão da literatura sobre o tema da dissertação, com objetivo de definir os termos e conceitos envolvidos no trabalho. A revisão foi conduzida em uma abordagem do geral para o particular, iniciando com conceitos mais gerais até chegar nos conceitos mais específicos relacionados ao tema. Essa abordagem permite ainda contextualizar o tema dentro da área de pesquisa de redes de sensores ambientais.

Esse capítulo inicia com as redes de sensores ambientais e segue com uma apresentação das redes de sensores sem fio *Ad Hoc*, uma das grandes categorias de redes de sensores sem fio, contrapondo-se às redes de sensores sem fio estruturadas. Com o objetivo de contextualizar o tema, é apresentada uma categorização dos protocolos usados nas redes de sensores sem fio *Ad Hoc*, com base no estudo de (YANG, 2013). Em seguida, apresenta-se as redes centradas em dados, conduzindo às redes de sensores baseadas em localização, que são o objeto desse estudo.

Apresentamos também uma breve discussão sobre métricas de qualidade de enlace em redes sem fio. O motivo dessa discussão é que nesse estudo vamos propor novos protocolos para redes de sensores baseadas em localização, levando-se em conta a qualidade dos enlaces nas rotas de comunicação. Uma abordagem que é pretendida seguir é explorar estratégias de múltiplos caminhos. Por essa razão também foi incluído nesse capítulo a discussão de um algoritmo de controle de múltiplos caminhos, que também faz parte da investigação.

2.1 Rede de Sensores Ambientais

As Redes de Sensores Ambientais são formadas por um conjunto de sensores que suportam as aplicações de gestão do meio ambiente. Têm como finalidade coletar dados sobre o ambiente onde os sensores estão implantados, conseqüentemente, facilitando o monitoramento de ambientes que são normalmente inóspitos para os seres humanos, coletando informações essenciais para entendimento de fenômenos que antes não era possível. Anteriormente os sistemas de coleta eram através de sistema de log passivos o qual era necessário download manual dos dados, algo que limita o sensoriamento em casos onde não é possível a presença humana. Atualmente, para muitas aplicações, o objetivo é ir em direção às RSSF, pois os cabos são geralmente impraticáveis, intrusivos e podem perturbar o ambiente que está sendo monitorado (HART; MARTINEZ, 2006).

2.2 Rede de Sensores *Ad Hoc*

Uma rede de sensores *Ad Hoc* é caracterizada por não possuir uma infraestrutura física, e pela sua organização ser descentralizada, onde cada nó ou host se auto organiza com outros nós, fechando conexões entre eles assim formando canais de comunicação que são utilizados para trocas de informações (BROCH et al., 1998). Após estabelecida as conexões entre os dispositivos através do conceito *Ad Hoc*, é possível que um nó que não tenha conexão direta com um determinado nó na rede, possa enviar dados através das conexões formadas, de salto em salto, até atingir o nó para qual a informação deve chegar. A decisão de roteamento é tomada individualmente a cada salto, e se adapta dinamicamente às condições da rede (ALOTAIBI; MUKHERJEE, 2012).

Por se tratar de uma rede sem infraestrutura definida e altamente dinâmica, existem várias aplicações para redes *Ad Hoc* em locais onde não se dispõe de uma infraestrutura instalada. De acordo o cenário de utilização, as *Ad Hoc* são usualmente classificadas do seguinte modo (AMADEO et al., 2014):

Rede *Ad Hoc* Móvel (termo em inglês, *Mobile Ad Hoc Network - MANET*): É uma rede no qual os nós, que também são chamados de roteadores, podem se mover arbitrariamente. Esses nós podem ser aplicados em carros, aviões, navios entre outros. A rede tem a capacidade de auto-organização, e pode comunicar-se com outros pontos isolados da rede (CORSON; MACKER, 1998).

Rede *Ad Hoc* Veicular Móvel (termo em inglês, *Vehicular Ad Hoc Network - VANET*): A rede veicular móvel *VANET* é uma variante da rede móvel *MANET*, porém com aplicação específica para veículos e rodovias. A rede inclui coleções de veículos e de elementos rodoviários conectados entre si, comunicando-se uns com os outros (HARTENSTEIN; LABERTEAUX, 2008).

Rede em Malha sem Fio (termo em inglês, *Wireless Mesh Network - WMN*): As redes em malha sem fio (*WMN*) diferente das *MANET* são organizadas em nós roteadores e nós clientes. Os roteadores são os nós que fornecem a conectividade com outros roteadores formando um *backbone* para que os nós clientes possam conectar-se. Os roteadores podem ter mais de uma interface de rede sem fio servindo como *gateway* para outra *WMN* ou para a internet. Os nós clientes podem também servir como roteadores, para o envio de dados entre outros nós, mas possuem um protocolo de comunicação mais simples quando comparado ao protocolo do nó roteador, não tendo a característica de *gateway* e *bridge*, e dispõem apenas de uma interface de rede sem fio (AKYILDIZ; WANG, 2005).

Redes de Sensores sem Fio (termo em inglês *Wireless Sensor Network - WSN*): A Rede de Sensor sem Fio (*RSSF*) é uma rede no qual tem como característica de monitoramento de um determinado ambiente ou fenômeno, normalmente implantados centenas ou milhares de nós sensores em locais de difícil acesso para seres humanos. Os

nós se conectam uns com os outros cooperando, formando uma rede conectada, podendo ter um ou mais nó sorvedouro (termo em inglês *sink*), que é o gateway da rede para onde as informações coletadas pelos sensores devem escorrer. Para cumprir esse objetivo são utilizados pequenos sensores, visando baixo custo e a longevidade da rede que por sua vez é definida pela carga residual de energia na bateria do nó. Esses nós sensores possuem baixo poder de processamento, armazenamento e energia finita determinada pela bateria. Por serem empregados em locais de difícil acesso e sem estrutura de rede elétrica a vida/bateria dos nós geralmente não são renováveis, sendo assim a rede permanece em funcionamento enquanto houver comunicação entre os nós até o nó *sink*.

Um dos principais desafios das *RSSFs* é utilizar eficientemente os recursos de energia, processamento e memória, de maneira que atenda a finalidade da rede. Sabendo que o rádio transmissor é o maior responsável pelo consumo de energia, a comunicação entre os nós sensores devem seguir uma estratégia para prolongar a vida da rede, tendo em vista o poder computacional e de armazenamento.

Esse trabalho aborda as *RSSFs*, visando a monitoração do meio ambiente, contribuindo com métodos e protocolos para coleta de informações tais como temperatura, umidade, pressão, acústico, sísmico entre outros. As informações estarão disponíveis para aplicações que poderão fazer inferências sobre a situação do meio ambiente, podendo ser usadas, por exemplo, para identificar um aumento brusco na temperatura, o que poderia indicar a ocorrência de um incêndio florestal, ou a diminuição nos níveis de umidade poderia ainda indicar que está havendo desmatamento da área, entre outras inferências que podem ser feitas com base nas informações coletadas.

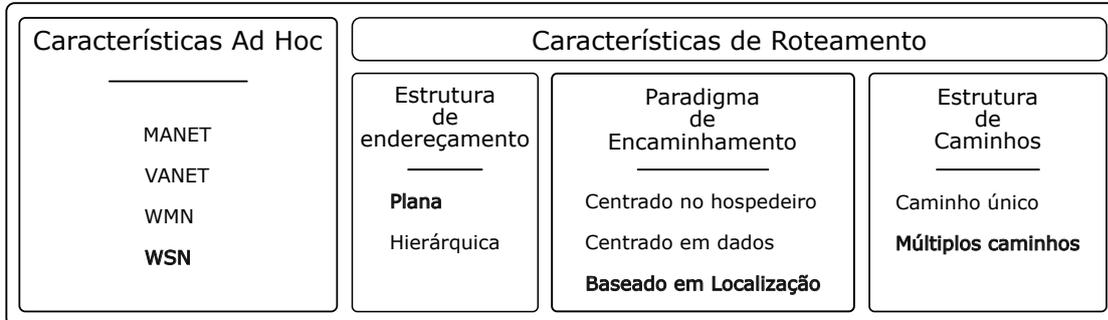
Para que seja possível realizar as coletas de informações é necessária uma camada de *software* sobre o *hardware* dos nós sensores. Essa camada realiza operações de trocas de mensagens entre os nós seguindo regras, ou seja, um protocolo de comunicação, cujo objetivo é gerar conexões entre os nós seguindo uma estratégia.

Após encontrar alguns trabalhos que classificam os protocolos de roteamento, tais como (AL-KARAKI; KAMAL, 2004; SINGH; SHARMA, 2015; GOYAL; TRIPATHY, 2012), foi constatado que não existe uma classificação padrão adotada por todos os autores. Nesse trabalho adota-se uma classificação semelhante ao autor (YANG, 2013), que identifica características de roteamento flexíveis, classificando um protocolo de acordo com a existência de uma ou mais dessas características presente em seu funcionamento. Existem protocolos que adotam várias estratégias diferentes e com isso não é possível classificá-lo segundo apenas uma determinada característica.

A figura 1 apresenta duas grandes características, a primeira referente às redes *Ad Hocs* apresentada anteriormente. E a segunda lista algumas características de roteamento mais relevantes consideradas na classificação utilizada. Os itens em negritos na figura 1 são as áreas de estudo deste trabalho. As características de roteamento agrupam-se em três

grandes áreas:

Figura 1 – Característica das redes sem fio.



Fonte: Autoria Própria

A estrutura de endereçamento, que classifica os protocolos segundo à estrutura dos endereços que suportam o roteamento e encaminhamento das mensagens. Essa categoria foi dividida em duas subcategorias plana e hierárquica. A estrutura de endereçamento plano não há níveis entre os nós da rede, tratando todos os nós igualmente quando falamos de roteamento. Na estrutura hierárquica os nós desempenham diferentes funcionalidades, existindo níveis na rede no qual os nós que estão abaixo devem reportar ao nó superior a ele.

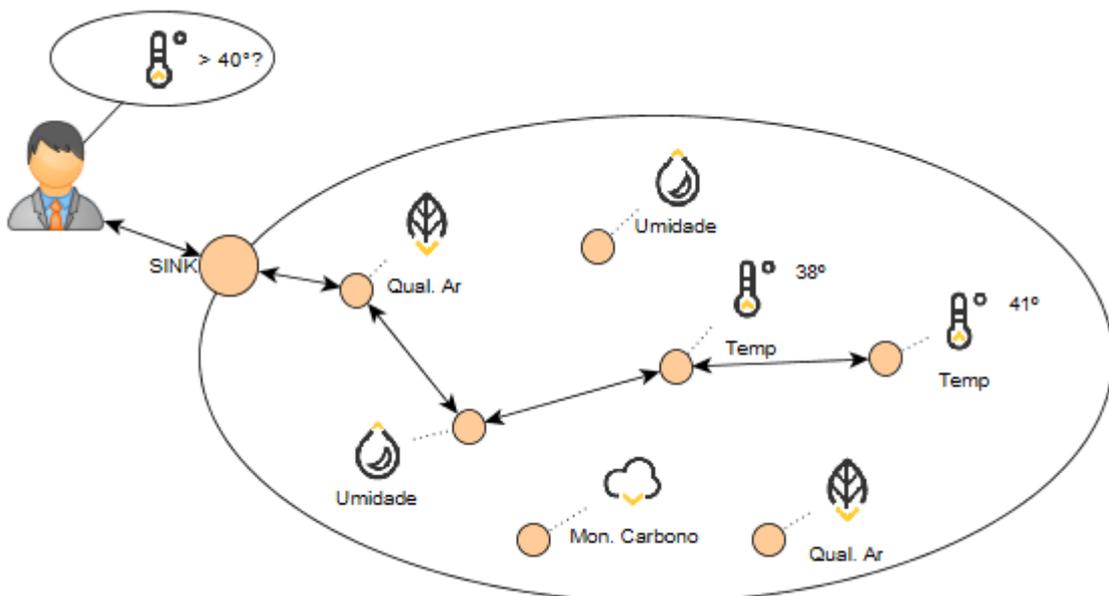
Foram classificados três paradigmas de encaminhamento: o paradigma centrado no hospedeiro que deu surgimento para a rede que conhecemos hoje como internet; o paradigma centrado em dados, que é voltado para recuperação de dados; e o paradigma baseado em localização, onde os nós realizam o encaminhamento considerando as posições geográficas da origem, destino e dos nós envolvidos. O paradigma centrado no hospedeiro foi concebido para conectar máquinas umas às outras, com a finalidade de compartilhamento de recursos considerados caro na época do seu surgimento. A sua principal característica é que cada *host* na rede tem um identificador único, através desse identificador é possível localizar um computador ou dispositivo conectado na rede e realizar comunicação entre eles. O paradigma centrado em dados trabalha com identificadores da informação, sem a existência de identificadores (endereços) para *hosts* e dispositivos da rede. Esse paradigma foi concebido para trabalhar com solicitação de dados independente onde esteja esses dados, desacoplando os dados de um endereço específico (XYLOMENOS et al., 2014). O paradigma baseado em localização os nós têm consciência de sua localização por meio de *GPS* (*Global Position System*) ou por outro método. O encaminhamento de requisições é feito através da informação de localização, não é necessário o endereço de um nó para encaminhar as requisições, apenas uma região definida por coordenadas geográficas (AL-KARAKI; KAMAL, 2004).

Estrutura de caminhos: Um caminho é definido pelo conjunto de nós e enlaces que são percorridos para realizadas a transmissão de uma mensagem a partir do nó origem até o nó de destino. Existem protocolos classificados como caminho único o qual possui como rota apenas um trajeto entre a origem e o destino, e o múltiplos caminhos, que tem como característica ter mais de um caminho entre eles. Os principais objetivos de utilização de um roteamento com múltiplos caminhos são o desempenho, o balanceamento de carga, e a tolerância a falhas (AKYILDIZ; WANG, 2005).

2.3 Rede Centrada em Dados

Diferentemente das redes de computadores tradicionais, que foram criadas para conectar máquinas ponto a ponto, as redes centradas em dados (*RCD*) (*Data-Centric Network*) têm como objetivo o acesso e a comunicação de informações, independentemente de seu endereço físico (XYLOMENOS et al., 2014). As *RCD* utilizam protocolos que são capazes de responder consultas realizadas pelo usuário através do nó *sink*, não especificando o endereço de um nó, mas em qual informação está interessado. Esses protocolos mantêm o foco nos dados, o que possibilita consultas contendo atributos relacionados à informação, nos quais os nós *sink* têm a capacidade de responder às questões feitas à rede, comparando informações coletadas com os atributos especificados na consulta (ANISI et al., 2012).

Figura 2 – Consulta *RCD*.



Fonte: Autoria Própria

A figura 2 demonstra um exemplo de uma consulta feita por um usuário através do nó *sink*. No exemplo existem vários nós em uma área, cada nó com um sensor capaz

de realizar medições individuais. A consulta é feita como uma pergunta contendo um ou mais atributos, devendo retornar apenas resultados que se encaixem dentro da solicitação. No exemplo, o retorno esperado é de nós que tenham o valor do atributo temperatura acima de 40 graus célsius, e a consulta terá como retorno a informação do nó que possui a temperatura de 41°C. Caso a consulta fosse realizada para temperatura maior que 36°C, teríamos dois retornos, o nó com 38°C e o nó com 41°C.

