



Universidade do Estado do Rio de Janeiro

Centro de Tecnologia e Ciência

Faculdade de Engenharia

Luciane Fernanda de Arruda Barreira


**Determinação de posicionamento de nós roteadores em redes
sem fio utilizando redes imunológicas**

Rio de Janeiro

2013

Luciane Fernanda de Arruda Barreira

**Determinação de posicionamento de nós roteadores em redes
sem fio utilizando redes imunológicas**



Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao programa de Pós-Graduação em Engenharia Eletrônica da Universidade do Estado do Rio de Janeiro. Área de concentração: Sistemas Inteligentes e Automação.

Orientador: Prof. Dr. Jorge Luís Machado do Amaral

Rio de Janeiro

2013

CATALOGAÇÃO NA FONTE
UERJ / REDE SIRIUS / BIBLIOTECA CTC / B

B272 Barreira, Luciane Fernanda de Arruda.
Determinação de posicionamento de nós roteadores em redes sem fio utilizando redes imunológicas / Luciane Fernanda de Arruda Barreira. - 2013.
97f.

Orientador: Jorge Luís Machado do Amaral.
Dissertação (Mestrado) – Universidade do Estado do Rio de Janeiro, Faculdade de Engenharia.

1. Engenharia Eletrônica. 2. Posicionamento de nós roteadores – Dissertação. 3. Rede Industrial – Dissertação. I. Amaral, Jorge Luís Machado do. II. Universidade do Estado do Rio de Janeiro. III. Título.

CDU 621.38

Autorizo, apenas para fins acadêmicos e científicos, a reprodução total ou parcial desta dissertação, desde que citada a fonte.

Assinatura

Data

Luciane Fernanda de Arruda Barreira

**Determinação de posicionamento de nós roteadores em redes
sem fio utilizando redes imunológicas**

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao programa de Pós-Graduação em Engenharia Eletrônica da Universidade do Estado do Rio de Janeiro. Área de concentração: Sistemas Inteligentes e Automação.

Aprovado em: 24 de Julho de 2013.

Banca Examinadora:

Prof. Dr. Jorge Luís Machado do Amaral. (Orientador)
Faculdade de Engenharia – UERJ

Prof. Dr. Pedro Henrique Gouvêa Coelho
Faculdade de Engenharia – UERJ

Prof. Dr. Felipe Maia Galvão França
Universidade Federal do Rio de Janeiro - UFRJ / COPPE

Rio de Janeiro

2013

DEDICATÓRIA

Dedico esta dissertação a todas as pessoas que durante este tempo estiveram ao meu lado me apoiando, dando forças e me ajudando a vencer mais essa etapa. Essas pessoas tão importantes na minha vida são: meu filho Lucas Barreira, minha mãe Maria Lucila Arruda, minhas amigas Mara Mello e Natália Mello, meu amigo Michelangelo Bianchi, meu orientador Professor Jorge Amaral e principalmente a Deus.

AGRADECIMENTOS

Durante esse longo tempo de estudo várias pessoas passaram pela minha vida. Cada uma me ensinou e contribuiu de alguma forma para que esse sonho se tornasse possível. Estarei aqui mencionando algumas delas, mas deixo o meu agradecimento a todos.

Agradeço:

À Deus por me fortalecer, cuidar, incentivar e encorajar durante toda a minha vida, e coloca na vida pessoas maravilhosas.

Ao meu filho Lucas Barreira por todo carinho, amor e compreensão pela minha ausência e falta de tempo.

À minha mãe Maria Lucila Arruda por me ajuda a cuida do meu filho, e muitas das vezes ter sido também mãe dele, pelas orações, pelo amor, compressão e incentivo.

A todos os meus amigos que sempre me incentivaram, apoiaram, ajudaram e motivaram, em especial a Natália Mello, Mara Mello, Letícia Guimarães e Michelangelo Bianchi.

Aos meus afilhados Thalles Fonseca, Gabriel Ozolins, Jéssyca Soares, Natália Mello, Érika Oliveira e Flávia Karoline por entenderem a minha ausência.

Ao meu amigo Ronaldo Allencar e aos colegas do curso de pós-graduação pela ajuda e apoio.

A todos os professores da UERJ por compartilhar os seus conhecimentos a todos os alunos com dedicação, amor e paciência. Em especial ao meu orientador Professor Jorge Amaral por me ajudar, apoiar e compartilhar todo o seu conhecimento com dedicação, atenção e paciência.

A todos os funcionários da UERJ que cuidaram das nossas salas de aula, para que estivessem em perfeito estado para as aulas, e aos secretários pela atenção.

À minha comunidade da paróquia Cristo Rei pelas orações, compressão, apoio, incentivo e motivação.

RESUMO

BARREIRA, Luciane F. A. *Determinação de posicionamento de nós roteadores em redes sem fio utilizando redes imunológicas*. 2013. 97f. Dissertação (Mestrado em Engenharia Eletrônica) – Faculdade de Engenharia, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2013.

A tecnologia sem fio (*wireless*) vem tomando conta do mundo. A cada dia mais pessoas estão trocando seus equipamentos com fio por equipamentos com a tecnologia *wireless*. Isso vem crescendo, devido as suas vantagens, tais como: facilidade de instalação e manutenção, redução de tempo de instalação de dispositivos, inexistência de estrutura de cabeamento, economia no custo de projetos, economia em infraestrutura, flexibilidade de configuração de dispositivos, economia no custo de montagem, flexibilidade na alteração de arquiteturas existentes e outros. Por essas facilidades supracitadas a área de automação industrial está também aumentando o seu interesse nessa tecnologia *wireless*. Nessa área, a segurança, confiabilidade e robustez dos dados são de suma importância. Então, para minimizar os efeitos das interferências geradas nesse meio são usadas técnicas de espalhamento em frequência e topologia em malha ou árvore para transmissão dos dados enviados pelos sensores aos nós roteadores até chegar ao *gateway*. Sendo assim, o posicionamento dos nós roteadores na rede em malha garantirá a menor influência dessas interferências. Esse trabalho propõe uma ferramenta de posicionamento de nós roteadores intermediários, chamado POSIMNET (*Positioning Immune Network* – Rede Imunológica de Posicionamento), que auxilia o projetista da rede de automação industrial a encontrar a melhor configuração da rede sem fio. O POSIMNET é baseado nas redes imunológicas artificiais, que propõe criar n caminhos quaisquer ou disjuntos para as informações enviadas pelos nós sensores chegarem ao *gateway*, através da supressão, clonagem e reconfiguração de nós roteadores intermediários. Além disso, o algoritmo também é capaz de atender os critérios de baixo grau de falha e baixo número de retransmissão pelos roteadores. Esses critérios podem ser habilitados individualmente ou combinados com pesos iguais ou diferentes para cada um, a critério do usuário. A ferramenta POSIMNET é formada por dois módulos: (i) Rede Imunológica – agrega elementos de dois modelos de redes imunológicas (SSAIS e AiNet); (ii) Campos Potenciais - posiciona os nós roteadores pelos campos potenciais, onde os sensores críticos os atraem enquanto que os obstáculos e outros roteadores os repelem.

Palavras-Chave: Posicionamento de nós roteadores; Automação industrial, Redes imunológicas; Campos potenciais.

ABSTRACT

The use of wireless transmission is part of everyone's life. Every day more people are exchanging their wired devices to wireless technology. This is due to their advantages, such as ease of installation and maintenance, reducing installation time devices, cost savings projects, economic infrastructure, device configuration flexibility, savings in assembly cost, flexibility in altering existing architectures and others. Now the area of industrial automation is also increasing interest in this technology wireless. In this area the safety, reliability and robustness of data is of great importance. So in order to minimize the effects of interferences scattering techniques in frequency and mesh topology are used for transmission of data from the sensors to the router nodes to reach the gateway. Thus, the positioning of the nodes in the mesh network routers ensures that the network will present a good performance. This work proposes a tool for positioning intermediate routers in mesh networks, called POSIMNET (Immune Network Positioning), which assists the designer to find the best configuration of the industrial automation wireless network. The POSIMNET is based on artificial immune networks, which proposes to create n paths between the sensor nodes and the gateway by removing, cloning and reconfiguration of intermediate routers. Furthermore, the algorithm is also able to meet the criteria for low-grade failure and low number of retransmission by routers. These criteria can be enabled individually or combined with equal or different weights at user's discretion. The POSIMNET tool consists of two modules: (i) Immune Network – which combines elements of two models of immune networks (SSAIS and AINET), (ii) Potential Fields - positions router nodes using potential fields, where critic sensors attracts them while obstacles and other network elements repel them.

Keywords: Placement of router nodes; Industrial Automation, immune Network; Potential fields.

LISTA DE ILUSTRAÇÃO

Figura 1 – Elementos da Rede de Sensores.....	17
Figura 2 – Estrutura do WirelessHART (HART Communication Foundation, 2011).....	19
Figura 3 – Características da uma rede em malha.....	22
Figura 4 – Ilustração da Condição Net (Adaptado de Poduri at al, 2006).....	25
Figura 5 – Arquitetura de combate ao agente invasor (Castro & Von Zuben, 1999).....	30
Figura 6 – Reconhecimento de um antígeno através da célula B (Castro, 2001).....	32
Figura 7 – Processo de maturação de afinidade (Bradley, 2000b).....	33
Figura 8 – Rede Imunológica (Castro, 2001). (a) Célula B com o seu paratopo e idiotopo; (b) Estimulo (resposta positiva) ou inibição (resposta negativa) resultante da tentativa da união do paratopo com o idiotopo ou do paratopo com a epítipo do antígeno.....	35
Figura 9 – Algoritmo de Rede Imunológica Artificial Geral (Versão Traduzida de (Galeano, 2005)).....	38
Figura 10 – Árvore genealógica dos modelos de redes imunológicas (Galeano, 2005).....	39
Figura 11 – Etapas do SSAIS (Versão traduzida de Neal, 2002).....	40
Figura 12 – Pseudocódigo do AiNet (Castro, 2001).....	42
Figura 13 – Configuração da rede. (a) Sem caminhos redundantes; (b) Com caminhos redundantes.....	43
Figura 14 – Fluxograma do POSIMNET.....	46
Figura 15 – Ilustração da Condição Net com ângulos $\theta=120^\circ$. (a) $\beta_1=30^\circ$; (b) $\beta_2=60^\circ$; (c) $\beta_3=90^\circ$	52
Figura 16 – Posicionamento dos nós sensores e do <i>gateway</i> . (a) POSA; (b) POSB.....	57
Figura 17 - Estudo do Caso 1 – Cenário POSA.....	60
Figura 18 – Trace do Caso 1.....	61
Figura 19 - Estudo do Caso 2 – Cenário POSA.....	63
Figura 20 – Trace do Caso 2.....	64
Figura 21 - Estudo do Caso 3 – Cenário POSA.....	66
Figura 22 – Trace do Caso 3.....	67
Figura 23 - Estudo do Caso 4 – Cenário POSA.....	69
Figura 24 – Trace do Caso 4.....	70
Figura 25 - Estudo do Caso 5 – Cenário POSB.....	73
Figura 26 – Trace do Caso 5.....	74

Figura 27 - Estudo do Caso 6 – Cenário POSB. (a) Configuração de rede final; (b) Configuração de rede final ampliada.....	78
Figura 28 – Trace do Caso 6.....	78
Figura 29 – Cenário com Obstáculos. (a) Cenário com dois obstáculos circulares; (b) Obstáculos com quatro obstáculos circulares e quatro obstáculos retangulares....	80
Figura 30 - Estudo do Caso 7 – Cenário com Obstáculos	82
Figura 31 – Trace do Cenário Completo	83
Figura 32 - Estudo de Caso 8 – Cenário POSC.....	86
Figura 33 – Trace do Cenário POSC	87

LISTA DE TABELAS

Tabela 1 – Estudo de Casos - Cenário	58
Tabela 2 – Caso 1 – Cenário – Parâmetros.....	58
Tabela 3 – Desempenho da Rede	59
Tabela 4 – Caso 2 – Cenário – Parâmetros.....	62
Tabela 5 – Desempenho da Rede	63
Tabela 6 – Caso 3 – Cenário – Parâmetros.....	65
Tabela 7 – Desempenho da Rede	66
Tabela 8 – Caso 4 – Cenário – Parâmetros.....	68
Tabela 9 – Desempenho da Rede	69
Tabela 10 – Caso 5 – Cenário – Parâmetros.....	71
Tabela 11 – Desempenho da Rede	72
Tabela 12 – Caso 6 – Cenário – Parâmetros.....	75
Tabela 13 – Desempenho da Rede	76
Tabela 14 – Caso 7 – Cenário – Parâmetros.....	81
Tabela 15 – Desempenho da Rede	82
Tabela 16 – Caso 8 – Cenário – Parâmetros.....	84
Tabela 17 – Desempenho de Rede	85
Tabela 18 – Tabela Comparativa.....	89

LISTA DE ABREVIACOES

AES	<i>Advanced Encryption Standard</i>
AIN	<i>Artificial Immune Network</i>
AiNet	<i>Artificial Immune Network</i>
AIS	<i>Artificial Immune System</i>
ARB	<i>Artificial Recognition Ball</i>
CLONALG	<i>CLONal selection ALGorithm</i>
DSSS	<i>Direct Sequence Spread Spectrum</i>
GAIN	<i>General Model of AIN</i>
HART	<i>Highway Addressable Remote Transducer</i>
ISM	<i>Industrial, Scientific and Medical</i>
MANET	<i>Mobile Ad Hoc Network</i>
MIC	<i>Message Integrity Code</i>
NET	<i>Neighbor-Every-Theta</i>
NSA	<i>Negative Selection Algorithm</i>
NSDR	<i>Negative Selection with Detection Rules</i>
POSIMNET	<i>Positioning Immune Network</i>
QoS	<i>Quality of Service</i>
RNSA	<i>Real Valued Negative Selection Algorithm</i>
RSSF	<i>Rede de Sensores sem Fio</i>
SSAIS	<i>Self-Stabilising Artificial Immune System</i>
TDMA	<i>Time Division Multiple Access</i>

SUMÁRIO

	INTRODUÇÃO	13
1	POSICIONAMENTO DE NÓS ROTEADORES EM REDES SEM FIO PARA AUTOMAÇÃO INDUSTRIAL.....	16
1.1	Conceitos Básicos sobre Redes de Sensores Sem Fio para Automação.....	16
1.2	Visão Geral do WirelessHART	18
1.3	Descrição do Problema de Posicionamento de Nós	21
1.4	Soluções Encontradas para o Problema de Posicionamento	22
1.5	O Problema de Posicionamento de Nós em Redes de Automação	26
2	O SISTEMA IMUNOLÓGICO	29
2.1	Visão Geral do Sistema Imunológico.....	30
2.1.1	<u>Células B no Reconhecimento de Agente Patogênico</u>	31
2.1.2	<u>Distinção entre o Próprio e Não-Próprio.....</u>	32
2.1.3	<u>Maturação de Afinidade / Seleção Clonal.....</u>	33
2.1.4	<u>Memória Imunológica</u>	34
2.1.5	<u>Redes Imunológicas</u>	34
2.2	Sistemas Imunológicos Artificiais	36
2.2.1	<u>Modelos de Redes Imunológicas.....</u>	36
2.2.1.1	Algoritmo SSAIS	39
2.2.1.2	Algoritmo AiNet.....	40
3	POSICIONAMENTO DE NÓS USANDO REDES IMUNOLÓGICAS	43
3.1	Modelagem do Problema	43
3.2	Descrição da Ferramenta.....	45
3.2.1	<u>Formulação das Afinidades</u>	47
3.2.2	<u>A Etapa de PODA</u>	49
3.2.3	<u>As Etapas de Seleção, Clonagem e Mutação</u>	49
3.2.3.1	ClonaHyper	50
3.2.3.2	ClonaCondicaoNet	51
3.2.4	<u>Módulo de Posicionamento por Campos Potenciais</u>	52
4	ESTUDO DE CASOS.....	56
4.1	Descrição dos Estudos de Casos	56
4.2	Estudo de Casos nos Cenários POSA e POSB.....	56
4.2.1	<u>Estudo de Caso 1 – Cenário POS A</u>	58

4.2.2	<u>Estudo de Caso 2 – Cenário POS A</u>	61
4.2.3	<u>Estudo de Caso 3 – Cenário POS A</u>	64
4.2.4	<u>Estudo de Caso 4 – Cenário POS A</u>	67
4.2.5	<u>Estudo de Caso 5 – Cenário POS B</u>	70
4.2.6	<u>Estudo de Caso 6 – Cenário POS B</u>	74
4.3	Estudo de Caso em Cenários com Obstáculos	78
4.3.1	<u>Estudo de Caso 7 – Cenário com Dois Obstáculos Circulares</u>	80
4.3.2	<u>Estudo de Caso 8 – Cenário POSC</u>	83
5	CONCLUSÕES	88
5.1	Resultados	88
5.2	Trabalhos Futuros	89
	REFERÊNCIAS	91

INTRODUÇÃO

A transmissão de dados através da utilização da tecnologia sem fio (*wireless*) vem crescendo vertiginosamente na sociedade. Novos equipamentos sem fio surgem a todo o momento e outros equipamentos cabeados são modernizados para a tecnologia *wireless*. Hoje em dia é inacreditável, por exemplo, que para uma pessoa realizar uma ligação telefônica, ela precise estar em um local fixo, sem mobilidade nenhuma. Ou mesmo, que para acessar a internet, ela precise estar no seu escritório ou na sua casa. O mundo vive hoje a febre da conectividade móvel, onde a utilização dos equipamentos sem fio é a primeira opção entre os meios convencionais, se tornando quase uma obrigatoriedade.

A tecnologia wireless tem tomado conta do mundo e a área de automação industrial não poderia ficar de fora, uma vez que esta tecnologia possui grandes atrativos para a área de automação, tais como: redução de tempo de instalação de dispositivos, inexistência de estrutura de cabeamento, economia no custo de projetos, economia em infraestrutura, flexibilidade de configuração de dispositivos, economia no custo de montagem, flexibilidade na alteração de arquiteturas existentes, possibilidade de instalação de sensores em locais de difícil acesso e outras, a utilização de equipamentos sem fio nesta área vem ao longo do tempo aumentando e tomando o seu espaço (Costa & Amaral, 2012).

Na área de automação industrial são de suma importância a segurança, confiabilidade, disponibilidade, robustez e desempenho da rede na realização do monitoramento e controle do processo. Ou seja, a rede não pode ser sensível às interferências e nem parar o seu funcionamento por causa da falha de um equipamento, tampouco pode ter alta latência na transmissão dos dados e garantir que as informações não sejam extraviadas (Zheng & Myung, 2006), (Santos, 2007).

No ambiente de automação industrial, a transmissão de dados em uma rede sem fio se depara com o problema de interferências, geradas por outros equipamentos eletromagnéticos, tais como, rádios de comunicação, outras redes de comunicação sem fio e equipamentos elétricos, e obstáculos móveis (caminhões, guindastes, etc) e fixos (prédios, tubulações, tanques, etc). Na tentativa de minimizar esses efeitos são utilizadas técnicas de espalhamento em frequência e topologias em malha ou árvore em que uma mensagem pode ser transmitida de um nó para outro com auxílio de outros nós, que funcionam como roteadores intermediários, direcionando as mensagens para outros nós até que ela chegue a seu destino.

Isto permite que a rede obtenha um maior alcance e seja mais tolerante a falhas, pois se um nó intermediário apresentar uma falha ou não puder receber uma mensagem, esta pode ser roteada para outro nó (Costa & Amaral, 2010). Entretanto, uma rede em malha também exige um estudo cuidadoso do posicionamento destes nós intermediários, uma vez que eles são responsáveis por fazer o encaminhamento dos dados gerados pelos sensores da rede até o *gateway* de forma direta ou indireta, através de saltos. São dispositivos responsáveis por atender o critério de segurança, confiabilidade e robustez da rede e de suma importância no direcionamento da transmissão dos dados. No entanto, podem deixar parte da rede ou toda ela inoperante, caso apresentem qualquer falha (Hoffert et al., 2007).

A maioria das soluções encontradas para o posicionamento de nós roteadores resolvem esse problema com algoritmos de otimização que minimizam a quantidade de nós roteadores intermediários para atender o critério de cobertura, conectividade da rede, longevidade da rede e fidelidade dos dados. (Youssef & Younis, 2007), (Molina et al., 2008) (Costa & Amaral, 2010). Porém, nenhum dos artigos estudados propõe atender o critério de tolerância a falhas, através da redundância de n caminhos, isto é garantir que cada elemento sensor da rede formada, tenha pelo menos n caminhos até o gateway, seja por conexão direta ou através de nós intermediários.

Nesta dissertação, propõe-se resolver este problema utilizando Redes Imunológicas Artificiais, baseadas no sistema imunológico humano. Os algoritmos baseados em redes imunológicas possuem características bastante desejáveis na solução deste problema, dentre as quais, podemos citar: escalabilidade, auto-organização, habilidade de aprendizado contínuo e tratamento de dados ruidosos.

Nesta dissertação o algoritmo proposto é POSIMNET (*Positioning Immune Network – Rede Imunológica de Posicionamento*). Ele é uma ferramenta de posicionamento de nós roteadores intermediários que auxilia o projetista da rede a encontrar a melhor configuração da rede sem fio, de forma que as informações coletadas pelos nós sensores cheguem ao *gateway* por n caminhos diferentes, criando uma rede tolerante à falha dos nós.

Esta dissertação está organizada em cinco capítulos que serão apresentados a seguir:

O Capítulo 1 apresenta os conceitos básicos de rede de sensores sem fio, os artigos estudados sobre a solução do problema de posicionamento dos elementos da rede sem fio e os conceitos de rede de sensores para aplicação de automação industrial. Ao fim, o leitor terá a

noção geral do problema de posicionamento de nós roteadores em redes sem fio para automação industrial. No Capítulo 2 são apresentados os conceitos necessários para o entendimento do algoritmo proposto. Tal apresentação descreve alguns aspectos do sistema imunológico humano e de que forma estes aspectos foram incorporados em algoritmos inspirados nos sistemas imunológicos. O Capítulo 3 descreve o algoritmo de rede imunológica proposto por esta dissertação. No Capítulo 4 serão detalhados os estudos de casos que comprovam que o algoritmo POSIMNET, proposto por essa dissertação, é capaz de resolver o problema de redundância de caminhos em redes sem fio para automação industrial. Concluímos o trabalho no Capítulo 5, com a explanação dos resultados obtidos e propondo trabalhos futuros.

1 POSICIONAMENTO DE NÓS ROTEADORES EM REDES SEM FIO PARA AUTOMAÇÃO INDUSTRIAL

Este capítulo descreve os conceitos básicos sobre redes de sensores sem fio para automação, uma visão geral do protocolo *WirelessHART*, a descrição do problema de posicionamento de nós, as soluções encontradas para o problema e, por fim, o problema de posicionamento de nós em redes de automação.

1.1 Conceitos Básicos sobre Redes de Sensores Sem Fio para Automação

Uma rede de sensores sem fio (RSSF) é uma rede autônoma de sensores inteligentes e com alto grau de cooperação entre si. Ela é responsável por realizar o monitoramento de um processo ou de um ambiente, processar a informação coletada, classificar o grau de importância da informação, e caso seja importante, difundi-la aos outros sensores ou roteadores mais próximos ao *gateway*. A grande vantagem de não utilizar cabos na transmissão de dados é a facilidade de instalação da rede em todos os ambientes, incluindo aqueles onde não é possível a passagem de cabos, seja pela dificuldade de acesso, ou por se tratar de área perigosa ou classificada. Outra vantagem é a facilidade de manutenção dos equipamentos (Loureiro et al, 2003) (Younis & Akkaya, 2008).

A rede de sensores é formada pelos elementos: sensor, observador, fenômeno, roteador e gateway, conforme ilustrado na Figura 1 (Pereira et al, 2012).

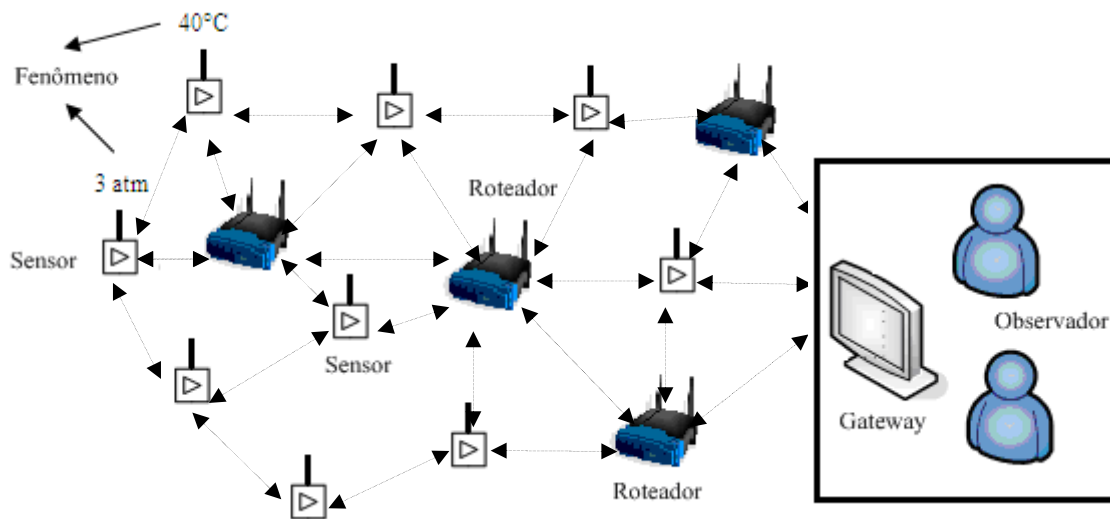


Figura 1 – Elementos da Rede de Sensores

O elemento sensor é o dispositivo responsável por realizar as medições das grandezas físicas dos fenômenos de mudança de fluxo, de pressão, de temperatura e de nível dos processos de produção industrial, e gerar relatórios de medidas através da difusão do sinal. Para cada tipo de fenômeno, existe um tipo diferente de sensor, que apresenta característica física específica do processo. Ele é composto por transceptor, memória, processador, bateria e detector do fenômeno.

O elemento observador é um usuário, ou múltiplos usuários, que recebem e/ou solicitam, quando necessário, as informações dos fenômenos coletadas pelos elementos sensores e difundidas pela rede de sensores sem fio.

O elemento fenômeno é o processo que será monitorado pelo elemento sensor, e difundido pela rede de sensores sem fio para avaliação final do elemento observador. A rede de sensores sem fio poderá coletar amostras discretas de múltiplos fenômenos, sujeito a precisão de cada elemento sensor.

O elemento roteador direciona a informação gerada pelo elemento sensor ao elemento da rede mais próximo e dentro do seu raio de transmissão, de forma que a informação possa chegar ao nó central (*gateway*).

O elemento *gateway*, ou nó central, é responsável por receber todas as informações eletromagnéticas enviadas pelos nós sensores, decodificá-las em grandezas físicas do fenômeno monitorado de forma que o observador seja capaz de entendê-los e acionar o alarme, caso a grandeza física esteja fora do parâmetro aceitável.

Ela é aplicada em diversas áreas como, por exemplo, monitoramento de florestas, gerenciamento de desastres, exploração espacial, proteção de fronteiras, vigilância de campo de batalha, automação industrial, monitoramento de tráfego e outros (Younis & Akkaya, 2008; Loureiro et al, 2003; Costa, 2011). Na maioria das aplicações, o monitoramento do fenômeno desejado é realizado por um tipo ou um conjunto de tipo de sensores (acústico, sísmico, infravermelho, vídeo-câmera, calor, etc) agrupados em *cluster*. Além disso, a rede pode ser composta por centenas de nós, de baixo custo, que operam com o menor consumo de energia possível para prolongar o tempo de vida de cada nó e que obtêm a maior cobertura possível do fenômeno.

1.2 Visão Geral do *WirelessHART*

O primeiro padrão, chamado *WirelessHART* (*Wireless Highway Addressable Remote Transducer*), para comunicação sem fio em controle de processos foi lançado em setembro de 2007 pela HART Communication Foundation. Ele incorpora no padrão HART de dispositivos com capacidade de transmissão de dados sem fio. No *WirelessHART*, cada dispositivo da topologia de rede em malha possui um mecanismo de roteamento de mensagens, que repassa os pacotes de informações a outros dispositivos até chegar ao *gateway*. Essa funcionalidade dos dispositivos faz com que o alcance da rede se torne extenso, além de criar alternativas de rotas redundantes de comunicação, aumentando a confiabilidade da rede (Costa & Amaral, 2012).

