

CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM MODELAGEM MATEMÁTICA E COMPUTACIONAL

DESENVOLVIMENTO DE UM MODELO DE ESTIMAÇÃO DE CONFIABILIDADE PARA REDES DE SENSORES SEM FIO

RONDINELLI LEONARDO JORGE

Orientador: Paulo Eduardo Maciel de Almeida
Centro Federal de Educação Tecnológica de Minas Gerais

BELO HORIZONTE
AGOSTO DE 2018

RONDINELLI LEONARDO JORGE

DESENVOLVIMENTO DE UM MODELO DE ESTIMAÇÃO DE CONFIABILIDADE PARA REDES DE SENSORES SEM FIO

Dissertação apresentada ao Programa de Pós-graduação em Modelagem Matemática e Computacional do Centro Federal de Educação Tecnológica de Minas Gerais, como requisito parcial para a obtenção do título de Mestre em Modelagem Matemática e Computacional.

Área de concentração: Modelagem Matemática e Computacional

Linha de pesquisa: Sistemas Inteligentes

Orientador: Paulo Eduardo Maciel de Almeida
Centro Federal de Educação Tecnológica de Minas Gerais

CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM MODELAGEM MATEMÁTICA E COMPUTACIONAL
BELO HORIZONTE
AGOSTO DE 2018

Jorge, Rondinelli Leonardo
J82d Desenvolvimento de um modelo de estimação de confiabilidade para redes de sensores sem fio / Rondinelli Leonardo Jorge. – 2018.
80 f.

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Modelagem Matemática e Computacional.
Orientador: Paulo Eduardo Maciel de Almeida.
Dissertação (mestrado) – Centro Federal de Educação Tecnológica de Minas Gerais.

1. Redes de sensores sem fio – Teses. 2. Internet das coisas – Teses. 3. Modelos econométricos – Teses. 4. Sistemas difusos – Teses. I. Almeida, Paulo Eduardo Maciel de. II. Centro Federal de Educação Tecnológica de Minas Gerais. III. Título.

CDD 006.3

Elaboração da ficha catalográfica pela Biblioteca-Campus II / CEFET-MG

Esta folha deverá ser substituída pela cópia digitalizada da folha de aprovação fornecida.

À LAURA ELISA QUE VEIO AO MUNDO NO EXATO MOMENTO DO INÍCIO DESTA CAMINHADA E VEM DEMONSTRANDO COM UM SORRISO A CADA ETAPA VENCIDA, COMO É RECOMPENSADOR O PROCESSO DE APRENDIZADO.

Agradecimentos

Ao Professor Paulo Vitor Campos Souza que me indicou o Programa de Pós-graduação em Modelagem Matemática e Computacional e que foi o primeiro a me fazer acreditar que poderia ser possível.

Ao Professor Doutor Paulo Eduardo Maciel de Almeida com seus *insights* fundamentais que abriram um leque de possibilidades para que esta pesquisa pudesse acontecer.

Aos Professores Doutores Thiago Souza e Antônio Scarpelli pela força, que foi sem dúvida fundamental para esta caminhada.

À Professora Doutora Camila Ferreira, amiga de longa data, pela paciência, disponibilidade incondicional, pelas discussões acirradas e pelo auxílio em todo o processo de pesquisa e escrita deste trabalho.

Aos amigos do Laboratório de Controle Automação e Sistemas Embarcados (LACSE) Professor Ramon Lopes, Túlio Ferreira, Wagner Cipriano e Lucas Braga que mesmo diante dos prazos apertados, sempre conseguiram um tempo extra para me auxiliar nos momentos cruciais para este trabalho.

Ao Breno Souza cuja dedicação e o encorajamento desde o início foram imprescindíveis para que eu chegasse até aqui.

À minha família, amigos e colegas que sempre tinham um ”vai dar certo” pronto pra dizer, mesmo quando nem imaginavam o quanto faltava caminhar até o final.

E finalmente ao CEFET-MG pelo auxílio financeiro sem o qual não seria possível a concretização deste trabalho.

“Por mim se vai à cidade das dores; por mim se vai à ininterrupta dor [...]. Abandonai toda a esperança, ó vós que entrais!” (Dante Alighieri, p. 17, inscrição à porta do Inferno)

Resumo

As Redes de Sensores Sem Fio (RSSF) são elementos fundamentais no ambiente da Internet das Coisas, adquirindo assim uma importância sem precedentes na evolução tecnológica. Sua aplicação se estende entre as mais diversas áreas estratégicas como militar, engenharia, meio ambiente, tráfego, aviação, automação de ambientes e diversas outras que são consideradas corriqueiras nos dias de hoje, como saúde e segurança. Com tanta utilidade, torna-se fundamental que haja um sistema de estimativa quanto ao grau de confiabilidade dessas redes, visando melhor desempenho nas áreas a que são propostas. O presente trabalho tem o intuito de propor e desenvolver um sistema de classificação das RSSF, a partir de modelos matemáticos, que trate objetivamente aspectos como confiabilidade entre os nós da rede, acurácia na comunicação, latência e eficiência energética. Esses valores servirão de entrada para um Sistema *Fuzzy* configurado para retornar como saída o grau de confiabilidade que a RSSF possui para a realização da tarefa para a qual foi designada. Experimentos práticos foram escolhidos a partir de simulações para demonstrar a eficácia do sistema proposto. Os resultados obtidos se mostraram satisfatórios na obtenção do grau de confiança da RSSF em escala de 0 a 1.

Palavras-chave: Redes de Sensores Sem Fio. Internet das coisas. Modelo de Confiabilidade. Sistema Fuzzy.

Abstract

The Wireless Sensor Networks (WSN) are fundamental elements in Internet of Things, thus acquiring an unprecedented technological importance. Its application extends among the most diverse strategic areas such as military, engineering, environment, traffic, aviation, automation of environments and several others that are considered common today, such as health and safety. With such utility, it is important to to have a system to estimate network reliability degrees of these networks, aiming at better performance in the proposed areas. The present work intends to propose and develop a system of WSN classification, based on mathematical models, which objectively addresses aspects such as reliability among network nodes, communication accuracy, latency and efficiency energy. These values will serve as input to a Fuzzy System configured to return the WSN reliability degree. Practical experiments were simulated to demonstrate the proposed system effectiveness. The results were satisfactory in obtaining a reliability degree in a scale from 0 to 1.

Keywords: Wireless Sensor Networks. Internet of things. Reliability Model. Fuzzy System.

Lista de Figuras

Figura 1 – Crescimento do número de dispositivos conectados 4
Figura 2 – Publicações específicas relacionadas a modelos de Confiabilidade de RSSF 5
Figura 3 – Arquitetura de um nó sensor 10
Figura 4 – Nó sensor real modelo Mica 2 11
Figura 5 – Rede de Sensores Sem Fio 11
Figura 6 – Grau de pertinência em pesquisa com margem de erro 18
Figura 7 – Grau de pertinência para números pares 18
Figura 8 – Grau de pertinência para ajuste de temperatura 19
Figura 9 – Grau de juventude 20
Figura 10 – Arquitetura do modelo de classificação proposto por Virendra et al.2005 29
Figura 11 – Raio de alcance de rádio de um nó sensor 29
Figura 12 – Metodologia 36
Figura 13 – RSSF criada para simulação e raio de comunicação do nó sensor ID1 . 37
Figura 14 – Raio de comunicação do nó sensor ID5 38
Figura 15 – Sequência de atividades 39
Figura 16 – Grafo da rede simulada do experimento 2 após a perda do nó 5 41
Figura 17 – Grafo da rede simulada no início do experimento 3 41
Figura 18 – Grafo da rede simulada do experimento 3 após a perda do nó 3 42
Figura 19 – Grafo da rede simulada do experimento 3 após a perda do nó 4 42
Figura 20 – Grafo da rede simulada no experimento 1 43
Figura 21 – Sistema *Fuzzy* para Classificação de RSSF 48
Figura 22 – Variável de entrada dos aspectos abordados no Sistema *Fuzzy* 49
Figura 23 – Funções do Sistema 50
Figura 24 – Eficiência Energética 52
Figura 25 – Experimento 2 54
Figura 26 – Experimento 3 55
Figura 27 – Experimento 4 57
Figura 28 – Experimento 5 58
Figura 29 – Experimento 6 59
Figura 30 – Experimento 7 61
Figura 31 – Experimento 8 62

Lista de Tabelas

Tabela 1 – Consumo Energético (mW) 53
Tabela 2 – Experimento 2 55
Tabela 3 – Experimento 3 56
Tabela 4 – Experimento 4 57
Tabela 5 – Experimento 5 58
Tabela 6 – Experimento 6 59
Tabela 7 – Experimento 5 60
Tabela 8 – Experimento 8 61
Tabela 9 – Regras do Sistema *Fuzzy* para classificação do grau de confiabilidade para RSSF 76
Tabela 10 – Atribuição de valores para a variável de saída do Sistema *Fuzzy* 79
Tabela 11 – Estados da variável de saída 80
Tabela 12 – Pesos para definição de saída 80

Sumário

1 – Introdução 1
1.1 Contextualização 3
1.2 Definição do Problema 4
1.3 Objetivos 6
1.4 Organização do trabalho 6

2 – Revisão da Literatura 7
2.1 Conceitos Básicos 7
2.1.1 Internet das Coisas 7
2.1.1.1 Arquitetura em Internet das Coisas 8
2.1.2 Redes de Sensores sem Fio (RSSF) 9
2.1.2.1 Arquitetura em RSSF 10
2.1.2.2 Padrões em RSSF 11
2.1.3 Aplicações das RSSF 12
2.1.3.1 Aplicações das RSSF em Engenharias 12
2.1.3.2 Aplicações de RSSF em Agricultura e Meio Ambiente . . . 13
2.1.3.3 Aplicações Militares para RSSF 13
2.1.3.4 Aplicações das RSSF na saúde 14
2.1.4 Classificação das RSSF 14
2.1.5 Lógica *Fuzzy* 17
2.1.5.1 Fusão de Dados *Fuzzy* 21
2.2 Trabalhos Relacionados 22
2.3 Modelos de Classificação de Confiança para RSSF 27
2.3.1 Confiabilidade 28
2.3.2 Acurácia 32
2.3.3 Latência 32
2.3.4 Eficiência Energética 32
2.3.5 Discussões Finais 33

3 – Metodologia 35
3.1 Hipóteses 39
3.2 Planejamento de Experimentos 40
3.2.1 Planejamento de Experimento 1 40
3.2.2 Planejamento de Experimento 2 40
3.2.3 Planejamento de Experimento 3 41
3.2.4 Planejamento de Experimento 4 42

3.2.5 Planejamento de Experimento 5 . . . 43
3.2.6 Planejamento de Experimento 6 . . . 43
3.2.7 Planejamento de Experimento 7 . . . 43
3.2.8 Planejamento de Experimento 8 . . . 43

4 – Modelagem . . . 45
4.1 Modelo de Confiabilidade de RSSF (μ) . . . 45
4.2 Modelo de Acurácia de comunicação entre nós da RSSF (α) . . . 46
4.3 Modelo de Latência da RSSF (λ) . . . 46
4.4 Modelo de Eficiência Energética da RSSF (β) . . . 47
4.5 Sistema *Fuzzy* para Estimativa de Confiabilidade . . . 47
4.6 Sistema para Automação do Processo . . . 50
4.7 A proposta do Modelo . . . 50

5 – Resultados . . . 52
5.1 Experimento 1 . . . 52
5.2 Experimento 2 . . . 53
5.3 Experimento 3 . . . 55
5.4 Experimento 4 . . . 56
5.5 Experimento 5 . . . 57
5.6 Experimento 6 . . . 59
5.7 Experimento 7 . . . 60
5.8 Experimento 8 . . . 61
5.9 Discussões Finais sobre os resultados . . . 62

6 – Considerações Finais . . . 64
6.1 Trabalhos Futuros . . . 66

Referências . . . 68

APÊNDICE A – Regras do Sistema *Fuzzy* para Classificação das RSSF . . . 73

APÊNDICE B – Atribuição de valores para a variável de saída do Sistema *Fuzzy* 77

APÊNDICE C – Estado e Pesos para atribuição de valores para a variável de saída do Sistema *Fuzzy* . . . 80

1 Introdução

A Internet das Coisas (*Internet of Things* - IoT) é uma realidade atualmente. É um paradigma que vêm sendo constantemente alterado. Uma definição bem aceita para *IoT* a apresenta como uma estrutura inteligente e apta a conectar informações, pessoas e coisas por meio de computadores (EVANS, 2011). Isto implica que qualquer máquina, objeto ou pessoa conectada consiga acessar qualquer informação em um sistema. Internet das coisas é uma infraestrutura de objetos, pessoas, sistemas e recursos de informação interconectados aliados a serviços inteligentes que lhes permitam processar informações do mundo físico e virtual e então reagir (JTC, 2014). De acordo com Minerva, Biru e Rotondi (2015), a *IoT* é vista como a internet dos itens, com seus componentes sensores e atuadores conectados à internet. Essa conexão recorre ao conceito de Redes de Sensores Sem Fio (RSSF), que é, segundo Mármol e Pérez (2011), basicamente constituída por um vasto número de nós sensores os quais são geograficamente distribuídos. Esses nós medem as condições em torno deles como temperatura, pressão e os convertem na forma de sinais que revelam informações. Os dados coletados são transferidos para um coletor chamado de estação base. Esses dados são então transferidos para o utilizador por meio de um *gateway*, satélite ou pela própria internet.

A *IoT* representa, neste momento, uma das tecnologias existentes mais promissoras e as RSSF são um dos principais pilares para as aplicações desta tecnologia (CAPELLA et al., 2016). Uma das principais características da *IoT* é que seus objetos devem estar inseridos em um mesmo contexto, isto é, as aplicações exigem cada vez mais que as “coisas” conheçam suas condições ambientais e ajustem seu comportamento à eles próprios e a outros objetos próximos. Deste modo, as RSSF são consideradas como extensão da internet para o ambiente físico da *IoT* culminando na certeza de que as RSSF se firmam como uma das partes mais importantes de qualquer sistema *IoT*.

Tecnicamente, a *IoT* é uma composição de diversas redes criadas para determinada finalidade (EVANS, 2011). Existem diversas aplicações que corroboram com esta proposição. Por exemplo, o controle de funções do motor de um carro, controle de temperatura em ambientes, serviços de segurança e alarme etc. A evolução da *IoT* contribui para que essas e outras aplicações sejam realizadas com maior segurança e maior possibilidade de gerenciamento. Para compreender a importância da *IoT* é necessário primeiramente perceber a diferença entre internet e *World Wide Web* ou simplesmente *Web* (ALBERT; JEONG; BARABÁSI, 1999). Evans (2011) entende que a internet é a camada física composta por *switches*, roteadores e demais equipamentos que têm por função o transporte de informações de ponto a ponto rapidamente. Ao passo que a Web é uma camada de aplicações que opera sobre a internet, tendo como principal função oferecer uma interface que permita a

utilização dessas informações. Estes dois conceitos, embora se complementem, evoluíram de forma distinta ao longo dos anos. A Web passou por várias etapas evolucionárias: a fase de pesquisa, o compartilhamento de informações comerciais, em seguida a fase do comércio eletrônico até a web social (ABREU, 2009). A internet por sua vez, embora tenha se desenvolvido e aprimorado, não logrou grandes mudanças e permanece realizando essencialmente o mesmo que foi projetada para fazer em seus primórdios (EVANS, 2011). A partir disso compreende-se a importância da *IoT* no sentido de que ela é de fato a primeira mudança substancial da internet quando se propõe a revolucionar consideravelmente a forma como as pessoas vivem, aprendem e trabalham.

As RSSF podem ser vistas como um tipo especial de rede móvel *ad hoc* (MANET – *Mobile Ad hoc Network*). Segundo Loureiro et al. (2003), uma rede tradicional, a comunicação entre os elementos computacionais é feita através de estações base de rádio, que constituem uma infraestrutura de comunicação. Esse é o caso da internet. Por outro lado, em uma rede móvel *ad hoc* os elementos computacionais trocam dados diretamente entre si. Do ponto de vista de organização, RSSF e MANET são idênticas, já que possuem elementos computacionais que comunicam diretamente entre si por meio de enlaces de comunicação sem fio. No entanto, as MANET tem como função básica prover um suporte a comunicação entre esses elementos computacionais, que individualmente, podem estar executando tarefas distintas. Em contrapartida, RSSF tendem a executar uma função colaborativa onde os elementos (sensores) proveem dados, que são processados (ou consumidos) por nós especiais chamados de sorvedouros (*sink nodes*). Pressupondo então que as redes *ad hoc* são uma classe e as RSSF uma subclasse, guardadas as devidas proporções, pode-se considerar que a maior divergência entre uma rede convencional e uma rede *ad hoc*, consequentemente RSSF, é a necessidade que a rede convencional tem de infraestrutura para seu funcionamento. Em RSSF esta necessidade não existe, pois, cada nó da rede exerce função de roteador, cliente e servidor.

Dessa forma passa a ser sumário o bom funcionamento desses nós para que a rede também funcione bem. Esta peculiaridade inibe a utilização dos protocolos desenvolvidos para redes convencionais em redes sem fio, ocasionando em novos protocolos e aplicações exclusivamente projetados para redes *ad hoc*. Uma premissa básica para o funcionamento de redes onde os nós executam tantas funções, é de que estes nós exerçam suas funções de forma plena e perfeita. Ou seja, torna-se extremamente necessário que esses nós funcionem perfeitamente de forma colaborativa. Cada protocolo desenvolvido para redes ad hoc tem a premissa de que todos os nós envolvidos participem efetivamente do processo. Neste contexto, isto implica em um funcionamento isento de erros. Porém, de acordo com Velloso et al. (2006), essa premissa nem sempre é verdadeira. Muitas vezes o funcionamento dos nós de uma rede *ad hoc* pode deixar de corresponder às expectativas e os motivos para que isto ocorra, são variados. Esta disfunção pode incidir diretamente sobre a inviabilização do funcionamento da rede dependendo da tarefa a ser executada. Essa dependência latente

de que todos os nós funcionem à plena capacidade, ocasiona invariavelmente em uma rede ineficiente e vulnerável.

A partir disso, surge a necessidade de modelos de estimação da confiabilidade dos nós de uma rede *ad hoc*, que neste contexto, segundo Lopez et al. (2010), é um aspecto que exerce influência direta sobre uma rede no que tange à garantia do funcionamento adequado da mesma. Neste propósito, inúmeros trabalhos ao longo dos anos vêm se dedicando a propor modelos que demonstrem os graus de confiança de cada nó da rede Uma forma de abordar o problema o problema colocado é a aplicação da Lógica *Fuzzy*.

A Lógica *Fuzzy* é uma lógica multivalorada, também conhecida como lógica nebulosa, de grande abrangência no quesito classificação. É um conceito utilizado tratar situações subjetivas, ou considerar situações imprecisas, como as que normalmente acontecem no cotidiano. Os sistemas *Fuzzy* se baseiam em uma teoria matemática denominada conjuntos *Fuzzy*. Trata-se de uma evolução nos conceitos da teoria clássica de conjuntos, nos quais a pertinência é feita de forma binária. Na lógica *Fuzzy* existe uma pertinência gradativa na qual uma mudança de estado ocorre paulatinamente (GOMIDE; GUDWIN; TANSCHEIT, 1995). Este conceito representado por um sistema, também denominado *Fuzzy*, possibilita o entendimento de outros conceitos como raciocínio de máquina qualitativo, quando por meio de cálculos, computadores conseguem emitir não apenas respostas precisas mas também respostas aproximadas ou subjetivas, elevando o nível de decisão das máquinas, justificando assim sua alcunha e aproximando cada vez mais a máquina do ser humano.

Utilizando os modelos e empregando-os como entradas do sistema *Fuzzy*, pode-se ter como saída o grau de confiabilidade da rede tal que a possibilite classificá-la neste quesito e identificar redes aptas a realizar determinadas tarefas em detrimento de outras redes com graus mais baixos de confiabilidade, que seriam desaconselhadas ao uso a menos que haja intervenção e melhora em seu funcionamento.

São inúmeras as contribuições almejadas com este trabalho. Uma vez aplicado, o modelo, apresentado adiante, poderá otimizar significativamente projetos de *IoT* que tem surgido em larga escala para facilitar o cotidiano das pessoas e organizações, com integração entre utensílios e troca de informações em tempo real. Conceitos como casas inteligentes, estradas inteligentes e até mesmo cidades inteligentes, que já vem sendo explorados em diversos países podem ser otimizados no tocante à confiabilidade das RSSF utilizadas em prol da aplicação destes conceitos.

1.1 Contextualização

Segundo Sousa e Lopes (2011) e Fantacci et al. (2014), existem desafios a serem transpostos para que haja uma real integração entre Internet das Coisas (*Iot*) e RSSF. Existem inúmeras vantagens decorrentes da união destes modelos, sendo oportunidades

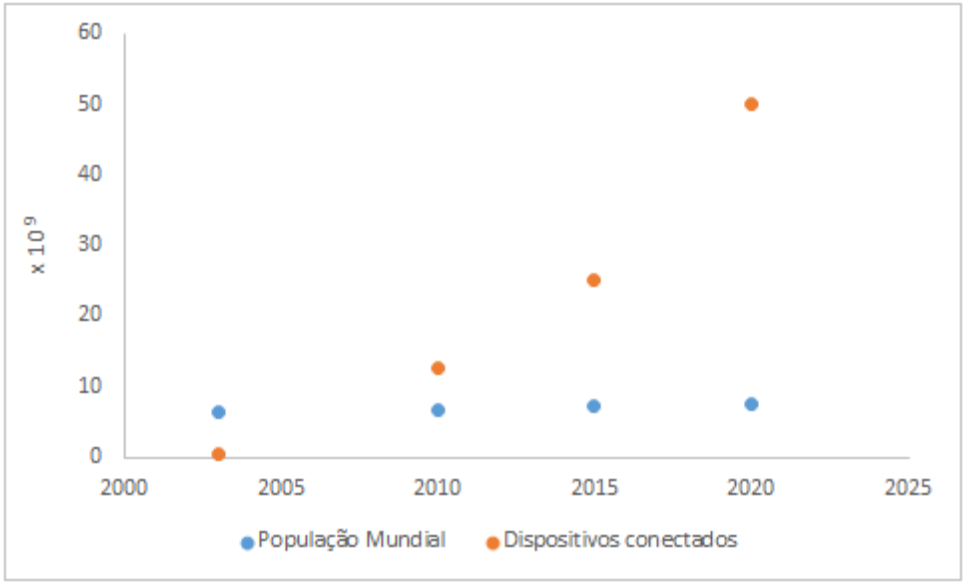
de inovação, a maior delas (GUBBI et al., 2013). Dessa forma, a possibilidade da integração dos referidos paradigmas de maneira adequada visa garantir resultados promissores quanto ao alcance desses modelos.

Neste contexto, criar um modelo para estimação do grau de confiabilidade de RSSF com o intuito de apontar as melhores redes de acordo com métricas relevantes é de extrema importância para o uso efetivo da *IoT*.

1.2 Definição do Problema

Brock (2001) afirma que *IoT* é uma estrutura inteligente capaz de conectar objetos, informação e pessoas, por meio da rede de computadores. Atualmente, a *IoT* é uma realidade latente e ubíqua. Estima-se que ela tenha de fato feito jus à sua alcunha em algum momento entre 2008 e 2009, quando o número de dispositivos conectados ultrapassou a população mundial (Figura 1). Estimava-se 25 bilhões de dispositivos conectados à internet em 2015 e 50 bilhões até 2020 (EVANS, 2011). Até o momento, as estimativas vêm se comprovando e grande parte dessa conectividade é feita através de RSSF. A ubiquidade das redes é uma via de mão única onde a quantidade de redes, nó, e sensores só tende a aumentar. Assim, surge a necessidade de avaliar redes que realmente suportam atividades demandadas no dia a dia.

Figura 1 – Crescimento do número de dispositivos conectados



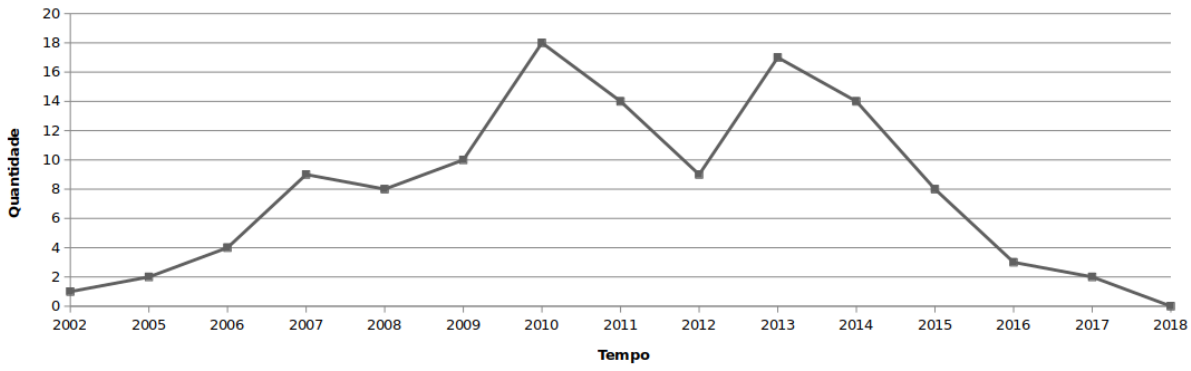
Fonte: Cisco IBSG, abril 2011

Modelos de confiança, em geral, permitem construir uma relação de confiabilidade entre nós de uma rede partindo da troca de informações e de monitoramento constante por parte dos nós vizinhos. De acordo com Velloso et al. (2008), já existem inúmeros trabalhos

que tratam a questão da confiabilidade das redes sem fio. Estes trabalhos, no entanto, têm seu foco geralmente em problemas de roteamento e identificação de nós maliciosos ou até mesmo exploram conceitos relacionados à maturidade da relação entre os nós. Entretanto, não foi identificado, na literatura, um padrão de classificação de toda a rede, baseada em diversos fatores simultâneos e com auxílio da lógica *Fuzzy*, que é uma lógica cujas aplicações abordam diversas áreas do conhecimento por meio de sistemas de suporte à decisão, algoritmos de aproximação de funções e outros tipos de sistemas de controle (REZENDE, 2003). No contexto deste trabalho, o sistema *Fuzzy* servirá para condensar as variáveis de entrada, oriundas de modelos matemáticos propostos, para geração de um grau de confiabilidade para a RSSF por uma escala semântica também proposta posteriormente para classificar o grau obtido.