As *RCDs* também são referenciadas como redes centradas em informação (*RCI*) (*Information-Centric Network*) (FAYAZBAKHS et al., 2013; PHAM, 2015). Alguns autores ainda classificam *RCD*, e *RCI* como sinônimos de rede centrada em conteúdo (*RCC*) (*Content-Centric Network*) (KARAMI; GUERRERO-ZAPATA, 2015a; KARAMI; GUERRERO-ZAPATA, 2015b). Nesse trabalho será utilizado o termo *RCD* como sinônimo de *RCI* e *RCC*.

2.4 Rede baseada em Localização

As redes baseadas em localização, diferentemente das tradicionais que encaminham os pacotes em direção a uma identificação ou um endereço lógico, realizam o encaminhamento de pacotes levando em consideração de seu posicionamento geográfico (CADGER et al., 2013). Esse posicionamento geográfico normalmente é obtido através do Sistema de Posicionamento Global (*Global Positioning System - GPS*) (LEMMON; LUI; LEE, 2009). Outro método que também pode ser utilizado para obter o posicionamento geográfico, é o método baseado em triangulação, permite que os nós sensores aproximem sua posição usando a força do rádio de alguns pontos conhecidos (AL-KARAKI; KAMAL, 2004).

Os protocolos de roteamento geográficos não precisam guardar informações de topologia para encaminhar seus pacotes, a única informação que deve ser guardada pelos nós da rede é a dos vizinhos diretos. Uma vez que os pacotes são encaminhados de salto em salto, selecionando em sua tabela de vizinhos, o vizinho mais apropriado com base em alguns critérios específicos de cada protocolo e, principalmente levando em conta o posicionamento geográfico até o pacote chegar em seu destino. Por não precisar manter informações de topologia da rede, isso significa que não é necessária manutenção da tabela de rotas, então não gera trocas de mensagens entre os nós para manter a topologia, evitando assim gastos de energia (CADGER et al., 2013).

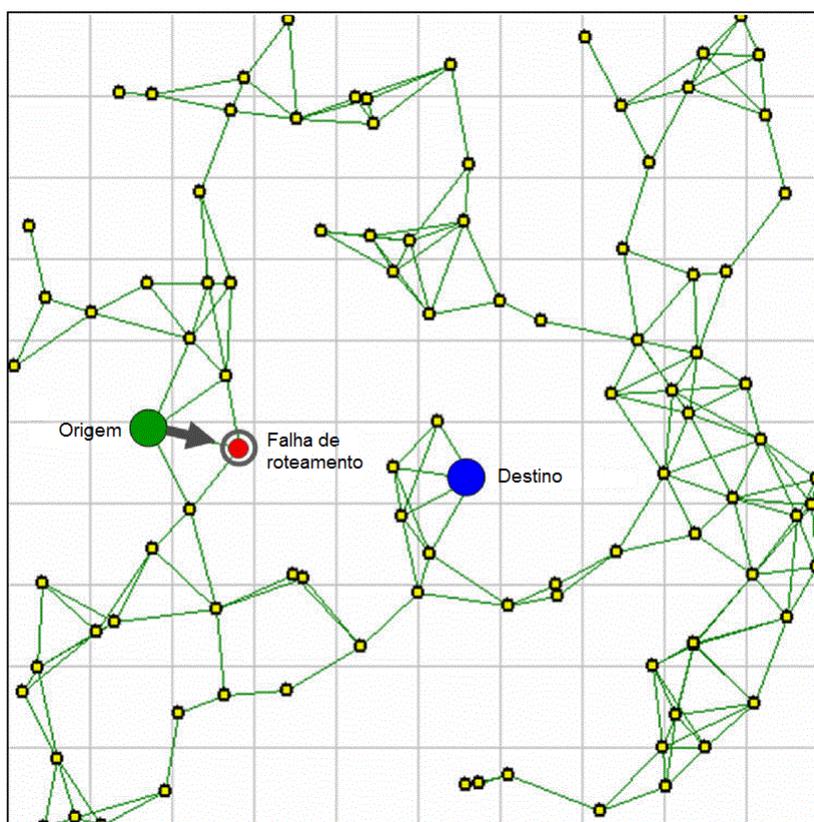
Dentro das redes baseadas em localização existem duas principais estratégias para encaminhamento de dados, são elas a estratégia gulosa e a estratégia encaminhamento de face (CADGER et al., 2013).

A estratégia gulosa é a estratégia mais antiga e também considerada a mais simples. Durante seu funcionamento, os pacotes são encaminhados optando-se sempre pelo vizinho que está mais próximo do destino, não levando em consideração o escopo global. A

estratégia gulosa é a mais eficiente, com a complexidade de pior caso de $O(d^2)$ onde d representa a distância entre a fonte e o destino.

A estratégia gulosa tem um sério problema. Devido ao envio dos pacotes para o vizinho que está mais próximo do destino, ela não garante a entrega, podendo ocorrer situações onde um pacote é encaminhado para um nó vizinho mais próximo do destino, mas que a partir desse nó não existam vizinhos mais perto que ele mesmo (CADGER et al., 2013). A situação mencionada é ilustrada na figura 3, o nó origem (verde) precisa encaminhar uma mensagem para o nó destino (azul), e encaminha o pacote para o vizinho mais próximo do destino (vermelho). A estratégia gulosa falha no nó vermelho por não existir nenhum outro nó mais próximo do destino do que ele mesmo. Essa situação é chamada de local máximo, na qual mesmo sendo possível chegar através de outros caminhos até o destino, o algoritmo guloso não é capaz encontrá-lo. O significado do nome local máximo para essa situação, é que o caminho encontrado até o nó onde o pacote chegou é o maior caminho que poderia ser percorrido com a estratégia gulosa.

Figura 3 – Falha encaminhamento guloso, local máximo.



Adaptado de: (LEMMON; LUI; LEE, 2009)

A estratégia encaminhamento de face é muitas vezes utilizada como alternativa ao encaminhamento guloso. As primeiras propostas de protocolos seguindo a estratégia

encaminhamento de face foram *Compass II* e *Face-2* em 1999 (RUHRUP, 2009).

O funcionamento da estratégia encaminhamento de face consiste em traçar uma reta r entre a origem e o destino, sendo que o pacote percorrerá uma sequência de faces (polígonos) adjacentes à reta r até atingir o destino. Como mostrado na figura 4, foi traçada uma reta r entre os nós de origem (o) até o nó de destino (d), e cada um dos nós encaminha o pacote no sentido anti-horário por dentro da face (cada um dos polígonos). Quando o encaminhamento no sentido anti-horário por dentro da face ocorrer por uma aresta que cruza a reta r , então o pacote é encaminhado para outra face assim sucessivamente até o pacote atingir o nó d (RUHRUP, 2009).

Antes da aplicação da estratégia encaminhamento de face é necessário empregar um processo de planarização do grafo que representa a topologia da rede. A planarização transforma o grafo em um grafo planar, onde as arestas do grafo não se cruzam e são compostos por uma sequência de regiões poligonais (CADGER et al., 2013). Detalhes dos algoritmos de planarização podem ser vistos em (YU; GOVINDAN; ESTRIN, 2001).

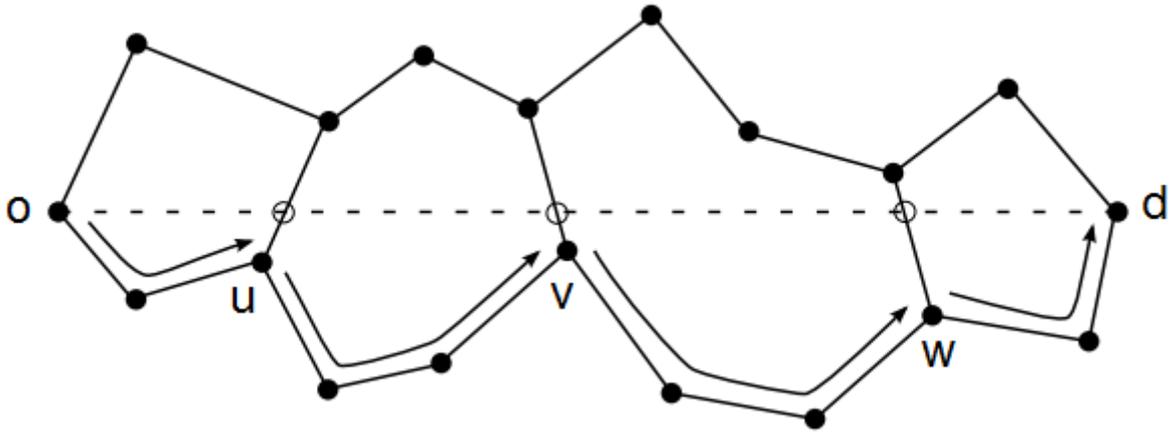
Uma terceira abordagem para os protocolos geográficos é denominada de estratégia híbrida, que corresponde a aplicar uma estratégia de recuperação quando o encaminhamento guloso encontra o problema do local máximo. Essa estratégia consiste em combinar a estratégia gulosa e a estratégia de face, alternando entre os modos de operação. Na estratégia híbrida, sempre que possível os pacotes são enviados utilizando a estratégia gulosa, isso porque o encaminhamento guloso é geralmente mais eficiente do que o encaminhamento de face. O protocolo é iniciado no modo guloso e ao encontrar um local máximo é alternado para o modo encaminhamento de face. Quando o encaminhamento se recupera do problema do local máximo, o modo de operação volta para o encaminhamento guloso (CADGER et al., 2013).

2.4.1 Temas de pesquisa relacionados à protocolos geográficos

Os protocolos geográficos foram estudados em diversos temas de pesquisa. Alguns dos temas em aberto citados pelos autores (CADGER et al., 2013) são:

- Recuperação do local máximo: O local máximo ocorre devido a utilização do encaminhamento guloso, o qual sempre faz a melhor escolha local. Por ser um algoritmo simples e ao mesmo tempo eficiente, é muito utilizado, porém nem sempre a melhor escolha local é a melhor escolha no escopo global. As redes *RSSFs* são alimentadas em sua maioria por baterias, e em algum momento em que a rede está em funcionamento, alguns nós podem ter a sua carga da bateria esgotada devido a utilização natural dos recursos, fazendo com que a rede venha a ter buracos. Um buraco corresponde à situação exemplificada na figura 3. A recuperação de local máximo estuda formas alternativas de contornar buracos de maneira eficiente, sendo uma delas a utilização da estratégia encaminhamento de face

Figura 4 – Encaminhamento de face.



Adaptado de: (RUHRUP, 2009)

(CADGER et al., 2013).

- Economia de energia: Como mencionado anteriormente as *RSSFs* na maior parte dos casos são alimentadas por baterias, as quais em funcionamento acabam esgotando o nível residual de energia. Quando um nó tem a sua bateria sem carga, ele se desliga tornando-se incomunicável. Sendo assim, a área de pesquisa de economia de energia foca seus esforços para prolongar a vida útil da rede, minimizando o consumo dos nós durante as operações (CADGER et al., 2013).

- Qualidade de serviço: Se preocupa em melhorar a qualidade da experiência do usuário final. Segundo os autores (CADGER et al., 2013) *QoS* é um campo emergente na área de redes *Ad Hoc* com muitos desafios para superar. Esse campo de pesquisa trabalha com políticas de qualidade que devem ser cumpridas para tornar a experiência do usuário final melhor, procurando melhores métricas para encaminhamento de pacotes (CADGER et al., 2013).

- Roteamento 3D: Em muitos casos os nós sensores são empregados em áreas nas quais tem grandes diferenças de altitude um nó para o outro, por exemplo em montanhas, arvores, solo entre outros. Essas variações de altura dos nós não são tratadas nos protocolos geográficos comuns, que utilizam apenas o plano 2D. A área de estudo dos protocolos com roteamento 3D visa lidar com coordenadas tridimensionais, lidando corretamente com demandas 3D (CADGER et al., 2013).

O foco de investigação desse trabalho será qualidade das rotas de comunicação, que é fortemente dependente da qualidade dos enlaces entre os diversos nós que compõem as rotas. Por essa razão, na sequência vamos discutir as principais métricas de qualidade

de enlace em redes sem fio.

2.5 Métricas de qualidade de *link*

Neste subcapítulo serão apresentados duas das principais métricas utilizadas em redes sem fio. A primeira chamada de *ETX*, avalia a quantidade necessária de transmissão e retransmissão para enviar um pacote. A segunda métrica a *ETT* que é uma variante da métrica *ETX*, com foco no tempo de transmissão de um pacote.

2.5.1 *Expected Transmission Count*

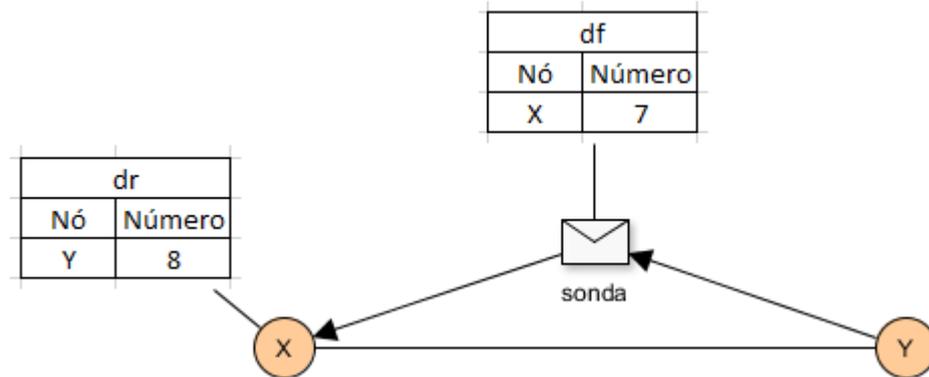
O *expected transmission count (ETX)* é uma métrica que avalia a qualidade dos enlaces em redes sem fio. O valor de *ETX* de um *link* é o número previsto de transmissões e retransmissões de dados necessários para enviar um pacote por este *link*. *ETX* é uma métrica cumulativa, e o valor de *ETX* de um caminho é dado pela soma do *ETX* de cada salto até o destino (COUTO et al., 2005).

O cálculo do *ETX* de um *link* utiliza as probabilidades de entrega em direção ao destino (“*forward*”), representada por *df*, e a probabilidade entrega na direção reversa (“*reverse*”), é representado por *dr*, correspondendo à probabilidade de que o pacote *ACK* seja recebido com êxito. A probabilidade de sucesso de uma transmissão em ambos os sentidos (“*forward*” e “*reverse*”) é *df.dr*. Portanto a métrica *ETX* é dada por (COUTO et al., 2005):

$$ETX = \frac{1}{df.dr}$$

Para calcular *df* e *dr* são enviadas mensagens chamadas de sonda (*probe*). Essas mensagens são enviadas por *broadcast* em um intervalo de tempo *t* (definido pelo autor como 1 segundo). Para evitar que ocorra o envio sincronizado dessas mensagens, o período de envio é variado em até +/- 10%. Os pacotes de sondas são enviados em *broadcast* para não ter a confirmação ou retransmissão em caso de falhas. O controle de entrega é feito através do próprio pacote. Cada sonda contém o número de pacotes de sondas recebido de cada vizinho do nó *X* durante uma janela de tempo *w* (utilizado pelo autor 10 segundos), permitindo que cada nó ao receber esse pacote possa calcular o *df* para *X*. Além de calcular o *df*, o nó receptor da sonda armazena no período de tempo *w* a mensagem que chegou de *X*, gerando uma base de dados para calcular o *dr* (COUTO et al., 2005).

