Universidade do Estado do Rio de Janeiro
Centro de Tecnologia e Ciências
Faculdade de Engenharia
Programa de Pós-Graduação em Engenharia Eletrônica

Márcio Sebastião Costa

Otimização de posicionamento de nós roteadores em redes de comunicação sem fio, aplicadas em automação industrial

Rio de Janeiro
Jun/2011

Márcio Sebastião Costa

Otimização de posicionamento de nós roteadores em redes de comunicação sem fio, aplicadas em automação industrial

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
Jun/2011

Márcio Sebastião Costa

Otimização de posicionamento de nós roteadores em redes de comunicação sem fio, aplicadas em automação industrial

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
Banca Examinadora:

_____
Professor Doutor Jorge Luís Machado do Amaral (Orientador)
Faculdade de Engenharia da UERJ

_____
Professor Doutor José Franco Machado do Amaral
Faculdade de Engenharia da UERJ

_____
Professora Doutora Karla Thereza Figueiredo Leite
Departamento de Engenharia Elétrica PUC- Rio

Rio de Janeiro
Jun/2011

DEDICATÓRIA

À minha mulher, aos meus filhos aos meus pais e a toda a minha família, que sempre me motivaram nos momentos mais difíceis desta trajetória.

AGRADECIMENTOS

À Deus, por ter me concedido realizar este sonho distante;

A minha querida Andreha, eterna companheira de todos os momentos;

Aos meus queridos pais, Ivette e Ronaldo, por não terem deixado faltar nada em minha vida;

Aos meus lindos filhos, que me dão todo motivo para continuar lutando.

Ao amigo e orientador professor Jorge Amaral, que me deu todo suporte desde o início nesta longa jornada. Sempre exigente, disciplinado e correto. Agradeço por todo aprendizado que tive e o empenho que fez, sem o qual não teria chegado a este ponto.

À Universidade do Estado do Rio de Janeiro, que me recebeu e acreditou que eu poderia;

Aos funcionários e professores do Programa de Pós-Graduação em Engenharia Eletrônica por todos os ensinamentos passados.

Ao professor Franco Amaral, que sempre esteve acompanhando e apoiando o meu trabalho.

Aos professores Biondi e Karla, pelos conselhos e ensinamentos.

A professora Luiza Mourelle, por ter me dado a oportunidade de ingressar no curso.

Ao amigo de mestrado Álvaro, companheiro inseparável de todas as disciplinas do curso, por todos os momentos passados;

A todos os colegas do mestrado, que tive a oportunidade de conhecer e conviver.

RESUMO

COSTA, Márcio S. *Otimização de posicionamento de nós roteadores em redes de comunicação sem fio aplicadas em automação industrial*, 2010. Dissertação (Mestrado em Engenharia Eletrônica) – Faculdade de Engenharia, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2011.

O presente trabalho descreve o desenvolvimento de uma ferramenta para otimização de posicionamento de nós roteadores em redes sem fio, aplicados em automação industrial, determinando a menor quantidade desse tipo de dispositivo a ser utilizado, e a melhor coordenada geográfica para cada um. A metodologia leva em conta critérios de otimização da menor quantidade de nós roteadores necessários à rede, otimização da menor quantidade de nós críticos potenciais para todos os dispositivos envolvidos e otimização da menor quantidade de saltos (hops) de mensagens transmitidas. Com isso, as redes sem fio que se submeterem à metodologia propostas neste projeto terão condições de atingir os requisitos de segurança, confiabilidade e eficiência necessários às aplicações a que forem submetidas.

Palavras-Chave: Rede sem Fio, Posicionamento de Roteadores, Automação Industrial.

ABSTRACT

This work describes the development of a tool for analyzing the positioning of nodes in wireless networks applied in industrial automation. Using the information gathered from the network, the tool is able to evaluate the coverage, the amount of potential critical nodes, the availability of alternative paths for all devices, and the latency. If it is necessary, it also suggests the smallest number of additional nodes (routers) and their locations to insure that the resulting network will reach safety's requirements, reliability and efficiency.

Keywords— Wireless Network, router placement, Industrial Automation.

LISTA DE FIGURAS

LISTA DE TABELAS

Lista de Acrônimos

BI	: *Beacon Interval*
BO	: *Beacon Order*
BPSK	: *Binary Phase Shift Keying*
BSS	: *Basic Service Set*
CAP	: *Contention Access Period*
CBR	: *Constant Bit Rate*
CCA	: *Clear Channel Assessment*
CFP	: *Contention Free Period*
CRC	: *Cyclic Redundancy Check*
CSMA-CA	: *Carrier sense Multiple Access with Collision Avoidance*
CTS	: *Clear to Send*
DSSS	: *Direct Sequence Spread Spectrum*
ED	: *Energy Detection*
ESS	: *Extended Service Set*
FCS	: *Frame Check Sequence*
FFD	: *Full-Function Device*
FH	: *Frequency Hopping*
FHSS	: *Frequency Hopping Spread Spectrum*
FTP	: *File Transfer Protocol*
GTS	: *Guaranteed Time Slot*
HMI	: *Human-Machine Interface*
HTTP	: *Hyper Text Transfer Protocol*
IEEE	: *Institute of Electrical and Electronics Engineers*
IFS	: *Interframe Spacing*
IP	: *Internet Protocol*
ISA	: *International Society of Automation*
ISM	: *Industrial, Scientific, and Medical*
LAN	: *Local Area Network*
RFID	*: Radio-Frequency IDentification*
RTS	*: Request to Send*
SSID	: *Service Set IDentifier*
VPN	: *Virtual Private Network*
WAN	: *Wide Area Network*
WEP	: *Wired Equivalent Privacy*
WLANs	: *Wireless Local Area Network*
ZOD	: *ZigBee Object Device*

SUMÁRIO

INTRODUÇÃO

O interesse na utilização de tecnologia de transmissão de dados sem fio em soluções para automação industrial tem crescido bastante nos últimos anos. Isto se deve às diversas vantagens trazidas por esse tipo de tecnologia que se adaptam bem aos sistemas de automação industrial. Podemos citar como algumas destas vantagens a facilidade e a rapidez de instalação, a economia em relação a projetos cabeados, a flexibilidade para alteração de instalações existentes, a integração de equipamentos móveis à rede, a possibilidade de posicionamento de sensores e atuadores em locais de difícil acesso, a não necessidade de infraestrutura para cabos e eletrodutos, dentre outras.

Entretanto, uma pesquisa realizada pela ControlGlobal (ControlGlobal, 2007) mostrou que o uso de redes sem fio em sistemas de automação ainda é muito pequeno (63,7% dos entrevistados possuem menos de 10 dispositivos sem fio em suas plantas); que os usuários têm receio de utilizá-las em aplicações de controle (apenas 24,6% estariam dispostos a usar dispositivos sem fio em aplicações de controle mesmo que o tempo de ciclo seja maior que 2 segundos) e ainda que existe uma grande preocupação com a confiabilidade e segurança dos dados (66,4%). Os resultados apresentados mostram que a utilização de comunicação sem fio em ambientes industriais ainda gera inseguranças e dúvidas entre os usuários, pois, a maioria das aplicações nestes ambientes exige segurança, confiabilidade e eficiência. Isto significa dizer que uma rede sem fio deve garantir, mesmo na presença de interferências e condições adversas ao meio de transmissão, que as mensagens chegarão aos seus destinos, que os requisitos temporais de baixa latência e determinismo na troca de mensagens serão respeitados e, por fim, assegurar a privacidade de comunicação e a integridade dos dados transmitidos (Santos, 2007), (Zheng & Myung, 2006).

Estabelecer uma boa comunicação entre todos os nós da rede torna-se um grande desafio devido às complicações inerentes a esses ambientes industriais, repleto de obstáculos móveis e imóveis, como, por exemplo, tanques, vasos, tubulações, prédios, estruturas metálicas, guindastes, caminhões, etc. Além disso, existem interferências eletromagnéticas provenientes de outras redes sem fio para comunicação de dados (WLAN e Bluetooth), interferências de rádios de comunicação (walkie-talkie), interferências eletromagnéticas oriundas de equipamentos elétricos (motores, geradores, transformadores, etc) e interferências causadas por reflexão do próprio sinal transmitido devido a obstáculos.

A potencialidade do emprego da solução de comunicação sem fio e o crescente interesse vindo do segmento industrial estão servindo como motivação para o surgimento de padrões específicos que tem o propósito de atender as necessidades de implantação de redes sem fio específicas para os ambientes industriais. Cabe destacar o surgimento de dois padrões importantes aplicados nesta área: WirelessHart (WirelessHart, 2007) e o ISA-SP100.11a (ISA-100.11a-2009). São padrões que utilizam técnicas de espalhamento em freqüência para lidar com as interferências eletromagnéticas e aumentar a confiabilidade da transmissão, podendo utilizar topologias em malha ou árvore, e utilizam técnicas de retransmissão de sinais em que uma mensagem é transmitida de um nó para outro com auxílio de outros nós intermediários, que funcionam como roteadores, até que a mensagem chegue ao seu destino. Isto faz com que a rede consiga ter um maior alcance e também apresente uma maior tolerância a falhas, pois se um nó intermediário apresentar uma falha ou não puder receber uma mensagem, esta pode ser redirecionada para outro nó (Hoffert at al, 2007).

Entretanto, uma rede em malha também exige um estudo cuidadoso do posicionamento dos nós que a compõem, isto porque se torna necessário verificar se os requisitos temporais vinculados a entrega de mensagens são obedecidos dentro de critérios pré-estabelecidos. Além disso, nesse tipo de solução, é fundamental garantir que todos os nós da rede tenham acesso ao nó central, assim como verificar a existência de nós críticos, cuja perda por falha possa acarretar em grande perda de conectividade e ou desempenho.

Uma das principais características dessas redes sem fio, senão a mais importante é o fato de poder utilizar dispositivos intermediários para retransmissão de pacotes. Esta funcionalidade tem uma série de vantagens, que estão relacionadas ao poder de escalabilidade da rede e a redundância da informação. Esses dispositivos intermediários, ou nós de retransmissão ou ainda nós roteadores, tem um papel fundamental no funcionamento da rede, e a definição das quantidades desses nós envolvidos, com suas coordenadas, são primordiais e ao mesmo tempo difíceis de serem definidas. A motivação deste trabalho é elaborar uma ferramenta que possa auxiliar o usuário no posicionamento desses nós roteadores nos ambientes a que eles se propõem, considerando determinados critérios e condições que potencializam a dificuldade de uma boa solução.