A arquitetura da rede *WirelessHART* apresenta os seguintes elementos de rede, conforme Figura 2 (HART Communication Foundation, 2011):

Dispositivos de campo sem fio – os dispositivos de campo são os dispositivos conectados diretamente ao processo ou a outro equipamento da rede. Eles são responsáveis por realizar a medição dos fenômenos, processá-los e difundi-los para os outros dispositivos. Além disso, eles também podem exercer a função de roteamento das informações enviadas por outros dispositivos.

O *Gateway* – é o elemento responsável por realizar a interligação da rede sem fio com o controlador de automação de processo e com as aplicações hosts, tais como, Sistemas de Automação de Processo ou Sistemas de Gerenciamento de Ativos.

O *Network Manager* é uma das funcionalidades lógicas do *Gateway*, que é responsável pelo sincronismo entre os dispositivos da rede, pela configuração da rede, pelo gerenciamento das tabelas de rotas e pelo monitoramento do estado dos dispositivos da rede (Costa & Amaral, 2012).

Security Manager – é a segunda funcionalidade lógica do *Gateway*, que é responsável pela geração, armazenamento, gerenciamento e distribuição das chaves utilizadas na autenticação de dispositivos e na criptografia de dados da rede (Costa & Amaral, 2012).

Wireless Handheld – este elemento é um dispositivo portátil que se conecta aos dispositivos de campo com a finalidade de configurá-los, calibrá-los, diagnosticar problemas na rede e gerenciar as informações da rede.

Wireless Adapter – este dispositivo tem a função de adaptar os dispositivos com fio à rede de sensores sem fio, fornecendo conectividade física e lógica ao dispositivo que não seja *WirelessHART*.

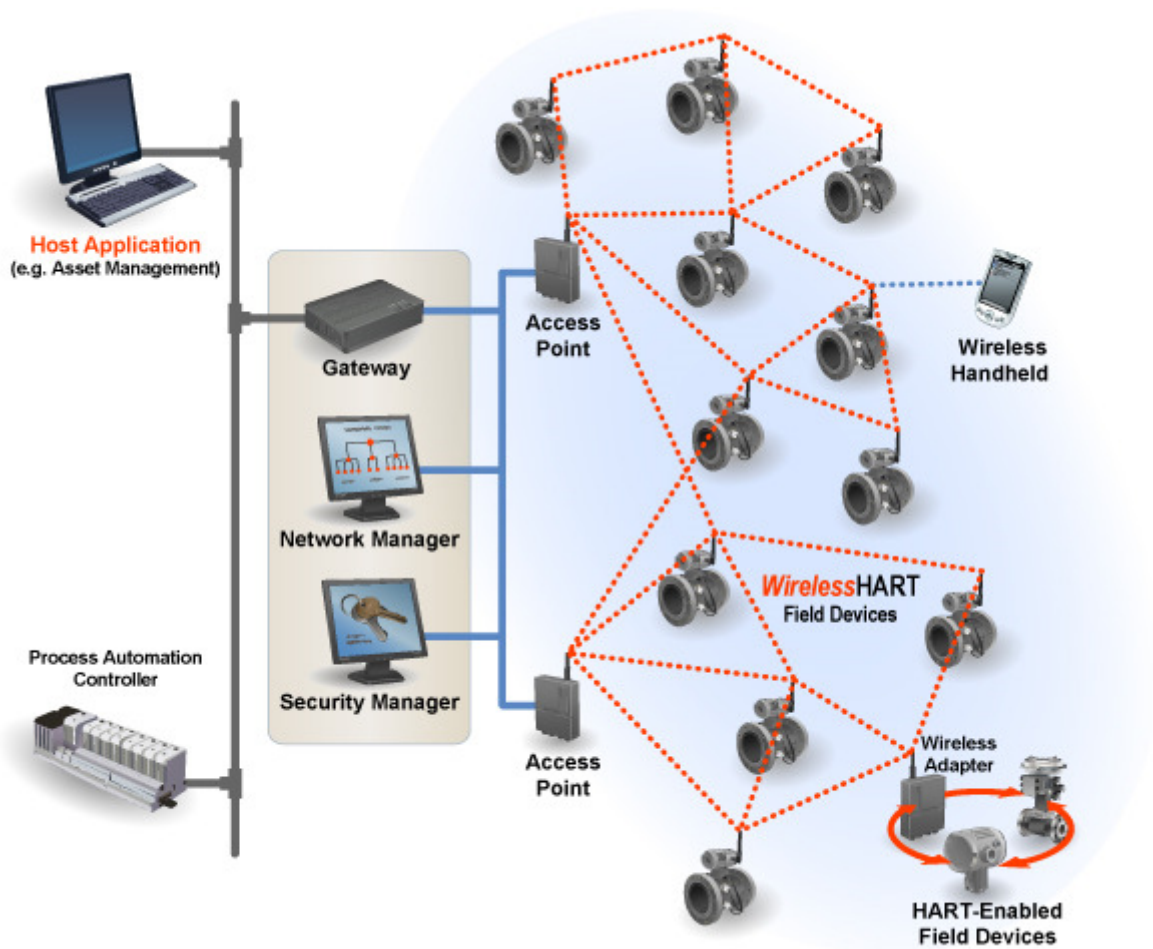


Figura 2 – Estrutura do WirelessHART (HART Communication Foundation, 2011)

O *WirelessHART*, como supracitado, é um padrão para comunicação de rede sem fio com aplicação em automação de processos. O *WirelessHART* utiliza a interface de rádio IEEE 802.15.4, com objetivo de atender a premissas de baixo consumo de energia e baixa manutenção. Os seus rádios operam em uma faixa de frequência livre de 2.407 a 2.447 GHz (largura de banda de 40 MHz) na banda ISM (*Industrial, Scientific and Medical*), dividida em 16 canais, com taxa de transmissão bruta de 250 kbps, utilizando as técnicas de modulação DSSS (*Direct Sequence Spread Spectrum*) e de salto de canais (*channel hopping*), para evitar interferências, perturbações e colisões com outros sistemas de comunicação. Além disso, a sua comunicação é coordenada com TDMA (*Time Division Multiple Access*), onde a duração do slot de tempo é fixa e igual a 10 ms e seus *superframes* são repetidos para suportar diferentes tipos de tráfegos de comunicação da rede (HART Communication Foundation, 2011).

No aspecto de segurança, o *WirelessHART* utiliza o esquema de criptografia AES-128 e o MIC (*Message Integrity Code*) combinados para garantir a integridade e fazer a autenticação em diferentes camadas em conjunto com as chaves apropriadas (*Network Key e Session Key*). Quando um dispositivo deseja entrada na rede, o mesmo envia um pedido de entrada (*join request*) e recebe uma resposta (*join response*) do *Network manager*. Além disso, para aumentar a segurança, o *WirelessHART* fornece para cada dispositivo ou para toda rede, de acordo com a política de segurança da rede, a chave *Join Key*. A chave *Join Key* é responsável por autenticar o dispositivo no processo de sua adesão à rede (Costa, 2011).

O padrão *WirelessHART* apresenta uma topologia de rede em malha, conforme ilustrado na Figura 2, onde cada dispositivo da rede serve como roteador para a informação dos outros dispositivos até chegar ao nó central, através de múltiplos saltos. Esse tipo de topologia faz com que a rede tenha uma maior cobertura, seja menos sensível às interferências causadas por obstáculos ou por ondas eletromagnéticas e tenha caminhos alternativos em caso de falha de um equipamento (Costa & Amaral, 2012).

Pelo exposto anteriormente, pode-se dizer que o *WirelessHART* é um padrão que apresenta as seguintes vantagens: gerenciamento eficaz de energia, confiabilidade, mesmo na presença de interferência causadas por obstáculos ou ondas eletromagnéticas, segurança e privacidade para a comunicação da rede. Em contrapartida às suas vantagens, o padrão *WirelessHART* apresenta algumas questões que ainda precisam ser equalizadas como, por exemplo: estar preparado para atender requisitos de tempo real na faixa de 1 a 10 ms, oferecer garantia de qualidade de serviço em redes heterogêneas, diminuir os efeitos de ataques de colisão e de inundação de pedidos de conexão e a reduzida quantidade de ferramentas de

projeto de rede (Costa & Amaral, 2012). Ao longo dos anos, a HART Communication Foundation vem realizando estudos no padrão *WirelessHART* na tentativa de equalizar as questões supracitadas.

1.3 Descrição do Problema de Posicionamento de Nós

As redes de sensores sem fio, geralmente, apresentam uma grande densidade de sensores posicionados em uma determinada região de interesse. Nessas redes, existe um conjunto de nós sensores organizados em um agrupamento, onde os sensores detectam o evento na região de interesse, processam os dados e decidem se devem ou não propagar os resultados para os outros nós (Costa, 2011).

As redes de sensores sem fio são aplicadas as áreas de automação industrial, monitoramento ambiental, localização de veículos rodoviários, monitoramento de tráfego, vigilância militar e outras. Para cada aplicação há uma peculiaridade sobre as características desejáveis da rede, como por exemplo: escalabilidade, auto-organização, baixo consumo de energia, cooperação, segurança, caminhos redundantes e outros.

Sendo assim, o atendimento dessas características é determinado pela quantidade e pela posição geográfica dos nós na área de interesse. O posicionamento dos nós da rede, ou seja, a determinação da posição geográfica dos nós na área de interesse pode ser realizada de duas formas: controlada e aleatória. A forma controlada do posicionamento dos nós geralmente é usada em ambiente fechados, e em poucos casos em área aberta (como exemplo, ambientes industriais), onde sua operação é afetada pela sua posição e os sensores são caros. Já na forma aleatória, os elementos da rede são posicionados aleatoriamente no ambiente de interesse e descartados após o término da sua vida útil. Esses ambientes geralmente estão ligados a lugares impróprios ou de difícil acesso para o seu posicionamento e manutenção.

Entretanto, ambos os casos, o posicionamento tem que ser realizado com o máximo de cuidado, pois ao se colocar os nós inadequadamente pode-se comprometer toda a rede de sensores sem fio, fazendo com que a cobertura de parte da área monitorada seja perdida, que não sejam atendidos os requisitos temporais e que apareçam nós críticos, isto é, nós onde um mau funcionamento pode comprometer o funcionamento de grande parte da rede. Na Figura 3 podem-se visualizar alguns desses problemas e apenas um benefício, tais como: (i) Os sensores 3 e 4 estão conectados entre si, porém sem conectividade direta ou indireta com o

gateway; (ii) Os sensores 1 e 2 apresentam conectividade indireta com o *gateway*, através de 3 hops ou 5 hops; (iii) O sensor 1 e 2 apresentam caminhos redundantes; (iv) O roteador 1 é nó crítico, pois se houver qualquer problema com ele, as informações enviadas pelos sensores 1 e 2 não chegarão ao *gateway*; (v) O roteador 3 também é um nó crítico, pois em caso de sua falha, o sensor 1 só terá um caminho ao *gateway* e o sensor 2 não conseguirá enviar a sua informação ao nó central; (vi) O roteador 3 é vizinho dos sensores 1 e 2, ou seja, logo ele será responsável por retransmitir as mensagens provenientes dos dois sensores (sensor 1 e sensor 2) e, portanto, poderá ter um maior consumo de energia. Isto significa que a duração de sua bateria será menor, e que este nó vai parar de funcionar antes dos outros.

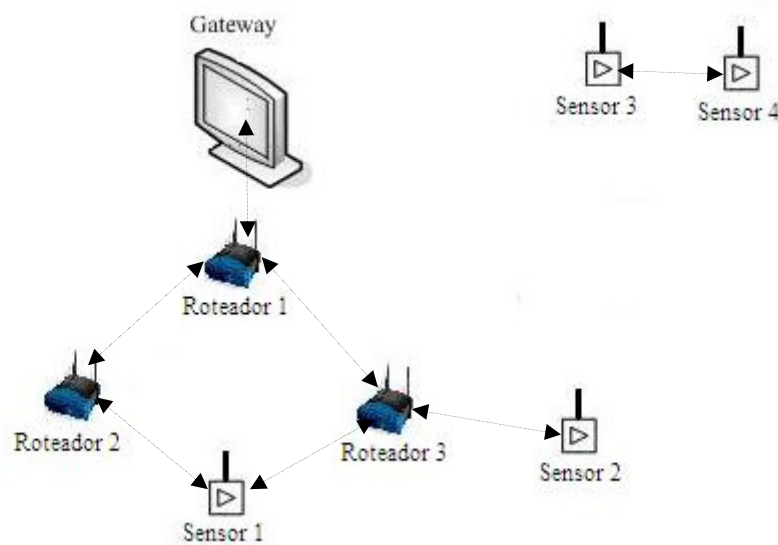


Figura 3 – Características da uma rede em malha

Os estudos relacionados ao posicionamento dos nós não estão apenas ligados a localização dos sensores, mas também no posicionamento dos roteadores, gateway e cabeça do cluster - nó responsável por coletar as informações dos sensores e difundi-las pelo resto da rede - (Younis & Akkaya, 2008).

1.4 Soluções Encontradas para o Problema de Posicionamento

Ao longo dos anos, o interesse pelo estudo de posicionamento de nós em rede sem fio vem aumentando. Abaixo estão relacionados e agrupados alguns artigos que descrevem

métodos para resolver o problema supracitado através do posicionamento dos nós roteadores, *gateway* e sensores.

- Posicionamento dos nós roteadores:

Em (Cannons et al, 2008), um algoritmo de posicionamento de nós roteadores e determinação de qual roteador retransmitirá as informações de cada sensor, com algumas similaridades do algoritmo de Lloyd (Gersho & Gray, 1992), é proposto para promover a confiabilidade da comunicação da rede de sensores sem fio, minimizando a probabilidade média do erro de transmissão do sensor. O algoritmo é dividido em duas etapas. Na primeira etapa, a posição do roteador e do sensor é fixada e a atribuição de cada sensor ao roteador é pesquisada exaustivamente para todas as combinações possíveis entre eles. Após a pesquisa, a melhor associação sensor-roteador é escolhida para uma boa retransmissão e recepção do sinal. Já na segunda etapa, fixa a atribuição do sensor ao roteador e determina a melhor posição do roteador, usando inicialmente uma abordagem numérica que quantifica um subconjunto de \mathcal{R}^2 em pontos de grade, onde o melhor ponto de grade é escolhido para a nova posição de cada roteador, e posteriormente, a técnica de gradiente descendente para aprimorar a posição final de cada roteador.

Em (Shi et al, 2009), é proposto um algoritmo de posicionamento de multi-nós roteadores para minimizar o consumo de energia na transmissão de dados em rede ad hoc móvel (MANET - *Mobile Ad Hoc Network*). O problema foi modelado como um problema de otimização de agrupamento. O algoritmo sugerido para resolver o problema usa os métodos heurísticos baseado no algoritmo de *k-means*. No seu primeiro passo é realizada a otimização do posicionamento de um só roteador e finalmente no último passo é realizado a otimização do posicionamento de múltiplos roteadores.

(Costa & Amaral, 2010) e (Costa, 2011) propõem um algoritmo de otimização de posicionamento de nós roteadores, baseado em algoritmo genético. O algoritmo proposto tem como critérios a otimização da menor quantidade de nós roteadores necessários à rede, a otimização da menor quantidade de nós críticos potenciais para todos os dispositivos envolvidos e a otimização da menor quantidade de saltos (hops) de mensagens transmitidas, para determinar a melhor configuração da rede de automação industrial.

- Posicionamento dos nós gateway:

Em (Wong et al, 2004), trata-se do problema de posicionamento de gateways para a redução da latência e da eficiência energética da agregação de dados em uma rede de sensores sem fio. O problema é resolvido através de dois métodos de otimização: (i) Programação linear inteira ideal - esse algoritmo é usado para uma rede de sensores com poucos elementos; (ii) Algoritmo heurístico – esse algoritmo é baseado no paradigma de seleção negativa, que exclui as piores posições para se posicionar os *gateways*. Ele é usado para uma rede de tamanho arbitrário.

Em (Aoun, 2006), trata-se do problema de posicionamento de *gateways* para o atendimento da qualidade de serviço (QoS), como a latência, banda, taxa de perdas e disponibilidade da rede, na rede em malha sem fio. Os autores sugerem um algoritmo ideal de aproximação de tempo polinomial que constantemente calcula o peso mínimo do conjunto dominante, sem perda da qualidade de serviço.

Em (Wu et al, 2009), estudam o posicionamento de *gateways* para o provimento de internet em rede sem fio. Neste artigo existe três objetivos a serem otimizados: o número de *gateways*, a média dos saltos entre a malha de roteamento e os gateways e a variância da carga dos *gateways*. A solução sugerida pelos autores foi iniciada pela modelagem do problema usando o programa linear de multiobjetivos, e finalizada com o uso do algoritmo de posicionamento de gateway para balanceamento de carga.

Em (Shi et al, 2007), é sugerido um algoritmo de aproximação que garante $(1 - \epsilon)$ do desempenho ideal do tempo de vida da rede para o problema de posicionamento do *gateways* em rede de sensores sem fio com o menor erro de aproximação desejado ($\epsilon > 0$). O algoritmo divide o espaço de busca em um número finito de subáreas, no qual cada subárea é representada por “ponto de custo fictício”. Após as divisões, o algoritmo linear é aplicado a cada ponto de custo fictício para analisá-los e escolher a subárea onde o *gateway* deverá ser posicionado no ponto que garante um tempo de vida $(1 - \epsilon)$.

- Posicionamento dos nós sensores:

Em (Poduri & Sukhatme, 2004), os autores propõem resolver o problema de auto-desenvolvimento da rede de sensores móveis utilizando um algoritmo baseado em campos potenciais artificiais. Este algoritmo é composto pela combinação de duas forças: F_{cover} – cada nó se repele do outro para aumentar a cobertura; e F_{degree} – restringe o grau do nó, fazendo com que ele seja atraído por outro nó quando eles estão próximos de serem desconectados.

Além disso, o algoritmo propõe resolver o problema maximizando a área de cobertura da rede e restringindo que cada nó tenha no máximo k vizinhos.

Os autores de (Poduri et al, 2006) propõem resolver o problema de posicionamento de nós sensores móveis e estáticos utilizando um algoritmo de implementação controlada que constrói uma topologia baseada em condições puramente locais e geométricas que podem garantir as propriedades de cobertura e conectividade da rede global. O posicionamento do novo nó tem que atender a condição NET (*Neighbor-Every-Theta*), onde tem pelo menos um vizinho em todo setor angular θ do seu range de comunicação, conforme Figura 4.

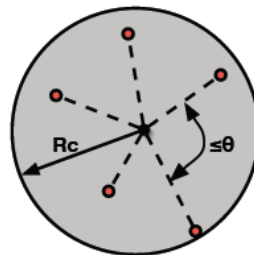


Figura 4 – Ilustração da Condição Net (Adaptado de Poduri et al, 2006)

Em (Nordlund et al, 2012), os autores apresentam o problema de localização de veículos rodoviários através de estações bases de rede sem fio. Este problema é altamente complexo, pois a rede é composta por multisensores com variáveis não lineares. Sendo assim, para resolver o problema é proposto o uso do filtro de partículas. O filtro de partícula é uma implementação recursiva de Monte Carlo baseada no processamento de sinal estatístico.

Nos artigos mencionados acima, foi observado que a maioria dos estudos de posicionamento de nós de rede sem fio trata o problema de posicionamento como um problema NP-Difícil, e o resolve com aplicações de heurísticas e de algoritmos de otimização. Além disso, a maioria deles propõe resolver o problema atendendo a no máximo duas características de qualidade da rede.

Conforme visto em (Costa, 2011), as seguintes características são relevantes na área de automação industrial:

1. A informação transmitida tem que ser entregue ao nó central com **baixa latência**;
2. Ser totalmente **tolerante a falha**;
3. Os sensores são instrumentos **caros**, que exercem as funções de **monitoramento do processo e roteamento** das informações enviadas de outros equipamentos. Eles não

são descartáveis, e apresentam escalabilidade da ordem de dezenas, podendo chegar à ordem de centenas;

4. A rede sem fio tem que ter **cobertura total** dos processos a serem monitorados, de forma que todos os nós sensores sejam capazes de se comunicar com o *gateway*, diretamente ou indiretamente, **sem oscilações** na entrega dos pacotes.

Diante destas características, considera-se a tolerância a falhas como a mais importante, sendo assim, neste trabalho propõe-se uma solução descentralizada e auto-organizável, que gere uma topologia, onde existam caminhos redundantes para a informação chegar ao destino final. Além disso, deseja-se observar o impacto desta escolha nas outras características.

1.5 O Problema de Posicionamento de Nós em Redes de Automação

A utilização de rede de sensores sem fio em automação industrial ainda é um assunto que causa preocupação com relação à confiabilidade e à segurança dos dados por parte dos usuários. Sendo assim, o posicionamento dos nós de forma adequada é de suma importância para que a rede sem fio atenda os critérios de segurança, confiabilidade e eficiência.

Realizar o posicionamento dos nós é uma tarefa difícil, pois para tal devem-se levar em consideração todos os obstáculos e as interferências que um ambiente industrial promove. Na automação industrial, o posicionamento dos nós sensores é pré-definido próximo ao fenômeno a ser monitorado pelo dispositivo. O gateway, assim como os nós sensores, em geral, tem sua posição fixa, próximo à sala de controle. Já o posicionamento dos nós roteadores, que são responsáveis pelo encaminhamento dos dados gerados pelos sensores da rede até o gateway de forma direta ou indireta, é determinado pelas características da rede de automação industrial.

As características da rede de sensores sem fio para automação industrial se diferenciam das redes de sensores sem fio tradicional pelos seguintes aspectos: (a) A quantidade de sensores na rede tradicional sem fio é na ordem de dezenas, milhares ou milhões. No entanto, nas redes de automação sem fio estão na ordem de dezenas, podendo chegar a centenas; (b) O grau de tolerância a falha das redes de sensores sem fio tradicional é maior do que nas redes de automação sem fio; (c) A topologia dos sensores nas redes de

sensores sem fio tradicional pode variar frequentemente. No entanto, nas redes de automação sem fio não é variável; (d) A topologia da rede de sensores sem fio tradicional é aleatória e da rede de automação sem fio é fixa, em malha; (e) Os nós sensores em termos de energia, capacidade computacional e memória são mais eficientes na rede de automação sem fio; (f) Os sensores são mais caros e robustos nas redes de automação sem fio; (g) A confiabilidade da rede e a latência são fatores imprescindíveis e fundamentais para a rede de automação sem fio, no entanto, nas redes de sensores sem fio tradicionais são importantes e pode ser tolerável, dependendo da aplicação a que se destina. (h) Com relação à manutenção dos equipamentos, a rede de automação sem fio é totalmente acessível, enquanto, na rede de sensores sem fio tradicional é menos acessível; (i) A rede de automação sem fio apresenta um maior grau de criticidade em relação às redes de sensores sem fio; (j) O posicionamento dos nós nas redes de automação sem fio é realizado de forma calculada e precisa, devido ao alto custo dos valores dos equipamentos, entretanto, nas redes de sensores sem fio tradicionais é realizado de forma densa e aleatória.

Para mensurar a quantidade de nós roteadores e definir o seu posicionamento na rede, alguns aspectos importantes em automação industrial devem ser considerados. Para tal, devem-se estabelecer:

- (1) caminhos redundantes de forma que o sistema seja o máximo possível tolerante a falhas dos nós;
- (2) conectividade total entre os nós (sensores e roteadores) da rede para que um nó possa se conectar com todos os outros aproveitando a função colaborativa dos roteadores;
- (3) a eficiência de energia dos nós de forma que nenhum nó fique sobrecarregado com retransmissão de muitas informações oriundas dos sensores;
- (4) a baixa latência do sistema para uma melhor eficiência no tempo de resposta;
- (5) a obtenção de atributos combinados para que os processos da indústria não venham a causar acidentes, devido, por exemplo, a alta temperatura do processo monitorado.
- (6) a sua capacidade de auto-organização. Ou seja, a capacidade da rede de reorganizar os caminhos de retransmissão dos dados, quando um novo sensor é adicionado à rede ou quando um sensor para de funcionar por falta de energia ou por problema no canal de comunicação sem fio.

Todos esses fatores devem ser atendidos, sempre levando em consideração o fator primordial de segurança: que é a **tolerância a falha**. Ao final do posicionamento dos nós roteadores, a rede de sensores sem fio aplicado a automação industrial será definida como um sistema robusto, confiável, escalável e auto-organizável.

2 O SISTEMA IMUNOLÓGICO

O sistema imunológico é um dos principais sistemas do corpo humano. Ele é responsável por fornecer proteção ao organismo contra agentes patogênicos responsáveis por diversas doenças. Esta tarefa é bastante complexa, pois existe uma infinidade de agentes químicos e mecânicos responsáveis pelo controle sobre uma determinada doença ou diversas doenças.

Na medicina, esse assunto tem sido bastante discutido, para que seja possível encontrar métodos eficientes de combate às doenças, e assim, proteger melhor as condições de vida dos seres humanos. A vacina é um exemplo destes métodos que foram desenvolvidos pelo estudo do sistema imunológico. A vacina tem, em alguns casos, pequenas quantidades dos agentes infecciosos, vivos ou mortos, capazes de estimular o sistema imunológico a reagir, criar detectores compatíveis com eles e memorizá-los para o caso de um segundo contato com esses agentes.

Na engenharia, os algoritmos baseados em sistemas imunológicos são utilizados principalmente na área da segurança da informação, agrupamento de dados, aprendizado de máquina e solução de problemas de busca e otimização, de caráter combinatório. As características de suma importância no algoritmo baseado em sistema imunológico são (Amaral, 2006):

Unicidade: não existem dois indivíduos com o mesmo sistema imunológico, cada pessoa tem o seu;

Reconhecimento: o reconhecimento é a capacidade de distinção entre as células próprias do organismo e as células estranhas ao organismo. Além disso, ele também tem a capacidade de reconhecer um agente patogênico anteriormente combatido pelo sistema imunológico;

Deteção de anomalia: capacidade de reação, de forma gradual, contra os agentes patogênicos nunca vistos anteriormente pelo sistema imunológico;

Deteção imperfeita (tolerância a ruídos): os detectores dos linfócitos não precisam ser totalmente iguais aos agentes patogênicos para o combate do agente invasor. Dessa forma, um detector é capaz de combater um conjunto de agentes patogênicos diferentes;

Aprendizagem e memória: o sistema imunológico tem a capacidade de modificar os seus detectores, até que os mesmos sejam capazes de combater os agentes patogênicos de forma eficientes. Após o primeiro contato com o agente patogênico, o sistema imunológico “grava”

o detector na sua memória, para a próxima infecção pelo mesmo agente patogênico ou por um agente patogênico semelhante ao anterior. Dessa forma, na segunda infecção, pelo mesmo agente patogênico, a reação do sistema imunológico é de forma mais rápida e eficaz.

2.1 Visão Geral do Sistema Imunológico

O sistema imunológico humano é um mecanismo muito complexo, que é capaz de reconhecer entre as células e moléculas do seu organismo das células e moléculas invasoras ao seu organismo, mesmo tendo um número de padrões próprios bem menores do que o número de padrões não-próprios. Além disso, ele tem que ser capaz de combater o agente patogênico sem parar o funcionamento de outros sistemas do corpo humano (Amaral, 2006).

O corpo humano, com o objetivo de se defender contra agentes invasores e nocivos à sua saúde, apresenta a arquitetura de múltiplas camadas mostrada na Figura 5.

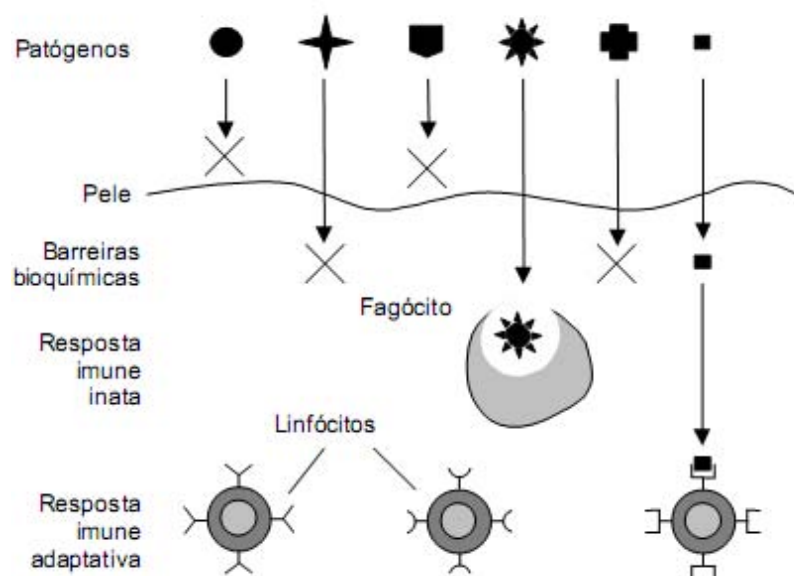


Figura 5 – Arquitetura de combate ao agente invasor (Castro & Von Zuben, 1999)

A arquitetura de múltiplas camadas é constituída por (Castro, 2001):

Pele: ela é a primeira barreira contra os agentes externos, infecciosos ou não.