Atualmente, não se encontram trabalhos relacionados a modelos de confiança com a mesma frequência de outrora. Uma busca por publicações relevantes e pertinentes ao tema proposto neste trabalho, corroborou com esta afirmação, além de identificar a sazonalidade nas pesquisas específicas sobre este assunto (Figura 2). Porém um intuito deste trabalho é trazer a tona novamente questões como esta, visto que ainda não foi identificado nenhum modelo que exprima confiança de uma RSSF sem que a confiabilidade fosse estabelecida limitada a seus nós, ou ainda de acordo com algum fator isolado dos demais.

Figura 2 – Publicações específicas relacionadas a modelos de Confiabilidade de RSSF



Fonte: Google Acadêmico / Agosto 2018

Dessa forma, presume-se que a obtenção do grau de confiabilidade das RSSF utilizando múltiplos fatores permita alcançar resultados que consigam identificar dentro de um espectro de redes avaliadas, quais delas estão aptas a realizar plenamente as tarefas a que foram propostas.

Existem diversos desafios para a classificação efetiva das RSSF. Dentre eles se destacam a grande quantidade de métricas para avaliação das redes como: Eficiência energética, latência e precisão, tolerância a falhas, escalabilidade, exposição dos sensores, vazão fim-a-fim e a reputação dos nós de uma rede (AKYILDIZ et al., 2002). O cerne

desta pesquisa será transpor as dificuldades encontradas e possibilitar uma classificação quanto ao grau de confiança de RSSF para detectar qual daquelas é a mais adequada para realização de sua tarefa fim.

1.3 Objetivos

Este trabalho propõe uma classificação de RSSF que avalie as condições de envio e recebimento de dados, bem como o potencial que a rede como um todo tem de se manter ativa e funcionando confiavelmente. Para isto, é proposto um modelo de classificação de confiança de RSSF baseado em lógica *Fuzzy*, o qual receberá como entrada para processamento fatores relevantes para a confiabilidade da rede e processá-los com emprego de um sistema *Fuzzy* configurado para este fim. O sistema deverá então retornar como saída o grau de confiabilidade da rede e classificá-lo mediante a proposta de uma escala para aferição da variável de saída.

O diferencial deste trabalho é classificar uma rede de acordo com o que ela pode fazer como um todo e não apenas com o que cada componente dela pode realizar. Para alcançar este objetivo são traçados os seguintes objetivos específicos:

- Executar experimentos práticos para validar o funcionamento e acurácia do modelo proposto em ambiente simulado;
- Verificar a sensibilidade do modelo quanto a oscilações nas variáveis de entrada, visando alcançar o comportamento esperado para que o modelo proposto se sustente;
- Demonstrar a sensibilidade de todo o modelo em relação a cada uma das variáveis de entrada e aos aspectos que ele considera individualmente ao calcular a confiabilidade de uma RSSF.

1.4 Organização do trabalho

Este documento está organizado em 6 (seis) capítulos. O segundo capítulo apresenta de forma introdutória os conceitos utilizados neste trabalho bem como traz discussões sobre o estado da arte na classificação das RSSF, Internet das Coisas e a lógica *Fuzzy* que será utilizada para determinar o grau de confiabilidade da RSSF. O terceiro capítulo aborda a metodologia do estudo proposto e aborda os experimentos realizados. Desde a escolha à elaboração dos mesmos. O quarto capítulo apresenta o modelo de classificação das RSSF proposto. No quinto capítulo são abordados e apresentados os resultados adquiridos após a realização dos experimentos. O último capítulo apresenta as discussões finais acerca do trabalho realizado bem como um contraste entre os resultados obtidos e as hipóteses formuladas previamente.

2 Revisão da Literatura

A primeira parte deste capítulo aborda definições e características dos conceitos inseridos no texto, esses conceitos são explanados de forma sucinta e focada estritamente no contexto deste trabalho. A segunda parte promove uma discussão em torno dos trabalhos relacionados a este tema encontrados na literatura.

2.1 Conceitos Básicos

2.1.1 Internet das Coisas

De acordo com Mello et al. (2016), a nova era da computação tenderá a ultrapassar as barreiras dos ambientes de trabalhos tradicionais e a Internet das Coisas é um modelo recente que faz parte dessa nova era. Seu principal objetivo é criar a possibilidade de comunicação entre pessoas e objetos e também entre objetos sem a necessidade de intervenção humana. Para compreender melhor a chamada nova era da computação, é necessário abordar as origens deste modelo promissor para o futuro. Como expresso anteriormente, a Internet das Coisas se tornou parte da história em algum momento entre 2008 e 2009 quando objetos conectados ultrapassaram em número a população mundial (Figura 1). Desde então essa quantidade de itens conectados à internet cresce exponencialmente ano após ano, a ponto de Capella et al. (2016) afirmarem que a Internet das Coisas é uma das tecnologias mais promissoras que surgiu nas últimas décadas. Confirmando isto, Gubbi et al. (2013) afirmaram que este conceito, àquela época, já havia obtido amadurecimento suficiente para ser considerado a próxima tecnologia revolucionária na transformação da internet em um sistema totalmente integrado, ou seja, a internet do futuro.

Nos últimos vinte anos a internet tem passado por constante estado de evolução. No início ela era caracterizada pela *World Wide Web* (www), uma rede que ligava documentos HTML (*HyperText Markup Language*) ao topo da estrutura da internet, ou seja, tornava estes documentos utilizáveis. Após uma gradual evolução, essa rede de documentos estáticos alcançou o que passou a ser chamado de *Web* 2.0. Este formato de rede marcou por sua principal característica que era a possibilidade de participação colaborativa por parte de seus usuários (WHITMORE; AGARWAL; XU, 2015).

O Estado da Arte da Internet das Coisas avança para o que alguns estudiosos chamam de *Web* 3.0. O objetivo neste caso é aprimorar as marcações realizadas na *Web* 2.0 para um padrão que a tornaria plenamente compreendida por máquinas, permitindo então que objetos ou itens se comportem de forma mais inteligente. No entanto, autores como

Capella et al. (2016) já pressupõem a existência bem definida da Internet das Coisas antes mesmo de se dar essa evolução por completo. Não há um consenso sobre a definição da Internet das Coisas (WHITMORE; AGARWAL; XU, 2015), apenas um conceito central de que objetos e itens podem ser identificados, detectados, inseridos em rede de processamento de forma que lhes seja permitido comunicar com outros dispositivos e serviços através da internet em prol de algum objetivo útil. Este conceito não é novo e remonta ao início dos anos 2000 (BROCK, 2001) e durante os anos, tecnologias como RFID (Identificação por Radio frequência) e sensores sem fio vêm sendo utilizados para atividades diversas, já que a Internet das Coisas, em toda sua amplitude, permite quantidade infindável de utilização e de diversas formas.

A Internet das Coisas tem ainda um vasto caminho a percorrer de modo que se firme como uma arquitetura inteligente. Diversos fatores e aspectos permeiam esta discussão, principalmente no que tange à segurança das mesmas (MELLO et al., 2016), o que embora seja um fator importante, devido a natureza da abordagem proposta neste trabalho, não será discutida por hora.

2.1.1.1 Arquitetura em Internet das Coisas

Da mesma forma como acontece com a definição universal sobre a Internet das Coisas, a sua arquitetura também carece da falta de consenso. Existem inúmeras propostas de arquitetura que fazem a ligação das diversas tecnologias associadas à Internet das Coisas. Padrões de arquitetura podem ser extremamente complexos, a julgar pelo fato de envolver diversos modelos de conexão, protocolos. Algumas das propostas encontradas na literatura unem modelos de referência e modelos de arquitetura e apresentam diretrizes, boas práticas e até perspectivas para a interoperabilidade da rede (BAUER; WALEWSKI, 2013). Porém outras linhas de raciocínio sobre esta arquitetura são defendidas e surgem para tentar complementar a complexidade do assunto supracitado.

Yun e Yuxin (2010) entendem que a Internet das Coisas pode ser dividida em três camadas: percepção, rede e aplicação. A camada de percepção é responsável pelo sensoriamento, e se subdivide em dois grupos: os marcadores e os leitores. A principal função desta camada é a identificação dos objetos na rede e a coleta de informações. A camada de rede consiste em uma rede convergente, formada por todos os tipos de redes de comunicação e internet. O gerenciamento da Internet das Coisas e o centro de informações são partes componentes desta camada, ou seja, a camada de rede não tem apenas a capacidade de fazer funcionar a rede, mas também a capacidade de operação da informação. Isso confere a esta o status da camada mais madura da arquitetura em consideração realizada por grande parte dos especialistas no assunto. A função primordial da camada de rede é tornar a Internet das Coisas universal. A camada de aplicação é a Internet das Coisas combinada com a experiência da indústria, a fim de alcançar um amplo

conjunto de soluções de aplicações inteligentes. Através dessa camada, a Internet das Coisas pode atingir um maior grau de integração das informações, tecnologias e também indústria. No entanto, ainda não há uma arquitetura formalmente estruturada.

Ainda de acordo com Yun e Yuxin (2010), a estrutura mais representativa da Internet das Coisas são o sistema EPC Global[1], apoiado pela Europa e Estados Unidos e o sistema japonês Ubiquitous ID. O sistema EPC é composto por três partes: sistema de codificação, sistema de identificação por radiofrequência e rede de informação. A arquitetura apresentada pela EPC ainda inclui seis áreas que consistem em código, *tags* EPC e leitores, *middleware* EPC, ONS (*Object Naming Service*) e EPCIS *servers*. O padrão EPC Global é dividido em três níveis, sendo eles: identificação , captura e troca. Já o propósito da criação do UID é estabelecer e popularizar as técnicas básicas necessárias à identificação automática de objetos. Eventualmente esse sistema pode alcançar o posto de onipresente. A arquitetura da tecnologia UID é composta por um ubíquo (uCode), um dispositivo de comunicação ubíquo, um servidor de sistema de informação e servidores de análise uCode. O sistema UID usa o uCode como uma identidade de objetos e lugares do mundo real. Ainda de acordo com Yun e Yuxin (2010), como uma das características da Internet das Coisas é permitir conexão entre diferentes tipos de redes de comunicação, existe também o viés dos serviços executados em camadas distintas que não são abordados nesta representação, o que confirma até então a ausência de consenso em definir essa arquitetura.

2.1.2 Redes de Sensores sem Fio (RSSF)

De acordo com Mármol e Pérez (2011), uma Rede de Sensores sem Fio é um vasto número de sensores geograficamente distribuídos. São redes baseadas em pequenos nós que atuam em cooperação uns com os outros. Sousa e Lopes (2011) classificam uma RSSF como uma rede composta de elementos de sensoriamento, processamento computacional e de comunicações que viabilizam ao administrador dessa rede, funcionalidades como monitoramento e reação a eventos em determinado ambiente. Já Loureiro et al. (2003) atentam para a diferença de uma RSSF para outras redes. Segundo ele, este tipo de rede se difere das demais em vários aspectos, pois normalmente possuem grande quantidade de nós distribuídos, contam com restrições energéticas e possuem mecanismos de auto configuração e adaptação para mitigar efeitos decorrentes de problemas como perda de nós ou falhas de comunicação.

Fantacci et al. (2014) chamam atenção para o desempenho deste tipo de rede na indústria e na academia, frisando sua versatilidade, e lembram que o avanço tecnológico faz com que a miniaturização dos nós decorrente deste avanço auxilie para o aumento das aplicações que podem ser abrangidas pelas RSSF. Gubbi et al. (2013) concordam quando

[1] A EPCglobal Network é um conjunto de tecnologias que permite a identificação imediata e automática e o compartilhamento de informações sobre itens na cadeia de suprimentos permitindo visibilidade real das informações sobre esses itens.

reiteram que os avanços tecnológicos nos circuitos integrados e nas comunicações sem fio permitiram a existência de microdispositivos eficientes, de baixo custo para aplicação em detecções remotas. Para eles, a combinação desses fatores melhorou a viabilidade de se utilizar uma rede de sensores constituída por um grande número de sensores inteligentes permitindo coleta, processamento, análise e disseminação de informações valiosas reunidas em uma variedade de ambientes. Capella et al. (2016) concluem que o comportamento correto das RSSF é fundamental para o sucesso das operações as quais forem submetidas e que isto garante, em tese, o funcionamento das aplicações em Internet das Coisas. Entretanto, ainda segundo os autores, embora projetos de RSSF apresentem bom desempenho e comportamento quando avaliados em ambientes controlados, experiências têm demonstrado resultados inferiores em ambientes reais.

2.1.2.1 Arquitetura em RSSF

Nós sensores são as peças fundamentais em uma RSSF e são comumente conhecidos por seu baixo consumo energético, baixo custo e obviamente por se comunicarem sem a necessidade de cabos (MÁRMOL; PÉREZ, 2011). Dependendo da aplicação, os nós sensores podem ser endereçados unicamente, mas isso não é uma premissa. Sensores de uma rede podem adquirir características diferentes tendo em vista a aplicação a qual são submetidos. Por exemplo, podem adquirir mobilidade se um sistema assim o permitir, e também pode ocorrer que não exista mobilidade caso a aplicação assim necessite (LOUREIRO et al., 2003). A Figura 3 apresenta a estrutura de um modelo real de nó sensor, enquanto a Figura 4 mostra um tipo real de nó sensor.

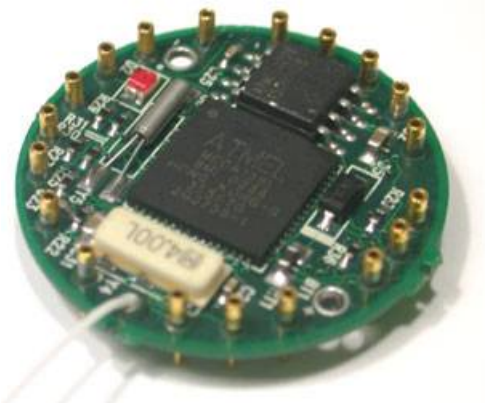
Figura 3 – Arquitetura de um nó sensor



A arquitetura básica de uma RSSF, demonstrada esquematicamente na Figura 5 é composta por nós sensores, um campo de sensoriamento, estação base (sink), o meio de difusão dos dados obtidos, um gerenciador de tarefas, o fenômeno de interesse, ou seja, a aplicação e o observador.

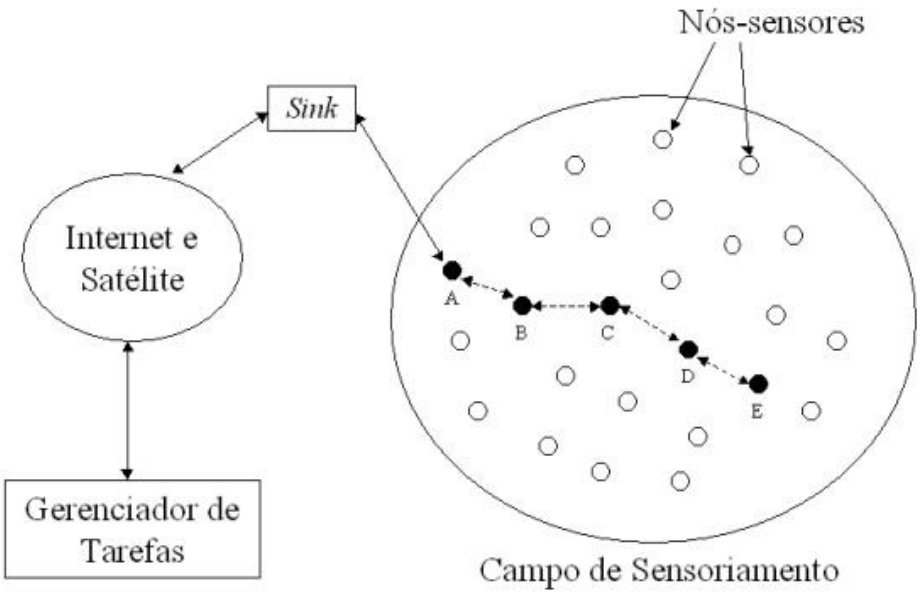
A Figura 5 permite observar que o nó sink representa o elemento responsável pela comunicação com o observador, que é o usuário do sistema que deseja receber informações

Figura 4 – Nó sensor real modelo Mica 2



do sensoriamento obtidas a partir da aplicação pelo meio de difusão dos dados obtidos (satélite ou internet). Comumente a estação base é estabelecida nas proximidades da rede.

Figura 5 – Rede de Sensores Sem Fio



2.1.2.2 Padrões em RSSF

Existem alguns padrões em RSSF que visam, entre outras coisas, reduzir ainda mais o consumo energético dos nós sensores, ocasionando um aproveitamento maior por parte da rede sobre cada nó envolvido na aplicação. O instituto IEEE, sigla que representa *Institute of Electrical and Electronics Engineers* ou Instituto de Engenheiros Eletricistas e Eletrônicos é um dos órgãos responsáveis por elaborar e definir diretrizes para as redes pessoais sem fio. Atualmente é adotado o padrão IEEE 802.15.4 para definir o canal físico de comunicação em baixa potência, através de radiofrequências nos valores de 3.1 a 10.6 GHz, 868.0 e 915.0 MHz. (MOLISCH et al., 2004).

Especificamente, as RSSF operam, em sua grande maioria, na faixa de 2,4 GHz (GAO, 2011). Segundo Spagnol et al. (2018),esta faixa de frequência proporciona largura de banda suficiente, pequenas antenas e disponibilidade de vários sensores de rádio baseados no padrão IEEE 802.15.4.

2.1.3 Aplicações das RSSF

São inúmeras as maneiras e diversas as formas de se utilizar uma RSSF. Graças a sua característica ubíqua, encontram-se infindáveis redes disponíveis para uso (PUCCINELLI; HAENGGI, 2005). Existe uma enorme gama de aplicações nas quais as RSSF podem ser utilizadas em diversas áreas do conhecimento e isso demonstra a relevância dessa tecnologia.(AKYILDIZ et al., 2002; PUCCINELLI; HAENGGI, 2005).

O intuito desta seção é demonstrar exemplos de algumas aplicações das RSSF e comprovar a relevância dessa tecnologia. Como existem inúmeras aplicações distintas e em diversas áreas, os exemplos de aplicações neste capítulo são apresentados de forma categorizada, por área de conhecimento, a fim de facilitar a compreensão e a abrangência deste conteúdo.

2.1.3.1 Aplicações das RSSF em Engenharias

No âmbito das engenharias, as RSSF podem ser utilizadas de inúmeras formas e aplicações (PICOZZI et al., 2010). Em veículos automotores os sensores podem ser embarcados de forma a monitorar o tráfego de veículos em rodovias (CRUZ; COUTO; COSTA, 2018), malhas viárias e urbanas e deste modo as RSSF podem contribuir na segurança e eficiência do tráfego nas vias(BENCKE; PEREZ; ARMENDARIS, 2017). Sistemas de sensores podem ser usados também para substituir os dispositivos de entrada dos computadores, uma vez que os sistemas serão alimentados por dados advindos dos próprios sensores e dispensam por consequência o uso convencional dos dispositivos comuns. Este passo pode fazer com que os sistemas tenham interfaces ainda mais amigáveis para seus usuários. Hoje em dia inúmeros parques industriais recorrem ao uso de robôs, todos equipados com grande quantidade de sensores geralmente conectados a uma central de processamento por meio de cabos. O custo de manutenção destes cabos tem sido fator preponderante para que as empresas empreguem RSSF. A preferência se acentua quando os robôs necessitam de mobilidade.

Outra forma de aplicação de RSSF é que os sensores podem trabalhar de forma a auxiliar o controle de aeronaves em determinado espaço aéreo. Podem ser realizados monitoramento de condições de vôo e até auxílio direto na pilotagem. Ambientes inteligentes (AKYILDIZ et al., 2002) podem ser equipados com sensor de luz, temperatura, movimento, pressão em poltronas, reconhecimento de voz, etc. A partir disso cunha-se termos como *Smart Offices*. O comércio e a indústria também podem ser contemplados com os benefícios

das RSSF. Sistemas de etiquetagem e codificação para facilitar o armazenamento e o gerenciamento de produtos são utilizados exaustivamente e tudo isso é possível por meio dos sensores de reconhecimento de padrões. Ainda neste contexto é bastante comum o uso de sensores para monitoramento de ambientes, que seja indústria ou comércio, empregando assim as RSSF em sistemas de vigilância e segurança. As RSSF podem realizar monitoramento de estruturas como pontes e viadutos para detectar falhas estruturais e também deterioração de materiais e então gerar alertas.

2.1.3.2 Aplicações de RSSF em Agricultura e Meio Ambiente

As RSSF também podem ser utilizadas na agricultura e no meio ambiente. Atividades como gerenciamento da colheita, controle de gado (EVANS, 2011), manutenção dos níveis de concentração de fertilizantes, que precisam ser exatos, etc. Podem seu usadas em explorações de ambientes inóspitos, uma vez que os sensores podem funcionar perfeitamente em diversas condições. Outro exemplo de utilização das RSSF em prol do meio ambiente é a possibilidade de se detectar atividades sísmicas e emitir comunicados evitando catástrofes.

O monitoramento da qualidade da água também é uma realidade em se tratando das RSSF. O uso de sensores é uma boa opção, pois ignora barreiras de locais remotos e de difícil acesso, ou locais com condições adversas para o homem, além do fato de permitirem uma realização eficiente de amostragens (CARVALHO et al., 2012). Sensores espalhados em praias podem avisar banhistas sobre os níveis de contaminação da água, etc.

Outro recurso para o uso de RSSF para esta área do conhecimento são projetos como o Zebranet [2] da Universidade de Princeton nos EUA (MARTONOSI, 2004) que usa redes de sensores sem fio com o intuito de rastrear o movimento da manada de zebras para pesquisas. Ainda no âmbito acadêmico, pesquisadores das Universidades de Berkeley e *College of the Atlantic*, ambas nos EUA, instalaram sensores na Ilha *Great Duck* [3] a fim de medir entre outras coisas radiação solar e infravermelha. Tudo isso sem deixar de citar sistemas para detecção de incêndios e demais desastres ambientais como enchentes. Havendo alta densidade espacial de sensores, é possível inclusive detectar o foco do problema.

2.1.3.3 Aplicações Militares para RSSF

Em um possível cenário de guerra, as RSSF podem ser bastante úteis no *front*. O estado de tropas e até sua localização podem ser monitorados por RSSF em operações militares. É possível inclusive monitorar armamentos e suprimentos. Sensores magnéticos e

[2] No Projeto ZebraNet são utilizados nós sensores sem fio, que são inseridos em colares colocados em zebras e coletam periodicamente informações sobre a localização dos animais.

[3] Great Duck Island é uma pequena ilha (2,4 km) de comprimento por 0,5 milhas (0,8 km) de largura) no Golfo do Maine

sensores de vibração podem detectar movimento de veículos e de pessoas, tornando mais eficientes o controle e a vigilância de forças inimigas. Sensores acústicos podem entregar a posição de franco-atiradores fornecendo vantagens estratégicas em um campo de batalha. Quartéis generais, de operações, centros de inteligência, depósito de suprimentos ou de munições, muros de retenção , trincheiras, etc. podem ser protegidos a partir de campos de sensores inteligentes capazes de distinguir entre diferentes tipos de intrusos.

Os sensores sem fio podem ainda atuar como um sistema de alarme para alertar contra ameaças químicas ou biológicas. Devido à possibilidade de reorganização inteligente de sensores sem fio, até mesmo uma mudança tática e reorganização de tropas inimigas podem ser interceptadas. Esses são apenas alguns exemplos de como os sensores podem, com fins militares, fornecer vantagens táticas de ataque e defesa dentro do campo de batalha, já que, de acordo com Manjunatha, Verma e Srividya (2008), existe grande variedade de aplicações para as RSSF em ambientes militares.

2.1.3.4 Aplicações das RSSF na saúde

Na medicina os sensores tem grande relevância antecipando o diagnóstico de algumas doenças (AKYILDIZ et al., 2002), ou ainda sendo usados em diversas outras modalidades como cirurgias minimamente invasivas e telemedicina (FURTADO; TROBEC, 2011).