O objetivo deste trabalho é elaborar uma ferramenta para analisar o posicionamento dos nós de uma rede sem fio em malha e determinar uma proposta de solução a partir de um determinado cenário, auxiliando o projetista da rede a encontrar as melhores configurações de posicionamento dos nós. A partir das informações dos pontos de medição de processo que o usuário deseja instrumentar, que consequentemente são pontos de comunicação, a ferramenta avaliará a cobertura da rede formada, a presença de nós críticos, a presença de caminhos redundantes, a quantidade de saltos das mensagens, a tolerância a falhas por perda de nós e, sugerirá o menor número de nós roteadores intermediários adicionais (se necessário) e suas coordenadas geográficas, de modo a garantir que a rede atenda aos critérios estabelecidos pelo projetista ou usuário da rede.

A procura das melhores configurações é vista como um problema de otimização, onde os parâmetros de entrada são os nós da rede com as respectivas coordenadas geográficas (nós de processo e nós roteadores), e a função de custo a ser otimizada levará em conta critérios como a otimização da menor quantidade de nós roteadores intermediários necessários à rede, a minimização da quantidade de retransmissões de pacotes por nó, menor quantidade de saltos (hops) das mensagens até seus destinos finais, a maximização da quantidade de nós vizinhos por nó de forma a garantir caminhos alternativos para as mensagens, maximização da tolerância à falha da rede por perda de nós e a maximização de nós com conexões diretas com o nó central (gateway).

Além disso, algumas restrições são impostas pelo algoritmo para compor a otimização do problema, que são determinadas por penalidades impostas pelo algoritmo por descumprimento de condições com relação à cobertura da rede, a quantidade mínima de nós vizinhos, quantidade mínima de conexões diretas com o gateway, quantidade máxima de número de saltos (hops) por pacotes, quantidade de transmissões excedentes por nó e pela distância máxima ponto a ponto com visada direta, com intuito de garantir a potência mínima de transmissão.

Na maioria dos casos, as redes sem fio voltadas para atender aplicações industriais tornam-se complexas pelas exigências de um funcionamento perfeito, não que em outras situações as redes não tenham que funcionar corretamente, mas pelo próprio grau de criticidade inerente dos processo industriais, aliadas às distâncias envolvidas e aos obstáculos encontrados nesses ambientes, exigindo que a rede tenha topologias mais elaboradas e robustas como malha ou árvore. Nessas topologias a comunicação realiza múltiplos saltos para alcançar outros

dispositivos da rede, passando por nós intermediários (nós roteadores) que exercem funções de roteamento. Devido a este fator, os nós intermediários acabam exercendo um papel fundamental na arquitetura da rede, pois, sendo responsáveis pela concentração e distribuição das informações, influenciam diretamente no funcionamento e desempenho da rede, podendo inserir atrasos consideráveis na transmissão das mensagens fim a fim. Por isso, os nós roteadores tornam-se pontos críticos de falhas, podendo interromper a comunicação de partes da rede que dependam dele caso ocorram problemas, ou até mesmo da rede toda dependendo da topologia e da posição desse nó. A ferramenta desenvolvida neste trabalho tem foco no posicionamento desses nós roteadores, devido a sua importância mencionada anteriormente e pela dificuldade inerente de solucionar estas questões de posicionamento sem o auxílio de uma ferramenta computacional. A ferramenta desenvolvida foi baseada no software MatLab, com *toolboxes* específicas para otimização através de Algoritmos Genéticos, que calculam as quantidades mínimas de nós roteadores adicionais em uma rede sem fio com as melhores coordenadas geográficas sob as métricas citadas anteriormente.

Esta dissertação está organizada em cinco capítulos, cujos conteúdos são descritos a seguir.

O capítulo 1 apresenta material de apoio em comunicação sem fio e discute alguns conceitos necessários à compreensão deste trabalho. São apresentados os principais tipos de redes de sensores sem fio e são mencionados alguns artigos relevantes. A pesquisa procurou demonstrar as potencialidades das redes sem fio e fornecer subsídios para o trabalho desenvolvido.

O capítulo 2 apresenta o problema de posicionamento dos nós em redes sem fio e discute algumas soluções encontradas.

O capítulo 3 descreve a solução proposta para o problema de posicionamento dos nós, descrevendo a modelagem utilizada.

No capítulo 4, são apresentados alguns estudos para avaliação de desempenho do algoritmo. Também é apresentado o estudo de caso, e comentários sobre os resultados obtidos.

A conclusão deste trabalho é apresentada no Capítulo 5 juntamente com uma relação de possíveis trabalhos futuros.

1 REDES DE SENSORES SEM FIO

1.1. Introdução

Rede de sensores é uma tecnologia de redes sem fio (RSSF) com capacidade de suportar um grande número de nós sensores inteligentes, com capacidade de processamento de sinais e comunicação de dados e são distribuídos densamente em uma determinada região de interesse. Os nós sensores não utilizam cabeamento, sendo alimentados por baterias e se conectam a rede sem fio de forma simples, possuem baixo custo e normalmente não são reaproveitados. Devido à necessidade de economia de energia, os nós sensores possuem funções e dimensões limitadas que estão relacionadas ao prolongamento da vida útil das suas baterias, dessa forma, as redes de sensores podem operar por longos períodos de tempo sem necessidade de manutenção de seus dispositivos. As redes de sensores têm uma vasta gama de áreas de aplicações englobando áreas militar, industrial, aviação, ambiental, controle de tráfego aéreo, engenharia, dentre outras. Além disso, as redes de sensores devem possuir características de auto-adaptação para correção de problemas que venham a ocorrer com seus nós sensores acarretando perda de comunicação.

Uma rede de sensores sem fio (RSSF) tende a ser autônoma e requer um alto grau de cooperação entre os nós sensores para que sejam executadas as tarefas definidas para a rede. Isto significa dizer que algoritmos distribuídos tradicionais, como protocolos de comunicação e eleição de líder, devem ser revistos para esse tipo de ambiente antes de serem usados diretamente. Os desafios e considerações de projeto de RSSFs vão muito além das redes tradicionais. Nessas redes, cada nó pode ser equipado com uma variedade de elementos sensores, tais como acústico, sísmico, infravermelho, vídeo-câmera, calor, temperatura e pressão, de acordo com a finalidade da aplicação a que se propõem. Esses nós sensores podem ser organizados em grupos (*clusters*) onde pelo menos um dos sensores deve ser capaz de detectar um evento na sua região de medição, processá-lo e tomar uma decisão se deve fazer ou não uma difusão (*broadcast*) do resultado para outros nós. A visão é que RSSFs se tornem disponíveis em todos os lugares executando tarefas e monitorando fenômenos dos mais variados possíveis (Loureiro at al, 2007).

1.2. Elementos das Redes de Sensores

As redes de sensores possuem como elementos principais: o sensor, o observador e o fenômeno, que estão definidos a seguir (Clicia at al, 2010).

O **sensor** é o dispositivo responsável pela monitoração de uma grandeza física de um determinado fenômeno, que pode ser um fenômeno ambiental e gera relatórios de medidas através de comunicação sem fio. Um sensor produz uma resposta mensurável a mudanças em condições físicas, tais como temperatura, campo magnético e luz. Os dispositivos de detecção ou medição, geralmente, têm características físicas diferentes. Muitos modelos possuem complexidades variadas e podem ser construídos de acordo com a necessidade da aplicação e com as características dos dispositivos. Na maioria dos modelos de dispositivos de sensores a capacidade de detecção ou medição diminui com o aumento da distância do sensor ao fenômeno e melhora conforme o tempo de exposição que o sensor fica exposto para coletar as informações. Um sensor, tipicamente, consiste de cinco componentes: detector de hardware, memória, bateria, processador embutido e transceptor.

O **observador** é o usuário final interessado em obter as informações coletadas pelos elementos sensores em relação a um determinado fenômeno e disseminadas pela rede de comunicação sem fio. O observador pode requisitar consultas para a rede e receber as respectivas respostas destas consultas. Além disso, uma rede de sensores pode suportar múltiplos observadores simultaneamente.

O **fenômeno** é a entidade de interesse do observador, que está sendo monitorada e cuja informação será capturada e analisada pela rede de sensores. Além disso, múltiplos fenômenos podem ser observados concorrentemente numa rede. Numa aplicação, o observador está interessado em monitorar o comportamento do fenômeno sob algum aspecto de desempenho específico, como por exemplo, precisão, ou retardo. Numa rede de sensores típica, os sensores individuais disponibilizam amostras de medidas locais e disseminam a informação para outros sensores e eventualmente para o observador. As medições realizadas pelos sensores são amostras discretas do fenômeno físico, sujeito a precisão do elemento sensor individual, assim como a localização com respeito ao fenômeno (Clicia at al, 2010).

Uma rede de sensores é uma ferramenta para medir e passar informação sobre o fenômeno para o observador dentro do limite de desempenho desejado e com melhor custo/benefício possível.

1.3. Características das Redes de Sensores

As redes de sensores são, por natureza, centradas em dados, diferente das redes tradicionais que são centradas em endereço. De acordo com esta característica, um nó sensor difunde informações baseadas em atributos, tais como, faixas de temperatura, níveis de vibrações, localização espacial, limite de velocidade e etc. Outra característica peculiar é que se espera que os nós sensores atendam aos requisitos específicos da aplicação, sendo comum o atendimento de um só atributo ou, no máximo, alguns poucos atributos combinados. Por exemplo, na detecção de um veículo em um cruzamento os atributos velocidade e direção poderão ser relevantes, o que implicará na capacidade de processamento da rede.

Os principais requisitos deste tipo de rede são baixa latência, limitações rígidas de energia, baixo custo e possibilidade de implementação de redes com um elevado número de dispositivos (alta densidade) e baixa complexidade dos nós da rede.

Outra característica, também derivada do baixo preço por sensor e, conseqüentemente, sua alta disponibilidade, será certamente a formação de *redes densas e altamente escaláveis*, com poucos cuidados com relação à instalação. Pode-se pensar numa distribuição saturada de nós sensores em certo ambiente que se deseje monitorar/analisar, tirando-se proveito de um alto grau de redundância e disponibilidade. As características de alta disponibilidade e de orientação de dados combinadas, remetem a agregação de dados nos nós sensores, determinada por interações localizadas entre nós que compartilham a mesma vizinhança para reduzir tráfego e economizar energia, coordenar sensoriamento e direcionar interesses.

1.4. Métricas de desempenho

As principais métricas para se avaliar protocolos de redes de sensores são: eficiência de energia e vida útil do sistema, latência, precisão, tolerância a falhas, escalabilidade e exposição dos sensores.