Barreiras químicas: elas são constituídas por substâncias como a saliva, suor e lágrimas, que apresentam temperaturas e pH não agradáveis para a sobrevivência dos agentes.

Resposta imune inata: a resposta imune inata é a resposta gerada pelo sistema imune inato que age de forma rápida e efetiva contra os agentes patogênicos, mesmo sem nunca ter visto o agente anteriormente. O sistema imune inato é formado por macrófagos e granulócitos, que são capazes de ingerir e digerir vários microorganismos e partículas antigênicas.

Resposta imune adaptativa: a resposta imune adaptativa, gerada pelo sistema imune adaptativo, exerce uma ação lenta no combate aos agentes patogênicos. O sistema imune adaptativo é a camada mais importante, e em consequência, a mais complexa. Pois quando o sistema imune inato não consegue combater o agente patogênico, ele entra em ação se adaptando ao novo antígeno para eliminá-lo.

2.1.1 Células B no Reconhecimento de Agente Patogênico

O reconhecimento de agente patogênico é realizado através dos linfócitos, células B, que apresentam receptores com o objetivo de se unir aos antígenos e posteriormente eliminá-lo.

O receptor da célula B é um anticorpo ligado a uma membrana, que será produzido e secretado pela célula B após sua ativação pelo antígeno. A ligação entre o anticorpo e o antígeno é uma ligação molecular necessária para que ocorra o reconhecimento entre eles. Essa ligação ocorre entre o epítipo do antígeno ao receptor da célula B (Figura 6), de forma que se tenham um encaixe perfeito entre eles ou dentro de limiar definido pela célula (Castro, 2001).

Cada antígeno apresenta na sua superfície uma grande quantidade de epítipos diferentes. E cada célula B apresenta aproximadamente 100.000 receptores com mesma estrutura, sendo assim, uma célula B só pode se encaixar a um epítipo do antígeno. A natureza, com o objetivo de minimizar a quantidade de células B e o tempo de ação de combate ao antígeno, fez com que o encaixe entre o epítipo e o anticorpo não precisasse ser perfeito e possuísse um limiar de ativação baixo. Dessa forma, uma única célula B é capaz de ter o seu receptor unido a diferentes epítipos, diminuindo a necessidade de evolução estrutural dos receptores e fornecendo maior proteção contra o maior número de agentes patogênicos possível (Amaral, 2006).

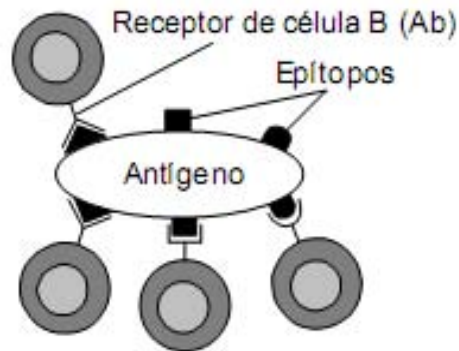


Figura 6 – Reconhecimento de um antígeno através da célula B (Castro, 2001)

2.1.2 Distinção entre o Próprio e Não-Próprio

O sistema imunológico é um sistema completo e complexo, que na grande parte dos seres vertebrados age de forma correta na distinção de moléculas do seu organismo (próprio), e moléculas invasoras (não próprio), mesmo passando pela hipermutação dos linfócitos para aumentar a sua diversidade. No processo de reconhecimento das proteínas próprias o linfócito T, chamado de célula T Helper, é a peça fundamental. Ele é uma célula gerada pela medula óssea que migra para o timo, para então, realizar a sua multiplicação e amadurecimento. O timo é um órgão localizado na parte superior do tórax, onde a maioria das proteínas próprias do organismo circulam. Dessa forma, durante o amadurecimento dessas células no timo, elas são expostas as proteínas próprias do organismo (Castro, 2001).

Na distinção entre o próprio e o não-próprio, a célula B, gerada na medula óssea e maturada de forma distribuída, é apenas um agente passivo, que não consegue fazer sozinha essa diferenciação. É nessa hora que a célula T Helper entra em ação para colaborar com a ativação do anticorpo da célula B para agir sobre o antígeno, esse processo é chamado de co-estimulação. A co-estimulação só ocorre quando a célula T Helper é capaz de reconhecer o agente patogênico. A ativação da célula B ocorre quando há o número de agentes patogênicos que se ligam ao receptor da célula B passa do limiar de afinidade e quando há co-estimulação por parte da célula T Helper (Amaral, 2006).

2.1.3 Maturação de Afinidade / Seleção Clonal

Quando o organismo é atacado por agentes patogênicos, o sistema imunológico precisa ser capaz de detectar e eliminar estes agentes o mais rápido possível. Com este objetivo ele possui um mecanismo, chamado de maturação de afinidade, no qual o sistema imunológico é capaz de evoluir células B com alto grau de afinidade com agentes patogênicos específicos, conforme Figura 7.

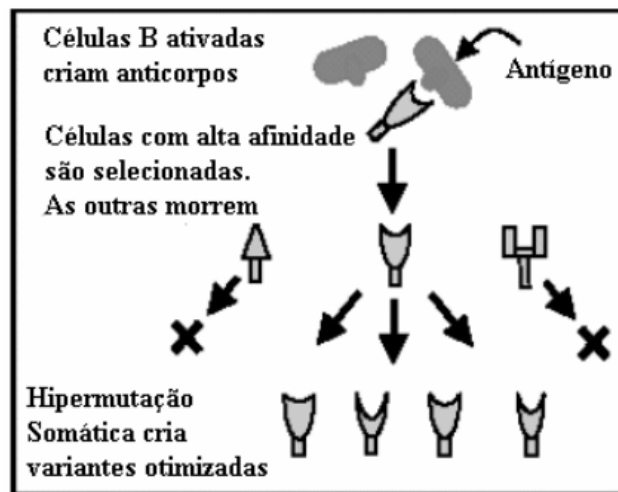


Figura 7 – Processo de maturação de afinidade (Bradley, 2000b)

O processo de maturação de afinidade inicia-se na tentativa de conectar algum receptor da célula B, que se encontra na biblioteca (memória), aos agentes patogênicos. Essa tentativa é a primeira resposta do sistema adaptativo ao agente invasor. Ela geralmente não é muito eficiente e pode permitir que o agente patogênico possa se reproduzir e agir, causando a manifestação da doença. Entretanto, é através dela que a célula B que apresentar a maior afinidade com os agentes patogênicos seja selecionada para sofrer clonagem e mutação. Essas células filhas (clones) tentarão se conectar aos agentes, gerando uma resposta secundária mais eficiente, porém mais demorada (Castro,2001).

A célula B, com a função de aumentar a afinidade entre o seu receptor e o epítipo do agente patogênico, sofre hipermutação somática. A hipermutação somática nada mais é do que a clonagem das células B com alta taxa de mutação, sendo os seus clones diferentes da célula clonada, podendo ter uma afinidade maior ou não com o antígeno. Esse processo é repetido diversas vezes, sendo que haverá distinção entre o nível de mutação e o número de réplicas em cada nova célula. Assim, quanto maior a afinidade, menor será a mutação e maior

será o número de réplicas, e quanto menor a afinidade maior será a mutação e menor é o número de réplicas (Amaral, 2006). A cada processo de maturação de afinidade, as células B aumentam a sua afinidade aos agentes patogênicos, tornando o combate a esses agentes mais efetivos e eficientes, porém mais demorado.

2.1.4 Memória Imunológica

A primeira vez que organismo é atacado por algum agente patogênico, a célula B passa por todo o processo de maturação de afinidade até que a doença seja eliminada (resposta primária). O que será que acontece com as células B, de alta afinidade, quando acaba a infecção? Será que serão eliminadas?

Estudos indicam que as informações são codificadas nas células B para a próxima infecção pelo mesmo agente, isso é chamado de memória imunológica. Se houver uma segunda infecção pelo mesmo agente, a resposta (resposta secundária) será mais rápida e eficiente do que a resposta primária. A resposta secundária torna a ação da célula B mais efetiva, de forma em que alguns casos, nem se percebe que houve uma nova infecção pelo mesmo antígeno (Amaral, 2006).

2.1.5 Redes Imunológicas

Jerne (Jerne, 1974) propôs uma nova teoria, chamada Redes Imunológicas, que descreve a atividade dos linfócitos. Essa teoria diz que o sistema imunológico apresenta células B, capazes de se reconhecerem e se recombinarem mesmo na ausência de antígeno, formando assim uma rede de células B. Cada célula B (Figura 8 (a)) é formada pelo seu paratopo, responsável por determinar a afinidade da célula B com outra célula B ou com o antígeno, e por idiotopo, responsável em fazer a ligação com outra célula B, de acordo com a sua afinidade com o paratopo da outra célula B. Cada paratopo reconhece um conjunto de epítopos e idiotopos diferentes, porém com forma semelhante à forma do paratopo.

Sendo assim, as células B são capazes de se estimular ou se inibir umas a outras (Figura 8 (b)), de acordo com a afinidade entre elas, até a estabilidade da rede. A estabilidade

da rede é estabelecida quando a ligação entre as células B tem uma afinidade superior a um determinado limiar. Após a estabilização da rede, a nova rede imunológica formada se torna mais resistente e eficiente na eliminação do agente patogênico (agente causador de doenças ao corpo humano) (Amaral, 2006).

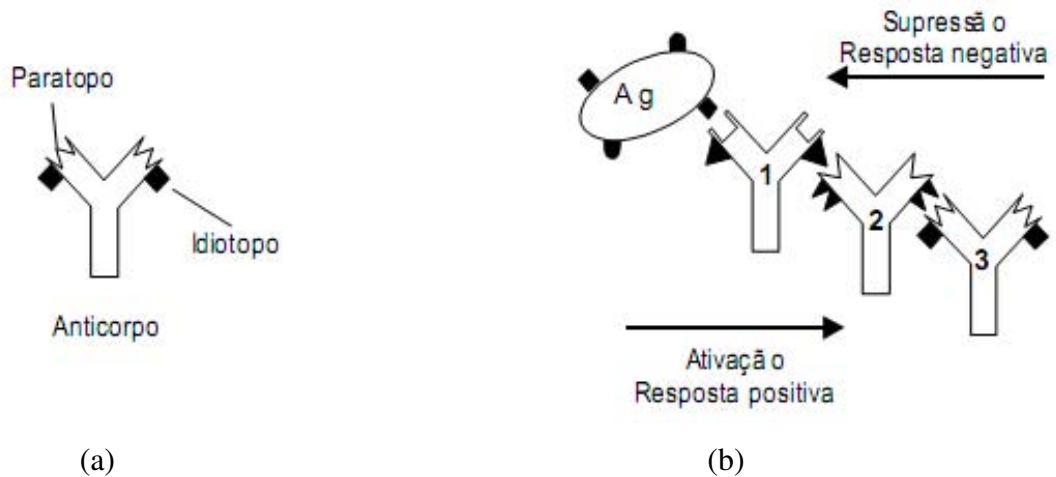


Figura 8 – Rede Imunológica (Castro, 2001). (a) Célula B com o seu paratopo e idiotopo; (b) Estimulo (resposta positiva) ou inibição (resposta negativa) resultante da tentativa da união do paratopo com o idiotopo ou do paratopo com a epítipo do antígeno.

Ao fim da análise do funcionamento das redes imunológicas podem-se destacar três características fundamentais delas: a estrutura, a dinâmica e a metadinâmica. A estrutura é o padrão formado pelas interconexões entre os elementos moleculares e celulares da rede, sem considerar a interação existente entre eles na formação da rede. Ou seja, ela é a forma estrutural que a rede imunológica terá ao final da sua formação. A segunda característica, a dinâmica, é responsável por tratar das interações entre os elementos da rede imunológica, na qual, ela se adapta a si e ao ambiente. Como exemplo de interações pode-se citar a variação de concentração dos anticorpos e a variação da afinidade dos anticorpos com relação às suas células e moléculas e aos antígenos. Já a metadinâmica é responsável por introduzir a diversidade à rede, produzindo e recrutando novos anticorpos a rede imunológica e eliminando os elementos não estimulados ou auto-reativos (De Castro, 2002).

De acordo com as características mencionadas acima, pode-se afirmar que as redes imunológicas apresentam uma estrutura complexa e dinâmica, que se modifica constantemente na presença ou não do agente patogênico para um eficiente combate do agente invasor, quando houver a invasão do agente causador de doença.

2.2 Sistemas Imunológicos Artificiais

Os sistemas imunológicos artificiais são modelos computacionais inspirados no funcionamento de sistema imunológico natural no combate a doenças geradas por bactérias, fungos, vírus e outros. As características dos sistemas imunológicos naturais de grande interesse na comunidade científica são unicidade, reconhecimento do próprio e do não próprio, detecção imperfeita, aprendizagem e memória.

Os algoritmos inspirados nos sistemas imunológicos, de um modo geral, podem ser agrupados em três grupos principais:

Redes Imunológicas – algoritmos que imitam o funcionamento das redes imunológicas naturais. Elas serão detalhadas na próxima seção.

Seleção Clonal - algoritmos que simula o funcionamento da seleção clonal natural e a maturação de afinidades na proliferação de anticorpos. Como exemplo de algoritmo de seleção clonal pode-se citar o algoritmo CLONALG (*CLONal selection ALGORITHM*) desenvolvido por Castro, em (Castro, 2001).

Seleção Negativa – algoritmos que imitam o funcionamento da seleção negativa natural na morte ou inativação de linfócitos para o reconhecimento do próprio. Como exemplo de algoritmo de seleção negativa: NSA (*Negative Selection Algorithm*, Forrest et al., 1994), NSDR (*Negative Selection with Detection Rules*, Gonzalez, 2003) e RNSA (*Real Valued Negative Selection Algorithm*, Gonzalez, 2003).

2.2.1 Modelos de Redes Imunológicas

As redes imunológicas artificiais são algoritmos inspirados no funcionamento das redes imunológicas dos animais e dos seres humanos no combate a doenças. Esse tipo de algoritmo, rede imunológica artificial, não é tão popular nas resoluções de problemas quanto outros algoritmos bioinspirados como as redes neurais artificiais, a lógica fuzzy e os algoritmos genéticos. Porém, as redes imunológicas apresentam as características de escalabilidade, de auto-organização, de habilidade de aprendizado contínuo e de tratamento de ruído, que são de suma importância em muitas aplicações, tais como, aprendizagem de

máquina, análise de dados, reconhecimento de padrão, navegação autônomas e função de otimização.

O modelo geral do algoritmo de Redes Imunológicas Artificiais (GAIN – *General Model of AIN* – Modelo Geral do AIN) pode ser visto na Figura 9. Ele apresenta os passos comuns presentes em vários modelos de redes imunológicas já publicados e introduz a notação que permite a sua comparação (Galeano, 2005).

O modelo geral GAIN está dividido em três passos principais. O primeiro passo é chamado de inicialização da rede, onde o conjunto inicial de célula B é atribuído ao conjunto B e é inicializando uma estrutura de rede L. No segundo passo, começa-se a interação entre os elementos da rede para alcançar o objetivo de cada aplicação. Ele inicializa o processo, apresentando o antígeno à célula B, através do cálculo de afinidade $f_{\text{afinidade}}(a,b)$ e de estimulação $f^A_{\text{estimulação}}(a,b)$, onde a pertence ao conjunto A de antígenos e b pertencem ao conjunto B (conjunto de células B). A seguir, tem-se o processo de interação das células B, no qual são calculadas a estimulação $f^B_{\text{estimulação}}(b',b)$ e a supressão $f^B_{\text{supressão}}(b',b)$ de cada células B em relação a outras células B, onde b e b' pertencem ao conjunto B. Em poder dos resultados das estimulações e das supressões são calculadas a estimulação total de cada célula B, através da soma da estimulação do antígeno a célula B com a estimulação e supressão de cada células B com outras células B. Com base na estimulação total, as n_b células B selecionadas sofrem clonagem e mutação, com uma determinada faixa. Então, são recalculadas as estimulações das novas células B (clonadas e mutadas). Na etapa metadinâmica haverá criação de novas células B, remoção de algumas células B da rede e reorganização dos links entre as células B, fazendo uma atualização da estrutura da rede. O último passo consiste em retornar para a etapa de apresentação do antígeno, caso o critério de parada não seja satisfeito, e repassar por todas as etapas anteriores.

GAIN (A: conjunto de antígenos)

1: inicialização

1.1: atribuir B a conjunto inicial de célula B

1.2: inicializar a estrutura de rede L

2: repetir até o critério de parada seja cumprido

2.1: apresentação do antígeno:

Afinidade Antígeno/Células B

2.1.1: calcular $f_{afinidade}(a,b)$ para todos $a \in A, b \in B$

Estimulação Antígeno/Célula B

2.1.2: calcular $f^{A_{estimulação}}(a,b)$ para todos $a \in A$ e $b \in B$

2.2: interação da célula B:

Célula B/ Estimulação célula B/ Supressão

2.2.1: calcular $f^{B_{estimulação}}(b',b)$ e $f^{B_{supressão}}(b',b)$ para todos $b, b' \in B$

2.3: maturação de afinidade:

Estimulação total

2.3.1: calcular $F(b) := \sum_{a \in A, b' \in B, b' \neq b} f^{A_{estimulação}}(a,b) + f^{B_{estimulação}}(b',b) + f^{B_{supressão}}(b',b), b \in B$

2.3.2: criar $f_{clonagem}(b)$ clones das células B b e mutá-los

2.3.3: calcular a estimulação de todas as células B novas

2.4: metadinâmica:

Deleção/Criação de células B e links

2.4.1: update na estrutura de rede L:

Retorna a rede imunológica

3: retornar (B,L)

Figura 9 – Algoritmo de Rede Imunológica Artificial Geral (Versão Traduzida de (Galeano, 2005))

Muitos dos modelos de redes imunológicas publicados são variações de modelos previamente propostos. Isto gera uma relação de dependência entre os modelos que pode ser representado na forma de uma árvore genealógica que pode ser vista na Figura 10 (Galeano, 2005). O modelo proposto nesta dissertação está mais fortemente relacionado com o SSAIS (Timmis et al, 2000) e com o AINET (Castro, 2001). Sendo assim, será feita uma breve descrição destes dois algoritmos nas seções a seguir.

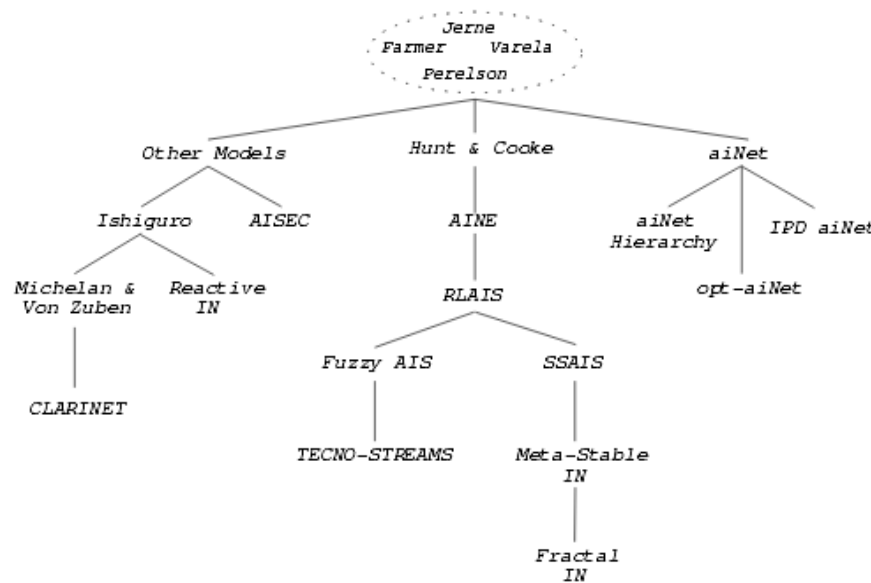


Figura 10 – Árvore genealógica dos modelos de redes imunológicas (Galeano, 2005)

2.2.1.1 Algoritmo SSAIS

O algoritmo SSAIS (*Self-Stabilising Artificial Immune System*) foi desenvolvido por Neal em 2002 para resolver o problema de análise contínua de dados variáveis no tempo. Ele usa o conceito de ARBs (*Artificial Recognition Balls* – Esfera de Reconhecimento Artificial) como elemento básico da rede, onde as etapas de dinâmica e de metadinâmica da rede são desenvolvidas (Neal, 2002).

As etapas do algoritmo são divididas em três. Na primeira etapa, chamada de estrutura, as ARBs são criadas aleatoriamente e os itens de dados são apresentados a cada ARBs, através do cálculo da distância euclidiana dos itens de dados ($dis(p)$) e da distância entre os vizinhos ao redor de cada ARBs ($dis(x)$). A segunda etapa diz respeito ao dinamismo da rede. Nela, a estimulação é calculada pela soma do fator de excitação dos itens de dados pelo complemento da $dis(p)$ e pela excitação normalizada dos vizinhos ao redor de cada ARB, também pelo complemento da $dis(x)$. Além disso, nessa etapa o algoritmo acrescenta ou diminui níveis de recursos a cada apresentação dos dados a cada uma das ARBs, de acordo com o nível de estimulação. Apenas a ARB mais estimulada pela apresentação dos antígenos terá seus recursos aumentados enquanto que os outros terão seus níveis de recurso diminuídos. O decaimento do nível de recurso da ARB é realizado proporcionalmente ao fator

de decaimento dr e o nível de recurso da ARB depois da apresentação dos antígenos. Na etapa metadinâmica da rede, as ARBs, com nível de recurso menor do que o limiar de mortalidade, são removidas da rede e a ARB com maior nível de recurso produzirá n_c clones com fator de mutação de 0,1%. O número de clones gerado é dado pela Equação 1:

$$n_c = \frac{\text{Recurso}_{(ARB)(item\ dados)}}{\text{limiar\ mortalidade} * 10} \quad (1)$$

Cada clone receberá uma quantidade de recurso igual ao limiar de mortalidade multiplicado por 10. Ao fim a rede se configurará e voltará para a etapa estrutura, até que o critério de parada seja satisfeita.

A Figura 11 mostra as principais etapas do algoritmo.

- (i) inocular a rede com ao conjunto aleatório de ARBs
- (ii) apresentar os itens de dados a todas as ARBs
- (iii) encontrar a ARB com maior ativação
- (iv) conceder à ARB o incremento do seu nível de recurso
- (v) exaurir o recurso de todas as outras ARBs
- (vi) selecionar a ARB com nível de recurso inferior ao limiar do nível de recurso
- (vii) aprovar a ARB com maior ativação para clonagem
- (viii) reorganizar a rede com os novos clones
- (ix) retornar ao (ii)

Figura 11 – Etapas do SSAIS (Versão traduzida de Neal, 2002)

2.2.1.2 Algoritmo AiNet

O AiNet (*Artificial Immune NETwork*) é um algoritmo criado por Castro & Von Zuben em 2000, que tem a capacidade de descrever estruturas internas dos dados de treinamento, seu perfil de distribuição de probabilidade e relações de vizinhança (clusters) (Castro, 2001). Ele não opera sozinho, precisando do algoritmo CLONALG (*CLONal selection ALGORITHM*, Castro, 2001) como parte do seu processo de treinamento.

O algoritmo AiNet é dividido em quatro passos principais, conforme pode ser visto na Figura 12. Na inicialização da rede, o conjunto de dados a serem treinados é chamado de antígeno (A_g) e o conjunto de anticorpos (A_b) é gerado aleatoriamente. O primeiro passo consiste na criação, maturação de afinidade e supressão dos clones e anticorpos de memória. Na etapa de criação dos clones de memória, os n anticorpos com maior afinidade, ou seja, os A_b mais próximos aos antígenos serão selecionados para serem clonados e sofrerem mutação. O número de clones está diretamente relacionado à afinidade que cada anticorpo selecionado contém. Já a mutação dos clones (C) terá uma taxa α inversamente proporcional à afinidade do anticorpo pai, conforme Equação 2. O novo conjunto de clones mutados (C^*) será apresentado aos antígenos e calculado a afinidade entre eles (inversamente proporcional ao módulo da distância entre C^* e A_g). Sendo assim, a matriz clone de memória (M) receberá ζ % dos clones mutados com maior afinidade.

$$C^* = C + \alpha(A_g - C) \quad (2)$$

Na criação do conjunto de anticorpos de memória (M), o conjunto clone de memória passa pelo processo de morte programada, onde os clones de memórias com afinidade maior do que o limiar de σ_d são removidos da rede. Então, é calculado o grau de similaridade (S) entre os clones de memórias, pelo módulo das suas distâncias. Com o objetivo de eliminar os clones de memórias com grau de similaridade inferior ao limiar de supressão σ_s , é utilizado a supressão clonal. Ao fim desse processo, a matriz clone de memória será concatenada com a matriz anticorpo de memória, formando uma “nova” matriz anticorpo de memória ($Ab_{\{m\}}$). O segundo passo calcula o grau de similaridade (S) entre os anticorpos de memória pelo módulo de suas distâncias. No terceiro passo é realizada a supressão da rede, retirando os anticorpos de memória com similaridade inferior ao limiar de σ_s . No quarto passo novos anticorpos ($Ab_{\{d\}}$) são gerados aleatoriamente e concatenados com os anticorpos de memória ($Ab_{\{m\}}$) na matriz anticorpos (A_b). Ao fim a rede se configurará e voltará para o primeiro passo, até que o critério de parada seja satisfeita.

```

function [Ab(m), S] = aiNet(Ag, L, gen, n,  $\zeta$ ,  $\sigma_d$ ,  $\sigma_s$ , d);
Ab := gera(N0, L); % Gera Ab inicial (N0 qualquer)
% A cada iteração, faça:
for t = 1 to gen, % Passo 1
    for j = 1 to M, % Passo 1.1
        f(j, :) := afinidade(Ab, Ag(j, :)); % Passo 1.1.1
        Ab(n)(j, :) := select(Ab, f(j, :), n); % Passo 1.1.2
        C := clona(Ab(n), 1, f(j, :)); % Passo 1.1.3
        C* := dmut(C, Ag(j, :), f(j, :)); % Passo 1.1.4
        f(j, :) := afinidade(C*, Ag(j, :)); % Passo 1.1.5
        M := select(C*, f(j, :),  $\zeta$ ); % Passo 1.1.6

        [M, f(j, :)] := suppress(M, 1/f(j, :),  $\sigma_d$ ); % Passo 1.1.7
        S := afinidade(M, M); % Passo 1.1.8
        [M, S] := suppress(M, S,  $\sigma_s$ ); % Passo 1.1.9
        Ab(m) := insere(Ab(m), M); % Passo 1.1.8
    end;
    S := afinidade(Ab(m), Ab(m)); % Passo 1.2
    [Ab(m), S] := suppress(Ab(m), S,  $\sigma_s$ ); % Passo 1.3
    Ab(d) := gera(d, L); % Gera Abd aleatoriamente
    Ab := insere(Ab(m), Ab(d)); % Passo 1.4
end;

```

Figura 12 – Pseudocódigo do AiNet (Castro, 2001)

3 POSICIONAMENTO DE NÓS USANDO REDES IMUNOLÓGICAS

Neste capítulo será apresentado à ferramenta computacional, chamada de POSIMNET, que auxilia ao projetista a obter uma configuração de rede onde cada sensor terá certo número de caminhos alternativos para se chegar ao *gateway*.

3.1 Modelagem do Problema

O posicionamento de nós roteadores em rede de sensores sem fio na indústria é uma tarefa complexa e de suma importância para a operação da rede. É através da posição final dos roteadores que podemos determinar o quão confiável, segura, disponível e robusta é a rede.