Na área da saúde ainda pode-se citar como exemplos de aplicação a aquisição de informações fisiológicas de naturezas diversas como temperatura corporal, pressão sanguínea, batimentos cardíacos, etc. Todas essas informações podem ser transmitidas para um computador ou um médico. Os sensores podem inclusive enviar alertas sobre possíveis infecções ou até mesmo auxiliar na prevenção de coágulos e trombos.

Em todas as aplicações exemplificadas, as RSSF funcionam com a mesma arquitetura, que apesar de básica, é extremamente funcional e poderosa. Nós sensores distribuídos por um campo de sensoriamento qualquer atuam como captadores de dados e enviam esses dados a uma estação e a partir dela, esses dados são transformados em informações pelo utilizador do sistema, que poderá reagir instantaneamente a alguma especificidade.

2.1.4 Classificação das RSSF

Puccinelli e Haenggi (2005) chamam atenção à onipresença das RSSF. Existem infinitas redes em pleno funcionamento neste momento, assim como outras infinitas redes prontas para uso. Existem incontáveis nós sensores conectados e outros tantos para se conectarem nos próximos minutos e tudo isso acontecendo de forma crescente, com forte tendência de que essas quantidades cresçam ainda mais nos próximos anos. Cada vez mais depende-se do correto funcionamento das RSSF, já que estas estão ocupando papéis mais e

mais importantes e relevantes na tecnologia, e consequentemente na vida das pessoas. Dito isto, torna-se pertinente um modelo de classificação das RSSF quanto à sua confiabilidade. Tarefas importantes podem necessitar ser refeitas caso, por mal funcionamento de uma RSSF, dados se percam ou deixem de ser entregues com garantia às respectivas estações, não garantindo a acurácia dos dados necessitados para tomadas de decisão em diversos níveis. À medida que as RSSF tornam-se mais importantes e abrangentes, a necessidade de garantir seu funcionamento correto cresce de forma proporcional.

Entretanto existem vários desafios a serem transpostos quando se refere a classificação de RSSF pela ampla quantidade de métricas para as avaliar, cada qual com suas peculiaridades (AKYILDIZ et al., 2002):

- **Eficiência Energética:** Consumo de energia é comumente fator fundamental no projeto de uma RSSF. Geralmente nós sensores são operados por meio de baterias. Dessa forma, os protocolos utilizados devem ser eficientes no consumo de energia a fim de maximizar a vida útil da rede. Essa vida útil, por sua vez, pode ser medida por parâmetros como período de atividade dos nós sensores ativos ou período decorrido até que a rede cesse de suprir o sistema com as informações desejadas sobre o fenômeno estudado. Diversos mecanismos vêm sendo propostos para otimizar os algoritmos responsáveis pelo envio e recebimento dos dados na rede. Existem também diversas propostas na literatura para criação de novos meios transmissores, estes mais eficientes no consumo de energia. Ainda de acordo com Akyildiz et al. (2002), o consumo energético de uma rede pode ser dividido em três domínios: sensoriamento, comunicação e processamento de dados. No que tange ao sensoriamento encontram-se as limitações de hardware. O motivo é que os nós sensores geralmente são ou estão em pontos inacessíveis ou de difícil acesso, daí o tempo de vida da rede depende do tempo de vida das fontes de energia, geralmente baterias, dos nós sensores. Embora haja esforços para que os nós sensores utilizem fontes de energias renováveis atualmente, essa dependência ainda é latente. Quanto à comunicação, estima-se que os nós sensores utilizam a maior parte da sua energia transmitindo e recebendo dados. No processamento de dados, argumenta-se que seria o caso de criar estratégias de organização de uma CPU onde o foco seria a energia gasta. Métodos de economia seriam implantados nessas CPU visando aumento da vida útil dos sistemas.

- **Latência e Precisão:** Latência é o espaço de tempo durante o qual há interesse do observador em estudar um fenômeno. Assim a definição de latência depende do objeto de estudo e da própria aplicação sobre este objeto. Informação precisa é o objetivo principal de todo observador, então a precisão é determinada pelo tipo de aplicação. Existe certa ligação entre latência, precisão e eficiência energética. A relação se estabelece cumprindo os requisitos de precisão e latência estipulados pelo sistema, dispensando a menor quantidade de energia possível.

- **Tolerância a Falhas:** Inúmeras são as ocasiões nas quais os nós sensores podem falhar, desde más condições físicas até falta de energia, e dependendo do sistema, pode ser praticamente impossível a substituição do nó sensor defeituoso. Entende-se então que naturalmente uma RSSF deve ser tolerante a algum tipo de falha, visto que são situações que podem ocorrer com certa facilidade. Outro ponto é que falhas não críticas sejam transparentes à aplicação. Geralmente há grande quantidade de sensores no ambiente sensoriado e entende-se que a falha de alguns poucos sensores não deve ser capaz de interferir no funcionamento do restante da rede, então é exatamente esse o objetivo da tolerância a falhas. Obviamente a tolerância deve variar conforme o objetivo da rede. Uma rede doméstica deve aceitar, em tese, uma quantidade muito menor de falhas do que uma aplicação militar, na qual os sensores podem ser destruídos por tropas inimigas, por exemplo.

- **Escalabilidade:** Uma rede escalável deve ser aquela que suporte que o sistema cresça até um tamanho considerado grande. Esse atributo é considerado fator importante em RSSF pela quantidade de nós sensores instalados que em algumas ocasiões pode chegar a milhares. A escalabilidade exige protocolos de roteamento, endereçamento e agregação de dados escaláveis de maneira que a quantidade de nós não influencie significativamente no desempenho da RSSF.

- **Exposição dos nós sensores:** Este fator pode ser definido a partir da medida de quão bem a rede se comporta ao observar determinado objeto movendo-se arbitrariamente em um determinado espaço de tempo.

- **Vazão fim-a-fim:** Largura de banda e quantidade de dados gerados pelo grande número de nós sensores são limitações das RSSF e dessa forma a vazão de dados fica comprometida. Então para garantir o bom desempenho da rede, é necessário a adoção de mecanismos que maximizem essa vazão.

A quantidade de métricas demonstradas acima serve para atenuar a complexidade do problema da classificação das RSSF. Atualmente existem diversos modelos, ou tentativas de se classificar uma RSSF com base em seus nós sob diversos aspectos como segurança, tolerância à falhas (WANG et al., 2005), implantação (DEIF; GADALLAH, 2014) etc. Porém como expresso anteriormente, todas as abordagens consultadas levam em conta apenas seus nós. Desse modo, acredita-se não ser possível lograr resultados mais abrangentes ou mais assertivos em relação à rede como um todo. Assim como as RSSF têm ganhado notoriedade com o passar dos anos, da mesma forma uma classificação plena ganha espaço, visto que as abordagens de classificação contemporâneas ainda não o fizeram.

Para tanto, estima se que o modelo de classificação de confiabilidade dos nós de uma RSSF proposto por Virendra et al. (2005) e aperfeiçoado por Velloso et al. (2006) sirva como base para alcançar um modelo geral de classificação das redes quanto à sua confiabilidade. Neste modelo que será analisado a fundo na seção 4 deste trabalho, o grau de confiabilidade de cada nó da rede é avaliado pelos demais nós e é dado por:

$$T_a(b) = (1 - \alpha)Q_a(b) + \alpha C_a(b), \tag{1}$$

na qual $T_a(b)$ é o grau de confiança do nó a em um vizinho b; $Q_a(b)$ é a capacidade de um nó a avaliar o grau de confiança do nó b baseado em suas próprias informações; $C_a(b)$ é a contribuição de seus vizinhos para avaliação; e α permite priorizar o fator mais relevante entre a contribuição dos vizinhos e as informações locais disponibilizadas pela camada de aprendizado.

2.1.5 Lógica *Fuzzy*

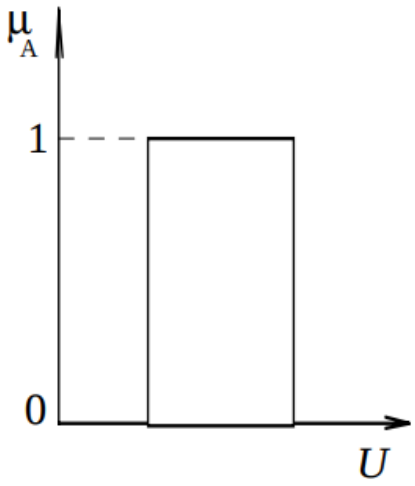
Idealizada por Lofti A. Zadeh no princípio da década de 1960, a lógica *Fuzzy* conhecida como difusa ou nebulosa é uma lógica multivalorada onde valores lógicos atribuído às variáveis podem assumir qualquer número real dentro de um intervalo fechado entre 0 e 1. Diferente da lógica booleana, onde existem apenas respostas binárias (0 ou 1), a lógica difusa representa situações do mundo real onde existem propriedades imprecisas ou imprecisas e portanto, impossíveis de serem caracterizados por predicados da lógica clássica bivalente (REZENDE, 2003, capítulo 7).

Para Gomide, Gudwin e Tanscheit (1995), a lógica nebulosa é aquela que suporta modos de raciocínio aproximados, ao invés de exatos. A lógica *Fuzzy* é derivada do conceito de conjuntos *Fuzzy*, que se difere da teoria clássica de conjuntos na questão da pertinência, pois na teoria clássica, um elemento pode pertencer ou não a determinado conjunto. Dado um universo U e um elemento x pertencente a este grupo ($x \in U$), seu grau de pertinência é dado unicamente pela condição:

$$\mu_A(x) = \begin{cases} 1 \; se \; x \in A \\ 0 \; se \; x \notin A \end{cases}$$

segundo os autores, a função $\mu_A(x)$ é denotada função característica na teoria clássica de conjuntos. Um exemplo de aplicação seria a pertinência ou não determinado valor a um grupo de margem de erro em uma pesquisa (Figura 6). Os números dentro do erro percentual aceito, recebem fator de pertinência 1, enquanto os demais números pertinência 0.

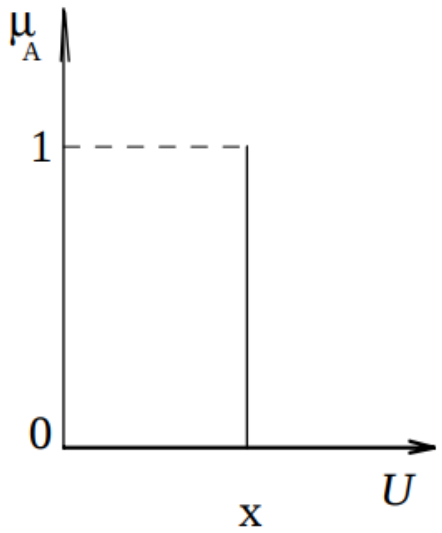
Figura 6 – Grau de pertinência em pesquisa com margem de erro



Fonte: (GOMIDE; GUDWIN; TANSCHEIT, 1995)

Outro exemplo, ilustrado na Figura 7 é quando o resultado esperado é exato. Apenas um fator recebe o grau total de pertinência, enquanto todos os outros recebem grau nulo. Um algoritmo que recebe uma entrada numérica real e classifica esta entrada como par ou ímpar representa este tipo de situação. Nele o algoritmo retornará o grau de pertinência 1 se o valor de entrada é um numero par e pertinência 0 se a entrada for um valor ímpar.

Figura 7 – Grau de pertinência para números pares

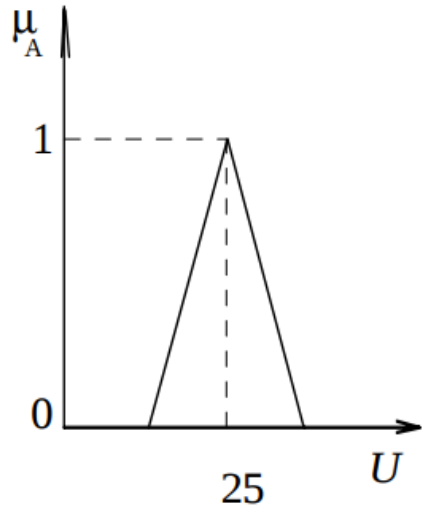


Fonte: (GOMIDE; GUDWIN; TANSCHEIT, 1995)

Enquanto a teoria de conjuntos Fuzzy propõe uma caracterização mais ampla, na medida em que adota a ideia de que alguns elementos são mais membros de um conjunto do que outros (ZADEH, 1965). Ou seja, enquanto 0 representa a total exclusão de um

elemento em um grupo e 1 representa sua total inserção, os valores entre 0 e 1 apontam quão mais ou menos pertencente é este elemento perante determinado grupo. A Figura 8 representa uma situação hipotética de temperatura do ar condicionado em uma sala de escritório quando a temperatura mais agradável é de 25 graus. Os valores de entrada para medição recebem graus de pertinência de acordo com a proximidade da temperatura eleita mais agradável. Neste caso, dentro do universo de discurso definido, pode se usar uma função de pertinência triangular, variando entre 20 e 30 graus. Qualquer temperatura não compreendida neste intervalo, recebe grau 0 de pertinência, enquanto à medida que as temperaturas vão se aproximando da temperatura pré-definida, recebem graus mais elevados de pertinência, até que se atinja o grau 1 para a temperatura ideal.

Figura 8 – Grau de pertinência para ajuste de temperatura



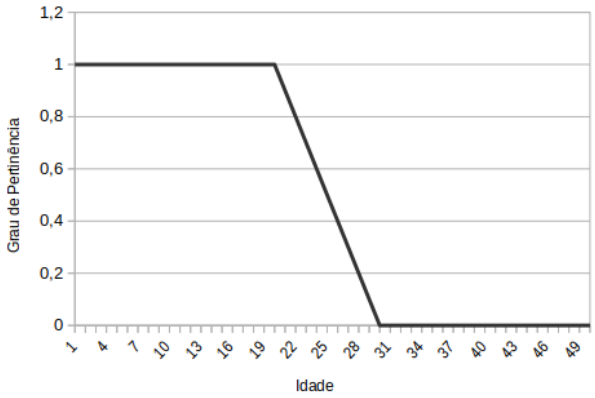
Fonte: (GOMIDE; GUDWIN; TANSCHEIT, 1995)

Outras representações hipotéticas da utilização da lógica *Fuzzy* se dão quando, por exemplo, se é necessário classificar um pessoa quanto à sua idade utilizando o atributo ”jovem” para essa definição. Neste caso, uma pessoa não deixa de ser jovem partir do momento que ultrapassa certa idade. O que ocorre de fato é que com o passar do tempo, uma pessoa vai deixando de pertencer a este *status* paulatinamente. A função que retrata essa mudança de *status* pode ser dada através da seguinte relação:

$$PessoaJovem = \begin{cases} 1, \text{ se idade } \leq 20 \\ \frac{30-idade}{10}, \text{ se } 20 \leq \text{idade} \leq 30 \\ 0, \text{ se idade } > 30 \end{cases}$$

Nota-se que o grau de pertinência referente ao conjunto ” PessoaJovem” varia conforme a idade avança de maneira gradativa, não de forma abrupta. Dessa forma a Figura 9 traduz a função ”PessoaJovem” segundo o grau de juventude.

Figura 9 – Grau de juventude



O objetivo de utilizar a lógica *Fuzzy* para elaborar a classificação de RSSF proposta neste estudo torna-se palpável a partir dos conceitos obtidos na esfera de suas proposições, quando sobre elas, (GOMIDE; GUDWIN; TANSCHEIT, 1995) afirmam que podem ser combinadas, utilizando-se diferentes operadores, gerando novas proposições. As proposições resultantes podem ser descritas em termos de relações *Fuzzy*. Esta possibilidade abre o precedente para que através de diversos fatores, como os que serão abordados adiante, que deverão compor o modelo de classificação de RSSF proposto neste trabalho, sejam tratados de formas distintas porém forneçam um resultado único, condizente com o contexto deste estudo. Por exemplo, sejam $x_1, x_2,..., x_n$ fatores determinantes para a Classificação das RSSF cujos universos de discurso são respectivamente $X_1, X_2,...,X_n$. Seja R uma relação *Fuzzy* definida em $X_1 \times X_2 \times ... \times X_n$. Tem-se então que

$$((x_1, x_2,..., x_n) \text{ é } R)$$

é uma proposição *Fuzzy* n-ária. Isto permite deduzir que a lógica *Fuzzy*, através de suas proposições pode ser utilizada tanto em um contexto simples, onde não haja tratamento de diversos fatores para se obter um resultado da forma

$$\text{se } (x \text{ é A}) \text{ então } (y \text{ é B})$$

quanto em um contexto complexo, onde o resultado dependa de uma série de fatores e sua forma de utilização obedeça

$$\text{se } ((x_1 \text{ é } A_1) \text{ e } (x_2 \text{ é } A_2) \text{ e ... e } (x_n \text{ é } A_n)) \text{ então } (y \text{ é B})$$

e que consequentemente se reduza à forma

$$((x_1, x_2,..., x_n,y) \text{ é } R).$$

Em acordo com tais afirmativas, a proposta de um modelo para Classificação da Confiabilidade das RSSF, assumirá como $x_1, x_2,..., x_n$ os valores resultantes da aplicação

dos modelos matemáticos referentes aos fatores críticos de influência nesta proposta de classificação, apresentados posteriormente. Um sistema *Fuzzy* devidamente dotado de regras para este fim, deverá fornecer como resultado um *score* que será o grau de confiabilidade que a RSSF avaliada possui para realização de suas tarefas. Este *score* poderá ser comparado ao de outras redes e finalmente servir de parâmetro para determinar a rede com maior grau de confiabilidade.

2.1.5.1 Fusão de Dados *Fuzzy*

A lógica *Fuzzy* se difere da lógica clássica por ser baseada no raciocínio humano, buscando refletir a forma de pensar a partir da modelagem de uma resposta adequada à realidade e deferente do sim ou não aplicado pela lógica clássica (JR; CEGIELSKI, 2012). Por definição, as decisões humanas tendem a possuir várias nuances (LAUDON; LAUDON, 2010), o que torna a categorização dessas decisões imprecisa e subjetiva.

A representação *Fuzzy* do conhecimento, com impacto direto sobre a tomada de decisão, abrange principalmente situações onde as classificações qualitativas, geralmente necessárias para problemas imprecisos, são esperadas. Este tipo de classificação carrega a ideia de uma variável linguística pra representação deste modo impreciso, que por sua vez, admite valores como expressões linguísticas, também chamadas de termos primários (ALMEIDA; EVSUKOFF, 2003).

A fusão de dados é um processo derivado da associação, correlação e combinação de dados providos de fontes diferentes, a fim de se obter resultados refinados que proporcionam análise mais significativas e em tempo hábil sobre determinada entidade ou objeto (WHITE, 1991). Os autores Liggins, Hall e Llinas (2017) afirmam que com o emprego da fusão, que é a combinação de informações providas de múltiplos sensores, é possível ascender a uma inferência tal que seria impossível alcançar com a utilização de apenas um sensor.

De acordo com Anzano (1999), o processo de fusão de dados é útil principalmente porque propicia redução da redundância da informação e, dessa forma, otimiza o processamento das mesmas no procedimento de visualização. Ela também facilita a construção de banco de dados agregados e possibilitam a integração desses dados, configurando inferências que não seriam possíveis sem fusão. Para o autor, a lógica *Fuzzy* se adapta muito bem a sistemas de acompanhamento com múltiplos sensores ou entradas, mas quais várias associações podem ser realizadas com dados provenientes de cada uma delas. A base de regras (IF-THEN-ELSE), existente em sistemas *Fuzzy*, é utilizada para estabelecer tais associações.

Oliveira e Belderrain (2008) completam que " as definições de pertinência dos termos nebulosos armazenadas na base de dados definem as medidas de similaridade dos dados. Se estes valores superarem um determinado limiar (*threshold*) estabelecido, é obtida a

decisão de associação, caso contrário, a associação é evitada." Além disso, para Almeida e Evsukoff (2003), termos primários definidos formam uma estrutura de conhecimento denominada partição *Fuzzy*. A utilização dessas partições depende das propriedades sintáticas e semânticas que orientarão o comportamento do sistema *Fuzzy*. As propriedades sintáticas vão definir o formato como as informações *Fuzzy* serão armazenadas ou disseminadas.

A descrição da base de regras e as propriedades semânticas eleitas e utilizadas neste trabalho estão disponíveis para consulta respectivamente nos apêndices A e B.

2.2 Trabalhos Relacionados

Este capítulo aborda os principais trabalhos encontrados com a finalidade de classificar RSSF. Nesta seção será possível também identificar a afinidade dos trabalhos relacionados com o objetivo deste, que é salientado na seção 1.3. É interessante notar que grande parte destes trabalhos estão focados na identificação de nós maliciosos, ou seja, voltados à questão da segurança. e não primam por uma classificação geral das RSSF quanto ao envio de pacotes ou mensagens, que é o cerne deste estudo.

Yan, Zhang e Virtanen (2003) sugerem um modelo para classificação da confiança de uma rede como uma solução de segurança. É proposto o uso de uma função linear para o cálculo do grau de confiança a partir de determinada ação. Para a função, é considerada uma espécie de lista negra dos invasores. Experiências passadas, avaliação de outros nós, estatísticas, e outros fatores são fatores determinantes para a composição desta lista negra. Entretanto a influência que cada um desses fatores exerce no cálculo não é especificada. É apresentado também um protocolo de roteamento que utiliza o modelo de confiança proposto e como supostamente esse protocolo minimizaria os ataques que um protocolo de roteamento normalmente está sujeito. O foco principal são os ataques, ou seja, a questão da segurança tende a ser resolvida por meio dos modelos de confiança que conforme expresso, julgam apenas os nós da rede separadamente para classificá-la.

Apesar de oferecer ampla visão de como mensurar resultados para a definição proposta e de sugerir a segurança como fator preponderante para definição de confiabilidade, de acordo com a proposta deste trabalho, este índice não representa aspecto relevante a ser observado no momento da estimativa do grau de confiabilidade, pois uma rede não segura pode deixar de ser utilizada para a realização de medições, tornando assim a estimativa de seu grau de confiabilidade inutilizada.

Buchegger e Boudec (2003) estudam o comprometimento entre robustez e eficiência das redes móveis. Propõem um mecanismo baseado em estatística Bayesiana para discernir nós impróprios. Para o cálculo são levados em conta dados obtidos através de observação e dados obtidos através de outros nós da rede. Eles fizeram a importante descoberta de que se se utilizar dados enviados por outros nós da rede pode-se acelerar o processo de

descoberta dos nós maliciosos.

O trabalho supracitado inclui conceitos importantes para a classificação, a utilização de elementos estatísticos para definição de resultados, porém a questão da segurança ainda é muito explorada como fator determinante para a confiabilidade de uma rede, mais uma vez fugindo à proposta deste trabalho.

Liu, Joy e Thompson (2004) sugerem um modelo de confiança para redes ad hoc com base na distribuição de relatórios sobre ameaças aos demais nós interessados da rede. Desse modo, constrói-se um roteamento no qual o grau de confiança é utilizado como uma métrica adicional. Os autores propõem uma abordagem diferente para calcular o grau de confiança, porém partem do pressuposto da cooperação completa e total de todos os nós da rede, o que nem sempre pode se considerar uma verdade. Outro problema é pressupor que todos os nós da rede serão capazes de identificar comportamentos maliciosos por via de sistemas de detecção de intrusão.

O resultado deste tipo de ação seria que cada nó obtivesse a permissão de "escutar" toda a rede, o que resultaria sem dúvida em um consumo muito maior de energia por parte da rede e vai em desencontro a tudo que se espera de uma RSSF.

Virendra et al. (2005) demonstram uma arquitetura baseada em confiança que permite que os nós da rede tomem decisões sobre a formação de grupos com outros nós. O esquema proposto se baseia na avaliação feita pelo próprio nó juntamente com a recomendação de outros nós. Tal procedimento apóia-se no monitoramento dos nós a partir de um mecanismo de pergunta e resposta. Dessa forma, o nó avaliador envia uma requisição ao nó avaliado e futuramente compara essa resposta com informações obtidas durante a fase de monitoramento. Novamente nota-se a avaliação ou a classificação realizada através dos nós da rede além de ser mais um modelo baseado em segurança. Porém esse estudo fornece um limiar que pode ser transpassado para que a classificação transcenda as partes e foque no todo, ou seja, ultrapasse os limites dos nós e atinja de fato toda a RSSF.

O modelo descrito acima é compatível com a proposta deste trabalho. Dessa forma será utilizado como base para um modelo matemático e resultará em um dos aspectos a serem considerados pelo sistema *Fuzzy* que, por meio de cálculos, retornará o grau de confiabilidade da RSSF.

O trabalho de Wang et al. (2005) baseia-se na teoria da correção de erros, tolerância a falhas e fusão de dados. A classificação proposta é referente a tolerância a falhas em uma RSSF que conforme explicam, é uma das funções fundamentais de uma rede. Eles propõem uma abordagem inovadora para a classificação multiclasse distribuída. Usando uma regra de fusão tolerante a falhas para RSSF. Decisões binárias de sensores locais, possivelmente na presença de falhas, são encaminhadas ao centro de fusão que determina

o resultado da classificação final.

Embora seja uma proposta de classificação de rede, a abordagem realizada por Wang et al. (2005) sobre tolerância a falhas é muito específica para se tornar um padrão de classificação de RSSF. Este trabalho tem, por proposta, uma estimativa mais abrangente sobre o grau de confiabilidade de uma RSSF, a qual deve relacionar mais do que apenas um fator para obtenção de resultados.