1.4.1 Eficiência de energia e vida útil do sistema

Como os nós sensores operam por baterias, os protocolos devem ser eficientes na utilização dos dispositivos, de forma a economizar energia para maximizar a vida útil do sistema.

A vida útil do sistema pode ser medida por parâmetros genéricos, como o tempo de nós ativos ou tempo de envio de informações à aplicação. Como exemplo, podemos citar o tempo necessário para que a metade dos nós da rede esteja ativos ou o tempo em que a rede pára de suprir a aplicação com a informação desejada sobre o fenômeno. Para atuar na eficiência de utilização de energia, existem protocolos de controle de acesso ao meio para redes de sensores sem fio. Como exemplo, podemos citar o protocolo *SMAC* (*Sensor-Medium Access Control*) que foi implementado visando redes de sensores com nós individuais que permanecem por longos períodos de tempo inativos, e que estes sensores tornem-se rapidamente ativos quando algum fenômeno for detectado. Os nós permanecem inativos periodicamente para reduzir o consumo de energia (Clicia at al, 2010).

1.4.2 Latência e precisão

As redes de sensores devem respeitar um espaço de tempo máximo para o envio das mensagens que seja satisfatório para uma dada aplicação, que determina a latência de transmissão da rede, onde a latência é dependente da variável a ser monitorada e da aplicação. Obter informações com precisão é o objetivo principal do usuário, onde a precisão é determinada pela aplicação dada. Há um compromisso entre precisão, latência e eficiência de energia. A infra-estrutura dada deve ser adaptativa tal que a aplicação obtenha a precisão e retardos desejados com uso mínimo de energia. Por exemplo, a aplicação pode requerer disseminação mais freqüente de dados dos mesmos nós sensores ou pode direcionar a disseminação de dados dos mesmos nós sensores com a mesma freqüência (Clicia at al, 2010).

1.4.3 Tolerância a falhas

Os sensores tipicamente realizam roteamento de informações para a estação base como se fosse uma rede conectada em árvore. A falha de um único nó pode resultar na interrupção da transmissão numa porção da rede, fazendo com que a estação base pare de receber aqueles dados. Os nós sensores podem apresentar falhas por diversos motivos, seja por dano físico no próprio sensor, por baixa carga de sua bateria, por interferências eletromagnéticas ou até outras causas, e dependendo do aspecto físico da aplicação, o reparo ou a substituição desses sensores poderá ser uma tarefa difícil. Dependendo do tamanho do dano, a rede deve ter a capacidade de recuperar as informações através de novos roteamentos ou, se não for possível, a

estação base deve emitir um aviso de que a propriedade de funcionamento da rede de sensores não pode mais ser garantida (Clicia at al, 2010). Por este motivo, a rede deve ser tolerante a falhas, e essa tolerância pode ser aumentada através da replicação de dados. Uma das vantagens do sensoriamento distribuído é permitir a redundância de informações por caminhos alternativos através dos nós sensores, e quanto maior forem essas alternativas de roteamento de mensagens entre nós origem e destino, maior será a tolerância a falhas da rede.

1.4.4 Escalabilidade

A escalabilidade em redes de sensores é um fator importante devido ao grande número de nós sensores utilizados que podem chegar à ordem de dezenas, centenas, milhares ou ainda milhões para algumas aplicações. A escalabilidade exige protocolos de roteamento, endereçamento e agregação de dados escaláveis, de forma que o grande número de nós não cause uma perda de desempenho significativa da rede garantida (Clicia at al, 2010).

1.4.5 Segurança em redes de sensores

Para que uma rede de sensores forneça dados com segurança é necessário que alguns requisitos sejam cumpridos. Em muitas aplicações de redes de sensores, a rede pode estar sujeita a uma situação onde um intruso pode ser motivado a uma invasão para alterar a funcionalidade da rede. Um intruso pode ser capaz de posicionar diversos nós dentro da rede e usá-los para transmitir falsas mensagens, ou até mesmo comprometer o funcionamento de um nó da rede e conseguir acesso as suas principais informações (Clicia at al, 2010). Em (L. Hu e D. Evans, 2003) é tratado o caso onde um intruso deseja corromper a informação que está sendo produzida pela rede de sensores. É apresentado um protocolo que provê um mecanismo de agregação segura para redes de sensores, dentro dos limites de consumo de energia e memória. A agregação de mensagem pode reduzir significantemente o *overhead* de comunicação, mas dificulta a segurança. Cada nó intermediário pode modificar, forjar ou descartar mensagens, ou simplesmente transmitir valores de agregação falsos. Dessa forma, um nó comprometido pode ser capaz de alterar significantemente o valor final da agregação. Não se pode criptografar mensagens com uma única chave compartilhada entre cada dispositivo e a estação base, já que cada nó intermediário precisa entender as mensagens recebidas para realizar a agregação. Além

disso, não se pode armazenar a mesma chave em todo dispositivo para permitir criptografar ou fazer autenticação, já que um intruso que descobrir a chave de um dispositivo poderá controlar a rede inteira. Por isso, foi desenvolvido um protocolo com mecanismos para detectar nós com comportamento errado, que possam estar modificando ou forjando mensagens, transmitindo valores agregados falsos. Com este mecanismo, uma estação base é capaz de garantir que os dados transmitidos sejam corretos, mesmo com nós falsos introduzidos ou que ele descubra as informações importantes de um único nó (Clicia at al, 2010). Segundo (L. Hu e D. Evans, 2003) foram implementadas duas idéias: agregação e autenticação atrasadas. Ao invés da agregação das mensagens ser realizada na próxima rota, as mensagens são passadas para a rota seguinte, sem alterações, onde são agregadas. Isto aumenta o custo da transmissão, mas garante a integridade dos dados para redes onde dois nós consecutivos não estão comprometidos. As mensagens são autenticadas com um atraso, mas isto permite que as chaves sejam simétricas e reveladas para o autenticador depois que o tempo de atraso tenha expirado. Estas estratégias aumentam a confidencialidade na integridade de leituras de sensores sem perder a oportunidade de agregar resultados intermediários na rede.

1.4.6 *Self Organizing* em redes de sensores

As redes de sensores auto-organizáveis são construídas a partir de nós sensores que possuem a capacidade de criar novas rotas para rede, de forma espontânea e por si próprios. Os nós sensores têm a capacidade se adaptar dinamicamente a rede para suprimir ou minimizar falhas de dispositivos e degradação da rede, gerenciar movimentos de nós sensores e reagir às requisições da rede. Nós sensores auto-organizáveis permitem que dispositivos sensores sejam autosuficientes, auto-reconfiguráveis e autônomos. Os principais benefícios destas características são: (i) Suporte a aplicações táticas e de vigilância, usando nós sensores reconfiguráveis que são capazes de formarem variações nas redes, realizadas de forma incremental e montadas automaticamente sem dependência da administração central; (ii) Prover capacidades para redes de sensores se adaptarem dinamicamente a falhas e degradação de dispositivos e mudarem requisições em tarefas e na rede e (iii) Integrar vários serviços de rede específicos de aplicações e serviços de sistemas providos por tipos mistos de nós sensores e aplicações de defesa (A. Lim, 2003), (Clicia at al, 2010).

1.5. Enlaces de rádios

As ondas de rádio são parte de um espectro eletromagnético, que também inclui outros tipos de radiação como a luz, raios gama, etc. Neste caso, as ondas de propagação de rádio podem, genericamente, ser comparadas à propagação da luz, pois movem-se de forma direta através do espaço e podem penetrar em materiais como vidro, podem ser absorvidas ou refletidas dependendo do material e do obstáculo, ou podem ser atenuadas por material como névoa ou simplesmente pela distância. Geralmente, no espaço livre, as ondas de rádio se propagam em todas as direções, sofrendo somente atenuação da potência do sinal pelo aumento da distância, como mostrado na figura 1 (HART Communication Foundation, 2011).

O sinal de rádio freqüência aplicado no ambiente industrial sofre efeitos, principalmente, de influências relacionadas à interferência, movimento de equipamentos e pessoas e o desvanecimento do sinal por múltiplos caminhos. A interferência sempre acontece quando uma onda é refletida ou sobreposta por outra onda, o que pode causar um efeito positivo, onde a onda resultante aumenta em amplitude pelas componentes da onda original e da onda refletida, ou negativo, onde a onda original pode sofrer anulação da onda refletida, como mostrado nas figuras 1 e 2 (LIT-131 HART Communication Foundation, 2011).

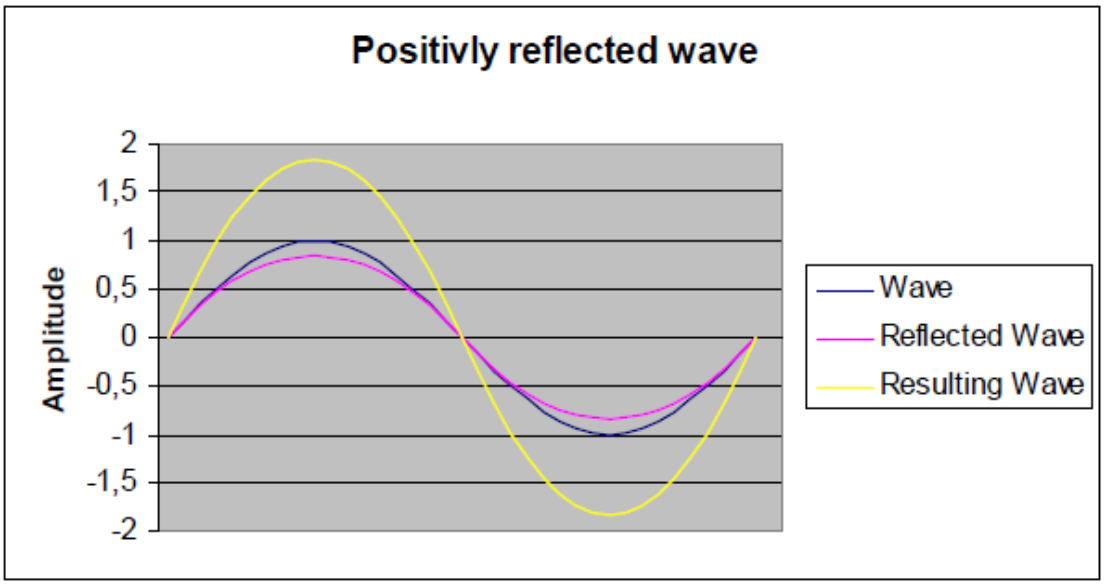

Figura 1 – Onda resultante efeito positivo (LIT-131 HART C. F., 2011)