A figura 5 é um exemplo de como funciona o cálculo do *ETX*. Nesse exemplo é realizado o cálculo do *ETX* entre os nós *X* e *Y*, do ponto de vista do nó *X*. No exemplo o nó *X* está recebendo um pacote sonda do nó *Y* com as informações referente ao nó *X*,

Figura 5 – Cálculo *ETX*.

Fonte: Autoria Própria

total de 7 pacotes recebidos do nó *X* pelo nó *Y* na janela de tempo w (foi assumido o valor de w 10s e t 1s) e t de intervalo entre os pacotes. O nó *X* tem armazenado a quantidade de sondas recebidas de *Y* na janela w que são 8 pacotes. Com essas informações, são substituídos os elementos da formula anterior da seguinte maneira para calcular o *ETX* (COUTO et al., 2005):

$$ETX = \frac{1}{\frac{7}{(w/t)} \frac{8}{(w/t)}}$$

$$ETX = \frac{1}{\frac{7}{(10/1)} \frac{8}{(10/1)}}$$

2.5.2 Expected Transmission Time

O *expected transmission time* (*ETT*) foi proposto para tratar o tempo médio necessário para transmitir um pacote. O *ETT* utiliza um pacote mais próximo do tamanho médio de um pacote de dados para calcular a média de tempo de transmissão. Essa abordagem é considerada como um *ETX* ajustável à largura de banda (DRAVES; PADHYE; ZILL, 2004). Assim sendo, o *ETT* pode ser considerado um complemento do *ETX*. O cálculo do *ETT* é realizado através da multiplicação do *ETX* pela largura de banda do *link* para obter o tempo gasto na transmissão do pacote, onde S representa o tamanho do pacote e B a largura da banda do *link*:

$$ETT = ETX \frac{S}{B}$$

A largura de banda é medida utilizando pares de pacotes. Cada nó envia dois pacotes a cada minuto para seus vizinhos. A primeira sonda é pequena com o tamanho de 137 bytes, enquanto que a segunda sonda é grande com 1137 bytes. Ao receber os pacotes, o vizinho calcula a diferença entre a recepção da primeira e da segunda sonda, e comunica o valor para o remetente. O nó que originou o par de sonda deve ter algumas amostras do atraso armazenadas (janela de 10 amostras), e divide o tamanho do segundo pacote de sonda pelo menor número de atraso (DRAVES; PADHYE; ZILL, 2004).

A métrica *ETT* também é cumulativa, ou seja, para calcular o *ETT* de uma rota basta somar o *ETT* dos enlaces individuais. Quanto menor o *ETT* significa que a rota é melhor (DRAVES; PADHYE; ZILL, 2004).

2.6 Controle de caminhos

O controle de caminhos é um mecanismo proposto para o protocolo *RPL* (*Routing Protocol for Low-Power and Lossy Networks*), que tem como objetivo controlar o número máximo de mensagens enviadas para a construção de múltiplas rotas em direção a um nó folha, e a priorização de caminho quando existem vários caminhos (PATH-CONTROL, 2016). O protocolo *RPL* realiza o encaminhamento através da construção de um grafo denominado *Destination Oriented Directed Acyclic Graph* (*DODAG*), que cria uma estrutura sem ciclos sobre as quais são construídas as rotas para atingir o nó *sink*, onde os nós para os quais cada nó deve encaminhar as mensagens em direção ao *sink* são chamados de pais.

Essa técnica adiciona na mensagem de divulgação de rotas, um mapa de *bits* que controla o número máximo de mensagens que cada nó pode enviar aos seus nós pais. Esse mapa de *bits* tem o tamanho de 8 *bits*, sendo que cada *bit* ativo representa uma mensagem que pode ser enviada para um nó pai. Quanto um *bit* está ativo é representado pelo número 1 e inativo número 0. Isso quer dizer que um mapa de *bits* representado por "00000111" tem 3 *bits* ativos.

O tamanho do controle de caminhos é definido por uma constante e pode variar de acordo com a configuração do protocolo. Os *bits* têm uma prioridade, quanto mais à direita, mais prioritário do que os *bits* mais à esquerda.

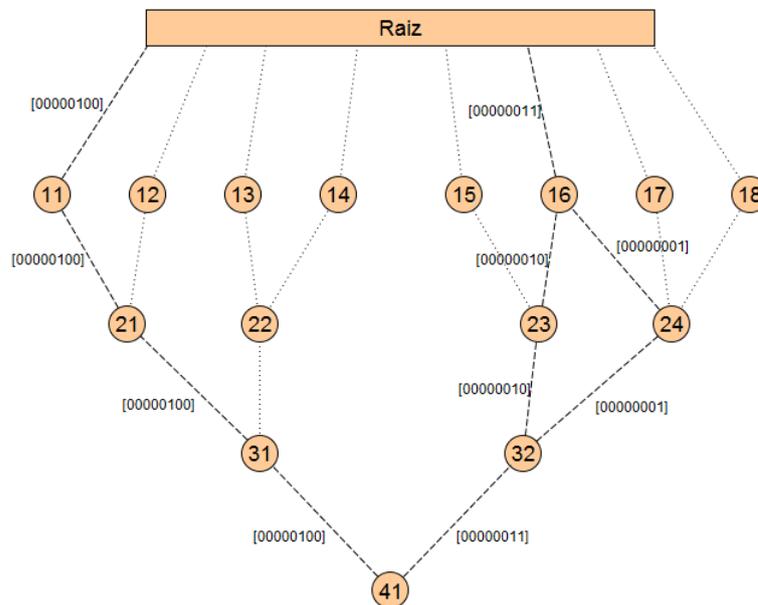
Como mencionado, o número de *bit* determina quantas mensagens de divulgação de rotas podem ser enviadas, supostamente um nó recebe uma mensagem de divulgação de rotas com um *bit* ativo pode encaminhar apenas para um pai, mesmo que tenha outros pais.

No caso que um nó recebe dois *bits* (ou mais) esses *bits* podem ser divididos em duas mensagens caso haja mais de um pai para o nó que recebeu o mapa de *bits*, o *bit* mais prioritário é enviado para o pai preferencial e o menos prioritário para o pai com

menor preferência.

Quando um nó recebe uma mensagem de divulgação de rotas com mais *bits* do que o número de pais que esse nó tem, os *bits* são distribuídos proporcionalmente entre as mensagens de divulgação de rotas para os nós pais. Um nó pode receber de seus nós filhos a mesma mensagem de divulgação de rotas com mapa de *bits* diferentes (*bits* em posições diferentes), quando ocorre essa situação o nó que recebeu a mesma mensagem com mapa de *bits* diferentes realiza o *merge* das mensagens e encaminha para frente de acordo com o número de pais e número de *bits*.

Figura 6 – Controle de caminhos com 3 *bits*.



Fonte: Autoria Própria

A figura 6 é um exemplo de aplicação do controle de caminhos. O nó 41 divulga uma mensagem com 3 *bits* e tem apenas dois pais, então é dividido os *bits* entre os pais priorizando o pai com maior preferência. Quando o nó 31 recebe a mensagem é escolhido no conjunto de pais o pai com maior preferência e então encaminha seu único *bit* por ele e assim acontece com o nó 21 até a mensagem com o *bit* "00000100" chegar ao nó raiz. O nó 32 recebe uma mensagem com dois *bits* ativos divide os dois e encaminha para seus pais (nó 23 e 24). Os nós 23 e 24 tem o mesmo pai como preferencial o nó 16, nesse caso é enviado as duas mensagens para o nó 16 que recebe e realiza o *merge* das mensagens e encaminha para o nó raiz a mensagem com o mapa de *bits* "00000011".

3 Trabalhos relacionados

Os protocolos geográficos utilizam informações de posicionamento dos nós para realizar o encaminhamento dos dados. Como mencionado anteriormente, essas informações de posicionamento podem ser obtidas através da utilização do *GPS*. Por se tratar de protocolos que não precisam manter grandes quantidades de dados sobre a topologia de rede, apenas um salto de distância, são protocolos eficientes em relação à economia de energia pelo fato de trocar poucas mensagens para se manter em funcionamento. A seguir serão apresentados alguns dos protocolos geográficos encontrados durante o levantamento bibliográfico. Depois será discutido com mais detalhes um protocolo híbrido e um protocolo que possui maior proximidade com o estudo que foi realizado, e que foi utilizado como base de comparação.

LOCALized Multiobjectives Routing (LOCALMOR) é um protocolo com foco em *QoS* proposto para *RSSF* que tem diversidade de tráfego. Com base na diferenciação dos tipos de tráfegos são aplicadas as políticas de *QoS* utilizando três tipos de filas para gerenciar o tráfego. Fila crítica é a mais sensível, não tolera perdas e nem atrasos. Fila sensível ao atraso não tolera entregas com atrasos, mas permite algum tipo de perda. E a fila sensível confiabilidade, não tolera perda mas permite atraso. Essa proposta utiliza o encaminhamento guloso, não trata local máximo na rede (DJENOURI; BALASINGHAM, 2011). Devido a característica de não tratar o local máximo, essa proposta não é recomendada para para aplicações críticas de sensoriamento ambiental. É comum em *RSA* os nós serem lançados aleatoriamente no local de sensoriamento, o que em muitos casos a distribuição dos nós na área não é regular e não favorece o encaminhamento guloso, além dos nós morrerem durante a atividade da rede.

Geographic Adaptive Fidelity (GAF) tem como foco principal reduzir o consumo de energia identificando nós que são equivalentes de uma perspectiva de roteamento e, em seguida, desativando nós desnecessários, sem afetar a entrega. Os nós que serão desativados são identificados através de uma grade virtual. Cada nó utiliza a sua posição geográfica para se associar com um ponto da grade virtual. Os nós associados com o mesmo ponto são considerados equivalentes, deixando-se apenas um nó ativo por ponto. O tempo de vida da rede com o protocolo *GAF* é proporcional à densidade de nós. De um modo mais geral, o *GAF* é um protocolo proposto para estender o tempo de vida da rede, explorando a redundância para conservar energia enquanto mantém a fidelidade da aplicação (XU; HEIDEMANN; ESTRIN, 2001). Esse protocolo funcionará bem quando houver nós sobrepostos, no caso em que uma rede não seja densa o suficiente para que haja mais de um nó em um ponto da grade virtual, não haverá economia de energia, não existindo nós redundantes para realizar o desligamento sem afetar a comunicação.

O protocolo *GeoTORA* derivado do algoritmo *TORA* (*Temporally Ordered Routing Algorithm*) combina a comunicação *unicast* com *geocast*. Com intenção de enviar um pacote para uma região, o nó de origem determina uma rota para ser utilizada no envio do pacote em *unicast* até um nó da região, quando o nó desta região recebe o pacote é inundado na região *geocast* (KO; VAIDYA, 2000). O *GeoTORA* tem características semelhantes ao protocolo *GEAR* (ver seção 3.2), porém o *GEAR* tem como objetivo minimizar o consumo de energia enquanto o *GeoTora* não segue essa linha.

A seguir serão apresentados dois protocolos geográficos para *RSSFs* com mais detalhes. A primeira alternando entre os modos guloso e face, visando exibir com mais detalhes um protocolo com o modo de operação híbrido. A segunda abordagem tem como característica a consciência de energia, tende balancear o consumo energético entre os nós sensores. Essa abordagem será comparada com o protocolo proposto nesse trabalho por ser a uma das mais tradicionais da área.

3.1 Greedy Perimeter Stateless Routing

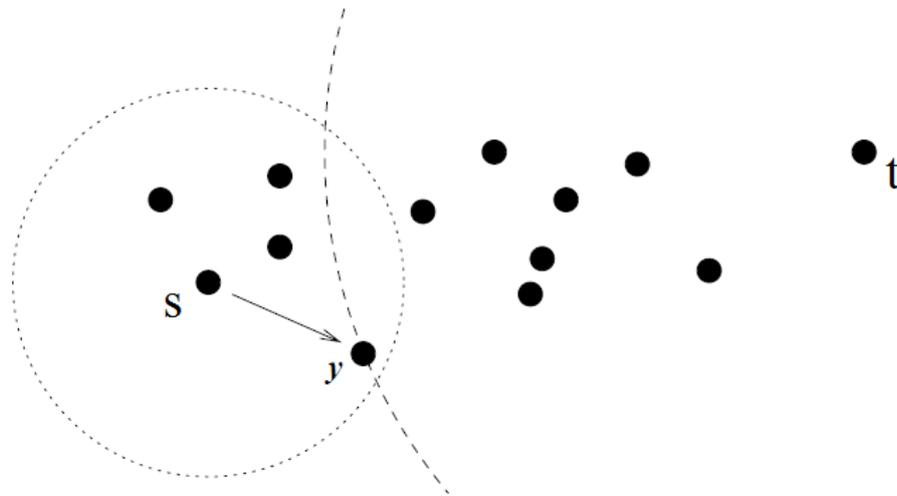
O protocolo *Greedy Perimeter Stateless Routing* (*GPSR*) é um protocolo híbrido que utiliza roteamento guloso, e quando não consegue encontrar nós mais próximo do destino que si mesmo é alterado para o modo de operação encaminhamento de face (KARP; KUNG, 2000).

Para realizar o encaminhamento os nós precisam ter consciência de sua localização e de seus vizinhos a um salto de distância. Os nós podem obter a localização através da utilização do *GPS* ou utilizar outra estratégia.

As posições dos vizinhos são obtidas através de mensagens de sonda que são enviadas em *broadcast* periodicamente. Uma sonda contém informações de quem enviou e a localização geográfica do mesmo. Quando um nó recebe uma sonda, então é armazenada a posição do vizinho que enviou, caso o nó não receba outra sonda deste vizinho em um período específico o roteador *GPSR* assume que o vizinho falhou e o remove da tabela de nós vizinhos.

O pacote é encaminhado utilizando as informações de localização geográfica que foram recebidas e armazenadas na tabela de nós vizinhos, sempre optando pelo caminho mais próximo do destino. A figura 7 demonstra como funciona o encaminhamento guloso. O nó s tem um pacote com destino ao nó t , então é verificado em sua tabela de nós vizinhos o vizinho mais próximo do nó t , no caso será endereçado o pacote para o nó y . Esse encaminhamento guloso continua até o pacote chegar ao destino ou encontrar um local máximo. O local máximo foi descrito na seção 2.4, e ocorre quando não existe nós mais próximos ao destino do que o próprio nó que recebeu o pacote.

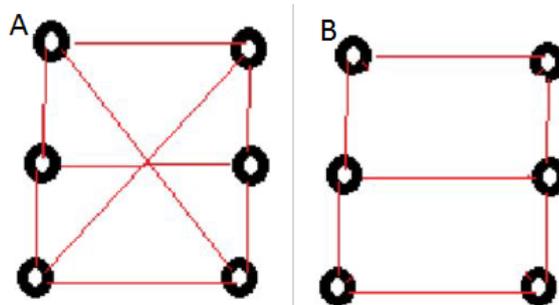
Figura 7 – Encaminhamento Guloso.