No POSIMNET, as células B que formam a rede imunológica serão compostas pelo conjunto de nós sensores e por um conjunto de nós roteadores. Os nós sensores estão localizados nos lugares onde a instrumentação da planta é necessária. Estes nós possuem coordenadas fixas, isto é, eles não podem ser movidos. Para que a segurança seja garantida é necessária a existência de caminhos redundantes entre estes nós e o *gateway*. O conjunto de nós roteadores é o conjunto de nós que será adicionado para permitir a redundância de caminhos, Figura 13. A posição destes nós será alterada durante o processo de obtenção da rede definitiva.

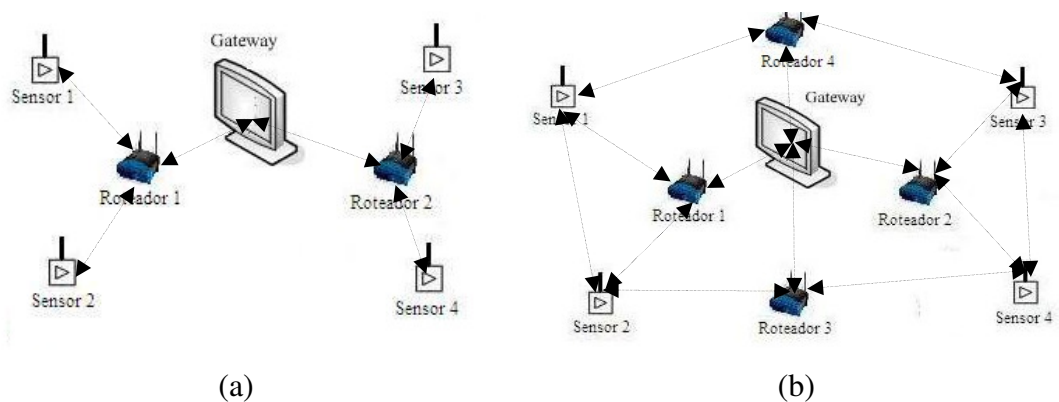


Figura 13 – Configuração da rede. (a) Sem caminhos redundantes; (b) Com caminhos redundantes.

Na etapa dinâmica, a estimulação das células B, conjunto de nós roteadores, será definida pelo grau de afinidade existente entre as células B na formação da rede. O papel de antígeno no POSIMNET não é realizado por um conjunto de dados separados como ocorre no AiNet e no SSAIS, mas o antígeno é visto de uma forma mais ampla como a entidade que estimula as células B. Sendo assim, a função do antígeno é realizada pela contabilização dos caminhos ausentes para os sensores críticos, pelo número de vezes que um roteador é usado e pela proximidade dos sensores.

A modelagem da afinidade das células B será a soma ponderada dos três critérios que o posicionamento de cada roteador poderá atender. Os critérios são: grau de falha de cada roteador, número de vezes que cada roteador é usado em função do caminho e número de nós sensores vizinhos a cada roteador (as funções matemáticas e as descrições detalhadas das afinidades serão descritas na próxima seção).

A etapa metadinâmica está dividida em dois processos: poda da rede e clonagem/mutação dos nós roteadores da rede. No processo de poda da rede, os n_p nós roteadores (parte do conjunto de células B) que durante um determinado tempo não conseguiram tornar-se útil a rede serão eliminados da rede. O último processo será responsável por gerar n_c clones dos nós roteadores mais estimulados. Os clones poderão sofrer mutação de duas naturezas: (i) Hipermutação – posiciona os novos elementos na rede de modo inversamente proporcional com grau de estimulação do nó roteador selecionado; e (ii) Condição Net de Mutação – posiciona os novos elementos na rede de forma a atender a condição NET (Poduri et al, 2006) entre o roteador selecionado e seus clones, isto é, seus clones são vizinhos do clone selecionado e existe pelo menos um vizinho a cada intervalo de ângulo teta (θ) de diferença entre eles.

Após a inclusão dos novos nós roteadores, é realizado o teste da condição de parada. Caso ele não seja atendido, todos os nós roteadores (parte das células B) sofrem a ação de forças repulsivas, geradas pelos obstáculos e por outros nós roteadores, e atrativas, geradas pelos nós sensores críticos, isto é, os sensores para os quais ainda não está determinado o número de caminhos necessários para chegar ao gateway. As ações dos campos potenciais repulsores nos nós roteadores têm a função de afastá-los de obstáculos, para permitir a visada direta entre os nós da rede para aumentar a confiabilidade da transmissão e também de aumentar a distância entre os roteadores para aumentar a cobertura da rede. Já os campos potenciais atrativos, atraem os roteadores para os sensores críticos, facilitando a formação de caminhos redundantes entre estes sensores e o gateway. Depois da ação dos campos

potenciais, a partir do novo posicionamento dos roteadores, uma nova rede é formada e o POSIMNET retorna para a etapa dinâmica até que o critério de parada seja atendido.

3.2 Descrição da Ferramenta

Nesta seção será descrita a ferramenta POSIMNET (*Positioning Immune Network – Rede Imunológica de Posicionamento*). A POSIMNET é uma ferramenta computacional baseada nas redes imunológicas artificiais, que resolve o problema de posicionamento de nós roteadores, de modo que todos os dispositivos sensores sejam capazes de se comunicarem com *gateway* de forma direta e/ou indireta por caminhos redundantes mais próximos.

A Figura 14 mostra os módulos principais da ferramenta que são utilizados para a construção da rede. O primeiro módulo é chamado de REDE IMUNOLÓGICA, agrega elementos de dois modelos de redes imunológicas (SSAIS e AiNet) e o segundo módulo é chamado POSICIONAMENTO POR CAMPOS POTENCIAIS que contém elementos usados no posicionamento de redes de sensores utilizando campos potenciais (Howard, 2002).

O módulo rede imunológica executa um algoritmo que pode ser descrito pelas seguintes etapas:

CRIAÇÃO: Criação de um conjunto inicial de células B para formar uma rede

AVALIAÇÃO: Determinação da afinidade das Células B para determinar a sua estimulação.

PODA: Faz o gerenciamento de Recursos e Retira da Rede as Células que estão sem recursos.

SELEÇÃO: Seleciona as Células B mais estimuladas para serem Clonadas.

CLONA: Gera um conjunto de Clones das Células B mais estimuladas.

MUTAÇÃO: Faz a mutação das Células Clonadas

Na etapa de criação, é gerado de forma aleatória um conjunto inicial de roteadores para dar início ao processo de obtenção da rede, sendo que o usuário pode especificar quantos roteadores ele deseja colocar inicialmente.

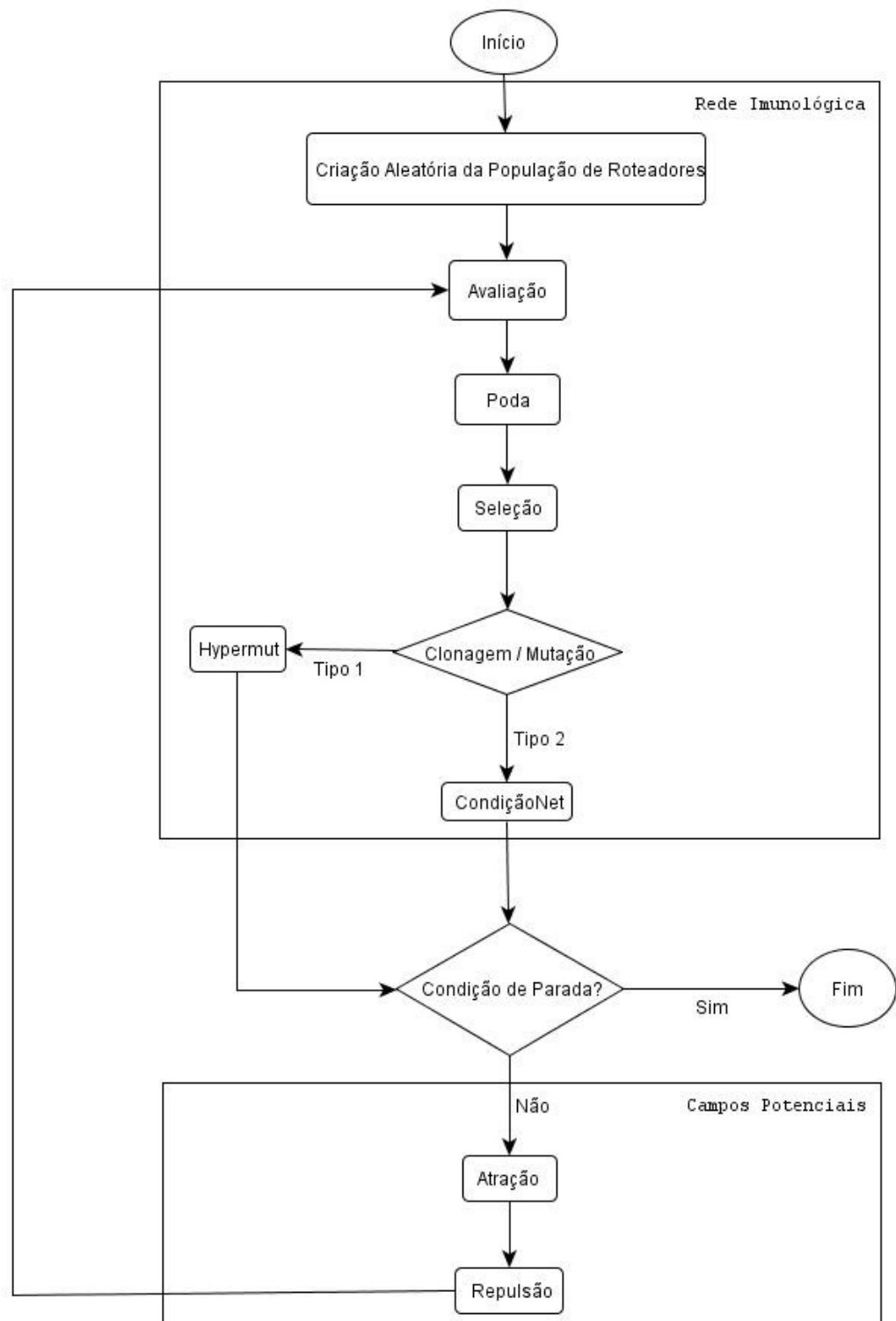


Figura 14 – Fluxograma do POSIMNET

Na etapa de avaliação, é formada uma rede com os nós sensores e os nós roteadores que é representada por um grafo. A partir deste grafo são obtidos os valores de diversas

variáveis que serão usadas para calcular a afinidade, tais como: o número de caminhos que existem entre cada sensor e o *gateway*, e o número de vezes que um roteador é usado nos caminhos formados. É importante destacar que o valor da afinidade é calculado para cada roteador e é composto por três parcelas, conforme descrito a seguir.

A primeira parcela fornece o grau de falha de cada roteador a rede – esta afinidade é a mais importante de todas. Ela definirá o quão importante é cada roteador na configuração da rede. Isto é realizado da seguinte forma: o roteador é retirado da rede, e verificam-se quantos caminhos permaneceram ativos para os sensores enviarem as suas informações ao *gateway*. Se o número de caminhos ativos restantes após a retirada do nó for pequeno, o nó roteador precisa de outro roteador próximo para diminuir o seu grau de falha. Além disso, no caso de fim da bateria ou problemas no roteador haverá outro caminho que a informação possa percorrer até que o mesmo seja substituído ou consertado.

A segunda parcela diz respeito ao número de vezes que cada roteador é usado nos caminhos que levam as informações dos sensores ao *gateway*. Quanto maior for o número de vezes que ele é usado, mais importante é esse roteador.

A terceira parcela se refere o número de nós sensores vizinhos a cada roteador – ao analisar esta afinidade pode-se dizer que quanto mais nós sensores vizinhos, maior será a probabilidade de que ele venha a fazer parte do caminho que o sensor necessita para transmitir a sua mensagem ao *gateway*.

3.2.1 Formulação das Afinidades

A afinidade (Equação 3) é composta por uma soma ponderada das três partes que são habilitadas a critério e necessidade dos usuários. Sendo assim, se o usuário achar que as parcelas afinidade 1 e 3, por exemplo, são fundamentais para a sua rede, o mesmo poderá desabilitar as outras afinidades e dar um peso, igual ou diferente, de modo que a soma seja 1, para as parcelas habilitadas.

$$Afinidade = \left(w1 * f_{Afinidade1} \right) + \left(w2 * f_{Afinidade2} \right) + \left(w3 * f_{Afinidade3} \right) \quad (3)$$

A Equação 4 define a primeira parcela da afinidade, levando em conta o grau de falha de cada roteador. Ele é calculado pela diferença normalizada entre número total de caminhos existentes entre os sensores e o *gateway* (valor da multiplicação dos números de sensores (*NumSensores*) pelo *k* caminhos (*Kpaths*)) e o número de caminhos restantes ao se retirar um determinado roteador da rede (*NumKpathsSemRoteador*), que esta sendo usado nos *k* caminhos. Os caminhos podem ser de duas formas: (i) Quaisquer – quando as informações são retransmitidas em alguns pontos pelo mesmo elo (*link*); (ii) Disjuntos – quando os dados são enviados por elos (*links*) diferentes. E sua determinação é feita pelos *k* menores caminhos existentes entre o sensor e o *gateway*. Os *k* menores caminhos quaisquer é calculado pelo algoritmo de Yen (Yen, 1971), que utiliza o algoritmo Dijkstra (Dijkstra, 1959) para encontrar o menor caminho entre dois nós com arestas positivas. Sendo assim, quanto maior o grau de falha, maior será a afinidade, e em consequência, mais crítica será a perda do roteador na rede.

$$Grau = \frac{(NumSensores * Kpaths) - NumKpathsSemRoteador}{NumSensores * Kpaths} \quad (4)$$

$$f_{Afinidade1} = Grau$$

A segunda parcela da afinidade, Equação 5, define o número de vezes que o roteador é usado em função do caminho. Ela é calculada utilizando o número de vezes que o roteador é usado nos caminhos formados (*NumVezeRoteadorUsado*) dividido pelo número de caminhos que devem existir, conforme a especificação do usuário. Este valor é calculado através da multiplicação dos números de sensores (*NumSensores*) pelos *k* caminhos (*Kpaths*), que usuário deseja que existam entre os sensores e o *gateway*. Quanto mais o roteador é usado, maior será a função afinidade.

$$f_{Afinidade2} = \frac{NumVezeRoteadorUsado}{(NumSensores * Kpaths)} \quad (5)$$

Por último, a Equação 6 fornecerá uma função de afinidade baseada nos sensores vizinhos (*NumSensoresVizinhos*) ao nós da rede. Esta afinidade está compreendida entre 0 e 1, sendo 1 o valor mais crítico para a rede.

$$f_{\text{Afinidade3}} = \frac{\text{NumSensoresVizinhos}}{\text{NumSensores}} \quad (6)$$

3.2.2 A Etapa de PODA

Na etapa de poda é feito o gerenciamento de recursos e eliminação dos roteadores que ficaram sem recursos. A idéia da utilização de recursos para o gerenciamento dinâmico do tamanho da rede está presente no SSAIS (Neal, 2002) e também foi utilizado aqui, embora com uma abordagem diferente. Enquanto que no SSAIS, os recursos aumentavam apenas para a célula mais estimulada e diminuía para todo o resto, o POSIMNET trata o recurso como o tempo necessário para que o roteador se torne útil à rede. Caso isso não ocorra, o roteador será eliminado da rede. Inicialmente, todos os roteadores recebem um valor inicial de recurso, determinado pelo usuário. Caso o roteador tenha afinidade maior do que certo limiar, o seu nível de recurso é mantido intacto. Se a afinidade estiver abaixo do limiar, então o recurso deste roteador será decrescido de uma unidade. Sendo assim, quando o recurso do roteador chegar ao valor zero, limiar de supressão da rede, o roteador será eliminado da rede. No entanto, é importante informar que só serão eliminados da rede os roteadores, desde que pelo menos um roteador fique atuando na rede.

3.2.3 As Etapas de Seleção, Clonagem e Mutação

Na etapa de seleção, a afinidade será ordenada de forma decrescente, onde os n_s melhores roteadores possam ser escolhidos com facilidade para a clonagem. A clonagem e mutação dos roteadores escolhidos poderá ser realizada por dois métodos (ClonaHyper e ClonaCondicaoNet), onde os métodos são classificados de acordo com a mutação usada em cada um (Hipermutação e Condição Net de Mutação). Ambos os métodos gerarão um número de roteadores adicionais à rede, que é definido pelo usuário. Além disso, é feita a divisão dos recursos entre o roteador selecionado e seus clones. Esta estratégia de gerenciamento de recursos faz com que os clones que não sejam úteis à rede sejam eliminados mais rapidamente.

3.2.3.1 ClonaHyper

O método clonaHyper, como descrito anteriormente, gera clones dos n_s roteadores selecionados, e muta-os pelo processo de hipermutação. A Hipermutação pode realizar a mutação de duas formas, gaussiana ou uniforme, e gera os novos roteadores de acordo com a afinidade dos n_s roteadores selecionados. Sendo assim, quanto maior a afinidade, mais próximo os clones se posicionarão do roteador selecionado, e quanto menor a afinidade, mais longe os clones se posicionarão do roteador selecionado.

No processo de mutação normal, as coordenadas X e Y do clone (filho) são geradas a partir das coordenadas do roteador selecionado (pai) considerando que se está gerando valores de uma distribuição normal cuja média é dada pelo valor da coordenada do pai e o desvio padrão é dado pelo parâmetro α conforme a Equação 7. A função $N(0,1)$ gera valor a partir de uma distribuição normal.

$$\begin{aligned} X_{filho} &= X_{pai} + \alpha \cdot N(0,1) \\ Y_{filho} &= Y_{pai} + \alpha \cdot N(0,1) \end{aligned} \tag{7}$$

O parâmetro α é calculado conforme pode ser visto na Equação 8, onde f representa a afinidade do roteador selecionado, sendo que esta está normalizada entre 0 e 1; $StdMut$ (*standard mutation*) representa o valor padrão de mutação, que no POSIMNET será igual ao raio de alcance dos sensores e roteadores e o parâmetro ρ é um fator multiplicativo da exponencial. De acordo com a Equação 8, o valor máximo de α (α_{max}) ocorre quando a afinidade f vale 0 e o valor mínimo (α_{min}) é obtido quando f igual a 1. Substituindo o valor de f por zero na Equação 8, obtem-se que α_{max} será igual a $StdMut$ e portanto igual ao raio de alcance, conforme pode ser visto na Equação 9. Para determinar o valor de ρ , arbitra-se que o valor de α_{min} seja igual a 10% do raio de alcance dos sensores e roteadores. Portanto, quando se substitui estes valores na Equação 8, obtém-se a Equação 10, de onde pode-se obter ρ (Equação 11). Sendo assim pela Equação 11 pode-se afirmar que ρ é igual a 2,3026.

$$\alpha = \exp^{(-f*\rho)} * StdMut \quad (8)$$

$$\alpha_{\max} = \exp^{(0)} * StdMut = StdMut \quad (9)$$

$$\alpha_{\min} = \exp^{(-\rho)} * StdMut = 0,1 \cdot StdMut \quad (10)$$

$$\rho = -\ln 0,1 = 2,3026 \quad (11)$$

A Equação 12 descreve a geração dos clones pela forma, respectivamente, uniforme. De forma semelhante ao caso gaussiano, coordenadas X e Y do clone são obtidas a partir coordenadas do roteador selecionado (pai) considerando que se está gerando valores de uma distribuição uniforme no intervalo entre -1 e 1 (U(-1,1)).

$$\begin{aligned} X_{filho} &= X_{pai} + \alpha \cdot U(-1,1) \\ Y_{filho} &= Y_{pai} + \alpha \cdot U(-1,1) \end{aligned} \quad (12)$$

3.2.3.2 ClonaCondicaoNet

O ClonaCondicaoNet é o segundo método de clonagem que o usuário tem como opção de escolha. Neste método os clones sofrem mutação do tipo condição NET (Figura 15). A condição NET (*Neighbor-Every-Theta* (θ)), proposta em (Poduri et al, 2006), define que cada roteador selecionado tem que ter pelo menos um vizinho dentro do setor angular θ do seu alcance de comunicação. Ao garantir a condição acima e posicionando os nós adicionais na borda do raio de comunicação, a nova topologia de rede garantirá uma maximização da cobertura da rede. No caso do POSIMNET, foi definido que o ângulo θ que define a condição NET dependerá do número de clones escolhido e será igual a $\frac{2\pi}{n_c}$. Os clones serão dispostos na circunferência dada pelo raio de alcance (R_c) de tal forma que exista entre dois clones consecutivos um ângulo θ . Por exemplo, se o número de clones escolhido for igual a 3, então a mutação condição NET posicionará três clones para cada um dos n_s roteadores selecionados,

de forma que o ângulo entre eles seja $\frac{2\pi}{3}$, ou seja, eles estarão dispostos com os ângulos $\gamma = [0, \frac{2\pi}{3} \text{ e } \frac{4\pi}{3}]$. Para garantir que a condição NET ocorra com diferentes rotações, acrescenta-se um ângulo β gerado por uma distribuição de probabilidade uniforme entre 0 e 2π .

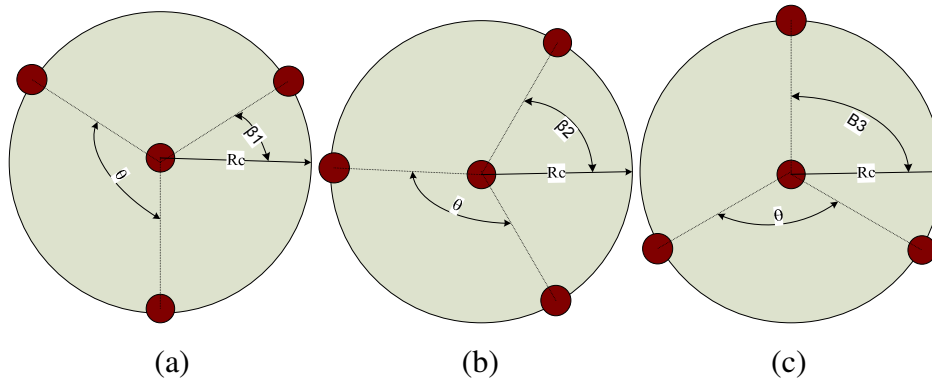


Figura 15 – Ilustração da Condição Net com ângulos $\theta=120^\circ$. (a) $\beta_1=30^\circ$; (b) $\beta_2=60^\circ$; (c) $\beta_3=90^\circ$.

As coordenadas X e Y dos roteadores clones (filhos) serão obtidas a partir das coordenadas do roteador selecionado (pai), conforme Equação 13.

$$\begin{bmatrix} X_{clone}^{(i)} & Y_{clone}^{(i)} \end{bmatrix} = \begin{bmatrix} X_{pai} & Y_{pai} \end{bmatrix} + (R_c \cdot [\cos(\beta + \gamma(i)) \quad \text{sen}(\beta + \gamma(i))]) \quad (13)$$

3.2.4 Módulo de Posicionamento por Campos Potenciais

O posicionamento dos roteadores é influenciado pela ação dos campos potenciais. Os roteadores são atraídos pelos chamados sensores críticos, isto é, por sensores que durante a formação da rede não conseguiram formar o número de caminhos necessários para chegar ao *gateway*, e repelidos pelos outros nós da rede e obstáculos. Cada roteador estará sujeito a um conjunto de forças F provenientes dos campos potenciais U , que são inversamente proporcionais a distância euclidiana entre os roteadores e os outros elementos da rede, conforme Equação 14.

$$F = -\nabla U \quad (14)$$

Conforme foi dito anteriormente, roteador sofrerá uma ação individual dos campos potenciais dos obstáculos, dos outros roteadores e dos sensores críticos, conforme Equação 15. Os campos potenciais são inversamente proporcionais à distância. Em consequência, a força também será composta pela soma das forças exercidas pelos obstáculos, pelos sensores e pelos roteadores em cada roteador.

$$\begin{aligned} U &= U_{obstaculos} + U_{Atração} + U_{Re pulsão} \\ F &= -(\nabla U_{Obstaculos} + \nabla U_{Atração} + \nabla U_{Re pulsão}) \\ F &= F_{obstaculos} + F_{Atração} + F_{Re pulsão} \end{aligned} \quad (15)$$

A $F_{Obstaculos}$ é a força que os obstáculos exercem sobre os roteadores, conforme Equação 16, onde $K_{obstaculos}$: constante de repulsão dos obstáculos, $x_i - x$: distância vetorial do roteador ao obstáculo i e $|x_i - x|$: módulo da distância do roteador ao obstáculo i . Essa força é repulsiva, e evita que os roteadores sejam posicionados dentro ou na borda dos obstáculos.

$$F_{Obstaculos} = -K_{Obstaculos} * \sum_i \frac{1}{|x_i - x|^2} * \frac{x_i - x}{|x_i - x|} \quad (16)$$

A $F_{Repulsão}$ está relacionada com a força de repulsão de cada roteador nos outros nós, determinada pela distância entre os dois, conforme Equação 17, onde $K_{Repulsão}$ é a constante de repulsão, $x_i - x$: distância vetorial do roteador ao nó i e $|x_i - x|$: módulo da distância do roteador ao nó i . Ela só terá efeito sobre o roteador, caso os dois nós estejam a uma distância menor que o raio de alcance.

$$F_{Re pulsão} = -K_{Re pulsão} * \sum_i \frac{1}{|x_i - x|^2} * \frac{x_i - x}{|x_i - x|} \quad (17)$$

A $F_{Atração}$ é a força de atração exercida pelos sensores críticos sobre cada roteador, calculada pela distância entre os dois, descrita na Equação 18, onde $K_{Atração}$ é a constante de atração, $x_i - x$: distância vetorial do roteador ao sensor crítico i e $|x_i - x|$: módulo da distância do roteador ao sensor crítico i . Essa força somente será exercida pelos nós sensores críticos, ou seja, os sensores que não apresentam os k caminhos, desejados.

$$F_{Atração} = K_{Atração} * \sum_i \frac{1}{(|x_i - x| - R_c)^2} * \frac{x_i - x}{|x_i - x|} \quad (18)$$

A constante de atração tem seu valor calculado em função da constante de repulsão, para que se um sensor crítico estiver próximo a um roteador, as forças de repulsão e atração exercidas pelo sensor fiquem em equilíbrio para uma determinada distância d , conforme pode ser visto na Equação 19. Esta distância pode ser expressa como uma fração do raio de alcance R_c , ou seja, $d = \eta R_c$, onde η representa a probabilidade que nós se desconectem, um valor baixo para η significa que eles estão próximos e dificilmente se desconectarão.

$$\begin{aligned} F_{Atração} &= F_{repulsão} \\ F_{Atração} &= \frac{K_{atração}}{(d - R_c)^2} = F_{repulsão} = \frac{K_{repulsão}}{(d)^2} \\ d &= \eta R_c \\ F_{Atração} &= \frac{K_{atração}}{(\eta R_c - R_c)^2} = F_{repulsão} = \frac{K_{repulsão}}{(\eta R_c)^2} \\ K_{atração} &= \frac{(\eta - 1)^2 \cdot K_{repulsão}}{\eta^2} \end{aligned} \quad (19)$$

Após definir a força resultante de cada nó roteador, será necessário calcular a nova posição dos roteadores. Ela começa pelo cálculo da aceleração, (Equação 20), passa pelo cálculo da velocidade, Equação 21 e por fim chega ao cálculo da nova posição dos roteadores, Equação 22. Para executar o cálculo da aceleração será necessário definir uma força que represente o atrito viscoso, para que na ausência de outras forças, o roteador pare de se locomover.

$$aceleração = \frac{(F_{resul\ tan\ te} - (v * velocidade))}{massa} \quad (20)$$

$$velocidade = (aceleração * dt) + velocidade_{atual} \quad (21)$$

$$Nos = (velocidade * dt) + Nos_{atual} \quad (22)$$

Tanto para a aceleração, velocidade e posição dos nós foram definidos limites para os valores máximos e mínimos destas variáveis para que o deslocamento acontecesse de forma gradual.

4 ESTUDO DE CASOS

Neste capítulo serão apresentados os estudos de casos que demonstram o comportamento do algoritmo POSIMNET, proposto por essa dissertação, na resolução do problema de posicionamento de nós roteadores em rede de automação industrial sem fio.