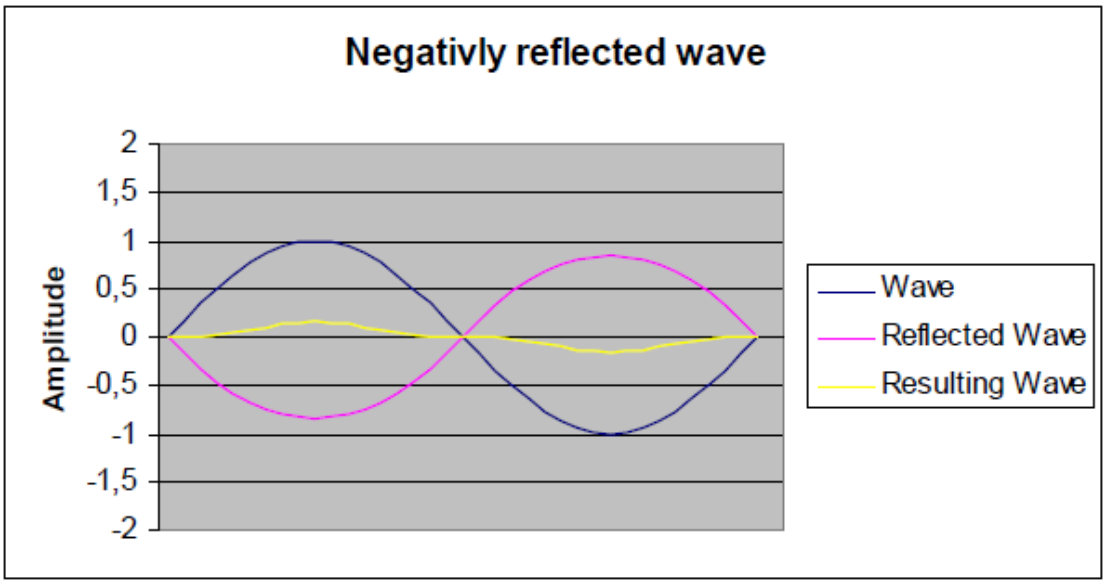

Figura 2 – Onda resultante efeito negativo (LIT-131 HART C. F., 2011)

O segundo efeito causado por elementos dinâmicos, como movimento de veículos, cargas, equipamentos e pessoas alteram o ambiente, podendo causar influências na propagação do sinal RF. O terceiro efeito é o enfraquecimento do sinal por múltiplos caminhos, devido à reflexão em obstáculos, a onda se move em diferentes caminhos desde a origem até o destino, chegando lá com defasagem de tempo. Este efeito pode distorcer o sinal a tal ponto do destino não reconhecer a mensagem original. Como resultados desses três efeitos, duas principais conseqüências devem ser consideradas quando se deseja realizar uma aplicação utilizando comunicação wireless em ambiente industrial: alcance e confiabilidade. O alcance diminui pelo decréscimo da potência com aumento da distância no espaço livre de propagação, como mostrado no exemplo de um ambiente industrial da figura 3. O movimento de equipamentos e as alterações no ambiente de comunicação afetam diretamente a confiabilidade da comunicação. Uma conexão em funcionamento não deve ser afetada por causa, por exemplo, de um caminhão parado no caminho do sinal. (LIT-131 HART C. F., 2011).

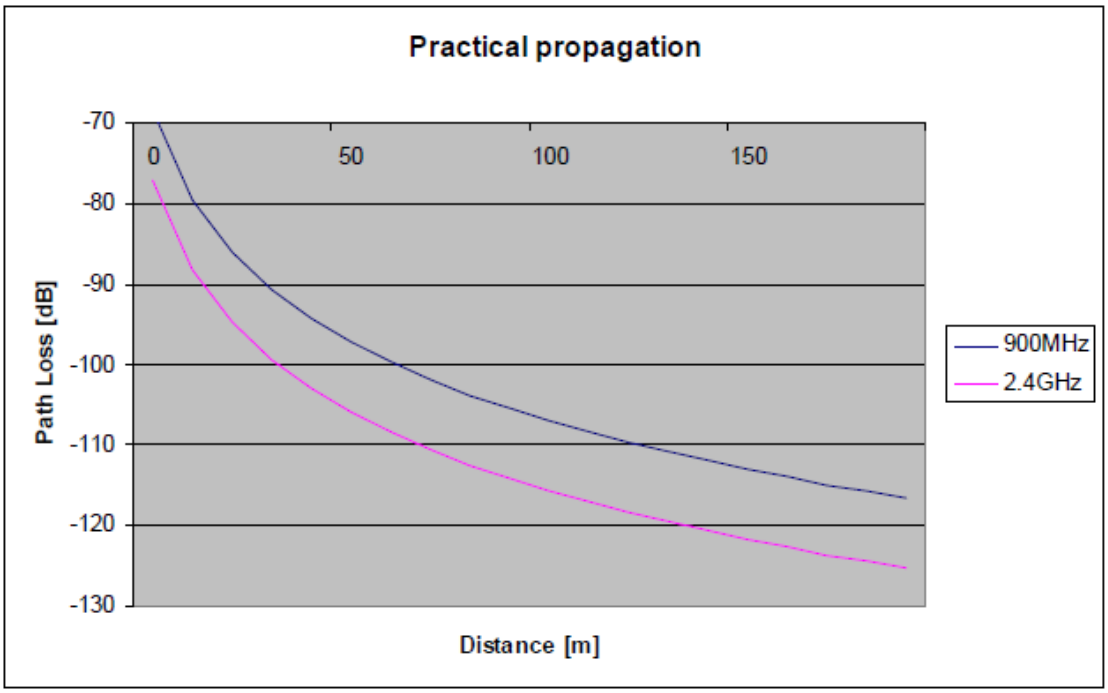

Figura 3 – Distância x Potência (LIT-131 HART C. F., 2011)

Para que haja comunicação entre transmissor e receptor em um circuito RF é preciso que haja visada direta entre as antenas dos dois lados. Por esse motivo, elas devem estar posicionadas nos lugares mais altos (normalmente topos dos prédios) e livres de obstáculos para que não ocorram os já citados fatores de reflexão, difração e espalhamento. A propagação do sinal de rádio é sem dúvida um fator fundamental para um bom desempenho da comunicação de redes sem fio (FONTÃO, 2008). Nos projetos de rede sem fio onde se tem visada direta entre dispositivos, a preocupação passa a ser de enquadrar a distância com os limites de transmissão do sinal e a atenuação no espaço livre. Obviamente, em ambientes industriais, haverá obstáculos entre dispositivos que precisam se comunicar, formados, por exemplo, por superfícies reflexivas. Desconsiderando que a distância ponto a ponto seja um limitante para essa propagação, o sinal transmitido sofrerá problemas, como a obstrução total do sinal e as reflexões do próprio sinal causadas por essas superfícies reflexivas. As ondas emitidas, ao se espalhar, passam por diferentes caminhos e se reflete em vários obstáculos até chegar ao destino; causando assim uma interferência. Isto é chamado de interferência de “Multi-Path” (múltiplos caminhos) (RORIZ at al, 2010), fenômeno que ocorre quando um sinal é recebido por várias vias indiretas, decorrentes da reflexão desses obstáculos, onde o sinal recebido é o somatório de sinais idênticos que se diferem em fase e amplitude. Além disso, existe ainda a atenuação por penetração, onde os

obstáculos atenuam, mas não impedem que o sinal atravesse o obstáculo, como por exemplo, vegetação, paredes finas, etc.

O enlace sem fio é uma linha de sinal compatível com a zona de Fresnel. A Zona de Fresnel é de suma importância no planejamento e manutenção de um link RF, e pode ser definida como uma série de elipses concêntricas em torno da linha de visada, como mostra figura 4. Ela é importante para a integridade do link porque determina uma área em torno da linha de visada que pode introduzir interferência no sinal caso ele seja bloqueado. Objetos na Zona de Fresnel tais como árvores, prédios entre outros, podem produzir reflexão, difração, absorção ou espalhamento do sinal, causando degradação ou perda completa do sinal (FONTÃO, 2008).

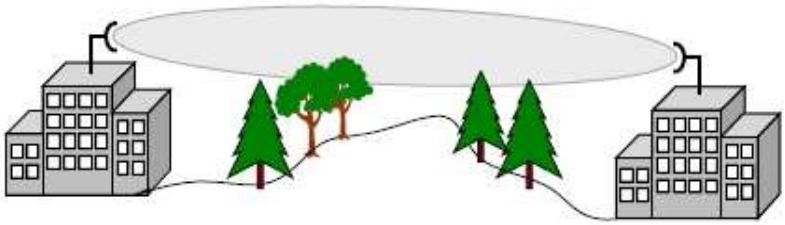

Figura 4– Zona de Fresnel

1.6. Padrões de Comunicação para Redes Sem Fio

Dentre diversos padrões e protocolos existentes para redes sem fios, estão descritos abaixo aqueles que mais estão próximos com o trabalho desenvolvido.

1.6.1 Padrão de comunicação IEEE 802.15.4

Este padrão define a camada física PHY (Physical Layer) e as especificações para camada de acesso ao meio MAC (Medium Access Control) para conectividades *wireless* que utilizem baixa taxa de dados com dispositivos de baixo consumo de energia. O padrão utiliza o mecanismo CSMA-CA (carrier sense multiple access with collision avoidance) para controle de acesso na camada MAC (Medium Access Control) e suporta as topologias estrela e ponto a ponto (IEEE Computer Society. IEEE Std. 802.15.4-2006).

O padrão IEEE 802.15.4 foi criado para atender baixas taxas de comunicação em redes sem fio. Outros padrões existentes de comunicação sem fio são voltados para otimização de vazão (throughput) e, freqüentemente, não se preocupam com o consumo de energia, que é fator preponderante a ser considerado em redes de sensores sem fio (RSSF). O padrão IEEE 802.15.4 baseia-se no baixo custo e na limitação de recursos dos dispositivos para alcançar as premissas de baixo consumo de energia e baixa manutenção. O padrão é dividido em duas camadas, a camada física (PHY) e a sua camada de controle de acesso ao meio (MAC). Essas camadas se situam abaixo da camada de roteamento ou das camadas de aplicação (como mostrado na figura 5). A camada física e a camada MAC fornecem recursos para a criação de diferentes tipos de topologias de rede, incluindo estrela, malha e agrupamento em árvore. Ela foi projetada para operar com duas classes distintas de dispositivos, o RFD e o FFD. Os FFDs (*fully functional devices* - dispositivo de função completa) são dispositivos com capacidade para se comunicar com qualquer tipo de dispositivos na rede sem fio dentro do seu alcance, enquanto os RFDs (*reduced function devices* - dispositivo de função reduzida) são dispositivos com funções limitadas, apenas com capacidade de se comunicarem diretamente com FFDs. Todas as redes sem fio possuem múltiplos FFDs e RFDs, sendo apenas um FFD designado para exercer a função de coordenador da rede (PAN Coordinator) (J. Hoffert, 2005). A tabela 1 apresenta características desse protocolo.