Contudo, no modelo de confiabilidade proposto, as falhas serão utilizadas como fator complementar, inseridas no contexto da acurácia da rede, onde as falhas detectadas farão com que o índice de acurácia sofra variação e consequentemente influencie o resultado do grau de confiabilidade da RSSF.

Sun et al. (2006) apresentaram um *framework* capaz de medir o grau de confiança de uma rede e propagá-lo pela rede com a finalidade de transformar o roteamento em uma atividade segura além de auxiliar na detecção de intrusos. O *framework* proposto inclui um mecanismo de defesa contra possíveis nós maliciosos. Eles utilizam um modelo probabilístico que é baseado na incerteza de um vizinho executar determinada ação e apenas considera informações locais.

De acordo com a proposta dos autores, à exceção do *framework* proposto por eles, o objetivo deste trabalho é propor uma escala, que será abordada adiante, para classificar as RSSF de acordo com o grau de confiabilidade das mesmas, ante ao envio e recebimento de pacotes ou mensagens.

He, Wu e Khosla (2006) propuseram uma arquitetura de incentivo à colaboração que se baseia na reputação dos nós. Novamente são consideradas apenas informações locais para a avaliação da reputação. O objetivo é identificar e se possível excluir nós que não participam ativamente de roteamentos.

A proposta apresentada pelos autores coincide com os objetivos deste trabalho porém não tão abrangente quanto a presente proposição para o modelo de confiabilidade que será descrita posteriormente.

Theodorakopoulos e Baras (2006) analisaram a questão da inferência de grau de confiança como uma generalização do problema do menor caminho em um grafo orientado e no qual as arestas correspondem ao julgamento que um vértice possui sobre outro. Eles defendem que nós formam sua opinião em relação a outro baseada estritamente em informações locais. O julgamento que um nó faz em relação a outro inclui o grau de confiança acrescido de um valor que representa a precisão do grau de confiança. O objetivo é dotar nós com a capacidade de construir indiretamente relações de confiança com base em interações locais.

A contribuição de Theodorakopoulos e Baras (2006) para este trabalho incide na geração de graus de confiança. A partir da obtenção deste grau, a presente proposta

acrescenta uma classificação semântica deste valor, categorizando as RSSF.

Pirzada e McDonald (2006) propõem um modelo de confiança para estimar confiabilidade de rotas, podendo ser esta uma métrica a ser acrescida no cálculo de rotas. Embora essa classificação não vise segurança, ainda sim o modelo permite que seja escolhida a rota mais confiável.

A proposta de Pirzada e McDonald (2006) contribui para este trabalho à medida que demonstra não ser necessário para as estimativas de confiança o fator segurança. O que serviu de motivação para que este fator fosse, como citado anteriormente, incrementado à acurácia da rede. Ou seja, a segurança é considerada, mas de acordo com os autores, não sendo fator determinante, pôde fazer parte do modelo como um dos componentes de entrada do sistema, porém não sendo uma variável específica, como será detalhado mais adiante.

Velloso et al. (2008) acrescentam que "ataques difamatórios" passaram a existir dentro do contexto de RSSF. Esse tipo de ataque se consolida quando um nó malicioso consegue enviar informações falsas sobre a reputação de outro nó, comprometendo a acurácia de redes que utilizam modelos colaborativos de classificação. Como alternativa a este problema, eles propõem um modelo robusto de classificação com mecanismos aptos a identificar e analisar apenas recomendações de nós vizinhos que sejam confiáveis.

Assim como o modelo de (VIRENDRA et al., 2005), este modelo contribui para este trabalho inserindo conceitos de recomendações entre nós da RSSF para exercer influência no resultado de confiabilidade. Apesar de descartar outros fatores para gerar o grau de confiabilidade, reforça a tese de que modelos colaborativos podem lograr êxito para o objetivo proposto.

Mármol e Pérez (2009) defendem que modelos de confiança e reputação para sistemas distribuídos como redes P2P, RSSF, ou sistemas multiagentes adquiriram grande importância dentro da comunidade acadêmica internacional, porém nem sempre é fácil checar a acurácia dos modelos propostos para classificar confiança e reputação. Partindo desse pressuposto, eles apresentam um modelo de confiança que promete facilidade nos testes e nas comparações. O modelo proposto é uma aplicação baseada em Java chamada TRMSim-WSN (*Trust Reputation Model Simulator for WSN* - Simulador de modelos de confiabilidade e reputação para redes de sensores sem fio) que visa oferecer possibilidades de simulações e comparações entre os diversos modelos de confiabilidade propostos.

Deif e Gadallah (2014) exploram a classificação das redes pelo aspecto dos projetos. Segundo eles os métodos de implantação das RSSF se enquadram em duas categorias: Implantação planejada e distribuição aleatória. Na implantação planejada é também definida como seletiva, são eleitos os locais de implante dos sensores otimizando um ou mais objetivos da aplicação. E é neste aspecto que o modelo de classificação proposto por eles

opera. Para eles tem sido grande a quantidade de estudos que propõem algoritmos para solucionar o problema da implantação planejada. Então neste estudo eles sugerem um novo modelo de classificação dos algoritmos propostos na literatura com base em uma abordagem matemática para modelar e resolver o problema da implantação. Para isto eles utilizam quatro abordagens matemáticas distintas: algoritmos genéticos, geometria computacional, campos potenciais artificiais e otimização de enxames de partículas. Para cada uma das abordagens, eles fornecem uma discussão de seus antecedentes e da matemática envolvida, em seguida analisam os algoritmos pertencentes a cada abordagem e os comparam. A partir disso, eles classificam seu desempenho.

A contribuição destes autores para o presente trabalho se dá na inserção de modelos matemáticos para classificação. Dessa forma, a partir da modelagem matemática dos aspectos selecionados, será possível a obtenção do grau de confiabilidade de uma RSSF.

Eskola e Heikkilä (2016) enfatizam que a confiabilidade na transmissão de dados em RSSF é sempre um problema em ambientes industriais severos e que estes ambientes definem desafios específicos para a otimização de desempenho das redes. Assim sendo, eles propõem um modelo de classificação de redes de acordo com as condições de propagação dos sinais na rede.

Os autores contribuem com este trabalho à medida que enfatizam a importância da transmissão dos dados, embora abordem ambiente especificamente industrial. No presente trabalho, como já mencionado, a presença do fator acurácia na comunicação entre os nós da rede é um fator considerado para a obtenção do grau de confiabilidade visto que transmissão de dados é fator preponderante para o bom funcionamento da rede.

Kumar e Singh (2017) suscitam discussão sobre confiabilidade de uma RSSF à luz do envio e recebimento de dados, porém com enfoque voltado à segurança deste envio durante o roteamento dos pacotes, com vistas a evitarem nós maliciosos ou defeituosos de forma eficiente, isto é, com o menor consumo de energia possível.

Os autores enfatizam a importância de três dos aspectos que serão estudados para compor o modelo proposto neste trabalho: A confiabilidade da rede, o consumo de energia e a latência da rede. A contribuição resultada deste último aspecto de atraso é a definição de que a latência da rede é calculada apenas para pacotes que foram entregues. Este detalhe, além de otimizar o resultado, representa um aspecto de medição mais compatível com os demais aspectos utilizados na construção do modelo proposto.

Já Zhu et al. (2018) reafirmam, em seu trabalho sobre comunicação baseada em confiança para Internet das Coisas na indústria, a importância da confiabilidade da comunicação entre dispositivos e sistemas neste setor. Apesar do assunto confiabilidade de rede possuir períodos de picos, no tocante à quantidade e especificidade de publicações, trabalhos como este enfatizam que o tema ainda é de suma importância para a manutenção

de um ambiente consistente em termos de arquitetura para a comunicação de dispositivos dentro do ambiente da Internet das Coisas.

Conforme pôde ser observado a partir da coletânea de trabalhos relacionados ao tema deste trabalho, alguns deles fornecem um ponto de partida para os objetivos deste trabalho, outros contribuem confirmando a importância da área estudada, adotando modelos matemáticos e incluindo fatores a serem considerados na obtenção do grau de confiabilidade das RSSF.

O estudo da classificação de RSSF deixa algumas lacunas e ao mesmo tempo, aborda diversas formas diferentes de classificação. Majoritariamente encontra-se trabalhos relacionados à segurança das redes, porém é possível perceber que sem o correto envio e recebimentos dos dados, pouco adianta uma RSSF que seja totalmente blindada contra invasões. Assim, este trabalho propõe a estimação de um grau de confiança de uma rede bem como uma classificação de RSSF que avalie as condições de envio e recebimento de dados e o potencial que toda a rede tem de se manter ativa e funcionando confiavelmente, independente se um suposto nó sensor mantém baixa reputação perante seus nós vizinhos.

2.3 Modelos de Classificação de Confiança para RSSF

O conceito de Confiabilidade de RSSF permeia por diversos aspectos que exercem influência direta no funcionamento de uma rede. Por exemplo, os processos de roteamento de pacotes e dados, a identificação de um nó em relação a seu vizinho, a certeza de que um pacote enviado a um nó específico prosseguirá com sua rota até seu destino, ou seja, confiabilidade de uma RSSF se refere às garantias de que uma decisão poderá ser tomada em tempo hábil e com os dados necessários para tal, que são trafegados através desta rede (LOPEZ et al., 2010).

Diversos aspectos se encaixam neste contexto e devem ser considerados para se determinar a confiabilidade de uma rede, visto que este é um conceito extremamente amplo. Dentre a infinidade de aspectos que podem ser levados em consideração ao se definir um modelo de confiabilidade, e ao contrastar com a literatura que apresenta modelos baseados em aspectos específicos e não relacionados com outros, a proposta de classificação de confiabilidade de RSSF deste trabalho se baseia em quatro elementos a serem estudados.

Nesta seção os aspectos componentes do modelo de classificação proposto, como o modelo demonstrado por Virendra et al. (2005), a acurácia de comunicação entre nós da rede proposto por Eskola e Heikkilä (2016), a latência da RSSF abordada por Souza (2013), Cheshire (1996) e Tanenbaum (2003) e finalmente a eficiência energética de uma RSSF discutida por Akyildiz et al. (2002) serão analisados. Estes modelos servirão como base para a proposição de um modelo geral de classificação de confiança de RSSF, que é o objetivo deste trabalho e, juntamente com o sistema *Fuzzy* implementado para este

fim, contribuirão para a proposição de um novo método de estimação de confiabilidade das RSSF.

Os seguintes aspectos foram determinados basado na importância exercida por cada um e na abrangência dos mesmos, conforme identificados na literatura. A confiabilidade entre os nós sensores vizinhos é importante pois, segundo Loureiro et al. (2003),estes elementos proveem dados que serão processados ou consumidos pelo nó *sink*, isto é, a principal finalidade das RSSF. A acurácia da comunicação das RSSF está diretamente ligada ao consumo de energia, pois quanto mais pacotes forem necessários para que um dado atinja seu objetivo, maior é o consumo de energia despendido para a conclusão de sua tarefa. Despender energia demasiada para uma atividade passível de otimização, incide sobre a vida útil da rede, que não dispõe de energia infinita (SHAIKH; ZEADALLY, 2016) e (LI; LIANG, 2018). A escolha do aspecto latência se dá pela importância das decisões em alguns ambientes necessitarem reações em tempo real. Por exemplo, nos projetos de estradas inteligentes, onde o intuito é de que java comunicação instantânea entre os objetos da estrada e os automóveis que trafegam por ela (CHOWDHRY et al., 2007). O atraso na comunicação de uma RSSF destinada a este fim, pode inviabilizar uma reação importante, não justificando assim seu emprego.

2.3.1 Confiabilidade

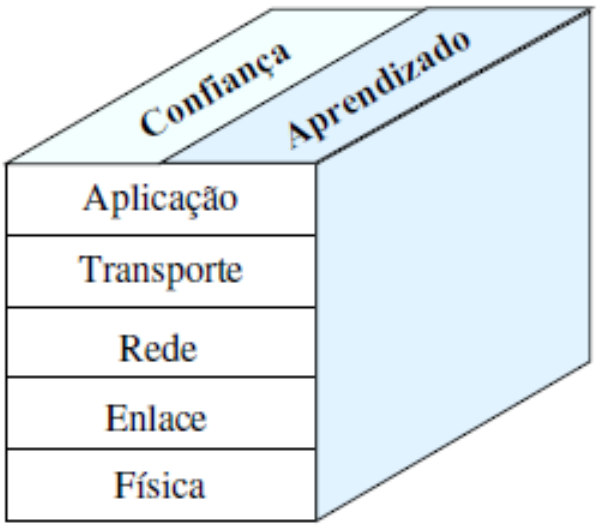
O modelo proposto por Virendra et al. (2005) tem por objetivo obter uma estimativa de confiabilidade, ou seja, um grau de confiança, para cada nó vizinho direto, partindo da coleta de dados locais e da troca de pacotes de mensagens entre os vizinhos. O modelo analisado é dividido em duas camadas: confiança e aprendizado, de acordo com a Figura 10.

A camada de confiança é responsável pelo cálculo do grau de confiança para cada vizinho direto, a partir de informações enviadas por seus vizinhos e nas informações armazenadas na camada de aprendizado. Este resultado é então enviado a todas as outras camadas, inclusive com a possibilidade de ser utilizado como métrica para protocolos e aplicações. A camada de aprendizado é responsável pelo julgamento dos nós vizinhos a partir das informações coletadas. Para que isto ocorra, é necessário que esta camada tenha acesso a todas as outras, além de monitorar os vizinhos sempre que possível. Este julgamento resulta nos dados passados para a camada de confiança (VELLOSO et al., 2006).

Todo nó da rede deve armazenar o grau de confiança de cada vizinho direto, ou seja, todos aqueles que estão em seu raio de alcance,[4] conforme esquematizado na

[4] Nós sensores se comunicam através de frequência de rádio e dessa forma tem seu alcance restrito a determinada distância que varia de acordo com as especificações da RSSF. Na Figura 11, o esquema mostra que os nós 2, 6 e 7 poderiam ser avaliados pelo nó 1, pois são seus vizinhos diretos. Os demais

Figura 10 – Arquitetura do modelo de classificação proposto por Virendra et al.2005

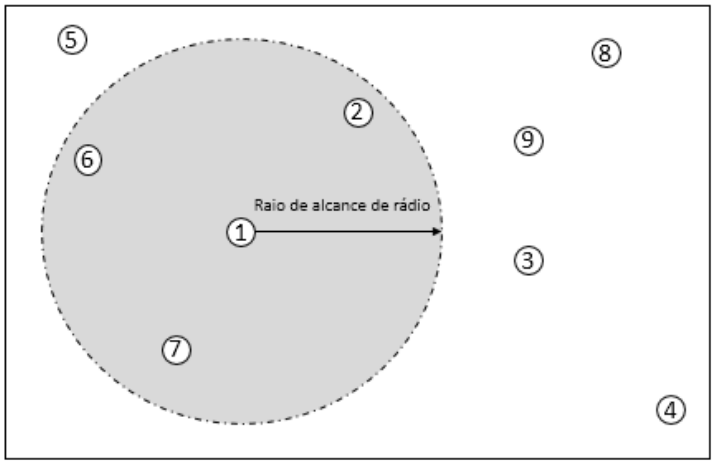


Fonte: (VELLOSO et al., 2006)

Figura 11. Este valor é atualizado periodicamente. Neste processo, os nós sensores da rede são inteiramente responsáveis pelos seus próprios processos de avaliação do grau de confiança.

Existe a premissa de que a recomendação dada por nós vizinhos da rede seja considerada no cálculo de confiança, e neste caso, uma recomendação é composta pelo parâmetro chamado grau de maturidade da relação entre os nós, pelo o grau de confiança e por sua precisão.

Figura 11 – Raio de alcance de rádio de um nó sensor



O grau de confiança é um valor contínuo que varia dentro do intervalo fechado [0,1]. O grau de maturidade do relacionamento, introduzido neste modelo por Velloso et al. (2006),

nós, como estão fora do alcance de comunicação do nó 1, não serão avaliados por ele de acordo com o modelo analisado.

considera a duração do relacionamento entre dois nós. A introdução deste conceito permite aos nós priorizarem as recomendações com base no tempo de relação de confiança que os nós estabelecem, de forma que os relacionamentos mais longos adquirem peso maior na sua recomendação. Para que isto seja possível, os nós devem utilizar um protocolo de troca de recomendações denominado por Velloso et al. (2006) como *Recommendation Exchange Protocol* (REP). Para efeitos de confiança do modelo, considera-se que todos os nós da rede possuam algum mecanismo de autenticação para garantir as mínimas condições de segurança ao sistema.

O cálculo do grau da confiança é realizado quando um nó encontra um novo vizinho na rede. Neste momento, um grau de confiança deve ser atribuído a este novo nó. O primeiro grau de confiança atribuído dependerá exclusivamente das condições da rede, da mobilidade e do estado atual do nó que vai atribuir a primeira avaliação. Na sequência, o nó inicia seu processo de cálculo do grau de confiança, que começa com uma solicitação de recomendações para os vizinhos diretos e o monitoramento e avaliação do comportamento do novo vizinho.

Como base no modelo demonstrado na seção 2.1.4, o grau de confiança de um nó a em um vizinho *b* ou $(T_a(b))$ é definido como a soma da própria confiança do nó a adquirida com a contribuição dos nós vizinhos conforme descrito em (1).

$Q_a(b)$ representa a capacidade de um nó tem, com base em suas próprias informações, de avaliar o grau de confiança, enquanto $C_a(b)$ representa a contribuição dos vizinhos. No mesmo contexto, α serve para ponderar o fator mais relevante entre a contribuição dos vizinhos e as informações locais fornecidas pela camada de aprendizado.

A capacidade que um nó tem de avaliar o grau de confiança baseado nas informações próprias é dada por:

$$Q_a(b) = \beta E_T + (1 - \beta) T_a^*(b), \tag{2}$$

na qual E_T representa um valor de grau de confiança adquirido com o julgamento do próprio nó *a* a respeito do comportamento do seu vizinho *b*. A camada de aprendizado (Figura 10) fornece essa informação. $T_a^*(b)$ é o valor do grau de confiança atribuído anteriormente. O parâmetro β, assim como αprioriza relevância, porém neste caso o termo mais relevante, podendo estes dois parâmetros variar de acordo com o evento, garantindo a atualização do grau de confiança.

$C_a(b)$ é o conjunto das recomendações de todos os nós *i* pertencentes ao conjunto K_a , que por sua vez representa vizinhos comuns entre os nós *a* e *b*. Essas recomendações denominadas $X_i(b)$ são ponderadas pelo grau de confiança do nó *a* sobre o nó *i* $(T_a(i))$

conforme a Equação 3.

$$C_a(b) = \frac{\sum_{i \in K_a} T_a(i) M_i(b) X_i(b)}{\sum_{j \in K_a} T_a(j) \sum_{j \in K_a} M_i(b)}. \tag{3}$$

A relevância da recomendação de nó $(T_i(b))$ tem relação com a seleção de K_a. Dessa forma, há uma relação diretamente proporcional entre K_a e a recomendação dos nós vizinhos. A recomendação inclui também a maturidade da relação. Essa medida $(M_i(b))$ é apresentada em segundos por uma variável contínua, enquanto $X_i(b)$ é uma variável aleatória de distribuição normal dada por:

$$X_i(b) = N(T_i(b), \sigma_i(b)) \tag{4}$$

Aqui σ representa a precisão e se define como o desvio padrão. Ou seja, todo valor da tabela do grau de confiança do nó *i* $(T_i(b))$ está associado a um desvio padrão $(\sigma_i(b))$, que faz referência à variação do grau de confiança que o nó *i* obteve. A partir daí, uma nova atualização do grau de confiança do nó *i* sobre *b* é realizada. O nó *i* então atualiza o valor de $(\sigma_i(b))$ de acordo com:

$$\sigma_i(b) = \sqrt{\frac{\sum_{j=1}^{k} (\overline{S}_k - S_j)^2}{k-1}}, \tag{5}$$

na qual $\overline{S}_k$ significa o conjunto das K últimas amostras de grau de confiança sobre o nó b, $K \in \mathbb{N} | 2 \leq K \leq 10$. $\overline{S}_k$ é o valor médio. O parâmetro σ denota a confiabilidade da medida do grau de confiança. Um valor alto para σ pode representar dificuldade do nó em avaliar o grau de confiança ou até mesmo uma instabilidade no comportamento do nó que está sendo avaliado.

$M_i(b)$, por fim, significa que quanto maior o tempo que os nós se conhecem, maior será a relevância de sua opinião para a formação do valor final de confiabilidade. Este parâmetro é a maior contribuição realizada por Velloso et al. (2006) ao modelo de Virendra et al. (2005). A fim de evitar que nós maliciosos possam interferir na rede de forma a forjar altos resultados de maturidade e obterem privilégios em indicações mal intencionadas, cada nó deve definir um limiar para o valor da maturidade da relação de forma que a maturidade seja baseada em valores médios e passe a ser expressa por:

$$M_i(b) = \begin{cases} M_i(b), & \textbf{if} M_i(b) < M_{max}; \\ M_{max}, & \textbf{if} M_i(b) \geq M_{max}. \end{cases} \tag{6}$$

2.3.2 Acurácia

Para compor o modelo geral de classificação quanto à confiabilidade das RSSF proposto neste trabalho, é necessário que sejam levados em conta aspectos individuais, que combinados incidirão no *score* de classificação geral. Essa combinação é fundamental para uma avaliação de qualidade, visto que a confiabilidade da transmissão de dados em RSSF é sempre um problema (ESKOLA; HEIKKILÄ, 2016). Dessa forma, a acurácia da comunicação entre os nós de uma rede é de suma importância para a avaliação da confiabilidade da mesma.

Esta avaliação identifica o percentual dos pacotes enviados e que foram recebidos em determinada RSSF. Este percentual será usado para a composição do modelo matemático-computacional que será detalhado ao final deste capítulo.

2.3.3 Latência

A latência de uma RSSF pode ser considerada como o tempo necessário para o envio e recebimento de dados, sendo dessa forma um parâmetro de grande importância (SOUZA, 2013). Em outras palavras, temos que latência equivale a atraso (CHESHIRE, 1996) das transmissões de dados e em uma RSSF, e portanto ela representa o somatório dos atrasos impostos por toda a rede durante seu funcionamento, e sua existência se dá pela combinação de diversos fatores como: capacidade de processamento do nó, disponibilidade de memória, mecanismos de *cache*, processamento nas camadas de nível superior, etc.

Segundo Tanenbaum (2003), em redes não triviais, como é o caso das RSSF, a latência mínima é a soma da latência mínima de cada nó da rede, mais o atraso de transmissão de cada nó com exceção do último, mais a latência de passagem adiante de cada roteador.

Uma vez não sendo necessários tantos aspectos para o cálculo da latência com as finalidades apresentadas neste trabalho, o cálculo da latência de uma RSSF pode ser obtido pela equação 7 quando Tr e Te assumem todos os fatores citados simplificando-os em função do tempo de resposta de cada nó:

$$L = Tr - Te, \tag{7}$$

na qual Tr é o tempo de resposta e Te é o tempo de envio do pacote de dados.

2.3.4 Eficiência Energética

A longevidade de um nó depende da quantidade de energia restante para seu funcionamento. Como consequência, toda a vida útil de uma RSSF está relacionada ao consumo energético de seus nós (AKYILDIZ et al., 2002). Do mesmo modo, a confiabilidade

de uma RSSF depende intrinsecamente da vida útil da mesma. Ou seja, uma RSSF só poderá ser considerada confiável para a realização de determinada tarefa, se houver garantias de que ela não sucumbirá aos problemas de cunho energético. Para uma boa classificação, é necessário que haja uma previsão de que haverá energia disponível para toda a rede até o término da medição e envio dos dados coletados, onde quer que a rede esteja instalada.

Pode-se observar então que este parâmetro tem como característica a volatilidade, visto que determinada tarefa atribuída a uma RSSF pode consumir mais ou menos energia. Com o intuito de alcançar uma classificação de confiabilidade da rede, será adicionado a este modelo um outro componente, proposto por Akyildiz et al. (2002), que considera dois fatores relevantes para o cálculo de consumo energético de uma RSSF, sendo eles comunicação e processamento de dados, cada qual com seu cálculo específico.

Para o consumo de energia (Pc) durante o processo de comunicação do nó, o valor, de acordo com Shih et al. (2001) e Akyildiz et al. (2002), é obtido por:

$$Pc = N_T[P_T(T_{on} + T_{st}) + P_{out}(T_{on})] + N_R[P_R(R_{on} + R_{st})], \tag{8}$$

na qual P_T e P_R são a energia consumida pelo transmissor/receptor; P_{out} a energia de saída do transmissor; T_{on} e R_{on} o transmissor e receptor no tempo; T_{st} e R_{st} o tempo de inicialização do transmissor/receptor; N_T e N_R número de vezes que o transmissor/receptor é ligado por unidade de tempo, que depende do controle de acesso da tarefa; T_{on} é a razão entre L/R onde L é o tamanho do pacote e R a taxa de dados.