4.1 Descrição dos Estudos de Casos

Os testes do POSIMNET foram simulados em um cenário de área quadricular, com extensão normalizada de 1 x 1. Considera-se um cenário normalizado para que ele seja facilmente adaptado a quaisquer outras dimensões. Além disso, foram definidos que η será de 80% e $K_{repulsão}$ será igual a 1, ou seja, quando um nó roteador afasta-se de um nó sensor crítico 80% do raio de alcance as forças de repulsão e atração exercidas pelos sensores estão em equilíbrio. No entanto para o cálculo da aceleração dos nós roteadores serão considerados os valores da massa igual a 1 e da v de $0,25 \frac{N.s}{m^2}$, para que não haja oscilação do sistema. Como parâmetro de clonagem foi escolhido que apenas o roteador com maior afinidade será selecionado para produzir três clones a cada geração. Na definição do valor do recurso será considerado recurso igual ao recurso inicial quando a afinidade for maior que o zero, e recurso decrescido de uma unidade quando a afinidade for igual a zero. Sendo assim, para cada estudo de caso foram realizados 10 experimentos, que comprovam a capacidade do POSIMNET em criar n caminhos redundantes para a informação chegar ao *gateway*.

4.2 Estudo de Casos nos Cenários POSA e POSB.

Dois cenários foram elaborados para demonstrar as funcionalidades do algoritmo desenvolvido, POSIMNET. O primeiro cenário (POSA) é formado por cinco nós de rede, sendo os nós 2, 3, 4 e 5 como sensores fixos e o nó 1 como *gateway*, em formato de cruz. Inicialmente no cenário POSA, o *gateway* está em visada direta com todos os nós da rede,

porém não há nenhuma conectividade entre eles, ou seja, as distâncias entre eles é maior do que os seus raios de alcance, conforme Figura 16 (a). O segundo cenário (POSB) é constituído por 9 nós de rede, sendo o nó 1 como *gateway* e os outros nós como sensores fixos. Como no cenário POSA, inicialmente no cenário POSB o *gateway* está em visada direta com todos os nós da rede, porém não há nenhuma conectividade entre eles, conforme Figura 16 (b).

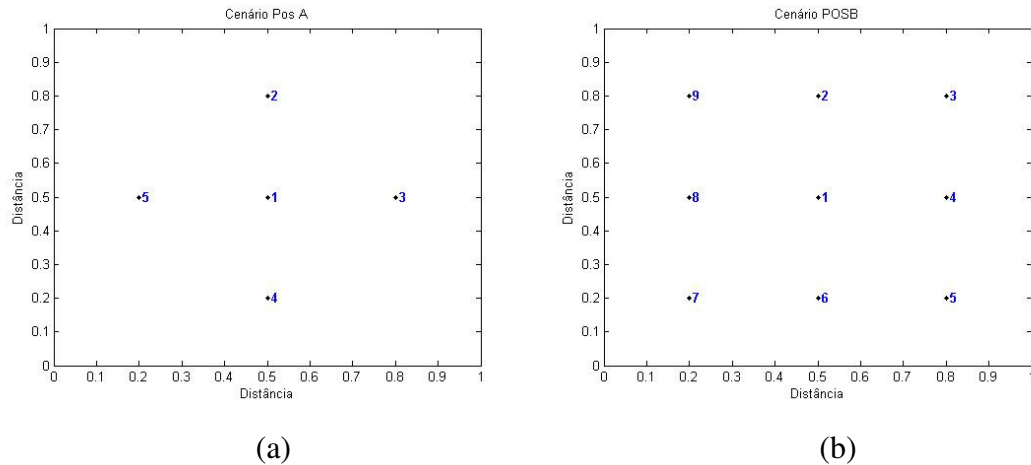


Figura 16 – Posicionamento dos nós sensores e do *gateway*. (a) POSA; (b) POSB.

Nas simulações do POSIMNET foram propostos 6 estudos de casos, de acordo com a Tabela 1. Cada estudo de caso considerou um tipo de cenário, um raio de alcance dos elementos da rede e um tipo e número de caminhos (*Kpaths*) para as informações chegarem ao nó central. Nos dois primeiros casos, a configuração de rede é o POSA e o seu raio de alcance está definido em 0,2. Entretanto, no caso 1 é desejável que os dados tenham dois caminhos quaisquer (as informações enviadas por um sensor podem ser retransmitidas, em alguns pontos, pelo mesmo roteador) e no caso 2 tenham dois caminhos disjuntos (os dados enviados por um sensor é encaminhado por elos (links) diferentes, podendo os links terem roteador em comum) para chegarem ao *gateway*. Nos casos 3 e 4 o raio de alcance foi reduzido para 0,1 e a configuração de rede também é o POSA. Contudo, eles têm o objetivo de posicionar os roteadores de forma que as informações percorram dois caminhos quaisquer (caso 3) e três caminhos disjuntos (caso 4). Os dois últimos casos utilizam o cenário POSB, e apresentam características de rede diferentes. Sendo assim, no caso 5 o raio de alcance é 0,2 e a formação de dois caminhos quaisquer, e no caso 6 o raio de alcance é 0,1 e a especificação de é três caminhos disjuntos.

Como explanado anteriormente, o objetivo do POSIMNET será posicionar os nós roteadores para que os dados cheguem ao *gateway* por dois e três caminhos quaisquer e dois e

três caminhos disjuntos. Para que isso ocorra, serão necessários alguns experimentos iniciais para encontrar o melhor conjunto de parâmetros para POSIMNET atender o objetivo de obter caminhos redundantes com o menor índice de falha. Os parâmetros escolhidos (descritos nas Tabelas 2, 4, 6, 8, 10 e 12) foram definidos para as simulações de cada caso dos dois cenários.

Tabela 1 – Estudo de Casos - Cenário

Estudo de Casos	Configuração	Raio	Caminhos	Kpaths
1	POSA	0.2	Quaisquer	2
2	POSA	0.2	Disjuntos	2
3	POSA	0.1	Quaisquer	2
4	POSA	0.1	Disjuntos	3
5	POSB	0.2	Quaisquer	2
6	POSB	0.1	Disjuntos	3

4.2.1 Estudo de Caso 1 – Cenário POS A

Nesta simulação o objetivo para o POSIMNET é obter dois caminhos quaisquer para cada sensor transmitir os dados monitorados para o nó central. Para tal, foi necessário utilizar o operador *ClonaHyper* e o peso 1 para afinidade grau de falha, conforme descrito na Tabela 2. Após realização de dez experimentos, a melhor configuração de rede pode ser vista na Figura 17, e a consolidação dos testes está descrita na Tabela 3.

Tabela 2 – Caso 1 – Cenário – Parâmetros

Parâmetros do POSIMNET	Valores	Método
Número de gerações	50	-
Número inicial de Roteadores	10	-
Recurso inicial fornecido	5	-
Operador de mutação	-	<i>ClonaHyper</i>
Afinidade	-	Grau de Falha

Como pode ser visto na Tabela 3, os pontos positivos desse estudo de caso são: (i) A previsão inicial do número de roteadores se mostrou adequada; (ii) Todos os cinco sensores conseguiram enviar seus dados por dois caminhos quaisquer; (iii) O grau de falha ficou em no máximo 40% em apenas um roteador, sendo que na média dos experimentos o grau de falha ficou em 0,27; (iv) O número de saltos até o *gateway* ficou estabilizado em três saltos para no máximo três sensores; (v) Apenas um roteador foi utilizado três vezes.

A Figura 18 representa a evolução do algoritmo POSIMNET para formar a melhor configuração de rede (Figura 17) dos 10 experimentos. Na Figura 18 pode-se observar que após 30ª geração, os índices de número de nós, de grau de falha, de número de caminhos detectados, de número de sensores críticos e de número de roteadores usados são quase ou totalmente estabilizados. Na Figura 17 é observado que um dos caminhos do nó sensor 3 apresenta três saltos (3-7-8-1) para as informações coletadas por ele cheguem ao *gateway*, ou seja, em um caminho a informação precisou ser retransmitida por dois roteadores para chegar ao nó central. Com relação ao grau de falha, todos os oito nós roteadores tem 20% de grau de tolerância de falha. Isto significa que 80% dos caminhos dos sensores para o *gateway*, continuam a existir mesmo após a retirada de um nó. Com relação ao máximo número de roteadores usados em função dos caminhos, o nó roteador 8 é usado duas vezes, nos caminhos 3-8-1 e 3-7-8-1. Em consequência, este roteador terá um consumo de bateria maior do que os outros, o que fará com que ele pare de funcionar e seja desligado da rede. Entretanto mesmo que isto aconteça, ainda haverá um caminho (3-7-10-1) para o nó 3 se comunicar.

Pelo exposto acima, o POSIMNET foi capaz de posicionar os nós roteadores para atender o critério de no mínimo dois caminhos redundantes com o menor índice de falha dos nós intermediários.

Tabela 3 – Desempenho da Rede

REDE	MÍNIMO	MÉDIA	MÁXIMO	STD
Número de Nós	13	13,7	15	0,67
Número de Roteadores	8	8,7	10	0,67
Número de Sensores Críticos	0	0	0	0,00
Max. Grau de Falha	0,2	0,27	0,4	0,08
Num. de Roteadores com Max. Grau de Falha	1	5,1	10	3,98
Tamanho Máximo dos Caminhos	3	3	3	0,00
Número de Nós com Tamanho Máximo	1	1,8	3	0,63
Num. Max. de Vezes que Roteador é Usado	1	2,1	3	0,57
Número de Roteadores que são Mais Usados	1	2	9	2,49

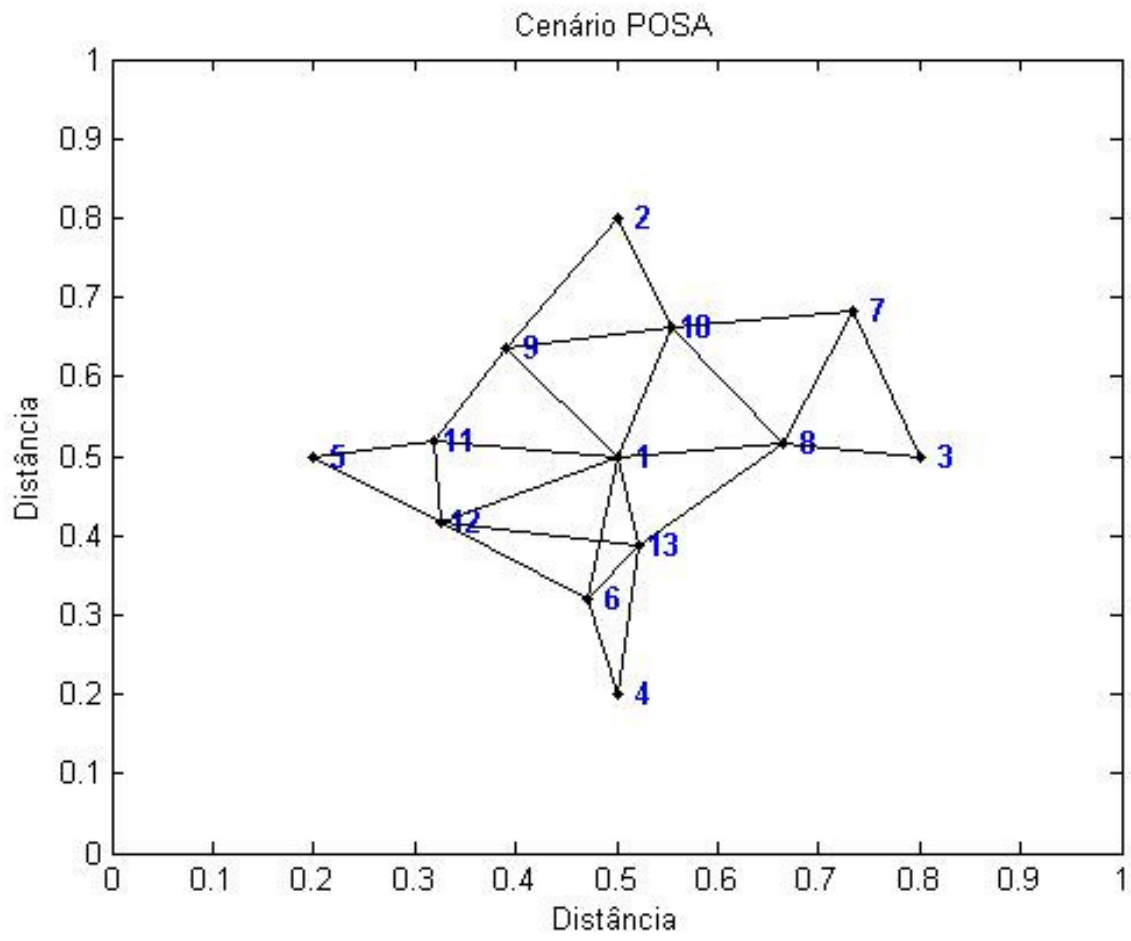


Figura 17 - Estudo do Caso 1 – Cenário POSA



Figura 18 – Trace do Caso 1

4.2.2 Estudo de Caso 2 – Cenário POS A

Nesta simulação o objetivo para o POSIMNET é obter dois caminhos disjuntos para cada sensor transmitir os dados monitorados para o nó central. Para tal, foi necessário utilizar o operador *ClonaCondicaoNet* e o peso 1 para afinidade grau de falha, conforme descrito na Tabela 4. Após realização de dez experimentos, a melhor configuração de rede pode ser vista na Figura 19, e a consolidação dos testes está descrita na Tabela 5. Comparando com o estudo de caso 1, apenas dois dos 10 experimentos precisaram acrescentar nós roteadores adicionais ao número inicial de roteadores.

Tabela 4 – Caso 2 – Cenário – Parâmetros

Parâmetros do POSIMNET	Valores	Método
Número de gerações	50	-
Número inicial de Roteadores	10	-
Recurso inicial fornecido	5	-
Operador de mutação	-	<i>ClonaCondicaoNet</i>
Afinidade	-	Grau de Falha

Comparando os resultados da Tabela 5 com o estudo de caso 1, pode-se destacar os seguintes pontos positivos: (i) O máximo grau de falha dos roteadores ficou estável em 30%; (ii) O número máximo de vezes que o roteador é usado permanece constante; (iii) Acréscimo de uma unidade nos hops para as informações chegarem ao nó central. Com relação aos pontos negativos pode-se destacar o número final dos nós roteadores, que se estabilizou em no máximo treze nós intermediários, sendo então, adicionados três roteadores aos dez iniciais.

A Figura 20 representa a evolução do algoritmo POSIMNET para formar a melhor configuração de rede (Figura 19) dos 10 experimentos. Na Figura 20 pode-se observar que após 5ª geração, os índices de número de sensores críticos, de número de nós, de grau de falha dos roteadores, de número de caminhos detectados, de número de sensores críticos e de numero de roteadores usados são quase ou totalmente estabilizados. Na figura 19 é observado que o nó sensor 2 e 4, nos caminhos 4-7-10-1 e 2-12-14-1, apresentam três saltos até o *gateway*. Isso significa que a informação enviada por esse dispositivo sofrerá um atraso para ser recebida pelo nó central, já que ela vai precisar ser retransmitida por dois nós intermediários. Com relação ao grau de falha, oito nós intermediários tem 30% de grau de falha, e o nó roteador 10 e 14 tem uma percentagem menor do que 30% de grau de falha. Sendo assim, a rede é bem tolerante a perda dos nós 10 e 14, permanecendo todos os sensores com dois caminhos disjuntos nas suas ausências. Com relação ao máximo número de roteadores usados em função dos caminhos, todos os nós roteadores são usados apenas uma vez em função do caminho. Ou seja, todos os nós intermediários terão o mesmo consumo de energia e o mesmo tempo de vida.

Tabela 5 – Desempenho da Rede

REDE	MÍNIMO	MÉDIA	MÁXIMO	STD
Número de Nós	13,00	14,70	18,00	1,42
Número de Roteadores	8,00	9,70	13,00	1,42
Número de Sensores Críticos	0,00	0,00	0,00	0,00
Max. Grau de Falha	0,30	0,30	0,30	0,00
Num. de Roteadores com Max. Grau da Falha	8,00	8,10	9,00	0,32
Tamanho Máximo dos Caminhos	3,00	3,10	4,00	0,32
Número de Nós com Tamanho Máximo	1,00	2,20	4,00	1,03
Num. Max. de Vezes que Roteador é Usado	1,00	2,00	3,00	0,47
Número de Roteadores que são Mais Usados	1,00	2,30	10,00	2,79

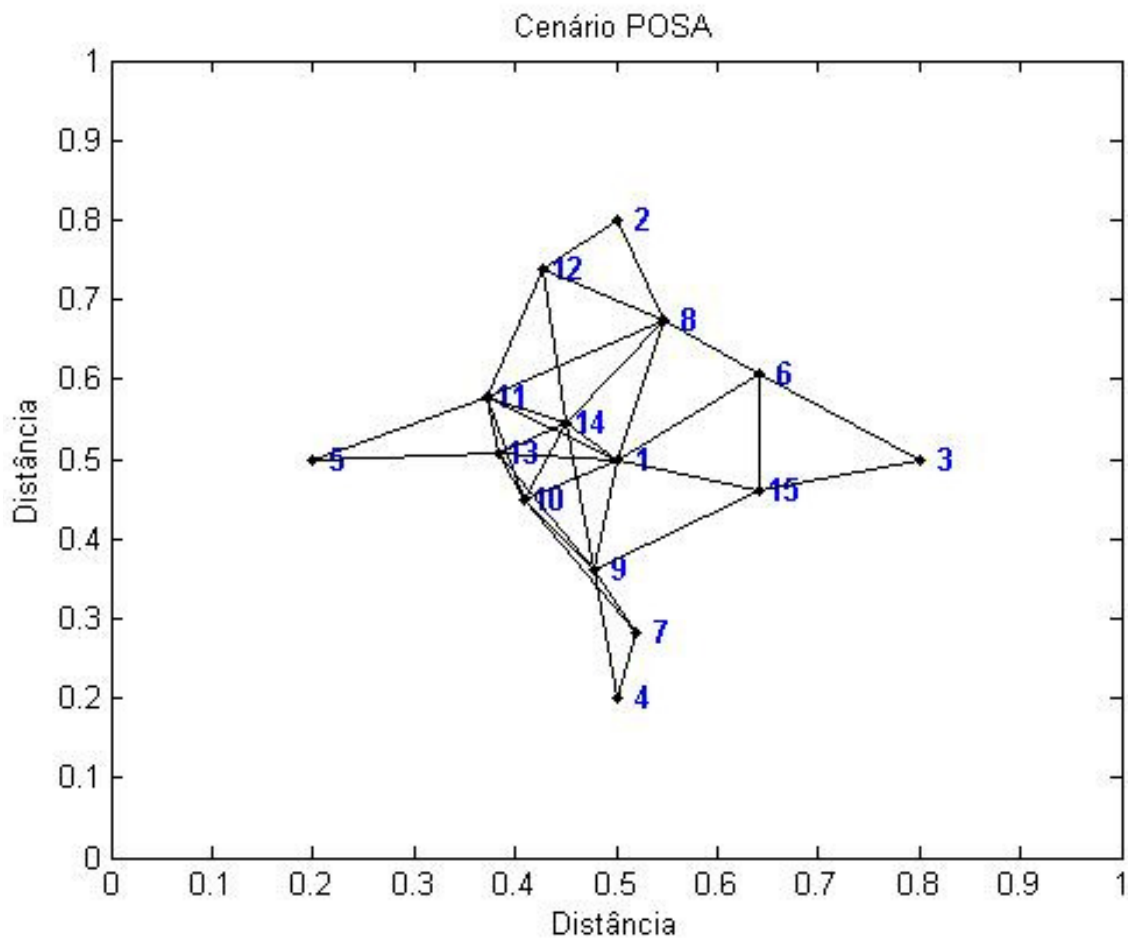


Figura 19 - Estudo do Caso 2 – Cenário POSA

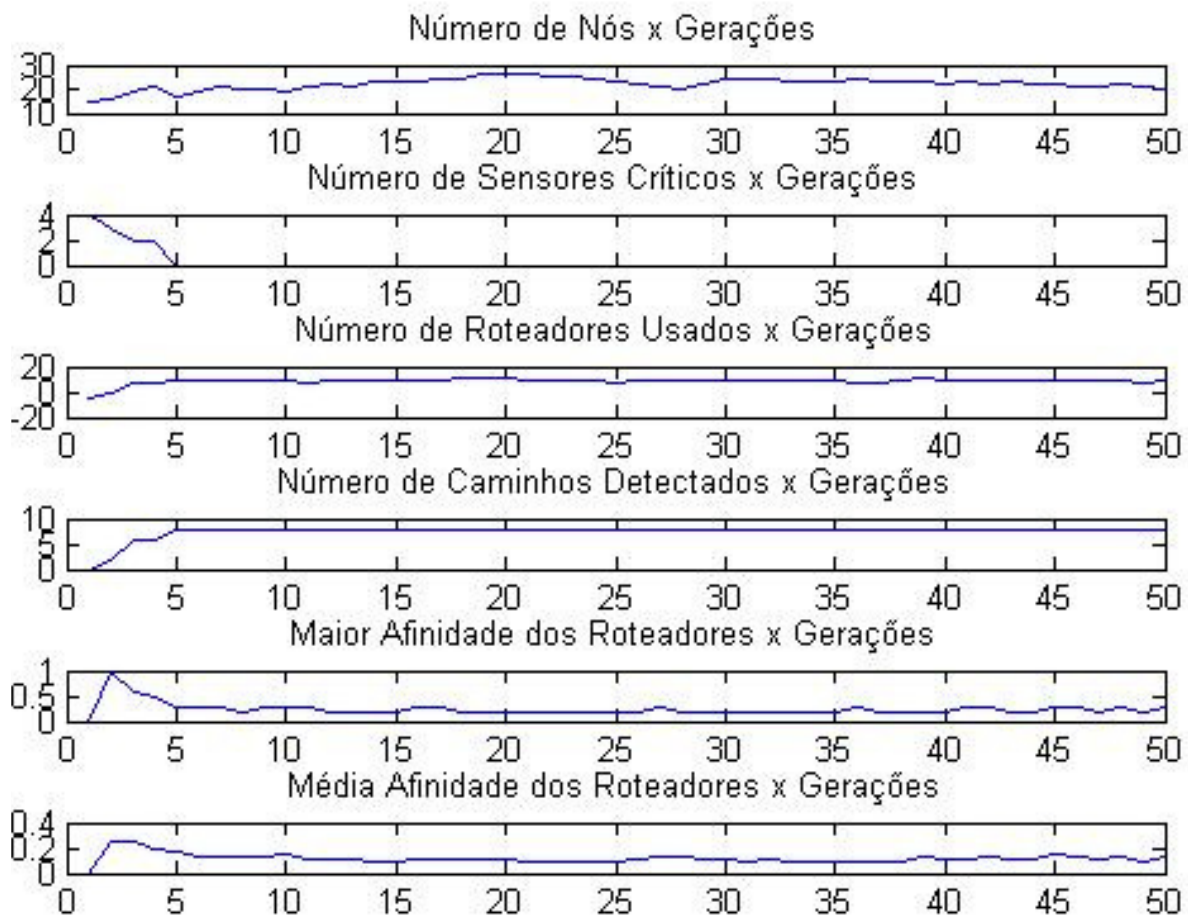


Figura 20 – Trace do Caso 2

4.2.3 Estudo de Caso 3 – Cenário POS A

Nesta simulação o objetivo para o POSIMNET é obter dois caminhos quaisquer para cada sensor transmitir os dados monitorados para o nó central, com raio de alcance dos elementos da rede de 0,1. Para tal, foi necessário utilizar o operador *ClonaCondicaoNet* e o peso 1 para afinidade grau de falha, conforme descrito na Tabela 6. Após realização de dez experimentos, a melhor configuração de rede pode ser vista na Figura 21, e a consolidação dos testes está descrita na Tabela 7. Antes de começar a análise desse experimento, é importante ressaltar que o seu raio de alcance é a metade do proposto nos casos 1 e 2, e em consequência, espera-se que seja necessário um maior número de roteadores e saltos no caminho.

Tabela 6 – Caso 3 – Cenário – Parâmetros

Parâmetros do POSIMNET	Valores	Método
Número de gerações	90	-
Número inicial de Roteadores	15	-
Recurso inicial fornecido	30	-
Operador de mutação	-	<i>ClonaCondicaoNet</i>
Afinidade	-	Grau de Falha

Como pode ser visto na Tabela 7, os pontos positivos desse estudo de caso são: (i) Todos os cinco sensores conseguiram enviar seus dados por dois caminhos quaisquer; (ii) O grau de falha ficou em no máximo 40%; (iii) O número de saltos até o *gateway* ficou estabilizado em seis saltos para no máximo um sensor; (iv) Apenas um roteador foi utilizado três vezes.

A Figura 22 representa a evolução do algoritmo POSIMNET para formar a melhor configuração de rede (Figura 21) dos 10 experimentos. Na Figura 22 pode-se observar que após 82ª geração, os índices de número de sensores críticos, de número de nós, de grau de falha dos roteadores, de número de caminhos detectados e de número de roteadores usados são quase ou totalmente estabilizados. Na Figura 21 é observado que os nós sensores 2, 4 e 5, nos caminhos 2-7-10-30-9-1, 4-23-15-29-18-1 e 5-20-11-19-9-1, apresenta cinco saltos até o *gateway*. Isso significa que a informação enviada por esses dispositivos sofrerão um atraso para ser recebida pelo nó central, já que ela vai precisar ser retransmitida por quatro nós intermediários. Com relação ao grau de falha, todos os nós intermediários têm 20% de Grau de falha. Sendo assim, todos os nós roteadores apresentam o mesmo grau de importância na rede. Com relação ao máximo número de roteadores usados em função dos caminhos, o nó roteador 9 é usado três vezes em função dos caminhos (2-7-10-30-9-1, 2-26-30-9-1 e 5-20-11-19-9-1). Ou seja, este dispositivo terá o seu tempo de vida reduzido, devido o seu alto índice de retransmissão. Mesmo que este roteador pare de operar, os nós 2 e 5 ainda terão caminhos para transmitir seus dados, como por exemplo, os caminhos 2-26-30-19-14-25-1 e 5-21-14-25-1.