Adaptado de: (KARP; KUNG, 2000)

No momento em que o pacote chega em um nó onde existe o local máximo o modo de operação é alterado para modo encaminhamento de face. No entanto para operar no modo encaminhamento de face é necessário transformar o grafo em grafo planar, ou seja, um grafo onde as arestas não se cruzam. A figura 8 demonstra um grafo (A) não planar onde as arestas se cruzam, e um grafo planar (B) não contendo arestas que cruzam a outra. Para transformar em um grafo planar podem ser utilizados os algoritmos: *Relative Neighborhood Graph (RNG)* e o *Gabriel Graph (GG)*, que devem ser executados de forma distribuída. O funcionamento dos algoritmos pode ser visto com mais detalhes em (KARP; KUNG, 2000).

Figura 8 – A) Grafo não planar - B) Grafo planar.



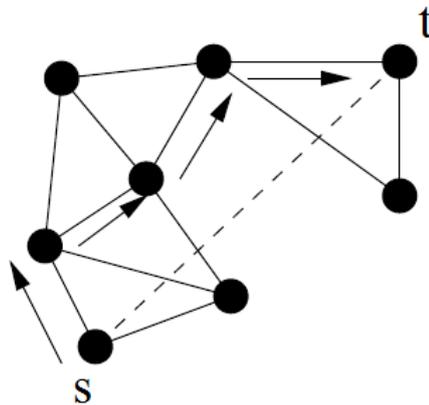
Adaptado de: (CADGER et al., 2013)

No algoritmo de encaminhamento de face, a regra da mão direita é aplicada ao

grafo planar. Utilizamos o exemplo da figura 9 para explicar a regra da mão direita: traça-se uma reta r (tracejada) a partir do nó onde falhou o encaminhamento guloso até o nó de destino. Essa reta serve para orientar o encaminhamento. Após traçada a reta o encaminhamento deve ser feito no sentido anti-horário, caso a aresta intercepte a reta r deve ser encaminhado novamente o pacote no sentido anti-horário assim sucessivamente até atingir o destino.

Quando o *GPSR* entra no modo encaminhamento de face é guardado em um campo no pacote a localização do nó atual. Essa informação de localização é utilizada por saltos subsequentes, comparando com a posição do nó atual. Se próximo no próximo salto o nó for mais próximo do destino do que a posição armazenada no pacote, o encaminhamento volta para o modo guloso. Caso contrário, o encaminhamento continua no modo encaminhamento de face.

Figura 9 – GEAR modo encaminhamento de face.



Adaptado de: (KARP; KUNG, 2000)

3.2 Geographical and Energy Aware Routing

Uma das grandes limitações das redes *Ad Hoc*, em especial as *RSSF*, é a sua fonte de alimentação. Os nós sensores que operam nessas redes normalmente são alimentados por baterias, para as quais, na maior parte dos casos, não são possíveis efetuar o carregamento. O protocolo *Geographical and Energy Aware Routing (GEAR)* tem como proposta o roteamento geográfico visando minimizar o consumo de energia durante seu funcionamento (YU; GOVINDAN; ESTRIN, 2001).

Um dos objetivos do *GEAR* é realizar o encaminhamento de pacotes para todos os nós que estão localizados dentro de uma região alvo. O roteamento do protocolo *GEAR* consiste em duas fases. A primeira fase encaminha os pacotes para a região alvo levando

em consideração a localização geográfica e o nível de energia residual dos nós vizinhos. A segunda fase é a disseminação do pacote dentro da região alvo.

Assim como o *GPSR* o protocolo *GEAR* necessita que os nós tenham ciência de sua própria localização geográfica que pode ser obtida através do *GPS* ou por outro método, e também precisa conhecer seus vizinhos a um salto de distância. Como o *GEAR* é um protocolo consciente de energia é necessário também ter conhecimento do seu próprio nível de energia e de seus vizinhos.

A localização geográfica e o nível de energia residual dos vizinhos são obtidos através de trocas de mensagens de sonda que são enviadas em *broadcast* periodicamente. Após receber a mensagem de sonda o nó adiciona a mensagem a sua tabela de nós vizinhos. Caso passado um período determinado, e o nó não tenha recebido outras ofertas de sonda do mesmo vizinho, então assume que este vizinho esteja inacessível e remove-o da tabela de nós vizinhos. Essa troca de mensagem é semelhante a mensagem utilizada no *GPSR*.

O *GEAR* também assume que cada pacote de consulta tem uma região alvo que é definida por algum critério. No estudo onde o protocolo é apresentado o autor assumiu que a região alvo tem forma retangular.

O comportamento de um nó (designado por N) no encaminhamento de pacotes é descrito a seguir. Um nó N encaminha um pacote P , com destino a região R . O centroide da região é o ponto D , e o nó N conhece as coordenadas de D . Para minimizar o consumo de energia, o nó N minimiza o valor de custo aprendido a partir de seus vizinhos. Seja N_i um vizinho de N , o custo aprendido é dado por $h(N_i, R)$. Caso o nó N não tenha o custo aprendido para o vizinho N_i ele utiliza o custo estimado $c(N_i, R)$ como um valor padrão de $h(N_i, R)$. O custo estimado é definido da seguinte forma:

$$c(N_i, R) = \alpha d(N_i, R) + (1 - \alpha)e(N_i)$$

Onde α é um valor ajustável entre 0 e 1, $d(N_i, R)$ é a distância euclidiana de N_i até o centroide D , e $e(N_i)$ é a energia consumida pelo nó N_i .

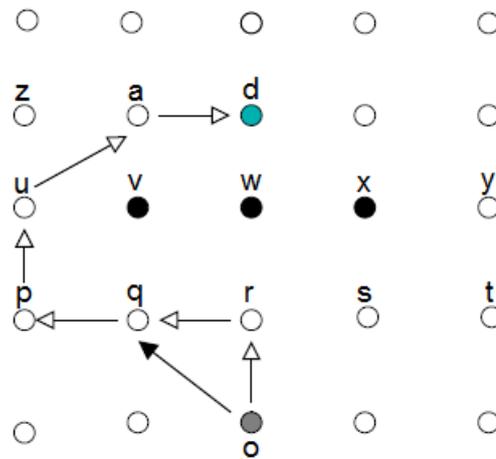
Na primeira fase do *GEAR* existem dois casos para serem considerados:

- Existência de um vizinho de N mais próximo ao centroide D . Essa situação ocorre quando não existem buracos na rede. Então é realizado o encaminhamento guloso optando pela melhor escolha local utilizando o custo aprendido.

- Todos os vizinhos de N estão mais longe do centroide D . Nesse caso N chegou no local máximo. O custo aprendido de um nó e sua regra de atualização são combinados para contornar o local máximo.

A figura 10 exemplifica como são aprendidas as rotas para contornar o buraco, onde é suposta distância entre os nós igual a 1, e cada nó tem o alcance de 1 salto. O

Figura 10 – Aprendendo rotas em volta do buraco.



Fonte: (YU; GOVINDAN; ESTRIN, 2001)

nó o deseja enviar uma informação para a região R cujo o centroide é o ponto d . Os nós que estão preenchidos na cor preta v , w e x são nós que estão desconectados da rede por algum motivo e não podem atender a solicitações de seus vizinhos, ou seja, fazem parte do buraco.

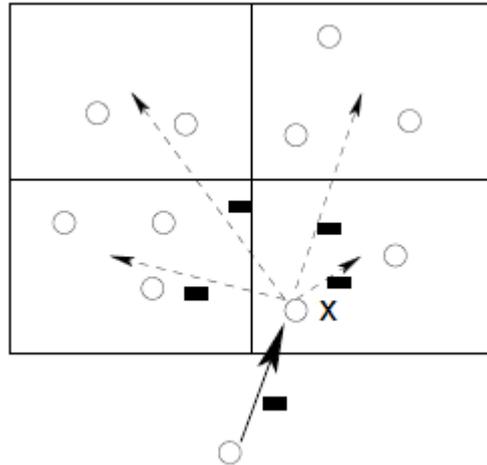
Os nós q , r e s estão mais próximos do d do que o nó o . Assumindo $\alpha = 1$, os valores dos custo aprendido são: $h(q, d) = c(q, d) = \sqrt{5}$, $h(r, d) = c(r, d) = 2$, $h(s, d) = c(s, d) = \sqrt{5}$. Para enviar um pacote destinado para d , o o encaminhará para o nó r pois tem menor custo $h(r, d) = 2$. Ao receber o pacote, o nó r identifica que é o nó mais próximo do destino, então o nó r procura em seus vizinhos qual tem o menor custo aprendido, no caso de empate, o desempate pode ser realizado utilizando o ID do nó. Nesse exemplo o nó r opta por encaminhar o pacote através do nó q (por desempate). Então o r atualiza seu custo aprendido para $h(r, d) = h(q, d) + c(r, q)$, onde $h(q, d) = \sqrt{5}$, e $c(r, q) = 1$. Cada vez que um pacote for entregue, o valor do custo aprendido correto será enviado um salto para trás. No exemplo, o custo aprendido é propagado de r para o nó o .

Quando um pacote atinge a região de destino, os pacotes são disseminados através de uma inundação controlada. Os nós que recebem o pacote que estão dentro da região alvo, retransmitem o pacote uma única vez para todos os seus vizinhos. Porém o autor argumenta que essa decisão pode ser cara em termos de custo energético.

Outra abordagem que pode ser utilizada para disseminar pacotes dentro da região alvo é o encaminhamento geográfico recursivo. A figura 11 demonstra como funciona essa abordagem. A região definida pelo maior retângulo é a região de destino. O nó x , o primeiro nó a receber o pacote na região R , encaminha uma cópia para outros quatro

nós cada um em uma sub-região. Esse processo recursivo continua recursivamente até o momento em que o nó atual seja o único da desta sub-região.

Figura 11 – Encaminhamento Geográfico Recursivo.



Fonte: (YU; GOVINDAN; ESTRIN, 2001)

3.3 Conclusão

Neste capítulo apresentamos os trabalhos relacionados. Foram discutidos, de maneira mais simplificada, as propostas de protocolos geográficos com certa relação com essa dissertação, e de modo mais detalhado os protocolos *GPSR* e *GEAR*. A partir desse estudo bibliográfico, selecionamos o *GEAR* como protocolo a ser comparado com o protocolo proposto nessa dissertação. O motivo dessa escolha foi porque o *GEAR* possui a característica de resiliência, que é um dos princípios do protocolo proposto (descrito no capítulo 4). O *GEAR* tem a habilidade de contornar buracos, a resiliência é obtida com um algoritmo leve de aprendizagem que evita o problema clássico do encaminhamento guloso, o local máximo.

4 *Resilient Geographic Protocol Oriented to Path Quality*

Neste capítulo é apresentado o protocolo de roteamento geográfico denominado *Resilient Geographic Protocol Oriented to Path Quality (RGPOP)*. Este capítulo organizado da seguinte forma: conceito, arquitetura e a especificação do protocolo. Este capítulo organizado em duas seções, na primeira são definidos os requisitos, os conceitos envolvidos, e é detalhada a arquitetura, enquanto que a segunda contém a especificação do protocolo.

4.1 Conceito e arquitetura

O projeto do protocolo proposto foi orientado por três princípios fundamentais: (i) não usa identificadores ou endereço dos sensores para rotear mensagens de solicitação de informação, mas sim as coordenadas geográficas da região a partir da qual a informação é procurada. (ii) Inundações controladas, através do número de réplicas da Mensagem de Interesse. (iii) Procura o caminho de retorno com a melhor qualidade do *link*, de acordo com a métrica *ETX*. O protocolo também deve apresentar as seguintes propriedades: resiliência, simplicidade e escalabilidade. O primeiro é conseguido fornecendo vários caminhos entre os sensores e o nó solicitante, garantindo a comunicação entre eles, mesmo com a ocorrência de perda de mensagem, degradação de *link* ou falha de nó. A simplicidade é assegurada porque o protocolo usa um pequeno conjunto de mensagens, e cada nó executa um algoritmo simples, que não precisa que os nós armazenem a topologia da rede inteira. A escalabilidade é uma consequência da resiliência e simplicidade.

Para implementar o roteamento geográfico, cada nó deve conhecer suas coordenadas e as coordenadas de seus vizinhos. Além disso, cada nó deve conhecer a qualidade dos *links* de comunicação com seus vizinhos, calculados pela métrica *ETX*. Para que cada nó seja identificado de forma exclusiva, é necessário um identificador e para isso o endereço *MAC* pode ser utilizado. Cada nó armazena as informações de seus vizinhos e o *ETX* dos *links* correspondentes em uma estrutura de dados mostrada na tabela 1. Os nós vizinhos são descobertos enviando mensagens de sondagem, que também são utilizadas para calcular o *ETX*. Essas mensagens de sonda são enviadas periodicamente a intervalos definidos por um parâmetro de configuração.

Como o propósito do protocolo é apoiar as aplicações de sensoriamento ambiental, este deve suportar consultas sobre informações ambientais, direcionadas aos sensores localizados em determinada região geográfica. Além disso, uma aplicação de sensoriamento pode precisar receber as informações em intervalos de tempo pré-definidos, com taxas de

Tabela 1 – Estrutura de dados para armazenar informações sobre os vizinhos de um nó

ID	Coordenadas	ETX
1	{50,23}	1.33
7	{45,27}	1.00

Tabela 2 – Parâmetros de Mensagem de Interesse

Parâmetro	Descrição
Tipo	Tipo da mensagem (interesse).
Origem	<i>ID</i> do nó que originou o interesse.
Região	Coordenadas da região geográfica em que o interesse será encaminhado.
Réplicas	Número de mensagens que podem ser enviadas por um nó que recebeu uma Mensagem de Interesse (controle de inundação).
Custo	Valor de <i>ETX</i> acumulado até o nó que recebeu a mensagem de interesse.
Validade	Duração do interesse em uma aplicação de sensoriamento de informação.
Taxa	Taxa de resposta.
Info	Informação requerida.

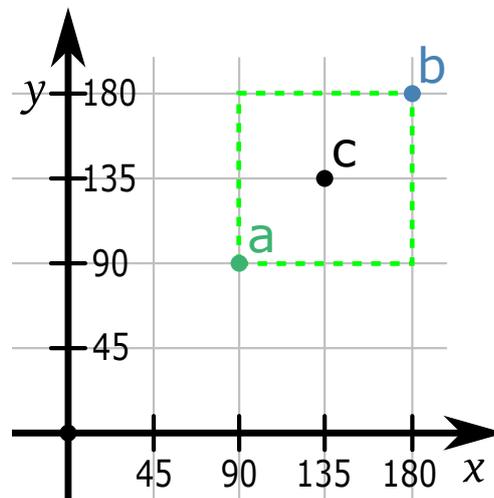
entrega determinadas pela aplicação. Para isso, o *RGPOP* define duas mensagens, uma para a aplicação solicitar o interesse em uma lista de informações ambientais e outra para que os sensores enviem os dados solicitados. A mensagem usada pela aplicação ambiental é chamada de Mensagem de Interesse, que inclui os parâmetros definidos na tabela 2.

Tipo identifica se é uma Mensagem de Interesse ou Resposta, enquanto **Origem** contém a *ID* do nó que recebeu a solicitação da aplicação e iniciou o cálculo de rota. **Região** define o destino, ou seja, a região geográfica para a qual uma Mensagem de Interesse deve ser encaminhada. Contém as coordenadas geográficas que definem a área onde estão localizados os sensores que devem responder à Mensagem de Interesse. A região inclui as coordenadas geográficas de dois pontos (*a* e *b*) que definem os pontos finais da diagonal de um retângulo. O retângulo definido por esta diagonal é a região de interesse. Para qualquer sensor *c*, com coordenadas (*x_c*, *y_c*) para pertencer à região definida pelos pontos *a* e *b*, é necessário que a seguinte condição seja satisfeita: ($x_a < x_c < x_b$) e ($y_a < y_c < y_b$).