Tabela 1 - IEEE 802.15.4

Taxa de dados de	250 Kbps, 40 Kbps, e 20 Kbps
Topologia	estrela, árvore e malha
Endereços	16 bits ou estendidos de 64 bits
Alocação de intervalos de tempo garantidos	(GTS)
Acesso ao canal	CSMA-CA
Confiabilidade na transferência	Protocolo com reconhecimento de dados
potência de consumo	Baixa
Detecção de energia (ED)	Sim
indicação da qualidade do Link (LQI)	Sim
Faixas de frequencia	16 canais na banda de 2450 MHz, 10 canais em 915 MHz, 1 canal em 868 MHz

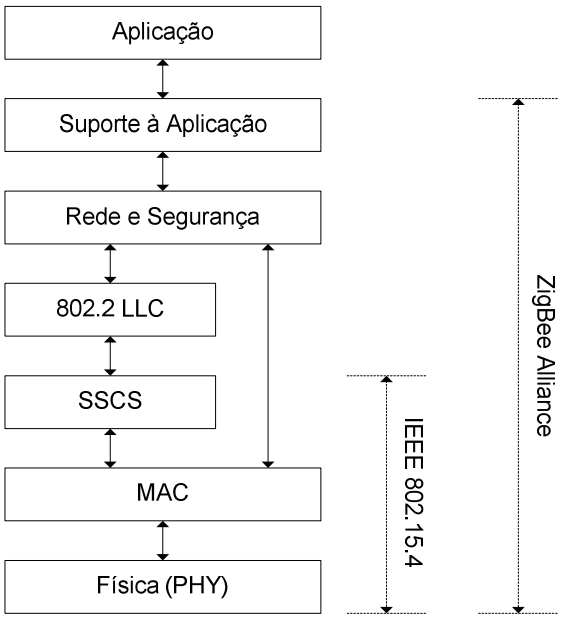

Figura 5– Camadas da Rede

Cada rede consiste de múltiplos FFDs e RFDs, sendo que um dos FFDs deve ser designado como coordenador da rede. Dependendo da aplicação, a rede pode operar nas topologias estrela, malha ou árvore. Na topologia estrela, cada nó sensor se conecta diretamente com o nó central, e tem a característica de ser mais veloz no envio de dados, mas todos os participantes devem estar no domínio do nó central. Esta topologia se aplica a instalações de baixo consumo de energia e com limitações geográficas. A topologia em malha tem conexões ponto a ponto entre nós, onde cada sensor atua como um roteador, enviando e recebendo dados de outros sensores ou do nó central. Este tipo de topologia é ideal para grandes áreas de rede, porém a energia consumida pelos participantes para realização das funções de roteamento é um fator crítico. A topologia em árvore é uma variação das topologias mencionadas anteriormente, como pode ser visto na figura 6. Na topologia estrela, a comunicação é estabelecida entre dispositivos e um único controlador central, chamado coordenador PAN. Após um FFD ser ativado pela primeira vez, ele pode estabelecer sua própria rede e tornar-se o Coordenador PAN. Cada rede inicializada escolhe um identificador PAN, que não esteja sendo concorrentemente usado por alguma outra rede dentro do alcance de influência do rádio. Isto permite que cada rede opere de forma independe. Uma vez escolhido o identificador PAN, o coordenador permite que outros dispositivos se liguem à sua rede. Todos os dispositivos operando na rede, em qualquer topologia, terão um único endereço estendido de 64 bits. Este endereço poderá ser utilizado para

comunicação direta dentro da PAN, ou pode ser trocado por um endereço curto alocado pelo coordenador PAN quando o dispositivo se associa. A topologia ponto a ponto (*peer to peer*) também tem um coordenador PAN, contudo, difere da topologia em estrela pelo fato de que qualquer dispositivo FFD pode se comunicar com outro, desde que ele esteja no seu raio de alcance de transmissão. Esta topologia permite a implementação de redes mais complexas, tais como formação em redes de malha ou em árvore (*Cluster-tree*). Uma rede ponto a ponto pode também permitir múltiplos saltos, para rotear mensagens de qualquer dispositivo para algum outro da rede. A rede *Cluster-tree* é um caso especial de uma rede ponto a ponto, onde a maioria dos dispositivos são FFDs e um dispositivo RFD pode conectar-se no final de um ramo. Qualquer FFD pode agir como um coordenador (roteador) e prover serviços de sincronização para outros dispositivos e coordenadores, porém somente um desses coordenadores será o coordenador PAN (Hoffert J., 2005), (Ergen S. C., 2004) (Zheng J., 2006)

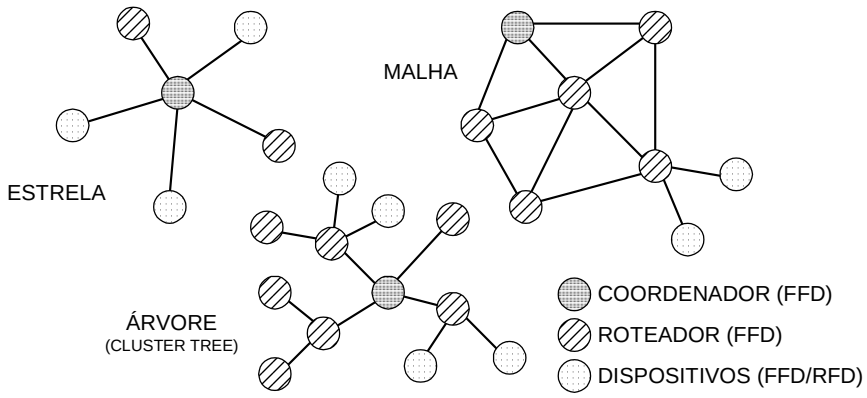

Figura 6 - Topologias de rede

A camada física (PHY) fornece uma interface entre a camada MAC e o canal de rádio-frequência. O link wireless pode operar nas três bandas livres de freqüência ISM permitidas para o uso, variando as taxas de bits. Para o padrão europeu (868 – 868,6 MHz) a taxa é de 20kbps, para o padrão americano (902 – 928 MHz) a taxa é de 40kbps e para a banda (2.4-2.4835 GHz) a taxa de bits é de 250kbps. Esta camada é responsável pela ativação e desativação do transmissor, pela seleção de canal de freqüência e pela transmissão e recepção dos dados. Além disso, são responsáveis pelas seguintes tarefas: Detecção de energia (ED - *energy detection*), Indicação da qualidade do link (LQI - *link quality indication*) para pacotes recebidos, estimativa de canal livre (CCA - *clear channel assessment*) para CSMA-CA (*carrier sense multiple access with collision avoidance)* (Hoffert J., 2005).

O protocolo da camada MAC especifica quando o dispositivo pode acessar o canal para comunicação. Os serviços básicos fornecidos pela camada MAC são, a geração e sincronização de *beacon*, o suporte a associação e desassociação, o suporte opcional a segurança dos dispositivos, o gerenciamento do canal de acesso CSMA-CA, o *time de slot* de comunicação garantido (GTS - *guaranteed time slot*) e a validação e reconhecimento de mensagem. A *Personal Area Network* (PAN) pode ser configurada de duas formas básicas, com habilitação de *beacon* e sem habilitação de *beacon*. Em uma rede sem *beacon*, os dispositivos podem se comunicar uns com os outros após a fase inicial de associação. O acesso e disputa ao canal são gerenciados utilizando-se o mecanismo CSMA-CA. Em uma rede com habilitação de *beacon*, o coordenador PAN transmite periodicamente *beacons* que são usados pelos outros dispositivos para duas funções: para sincronização e para determinar quando um dispositivo está habilitado para transmissão e recepção de mensagens. Essas mensagens de beacon são usadas para se definir a estrutura do superframe em que todos os nós da rede (PAN) serão sincronizados (Hoffert J., 2005). A estrutura de superframe é apresentada na figura 7.

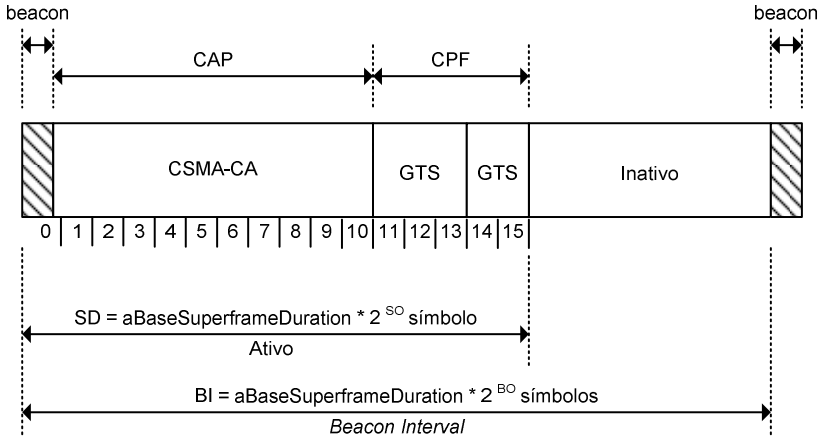

Figura 7 – Estrutura do *Superframe*

O quadro *superframe* é dividido em diversas seções, sendo o seu comprimento configurável. Existe um período ativo, na qual a comunicação é realizada, e existe um período inativo, onde os dispositivos podem desligar seus circuitos para conservar energia. O comprimento do *superframe* é definido pelo parâmetro *beacon interval* (BI) e o comprimento da parte ativa do frame é definido pelo parâmetro *superframe duration* (SD), conforme descrito abaixo (Zheng J., 2006).