Tabela 7 – Desempenho da Rede

REDE	MÍNIMO	MÉDIA	MÁXIMO	STD
Número de Nós	21,00	26,60	30,00	3,13
Número de Roteadores	16,00	21,60	25,00	3,13
Número de Sensores Críticos	0,00	0,00	0,00	0,00
Max. Grau de falha	0,20	0,36	0,40	0,08
Num. de Roteadores com Max. Grau de Falha	1,00	9,30	25,00	8,59
Tamanho Máximo dos Caminhos	4,00	5,10	6,00	0,57
Número de Nós com Tamanho Máximo	1,00	2,20	4,00	1,03
Num. Max. de Vezes que Roteador é Usado	2,00	2,60	3,00	0,52
Número de Roteadores que são Mais Usados	1,00	3,00	8,00	2,71

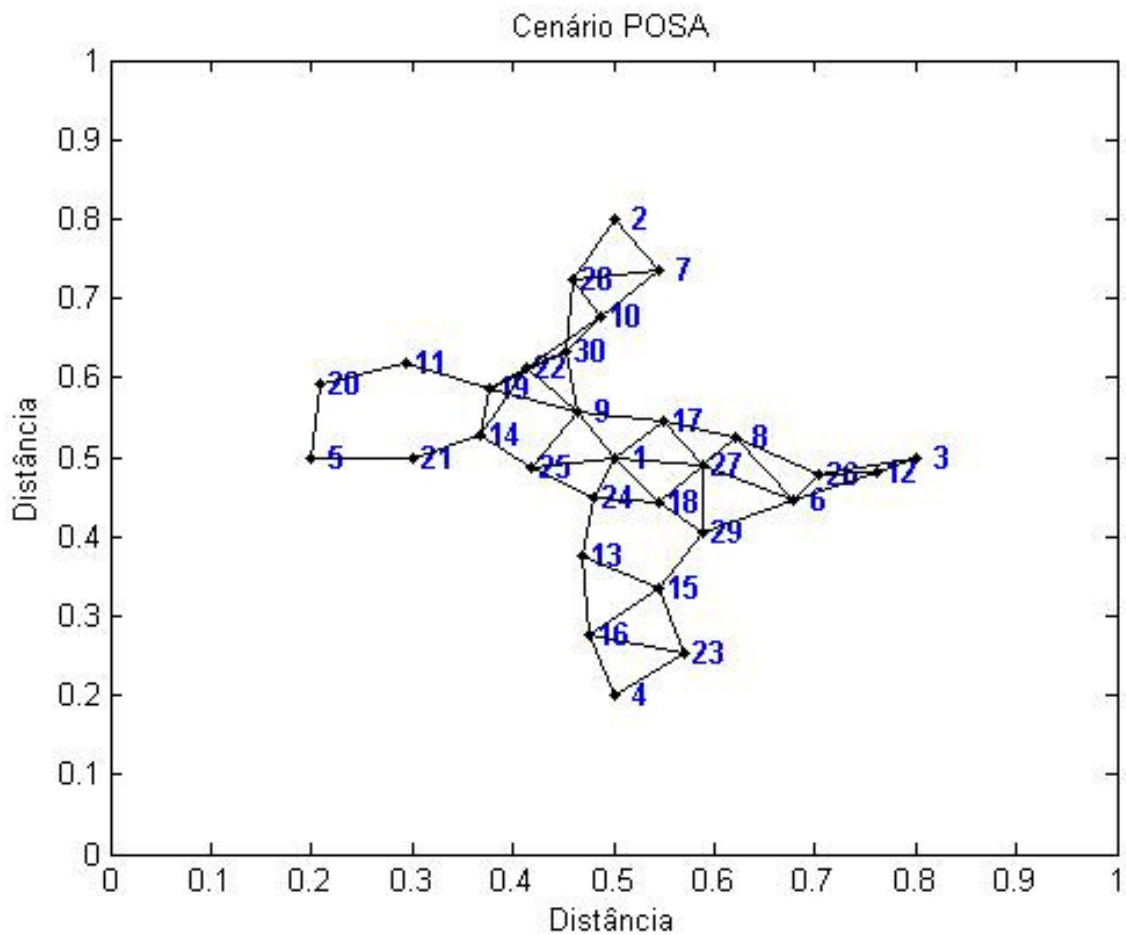


Figura 21 - Estudo do Caso 3 – Cenário POSA

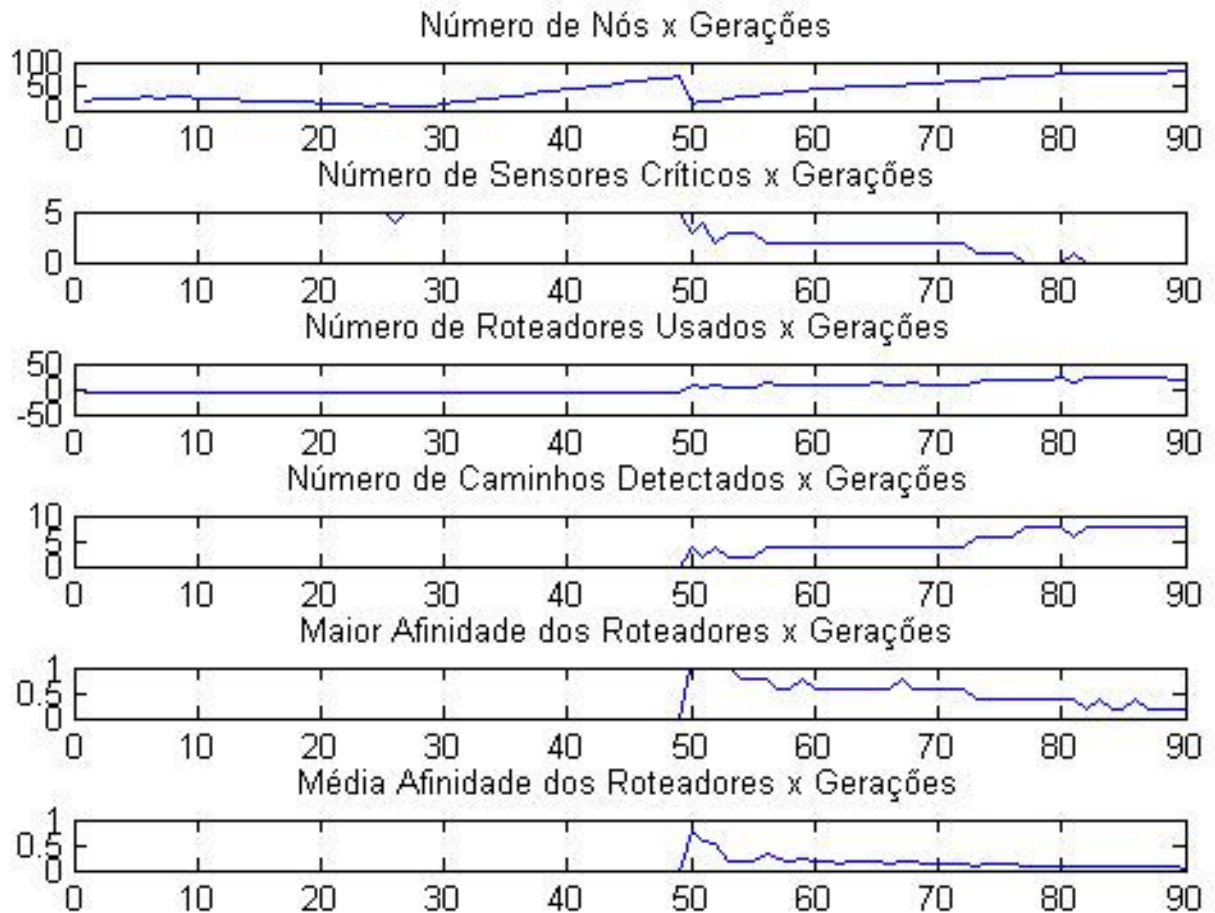


Figura 22 – Trace do Caso 3

4.2.4 Estudo de Caso 4 – Cenário POS A

Nesta simulação o objetivo para o POSIMNET é obter três caminhos disjuntos para cada sensor transmitir os dados monitorados para o nó central, com o raio de alcance dos elementos da rede de 0,1. Para tal, foi necessário utilizar o operador *Hipermut* e o peso 1 para afinidade grau de falha, conforme descrito na Tabela 8. Após realização de dez experimentos, a melhor configuração de rede pode ser vista na Figura 23, e a consolidação dos testes está descrita na Tabela 9. Antes de começar a análise desse experimento, é importante ressaltar que o seu raio de alcance é a metade do proposto nos casos 1 e 2, e em consequência, espera-se que seja necessário um maior número de roteadores e saltos no caminho.

Tabela 8 – Caso 4 – Cenário – Parâmetros

Parâmetros do POSIMNET	Valores	Método
Número de gerações	100	-
Número inicial de Roteadores	15	-
Recurso inicial fornecido	30	-
Operador de mutação	-	<i>Hipermut</i>
Afinidade	-	Grau de Falha

Como pode ser visto na Tabela 9, os pontos positivos desse estudo de caso são: (i) Não há sensores críticos; (ii) O grau de falha ficou em no máximo 40%, em apenas um experimento; (iv) Apenas um roteador foi utilizado cinco vezes. Como ponto negativo pode-se citar o número máximo de hop até o *gateway*, que foi igual a 9 em dois experimentos para o sensor 4.

A Figura 24 representa a evolução do algoritmo POSIMNET para formar a melhor configuração de rede (Figura 23) dos 10 experimentos. Na Figura 24 pode-se observar que após 75ª geração, os índices de número de sensores críticos, de número de nós, de grau de falha dos roteadores, de número de caminhos detectados e de número de roteadores usados são quase ou totalmente estabilizados. Na Figura 23 é observado que os nós sensores 3 e 5, nos caminhos 3-29-25-27-10-41-1, 3-44-22-28-26-13-1 e 5-43-35-18-12-41-1, apresenta seis saltos até o *gateway*. Isso significa que a informação enviada por esses dispositivos sofrerão um atraso para ser recebida pelo nó central, já que ela vai precisar ser retransmitida por cinco nós intermediários. Com relação ao grau de falha, os nós intermediários 22 e 26 têm 33,33% de grau de falha, e os outros têm o grau de falha menor do que 33,33%. Isso significa que pelo menos 66,67% dos caminhos dos sensores para o *gateway* continuam a existir mesmo após a retirada de um nó. Com relação ao máximo número de roteadores usados em função dos caminhos, os nós roteadores 13, 21 e 41 são usados três vezes em função dos caminhos 3-29-25-27-10-41-1, 3-22-6-26-13-1, 3-44-22-28-26-13-1, 4-40-21-41-1, 4-30-31-10-13-1, 4-7-21-12-11-1 e 5-43-35-18-21-41-1. Ou seja, este dispositivo terá o seu tempo de vida reduzido, devido o seu alto índice de retransmissão. Isso significa que mesmo que esses dispositivos parem de funcionar os sensores 3, 4 e 5 ainda terão pelo menos um caminho (3-44-22-28-26-14-1, 4-40-18-12-11-1 e 5-42-20-19-1) para transmitir suas informações ao *gateway*.

Tabela 9 – Desempenho da Rede

REDE	MÍNIMO	MÉDIA	MÁXIMO	STD
Número de Nós	39	44,1	46	2,02
Número de Roteadores	34	39,1	41	2,02
Número de Sensores Críticos	0	0	0	0,00
Max. Grau de Falha	0,27	0,33	0,4	0,03
Num. de Roteadores com Max. Grau de Falha	1	5,2	22	6,11
Tamanho Máximo dos Caminhos	6	7,3	9	1,06
Número de Nós com Tamanho Máximo	1	1,9	4	1,10
Num. Max. de Vezes que Roteador é Usado	2	3,5	5	0,97
Número de Roteadores que são Mais Usados	1	2,9	9	2,51

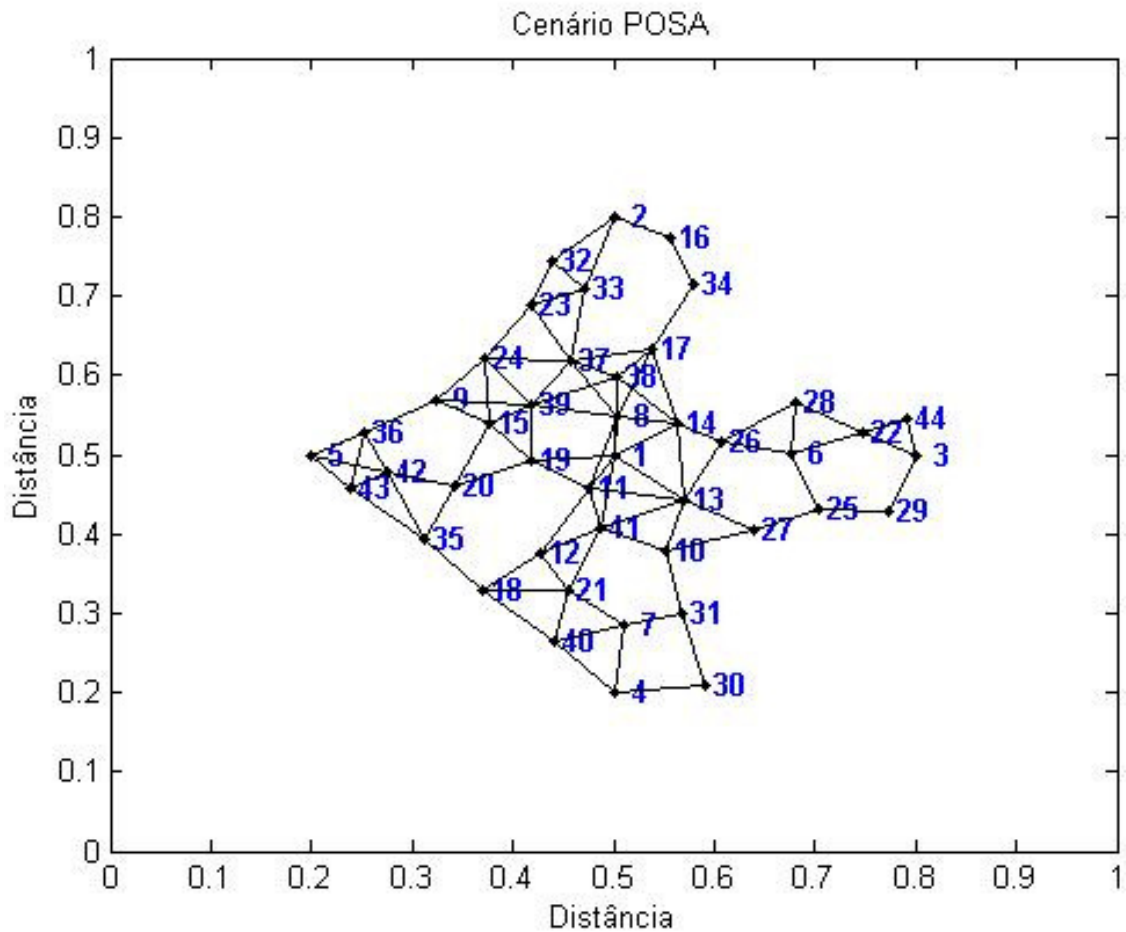


Figura 23 - Estudo do Caso 4 – Cenário POSA

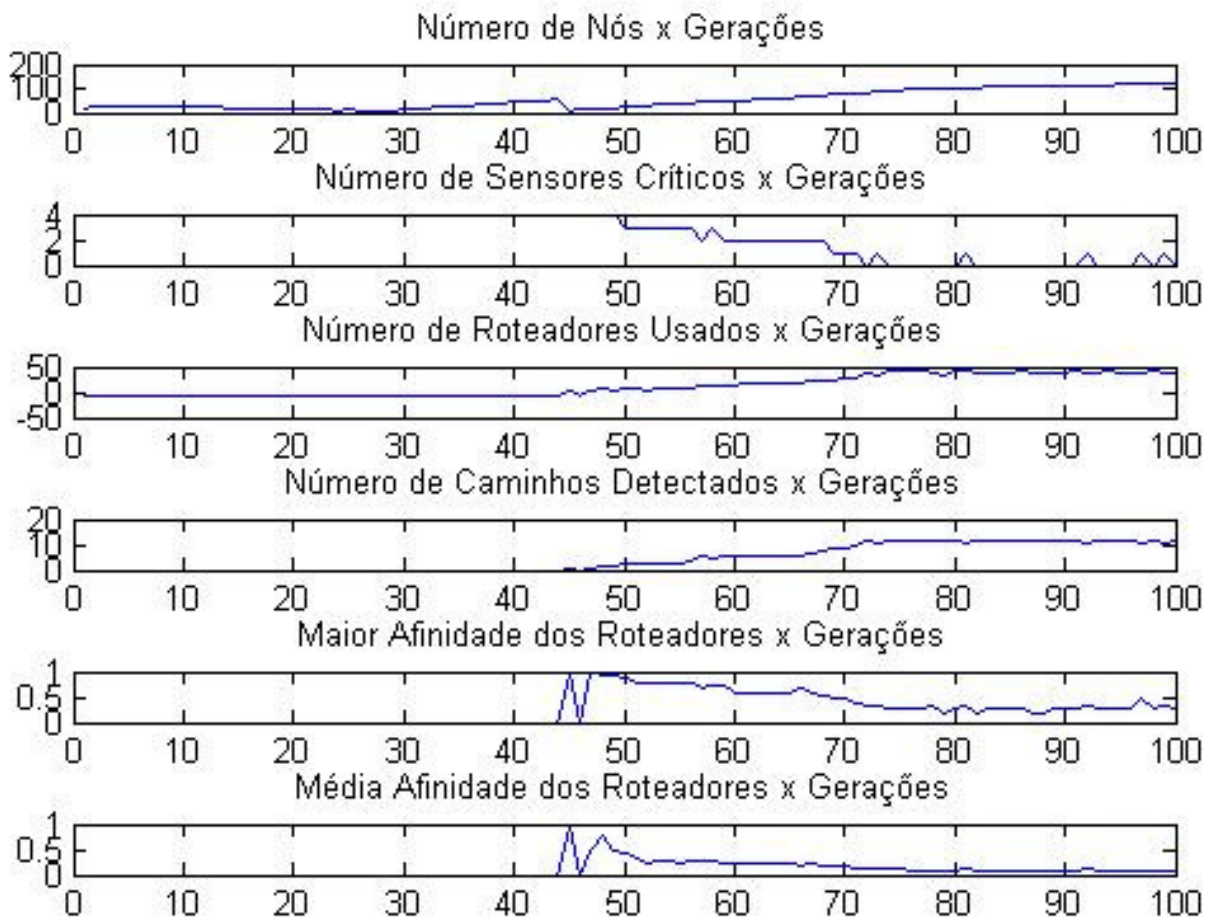


Figura 24 – Trace do Caso 4

4.2.5 Estudo de Caso 5 – Cenário POS B

Nesta simulação o objetivo para o POSIMNET é obter dois caminhos quaisquer para cada sensor transmitir os dados monitorados para o nó central, com raio de alcance de 0,2 e com a configuração POSB. Para tal, foi necessário utilizar o operador *ClonaCondicaoNet* e os pesos de 0,5 para a afinidade grau de falha, 0,25 para a afinidade número de vezes que o roteador é usado em função dos caminhos e 0,25 para a afinidade número de sensores vizinhos, conforme descrito na Tabela 10. Sendo assim, objetivo do POSIMNET será obter dois caminhos redundantes quaisquer atendendo os critérios de afinidade de grau de falha, de número de vezes que o roteador é usado em função dos caminhos e de número de sensores vizinhos. Após realização de dez experimentos, a melhor configuração de rede pode ser vista na Figura 25, e a consolidação dos testes está descrita na Tabela 11.

Tabela 10 – Caso 5 – Cenário – Parâmetros

Parâmetros do POSIMNET	Valores	Método
Número de gerações	15	-
Número inicial de Roteadores	3	-
Recurso inicial fornecido	5	-
Operador de mutação	-	<i>ClonaCondicaoNet</i>
Afinidade	-	Grau de falha, Número de Vezes que o Roteador é Usado e Número de Sensores Vizinhos

Conforme demonstrado na Tabela 11, os pontos positivos deste estudo de caso são: (i) O grau de falha ficou estável em 0,22%; (ii) O número de hops (saltos) até o *gateway* é entre 3 e 4; (iii) Mesmo utilizando um baixo número de roteadores iniciais (três roteadores), o algoritmo foi capaz de atender o objetivo e as afinidades requisitados, com o acréscimo de no mínimo onze nós roteadores.

A Figura 26 representa a evolução do algoritmo POSIMNET para formar a melhor configuração de rede (Figura 25) dos 10 experimentos. Na Figura 26 pode-se observar que após 13ª geração, os índices de número de sensores críticos, de número de nós, de grau de falha dos roteadores, de número de caminhos detectados e de número de roteadores usados são quase ou totalmente estabilizados. Na Figura 25 é observado que o nó sensor 3, no caminho 3-15-17-13-1, apresenta quatro saltos até o *gateway*. Isso significa que a informação enviada por esses dispositivos sofrerão um atraso para ser recebida pelo nó central, já que ela vai precisar ser retransmitida por três nós intermediários. Com relação ao grau de falha, o nó intermediário 22 tem 22% de grau de falha, e os outros nós roteadores tem um índice menor do que 22%. Sendo assim, a perda dispositivo 22, por falha no dispositivo ou término de bateria, fará com que as informações enviadas pelo o sensor 5 não cheguem ao nó central. Com relação ao máximo número de roteadores usados em função dos caminhos, os nós roteadores 10 e 13 são usados três vezes nos caminhos 3-15-17-13-1, 3-26-13-1, 4-13-1, 9-18-12-10-1, 9-24-10-1 e 2-11-10-1. Ou seja, estes dispositivos terão o seu tempo de vida reduzido, devido os seus altos índices de retransmissão. Com relação ao número de sensores vizinhos aos roteadores, os roteadores 15, 19, 22 e 26 podem retransmitir os dados enviados por dois sensores, além dos sensores também serem usados com retransmissores. Isso faz com

esses roteadores e sensores consomem mais energia, e em consequência, sua bateria acaba mais cedo. Como caminhos alternativos em caso de falha do roteador 15, os sensores 2 e 3 apresentam os caminhos 2-25-1, 2-11-10-1 e 3-26-13-1, do roteador 19, os sensores 7 e 8 apresentam os caminhos 7-14-16-1, 8-10-1, 8-12-1 e 8-16-1, do roteador 22, o sensor 5, como citado anteriormente, não apresentará caminhos e o sensor 6 apresenta os caminhos 6-23-1 e 6-21-1 e do roteador 26, os sensores 3 e 4 apresentam os caminhos 3-15-17-13-1, 4-13-1 e 4-20-1.

Tabela 11 – Desempenho da Rede

REDE	MÍNIMO	MÉDIA	MÁXIMO	STD
Número de Nós	23,00	25,30	28,00	1,49
Número de Roteadores	14,00	16,30	19,00	1,49
Número de Sensores Críticos	0,00	0,00	0,00	0,00
Max. Grau de falha	0,22	0,22	0,22	0,00
Num. de Roteadores com Max. Grau de falha	1,00	1,20	2,00	0,42
Tamanho Máximo dos Caminhos	3,00	3,50	4,00	0,53
Número de Nós com Tamanho Máximo	1,00	3,50	7,00	2,22
Num. Max. de Vezes que Roteador é Usado	3,00	3,70	5,00	0,67
Número de Roteadores que são Mais Usados	1,00	1,70	3,00	0,82

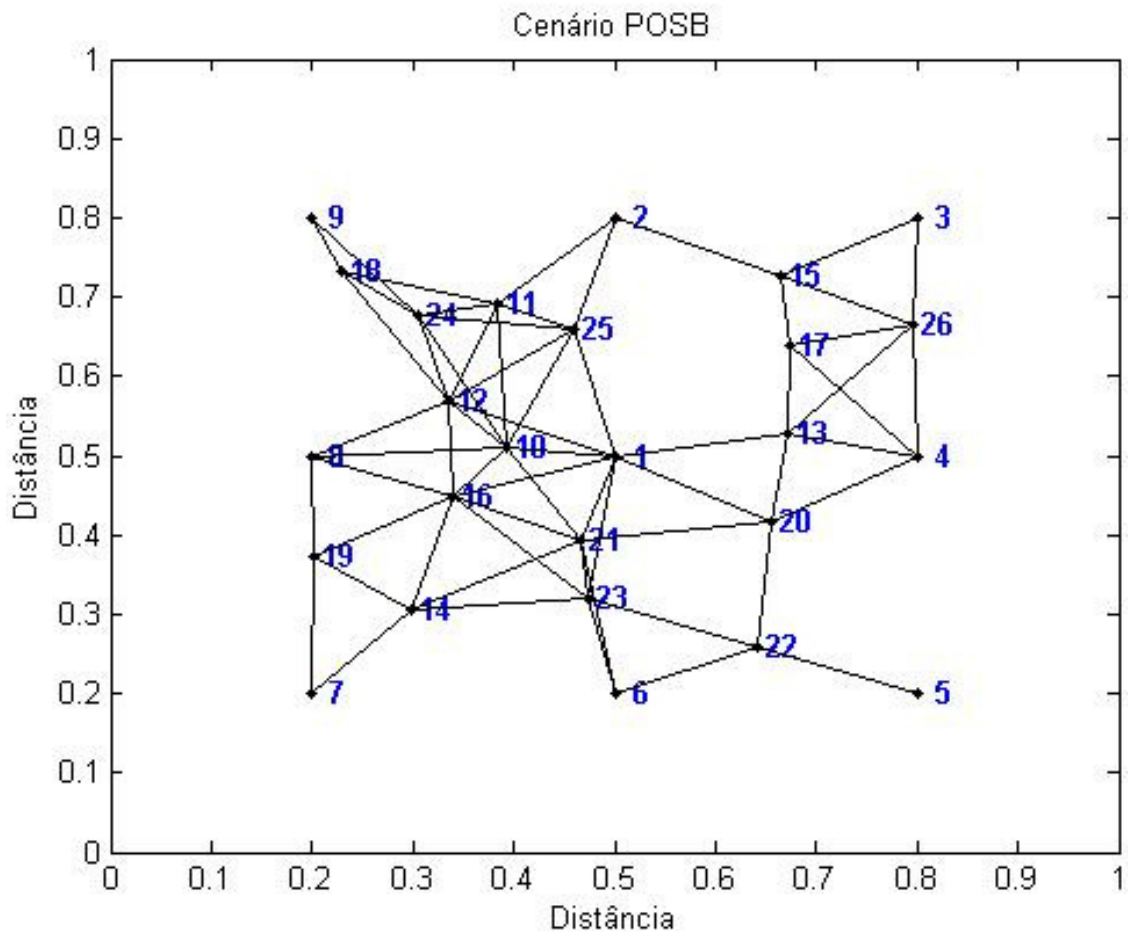


Figura 25 - Estudo do Caso 5 – Cenário POSB

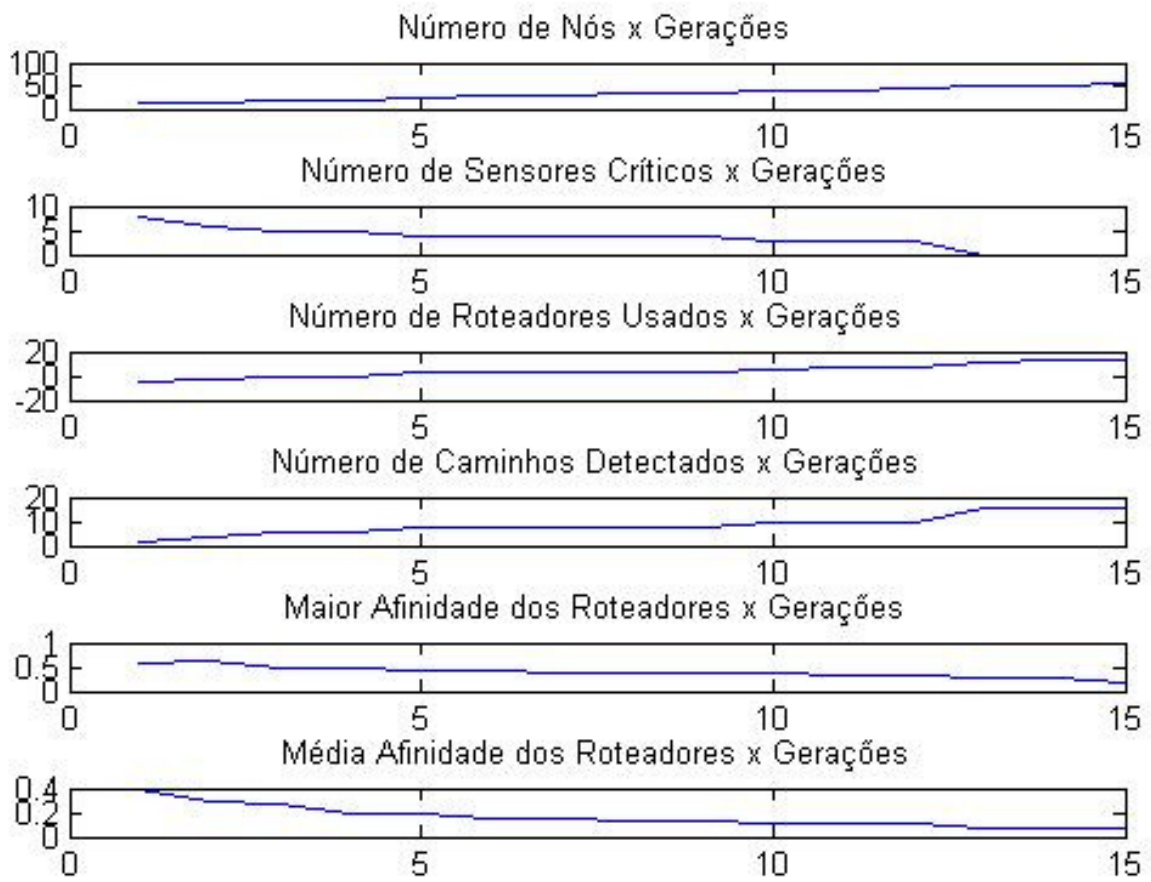


Figura 26 – Trace do Caso 5

4.2.6 Estudo de Caso 6 – Cenário POS B

Nesta simulação o objetivo para o POSIMNET é obter três caminhos disjuntos para cada sensor transmitir os dados monitorados para o nó central, com raio de alcance de 0,1 e com a configuração POSB. Para tal, foi necessário utilizar o operador *ClonaCondicaoNet* e os pesos de 0,5 para a afinidade Grau de Falha, 0,25 para a afinidade número de vezes que o roteador é usado em função dos caminhos e 0,25 para a afinidade número de sensores vizinhos, conforme descrito na Tabela 12. Sendo assim, objetivo do POSIMNET será obter três caminhos redundantes disjuntos atendendo os critérios de afinidade de grau de falha, de número de vezes que o roteador é usado em função dos caminhos e de número de sensores vizinhos. Após realização de dez experimentos, a melhor configuração de rede pode ser vista na Figura 27, e a consolidação dos testes está descrita na Tabela 13. Antes de começar a análise desse experimento, é importante ressaltar que o seu raio de alcance é a metade do

proposto nos casos 1, 2 e 5, e em consequência, espera-se que seja necessário um maior número de roteadores e saltos no caminho.