Figura 12 mostra um exemplo de uma região definida por pontos *a* e *b*, com coordenadas (90, 90) e (180, 180), e um sensor *c* com coordenadas (135, 135) pertencentes a região. Quando uma Mensagem de Interesse é encaminhada, é entregue a um dos sensores

pertencentes à região, o primeiro alcançado pelo procedimento de roteamento. Assim que este sensor for atingido, ele inicia um procedimento de difusão dentro da região para que a mensagem seja entregue a todos os sensores incluídos nela. O procedimento de difusão de mensagens de interesse dentro de uma região está fora do escopo desse trabalho. Em (YU; GOVINDAN; ESTRIN, 2001) dois métodos são propostos para esta finalidade, um recursivo e um baseado em inundações. O primeiro cria subdivisões (recursivamente) dentro da região, encaminhando a Mensagem de Interesse para o próximo nó dentro da sub-região, repetindo este procedimento até que todos os nós da região sejam atingidos. O segundo executa uma inundação de modo a alcançar todos os nós da região.

Figura 12 – Parâmetro da região



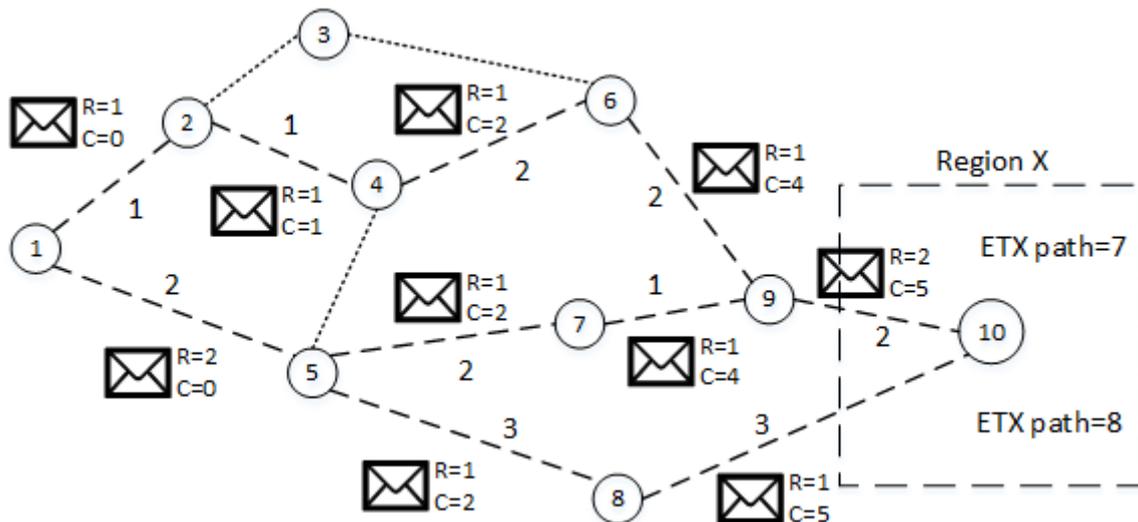
Fonte: Autoria Própria

Um conceito importante usado no *RGPOP* é a inundação controlada, que limita a quantidade de réplicas de uma Mensagem de Interesse que pode ser enviada por um nó para seus vizinhos, durante o cálculo do caminho. O parâmetro **Réplicas** define o número de réplicas. As réplicas da Mensagem de Interesse são encaminhadas para os nós vizinhos. Para isso, a lista de vizinhos é ordenada por ordem crescente de acordo com sua distância (Euclidiana) ao destino. A distribuição é feita através de um procedimento *round-robin*, começando com o vizinho mais próximo do destino. Se houver mais réplicas do que o número de vizinhos, a distribuição recomeça no início da lista e continua até que não haja mais réplicas para serem distribuídas. Após a conclusão da distribuição, a Mensagem de Interesse é enviada aos vizinhos, com o parâmetro **Réplicas** atualizado.

Figura 13 mostra, a título de exemplo, a operação do controle de inundação. O nó 1 recebeu da aplicação (não mostrada na figura) um pedido de interesse para a Região X, com **Réplicas** = 3. Os vizinhos do nó 1 são os nós 2 e 5, formando a lista (5, 2) em ordem crescente das distâncias respectivas para a região de destino. Aplicando o procedimento de

distribuição, uma mensagem com **Réplicas** = 2 é enviada para o nó 5 e uma mensagem com **Réplicas** = 1 é enviada para o nó 2, representado por $R = 2$ e $R = 1$ na Figura 13. Os caminhos cobertos pelas mensagens são marcados por linhas tracejadas. Pode ser observado que quando a mensagem com **Réplicas** = 2 chegando ao nó 5, ela separada em duas mensagens, uma para cada vizinho (7 e 8) em direção ao destino. Quando um nó recebe a mesma Mensagem de Interesse proveniente de um antecessor diferente, deve encaminhar a Mensagem de Interesse com o parâmetro Réplica atualizado, de modo que os nós descendentes no caminho possam dividir a mensagem novamente em dois caminhos. Esse comportamento pode ser observado no nó 9, que recebe uma mensagem do nó 6 com **Réplicas** = 1 e outra do nó 7 também com **Réplicas** = 1 e, em seguida, envia uma mensagem ao nó 10 com **Réplicas** = 2.

Figura 13 – Controle de réplicas e cálculo do custo dos caminhos.



Fonte: Autoria Própria

Outra característica importante do *RGPOP* é o controle de qualidade dos caminhos de comunicação. Usamos a métrica *ETX* para avaliar a qualidade do *link*, que é uma métrica acumulativa. Isto significa que a qualidade de um caminho (medido em *ETX*) é calculada pela soma do *ETX* dos *links* que compõem o caminho. Nós nomeamos o *ETX* de um caminho como *ETX-Path*. Durante o cálculo do caminho, o valor *ETX* é acumulado e atualizado para cada nó, sendo armazenado no parâmetro **Custo** da Mensagem de Interesse.

A figura 13 também ilustra o cálculo dos parâmetros **Custo** e *ETX-Path*. Pode-se observar que as duas mensagens enviadas pelo nó 1 indicam que o custo para a origem é igual a zero ($C = 0$). À medida que as mensagens são encaminhadas ao longo do caminho, o parâmetro **Custo** acumula o *ETX-Path*. Por exemplo, a mensagem encaminhada pelo

Tabela 3 – Exemplo de Mensagem de Interesse

Tipo	Origem	Região	Réplicas	Custo	Validade	Taxa	Info
Interesse	1	{ { 90,90 }, { 180,180 } }	2	0	10000	10	{ umidade, temperatura }

Tabela 4 – Exemplo de Mensagem de Resposta

Tipo	Origem	Região	Info
Resposta	1	{{90,90},{180,180}}	{umidade = 39, temperatura= 23}

nó 8 tem **Custo** = 5 ($C = 5$), correspondente à soma do *ETX* dos *links* (1, 5) e (5, 8). O nó no destino calcula o *ETX-Path*. No exemplo, duas mensagens com **Custo** = 5 chegam ao nó 10, que calcula o *ETX-Path* para cada opção. Um dos caminhos de resposta (10, 9, 7, 5, 1) tem *ETX-Path* = 7, enquanto o outro (10, 8, 5, 1) possui *ETX-Path* = 8.

Validade é o parâmetro que define a duração de uma solicitação (em milissegundos), ou seja, o intervalo de tempo durante o qual um sensor que recebe uma Mensagem de Interesse deve enviar as informações solicitadas. Esse parâmetro também determina o tempo de vida dos caminhos definidos por uma Mensagem de Interesse. Quando a vida útil expira, os nós que possuem informações de roteamento para a mensagem expirada em suas tabelas removem essas informações. O parâmetro **Taxa** controla a taxa de envio das Mensagens de Resposta (em mensagens por segundo). Finalmente, o parâmetro **Info** define o conteúdo da informação de sensoriamento solicitada. Ele corresponde a uma lista com os nomes das informações solicitadas. Está fora do escopo deste trabalho para discutir a semântica das informações em aplicações ambientais, mas um exemplo típico seria a umidade e temperatura. Tabela 3 mostra um exemplo de Mensagem de Interesse.

A Mensagem de Resposta carrega a informação de sensoriamento solicitada. É uma mensagem com menos parâmetros que a Mensagem de Interesse, uma vez que os caminhos já foram calculados e cada nó no caminho já armazenou as informações necessárias para reencontrar a Mensagem de Resposta em tabelas de roteamento. Entre os parâmetros da Mensagem de Resposta, o único que muda em relação à Mensagem de Interesse é **Info**. Em Mensagens de Resposta, ele contém uma lista de nomes-valores, correspondentes à lista de nomes enviados na Mensagem de Interesse associada. Tabela 4 mostra um exemplo de Mensagem de Resposta.

Para enviar as Mensagens de Resposta, cada nó ao longo do caminho armazena, para cada interesse, os nós antecessores e seus custos. Por exemplo, na Figura 13, para o nó 10, seriam armazenados como predecessores o nó 9 com *ETX-Path* = 7 e nó 8 com *ETX-Path* = 8. Também na Figura 13, para o nó 9, seriam armazenados como

Tabela 5 – Entrada da tabela de interesse

Campo	Descrição
Chave	Identificador único.
Validade	Duração do interesse em uma aplicação de sensoriamento de informação.
Encaminhamento	Lista de nós de encaminhamento.
Antecessor	Lista de nós antecessor.

predecessores, o nó 6 com $ETX-Path = 6$ e nó 7 com $ETX-Path = 5$. Os outros nós no exemplo possuem apenas um antecessor, que também é armazenado da mesma maneira. Assim, se as condições da rede não forem alteradas, as Mensagens de Resposta serão enviadas através do caminho (10, 9, 7, 5, 1).

O *RGPOP* foi projetado para se adaptar às mudanças de qualidade nos *links* de comunicação. Por esse motivo, o *ETX* é continuamente reavaliado em cada *link*, permitindo que o protocolo altere o caminho da resposta se as condições mudarem. Por exemplo, na Figura 13, se o *ETX* do *link* (9, 7) mudar de 1 para 4, o nó 9 perceberia essa alteração e recalcularia o *ETX-Path* do caminho de retorno através do nó 7, mudando seu valor para 8. Supondo que não houve variação no *ETX* do *link* (9, 6), o nó 9 encaminharia Mensagens de Resposta através do nó 6.

Para que um nó *RGPOP* possa encaminhar Mensagens de Interesse e Mensagens de Resposta, ele deve armazenar informações de roteamento na tabela de interesse. O *RGPOP* é um protocolo de *soft-state* no sentido que as entradas da tabela de interesses são descartadas quando o **Validade** de um interesse expira. As entradas na tabela de interesse são apresentadas na tabela 5.

O campo **Chave** identifica um único interesse e é formado pelo identificador do nó **Origem**, pelas coordenadas do nó **Origem** e pelas coordenadas da **Região** de destino. O campo **Validade** é obtido da Mensagem de Interesse e é usado para remover a entrada da tabela quando a Mensagem de Interesse expira. O campo **Encaminhamento** contém a lista de nós de encaminhamento e inclui para cada vizinho elegível (uma mensagem não pode ser enviada para o nó a partir do qual foi recebida) e o valor do parâmetro **Réplicas**, que é usado no procedimento de inundação controlada descrito anteriormente. O campo **Antecessor** contém a lista de nós anteriores, ou seja, vizinhos de onde as mensagens de interesse com a mesma **Chave** chegaram. A lista de antecessores também armazena, para cada antecessor, o *ETX-Path* da fonte para ele. A soma deste valor com o *ETX* do *link* entre o nó e o antecessor forma o *ETX-Path* do caminho da fonte até o nó que chega por esse antecessor.

4.2 Especificação do protocolo

Quando uma aplicação de monitoramento ambiental precisa obter informações de sensores em uma região, ele envia uma Mensagem de Interesse para o nó ao qual está conectado (nó de origem). *RGPOP* usa a heurística gulosa com inundação controlada para propagar a Mensagem de Interesse.

Quando um nó recebe uma Mensagem de Interesse, ele executa o procedimento *Receber_Interesse*, apresentado no Algoritmo 1. Depois de receber a mensagem, o nó insere uma entrada (linha 4) na tabela de Interesse (definida na tabela 5). Se já existe uma entrada com a mesma **Chave**, os campos na entrada são atualizados. Então, o nó agenda um evento para remover a entrada da tabela quando o interesse expira, com base no parâmetro **Validade**. É adicionado uma salvaguarda para evitar que uma mensagem que esteja trafegando pelo caminho seja perdida. A salvaguarda é equivalente o valor da **Taxa**, são removidas as entradas que satisfaçam a seguinte condição: **Validade**+Salvaguarda > tempo atual. Se o nó que recebeu a Mensagem de Interesse pertencer a **Região** alvo, ele entrega a mensagem para a camada de aplicação (linha 11). Se o nó não pertence ao **Região** alvo, o algoritmo de distribuição **Réplicas** descrito no capítulo 4 é executado (linha 13).

Algoritmo 1: Receber Interesse

```

1 Receber_Interesse (mensagem);
2 begin
3   if (Interesse novo) then
4     Criar nova entrada na Tabela de Interesse;
5   else
6     Atualizar entrada na Tabela de Interesse;
7   end
8 end
9 Agendar (Remover_Entrada, Chave, Validade + salvaguarda);
10 if (Região == minha_região) then
11   Entregar mensagem para camada de aplicação;
12 else
13   Atualizar parâmetro Réplicas;
14   Enviar Mensagem de Interesse para nós de encaminhamento;
15 end
16 end
17 end

```

Quando o evento de expiração de uma entrada na tabela de interesse (agendada na linha 9 do Algoritmo 1) é acionada, uma consulta é feita para a tabela de interesse para verificar se a entrada expirou. Essa consulta ocorre porque um interesse pode ser renovado atualizando o campo **Validade**. Se expirou, a entrada correspondente é removida da tabela.

Quando o nível de aplicação do nó de destino recebe uma Mensagem de Interesse, ele registra os parâmetros **Chave**, **Validade**, **Taxa** e **Info**. A informação de sensoriamento é obtida do sensor e completada no campo **Info** das Mensagens de Resposta, que são enviadas na **Taxa** solicitada durante o período de tempo definido em **Validade**. Uma vez

montado no nível da aplicação, a Mensagem de Resposta é enviada ao respectivo nó e encaminhada pelo caminho de menor custo, conforme descrito na seção 4.1.

Quando uma Mensagem de Resposta chega a um nó *RGPOP*, a função *Responder_Interesse* apresentada no Algoritmo 2 é executada. Se o campo **Origem** for igual à *ID* do nó, a mensagem chegou ao nó de origem e deve ser entregue à camada da aplicação. Caso contrário, a lista de antecessor é procurada para encontrar o antecessor com o menor *ETX-Path*, para quem a Mensagem de Resposta seja encaminhada (linhas 24 e 25).