BI = *aBaseSuperframeDuration* * 2^{BO}

SD = *aBaseSuperframeDuration* * 2^{SO}

onde,

aBaseSuperframeDuration = 960 símbolos

BO = beacon order

SO = superframe order

Os valores de *beacon order* (BO) e de *superframe order* (SO) são determinados pelo coordenador PAN. A parte ativa do *superframe* é dividida em 16 slots de igual tamanho, e o quadro de *Beacon* é transmitido no primeiro *slot* de cada *superframe*. A parte ativa pode ser dividida em dois períodos, sendo, um período de acesso com disputa (CAP - *contention access period*) e um período livre de disputa (CFP - *contention free period*). Entretanto, uma porção suficiente do CAP deve permanecer com acesso baseado em disputa para outros dispositivos de redes ou para novos dispositivos que desejarem se juntar à rede. O mecanismo CSMA-CA é usado para acesso dos canais durante o CAP (Zheng J., 2006). O período compreendido pelo CAP deve conter no mínimo 9 slots, mas poderá ocupar todos os 16 slots. Após o CAP temos um período livre de contenção (CFP - *contention free period*), que é opcional, e que pode conter até 7 slots ativos. Em um CFP, os dispositivos são alocados em slots GTS (*Guaranteed Time Slot*) pelo coordenador da rede PAN. Durante o GTS, um dispositivo tem acesso exclusivo ao canal e não executa o CSMA-CA. Durante um desses GTSs, um dispositivo pode tanto transmitir quanto receber dados de seu coordenador PAN, desde que não seja simultaneamente. Um GTS será reservado somente pelo coordenador da rede (PAN), e devem ser contínuos no CFP, e são alocados no final do período ativo do *superframe*. Um dispositivo pode desabilitar seu transceptor durante um GTS designado para outro dispositivo a fim de conservar energia. Para cada GTS o coordenador armazenará no pacote *beacon* o intervalo de tempo (*slot*), comprimento, direção e endereço do dispositivo associado. Todos os dispositivos devem passar por uma fase inicial de associação para fazer parte da PAN (personal area network), através de uma primitiva definida na camada MAC. A camada MAC permite configurações para ser ajustadas para iniciar um dispositivo na PAN, permitindo que um coordenador tenha dispositivos associados a ele. O reconhecimento de mensagens de um dispositivo para o seu coordenador é opcional, porém ele é requerido quando a transferência de mensagens é feita do coordenador para o dispositivo. (Hoffert J., 2005).

1.7. Zigbee

ZigBee é um padrão de rede sem fio (RSSF) definido por uma aliança de empresas de diferentes segmentos do mercado chamada "ZigBee Alliance". A especificação *ZigBee* de responsabilidade da *ZigBee Alliance* define as camadas superiores de rede, segurança e aplicação da pilha do protocolo.

O *ZigBee* é projetado para aplicações com baixas taxas de dados e baixo consumo de potência. Atualmente, a *ZigBee Alliance* disponibiliza duas especificações que servem como base para sistemas de comunicação e interoperabilidade com padrões de mercado**:** *ZigBee Specification* e *ZigBee RF4CE Specification***.** A especificação *ZigBee,* é a especificação principal, oficialmente chamada *ZigBee 2007,* que define as características de comunicação wireless. A especificação *ZigBee* tem duas opções de implementação ou dois conjuntos de características, onde ambas definem como a rede *ZigBee* funciona. A primeira característica *ZigBee* é projetada para suportar pequenas redes, operando com centenas de dispositivos em uma única rede, sendo adequada para uso em casas e escritórios (exemplo: iluminação artificial de casa). A especificação *ZigBee PRO*, mais amplamente usada, é otimizada para baixo consumo de potência e para suportar grandes redes com milhares de dispositivos, por ser mais robusto é adequado para aplicações de âmbito industrial. Ambas as características são projetadas para manter interoperabilidade de uma com a outra. A *ZigBee RF4CE Specification* foi projetada para aplicações de controle simples, ponto a ponto, que não requerem todas as características oferecidas pelo ZigBee 2007. O *ZigBee RF4CE* oferece baixos requisitos de memória permitindo baixos custos de implementação. A simplicidade da topologia ponto a ponto fornece facilidade em desenvolvimento e testes. Esta especificação prevê a utilização de controle em uma vasta gama de produtos incluindo dispositivos de entretenimento domiciliar, abertura de porta de garagem, sistema de acesso sem chaves e outros (ZigBee Alliance, 2011).

O *ZigBee* define três classes de dispositivos: ZigBee Coordinators (ZC), ZigBee Routers (ZR), and ZigBee End Devices (ZED). Cada rede tem um ZC, que é responsável pela formação da rede e que também pode apoiar o roteamento de mensagens. ZR´s também participam do roteamento e podem executar também aplicações de sensoriamento/atuação. Somente os ZED´s executam aplicações e não podem participar em mensagens de roteamento, onde cada ZED deve se reportar a um ZR ou um ZC. A rede *ZigBee* pode ter uma das seguintes topologias: (1) estrela,

onde todos os dispositivos não-coordenadores se conectam diretamente com o coordenador central; (2) árvore, onde todos os ZOD´s (*ZOD ZigBee Object Device*) são direcionados para um dispositivo de roteamento, que se comunicam entre si na árvore de acordo com a melhor hierarquia definida pelo ZC; e (3) malha (*mesh*), onde ambos ZOD´s e dispositivos de roteamento estão livres para se comunicarem com qualquer outro dispositivo de roteamento dentro da cobertura de rádio (Raymond S. Wagner, 2010).

As redes *ZigBee* podem ser classificadas quanto a topologia em estrela (*star)*, árvore (*tree)* e malha (*mesh)*. Esta classificação é definida a partir da caracterização da conexão entre os dispositivos em uma determinada rede. As redes classificadas como árvore e malha são formadas por um coordenador e vários roteadores e dispositivos finais associados a ele, sendo que esta associação pode ser direta, quando os dispositivos estão conectados diretamente ao coordenador, ou indireta, quando os dispositivos finais estão ligados a roteadores que por sua vez estão ligados diretamente ao coordenador ou em outros roteadores. Na topologia em estrela, a rede é controlada por um único dispositivo *e* não há presença de roteadores. Para implementação das camadas MAC (Medium Access Control) e PHY (Physical Layer) o ZigBee utiliza o padrão 802.15.4 do IEEE que opera em bandas de freqüências livres ISM (Instrumental, Scientific and Medical), operam nas faixas de freqüência de 868 MHz na Europa, 915 MHz nos Estados Unidos e 2.4 GHz nos outros lugares do mundo. A faixa de 2.4GHz é dividida em 16 canais, a faixa de 900MHz é dividida em 10 canais e a faixa de 860MHz tem apenas um canal. A faixa mais utilizada é a de 2.4GHz, que é a mesma faixa utilizada pelo Wi-Fi e Bluetooth**.** O *ZigBee* utiliza modulação espalhamento de espectro de seqüência direta (*Direct Sequence Spread Spectrum* DSSS) e o protocolo de acesso ao meio usado é o CSMA/CA. Em função de seu baixo ciclo de operação (*low duty cycle*) se torna mais imune à interferência do que os demais sistemas (Santos, 2007). A tabela 2 apresenta características desse protocolo.

Tabela 2 - Características ZigBee

Padrão (MAC + PHY)	IEEE 802.15.4
Taxa de Transferência	250 Kbps
Frequência	868 MHz / 915MHz / 2.4GHz
Modulação	DSSS
Corrente na Transmissão	30mA
Corrente em *Standby*	3uA
Expectativa de vida da bateria	1000 dias
Tempo de acesso à rede	30ms
Tempo de transição dos escravos	15ms
Tempo de acesso ao canal	15ms
Esquema de segurança	AES-128
Alcance (m)	10/30

1.8. Wireless Hart

O *WirelessHart* é um protocolo de rede de comunicação sem fio em malha voltado para atender as necessidades de aplicações de automação de processo. Ele acrescenta funcionalidades wireless ao protocolo HART, além de manter compatibilidade com os dispositivos HART existentes. O *WirelessHart* é uma parte principal do protocolo de comunicação de campo *HART* revisão 7. O protocolo HART, que é uma abreviação para "*Highway Addressable Remote Transducer*", tornou-se uma tecnologia de comunicação aberta em 1990 e atualmente é um padrão global (IEC 61158), e é a principal tecnologia de comunicação para instrumentos inteligentes de automação industrial com mais de 30 milhões de dispositivos instalados no mundo (HCF_LIT-89, HART Communication Foundation, 2011).

Como dito anteriormente, o *WirelessHart* é totalmente compatível com dispositivos *HART* existentes, o que possibilita a integração dessa tecnologia sem fio com as aplicações existentes nas plantas de processo. O protocolo *HART* tradicional utiliza o token-passing como controle de acesso para suportar o tráfego de dados, com o surgimento do *WirelessHart*, uma camada física (*Physical Layer*) e uma camada de dados (*Data Link Layer*) foram adicionadas pelo padrão. O *WirelessHart* é uma tecnologia segura e robusta, que utiliza topologia de rede em malha (*mesh)*, operando na faixa de freqüência rádio de 2.407 a 2.447 GHz na banda ISM (Industrial, Scientific, and Medical), que resulta em uma largura de banda de 40 MHz, e quanto maior a largura de banda mais dados podem ser transmitidos. Na camada física e na camada de dados, o *WirelessHart* utiliza protocolo IEEE 802.15.4 com técnica de transmissão DSSS (*Direct Sequence Spread Spectrum*) e salto de canais (*channel hopping*) para garantir comunicação segura e confiável, além do controle de latência de transmissão entre os dispositivos. Como método de acesso, a rede utiliza o *TDMA* (*Time Division Multiple Access*) para coordenar a comunicação entre os dispositivos da rede. A camada *TDMA Data-Link Layer* estabelece enlaces especificando o tempo de slot (*timeslot*) e a freqüência a ser usada entre os dispositivos. Esses links são organizados em superquadros (*superframe*) que periodicamente são repetidos para suportar tráfego de comunicação cíclico e acíclico. O enlace pode ser dedicado, para garantir uma latência mínima de um dado de processo, ou pode ser compartilhado, para permitir uma ampla utilização da largura de banda da rede. O protocolo suporta múltiplos tipos de mensagens como publicação de dados de processo, notificação por exceção, requisição/resposta ad-hoc e fragmentação automática de grandes pacotes de dados. A segurança da comunicação utiliza o

esquema de encriptação AES-128 com chaves individuais: *Join Key*, *Session Key* e *Data-Link Network Key*. Estas chaves são usadas para autenticação de dispositivos e criptografia dos dados. Todas as mensagens possuem prioridade definida, assegurando qualidade de serviço (*QoS*) na entrega de pacotes, e as mensagens com alta prioridade e comunicações periódicas utilizam largura de banda dedicada (HCF_LIT-89, HART Communication Foundation, 2011).