Tabela 12 – Caso 6 – Cenário – Parâmetros

Parâmetros do POSIMNET	Valores	Método
Número de gerações	90	-
Número inicial de Roteadores	10	-
Recurso inicial fornecido	30	-
Operador de mutação	-	<i>ClonaCondicaoNet</i>
Afinidade	-	Grau de falha, Número de Vezes que o Roteador é Usado e Número de Sensores Vizinhos

A Tabela 13 descreve o desempenho da rede dos dez experimentos realizados nesse estudo de caso. Os seus pontos positivos são: (i) Baixo índice de grau de falha, de 0,19; (ii) Sem sensores críticos; (iii) Baixa variação do número máximo de vezes que o roteador é usado. Seus pontos negativos: (i) Alto número de roteadores adicionados, no máximo 73 roteadores; (ii) Alto número de hops (saltos) para a informação chegar o nó central, entre 7 e 9.

A Figura 28 representa a evolução do algoritmo POSIMNET para formar a melhor configuração de rede (Figura 27) dos 10 experimentos. Na Figura 28 pode-se observar que após 50ª geração, os índices de número de sensores críticos, de número de nós, de grau de falha dos roteadores, de número de caminhos detectados e de número de roteadores usados são quase ou totalmente estabilizados. Na Figura 27 é observado que os nós sensores 3, 5, 7 e 9, nos caminhos 3-48-35-41-75-56-80-1, 5-26-11-34-65-85-71-1, 5-14-17-45-55-53-72-1, 7-25-23-37-67-84-69-1, 7-10-30-18-81-79-61-1, 9-22-27-46-44-66-89-1 e 9-13-33-42-68-29-80-1, apresenta sete saltos até o *gateway*. Isso significa que a informação enviada por esses dispositivos sofrerá um atraso para ser recebida pelo nó central, já que ela vai precisar ser retransmitida por seis nós intermediários. Com relação ao grau de falha, os nós intermediários 35 e 41 têm 19% de grau de falha, e os outros nós roteadores tem um índice menor do que 19%. Isso significa que pelo menos 81,00% dos caminhos dos sensores para o *gateway* continuam a existir mesmo após a retirada de um nó. Com relação ao máximo número de

roteadores usados em função dos caminhos, o nó roteador 89 é usado quatro vezes em função dos caminhos (2-28-68-29-89-1, 2-52-39-64-89-1, 9-22-27-46-44-66-89-1 e 8-36-78-24-89-1). Com relação ao número de sensores vizinhos aos roteadores, nenhum dos 89 roteadores teve mais de um sensor vizinho. Sendo assim, o consumo de energia dos dispositivos será o mesmo, aumentando o tempo de vida dos dispositivos da rede.

Tabela 13 – Desempenho da Rede

REDE	MÍNIMO	MÉDIA	MÁXIMO	STD
Número de Nós	83,00	87,70	92,00	2,87
Número de Roteadores	74,00	78,70	83,00	2,87
Número de Sensores Críticos	0,00	0,00	0,00	0,00
Max. Grau de Falha	0,19	0,19	0,19	0,00
Num. de Roteadores com Max. Grau de Falha	2,00	3,90	6,00	1,52
Tamanho Máximo dos Caminhos	7,00	8,20	9,00	0,79
Número de Nós com Tamanho Máximo	1,00	2,10	5,00	1,37
Num. Max. de Vezes que Roteador é Usado	4,00	4,70	6,00	0,82
Número de Roteadores que são Mais Usados	1,00	1,80	5,00	1,23

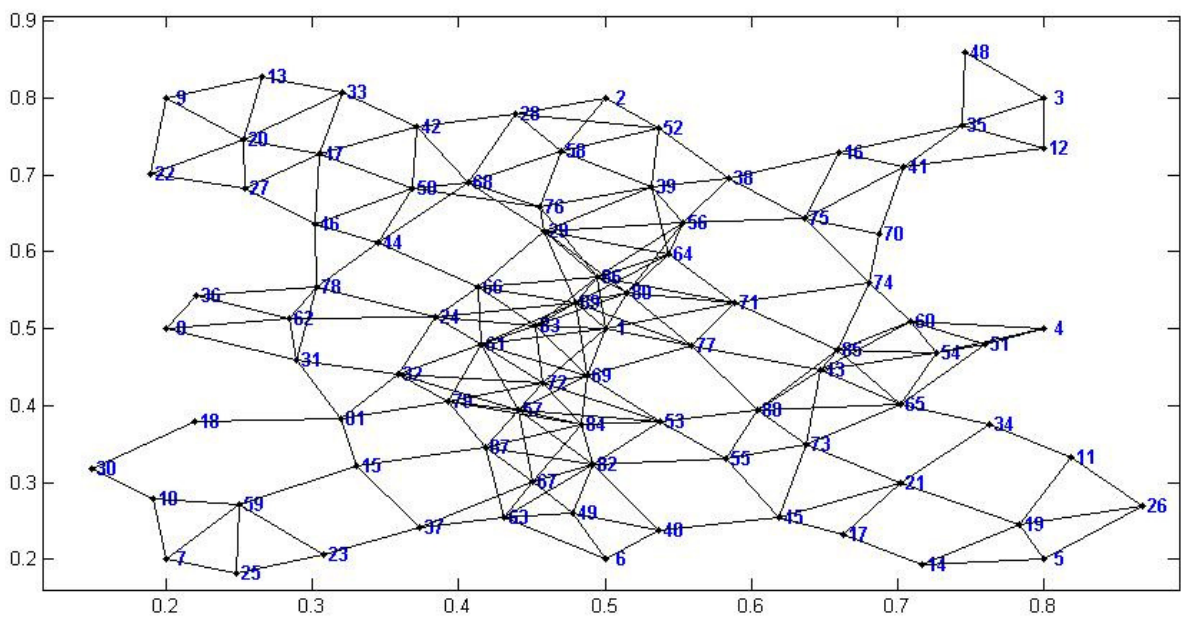
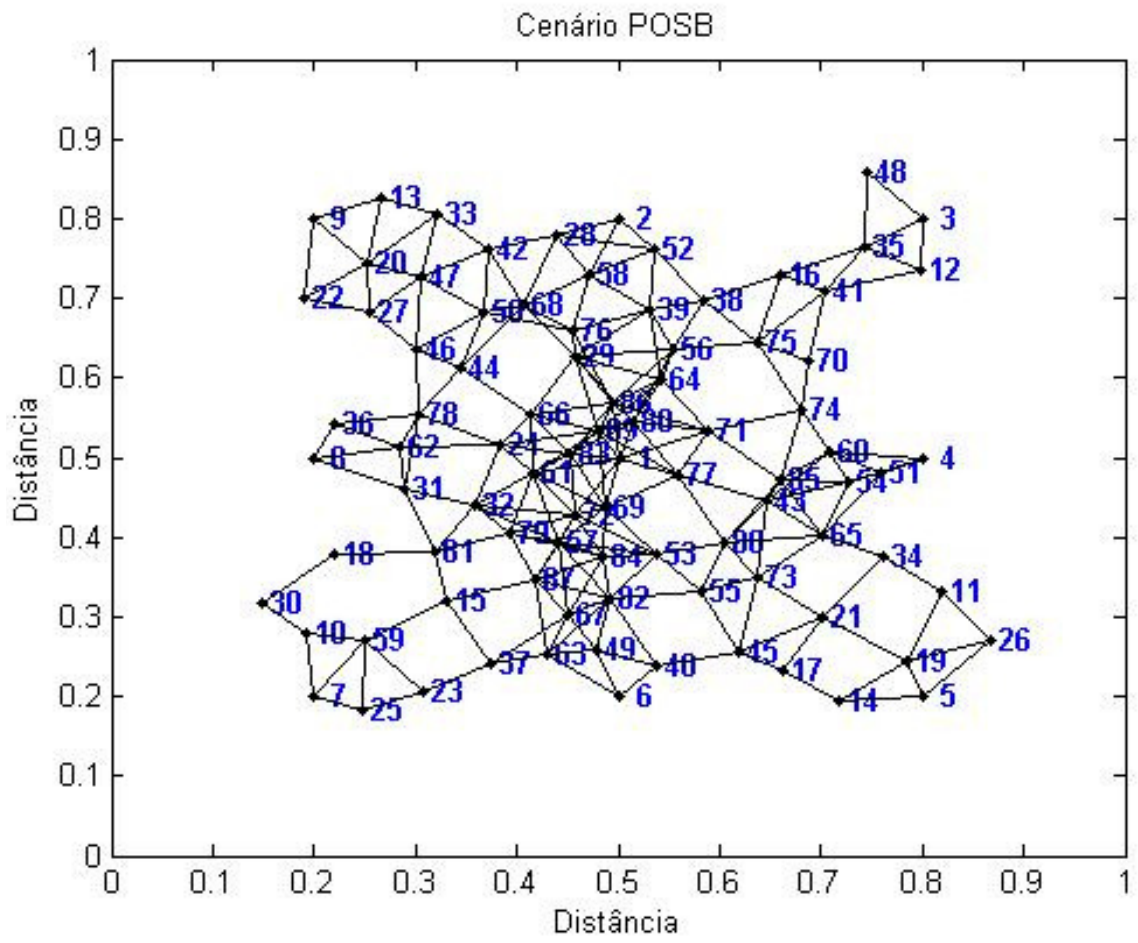


Figura 27 - Estudo do Caso 6 – Cenário POSB. (a) Configuração de rede final; (b) Configuração de rede final ampliada.

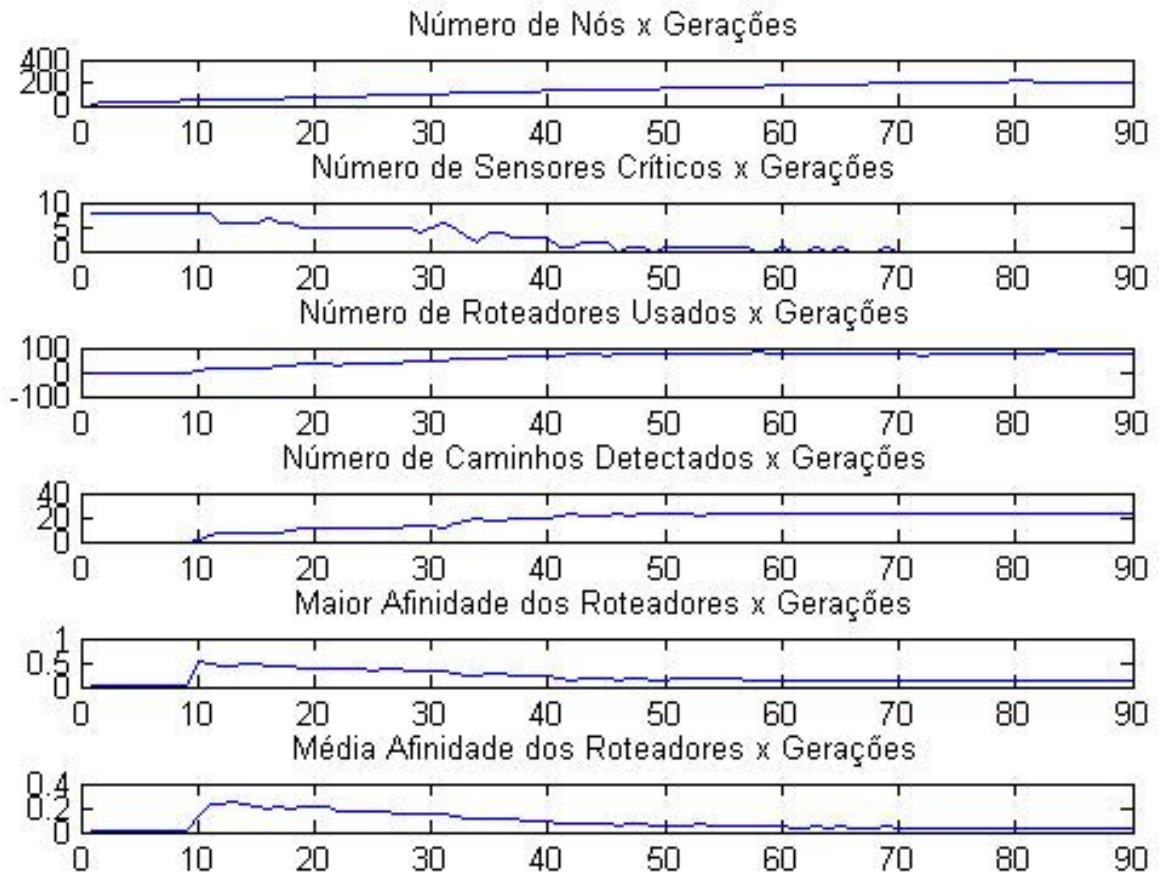
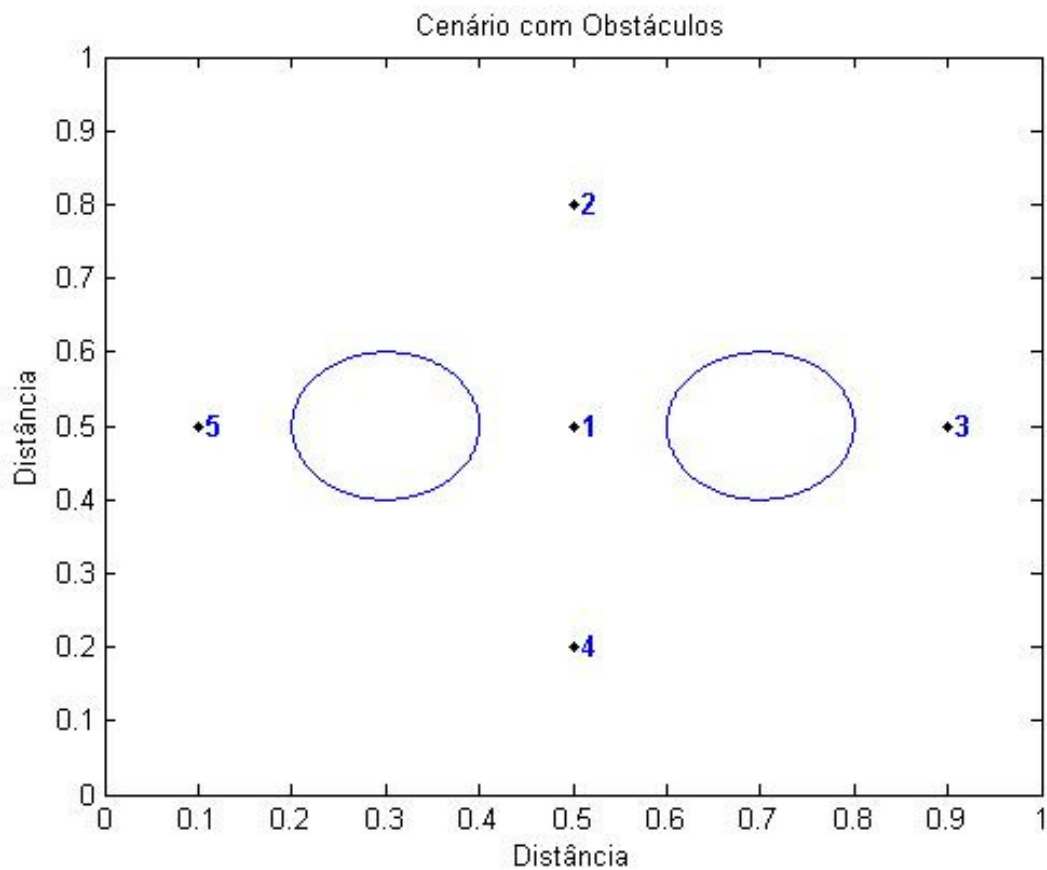


Figura 28 – Trace do Caso 6

4.3 Estudo de Caso em Cenários com Obstáculos

Dois cenários com obstáculos foram elaborados para comprovarem que o algoritmo POSIMNET também é capaz de posicionar os nós roteadores mesmos em ambientes com obstáculos fixos ou móveis. O primeiro cenário com obstáculos proposto é composto por dois obstáculos circulares, com raio de 0,1, e por cinco nós, no qual o nó 1 é o *gateway* e os outros são os nós sensores. Inicialmente o *gateway* não tem visada direta com os nós 3 e 5 e não está conectado com nenhum dos nós de rede, conforme ilustrado na Figura 29 (a). O segundo cenário com obstáculos (POSC) apresentam oito obstáculos, nos quais três obstáculos circulares têm raio de 0,05, um obstáculo circular tem raio de 0,15 e quatro obstáculos retangulares com tamanhos diferentes, e um nó *gateway* (nó 1) e sete nós sensores

(nós de 2 a 8). Inicialmente o *gateway* não tem visada direta com nenhum dos nós sensores e não está conectado a nenhum nó da rede. Além disso, os nós sensores também não têm visada direta entre si e não estão conectados, conforme ilustrado na figura 29 (b). Nos cenários com obstáculos foram realizados dois estudos de casos (estudo de caso 7 e 8). No estudo de caso 7 a configuração da rede está em cruz, o raio de alcance dos elementos da rede é de 0,2 e deseja-se obter dois caminhos disjuntos. No entanto o estudo de caso 8 utiliza a configuração de rede POSC, deseja-se obter três caminhos disjuntos para os sensores enviarem as informações ao *gateway* e raio de alcance dos elementos de rede de 0,2 e deseja-se obter três caminhos disjuntos. Os parâmetros escolhidos para a obtenção dos n caminhos redundantes requisitados em cada estudo de caso estão descritos nas tabelas 14 e 16.



(a)

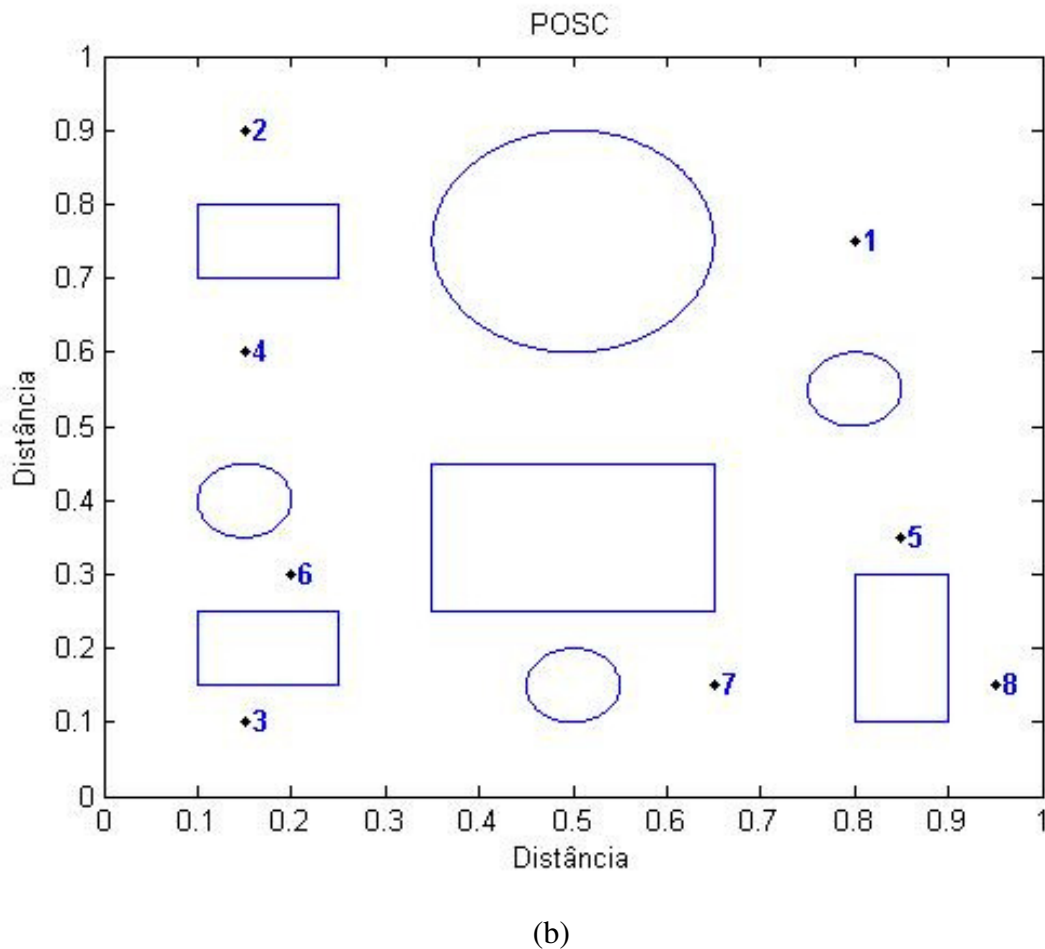


Figura 29 – Cenário com Obstáculos. (a) Cenário com dois obstáculos circulares; (b) Obstáculos com quatro obstáculos circulares e quatro obstáculos retangulares.

4.3.1 Estudo de Caso 7 – Cenário com Dois Obstáculos Circulares

Na simulação do estudo de caso 7 o objetivo para o POSIMNET é obter dois caminhos disjuntos para cada sensor transmitir os dados monitorados para o nó central, com raio de alcance de 0,2. Para tal, foi necessário utilizar o operador *ClonaCondicaoNet* e os pesos 0,7 para afinidade Grau de Falha, 0,15 para o número de vezes que o nó é usado em função do caminho e 0,15 número de nós sensores vizinhos, conforme descrito na Tabela 14. Após realização de dez experimentos, a melhor configuração de rede pode ser vista na Figura 30, e a consolidação dos testes está descrita na Tabela 15.

Tabela 14 – Caso 7 – Cenário – Parâmetros

Parâmetros do POSIMNET	Valores	Método
Número de gerações	30	-
Número inicial de Roteadores	10	-
Recurso inicial fornecido	20	-
Operador de mutação	-	<i>ClonaCondicaoNet</i>
Afinidade	-	Grau de falha, Número de Vezes que o Roteador é Usado e Número de Sensores Vizinhos

A Tabela 15 descreve o desempenho da rede dos dez experimentos realizados nesse estudo de caso. Os seus pontos positivos são: (i) Baixa adição dos nós roteadores, apenas 7; (ii) Índice de grau de falha entre 30% e 40%; (iii) Sem sensores críticos; (iv) Baixo número de vezes que o roteador é usado em função do caminho, entre 1 e 2. Seus pontos negativos: (i) Alto número de hops, entre 4 e 5.

A Figura 31 representa a evolução do algoritmo POSIMNET para formar a melhor configuração de rede (Figura 30) dos 10 experimentos. Na Figura 31 pode-se observar que após 18ª geração, os índices de número de sensores críticos, de número de nós, de grau de falha dos roteadores, de número de caminhos detectados e de número de roteadores usados são quase ou totalmente estabilizados. Na Figura 30 é observado que os nós sensores 3e 5, nos caminhos 3-16-17-20-1, 3-19-7-10-1, 5-13-11-18-1 e 5-12-14-15-1, apresentam quatro saltos até o *gateway*. Isso significa que a informação enviada por esses dispositivos sofrerão um atraso para ser recebida pelo nó central, já que ela vai precisar ser retransmitida por três nós intermediários. Com relação ao grau de falha, os nós intermediários 7, 10, 11, 12, 13, 14, 16, 17 e 19 têm 30% de grau de falha, e os outros nós roteadores tem um índice menor do que 30%. Isso significa que 70,00% dos caminhos dos sensores para o *gateway*, continuam a existir mesmo após a retirada de um nó. Com relação ao máximo número de roteadores usados em função dos caminhos, o nó roteador 15 é usado duas vezes em função dos caminhos (2-15-1 e 5-12-14-15-1). Sendo assim, o consumo de bateria do roteador 15 será maior do que nos outros dispositivos, e em consequência, o seu tempo de vida é reduzido. Com relação ao número de sensores vizinhos aos roteadores, nenhum roteador é vizinho de

mais de um sensor. Então, com relação a esse parâmetro, os roteadores consumiram a mesma energia e terão o seu tempo de vida prolongado.

Tabela 15 – Desempenho da Rede

REDE	MÍNIMO	MÉDIA	MÁXIMO	STD
Número de Nós	19	19,9	22	0,99
Número de Roteadores	14	14,9	17	0,99
Número de Sensores Críticos	0	0	0	0,00
Max. Grau de Falha	0,30	0,35	0,40	0,05
Num. de Roteadores com Max. Grau de Falha	1	7,8	17	5,87
Tamanho Máximo dos Caminhos	4	4,4	5	0,52
Número de Nós com Tamanho Máximo	1	1,6	2	0,52
Num. Max. de Vezes que Roteador é Usado	2	2	2	0,00
Número de Roteadores que são Mais Usados	1	2,2	4	1,14

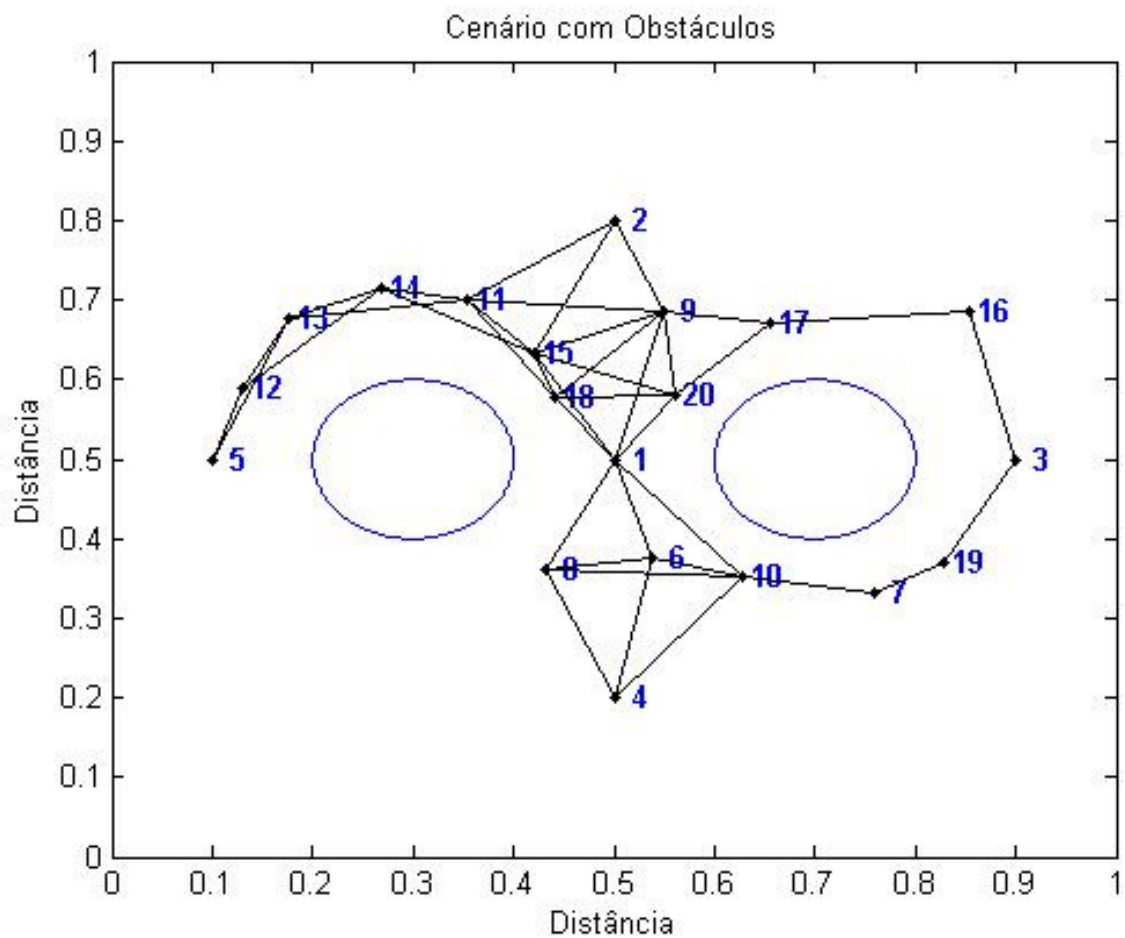


Figura 30 - Estudo do Caso 7 – Cenário com Obstáculos

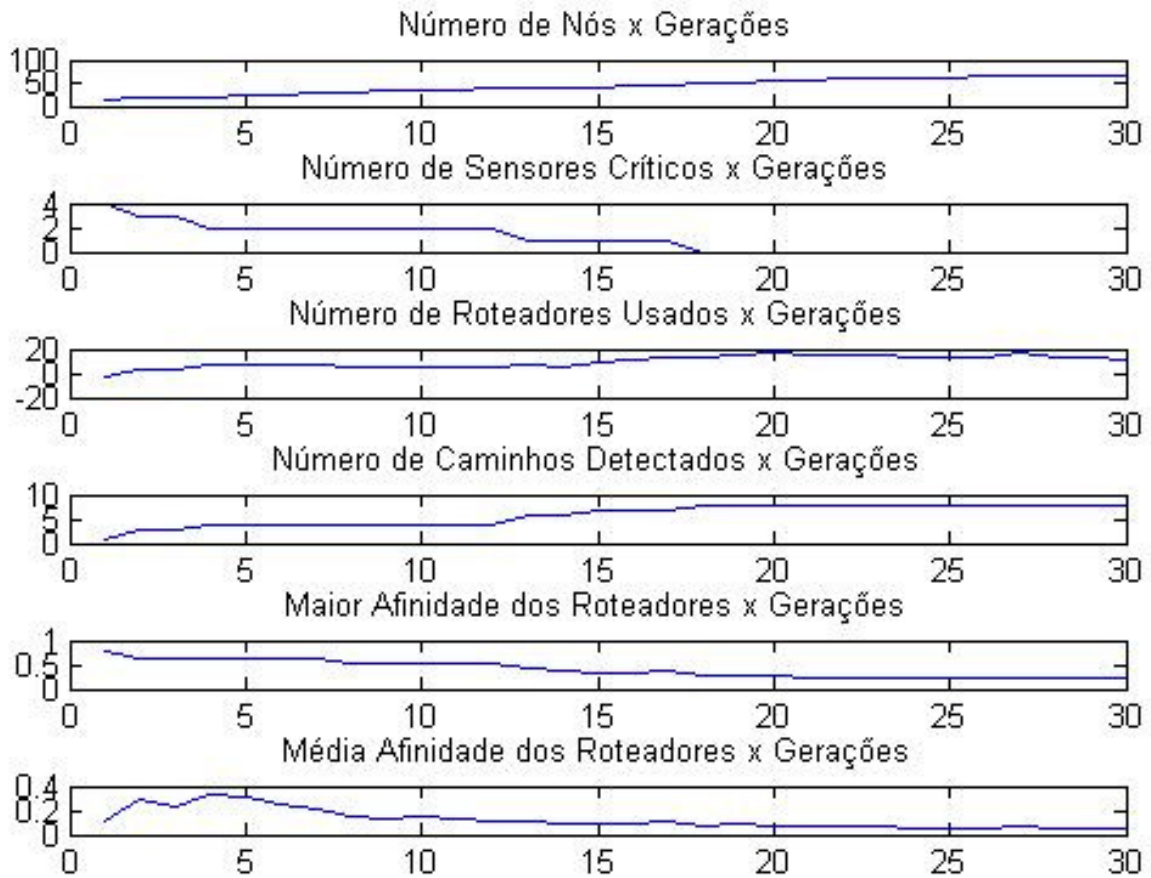


Figura 31 – Trace do Cenário Completo

4.3.2 Estudo de Caso 8 – Cenário POSC

Na simulação do estudo de caso 8 o objetivo para o POSIMNET é obter três caminhos disjuntos para cada sensor transmitir os dados monitorados para o nó central, com raio de alcance de 0,2. Para tal, foi necessário utilizar o operador `ClonaCondicaoNet` e os pesos 0,7 para afinidade Grau de Falha, 0,15 para o número de vezes que o nó é usado em função do caminho e 0,15 número de nós sensores vizinhos, conforme descrito na Tabela 16. Após realização de dez experimentos, a melhor configuração de rede pode ser vista na Figura 32, e a consolidação dos testes está descrita na Tabela 17.