Algoritmo 2: Responder Interesse

```
18 Responder_Interesse(mensagem);
19 begin
20   if (Origem == meu_ID) then
21     Entregar mensagem para a camada de aplicação;
22   else
23     Recuperar Antecessor da Tabela_Interesse;
24     próximo_salto ← antecessor com menor ETX – Path;
25     Enviar(mensagem, próximo_salto);
26   end
27 end
28 end
```

5 Método

Este capítulo descreve como foram organizados os experimentos, começando pela subseção 5.1 que descreve como são geradas as topologias e os parâmetros aplicados. Na subseção 5.2 é descrito como foi planejada a geração de tráfego durante a execução das simulações. A subseção 5.3 detalha as métricas que foram elaboradas para avaliar o desempenho dos protocolos contrapostos. E a subseção 5.4 detalha como foi planejada a escolha da quantidade de réplicas a serem utilizadas no protocolo *RGPOP* para contrapor ao protocolo *GEAR*.

5.1 Cenários

Em situações reais de posicionamento dos nós sensores em uma determinada área, geralmente os nós são ligados por aeronaves, para criar um ambiente mais próximo ao real os nós foram sorteados com distribuição uniforme em um disco de raio 180m. Os nós sensores utilizam o padrão IEEE 802.15.4. As condições do canal sem fio foram modeladas usando a distribuição Nakagami- m e o modelo de perda de caminho log-distance. Os rádios operam na faixa de 914 MHz, o expoente de perda de caminho foi ajustado para 2,5 e a gravidade de desvanecimento de Nakagami foi ajustada para $m = 2$. Com a intenção de criar topologias com densidade diversificada, o número de nós varia de 20 a 120 com intervalos de 20 nós, em uma área fixa de aproximadamente 101787 m². O tamanho da área é fixo, diante disso, o número de nós influencia o grau médio das topologias sorteadas, ou seja, quanto maior o número de nós, maior será o grau médio. A tabela 7 apresenta o grau médio de nó em cada cenário. Para cada número de nós no intervalo de avaliação, foram sorteadas aleatoriamente 10 topologias com o propósito de ter 10 amostras para cada ambiente avaliado. Os parâmetros de topologia foram setados de acordo com a tabela 6.

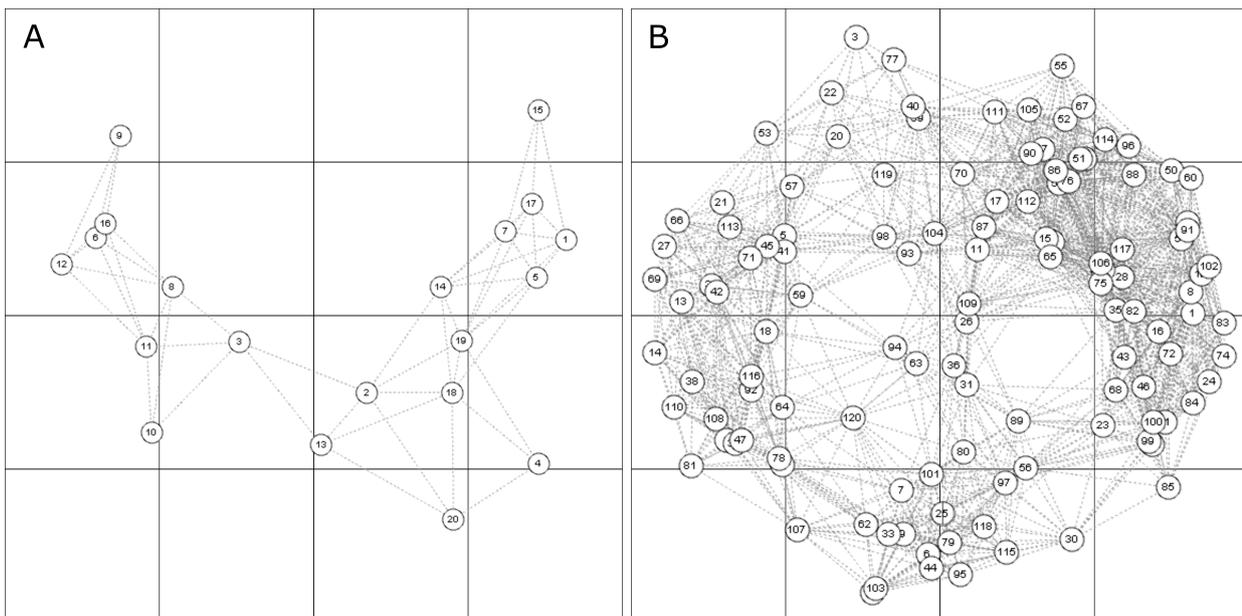
A figura 14 apresenta dois exemplos de topologias que foram sorteadas neste trabalho, com o propósito de demonstrar dois exemplos de configuração de topologias após o posicionamento dos nós sensores. A figura 14 **A** é uma topologia com 20 nós, propondo-se observar que os sensores sorteados não são suficientes para cobrir toda a área (101787 m²). A figura 14 **B** é uma topologia com 120 nós, sendo possível visualizar que mesmo existindo uma quantidade 6 vezes maior do que no exemplo apresentado na topologia **A** ainda existem buracos.

A área de cobertura da rede é subdividida em regiões de igual tamanho, conforme ilustrado na figura na 14. Os quadrados representam regiões para as quais são solicitados dados. A entrega de Mensagens de Interesse dentro de uma região não está sendo avaliada,

Tabela 6 – Características de topologia

Características	Parâmetros
Tempo de execução	12h
Quantidade de nós	20, 40, 60, 80, 100, 120
Sorteio da posição dos nós	Distribuição uniforme
Raio de distribuição	180m
Regiões	90 metros x 90 metros

portanto, o primeiro nó da região que recebe a Mensagem de Interesse envia a resposta. Ambos os protocolos enviam mensagens de sonda periodicamente para manutenção da tabela de nós vizinhos. O período de envio deve ser cuidadosamente selecionado para não sobrecarregar a rede, mas deve ser suficientemente curto para que a qualidade do *link* e as informações de energia sejam atualizadas na frequência apropriada para o bom funcionamento dos protocolos. Foram realizados experimentos com o intervalo entre duas sondas consecutivas com valores: 5, 30 e 120 segundos, observado que havia um número excessivo de sondas e afetava a comunicação dos nós, o intervalo entre duas mensagens de sonda consecutivas foi definido empiricamente em 200 segundos, o que apresentou um resultado que não congestionava a rede e atualizava as informações em um tempo adequado.

Figura 14 – **A**: Topologia com 20 nós. **B**: Topologia com 120 nós.

Fonte: Autoria Própria

Tabela 7 – Grau médio de nó

Nós	20	40	60	80	100	120
Grau médio de nó	4.16	8.05	12.25	16.16	20,49	25.20

Tabela 8 – Parâmetros de protocolo

Características	Parâmetros
Modelo de geração das Mensagens de Interesse	Processo de <i>Poisson</i> com média de 2h
Sorteio da região de destino	Distribuição uniforme
Quant. Réplicas (<i>RGPOP</i>)	3R
Validade do interesse	30min
Frequência do interesse	3min
Intervalo entre sonda	200seg

5.2 Modelo de tráfego

Em uma *RSA* estabelecida em um ambiente real, o tráfego acontece naturalmente, dependendo da necessidade dos dados. Porém em um ambiente simulado é necessário definir um modelo de tráfego para simular a carga na rede, tornando possível a observação do comportamento dos protocolos em variadas situações. Para esse fim, foi desenvolvido o modelo de tráfego. Os nós enviam solicitações de informações (Mensagens de Interesse) de acordo com um processo de *Poisson*, no qual o tempo médio entre duas solicitações consecutivas é de 2 horas. Um interesse é enviado para uma região selecionada aleatoriamente. Quando o resultado do sorteio seleciona a região à qual o nó de envio pertence, outro sorteio é realizado. Conforme explicado no capítulo 4, cada solicitação define as informações desejadas, além da taxa na qual as informações devem ser enviadas. A tabela 8 lista os parâmetros de protocolo que foram utilizados para execução dos experimentos.

As Mensagens de Interesse são agendadas aleatoriamente de acordo com um processo de *Poisson*, para cada uma das 60 topologias. Todas as topologias possuem uma agenda única, que corresponde a todas as Mensagens de Interesse que foram sorteadas para ela. Essa agenda foi criada para que os protocolos *RGPOP* e *GEAR* sejam avaliados sob as mesmas condições. O parâmetro **Validade** da Mensagem de Interesse é definido como 30 minutos e **Frequência** de resposta a cada 3 minutos. Cada simulação é executada ao longo de um período de 12 horas.

Para comparar os dois protocolos em uma configuração com *links* menos estáveis, inserimos distúrbios (nós interferentes) em determinadas posições da rede. Foram inseridos seis padrões de interferência, cada um com quatro nós interferentes, de modo que os nós

estavam localizados em diferentes regiões. A cada 2 horas a localização do padrão de interferência é sorteada aleatoriamente, e então os nós produzem distúrbios por 20 minutos. São geradas agendas de interferências para todas as topologias para que os distúrbios sejam os mesmos para os dois protocolos avaliados.

5.3 Métricas

Para avaliar o desempenho dos protocolos contrapostos neste trabalho, foi planejada a utilização quatro métricas, com o objetivo de analisar a *QoS* oferecida pelos protocolos. As métricas selecionadas são: proporção de Mensagens de Interesse recebidas com sucesso (*PMIRS*), proporção de Mensagens de Resposta recebidas com sucesso (*PMRRS*), média do *ETX-Path* e média da contagem de Saltos.

A Proporção de Mensagens de Interesse recebidas com sucesso é calculada dividindo a quantidade de Mensagens de Interesse recebidas (*MIR*) pelos nós de destino, pela quantidade de Mensagens de Interesse enviadas (*MIE*) pelos nós solicitantes (equação 5.1).

$$PMIRS = \sum_{i=1}^n \frac{MIR_i}{MIE_i} \quad (5.1)$$

A proporção de Mensagens de Resposta recebidas com sucesso é calculada dividindo o total de Mensagens de Resposta recebidas pelos nós solicitantes (*MRR*) pela quantidade esperada Mensagens de Resposta (*MRE*), ou seja, a quantidade de Mensagens de Resposta que deveriam ser recebidas se não ocorresse nenhum erro na rede (equação 5.2). Inclui todas as Mensagens de Resposta enviadas durante o período de validade dos interesses.

$$PMRRS = \sum_{i=1}^n \frac{MRR_i}{MRE_i} \quad (5.2)$$

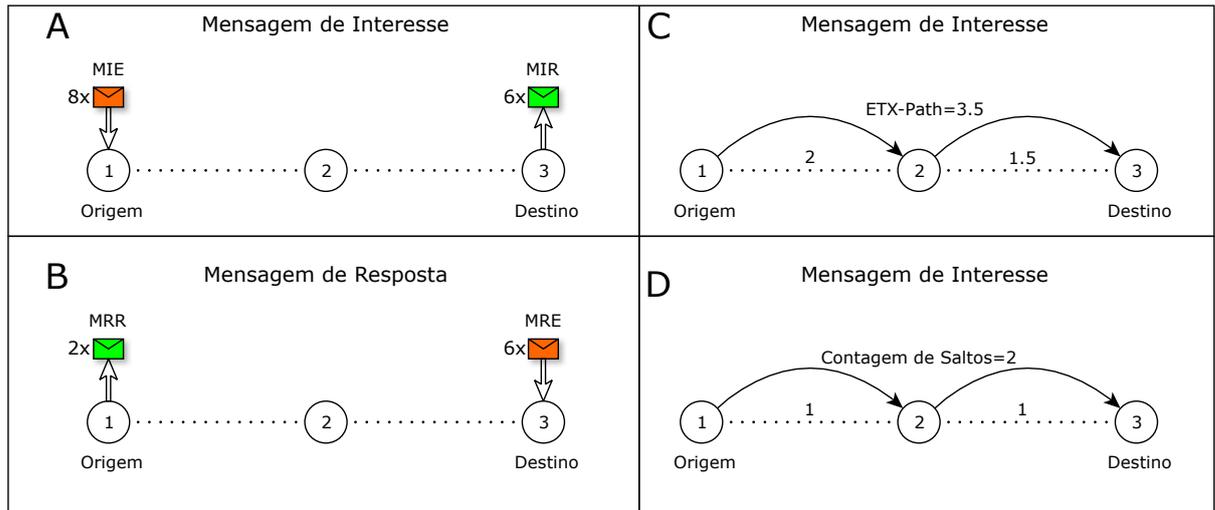
A qualidade da comunicação é avaliada através da média do *ETX-Path*, cujo cálculo já foi apresentado na seção 2.5. O cálculo da média dos *ETX-Path* em cada cenário de simulação é realizado da seguinte maneira. Para o protocolo *GEAR*, soma-se o *ETX-path* de cada caminho encontrado, dividindo-se pelo número total de caminhos. Como o protocolo *RGPOP* pode encontrar vários caminhos para uma única Mensagem de Interesse, a média dos *ETX-path* é calculada considerando-se o caminho com menor *ETX*.

A Contagem de Saltos é calculada de forma semelhante ao *ETX-Path*, a diferença é o custo de cada *link*, para a Contagem de Salto cada *link* sempre terá o custo de uma unidade. O cálculo da média também é realizado seguindo o mesmo princípio.

A Figura 15 exemplifica o cálculo das métricas. Na figura 15 **A** o nó de destino recebe 6 *MIR* de um total de 8 *MIE*, neste caso $PMIRS = \frac{6}{8}$. A figura 15 **B** o nó de origem recebe 2 *MRR*, porém era esperado receber 6 *MRE* do nó de destino. O cálculo da

métrica fica da seguinte maneira: $PMRRS = \frac{2}{6}$. Nas figuras 15 **C** e **D** respectivamente apresentam de onde são coletados os dados para os cálculos de Média *ETX-Path* e Média de Contagem de Saltos, os cálculos seguem o mesmo princípio: $ETX-Path = 2 + 1.5$ e $Contagem\ de\ Saltos = 1 + 1$.

Figura 15 – **A**: *PMIRS*. **B**: *PMRRS*. **C**: *ETX-Path*. **D**: Contagem de Saltos



Fonte: Autoria Própria

5.4 Experimentos

Para avaliar e validar o protocolo proposto foram planejados seis experimentos: o primeiro tem por objetivo avaliar o desempenho do *RGPOP* variando-se o parâmetro que controla a quantidade de réplicas. O protocolo *RGPOP* utiliza um mecanismo de difusão controlada, onde a difusão é contida pelo número de réplicas. Esse parâmetro define a quantidade Mensagens de Interesse que podem ser enviadas simultaneamente, as réplicas influenciam diretamente na quantidade de caminhos que podem ser criados durante o enviado da Mensagem de Interesse. Para entender como o número de réplicas afeta o desempenho do *RGPOP*, foi planejado um experimento para avaliar o seu efeito considerando três alternativas, 1, 3 e 5 réplicas. O objetivo é selecionar a quantidade de réplicas adequada para as características dos experimentos de comparação, que são então executados como a quantidade de réplicas indicada por esse primeiro experimento.

Os demais experimentos avaliam o desempenho de *RGPOP* em comparação ao *GEAR*, sendo utilizadas as métricas *PMIRS*, *PMRRS* e Média *ETH-Path*, por serem métricas que refletem diretamente o resultado dos caminhos formados do nó de origem até a região de destino. A métrica *PMIRS* demonstrará qual o protocolo consegue entregar

mais Mensagens de Interesse, esta mensagem que é responsável por formar o caminho entre a origem e o destino. A métrica *PMRRS* tem relação com a qualidade dos caminhos formados entre origem e destino. E a métrica Média *ETX-Path* irá demonstrar a qualidade dos caminhos encontrados. Outra métrica de qualidade que é amplamente difundida é a métrica de Contagem de Saltos, irá mostrar qual protocolo consegue encontrar caminhos com menor número de saltos.