1.8.1 Arquitetura

Cada dispositivo na topologia em malha (*mesh*) da rede pode servir como um roteador para as mensagens de outro dispositivo, o que determina que um dispositivo não precise se comunicar diretamente com *gateway*, mas precisa de um dispositivo próximo para repassar sua mensagem. Esse extenso alcance da rede permite rotas redundantes de comunicação, aumentando a sua confiabilidade. A arquitetura da rede *WirelessHart* suporta uma grande variedades de dispositivos de vários fabricantes. Os tipos de dispositivos e outros elementos associados à arquitetura *WirelessHart* são descritos a seguir (IEC/PAS 62591, *Industrial communication networks – Fieldbus specifications – WirelessHART™*):

Dispositivos de campo: Os dispositivos de campo (*Field Devices*) são conectados diretamente ao processo, sendo responsáveis pelas medições de valores de variáveis de campo. Ele é um produtor/consumidor de pacotes de dados, além de ter a capacidade de retransmitir mensagens recebidas vindas de outros dispositivos da rede. Cada dispositivo de campo possuem um identificador único que o diferencia na rede e mantém uma lista de dispositivos vizinhos com as respectivas identificações durante a operação da rede.

Adaptadores: Os dispositivos adaptadores tem a função de fornecer conectividade física e lógica para um dispositivo que não seja *WirelessHart*, e que queira fazer parte da rede sem fio. Ele possui as interfaces para conexão física e tabelas de rotas para coordenar o fluxo de informação entre um dispositivo com fio e a rede sem fio. Os adaptadores não possuem conexão direta com o processo de campo.

Gateway: O dispositivo Gateway tem a função de conectar a rede sem fio com a rede de automação da planta, fornecendo acesso das aplicações *host*, tais como Sistemas de Automação de Processo ou Sistemas de Gerenciamento de Ativos, aos dispositivos das redes sem fio. Os

dados coletados dos dispositivos da rede pelo *Gateway* são disponibilizados para automação da planta através de protocolos e interfaces, isso incluiu: (i) Dados e eventos relacionados ao processo por rotinas de comunicação cíclicas e periódicas, (ii) Status ou eventos resultantes de manutenção de dispositivos de campo ou falhas de condições anormais de processo. Estas mensagens ocorrem esporadicamente, mas devem ser imediatamente publicadas; (iii) Configuração, manutenção e diagnósticos relacionados a comunicação geralmente ocorrem em rajadas e em curtos intervalos de tempo. Um *Gateway* requer pelo menos um ponto de acesso para se conectar com a rede sem fio, mas pode suportar mais de um ponto de acesso. Estes múltiplos pontos de acesso têm seus próprios endereços físicos e são usados com objetivo de melhorar a vazão e a confiabilidade da rede sem fio.

Dispositivo *Handheld*: O dispositivo *Handheld* é um computador portátil que contem uma aplicação *Host.* Ele é utilizado na configuração de dispositivos, na execução de funções de diagnóstico, na execução de calibrações de dispositivos e no gerenciamento de informações de rede através de cada dispositivo. Ele é um dispositivo que não deve permanecer conectado diretamente na rede por, se tratar de um equipamento portátil. Ele requer a necessidade de operação de uma pessoa para utilizá-lo. O dispositivo *Handheld* se conecta a rede sem fio como se fosse um dispositivo de campo, porém não necessita de suporte de roteamento. Quando utilizado em bancada de laboratório, ele pode se conectar diretamente aos dispositivos de campo *WirelessHart*.

Network Manager: Este dispositivo não se conecta diretamente à rede sem fio, ele faz parte de uma funcionalidade lógica do *Gateway*. O *Network Manager* é uma aplicação que gerencia a rede *WirelessHart*, e é responsável pela configuração da rede, pelo sincronismo entre os dispositivos, pelo gerenciamento das tabelas de rotas e pelo monitoramento do estado dos dispositivos. O Network Manager coleta informações de desempenho e diagnóstico da rede para análise do seu funcionamento e realiza possíveis reconfigurações para correções de problemas.

Security Manager: Esta também é uma funcionalidade do *Gateway*, e é responsável pela geração, armazenamento, gerenciamento e distribuição das chaves *Join Key, Session Key* e *Data-Link Network Key*, que são utilizadas na autenticação de dispositivos que entram na rede e na criptografia de dados que trafegam pela rede sem fio. A segurança da comunicação utiliza o esquema de criptografia AES-128. Existe um componente *Security Manager* associado para cada rede *WirelessHart*. Ele pode ser uma função centralizada em algumas redes de automação,

prestando serviço a mais de uma rede *WirelessHart*. A figura 8 apresenta uma arquitetura da rede WirelessHart com os seus componentes típicos.

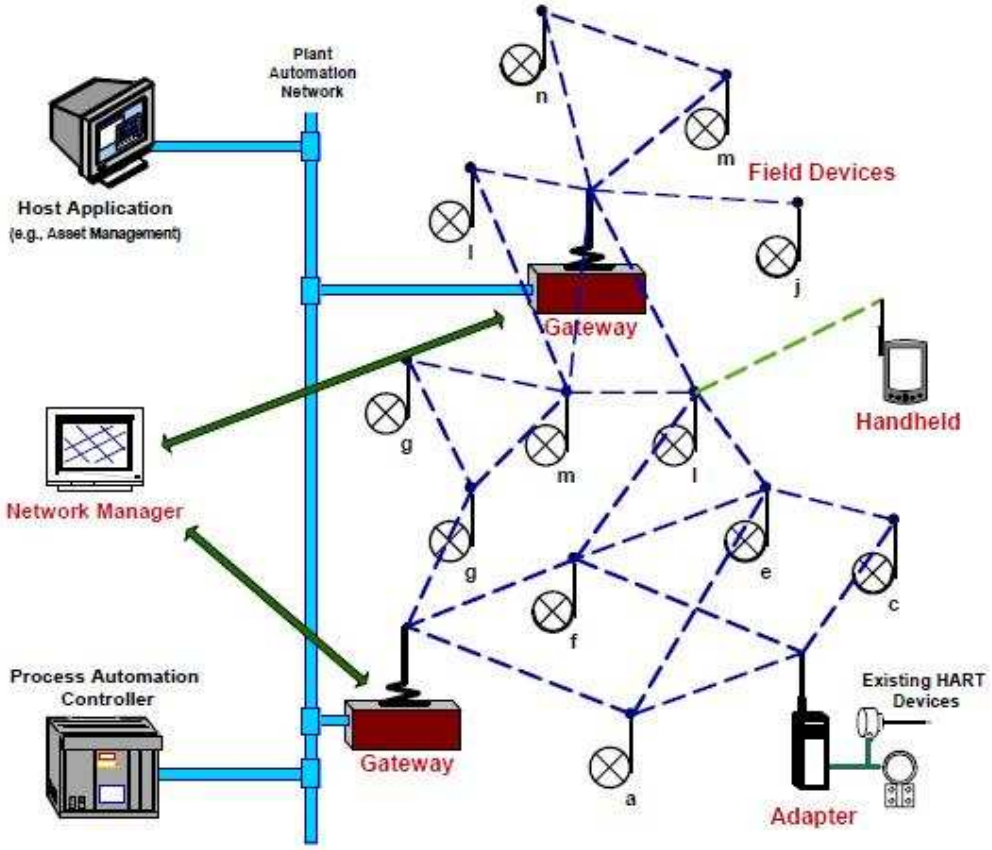

Figura 8 – Componentes típicos rede (Technical Data Sheet, HART Communication Foundation, 2007)

1.8.2 Transferência de dados

Dados de processo e *set-points* podem ser publicados periodicamente na rede quando houver mudança significativa dos seus valores ou se um valor ultrapassou um limiar crítico de operação (*threshold*). Mensagens de notificação são geradas automaticamente para as aplicações quando os dados ou os estados de processo são alterados. Tráfego de requisição/resposta Ad-hoc são suportados para rotinas de manutenção, configuração e calibração. A segmentação automática durante a transferência de grandes blocos de dados também são suportados pelo protocolo. A topologia em malha do *WirelessHart* possui duas importantes características: auto-organização (*self-organizing*) e auto-reparo (*self-healing*). Estas características permitem manter a preservação da rede por um longo período de tempo, com confiabilidade e robustez e sem

necessidade de intervenção do usuário. Quando interferências ou outros obstáculos interrompem um determinado caminho de comunicação, a rede imediatamente redefine o roteamento da transmissão perdida, de forma automática, evitando a perda de dados (Technical Data Sheet, HART Communication Foundation, 2007).

1.8.3 Segurança

O *WirelessHart* utiliza o esquema de criptografia AES-128 bits para realizar a segurança de comunicação de seção fim a fim entre os dispositivos da rede. Na seção, as mensagens são cifradas e somente o destinatário final pode decifrá-la. A segurança da rede pode ser dividida em duas categorias principais: (i) *Data Protection*, trata da privacidade e integridade das informações que trafegam na rede. Ele previne que dispositivos não autorizados capturem dados que trafegam pela rede. Existe uma chave individual de seção e uma chave comum da rede para todos os dispositivos em mensagens *broadcast*. Uma chave separada *Join Key* é utilizada para autenticação do dispositivo no processo de adesão do dispositivo à rede, e pode ser única para cada dispositivo ou ser uma chave comum para toda rede dependendo da política de segurança adotada. A integridade dos dados transmitidos é realizada pela adição do campo de integridade criptografado para cada pacote, e que é verificado pelo dispositivo de destino para validação da mensagem; (ii) *Network Protection*, é responsável pela manutenção da rede contra ataques internos ou externos que possam danificar o seu funcionamento, usando técnicas de autenticação, autorização e detecção de ataques. O Gateway possui um processo de autenticação que é utilizado para negociação da entrada de dispositivos legítimos na rede. Os ataques podem interferir na transmissão de rádio ou na sobrecarga de pacotes da rede. Os dispositivos *WirelessHart* podem reportar condições de anomalias que possam ser identificadas como possíveis ataques, tais como, retransmissões, falhas de acesso, falhas em cheques de integridades de mensagens, falhas de autenticação, etc. (HCF_LIT-114, HART Communication Foundation, 2010).

1.8.4 Redundância

A necessidade de utilização de sistemas redundantes em plantas industriais reduz a probabilidade de perda de dados importantes para operação do processo, especialmente onde há dados críticos ou onde a falha em algum componente possa causar danos ou perdas no processo. No *WirelessHart*, a redundância pode ser aplicada nos seguintes níveis da rede: (i) Redundância nos dispositivos sensores, através de mecanismos de múltiplos caminhos entre os dispositivos de campo e o *gateway* ou através de múltiplos canais de freqüência de rádio; (ii) Redundância nos pontos de acesso, disponibilizam uma maior largura de banda e caminhos redundantes para *o gateway* e *network manager*; (iii) Redundância de *gateway, network manager* e *security manager,* (LIT-128, HART Communication Foundation, 2009).