Já para a obtenção do consumo referente ao processamento de dados (P_p), Akyildiz et al. (2002) apresentam a seguinte formulação:

$$P_p = CV_{dd}^2 f + V_{dd} I_0 e^{V_{dd}/n'V_T}, \tag{9}$$

na qual C é a capacitância de comutação total; V_{dd}, o balanço de tensão e f, a frequência de comutação. O segundo termo denota a perda de energia devido a correntes de vazamento. Para Shih et al. (2001), a redução da tensão de limiar para satisfazer os requisitos de desempenho resulta em correntes de vazamento sub-limiar altas. Este fator, em conjunto com a baixa operação do ciclo de trabalho do microprocessador do nó sensor, pode resultar em uma perda de energia significativa.

2.3.5 Discussões Finais

Conforme apresentado, existe grande número de trabalhos sobre classificação de RSSF. Estes estudos divergem principalmente sobre aspectos estudados a fim de apontar a confiabilidade de uma rede. A complexidade do tema abordado corrobora com a ausência de consenso sobre uma definição de quais aspectos são mais relevantes no momento da definição da classificação da rede.

A partir dos trabalhos referenciados, constatou-se as principais variáveis para a estimativa do grau de confiança das RSSF, a saber: o grau de confiabilidade dos nós de uma rede, a acurácia no envio dos pacotes, o atraso no processo de comunicação da rede e finalmente a eficiência no consumo de energia. O referencial apresentado serviu para delimitar o escopo do trabalho, uma vez que foi possível perceber todas as possibilidades existentes e válidas para se classificar uma RSSF. Os trabalhos apresentados foram essenciais, tanto na escolha das variáveis a serem estudadas neste trabalho, quanto para demonstrar a abrangência e complexidade do tema em questão. Dessa forma, os modelos eleitos e apresentados, serão, de acordo com os objetivos deste estudo, adaptados e transformados em variáveis de entrada de um sistema que fornecerá estimativa do grau de confiabilidade de RSSF arbitrárias.

A quantidade de trabalhos sobre RSSF, existente atualmente, coopera com a ideia de que este ainda é, indubitavelmente um tema de considerável relevância tecnológica, sobretudo inserido no contexto da Internet das Coisas, que é um conceito que ainda se encontra longe de ser totalmente explorado e aponta novos avanços a todo instante.

Os demais capítulos enfatizarão metodologia e proposta de um novo modelo de estimativa de confiabilidade de RSSF que nasce a partir da adaptação dos modelos dos aspectos apresentados ao escopo deste trabalho e se aperfeiçoa com o emprego de um sistema de lógica *Fuzzy* que condensará todas as entradas e retornará o grau estimado conforme se discutirá em detalhes no próximo capítulo.

3 Metodologia

Silva e Menezes (2005 apud GIL, 1999) afirmam que a investigação científica depende de um conjunto de procedimentos intelectuais e técnicos para que seus objetivos sejam alcançados e definem método científico como conjunto de processos ou operações mentais que se deve empregar na investigação. Para Gil (1999), Lakatos e Marconi (1993) os métodos que fornecem as bases lógicas para investigação são: dedutivo, indutivo, hipotético-dedutivo, dialético e fenomenológico.

Este trabalho pauta-se no método hipotético dedutivo pois se insere na seguinte linha de raciocínio:

> Quando os conhecimentos disponíveis sobre determinado assunto são insuficientes para a explicação de um fenômeno, surge o problema. Para tentar explicar as dificuldades expressas no problema, são formuladas conjecturas ou hipóteses. Das hipóteses formuladas, deduzem-se consequências que deverão ser testadas ou falseadas. Falsear significa tornar falsas as consequências deduzidas das hipóteses. Enquanto no método dedutivo se procura a todo custo confirmar a hipótese, no método hipotético-dedutivo, ao contrário, procuram-se evidências empíricas para derrubá-la (GIL, 1999)

A metodologia por sua vez é o estudo dos métodos e especialmente dos métodos da ciência, enquanto método é o modo de proceder, a maneira de agir, o meio propriamente. Assim, metodologia é a ciência integrada dos métodos. Dessa forma, este capítulo apresenta seu conteúdo em duas seções. A primeira delas dedicada à hipótese explorada neste trabalho e a segunda, ao planejamento dos experimentos que serão realizados ao longo da pesquisa.

A metodologia aplicada neste trabalho torna-se melhor compreendida a partir do fluxograma apresentado na Figura 12.

Figura 12 – Metodologia



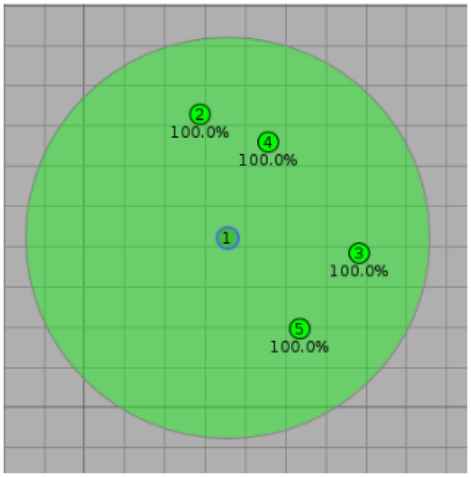
No primeiro momento, realizou-se um levantamento bibliográfico dos trabalhos referentes a modelos de Classificação de RSSF. A partir disso foram elencados, de acordo com a proposta deste trabalho, alguns modelos matemáticos que pudessem representar aspectos importantes para a classificação das redes quanto ao envio e recebimento de mensagens.

Os modelos propostos por Virendra et al. (2005), Velloso et al. (2006), Eskola e Heikkilä (2016), Tanenbaum (2003) e Akyildiz et al. (2002) foram adaptados de acordo com a finalidade da classificação proposta neste trabalho. Em seguida, cálculos foram realizados para confirmar a factibilidade da execução de uma classificação quanto ao grau de confiabilidade das redes a partir da combinação dos quatro fatores contemplados pelos modelos matemáticos citados acima. Como o modelo de Virenda et al. e de Velloso et al. visam classificar apenas os nós da rede, oferecendo resultados matriciais para a confiança da rede, o modelo foi adaptado, a fim de que, como saída houvesse um resultado que representasse a confiança de toda a rede. Em outras palavras, o objetivo desta etapa era que fosse possível desenvolver um modelo matemático, derivado destes, que representasse melhor a nota de confiança de toda a rede, de forma que se obtivesse uma única saída. Esta saída, de igual modo obtida dos demais modelos, de acurácia, latência e eficiência energética compõem a entrada do sistema *Fuzzy* que, mais tarde, foi projetado para oferecer

o grau de confiabilidade da RSSF quanto ao envio de mensagens.

No segundo momento, com os modelos matemáticos programados e organizados em funções, foi construída, no ambiente de simulação de RSSF denominado Cooja[1], dentro do emulador de redes Contiki,[2] uma RSSF com 5 nós sensores, conforme Figura 13.

Figura 13 – RSSF criada para simulação e raio de comunicação do nó sensor ID1



Os nós são identificados pelo mote ID, que é o número de identificação de cada nó na rede. A área destacada na figura, representa o raio de alcance de comunicação do nó 1. Conforme apresentado, o nó 1 é vizinho direto de todos os nós da rede. Já o nó 5, por exemplo, não tem o nó 2 como seu vizinho direto, embora figurem a mesma rede (Figura 14).

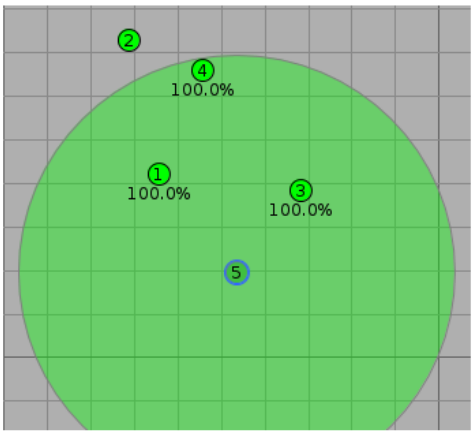
Com a rede em funcionamento dentro do ambiente de simulação citado, foram coletados dados que foram submetidos à aplicação dos modelos propostos nas seções referentes à confiabilidade 4.1, a acurácia da RSSF 4.2, a latência da rede 4.3 e por ultimo a eficiência energética 4.4, para obtenção das entradas do sistema *Fuzzy* que determinará o grau de confiabilidade da RSSF, que é a proposta deste trabalho.

A fim de verificar o modelo em funcionamento, bem como sua capacidade dinâmica dentre diversas possibilidades, foram apresentados os resultados dos experimentos listados na seção de Planejamento de Experimentos. Os dados referentes à estimativa de confiabilidade proposta neste estudo foram os resultados da aplicação dos valores normalizados obtidos por todos os aspectos estudados e inseridos no sistema *Fuzzy* preparado para este

[1] Cooja é um simulador baseado em Java, que foi projetado para redes de sensores sem fio e é executado no sistema operacional Contiki. O Cooja simula rede de nós sensores, onde cada nó pode ser de um tipo diferente, diferindo tanto no software quanto no hardware. Muitas partes do simulador podem ser facilmente substituídas ou estendidas com novas funcionalidades. Exemplos de partes que podem ser estendidas incluindo na simulação meio rádio, hardware nó simulado, e plugins para simulação de entrada e saída.

[2] Contiki é um sistema operacional de código aberto que conecta micro controladores de baixa potência à internet e que apoia plenamente o padrão IPv6 e IPv4 e os últimos padrões wireless de baixo consumo: 6LoWPAN , RPL, COAP. Contiki é executado em uma grande quantidade de dispositivos sem fio de baixa potência

Figura 14 – Raio de comunicação do nó sensor ID5



fim. A medição do modelo proposto obedeceu aos intervalos de dois minutos propostos para a coleta de dados dos aspectos componentes do modelo, a fim de que proporcionasse melhor comparação acerca dos dados e possibilitasse a avaliação do modelo frente aos outros modelos estudados. Nesta seção cada experimento foi abordado separadamente. Em seguida foram tratadas as hipóteses levantadas no capítulo 3.1.

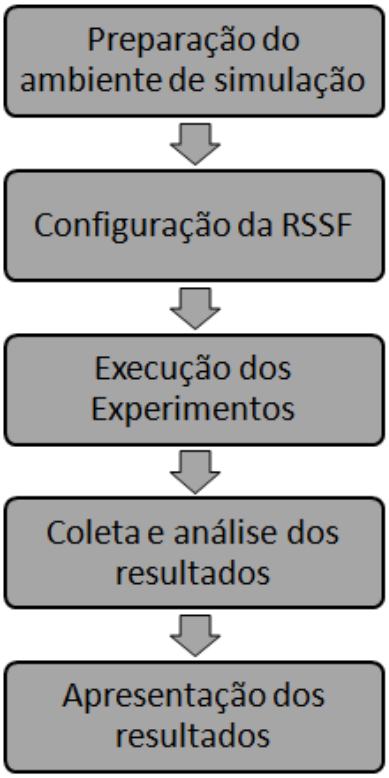
Com a rede configurada para os testes e em funcionamento, o segundo experimento consistiu em aplicar os modelos resultantes da primeira etapa destes experimentos aos valores adquiridos da RSSF. O próximo passo foi repetir a simulação dessa rede e aplicar os modelos aos demais resultados encontrados, para obter o *score* de classificação. Simulações representaram diversas características e situações diferentes, a fim de comprovar a eficácia da interação dos modelos propostos juntamente com o sistema configurado para este fim e checar a coerência das respostas obtidas em diversas situações.

O próximo passo experimental foi a condensação dos *scores* gerados a partir dos modelos na primeira fase dos experimentos referentes confiabilidade dos nós ativos da rede, a acurácia de comunicação ente nós, eficiência energética e latência, dentro do Sistema *Fuzzy* configurado para classificar as RSSF, que a partir destes valores, retornou o grau de confiabilidade da RSSF em uma escala de 0 a 1. Todos os valores obtidos para todas as variáveis estudadas tiveram os valores normalizados, a partir dos valores mínimo e máximo possíveis, resultante da aplicação dos modelos apresentados no próximo capítulo. O objetivo desta fase foi demonstrar abrangência, o comportamento do modelo de classificação e a diversidade de elementos que foram avaliados antes de compor o valor que cada rede obteve a partir da aplicação do sistema de classificação proposto neste trabalho.

Por fim, testes subsequentes foram executados em ambiente simulado que permitiram comprovar a sensibilidade no modelo proposto às diversas situações às quais RSSFs são expostas no cotidiano. Feito isto, pretendeu-se comprovar também a eficiência e a eficácia do modelo de classificação de RSSF proposto. A última fase consistiu na coleta, organização e análise destes resultados.

Os passos descritos nesta sessão, obedecem ao fluxograma da Figura 15.

Figura 15 – Sequência de atividades



3.1 Hipóteses

Hipótese é uma teoria não testada mas provável. Para o presente projeto de pesquisa foram formuladas as seguintes hipóteses:

- **A classificação quanto ao grau de confiabilidade determina o funcionamento de uma RSSF.**

- **O grau de confiabilidade de uma RSSF esta diretamente relacionada com a aptidão à utilização da mesma.**

Estas hipóteses deverão apresentar indícios de sua comprovação a partir da execução dos primeiros experimentos. Os resultados destes experimentos estarão dispostos na seção 5.

3.2 Planejamento de Experimentos

Nesta seção é apresentada uma breve descrição de como foi conduzido o processo de experimentação deste trabalho a fim de avaliar as hipóteses formuladas acima.

Uma RSSF constituída de 5 nós sensores, sendo um nó *sink* que recebe as informações e as disponibiliza para o observador, outros quatro nós executando as devidas medições, foram simulados e tiveram seus resultados analisados em espaço de tempo de 10 minutos de funcionamento. Os dados para análise foram recolhidos de 2 em 2 minutos e para fins de obtenção de resultados com variação nas condições ao longo do período de funcionamento da RSSF, de maneira a se aproximar mais das condições adversas existentes no mundo real, à exceção dos três últimos experimentos que tem objetivos diferentes e explanados adiante. Os dados para análise são resultante da média de dez medições para cada um dos planejamentos. Os experimentos consistiram efetivamente em checar se os resultados do modelo apresentados neste trabalho fizeram jus àquilo que foi proposto, que é avaliar e classificar uma RSSF de acordo com sua confiabilidade. Dessa forma, os cinco primeiros experimentos foram realizados a fim de demonstrar a eficácia do modelo de acordo com os quatro aspectos escolhidos para compô-lo. Esperou-se com isto que o modelo reagisse tão logo os resultados do simulador fossem obtidos, de modo a proporcionar uma aferição contínua e em tempo real das condições da rede. Os demais experimentos visaram validar o modelo quanto sua coerência, abrangendo índices mínimos, médios e máximos dos aspectos estudados e observando as respostas fornecidas pelo modelo proposto. Os experimentos foram definidos da seguinte forma:

3.2.1 Planejamento de Experimento 1

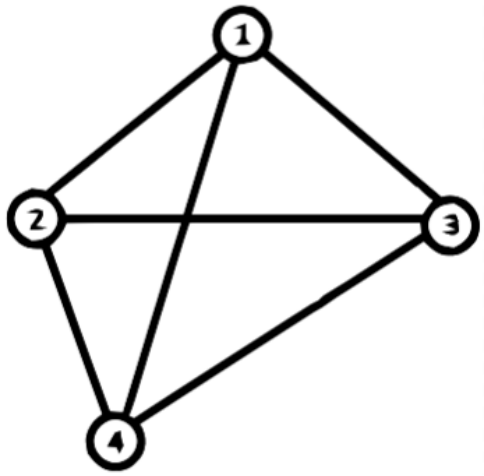
O experimento 1 consistiu na coleta de dados da simulação da rede ao longo do tempo estipulado (10 minutos). Esse experimento teve o objetivo de verificar a sensibilidade do modelo proposto exclusivamente com relação à eficiência energética, ou seja, consumo eficiente de energia, a partir de simulação de uma RSSF funcionando em seu estado ótimo, e outra simulação considerando problemas de ordem aleatória que em tese afetariam no desempenho da RSSF. O comportamento do modelo proposto nesse tipo de situação era atestar sua eficiência em termos do conjunto de aspectos avaliados, conferindo a este modelo uma recomendação para uso em redes reais.

3.2.2 Planejamento de Experimento 2

O segundo experimento teve por objetivo analisar como a acurácia da rede se comporta no momento de uma adversidade, no caso, o desligamento inesperado ou perda de um nó da rede de forma abrupta (Nó 5 no minuto 2) conforme grafo da Figura 16. Foi

realizada uma comparação do resultado do modelo proposto, que sempre atua com quatro parâmetros, com o conceito de acurácia apresentado por Eskola e Heikkilä (2016).

Figura 16 – Grafo da rede simulada do experimento 2 após a perda do nó 5



3.2.3 Planejamento de Experimento 3

A RSSF foi simulada inicialmente com todos os nós vizinhos e em pleno funcionamento. No minuto 3 da simulação a RSSF perdeu um de seus nós (nó 3) e prosseguiu seu funcionamento com 4 nós até o tempo de 6 minutos, onde perdeu outro nó (nó 4). Os grafos das Figuras 17,18 e 19 ilustram a comunicação da rede nos três momentos distintos. O objetivo deste experimento foi demonstrar o funcionamento do modelo de estimação de confiabilidade frente a situações adversas que podem ocorrer no dia a dia de uma RSSF, além de comparar o comportamento da latência da rede, um dos aspectos relevantes do modelo proposto de forma isolada com o resultado da estimativa de confiabilidade da RSSF resultante da inserção de todas as variáveis no sistema *Fuzzy*.

Figura 17 – Grafo da rede simulada no início do experimento 3

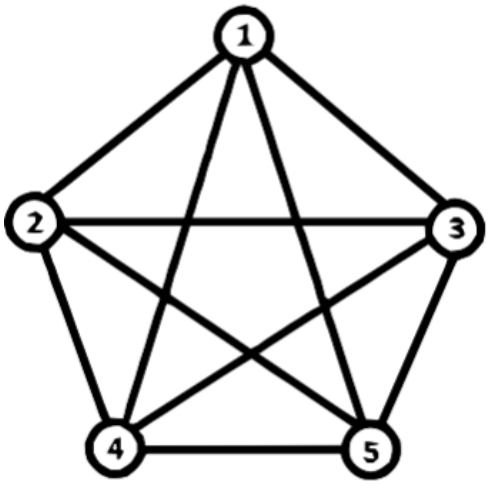


Figura 18 – Grafo da rede simulada do experimento 3 após a perda do nó 3

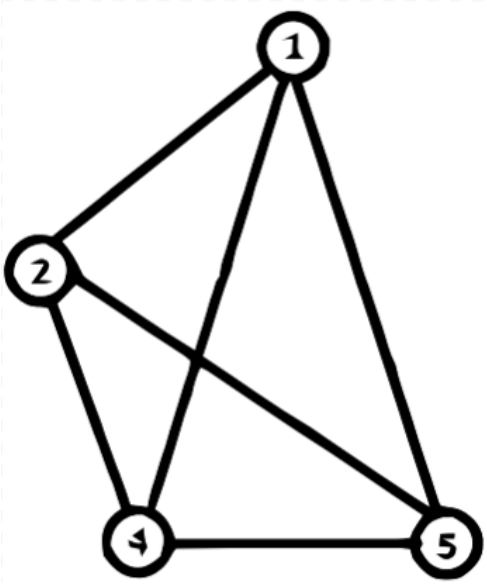
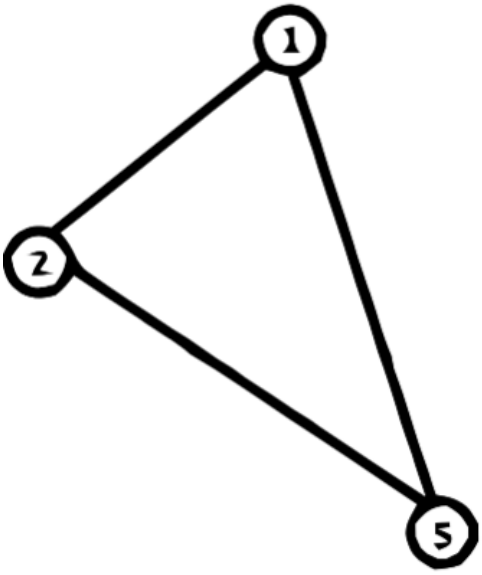


Figura 19 – Grafo da rede simulada do experimento 3 após a perda do nó 4



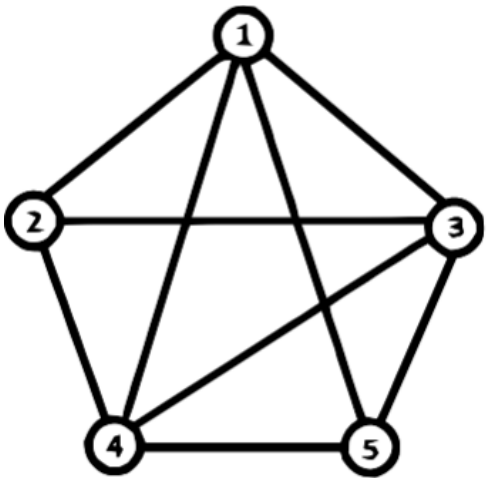
3.2.4 Planejamento de Experimento 4

Este experimento teve por finalidade comparar os resultados do modelo proposto com o aspecto de latência da rede em uma situação onde houvesse falha na comunicação de um dos nós da rede durante um período da simulação, retornando ao seu funcionamento três minutos depois (pausa no minuto 3 e retorno no minuto 6). Sendo a comunicação no primeiro momento do experimento de acordo com o grafo da Figura 17 e no período adverso, conforme a Figura 16, retornando ao estado inicial na sequência. O objetivo foi verificar a sensibilidade do modelo frente a eventuais falhas que possam ocorrer no momento em que uma RSSF esteja exposta no ambiente, e dessa forma sujeita a este tipo de situação.

3.2.5 Planejamento de Experimento 5

Este experimento teve objetivo de demonstrar a sensibilidade do modelo de estimação de confiabilidade proposto frente aos aspectos que o compõem de maneira independente. A RSSF montada para a avaliação, contém 5 nós, dentre os quais à exceção nós 5 e 2 todos os demais são vizinhos conforme grafo apresentado na Figura 20. A Figura 14 demonstra o raio de comunicação do nó 5.

Figura 20 – Grafo da rede simulada no experimento 1



3.2.6 Planejamento de Experimento 6

Este experimento visou demonstrar a possibilidade de funcionamento de uma RSSF mediante ao seu pior caso, ou seja, dotada de condições extremamente adversas. Este experimento visou demonstrar a eficácia do modelo de estimação de classificação de RSSF proposto neste trabalho, também em situações onde se faça necessária intervenção humana para que a rede retome seu funcionamento pleno. Isto é, este experimento demonstra a reação do modelo em situações onde as condições de funcionamento de uma RSSF são insuficientes.

3.2.7 Planejamento de Experimento 7

Este experimento se propôs a demonstrar o grau de confiabilidade em uma rede com dados médios manipulados. O objetivo foi demonstrar a dinâmica do modelo proposto, afim de validá-lo em todas as possibilidades de uso de uma rede no mundo real.

3.2.8 Planejamento de Experimento 8

Do mesmo modo do experimento anterior, este tratou de uma rede com os níveis mais altos de confiabilidade em todos os aspectos. Os dados de entrada dos experimentos 6, 7 e 8 estão apresentados na etapa de análise dos resultados.

Os experimentos 6, 7 e 8 visaram demonstrar a sensibilidade do modelo nas situações mais diversas, extremas e média, de uma RSSF, comprovando assim a eficiência do modelo em estimar o grau de confiabilidade de uma RSSF, que é a proposta deste trabalho. O grafo da rede destes experimentos correspondem à Figura 17.

4 Modelagem

4.1 Modelo de Confiabilidade de RSSF (μ)

O modelo de confiabilidade de RSSF, proposto neste trabalho, está representado na Equação 10. Este modelo apresenta em um tempo *t* o somatório do grau de confiança de cada nó da rede sobre a quantidade de nós ativos da rede. Uma vez que se considerassem todos os nós, a classificação não lograria êxito, visto que redes portadoras de nós inativos poderiam adquirir o *score* máximo de confiabilidade, o que seria uma inverdade. Outra necessidade para adaptação se dá pela forma como o resultado é apresentado. No modelo proposto por Virendra et al. (2005) o resultado de confiabilidade da RSSF é dado na forma matricial, uma vez que a avaliação de confiança é feita por cada nó da rede em relação a seus vizinhos. O resultado obtido pela equação 7 condensa em um tempo *t* o valor necessário para a aplicação do modelo de estimativa proposto neste trabalho.

$$\mu(t) = \frac{1}{N} \sum_{i=1}^{N_a} T_i(t), \tag{10}$$

na qual N_a representa os nós ativos na rede; N representa a quantidade de nós da rede; $T_c(t)$ representa o grau de confiança total de um nó da rede em um tempo específico. Este índice é o conhecido pelo somatório da aplicação do modelo proposto por Virendra et al. (2005) frente a todos os seus nós vizinhos.

O resultado da aplicação do modelo proposto apresenta *scores* dentro do intervalo de 0 a 1, que servirão como a classificação das RSSF quanto a sua confiabilidade. Em aplicações práticas o modelo proposto neste trabalho transforma os dados de confiabilidade dos nós da rede, obtidos a partir do modelo proposto por Virendra et al. (2005) e adaptado por Velloso et al. (2006), em informação quanto a confiabilidade de uma RSSF e que posteriormente pode ser comparada com outras redes dentro do mesmo padrão de medidas.