6 Resultados

Neste capítulo é comparado o desempenho dos protocolos *RGPOP* e *GEAR* por simulação, utilizando o simulador *SensorSim* desenvolvido pelo grupo de pesquisa de redes e telecomunicações do *PPGIA*. O primeiro resultado busca definir a quantidade de réplicas que serão utilizadas no protocolo *RGPOP* para comparação com o *GEAR*. Após definir as réplicas, é comparada a capacidade de entrega de mensagens dos dois protocolos, observando a *PMIRS* e a *PMRRS*, e é comparada a qualidade dos caminhos formados pelos protocolos aplicando as métricas Média *ETX-Path* e Média de Contagem de Saltos. As comparações foram feitas nos cenários com e sem interferências. Para todas as métricas, os valores apresentados nos gráficos de avaliação correspondem ao valor médio obtido em todas as simulações. Os resultados são avaliados considerando um intervalo de confiança de 95%. Para evitar distorções no cálculo da média do *ETX-Path* e Contagem de Saltos, somente os caminhos que foram encontrados por ambos os protocolos foram considerados.

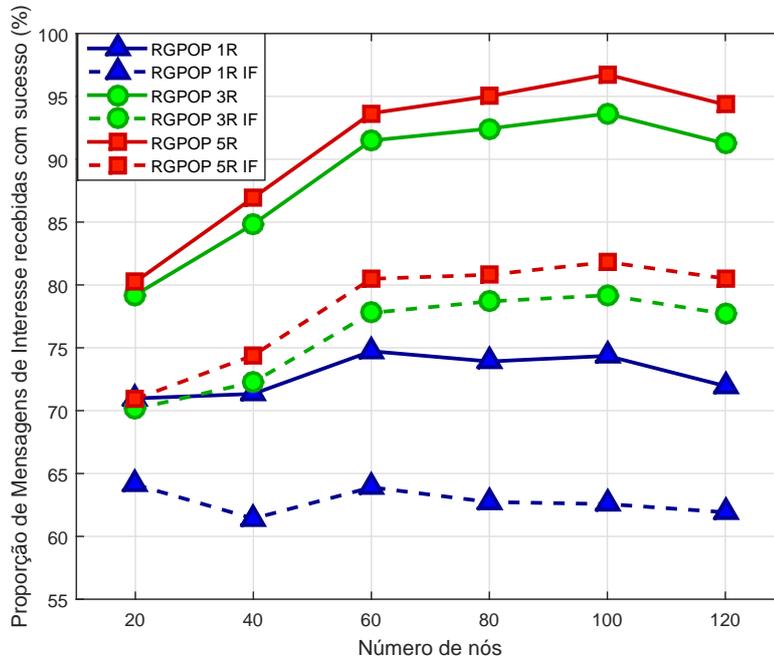
Para facilitar a visualização dos gráficos foram adotadas algumas legendas. Nos gráficos 16 e 17 o padrão para o *RGPOP* é o nome seguido pela quantidade de réplicas representada por um número e a letra **R** e caso tenha interferência é representado por **IF**. A legenda utilizada para o *GEAR* é o nome do protocolo e **IF** caso seja experimentos com interferência. Os gráficos 18, 19, 20 e 21 é alterado o padrão da lenda apenas para o protocolo *RGPOP*, ficando da seguinte maneira: nome e caso tenha interferência **IF**.

6.1 Quantidade de réplicas do *RGPOP*

A Figura 16 mostra o desempenho em relação à métrica *PMIRS*. De acordo com a figura, é possível observar que o desempenho do *RGPOP* com **Réplicas** = 3 e com **Réplicas** = 5 são equivalentes, em ambos os cenários (com e sem interferências) para todas as topologias. Embora a opção **Réplicas** = 5 tenha um desempenho ligeiramente superior (2.74%), as duas opções são estatisticamente equivalentes. Observamos a mesma equivalência entre as duas opções ao avaliar a métrica do Média do *ETX-Path* (ver figura 17). Nesse caso, o ganho médio da opção com **Réplicas** = 5 é 1.44%. A figura 16 e figura 17 também mostram que o mecanismo de difusão controlado proposto (**Réplicas** > 1) melhora o desempenho do *RGPOP*, uma vez que a performance com **Réplicas** = 3 ou **Réplicas** = 5 apresentam um ganho médio de 26% quando comparado à opção sem réplicas (**Réplicas** = 1) para a primeira métrica e 21,41% para a segunda. Para as comparações com o *GEAR*, foi escolhido considerar apenas a opção com **Réplicas** = 3. Essa configuração é adotada apenas para a padronização dos experimentos, uma vez que o protocolo é dinâmico e o valor do parâmetro pode ser atribuído pela aplicação ao enviar a

Mensagem de Interesse.

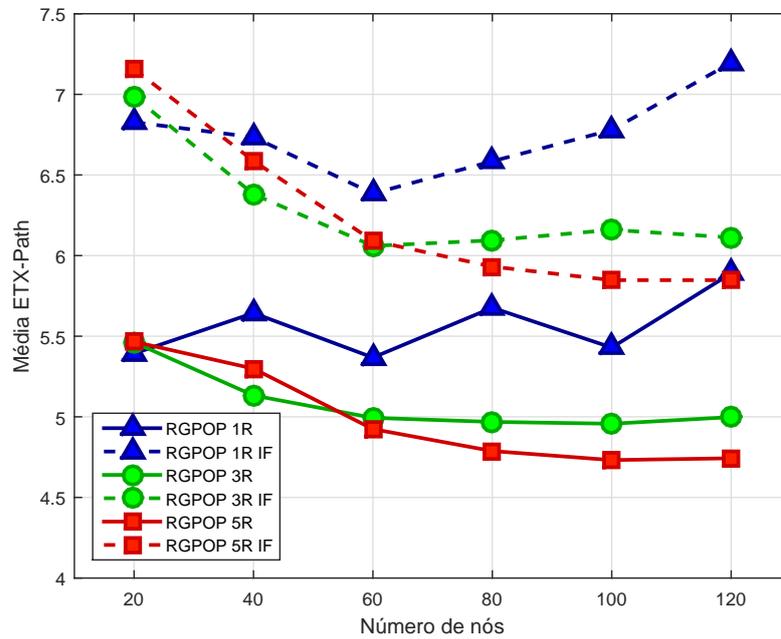
Figura 16 – Proporção de Mensagens de Interesse recebidas com sucesso.



Fonte: Autoria Própria

6.2 Proporção de Mensagens de Interesse recebidas

A figura 18 mostra a comparação em direção a região alvo, onde é possível observar um desempenho superior do *RGPOP*, em cenários com e sem interferência, e para todas as quantidades de nós avaliados. Quando o grau médio da rede é menor (menos número de nós), o ganho médio é de 10,85% no cenário sem interferência e 5,59% no cenário com interferência. À medida que o grau médio da rede aumenta, o ganho também aumenta em mais de 27% em topologias com 100 e 120 nós. O melhor desempenho é esperado porque o *RGPOP* explora opções diferentes durante a construção do caminho. Quando o grau médio é menor, as possibilidades do caminho são menores, e mesmo que 3 réplicas da Mensagem de Interesse sejam enviadas, pode não haver 3 caminhos a serem encontrados. Outro fator que melhora o desempenho do *RGPOP* é o uso de uma métrica para avaliar a qualidade dos *links* (*ETX*), pois quando ele possui uma opção, não é enviado Mensagens de Interesse através de *links* ruins (com $ETX > 4$).

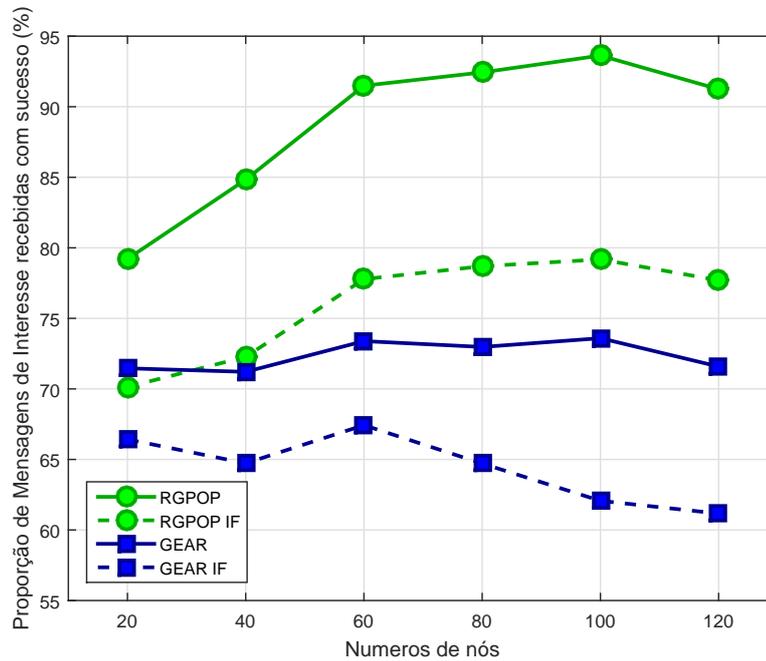
Figura 17 – Média *ETX-Path*.

Fonte: Autoria Própria

6.3 Proporção de Mensagens de Resposta recebidas com sucesso

A Figura 19 mostra a comparação da entrega das Mensagens de Resposta. É possível observar um ganho de desempenho significativo do *RGPOP* em relação ao *GEAR*, devido às boas escolhas que o primeiro faz durante a construção dos caminhos, especialmente nas topologias com o grau médio maior. Em topologias com 20 nós, o desempenho do *RGPOP* é 10% maior no cenário sem interferência e 2% maior no cenário com interferência. Os ganhos de desempenho aumentam significativamente a partir 60 nós. Em topologias de 80 nós, o *RGPOP* é superior a 64% no cenário sem interferência e 50% no cenário com interferência. A maior diferença ocorre em topologias com 120 nós, com um ganho de 72% e 57%. Por outro lado, é possível observar que o aumento do grau médio da rede afeta negativamente o desempenho do *GEAR*. A explicação para o bom desempenho do *RGPOP* é a sua capacidade de evitar *links* com má qualidade de transmissão. Outra razão é a sua resiliência, uma vez que é capaz de identificar a degradação da qualidade dos *links* (incremento *ETX*) pode escolher um caminho com melhor *ETX-Path*.

Figura 18 – Proporção de Mensagens de Interesse recebidas com sucesso.



Fonte: Autoria Própria

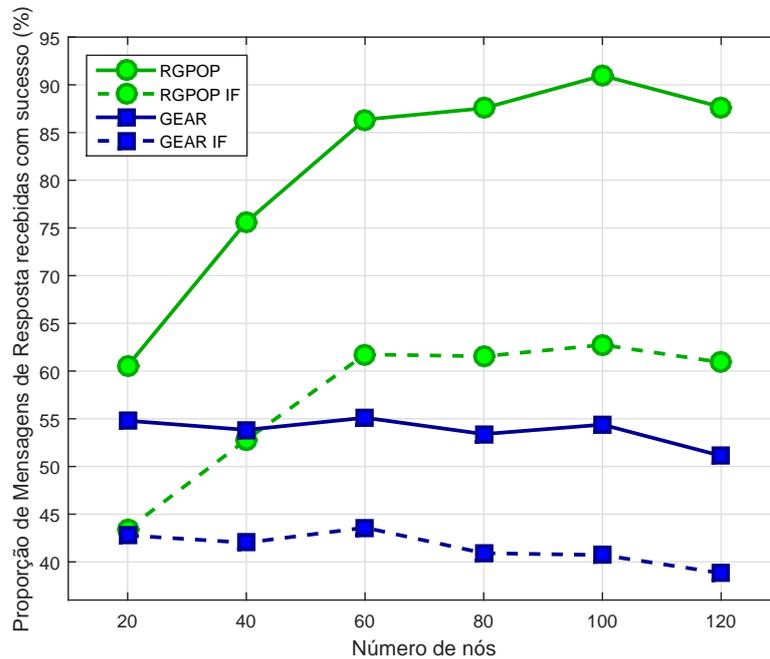
6.4 Média *ETX-Path*

Neste momento é iniciado as comparações utilizando as métricas de qualidade. A Figura 20, é comparado a qualidade dos caminhos em relação à métrica *ETX-Path*. Nesse caso, os dois protocolos apresentam desempenho semelhante nas topologias menos densas. Por exemplo, com 20 nós, o desempenho *GEAR* é 4,74% maior no cenário sem interferência. Em topologias com graus mais elevados de nó, o *RGPOP* funciona melhor. No melhor caso (120 nós), seu desempenho é 22,41% maior no cenário sem interferência e 23,21% maior no cenário com interferência. Este resultado é devido as escolhas feitas pelo *RGPOP* durante a construção dos caminhos, que opta por *links* com menor custo de *ETX* e explora diferentes alternativas, o que oferece ao nó que tem uma Mensagem de Resposta para enviar, uma visão mais ampla das condições da rede através do *ETX-Path*.

6.5 Média de Contagem de Saltos

A figura 21 apresenta resultados a partir da métrica Média de Contagem de Saltos. Em ambos os protocolos a interferência afetou pouco o resultado, a maior diferença é nas topologias com 20 nós, a qual *RGPOP* x *RGPOP IF* a diferença é de 7,29% e *GEAR* x *GEAR IF* é de 6,45%. Por haver uma diferença mínima entre os cenários

Figura 19 – Proporção de Mensagens de Resposta recebidas com sucesso.



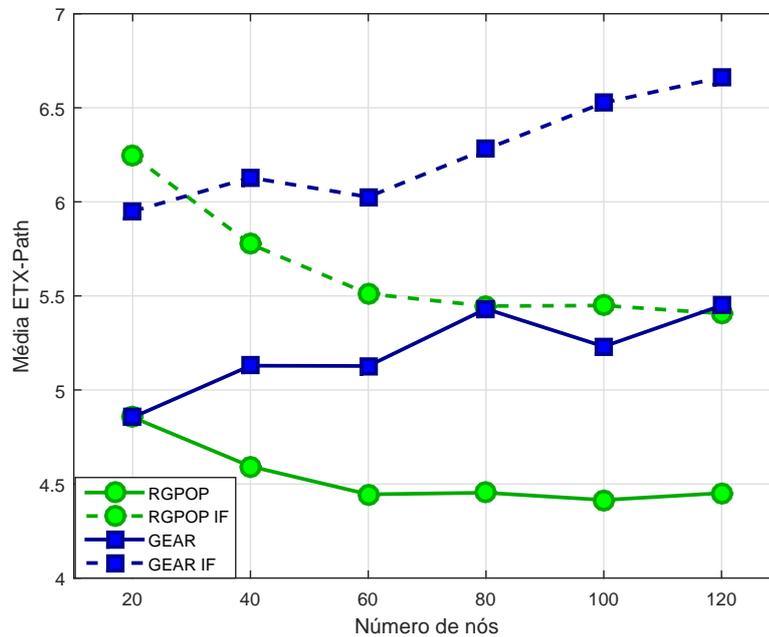
Fonte: Autoria Própria

com e sem interferências será utilizado como base os resultados com interferência por serem mais próximo das condições reais de uma *RSA*. A diferença entre *RGPOP IF* e *GEAR IF* é pequena, no pior caso (com 20 nós) o *GEAR IF* tem um melhor desempenho com 11,98%, essa pequena diferença ainda diminui gradualmente quando submetido as topologias com maior o número de nós, nas topologias com 60 nós a diferença é de 7,01%, a menor diferença encontrada é com 120 nós o *GEAR IF* tem um desempenho de 3,80% melhor. Esse desempenho é devido o *GEAR* realizar escolhas considerando a distância, optando por *links* que sejam mais próximos do destino, não levando em conta a qualidade de comunicação. Desta forma o *GEAR* encontra caminhos com menos saltos, porém a qualidade de transmissão pode não ser boa. O *RGPOP* no momento em que encontra caminhos com más condições de transmissão, caso tenha opções é evitado o *link* e é selecionado outro mais distante.