Tabela 16 – Caso 8 – Cenário – Parâmetros

Parâmetros do POSIMNET	Valores	Método
Número de gerações	100	-
Número inicial de Roteadores	10	-
Recurso inicial fornecido	35	-
Operador de mutação	-	ClonaCondicaoNet
Afinidade	-	Grau de falha, Número de Vezes que o Roteador é Usado e Número de Sensores Vizinhos

A Tabela 17 descreve o desempenho da rede dos dez experimentos realizados nesse estudo de caso. Os seus pontos positivos são: (i) Baixo índice de grau de falha entre 21% e 25%; (ii) Sem sensores críticos; (iii) Apenas em dois experimentos o número máximo de vezes que roteador é usado ultrapassou cinco vezes, o roteador 37 foi usado oito vezes em função dos caminhos e o roteador 28 foi usado seis vezes; (iv) Sem sensores críticos. Seus pontos negativos: (i) Alto número de hops, entre 8 e 10; (ii) Alto número de roteadores adicionais, entre 51 e 55.

A Figura 33 representa a evolução do algoritmo POSIMNET para formar a melhor configuração de rede (Figura 32) dos 10 experimentos. Na Figura 33 pode-se observar que após 70ª geração, os índices de número de sensores críticos, de número de nós, de grau de falha dos roteadores, de número de caminhos detectados e de número de roteadores usados são quase ou totalmente estabilizados. Na Figura 32 é observado que os nós sensores 3e 6, nos caminhos 3-20-22-24-7-40-63-53-36-1, 3-50-49-61-4-52-15-56-39-1 e 6-58-61-4-60-31-15-37-26-1, apresentam nove saltos até o *gateway*. Isso significa que a informação enviada por esses dispositivos sofrerão um atraso para ser recebida pelo nó central, já que ela vai precisar ser retransmitida por oito nós intermediários. Com relação ao grau de falha, o nó intermediário 32 têm 21% de grau de falha, e os outros nós roteadores tem um índice menor do que 21%. Isso significa que 79,00% dos caminhos dos sensores para o *gateway*, continuam a existir mesmo após a retirada de um nó. Com relação ao máximo número de roteadores usados em função dos caminhos, o nó roteador 31 é usado cinco vezes em função dos caminhos (3-10-19-33-38-31-37-25-1, 4-57-31-37-25-1, 4-60-31-15-37-26-1, 6-32-31-37-25-1e 6-58-61-4-60-31-15-37-26-1). Sendo assim, o consumo de bateria do roteador 31 será maior do que nos outros dispositivos, e em consequência, o seu tempo de vida é reduzido. Com relação ao número de sensores vizinhos aos roteadores, nenhum roteador é vizinho de

mais de um sensor. Então, com relação a esse parâmetro, os roteadores consumiram a mesma energia e terão o seu tempo de vida prolongado.

Tabela 17 – Desempenho de Rede

REDE	MÍNIMO	MÉDIA	MÁXIMO	STD
Número de Nós	59,00	60,50	63,00	1,18
Número de Roteadores	51,00	52,50	55,00	1,18
Número de Sensores Críticos	0,00	0,00	0,00	0,00
Max. Grau de Falha	0,21	0,21	0,25	0,01
Num. de Roteadores com Max. Grau de Falha	1,00	1,50	4,00	1,08
Tamanho Máximo dos Caminhos	8,00	9,50	10,00	0,71
Número de Nós com Tamanho Máximo	1,00	1,20	2,00	0,42
Num. Max. de Vezes que Roteador é Usado	5,00	5,40	8,00	0,97
Número de Roteadores que são Mais Usados	1,00	1,60	2,00	0,52

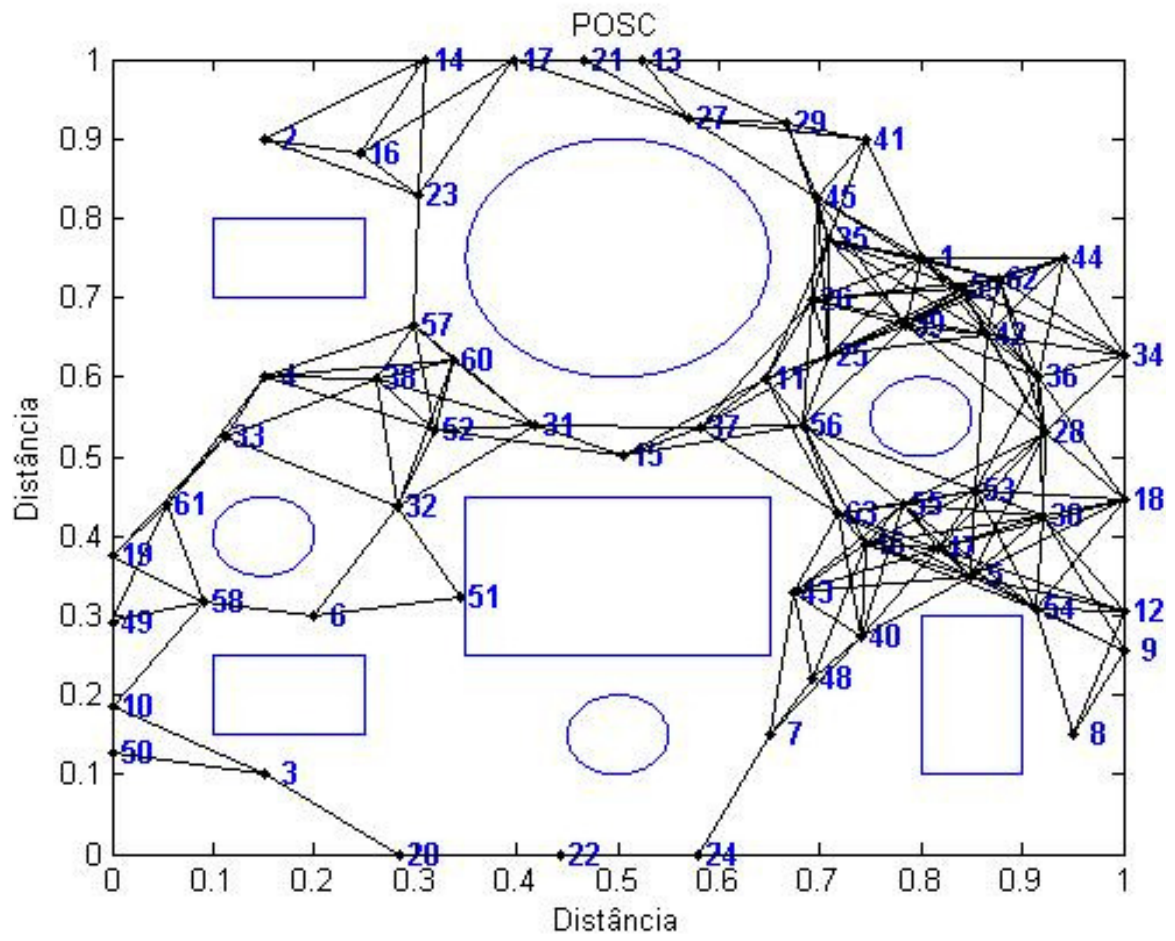


Figura 32 - Estudo de Caso 8 – Cenário POSC

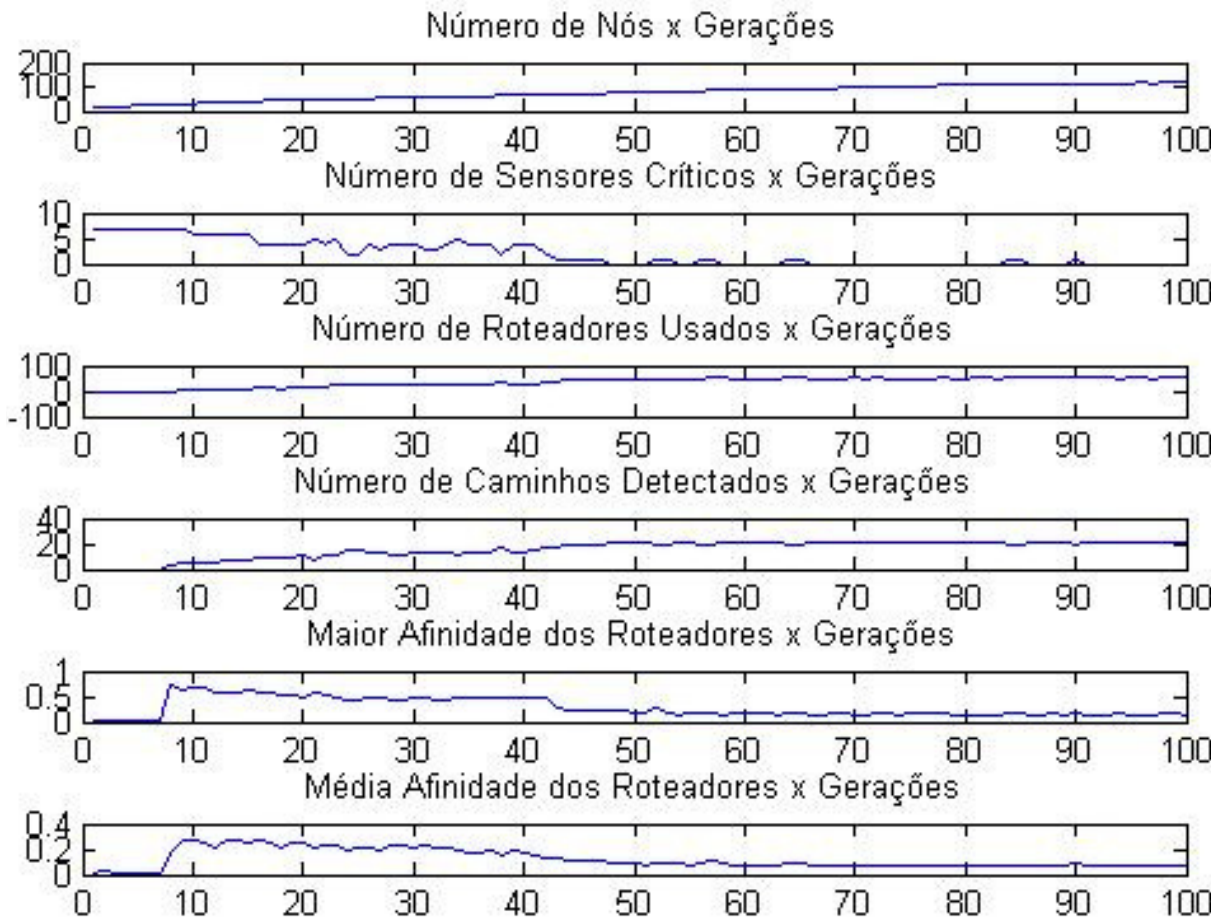


Figura 33 – Trace do Cenário POSC

5 CONCLUSÕES

A utilização de instrumentos sem fio na área de automação industrial vem crescendo ao longo do tempo, devido suas principais vantagens, como facilidade de manutenção e instalação, flexibilidade na alteração de arquiteturas existentes e outros. Nessa área, a segurança, confiabilidade, disponibilidade, robustez e desempenho da rede na realização do monitoramento e controle do processo são primordiais, para que não haja um acidente de grande proporção na malha industrial. Por esse motivo, os nós intermediários (elementos da rede que deverão atender os critérios supracitados) têm que ser muito bem posicionados para que as informações enviadas pelos nós sensores tenham caminhos redundantes para chegarem ao *gateway*.

Neste trabalho foi desenvolvida uma ferramenta de análise do posicionamento de nós roteadores em rede sem fio, chamado POSIMNET. O POSIMNET propõe criar caminhos redundantes para que os dados coletados pelos sensores sejam enviados ao *gateway* por dois ou mais caminhos quaisquer ou disjuntos, atendendo os critérios de grau de falha, de número de retransmissão pelos roteadores e de número de sensores vizinhos aos roteadores. O algoritmo permite que cada critério seja habilitado por vez ou que eles sejam combinados com pesos iguais ou diferentes para cada um.

5.1 Resultados

Nos estudos casos descritos no Capítulo 4, a ferramenta POSIMNET foi capaz de analisar quatro tipos de cenários diferentes com grau de dificuldade adicionais. No primeiro estudo de caso foi proposta uma configuração de rede simples que tinha como objetivo encontrar dois caminhos redundantes quaisquer e atender o critério de baixo Grau de Falha. Até o quarto estudo de caso foi variado o número (dois ou três) e o tipo (disjunto ou quaisquer) de caminhos desejados e o raio de alcance (0,1 ou 0,2) dos elementos da rede. Sendo o estudo de caso 4, o mais difícil com conjunto de configuração de rede POSA, raio de alcance de 0,1 e de critério de baixo grau de falha da rede e com objetivo de criar três caminhos disjuntos. O segundo cenário é mais complicado do que o anterior, pois ele contém oito nós sensores sem nenhuma ligação entre si e com o nó central. Este cenário foi utilizado

nos estudos de casos 5 e 6, sendo o caso 6 o mais difícil de atender o objetivo. O terceiro cenário acrescenta dois obstáculos circulares impedindo a visada direta entre os sensores 3 e 4 com o *gateway*. Por último, o quarto cenário apresenta oito obstáculos, circulares e retangulares, que impedem a visada direta e a conexão entre todos os elementos da rede (nós sensores e *gateway*). Além disso, o raio de alcance dos dispositivos da rede é de 0,2 e deseja-se obter três caminhos disjuntos para as informações enviadas pelos sensores cheguem ao *gateway*. Em todos os estudos de casos, as configurações de rede geradas não possuíam sensores críticos indicando que o algoritmo foi capaz de atender a especificações do número de caminhos necessários. Também foi observado que conforme o grau de dificuldade foi aumentando, o número de roteadores adicionais foram necessariamente aumentados. Além disso, verificou-se, conforme esperado, um aumento no número médio de hops (saltos) quando o raio de alcance dos roteadores era menor (estudos 3, 4 e 6). Constatou-se que o número médio de vezes que um roteador é usado cresce com a dificuldade da configuração proposta. A Tabela 18 resume os resultados dos experimentos realizados.

Tabela 18 – Tabela Comparativa

Estudos de Casos	Num. de Sensores Críticos		Máximo Grau de Falha		Tamanho Max. de Caminhos		Num. Max. de Roteadores Usados	
	$\mu \pm \sigma$	(Max - Min)	$\mu \pm \sigma$	(Max - Min)	$\mu \pm \sigma$	(Max - Min)	$\mu \pm \sigma$	(Max - Min)
1	0	0	0,27±0,08	0,20	3,00±0,00	0,00	2,10±0,57	2,00
2	0	0	0,30±0,00	0,00	3,10±0,32	1,00	2,00±0,47	2,00
3	0	0	0,36±0,08	0,20	5,10±0,57	2,00	2,60±0,52	1,00
4	0	0	0,33±0,03	0,13	7,30±1,06	3,00	3,50±0,97	3,00
5	0	0	0,22±0,00	0,00	3,50±0,53	1,00	3,70±0,67	2,00
6	0	0	0,19±0,00	0,00	8,20±0,79	2,00	4,70±0,82	2,00
7	0	0	0,35±0,05	0,10	4,40±0,52	1,00	2,00±0,00	0,00
8	0	0	0,21±0,01	0,04	9,50±0,71	2,00	5,40±0,97	3,00

5.2 Trabalhos Futuros

Como proposta para os trabalhos futuros pode-se citar:

- Controle do número máximo de roteadores a ser utilizado. Isto pode ser feito explicitamente na etapa de poda ou através da inclusão de um termo de supressão para diminuir a afinidade, caso o número de roteadores seja maior do que o especificado;
- Implementação de uma análise de confiabilidade da rede, levando em conta a possibilidade de diferentes roteadores não serem capazes de transmitir as informações;
- O emprego de outros modelos de propagação para a determinação das conexões entre os nós, levando em consideração o índice de reflexão de alguns obstáculos móveis e fixos comuns (tanques, caminhões, tubulações e outros);
- Além disso, pode-se propor um aprimoramento deste algoritmo para cenários em 3D, considerando o posicionamento dos nós roteadores nos eixos x, y e z.

REFERÊNCIAS

AMARAL, J.L.M. *Sistemas Imunológicos Artificiais aplicados à Detecção de Falhas*. Tese (Doutorado em Engenharia Elétrica). PUC. Rio de Janeiro. 2006. 121 f.

AOUN, B.; BOUTABA, R.; IRAQI, Y.; KENWARD, G. *Gateway Placement Optimization in Wireless Mesh Networks With QoS Constraints*. IEEE Journal on Selected Areas in Communications. Canada. Nov. 2006. vol. 24. n° 11. pp. 2127-2136.

BRADLEY, D.W.; TYRRELL, A.M. *Hardware Fault Tolerance: An Immunological Solution*. Proc. of IEEE Conference on Systems, Man and Cybernetics Nashville, USA, Vol. 1, pp. 107-112, October 2000b.

CANNONS, J.; MILSTEIN, L. B.; ZEGER, K., 2008. "An Algorithm for Wireless Relay Placement". IEEE Transactions on Wireless Communications. USA. Nov. 2006. vol. 8 n° 11 . pp. 5564-5574

CASTRO, L. N.; VON ZUBEN, F. J. *Artificial Immune Systems: Part I – Basic Theory and Applications*. Technical Report TR-DCA 01/99. 1999. p.95.

CASTRO, L.N. *Engenharia Imunológica: Desenvolvimento e Aplicação de Ferramentas Computacionais Inspiradas em Sistemas Imunológicos Artificiais*. Tese (Doutorado em Engenharia Elétrica e Computação). 2001. 144f. Universidade Estadual de Campinas, São Paulo, 2001.

COSTA, MÁRCIO S.; AMARAL, J. L.M. "Uma ferramenta para análise do posicionamento de nós em redes sem fio aplicadas a automação industrial", XVIII Congresso Brasileiro de Automática. Bonito. 2010. pags. 1521-1527.

COSTA, MÁRCIO S.; AMARAL, J. L.M.. *Análise de Redes sem Fio Industriais – ISA 100 X WirelessHart*. Intech. América do Sul. 2012. vol. 140. p. 61-67.

COSTA; MÁRCIO S. *Otimização de posicionamento de nós roteadores em redes de comunicação sem fio aplicadas em automação indústria*. 2011. 51f. Dissertação (Mestrado

em Engenharia Eletrônica) – Faculdade de Engenharia, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2011.

DE CASTRO, L. N. ; VON ZUBEN, F. J., 2000b. *Artificial Immune Systems: Part II – A Survey of Applications*. Technical Report – RT DCA 02/00. 2000b. p. 65.

DE CASTRO, L. N. ; TIMMIS, J. I. . *Artificial Immune Systems: A New Computational Intelligence Approach*. 1. ed. Londres: Springer-Verlag, 2002. 385p.

DIJKSTRA, E. W. *A Note on Two Problems in Connexion with Graphs*. Numerische Mathematik, 1959. vol. 1, pp. 269-271.

FORREST, S., et al. *Self-Nonself Discriminator in a Computer*. Proc. of the 1994 IEEE Symposium on Research in Security and Privacy, Los Alamitos, CA: IEEE Comput. Soc. Press, 1994, p. 202-212.

GALEANO, J. C.; SUAN, A. V. ; GONZALEZ, F. A. *A comparative analysis of artificial immune network models* GECCO 2005: Proceedings of the 2005 conference on Genetic and evolutionary computation. 2005. vol. 1, pp.361 -368.

GERSHO, A.; GRAY, R. M., *Vector Quantization and Signal Compression*. Norwell, MA. Kluwer Academic Publishers. 1992.

GONZÁLEZ, F., DASGUPTA, D., NIÑO, L. F. *A Randomized Real-Valued Negative Selection Algorithm*. Proceedings of the 2nd International Conference on Artificial Immune Systems ICARIS). 2003. p.261–272

HART COMMUNICATION FOUNDATION. Disponível em: <http://www.hartcomm.org/protocol/wihart/wireless_technology.html>. Acesso em: 10 set. e 2011.

HOFFERT ,J.; KLUES, K.; ORJIH, O., 2007. *Configuring the IEEE 802.15.4 MAC Layer for Single-sink Wireless Sensor Network Applications*. Technical Report. Disponível em: <http://www.cs.wustl.edu/~joeh/802_15_4_Eval_Report.pdf>. Acesso em: 12 dez. 2011

HOWARD, A.; MATARIC, M. J.; SUKHATME, G. S. *Mobile Sensor Network Deployment using Potential Fields: A Distributed, Scalable Solution to the Area Coverage Problem*. Proceedings of the 6th International Symposium on Distributed Autonomous Robotics Systems (DARS02), Fukuoka, Japan. 2002. pp. 299-308

JERNE, N. K. *Towards a network theory of the immune system*. Ann. Immunol, (Inst. Pasteur). 125C. 1974^a. pp.373-389.

LOUREIRO, A. A.F.; NOGUEIRA, J. M. S.; RUIZ, L. B.; MINI, R. A. F.; NAKAMURA, E. F.; FIGUEIREDO, C. M. S. , 2003. *Redes de Sensores Sem Fio*, XXI Simpósio Brasileiro de Redes de Computadores. Belo Horizonte. 2002. p.48

MOLINA, G.; ALBA, E.; TALBI, E.G. *Optimal Sensor Network Layout Using Multi-Objective Metaheuristics* - Journal of Universal Computer Science. 2008. vol.14 . n° 15. pp. 2549- 2565.

NEAL, M., 2002. *An Artificial Immune System for Continuous Analysis of Time Varying Data*. Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS). 2002. vol. 1. pp. 76 – 85.

NORDLUND, P.-J.; GUNNARSSON, F.; GUSTAFSSON, F.. *Particle Filters for Positioning in Wireless Networks*. Disponível em:

<<http://www.eurasip.org/Proceedings/Eusipco/2002/articles/paper750.pdf>> 2011. Acesso em: 10 fev. 2012.

PEREIRA, M. R., AMORIM, C. L., DE CASTRO, M. C. S. *Tutorial sobre Redes de Sensores*. Disponível em: < <http://magnum.ime.uerj.br/cadernos/cadinf/vol14/3-clicia.pdf> >. Acesso em: 10 fev. 2012.

PODURI, S.; SUKHATME, G. S. *Constrained Coverage for Mobile Sensor Networks*. IEEE International Conference on Robotics and Automation. USA. 2004. pp. 165-172.

PODURI, S.; PATTEM, S.; KRISHNAMACHARI, B.; SUKHATME, G. *Controlled Deployments of Sensor Networks*. In Press. 2006

SHI, Y.; HOU, Y. T., 2007. *Approximation Algorithm for Base Station Placement in Wireless Sensor Networks*. Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. San Diego. 2007. pp. 512-519.

SHI, Y. ; JIA,F. ; HAI-TAO, Y. , 2009. *An Improved Router Placement Algorithm Base on Energy Efficient Strategy for Wireless Network*. ISECS International Colloquium on Computing, Communication, Control and Management (CCCM2009). Sanya. 2009. pp. 421-423.

SANTOS, S. T. DOS. *Redes de Sensores Sem Fio em Monitoramento e Controle*. 2007. 87 p. Dissertação(Mestrado em Engenharia Elétrica)- COPPE/UFRJ, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2007.

TIMMIS, J.; NEAL, M.; HUNT, J. *An Artificial Immune System for Data Analysis*. Biosystems. vol. 55. n° 1. 2000. pp.143-150.

WONG, J. L.; JAFARI, R.; POTKONJAK, M. *Gateway Placement for Latency and Energy Efficient Data Aggregation*. Proceeding of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04). USA. 2004. pp.490-497

WU, W. ; LOU, J. ; YANG, M. *Gateway Placement Optimization for Load Balancing in Wireless Mesh Networks*. Proceeding of the 2009, 13th International Conference on Computer Supported Cooperative Work in Design.Chile.2009. pp. 408-413

YEN, J. Y. *Finding the K-Shortest Loopless Paths in a Network*. Management Science. 1971. vol. 17. n° 11. pp. 712–716.

YOUNIS, M.; AKKAYA, K.. *Strategies and techniques for node placement in wireless sensor networks: A survey*. Elsevier Ad Hoc Network Journal. 2008. vol. 6. n° 4. pp. 621–655.

YOUSSEF, W.; YOUNIS, M. *Intelligent Gateways Placement for Reduced Data Latency in Wireless Sensor Networks*. IEEE International Conference on Communications. Glasgow. 2007. pp. 3805-3810.

ZHENG, J.G; LEE, M. J. *A Comprehensive Performance Study of IEEE 802.15.4. Sensor Network Operations*. IEEE Press. Wiley InterScience. Chapter 4. pp. 218-237. 2006.