Neste modelo, o grau de confiabilidade obtido varia dentro do intervalo [0,1], onde, quanto mais os valores obtidos se aproximam de zero, menor é o grau de confiabilidade da RSSF. Ou seja, maior a probabilidade de que um dado enviado não seja entregue. Este fato ocasionará na tentativa de reenvio do pacote, impactando no tempo total de comunicação, no consumo de energia e também na acurácia da rede.

4.2 Modelo de Acurácia de comunicação entre nós da RSSF (α)

O modelo de acurácia de RSSF utilizado neste trabalho está representado na equação 11, tendo em vista que a acurácia depende exclusivamente da quantidade de pacotes enviados e recebidos pela rede, conforme mencionado no capítulo 2 deste trabalho. Para fins de composição do modelo, o cálculo da acurácia da RSSF é dado por α, sendo:

$$\alpha = \sum_{i=1}^{n} \frac{100 P_r(i)}{P_e(i)} \tag{11}$$

na qual P_e representa a quantidade de pacotes de dados enviados; P_r representa a quantidade de pacotes de dados recebidos.

A acurácia é importante na composição do modelo de estimativa de confiabilidade de RSSF proposto, pois indica, em conjunto com a confiabilidade da rede em relação a seus nós, a eficácia da comunicação dentro da rede. Qual é a probabilidade de um pacote ser endereçado a um nó específico, no momento do cálculo das rotas, e alcançar este nó utilizando apenas a quantidade de envios necessários para que a informação saia do ponto A e alcance o ponto B dentro da RSSF. Índices de acurácia são de suma importância para a confecção do grau de confiabilidade da RSSF.

4.3 Modelo de Latência da RSSF (λ)

A latência é composta pelo atraso da comunicação, ou seja, a diferença entre o tempo de recebimento e o tempo de envio das mensagens na rede, todas as vezes que um pacote for recebido, conforme equação 12.

$$L = T_r - T_e \ \forall \ T_r \neq 0. \tag{12}$$

Assim a obtenção da latência(λ) de toda rede é dada pelo somatório de todos os atrasos registrados em cada nó da rede. Ou seja, aplicando a equação 7 para aferir o tempo gasto na comunicação de cada nó da rede em relação aos demais, atribuindo o valor zero aos nós não participantes e excetuando quaisquer valores resultantes da relação de comunicação de cada nó com ele mesmo, a partir da restrição $i \neq j$ conforme apresentado na equação 13:

$$\lambda = \sum_{i=1}^{n} \sum_{j=1}^{n} Tr_{(j)} - Te_{(i)} \ \forall \ i \neq j, \tag{13}$$

na qual n representa a quantidade de nós da rede; i representa o índice do nó emissor do pacote; j representa o índice dos nós receptores do pacote enviado.

O atraso na comunicação é o único dos aspectos observados na composição do modelo de estimativa de confiabilidade da RSSF dotado de grandeza inversamente proporcional ao resultado esperado. Ou seja, Quanto maior a latência, ou o atraso, pior é para o modelo em termos de confiabilidade da RSSF.

A comunicação entre os nós da rede não se dá instantaneamente, entretanto, um período muito longo de espera, tende a prejudicar a comunicação entre dois nós e consequentemente da rede como um todo. O resultado do aspecto latência, que comporá o modelo será normalizado entre o menor valor possível de medição entre o envio e o recebimento de dados, e o maior tempo de espera observado no momento das simulações.

4.4 Modelo de Eficiência Energética da RSSF (β)

A partir dos dados obtidos pela rede em ambiente simulado, o cálculo adotado para a contribuição do aspecto do consumo energético ao modelo proposto se distancia um pouco do modelo demonstrado como base no capítulo 2, em virtude do formato de resposta que mais se adaptou aos demais aspectos, além das variáveis disponibilizadas no ambiente simulado que permitiram com que o cálculo de consumo energético fosse realizado de acordo com a seguinte representação:

$$Consumo = \frac{ValorEnergtico \times Corrente \times Voltagem}{RTIMERSECOND \times Runtime}. \tag{14}$$

Entretanto, para fins de classificação, alguns fatores serão condensados para compor o modelo proposto neste trabalho, de modo que apenas o resultado final do consumo de energia seja suficiente para a composição da classificação da RSSF. Assim, o parâmetro a ser utilizado neste trabalho será resultante do somatório do consumo de energia de todos os nós da rede. O consumo de cada nó da rede é representado pela equação acima. O parâmetro componente do modelo de classificação da RSSF será representado pelo consumo de energia total (β) da rede e será obtido pelo somatório abaixo:

$$\beta = \sum_{i=1}^{n} Consumo(i), \tag{15}$$

na qual n é o total de nós da rede e i é o índice dos nós de modo a garantir que todos os nós sejam avaliados e seu consumo computado.

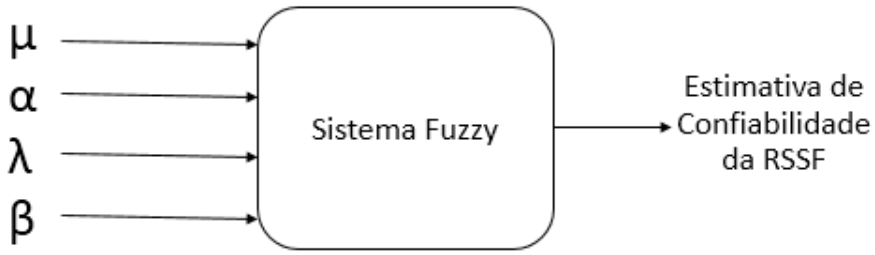
4.5 Sistema *Fuzzy* para Estimativa de Confiabilidade

Um sistema *Fuzzy*, dotado de regras específicas, receberá como entrada os valores resultantes da aplicação dos modelos propostos em 4.1, 4.2, 4.3 e 4.4. A construção da base de regras do sistema *Fuzzy* se baseou no alcance de todas as possibilidades existentes a

partir dos aspectos utilizados na construção do modelo de estimação da confiabilidade de RSSF. Considerando a existência de quatro aspectos, com três funções de pertinência cada, todas a possibilidades precisam ser contempladas nas regras do sistema. Ou seja, para que o sistema *Fuzzy* possa realizar uma inferência na qual considere todos os aspectos, cobrindo todas as probabilidades, deve conter um total de 81 regras.

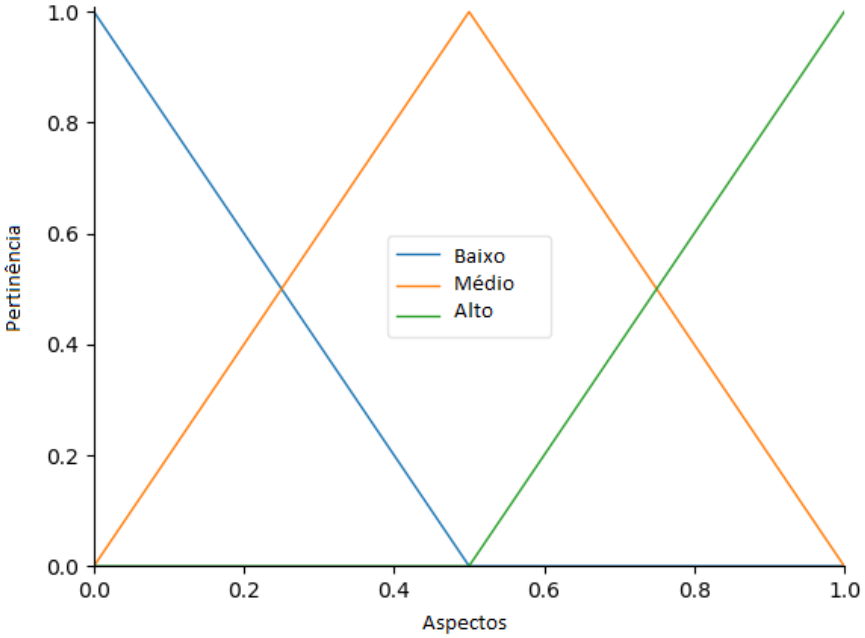
Os valores obtidos através dos aspectos definidos, serão submetidos às regras do sistema conforme Figura 21 e resultarão no *score* de classificação da RSSF quanto à sua confiabilidade. O sistema *Fuzzy* elaborado neste trabalho para classificar RSSF obedece a estrutura:

Figura 21 – Sistema *Fuzzy* para Classificação de RSSF



Os valores de entrada para o aspecto de confiabilidade, acurácia, latência e eficiência energética da rede são compreendidos no intervalo de 0 a 1. Dentro do sistema *Fuzzy* esses valores são classificados de acordo com os critérios linguísticos demonstrados na Figura 22. Estas entradas são submetidas às regras descritas no Apêndice A.

Figura 22 – Variável de entrada dos aspectos abordados no Sistema *Fuzzy*



As configurações da variável de saída estão detalhadas no Apêndice B, no qual está a tabela com os valores arbitrados para a classificação quanto aos níveis de aceitação da RSSF da variável de saída do sistema.

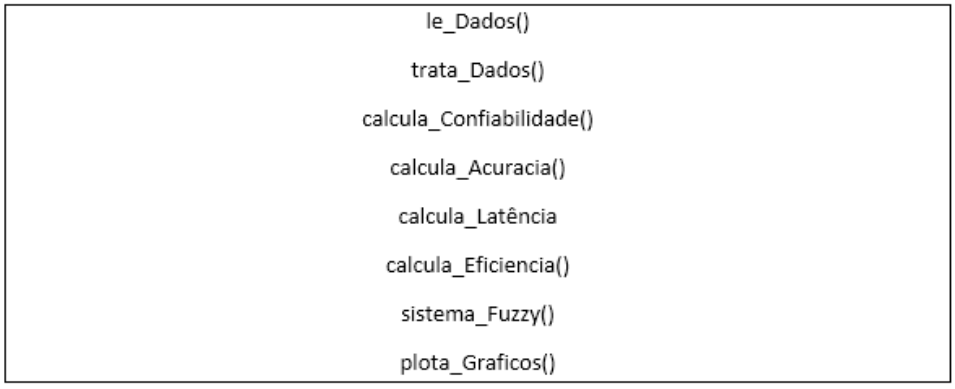
4.6 Sistema para Automação do Processo

Para a automação da aquisição da estimativa do grau de confiabilidade da RSSF, foi desenvolvido um *software*, em linguagem de programação *Python*, para automatizar o processo de coleta das informações referente aos aspectos componentes do modelo de Classificação do Grau de Confiabilidade de RSSFs quanto ao envio e recebimento de mensagens.

O objetivo do desenvolvimento deste *software* se da, não apenas pela praticidade de aquisição das informações necessárias ao processo de avaliação das redes, como também para viabilizar a avaliação de RSSF de qualquer tamanho e quantidade de nós sensores.

A estrutura do *software* em questão segue o seguinte esquema de funções:

Figura 23 – Funções do Sistema



A função principal chama uma função que lê os dados da rede, recebidos neste caso, via simulador. A segunda função trata os dados de forma que as demais funções de cálculo recebam apenas os dados necessários para retornar as saídas para o sistema *Fuzzy*. Este sistema é a próxima função a ser chamada e retorna o grau de confiança da RSSF. A ultima função transforma estes dados em gráfico e os apresenta.

4.7 A proposta do Modelo

Uma vez aplicado, este modelo proporciona ao usuário do sistema, no caso, administrador da RSSF a possibilidade de identificar falhas na rede antes mesmo do final da medição, uma vez que este modelo tem a capacidade de gerar parciais da performance da rede. Do ponto de vista da eficiência, é de suma importância identificar e mitigar falhas antes que os dados obtidos ao final de todo o processo de medição sejam submetidos a equívocos ocasionados por falhas de comunicação ou de confiabilidade da rede.

Diante disso, a utilização deste modelo pode reduzir prejuízos causados pela observação tardia de falhas de medição. Dentre todas as compensações que o modelo oferece, a

possibilidade de retrabalho, ou de uma nova etapa de coleta de dados pode ser suprimida, ou passa a ser desnecessária quando se tem certeza de que uma rede tem um elevado grau de confiabilidade de uma RSSF.

Outro ponto que merece atenção está relacionado aos valores adequados para a aplicação deste modelo. Os valores dependerão, em suma, do projeto avaliado. Esta característica garante a aplicabilidade em diversos tipos de projetos de RSSF para variados fins, incluindo toda a diversidade de modelos de nós sensores existentes.

5 Resultados

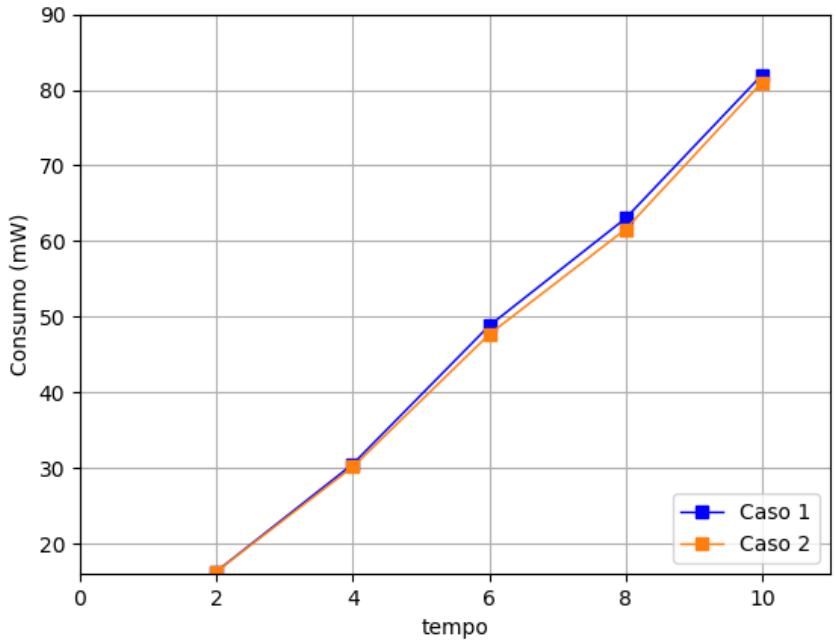
Nesta seção do trabalho, são apresentados resultados obtidos consequentes do planejamento dos experimentos mencionado na seção 3.2 deste trabalho. Os experimentos serão discutidos como casos, na mesma sequência em que foram apresentados na etapa do planejamento.

A coleta de dados para os resultados a seguir, foram obtidos através da simulação de cada um dos experimentos planejados, totalizando 10 medições para cada experimento e trabalhados com a média dos resultados adquiridos em cada um deles.

5.1 Experimento 1

O primeiro experimento visa demonstrar o comportamento de uma RSSF, formada por um nó *sink* (Z1 border router que receberá toda informação trafegada na rede) e quatro nós que comunicam entre si disponibilizando, por meio de diferentes rotas, o acesso do nó *sink* às informações obtidas durante o sensoriamento, em relação ao consumo de energia. Na Figura 24, o caso 1 apresenta uma rede de cinco nós nos quais, à exceção dos nós 2 e 5 todos os nós são vizinhos, ou seja, comunicam-se, e estão em funcionamento pleno por todo o período de 10 minutos. Já o caso 2 apresenta a mesma rede enfrentando a perda de um nó, no segundo minuto de simulação.

Figura 24 – Eficiência Energética



É possível perceber pelas curvas do consumo de energia que, ao perder um nó, o consumo cai. Entretanto, a queda no consumo não é acentuada. De acordo com os critérios de medição do experimento, a queda começa a ser notada a partir quarto minuto de simulação, apresentando uma diferença de 0,37 mW. Esta diferença chega ao ápice no sexto minuto de simulação, quando a diferença no consumo passa a ser de 1,44 mW.

Os nós restantes de uma rede com as características apresentadas, procurarão novas rotas para o tráfego dos pacotes necessários à realização de sua tarefa, e ao suprir a falta do nó perdido, cada nó da rede consome mais energia. A tabela 1 apresenta os dados de consumo energético e ilustra a situação supracitada.

Tabela 1 – Consumo Energético (mW)

tempo(m)	**caso 1**	**caso 2**
2	16,34	16,34
4	30,53	30,16
6	48,82	47,68
8	63,02	61,58
10	81,98	81,00

O aspecto Eficiência Energética leva em conta questões como quantidade de dados trafegados, quantidade de nós ativos na rede, bem como o tipo de sensoriamento realizado e apresenta o quão eficiente esta rede é em termos de consumo de energia. Ou seja, quanto essa rede pode realizar otimizando o consumo energético que é indispensável para o seu funcionamento.

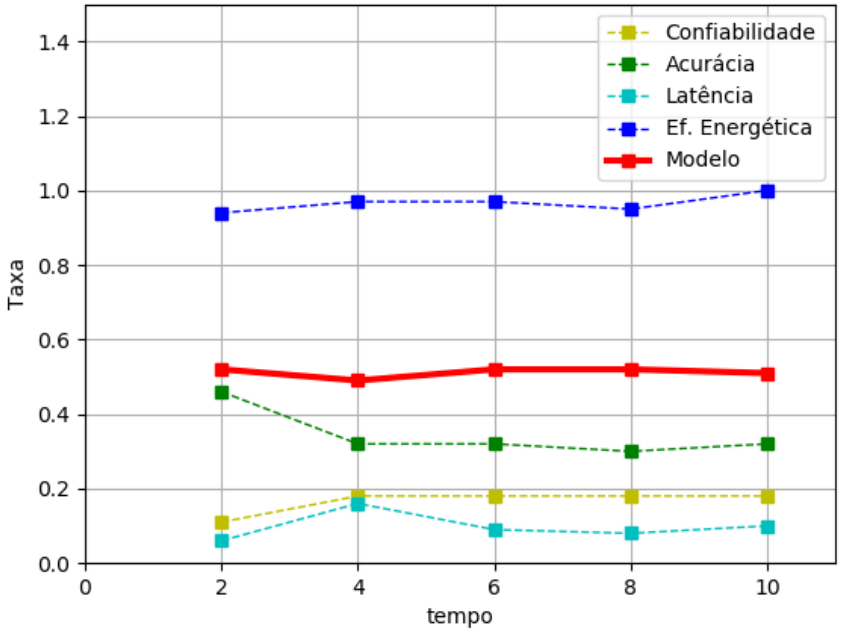
A partir do momento que a rede perde um nó, é possível perceber uma variação no consumo que não obedece proporcionalmente ao que o nó perdido representa para a rede. Uma rede com 5 nós, sendo um nó *sink*, perdendo um nó, proporcionalmente, no melhor caso, sofreria uma variação de 20% no consumo de energia. No pior caso, a variação chegaria a 25%. Entretanto, devido às características apresentadas, a variação é de apenas 1,65% no consumo de energia. Dessa forma é possível perceber, como característica comum das RSSF, um aumento no consumo ao mesmo tempo em que há uma queda na eficiência energética de toda rede.

5.2 Experimento 2

O segundo experimento retrata uma rede semelhante àquela utilizada no experimento 1, com perda de um dos nós da rede com a simulação em curso, devido à pane da bateria de um dos nós, ocasionando seu desligamento inesperado. É uma situação bastante comum quando, por exemplo, os nós sensores são posicionados em campos de difícil acesso, e que inviabilizam a troca do mesmo. A RSSF precisa enviar as informações

de leitura e, dessa forma, escolherá outras rotas para que os dados que antes passariam pelo nó defeituoso, cheguem até o nó *sink*, além do esforço maior que cada nó da rede precisará realizar para monitorar a área do nó defeituoso. Neste caso, no segundo minuto de simulação, o nó 5 da rede é perdido. Neste momento, conforme é mostrado na Figura 26, é possível perceber uma queda considerável na acurácia da rede, pois muitos pacotes continuam a ser enviados ao nó ausente, até que a rede aprenda novas rotas para minimizar esta perda.

Figura 25 – Experimento 2



Quando um dos nós é desativado, o Modelo de Estimativa do Grau de Confiabilidade de RSSF proposto passa a emitir menor pontuação para este nó. Consequentemente esta pontuação impactará toda a avaliação da rede. A Latência demonstra mais uma vez a capacidade que a RSSF tem de encontrar um novo caminho para enviar a informação, pois apesar de sofrer uma pequena queda no gráfico, o que indica o aumento do atraso na comunicação, logo ela se restabelece. Ou seja, a rede aprende novas rotas, por meio de cálculos, para substituir a rota perdida. Uma pequena queda ao fim do período de observação é detectada, pois os nós restantes passam a ser mais exigidos de forma a ocorrer certo atraso na comunicação, em comparação com seu funcionamento pleno. A acurácia da RSSF é o aspecto mais suscetível às perturbações geradas pela simulação em questão. Confirma-se, deste modo, as conclusões do último experimento: enquanto a rede aprende novas rotas, pacotes de informação ainda são enviados ao nó suspenso e acabam impactando diretamente sobre os níveis de acurácia de comunicação da rede. Mais tarde estes níveis tendem a se normalizar. Como a eficiência energética é medida com base em toda rede, sua queda se dá pelo nó desativado na simulação, outros nós compensarão a

falha e consumirão mais energia. O Modelo de Estimativa do Grau de Confiabilidade de RSSF proposto também reage bem à adversidade proposta, uma vez que seus níveis são influenciados pela queda do nó desativado, e logo tende a buscar novo equilíbrio, provando sua eficiência. Os valores obtidos para este experimento estão apresentados na tabela a seguir:

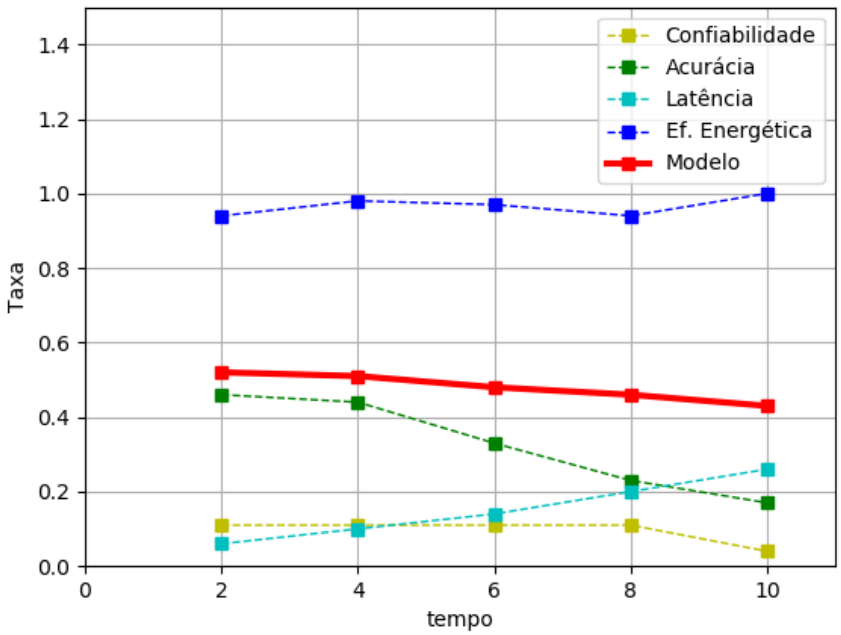
Tabela 2 – Experimento 2

tempo (m)	μ	α	λ	β	**Estimativa do Grau de Confiabilidade**
2	0,11	0,46	0,06	0,94	0,52
4	0,18	0,32	0,16	0,97	0,49
6	0,18	0,32	0,09	0,97	0,52
8	0,18	0,30	0,08	0,95	0,52
10	0,18	0,32	0,10	1,00	0,51

5.3 Experimento 3

No terceiro experimento a rede semelhantemente ao experimento anterior passa por perda em dois de seus nós, em momentos distintos da simulação. É possível notar no gráfico da Figura 26 que o Modelo de confiabilidade proposto acusa a queda nos níveis de confiabilidade uma vez que o conjunto de aspectos observados respondem negativamente à sucessão de perdas.

Figura 26 – Experimento 3



A partir da tabela 3, pode-se determinar a variação dos aspectos durante a simulação, bem como a variação da estimativa do grau de confiabilidade de rede proposto.