6.6 Discussão

Neste capítulo foi apresentado o desempenho do protocolo *RGPOP* comparando com o protocolo *GEAR*.

De acordo com os resultados apresentados, é possível concluir que o *RGPOP* teve um desempenho melhor em muitos aspectos. A justificativa deste desempenho é a natureza

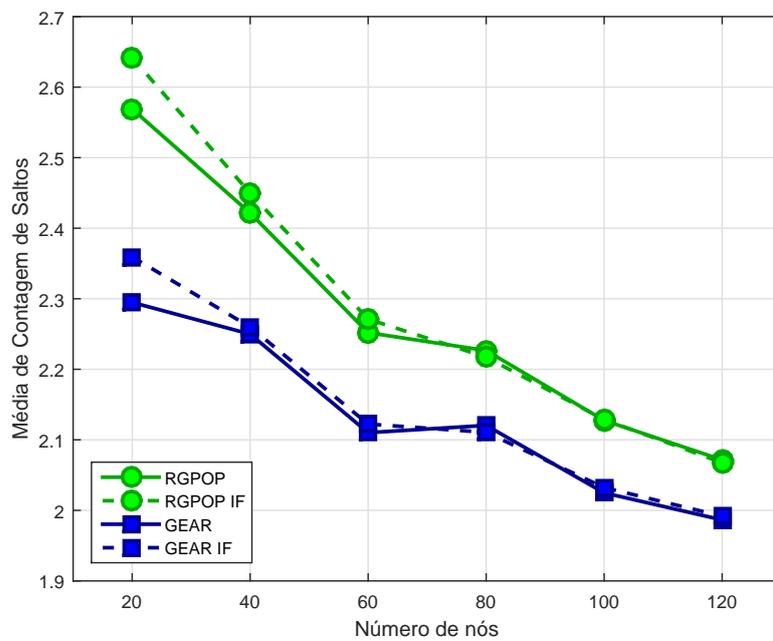
Figura 20 – Média *ETX-Path*.

Fonte: Autoria Própria

deste protocolo, que foi projetado para trabalhar com *RSA* que tem como característica ser dinâmica, onde é esperado que haja falhas de comunicação que podem ser causadas por obstáculos interferentes algo comum no meio ambiente, como por exemplo, arvores, rochas, aclives, declives entre outros. O *GEAR* tem como característica contornar buracos, mas não é sensível a qualidade dos *links*, mesmo que um *link* esteja degradado é considerado encaminhar mensagens por ele.

Mesmo o *RGPOP* escolhendo caminhos mais longos em relação a quantidade de saltos do que o *GEAR*, os resultados demonstram que se não for levado em conta a qualidade dos *links*, pode influenciar diretamente a entrega de mensagens. O *RGPOP* consegue entregar mais dados do que o *GEAR* nas mesmas condições submetidas, entregando até 72% a mais. Além da característica do *RGPOP* ser sensível a qualidade de transmissão, são formados múltiplos caminhos, o que faz com que o *RGPOP* tenha melhores condições de avaliar qual é o caminho encontrado mais adequado para envio de dados.

Figura 21 – Média de Contagem de Saltos.



Fonte: Autoria Própria

7 Conclusão

Este trabalho apresentou um protocolo de roteamento geográfico orientado para qualidade de serviço. O protocolo desenvolvido tem como características resiliência que é obtida através dos múltiplos caminhos formados, e a qualidade de transmissão atingida através da escolha de caminhos de melhor qualidade durante a construção das rotas. Essas características apresentadas são adequadas para o sensoriamento ambiental, uma vez que as *RSA* estão sujeitas a erros causados por ruídos, sombreamento e interferências, gerando perda de pacotes. Além das características do protocolo proposto, a característica do paradigma de encaminhamento baseado em localização, contribui para a economia de energia devido os nós necessitarem apenas das informações dos vizinhos diretos para manter a topologia.

O estudo mostra que *RGPOP* fornece um alto grau de resiliência quando comparado a um protocolo geográfico clássico (*GEAR*). O *RGPOP* não só escolheu caminhos com melhor qualidade de transmissão como em consequência disto conseguiu entregar mais mensagens de dados do que o *GEAR*. As descobertas mostram que o protocolo proposto é muito promissor porque é capaz de fornecer consultas e respostas com taxas de perda de mensagens consideravelmente menores e caminhos de comunicação de melhor qualidade, principalmente em cenários em que a qualidade dos links é afetada pelas condições ambientais, o desempenho do protocolo mostrou-se comparativamente muito maior.

Através dos objetivos alcançados durante o desenvolvimento deste trabalho especificados no capítulo 1, com o propósito de responder à questão de pesquisa, é seguro afirmar com base nos resultados obtidos: **é vantajoso desenvolver protocolos de roteamento geográfico para *RSA* que levem em conta múltiplos caminhos e a qualidade dos enlaces de comunicação em *RSSF*.**

Este trabalho tem como limitações estudar o emprego da difusão controlada, os caminhos formados por ela e a utilização da métrica *ETX*, a qual demonstrou fazer boas escolhas durante a formação dos caminhos, optando por *links* de melhor qualidade de transmissão. Não contemplando este estudo a entrega de interesse na região de destino, foram citadas duas abordagens que se comprometem em fazer a entrega de interesses pelos autores: (YU; GOVINDAN; ESTRIN, 2001).

Os resultados demonstraram que a qualidade de transmissão dos caminhos encontrados pelo *RGPOP* são satisfatórios, porém não foi aprofundado o estudo sobre a quantidade de réplicas e intervalo entre sondas ideal para casos específicos. O *RGPOP* implementa o *ETX* em suas mensagens de sonda, se o intervalo entre uma mensagem de sonda é alterado o nível de sensibilidade muda, por exemplo, quanto menor o intervalo

entre sondas, mais rápido é percebido caso haja degradação do *link*, por outro lado o número de mensagens de sonda aumenta e pode prejudicar a comunicação. Estudos mais detalhados irão demonstrar quais as configurações que terão mais efetividade em situações específicas melhorando o desempenho do *RGPOP*.

7.1 Publicação

No desenvolvimento deste trabalho de pesquisa foi publicado o seguinte artigo:

Espindola, A. S.; Penna, M. C.; Pellenz, M. E.; Jamhour, E. Geographical QoS-Oriented Protocol for Environmental Sensor Networks. IEEE International Conference on Advanced Information Networking and Applications, 2018. (AINA - Qualis A2)

Referências

- AKYILDIZ, I. F.; WANG, X. A survey on wireless mesh networks. *IEEE Communications Magazine*, v. 43, n. 9, p. S23–S30, Sept 2005. ISSN 0163-6804. Citado 2 vezes nas páginas 24 e 27.
- AL-KARAKI, J. N.; KAMAL, A. E. Routing techniques in wireless sensor networks: a survey. *IEEE Wireless Communications*, v. 11, n. 6, p. 6–28, Dec 2004. ISSN 1536-1284. Citado 3 vezes nas páginas 25, 26 e 28.
- ALOTAIBI, E.; MUKHERJEE, B. A survey on routing algorithms for wireless ad-hoc and mesh networks. *Computer Networks*, v. 56, n. 2, p. 940 – 965, 2012. ISSN 1389-1286. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S138912861100377X>>. Citado na página 24.
- AMADEO, M. et al. Content-centric wireless networking: A survey. *Computer Networks*, Elsevier, v. 72, p. 1–13, 2014. Citado na página 24.
- ANISI, M. H. et al. Overview of data routing approaches for wireless sensor networks. *Sensors*, v. 12, n. 4, p. 3964, 2012. ISSN 1424-8220. Disponível em: <<http://www.mdpi.com/1424-8220/12/4/3964>>. Citado na página 27.
- BROCH, J. et al. A performance comparison of multi-hop wireless ad hoc network routing protocols. In: *Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking*. New York, NY, USA: ACM, 1998. (MobiCom '98), p. 85–97. ISBN 1-58113-035-X. Disponível em: <<http://doi.acm.org/10.1145/288235.288256>>. Citado na página 24.
- CADGER, F. et al. A survey of geographical routing in wireless ad-hoc networks. *IEEE Communications Surveys Tutorials*, v. 15, n. 2, p. 621–653, Second 2013. ISSN 1553-877X. Citado 7 vezes nas páginas 20, 21, 28, 29, 30, 31 e 39.
- CORKE, P. et al. Environmental wireless sensor networks. *Proceedings of the IEEE*, IEEE, v. 98, n. 11, p. 1903–1917, 2010. Citado 2 vezes nas páginas 20 e 21.
- CORSON, S.; MACKER, J. *Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations*. [S.l.], 1998. Disponível em: <<https://www.rfc-editor.org/info/rfc2501>>. Citado na página 24.
- COUTO, D. S. D. et al. A high-throughput path metric for multi-hop wireless routing. *Wireless Networks*, Springer-Verlag New York, Inc., v. 11, n. 4, p. 419–434, 2005. Citado 2 vezes nas páginas 32 e 33.
- DJENOURI, D.; BALASINGHAM, I. Traffic-differentiation-based modular qos localized routing for wireless sensor networks. *IEEE Transactions on Mobile Computing*, v. 10, n. 6, p. 797–809, June 2011. ISSN 1536-1233. Citado na página 37.
- DRAVES, R.; PADHYE, J.; ZILL, B. Routing in multi-radio, multi-hop wireless mesh networks. In: ACM. *Proceedings of the 10th annual international conference on Mobile computing and networking*. [S.l.], 2004. p. 114–128. Citado 2 vezes nas páginas 33 e 34.

- FAYAZBAKSH, S. K. et al. Less pain, most of the gain: Incrementally deployable icn. In: *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*. New York, NY, USA: ACM, 2013. (SIGCOMM '13), p. 147–158. ISBN 978-1-4503-2056-6. Disponível em: <<http://doi.acm.org/10.1145/2486001.2486023>>. Citado na página 28.
- GOYAL, D.; TRIPATHY, M. R. Routing protocols in wireless sensor networks: A survey. In: *2012 Second International Conference on Advanced Computing Communication Technologies*. [S.l.: s.n.], 2012. p. 474–480. ISSN 2327-0632. Citado na página 25.
- HAMILTON, M. P. et al. New approaches in embedded networked sensing for terrestrial ecological observatories. *Environmental Engineering Science*, Mary Ann Liebert, Inc. 2 Madison Avenue Larchmont, NY 10538 USA, v. 24, n. 2, p. 192–204, 2007. Citado na página 19.
- HART, J. K.; MARTINEZ, K. Environmental sensor networks: A revolution in the earth system science? *Earth-Science Reviews*, Elsevier, v. 78, n. 3, p. 177–191, 2006. Citado 2 vezes nas páginas 19 e 23.
- HARTENSTEIN, H.; LABERTEAUX, L. P. A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*, v. 46, n. 6, p. 164–171, June 2008. ISSN 0163-6804. Citado na página 24.
- KARAMI, A.; GUERRERO-ZAPATA, M. A fuzzy anomaly detection system based on hybrid pso-kmeans algorithm in content-centric networks. *Neurocomputing*, v. 149, Part C, p. 1253 – 1269, 2015. ISSN 0925-2312. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S0925231214011588>>. Citado na página 28.
- KARAMI, A.; GUERRERO-ZAPATA, M. A hybrid multiobjective rbf-pso method for mitigating dos attacks in named data networking. *Neurocomputing*, v. 151, Part 3, p. 1262 – 1282, 2015. ISSN 0925-2312. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S0925231214014775>>. Citado na página 28.
- KARP, B.; KUNG, H.-T. Gpsr: Greedy perimeter stateless routing for wireless networks. In: ACM. *Proceedings of the 6th annual international conference on Mobile computing and networking*. [S.l.], 2000. p. 243–254. Citado 3 vezes nas páginas 38, 39 e 40.
- KO, Y.-B.; VAIDYA, N. H. Geotora: a protocol for geocasting in mobile ad hoc networks. In: IEEE. *Network Protocols, 2000. Proceedings. 2000 International Conference on*. [S.l.], 2000. p. 240–250. Citado na página 38.
- LEMMON, C.; LUI, S. M.; LEE, I. Geographic forwarding and routing for ad-hoc wireless network: A survey. In: *INC, IMS and IDC, 2009. NCM '09. Fifth International Joint Conference on*. [S.l.: s.n.], 2009. p. 188–195. Citado 2 vezes nas páginas 28 e 29.
- PATH-CONTROL. *Path Control Description*. 2016. <https://www.ietf.org/mail-archive/web/roll/current/pdfu4TGDiz4XI.pdf>. Acessado: 16/11/2016. Disponível em: <<https://www.ietf.org/mail-archive/web/roll/current/pdfu4TGDiz4XI.pdf>>. Citado na página 34.
- PHAM, T. M. Analysis of isp caching in information-centric networks. In: *Computing Communication Technologies - Research, Innovation, and Vision for the Future (RIVF), 2015 IEEE RIVF International Conference on*. [S.l.: s.n.], 2015. p. 151–156. Citado na página 28.

- RUHRUP, S. Theory and practice of geographic routing. *Ad Hoc and Sensor Wireless Networks: Architectures, Algorithms and Protocols*, Bentham Science Publishers, p. 69, 2009. Citado 2 vezes nas páginas 29 e 30.
- SINGH, S. P.; SHARMA, S. A survey on cluster based routing protocols in wireless sensor networks. *Procedia Computer Science*, v. 45, p. 687 – 695, 2015. ISSN 1877-0509. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S1877050915003695>>. Citado na página 25.
- XU, Y.; HEIDEMANN, J.; ESTRIN, D. Geography-informed energy conservation for ad hoc routing. In: *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*. New York, NY, USA: ACM, 2001. (MobiCom '01), p. 70–84. ISBN 1-58113-422-3. Disponível em: <<http://doi.acm.org/10.1145/381677.381685>>. Citado na página 37.
- XYLOMENOS, G. et al. A survey of information-centric networking research. *IEEE Communications Surveys Tutorials*, v. 16, n. 2, p. 1024–1049, Second 2014. ISSN 1553-877X. Citado 2 vezes nas páginas 26 e 27.
- YANG, Y. *Routing protocols for wireless sensor networks: A survey*. 66 p. Dissertação (Mestrado) — Mid Sweden University, Department of Information Technology and Media, 2013. Disponível em: <<http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A640219&dswid=-2101>>. Citado 2 vezes nas páginas 23 e 25.
- YU, Y.; GOVINDAN, R.; ESTRIN, D. *Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks*. [S.l.]: Technical report ucla/csd-tr-01-0023, UCLA Computer Science Department, 2001. Citado 7 vezes nas páginas 20, 30, 40, 42, 43, 47 e 67.