Tabela 3 – Experimento 3

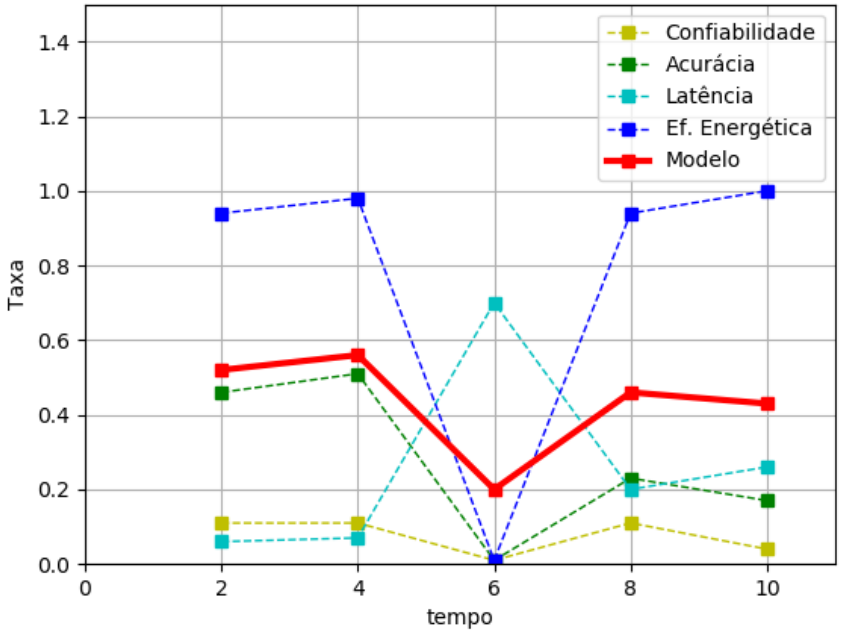
tempo (m)	μ	α	λ	β	**Estimativa do Grau de Confiabilidade**
2	0,11	0,46	0,06	0,94	0,52
4	0,11	0,44	0,10	0,98	0,51
6	0,11	0,33	0,14	0,97	0,48
8	0,11	0,23	0,20	0,94	0,46
10	0,04	0,17	0,26	1,00	0,43

Os aspectos confiabilidade, acurácia, latência e eficiência energética variaram respectivamente 1,00%, 3.63%, 2.50% e 0.80%, enquanto a estimativa do grau de confiabilidade da RSSF varia em 1,10% no período de simulação. Acurácia na comunicação entre os nós da RSSF demonstra-se como o aspecto mais sensível do modelo. A Latência absorveu o impacto da ausência abrupta de nós da rede, pois uma vez que algum nó para de receber alguma mensagem, ele precisa ser substituído por outro para que a RSSF continue em funcionamento. Deste modo, nota-se o aumento no atraso da comunicação, que varia cerca de 2,5% durante todo o período de simulação.

5.4 Experimento 4

O experimento 4 demonstra uma particularidade interessante das RSSF. De acordo com a simulação realizada, há uma pausa no funcionamento de um nó da rede entre os minutos 3 e 6 da simulação. Entretanto, foi possível notar que este nó, devido a sua posição no campo de sensoriamento, era a melhor rota para que o nó *sink* obtivesse informações de todos os demais. Com a pausa em seu funcionamento, o tráfego de pacotes na rede fica momentaneamente comprometido e os aspectos atingem valores comprometedores à confiabilidade da rede. Ente os minutos 6 e 8, há novamente o ingresso do nó ausente na comunicação. Este processo apresenta um consumo de energia extra, uma vez que os pacotes ainda continuam a trafegar pela rede no momento do reconhecimento do nó entrante. Isto implica na queda vertiginosa na eficiência energética da rede, bem como um aumento considerável no aspecto do atraso da comunicação. A acurácia e a confiabilidade também são aspectos comprometidos e consequentemente o modelo proposto acusa queda no grau estimado para confiabilidade da RSSF, conforme o gráfico da Figura 27.

Figura 27 – Experimento 4



Os valores de entrada deste experimento estão dispostos na tabela 4

Tabela 4 – Experimento 4

tempo (m)	μ	α	λ	β	**Estimativa do Grau de Confiabilidade**
2	0,11	0,46	0,06	0,94	0,52
4	0,11	0,51	0,07	0,98	0,56
6	0,01	0,01	0,70	0,01	0,20
8	0,11	0,23	0,20	0,94	0,46
10	0,04	0,17	0,26	1,00	0,43

5.5 Experimento 5

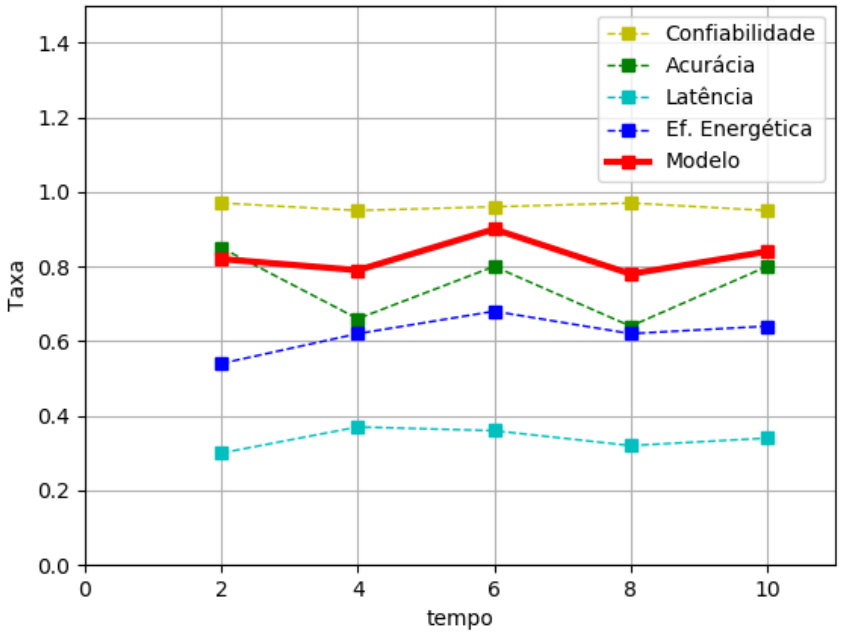
Para demonstrar a sensibilidade do modelo de estimação de confiabilidade proposto, perante as variáveis de entrada, o experimento em questão conta com uma rede de cinco nós em pleno funcionamento de seus sensores. A adversidade, simulada neste experimento, é a ausência de comunicação entre dois nós, que apesar de estarem funcionando perfeitamente, estão limitados em envios diretos de pacotes pelo fator distância, ou área de cobertura de comunicação.

Após a simulação, os dados obtidos em espaços de tempo de dois minutos estão descritos na tabela 5 e dispostos no gráfico da Figura 28 .

Tabela 5 – Experimento 5

tempo (m)	μ	α	λ	β	**Estimativa do Grau de Confiabilidade**
2	0,97	0,85	0,3	0,54	0,82
4	0,95	0,66	0,37	0,62	0,79
6	0,96	0,8	0,36	0,68	0,9
8	0,97	0,64	0,32	0,62	0,78
10	0,95	0,8	0,34	0,64	0,84

Figura 28 – Experimento 5



A análise do comportamento da RSSF demonstrou que o modelo proposto de Estimação de Confiabilidade para RSSF, formado por quatro aspectos pré-definidos, se comporta de forma coerente com as variações apresentadas por cada aspecto distinto, conforme Figura abaixo: Em condições normais de funcionamento da RSSF, conforme predito neste experimento, a Acurácia de comunicação entre os nós da rede exerce maior influência no modelo de Estimação de confiabilidade proposto. Isto ocorre porque as condições de comunicação estão estáveis, ou seja, não há mudanças bruscas ocorrendo ao longo do funcionamento da rede variando de forma significativa algum outro aspecto estudado para compor o modelo. Em primeira análise, os resultados sugerem a tendência que os aspectos escolhidos e consequentemente o modelo proposto tendem a se estabilizar à medida que a rede procura rotas de comunicação para manter seu funcionamento constante. Comparando os resultados com os modelos individuais dos aspectos apresentados na literatura e utilizados neste estudo, percebe-se que, tomados individualmente, estes aspectos podem não

representar fielmente as condições em que as RSSF são expostas no mundo real. Assim, é possível compreender que fatores externos exercem bastante influência no funcionamento de uma RSSF e o modelo proposto reage coerentemente a isto.

5.6 Experimento 6

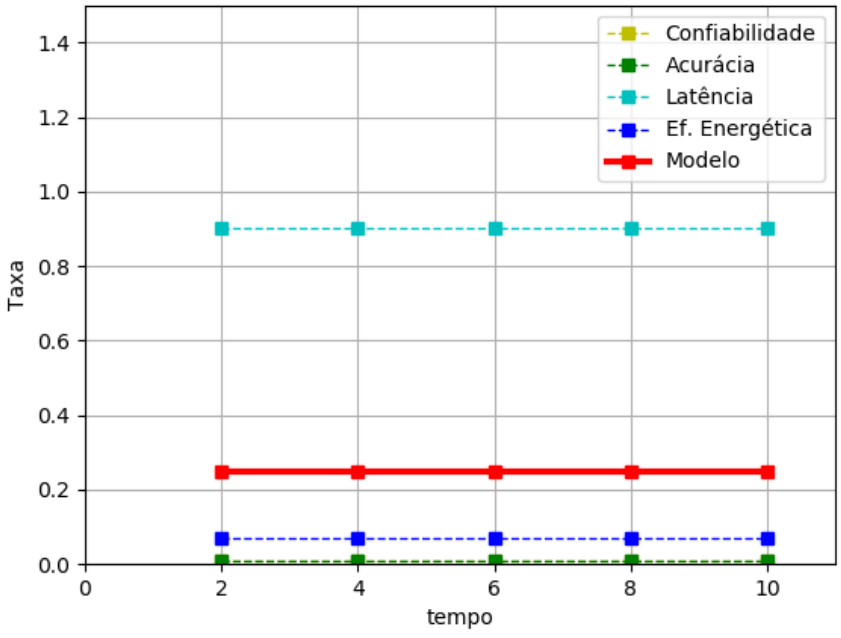
Conforme é apresentado na tabela 6, os dados de entrada para o primeiro caso resultaram em uma rede de baixo grau de confiabilidade.

Tabela 6 – Experimento 6

tempo (m)	μ	α	λ	β	**Estimativa do Grau de Confiabilidade**
2	0,1	0,1	0,9	0,07	0,25
4	0,1	0,1	0,9	0,07	0,25
6	0,1	0,1	0,9	0,07	0,25
8	0,1	0,1	0,9	0,07	0,25
10	0,1	0,1	0,9	0,07	0,25

Os valores para confiabilidade figuraram na categoria linguística ”baixo” conforme apêndice B, ou seja, com índices insuficientes para o funcionamento ótimo da RSSF, do mesmo modo em que as variáveis acurácia e eficiência energética, conforme gráfico a seguir:

Figura 29 – Experimento 6



Já a variável latência teve o valor de entrada no sistema classificado como alto, o que em nenhuma hipótese faria com que a rede obtivesse boa qualificação quando a seu grau de confiabilidade. A tabela 6 apresenta o processo de avaliação do sistema *Fuzzy* a partir das entradas obtidas, quando o sistema retorna um resultado de 0,25 para o grau de confiabilidade da RSSF em uma escala de 0 a 1. O experimento 6 refuta a segunda hipótese levantada, de que uma rede com baixo grau de confiabilidade não está apta para o uso. O grau de confiabilidade se refere ao aumento da possibilidade de falha nas tarefas de envio e recebimento de mensagens, atraso na comunicação entre os nós ou queda de energia, o que resultaria no desativamento de algum nó da rede, porém conforme simulação, não impedindo a rede de funcionar.

O experimento 6 demonstra que quando os aspectos do modelo obtém valores baixos para a entrada no sistema Fuzzy, o resultado final da estimativa de confiabilidade da RSSF tende a apontar valor baixo, dentro da escala adotada, para confiabilidade. O resultado obtido pelo modelo é condizente com o resultado de entrada de cada aspecto.

5.7 Experimento 7

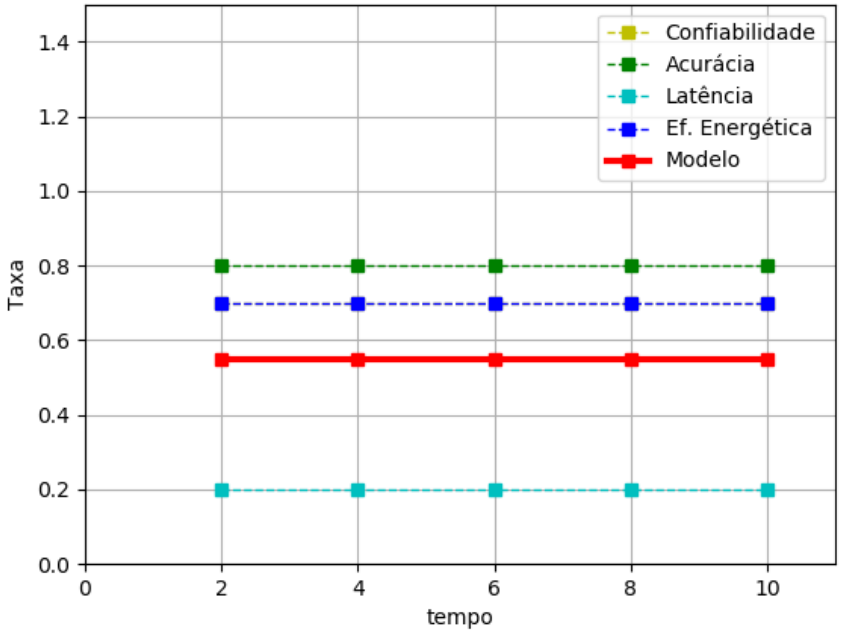
Para este caso, os valores de entrada que foram obtidos, de acordo com a tabela a seguir, fornecem uma classificação média à RSSF.

Tabela 7 – Experimento 5

tempo (m)	μ	α	λ	β	**Estimativa do Grau de Confiabilidade**
2	0,7	0,8	0,2	0,7	0,55
4	0,7	0,8	0,2	0,7	0,55
6	0,7	0,8	0,2	0,7	0,55
8	0,7	0,8	0,2	0,7	0,55
10	0,7	0,8	0,2	0,7	0,55

O resultado apresentado pelo Sistema *Fuzzy* como grau de Confiabilidade da rede foi de 5,54 em escala de 0 a 10, conforme apresentado no gráfico da Figura 30

Figura 30 – Experimento 7



O experimento 7 objetiva demonstrar que os resultados médios dos aspectos componentes do modelo. Resultam invariavelmente em uma estimativa média de confiabilidade de RSSF. É possível perceber que à menor variação em qualquer dos aspectos componentes do modelo, resultará em uma alteração na estimativa de confiabilidade.

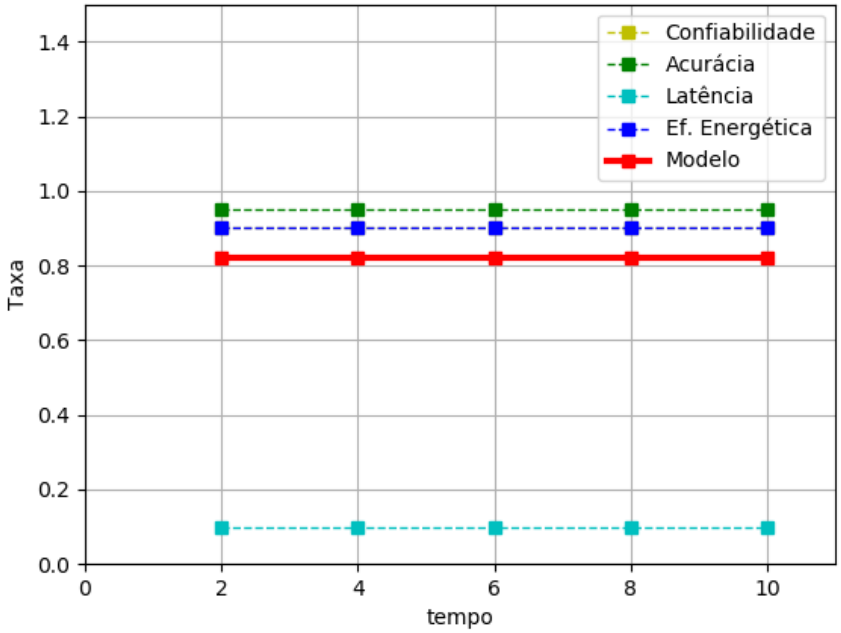
5.8 Experimento 8

O experimento 8 aponta uma rede com resultados satisfatórios para o grau de confiabilidade da rede de acordo com o modelo proposto e explicitado no apêndice B deste trabalho. O grau de confiança apontado pelo sistema para esta RSSF foi de 0,821 também em escala de 0 a 1 como mostra a tabela e o gráfico abaixo:

Tabela 8 – Experimento 8

tempo (m)	μ	α	λ	β	**Estimativa do Grau de Confiabilidade**
2	0,9	9,5	0,1	0,9	0,82
4	0,9	9,5	0,1	0,9	0,82
6	0,9	9,5	0,1	0,9	0,82
8	0,9	9,5	0,1	0,9	0,82
10	0,9	9,5	0,1	0,9	0,82

Figura 31 – Experimento 8



O experimento 8 mostra a reação do modelo de estimativa de confiabilidade frente a bons níveis individuais de entrada dos aspectos componentes. Os experimentos 6, 7 e 8 servem para demonstrar de forma clara a sensibilidade que o modelo de estimativa de confiabilidade de RSSF possui mediante a suas entradas. Reafirmando assim a importância dos aspectos escolhidos para compor o modelo diante do seu resultado final. Neste caso em particular, quando os valores e entradas estão detidos em categorias denominadas ótimas, o resultado tende a ser igualmente ótimo. Estes experimentos comprovam que o modelo proposto é funcional e os aspectos escolhidos para a confecção do modelo proposto, compõem-no de maneira eficaz.

5.9 Discussões Finais sobre os resultados

Os experimentos demonstraram coerência e sensibilidade do modelo proposto às diversas situações simuladas. O experimento 1 apresenta a coerência do aspecto eficiência energética. A perda de um nó da rede influencia diretamente no consumo de energia da mesma. Os experimentos 2 a 5 comprovam a sensibilidade do resultado obtido em relação às diversas alterações simuladas nos aspectos investigados. Já os experimentos 6 a 8 sugerem coerência e eficácia da estimativa do grau de confiabilidade das RSSF.

Os resultados obtidos permitem concluir que o desempenho da estimativa do grau de confiabilidade da RSSF é afetado por qualquer alteração em qualquer um dos aspectos. Permite ainda inferir que todos estes aspectos representam a mesma importância no resul-

tado obtido. Cada aspecto corresponde a exatos 25% da configuração do resultado final. Os valores de latência da rede são inversamente proporcionais aos demais aspectos estudados. Quando analisados dessa forma, corroboram com a correspondência de influência no modelo frente aos demais aspectos da rede.

O sistema *Fuzzy* desenvolvido para este trabalho utiliza o controlador *Mamdani*. Este tipo de controlador foi escolhido, de acordo com a literatura, por apresentar melhor desempenho para baixa quantidade de dados, como foi o caso desta pesquisa. Dessa forma acredita-se que as estimativas do grau de confiabilidade da RSSF obtidas nestes experimentos exprimam valores assertivos, com validade tanto em ambientes simulados como em ambientes reais.

6 Considerações Finais

A *IoT* é uma realidade e as previsões são de que a cada dia mais dispositivos estejam conectados com a finalidade de proporcionar comodidade e praticidade às pessoas, instituições e governos. É sem dúvida um avanço em termos tecnológicos e sociais, já que suas aplicações utilizam recursos tecnológicos de ponta e resultam em benefícios para toda a sociedade. A cada ano inúmeros dispositivos novos são conectados e conseguem reagir a situações sem a intervenção humana. Tudo isto é realizado graças a tecnologias como as RSSF, onde os sensores são os primeiros objetos a reagirem a algum estímulo, sem a necessidade de interação de um operador. As RSSF, embora em seus primórdios fossem utilizadas largamente para medições, são atualmente usadas nas mais diversas atividades como na indústria, na viabilização de carros autônomos, nas *smart houses*, nos *smart offices*, além das finalidades já apresentadas neste estudo. Não há dúvidas de que este tipo de rede ainda evoluirá de forma significativa nos próximos anos e dessa forma este trabalho visa contribuir com esta evolução.

Um mecanismo de medição de confiabilidade de rede pode facilitar o projeto e a simulação de uma RSSF com base em eficiência, disponibilizando, por exemplo, apenas os nós necessários para a realização de determinada tarefa. A indústria automobilística atualmente investe muito em projetos das chamadas VANETs (*Veicular Ad Hoc Network*) que são redes móveis para se estabelecer comunicação intra-carros e entre carros e estradas. Este modelo de comunicação veicular objetiva segurança em rodovias, informações sobre tráfego e até mesmo entretenimento. É uma tipologia diferente daquela abordada neste trabalho, porém com os mesmos princípios e o modelo proposto neste trabalho reúne condições para adentrar este campo.

Após a realização da etapa inicial desta pesquisa, foi possível verificar que os resultados obtidos a partir do modelo proposto apresentaram grandes chances de serem validados através de demais simulações. O sistema *Fuzzy* configurado para estimação do grau de confiabilidade da rede de sensores sem fio também demonstrou, desde o início, coerência entre entrada e saída de dados. Este fato atesta a sensibilidade do modelo proposto a alterações nas variáveis de entrada, que são medidas do estado atual das RSSF.

Todos os experimentos constantes neste trabalho foram realizados por meio do emulador de RSSF Cooja, no sistema operacional Contiki. Os dados obtidos foram tratados em um programa desenvolvido para este fim, na linguagem de programação Python. Após o tratamento destes dados, os aspectos estudados foram calculados e enviados a um sistema *Fuzzy*, também desenvolvido em Python, para que se fosse obtida a Estimativa do Grau de Confiabilidade de RSSF.

Os três últimos experimentos refutam a primeira hipótese levantada, de que o funcionamento da rede dependeria do grau de confiabilidade, pois a análise de resultados detectou que algumas redes podem funcionar por todo o período determinado para a coleta de suas medições, ainda que tenha um grau baixo de confiabilidade.

Os experimentos também refutaram a segunda hipótese de que, com baixo grau de confiabilidade, a rede não estaria apta ao uso. Inclusive, mediante uma adversidade, a própria RSSF possui intrinsecamente a característica de se adaptar, ainda que este processo resulte em aumento do consumo energético, ou ainda comprometa sua acurácia, ou latência.

Os resultados apontam que o sistema *Fuzzy*, configurado para classificação do grau de confiabilidade das RSSF, se comporta conforme o esperado em relação aos dados obtidos por simulação. Dessa forma ele retorna dados consistentes sobre grau de confiabilidade de uma RSSF.

Como saída dos dados, o grau de confiabilidade é dado em escala numérica de 0 a 1 e a classificação semântica para o grau de confiabilidade obtido segue a tabela constante no apêndice C. Esta tabela é uma proposta de classificação semântica pós obtenção da estimativa do grau de confiabilidade de uma RSSF, e como tal, poderá ter comprovada, em estudos futuros, sua utilidade em redes reais. A classificação semântica proposta varia de acordo com o grau obtido por meio dos modelos matemáticos apresentados no capítulo 4. A aplicação destes modelos fornece as quatro entradas para o sistema *Fuzzy*, que foi configurado para resultar no grau de confiabilidade da RSSF de acordo com o apêndice A.

Espera-se que a medida que esta pesquisa alcance novos patamares, tanto a obtenção dos dados para análise, quanto o modelo em si sejam aprimorados para viabilizar maior acurácia dos resultados.

O desenvolvimento deste trabalho se deu por meio da simulação de uma RSSF em ambiente aberto para medições diversas. Neste contexto foi planejada, desenvolvida e testada uma RSSF capaz de realizar medições em ambientes externos com influência de fatores adversos comuns no cotidiano. A estrutura e funcionamento da rede foram definidos de forma padronizada a fim de detectar cada situação adversa sob o prisma da confiabilidade da rede. As medições concentraram-se nos níveis de envios e recebimentos de pacotes de comunicação da RSSF. Os aspectos observados para a detecção do grau de confiabilidade da RSSF foram a eficiência e a eficácia com que os pacotes eram entregues, realizando assim as funções para as quais a rede foi criada, representadas por Latência e Acurácia na comunicação. Além disso, foi observada também a confiabilidade de cada nó da rede baseada em seu funcionamento e no funcionamento dos nós vizinhos. Dessa forma a avaliação de confiabilidade quanto aos nós da RSSF é realizada, em parte pelos próprios nós da rede, confirmando a possibilidade de que os nós da rede reajam a alguma situação sem a necessidade da intervenção humana no processo. Por fim, também foi

considerado o consumo energético da RSSF em seu funcionamento, visto que este é um aspecto considerado crítico para o funcionamento da mesma.

6.1 Trabalhos Futuros

Devido à enorme quantidade de influência que uma rede pode sofrer durante seu funcionamento e também das inúmeras aplicações que as RSSF exercem, urge a necessidade de se implementar modelos mais complexos para estimativa do grau de confiabilidade da RSSF. Este trabalho se ateve a quatro aspectos para estimar o grau de confiabilidade da rede. Outra questão importante é que este trabalho objetivou observar a confiabilidade quanto ao envio e recebimento de pacotes, ou seja, dedicou-se exclusivamente ao tráfego de dados na rede. Este fato abre caminho para novos estudos que contemplem outras complexidades que as RSSF possuem, como por exemplo, a escalabilidade, a própria questão da segurança, desde que abordada de forma separada, etc. À medida que novos aspectos sejam incrementados ao modelo de estimativa de confiabilidade, maior será a precisão do resultado e maior será sua abrangência de atuação.

Como os elementos componentes deste estudo estão presentes em todo tipo de rede de comunicação, uma proposta de continuidade deste trabalho, é a adequação deste modelo para redes móveis. A suspeita é de que, alcançando resultados satisfatórios, as redes de comunicação móveis podem ser otimizadas em relação ao seu custo e qualidade. A importância deste tipo de investigação pode ser comprovada ao se confrontar as grandezas em investimento que são realizados anualmente nestas tecnologias e principalmente o panorama de novos investimentos que já se projetam para o futuro na área das telecomunicações, por exemplo.

Outra investigação a ser conduzida, se refere à avaliação da confiabilidade mediante a um modelo diferente de comunicação, usado em redes veiculares sem fio e nas *smart highways*. Averiguar o comportamento dos elementos de comunicação da rede e otimizar seu funcionamento. Esta investigação se torna relevante à medida que se dissemina a construção deste tipo de estrada, uma vez que favorecerá o desenvolvimento desta tecnologia de forma eficiente e eficaz.

Outra proposta de continuidade é trabalhar este modelo em ambiente real de forma que o *software* desenvolvido obtenha como entrada, dados em períodos pré determinados, impossíveis de se conseguir em ambiente simulado, para que seja possível realizar o monitoramento da rede em tempo real, detectando falhas no momento em que elas acontecem e então mitigá-las, reduzindo assim os períodos em que a RSSF trabalharia com a capacidade de comunicação comprometida.

Finalmente, pode-se considerar a realização de uma análise quantitativa sobre a sensibilidade do modelo apresentado. Esta análise estaria apta a averiguar, em termos esta-

tísticos, qual é a variação de cada aspecto do modelo a partir de perturbações direcionadas a cada um deles, e posteriormente, ao conjunto de todos os aspectos componentes do mesmo. Este tipo de trabalho ofereceria subsídios para utilizar a aplicação deste modelo de forma adaptada à situações variadas, certamente não abordadas neste estudo, e das quais seriam necessárias alterações nos pesos das regras do sistema *Fuzzy*. Por exemplo, quando houver demanda por avaliação de algum dos aspectos de forma independente. Dessa forma, declina-se a necessidade da criação de um novo modelo para contemplar tal situação, aumentando ainda mais a aplicabilidade do modelo proposto neste trabalho.

Referências

ABREU, K. C. K. História e usos da internet. **Biblioteca on-line de Ciências da Comunicação. Universidade da Beira Interior. Covilhã**, 2009. Citado na página 2.

AKYILDIZ, I. F. et al. Wireless sensor networks: A survey. **Computer networks**, Elsevier, v. 38, n. 4, p. 393–422, 2002. Citado 8 vezes nas páginas 5, 12, 14, 15, 27, 32, 33 e 36.

ALBERT, R.; JEONG, H.; BARABÁSI, A.-L. Internet: Diameter of the world-wide web. **nature**, Nature Publishing Group, v. 401, n. 6749, p. 130–131, 1999. Citado na página 1.

ALMEIDA, P. E.; EVSUKOFF, A. G. Sistemas fuzzy. **Rezende, SO Sistemas Inteligentes: fundamentos e aplicaçoes. Barueri, SP: Manole, Cap**, v. 7, p. 169–201, 2003. Citado 2 vezes nas páginas 21 e 22.

ANZANO, E. S. **Fuzzy Clustering Means Algorithm for Track Fusion in US Coast Guard Vessel Traffic Service Systems.** [S.l.], 1999. Citado na página 21.

BAUER, M.; WALEWSKI, J. W. The iot architectural reference model as enabler. In: **Enabling Things to Talk**. [S.l.]: Springer, 2013. p. 17–25. Citado na página 8.

BENCKE, L. R.; PEREZ, A. L. F.; ARMENDARIS, O. da C. Rodovias inteligentes: Uma visão geral sobre as tecnologias empregadas no brasil e no mundo. **iSys-Revista Brasileira de Sistemas de Informação**, v. 10, n. 4, p. 80–102, 2017. Citado na página 12.

BROCK, D. L. Integrating the electronic product code (epc) and the global trade item number (gtin). **White Paper available at www. autoidcenter. org/pdfs/MIT-WUTOID-WH-004. pdf**, v. 25, 2001. Citado 2 vezes nas páginas 4 e 8.

BUCHEGGER, S.; BOUDEC, J. L. The effect of rumor spreading in reputation systems for mobile ad-hoc networks. In: **WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks**. [S.l.: s.n.], 2003. p. 10–pages. Citado na página 22.

CAPELLA, J. V. et al. A reference model for monitoring iot wsn-based applications. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 16, n. 11, p. 1816, 2016. Citado 4 vezes nas páginas 1, 7, 8 e 10.

CARVALHO, F. B. S. de et al. Aplicacoes ambientais de redes de sensores sem fio. **Revista de tecnologia da informação e comunicação**, v. 2, n. 1, p. 14–19, 2012. Citado na página 13.

CHESHIRE, S. Latency and the quest for interactivity. In: **White paper commissioned by Volpe Welty Asset Management, LLC, for the Synchronous Person-to-Person Interactive Computing Environments Meeting**. [S.l.: s.n.], 1996. Citado 2 vezes nas páginas 27 e 32.

CHOWDHRY, B. et al. Development of wireless sensor networks for smart civil structures and highway safety. In: IEEE. **Signal Processing and Communications, 2007. ICSPC 2007. IEEE International Conference on**. [S.l.], 2007. p. 420–423. Citado na página 28.

CRUZ, P.; COUTO, R. S.; COSTA, L. H. M. Análise da cobertura espacial de uma rede de sensores baseada em ô nibus urbanos. In: **Simpósio Brasileiro de Redes de Computadores (SBRC)**. [S.l.: s.n.], 2018. v. 36. Citado na página 12.

DEIF, D. S.; GADALLAH, Y. Classification of wireless sensor networks deployment techniques. **IEEE Communications Surveys & Tutorials**, IEEE, v. 16, n. 2, p. 834–855, 2014. Citado 2 vezes nas páginas 16 e 25.

ESKOLA, M.; HEIKKILÄ, T. Classification of radio channel disturbances for industrial wireless sensor networks. **Ad Hoc Networks**, Elsevier, v. 42, p. 19–33, 2016. Citado 5 vezes nas páginas 26, 27, 32, 36 e 41.

EVANS, D. Internet das coisas: Como a próxima evolução da internet está mudando tudo. **Cisco Internet Business Solutions Group (IBSG). San Jose, Canada**, 2011. Citado 4 vezes nas páginas 1, 2, 4 e 13.

FANTACCI, R. et al. A network architecture solution for efficient iot wsn backhauling: Challenges and opportunities. **IEEE Wireless Communications**, IEEE, v. 21, n. 4, p. 113–119, 2014. Citado 2 vezes nas páginas 3 e 9.

FURTADO, H.; TROBEC, R. Applications of wireless sensors in medicine. In: IEEE. **MIPRO, 2011 Proceedings of the 34th International Convention**. [S.l.], 2011. p. 257–261. Citado na página 14.

GAO, J. **Intelligent and interactive package based on RFID and WSN**. Tese (Doutorado) — KTH Royal Institute Of Technology, 2011. Citado na página 12.

GIL, A. C. Pesquisa social: Métodos e técnicas. **São Paulo: Atlas**, v. 5, 1999. Citado na página 35.

GOMIDE, F.; GUDWIN, R. R.; TANSCHEIT, R. Conceitos fundamentais da teoria de conjuntos fuzzy, lógica fuzzy e aplicações. In: **Proc. 6 th IFSA Congress-Tutorials**. [S.l.: s.n.], 1995. p. 1–38. Citado 5 vezes nas páginas 3, 17, 18, 19 e 20.

GUBBI, J. et al. Internet of things (iot): A vision, architectural elements, and future directions. **Future generation computer systems**, Elsevier, v. 29, n. 7, p. 1645–1660, 2013. Citado 3 vezes nas páginas 4, 7 e 9.

HE, Q.; WU, D.; KHOSLA, P. A secure incentive architecture for ad hoc networks. **Wireless Communications and Mobile Computing**, Wiley Online Library, v. 6, n. 3, p. 333–346, 2006. Citado na página 24.

JR, R. K. R.; CEGIELSKI, C. G. Introdução a sistemas de informação. **Rio de Janeiro: Campus**, 2012. Citado na página 21.

JTC, I. I. **Internet of Things (IoT):Preliminary Report**. [S.l.], 2014. Citado na página 1.

KUMAR, N.; SINGH, Y. Trust and packet load balancing based secure opportunistic routing protocol for wsn. In: IEEE. **Signal Processing, Computing and Control (ISPCC), 2017 4th International Conference on**. [S.l.], 2017. p. 463–467. Citado na página 26.

LAKATOS, E.; MARCONI, M. d. Fundamentos da metodologia do trabalho científico. ampliada. **São Paulo: Atlas**, 1993. Citado na página 35.

LAUDON, K.; LAUDON, J. **Sistemas de Informações Gerenciais. Tradução de Luciana do Amaral Teixeira; Revisão técnica Belmiro Nascimento João**. [S.l.]: São Paulo: Pearson Prentice Hall, 2010. Citado na página 21.

LI, Y.; LIANG, Y. Compressed sensing in multi-hop large-scale wireless sensor networks based on routing topology tomography. **IEEE Access**, IEEE, v. 6, p. 27637–27650, 2018. Citado na página 28.

LIGGINS, M.; HALL, D.; LLINAS, J. **Handbook of Multisensor Data Fusion: Theory and Practice**. [S.l.]: CRC press, 2017. Citado na página 21.

LIU, Z.; JOY, A. W.; THOMPSON, R. A. A dynamic trust model for mobile ad hoc networks. In: IEEE. **Distributed Computing Systems, 2004. FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends of**. [S.l.], 2004. p. 80–85. Citado na página 23.

LOPEZ, J. et al. Trust management systems for wireless sensor networks: Best practices. **Computer Communications**, Elsevier, v. 33, n. 9, p. 1086–1093, 2010. Citado 2 vezes nas páginas 3 e 27.

LOUREIRO, A. A. et al. Redes de sensores sem fio. In: SN. **Simpósio Brasileiro de Redes de Computadores (SBRC)**. [S.l.], 2003. p. 179–226. Citado 4 vezes nas páginas 2, 9, 10 e 28.

MANJUNATHA, P.; VERMA, A.; SRIVIDYA, A. Multi-sensor data fusion in cluster based wireless sensor networks using fuzzy logic method. In: IEEE. **Industrial and Information Systems, 2008. ICIIS 2008. IEEE Region 10 and the Third international Conference on**. [S.l.], 2008. p. 1–6. Citado na página 14.

MÁRMOL, F. G.; PÉREZ, G. M. Trmsim-wsn, trust and reputation models simulator for wireless sensor networks. In: IEEE. **2009 IEEE International Conference on Communications**. [S.l.], 2009. p. 1–5. Citado na página 25.

MÁRMOL, F. G.; PÉREZ, G. M. Providing trust in wireless sensor networks using a bio-inspired technique. **Telecommunication systems**, Springer, v. 46, n. 2, p. 163–180, 2011. Citado 3 vezes nas páginas 1, 9 e 10.

MARTONOSI, M. The princeton zebranet project: Sensor networks for wildlife tracking. **Princeton University**, p. 2–7, 2004. Citado na página 13.

MELLO, R. de A. et al. An architecture for self-protection in internet of things. **ICWMC 2016**, p. 51, 2016. Citado 2 vezes nas páginas 7 e 8.

MINERVA, R.; BIRU, A.; ROTONDI, D. Towards a definition of the internet of things (iot). **IEEE Internet Initiative, Torino, Italy**, 2015. Citado na página 1.

MOLISCH, A. F. et al. Ieee 802.15. 4a channel model-final report. **IEEE P802**, Citeseer, v. 15, n. 04, p. 0662, 2004. Citado na página 11.

OLIVEIRA, C. A. D.; BELDERRAIN, M. C. N. Aplicação de lógica "fuzzy" para fusão de dados de acompanhamento de plataformas no cenário marítimo. **Anais do XL SBPO–Simpósio Brasileiro de Pesquisa Operacional**, 2008. Citado na página 21.

PICOZZI, M. et al. Wireless technologies for the monitoring of strategic civil infrastructures: An ambient vibration test on the fatih sultan mehmet suspension bridge in istanbul, turkey. **Bulletin of Earthquake Engineering**, Springer, v. 8, n. 3, p. 671–691, 2010. Citado na página 12.

PIRZADA, A. A.; MCDONALD, C. Trust establishment in pure ad-hoc networks. **Wireless Personal Communications**, Springer, v. 37, n. 1-2, p. 139–168, 2006. Citado na página 25.

PUCCINELLI, D.; HAENGGI, M. Wireless sensor networks: Applications and challenges of ubiquitous sensing. **IEEE Circuits and systems magazine**, IEEE, v. 5, n. 3, p. 19–31, 2005. Citado 2 vezes nas páginas 12 e 14.

REZENDE, S. O. **Sistemas inteligentes: Fundamentos e Aplicações**. [S.l.]: Editora Manole Ltda, 2003. Citado 2 vezes nas páginas 5 e 17.

SHAIKH, F. K.; ZEADALLY, S. Energy harvesting in wireless sensor networks: A comprehensive review. **Renewable and Sustainable Energy Reviews**, Elsevier, v. 55, p. 1041–1054, 2016. Citado na página 28.

SHIH, E. et al. Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks. In: ACM. **Proceedings of the 7th annual international conference on Mobile computing and networking**. [S.l.], 2001. p. 272–287. Citado na página 33.

SILVA, E. L. D.; MENEZES, E. M. Metodologia da pesquisa e elaboração de dissertação. **UFSC, Florianópolis, 4a. edição**, v. 123, 2005. Citado na página 35.

SOUSA, M. P.; LOPES, W. T. A. Desafios em redes de sensores sem fio. **dados**, v. 2, p. 3, 2011. Citado 2 vezes nas páginas 3 e 9.

SOUZA, d. Estudo das tecnologias de monitoramento de painéis em usinas fotovoltaicas através de redes de sensores sem fio. **Arquitetura. Disponível em:. Acesso em**, v. 8, n. 04, p. 2016, 2013. Citado 2 vezes nas páginas 27 e 32.

SPAGNOL, W. A. et al. Monitoring the cold chain: new technologies and recent advances. **Brazilian Journal of Food Technology**, SciELO Brasil, v. 21, 2018. Citado na página 12.

SUN, Y. L. et al. A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks. In: **INFOCOM**. [S.l.: s.n.], 2006. v. 2006, p. 1–13. Citado na página 24.

TANENBAUM, E. C. **Tradução da 4a**. [S.l.]: Edição, 2003. Citado 3 vezes nas páginas 27, 32 e 36.

THEODORAKOPOULOS, G.; BARAS, J. S. On trust models and trust evaluation metrics for ad hoc networks. **IEEE Journal on selected areas in Communications**, IEEE, v. 24, n. 2, p. 318–328, 2006. Citado na página 24.

VELLOSO, P. B. et al. Análise de um modelo de confiança para redes móveis ad hoc. **24º Simpósio Brasileiro de Redes de Computadores**, 2006. Citado 8 vezes nas páginas 2, 17, 28, 29, 30, 31, 36 e 45.

VELLOSO, P. B. B. et al. A trust model robust to slander attacks in ad hoc networks. In: IEEE. **2008 Proceedings of 17th International Conference on Computer Communications and Networks**. [S.l.], 2008. p. 1–6. Citado 2 vezes nas páginas 4 e 25.

VIRENDRA, M. et al. Quantifying trust in mobile ad-hoc networks. In: **Proc. IEEE Int'l Conf. Integration of Knowledge Intensive Multi-Agent Systems (KIMAS)**. [S.l.: s.n.], 2005. Citado 8 vezes nas páginas 17, 23, 25, 27, 28, 31, 36 e 45.

WANG, T.-Y. et al. Distributed fault-tolerant classification in wireless sensor networks. **IEEE Journal on Selected Areas in Communications**, IEEE, v. 23, n. 4, p. 724–734, 2005. Citado 3 vezes nas páginas 16, 23 e 24.

WHITE, F. Data fusion lexicon: Data fusion subpanel of the joint directors of laboratories technical panel for c3. **IEEE Trans.: San Diego, CA, USA**, 1991. Citado na página 21.

WHITMORE, A.; AGARWAL, A.; XU, L. D. The internet of things—a survey of topics and trends. **Information Systems Frontiers**, Springer, v. 17, n. 2, p. 261–274, 2015. Citado 2 vezes nas páginas 7 e 8.

YAN, Z.; ZHANG, P.; VIRTANEN, T. Trust evaluation based security solution in ad hoc networks. In: **Proceedings of the Seventh Nordic Workshop on Secure IT Systems**. [S.l.: s.n.], 2003. v. 14. Citado na página 22.

YUN, M.; YUXIN, B. Research on the architecture and key technology of internet of things (iot) applied on smart grid. In: IEEE. **Advances in Energy Engineering (ICAEE), 2010 International Conference on**. [S.l.], 2010. p. 69–72. Citado 2 vezes nas páginas 8 e 9.

ZADEH, L. A. Fuzzy sets. **Information and control**, Elsevier, v. 8, n. 3, p. 338–353, 1965. Citado na página 18.

ZHU, C. et al. Trust-based communication for the industrial internet of things. **IEEE Communications Magazine**, IEEE, v. 56, n. 2, p. 16–22, 2018. Citado na página 26.

APÊNDICE A – Regras do Sistema *Fuzzy* para Classificação das RSSF

REGRA	SE Confiabilidade é	E Acurácia é	E Latência é	E Eficiência Energética é	Então o Grau de Confiabilidade da RSSF é
1	Baixa	Baixa	Alta	Baixa	Insuficiente
2	Baixa	Baixa	Alta	Média	Regular
3	Baixa	Baixa	Alta	Alta	Muito Ruim
4	Baixa	Baixa	Média	Baixa	Insuficiente
5	Baixa	Baixa	Média	Média	Muito Ruim
6	Baixa	Baixa	Média	Alta	Ruim
7	Baixa	Baixa	Baixa	Baixa	Muito Ruim
8	Baixa	Baixa	Baixa	Média	Ruim
9	Baixa	Baixa	Baixa	Alta	Regular
10	Baixa	Média	Alta	Baixa	Insuficiente
11	Baixa	Média	Alta	Média	Muito Ruim
12	Baixa	Média	Alta	Alta	Ruim
13	Baixa	Média	Média	Baixa	Insuficiente
14	Baixa	Média	Média	Média	Muito Ruim
15	Baixa	Média	Média	Alta	Regular
16	Baixa	Média	Baixa	Baixa	Muito Ruim

17	Baixa	Média	Baixa	Média	Insuficiente
18	Baixa	Média	Baixa	Alta	Muito Ruim
19	Baixa	Alta	Alta	Baixa	Insuficiente
20	Baixa	Alta	Alta	Média	Muito Ruim
21	Baixa	Alta	Alta	Alta	Ruim
22	Baixa	Alta	Média	Baixa	Muito Ruim
23	Baixa	Alta	Média	Média	Ruim
24	Baixa	Alta	Média	Alta	Regular
25	Baixa	Alta	Baixa	Baixa	Muito Ruim
26	Baixa	Alta	Baixa	Média	Regular
27	Baixa	Alta	Baixa	Alta	Bom
28	Média	Baixa	Alta	Baixa	Muito Ruim
29	Média	Baixa	Alta	Média	Ruim
30	Média	Baixa	Alta	Alta	Regular
31	Média	Baixa	Média	Baixa	Muito Ruim
32	Média	Baixa	Média	Média	Regular
33	Média	Baixa	Média	Alta	Bom
34	Média	Baixa	Baixa	Baixa	Ruim
35	Média	Baixa	Baixa	Média	Regular
36	Média	Baixa	Baixa	Alta	Bom
37	Média	Média	Alta	Baixa	Muito Ruim
38	Média	Média	Alta	Média	Ruim
39	Média	Média	Alta	Alta	Regular
40	Média	Média	Média	Baixa	Ruim

41	Média	Média	Média	Média	Regular
42	Média	Média	Média	Alta	Bom
43	Média	Média	Baixa	Baixa	Regular
44	Média	Média	Baixa	Média	Bom
45	Média	Média	Baixa	Alta	Muito Bom
46	Média	Alta	Alta	Baixa	Ruim
47	Média	Alta	Alta	Média	Regular
48	Média	Alta	Alta	Alta	Bom
49	Média	Alta	Média	Baixa	Ruim
50	Média	Alta	Média	Média	Regular
51	Média	Alta	Média	Alta	Muito Bom
52	Média	Alta	Baixa	Baixa	Regular
53	Média	Alta	Baixa	Média	Bom
54	Média	Alta	Baixa	Alta	Ótimo
55	Alta	Baixa	Alta	Baixa	Ruim
56	Alta	Baixa	Alta	Média	Regular
57	Alta	Baixa	Alta	Alta	Muito Bom
58	Alta	Baixa	Média	Baixa	Regular
59	Alta	Baixa	Média	Média	Bom
60	Alta	Baixa	Média	Alta	Ótimo
61	Alta	Baixa	Baixa	Baixa	Bom
62	Alta	Baixa	Baixa	Média	Muito Bom
63	Alta	Baixa	Baixa	Alta	Excelente
64	Alta	Média	Alta	Baixa	Regular

65	Alta	Média	Alta	Média	Bom
66	Alta	Média	Alta	Alta	Regular
67	Alta	Média	Média	Baixa	Regular
68	Alta	Média	Média	Média	Muito Bom
69	Alta	Média	Média	Alta	Ótimo
70	Alta	Média	Baixa	Baixa	Bom
71	Alta	Média	Baixa	Média	Ótimo
72	Alta	Média	Baixa	Alta	Excelente
73	Alta	Alta	Alta	Baixa	Regular
74	Alta	Alta	Alta	Média	Bom
75	Alta	Alta	Alta	Alta	Ótimo
76	Alta	Alta	Média	Baixa	Bom
77	Alta	Alta	Média	Média	Muito Bom
78	Alta	Alta	Média	Alta	Excelente
79	Alta	Alta	Baixa	Baixa	Muito Bom
80	Alta	Alta	Baixa	Média	Ótimo
81	Alta	Alta	Baixa	Alta	Excelente

Tabela 9 – Regras do Sistema *Fuzzy* para classificação do grau de confiabilidade para RSSF

APÊNDICE B – Atribuição de valores para a variável de saída do Sistema *Fuzzy*

REGRA	CONFIABILIDADE	ACURÁCIA	LATÊNCIA	EFICIÊNCIA	TOTAL
1	0	0	0	0	0
2	0	0	0	1,5	1,5
3	0	0	0	3	3
4	0	0	1	0	1
5	0	0	1	1,5	2,5
6	0	0	1	3	4
7	0	0	2	0	2
8	0	0	2	1,5	3,5
9	0	0	2	3	5
10	0	0,5	0	0	0,5
11	0	0,5	0	1,5	2
12	0	0,5	0	3	3,5
13	0	0,5	1	0	1,5
14	0	0,5	1	1,5	3
15	0	0,5	1	3	4,5
16	0	0,5	2	0	2,5
17	0	0,5	2	1,5	4
18	0	0,5	2	3	5,5
19	0	1	0	0	1
20	0	1	0	1,5	2,5
21	0	1	0	3	4
22	0	1	1	0	2
23	0	1	1	1,5	3,5
24	0	1	1	3	5
25	0	1	2	0	3
26	0	1	2	1,5	4,5
27	0	1	2	3	6
28	2	0	0	0	2
29	2	0	0	1,5	3,5

30	2	0	0	3	5
31	2	0	1	0	3
32	2	0	1	1,5	4,5
33	2	0	1	3	6
34	2	0	2	0	4
35	2	0	2	1,5	5,5
36	2	0	2	3	7
37	2	0,5	0	0	2,5
38	2	0,5	0	1,5	4
39	2	0,5	0	3	5,5
40	2	0,5	1	0	3,5
41	2	0,5	1	1,5	5
42	2	0,5	1	3	6,5
43	2	0,5	2	0	4,5
44	2	0,5	2	1,5	6
45	2	0,5	2	3	7,5
46	2	1	0	0	3
47	2	1	0	1,5	4,5
48	2	1	0	3	6
49	2	1	1	0	4
50	2	1	1	1,5	5,5
51	2	1	1	3	7
52	2	1	2	0	5
53	2	1	2	1,5	6,5
54	2	1	2	3	8
55	4	0	0	0	4
56	4	0	0	1,5	5,5
57	4	0	0	3	7
58	4	0	1	0	5
59	4	0	1	1,5	6,5
60	4	0	1	3	8
61	4	0	2	0	6
62	4	0	2	1,5	7,5
63	4	0	2	3	9
64	4	0,5	0	0	4,5
65	4	0,5	0	1,5	6
66	4	0,5	0	3	7,5

67	4	0,5	1	0	5,5
68	4	0,5	1	1,5	7
69	4	0,5	1	3	8,5
70	4	0,5	2	0	6,5
71	4	0,5	2	1,5	8
72	4	0,5	2	3	9,5
73	4	1	0	0	5
74	4	1	0	1,5	6,5
75	4	1	0	3	8
76	4	1	1	0	6
77	4	1	1	1,5	7,5
78	4	1	1	3	9
79	4	1	2	0	7
80	4	1	2	1,5	8,5
81	4	1	2	3	10

Tabela 10 – Atribuição de valores para a variável de saída do Sistema *Fuzzy*

APÊNDICE C – Estado e Pesos para atribuição de valores para a variável de saída do Sistema *Fuzzy*

Definição de estado das variáveis de saída do Sistema *Fuzzy*	
Excelente	9 a 10
Ótimo	8 a 8,9
Muito Bom	7 a 7,9
Bom	6 a 6,9
Regular	4,5 a 5,5
Ruim	3,5 a 4,4
Muito Ruim	2 a 3,4
Insuficiente	0 a 1,9

Tabela 11 – Estados da variável de saída

ASPECTOS	Total	Alta	Média	Baixa
Confiabilidade	4	4	2	0
Acurácia	1	1	0,5	0
Latência	2	2	1	0
Eficiência	3	3	1,5	0

Tabela 12 – Pesos para definição de saída