1.8.5 Camada física *(Physical Link Layer*)

A rede *WirelessHART* utiliza Radio Frequência (RF) para comunicação entre dispositivos com até 100 metros de distância, em visada direta, quando transmitido a 0 db. A camada física é responsável pelo método de sinalização, sinal transmitido, sensibilidade dos dispositivos e codificação binária do sinal. A camada física é baseada no protocolo IEEE STD 802.15.4, e possui algumas características a seguir (Technical Data Sheet, HART Communication Foundation, 2007):

Tabela 3 - Características Physical Link Layer

Padrão (MAC + PHY)	IEEE 802.15.4
Freqüência de operação	2400-2483.5 MHz
Modulação	O-QPSK
Taxa de transferência	250 KBPS (62.5 KBAUD)
Técnica de transmissão	DSSS (*Direct Sequence Spread Spectrum)*
Potência de transmissão	10dBm (Nominal) ajustável
Camada física IEEE	Compatível com PDU
Payload (carga útil)	127 bytes

1.8.6 Camada Data-Link (*Data-Link Layer*)

A camada Data-Link é responsável pela segurança, confiabilidade e comunicação livre de erros entre os dispositivos da rede. Possui compatibilidade com IEEE 802.15.4 MAC PDU, onde a comunicação é coordenada com TDMA (*Time Division Multiple Access*) que ocorre em slots de tempo (*timeslot*) e canais de freqüência determinados para todas as mensagens. O reconhecimento de pacotes inclui informações de temporização para sincronização das operações TDMA de toda rede. Os *timeslots* são organizados em *superframes* (100 *timeslots*/seg) que permitem diferentes tipos de tráfego de rede (rápido, lento, cíclico e acíclico). Para evitar interferências, perturbações e colisões com outros sistemas de comunicação, o *WirelessHart* também utiliza o FHSS (*Frequency Hopping Spread Spectrum*), usando os 15 canais definidos no IEEE 802.15.4 em paralelo, para saltar através desses canais. Os enlaces podem ser dedicados (um por cada dispositivo fonte) ou podem ser compartilhados entre múltiplos dispositivos através de contenção de acesso e utilizam *superframe, timeslot and channel offset* para habilitar a comunicação entre dispositivos vizinhos. Possui suporte para priorização de mensagens para controle de vazão e gerenciamento de latência (Technical Data Sheet, HART Communication Foundation, 2007).

1.8.7 Camada de rede (*Network Layer*)

A topologia da rede é em malha (*mesh*) onde todos os dispositivos são do tipo FFD *(full function device)* e suportam roteamento em benefício dos outros dispositivos da rede. Dessa forma, a rede é constituída por múltiplas rotas de comunicações redundantes, que são continuamente verificadas, para garantir confiabilidade e baixa latência. Tipicamente, a confiabilidade para um boa formação da rede *WirelessHART* é maior que 3σ *(3-sigma = 99.7300204%)* e normalmente maior que 6σ *(99.9999998%)* (Technical Data Sheet, HART Communication Foundation, 2007).

O roteamento é feito na origem para comunicações ad-hoc, com confirmação de viabilidade de uso desse caminho e com suporte à transmissão *broadcast, multi-cast e unicast*. Essa camada é responsável por realizar o gerenciamento dinâmico de largura de banda para alocação de *superframe* e enlaces. Como os dispositivos de campo são configuráveis, a largura de banda é requisitada ou liberada de acordo com a necessidade de comunicação, e os *slots* são

alocados para disponibilizar banda básica e banda flexível para comunicação. Possui os seguintes tipos de rotas: (i) *Graph routing*, caminho unidirecional que conecta os dispositivos com registro do próximo salto; (ii) *Source Routing*, caminho fixo com determinação de cada salto; (iii) Superframerouting, roteamento específico do GraphRouting onde é indicado o superframe a ser utilizado.

A camada de transporte fornece uma comunicação fim a fim com reconhecimento de mensagens. Transmissões com reconhecimento incluem tentativas de retransmissões automáticas (*retries*) para garantir o sucesso da transferência de dados. Os conjuntos de dados são automaticamente fragmentados no dispositivo de origem e remontados no destino.

O desempenho da rede é permanentemente monitorado, onde cada dispositivo mantém estatísticas de comunicação com seus vizinhos, como por exemplo, nível de sinal recebido, contagem de pacotes, etc. Também são monitoradas as listas atualizadas com novos vizinhos encontrados na rede e os dispositivos que foram desconectados a ela. Além disso, o gerenciador de rede (*Network Manager*) é responsável por inserir caminhos redundantes de comunicação e reduzir o consumo de potência.

2 POSICIONAMENTO DE NÓS EM REDES SEM FIO

Em desenvolvimentos de projetos de redes sem fio, um dos principais fatores de preocupação é o posicionamento dos nós sensores na rede. As estratégias de posicionamento de sensores são variadas e devem ser feitas de forma planejada e de acordo com o tipo de aplicação a que se destinam. De forma geral, um bom posicionamento dos nós sensores deverá garantir a cobertura total da rede, menores latências de transmissão, facilidade de manutenção e alta disponibilidade com rotas alternativas.

2.1. Descrição do problema de posicionamento de nós

Cada vez mais os sensores possuem características que são importantes nessa difícil tarefa de posicionamento, como por exemplo, ter baixo custo, ter baixo consumo de energia, ter capacidade de adquirir/processar as informações, ser autônomos quanto à manutenção, poder operar em grandes densidades, ser adaptativo ao ambiente e ter capacidade de comunicação com outros sensores vizinhos. Os nós sensores geralmente são organizados em clusters, com objetivo de detectar o evento na região de interesse, processar o dado e decidir se deve ou não propagar os resultados para outros nós.

Na maioria das redes de sensores sem fio se tem um grande número de sensores posicionados densamente na região de interesse, seja para aplicações militares, monitoramento ambiental, monitoramento de tráfego, e outros. Em algumas aplicações, como por exemplo, em monitoramento ambiental, pode-se não ter acesso à área de monitoramento dos sensores, dificultando o seu posicionamento e manutenção, o que faz com que os mesmos sejam posicionados aleatoriamente e descartados após utilização da sua vida útil. Portanto, a rede deve estar preparada para ter mobilidade e ser reconfigurável na presença de novos sensores, e seus protocolos e algoritmos devem possuir capacidade de auto-organização. Outra característica interessante é que na rede de sensores existe o esforço cooperativo, onde sensores processam dados localmente e os enviam para os nós responsáveis pela fusão de dados, o que faz com que toda a rede tenha melhor desempenho, robustez e precisão, pois não depende apenas de um único sensor. Além disso, há melhor eficiência no consumo de energia pela redução da quantidade de dados e mensagens.

A topologia de rede de sensores pode chegar à densidade de 20 nós/m^3, onde o posicionamento dos sensores pode ser feitos por um avião, jogando os sensores ou colocados por pessoas ou robôs. A topologia variará de acordo com a posição, alcance, energia disponível, mau funcionamento e objetivo das tarefas. A manutenção da topologia inclui a colocação de novos nós em substituição aos nós não operantes e da dinâmica das tarefas.

2.2. Soluções encontradas sobre o problema

O estudo de problemas relacionados ao posicionamento de nós em redes sem fio tem recebido bastante atenção e podendo também ser encontrado em redes de sensores (Molina et al, 2008), (Youssef &Mohamed, 2007), em redes de computadores Wi-Fi (Wang et. al, 2007), (Muthaiah & Rosenberg ,2008) e no planejamento de infraestrutura para telefonia celular (Whitaker et al.,2004).

Em Molina et al (2008), trata-se o problema de modo a encontrar o melhor layout para uma rede de sensores, isto é, encontrar o menor número de nós e seu respectivo posicionamento. A estratégia de posicionamento é vista como um problema de otimização onde os parâmetros são as coordenadas dos nós sensores e dois objetivos são otimizados, a saber: a energia consumida nas comunicações e o número de sensores colocados. A cobertura obtida pela rede é vista como uma restrição.

Em Youssef & Mohamed (2007), são propostos dois algoritmos baseados em Algoritmos Genéticos para resolver o problema de se colocar um número fixo de gateways que servirão como nós coletores de informação em uma rede de sensores sem fio. O posicionamento dos gateways é feito com o objetivo de minimizar a latência, que é medida através do cálculo do atraso médio por pacote de informação recebido.

Em Wang et al, 2007, estudam o problema de posicionar roteadores para uma rede sem fio (Wi-Fi) de modo a atingir a vazão de dados desejada. Neste artigo, se determina o número de roteadores que devem ser colocados e o seu posicionamento é escolhido a partir de um conjunto de posições predeterminadas.

Em Muthaiah & Rosenberg (2008), trata-se do problema de posicionar apenas o gateway para a Internet em uma rede sem fio. Através de heurísticas, procura-se determinar a melhor posição para o gateway entre (N+1) posições pré-especificadas, sendo que as N posições remanescentes são preenchidas pelos nós. Neste trabalho, utiliza-se um modelo bem definido para a camada física que leva em conta a interferência gerada por ruídos.

Em Whitaker at al (2004), um algoritmo de otimização multiobjetivo é proposto para garantir a cobertura de uma rede de telefonia celular em uma determinada área usando o menor número de estações. A cobertura e o menor número de estações são objetivos conflitantes que são otimizados.

Os artigos relacionados demonstram a importância do posicionamento de nós em uma rede sem fio e suas variações. Todos eles mencionam que o problema de posicionamento é um problema *NP-Hard* e por isso é comum o uso de heurísticas e de métodos de otimização estocástica como os algoritmos genéticos. Embora o trabalho aqui apresentado possua diversas semelhanças com os artigos relacionados, como por exemplo, tratar o problema de posicionamento como um problema de otimização, existem algumas diferenças, dentre elas pode-se citar: (i) Quanto à latência, as mensagens carregam informações de processo que podem ter uma importância tal que não suportem um atraso máximo de entrega, e neste caso, a rede sem fio deve ser determinística; (ii) Quanto à tolerância a falhas, conforme as características de processo, a aplicação pode não suportar perdas de mensagens e aguardar uma possível retransmissão por ocorrência de um evento importante; (iii) Quanto ao sensores, têm uma importância crucial tanto na medição de dados de processo quanto na função de roteamento, o que os tornam não descartáveis; (iv) Ainda quanto aos sensores, os mesmos são caros e possuem funções de medição distintas e na maioria das vezes não redundantes. Normalmente, são usados com dupla função para medição e roteamento de mensagens e a escalabilidade de nós está na ordem de dezenas, podendo em alguns casos chegar à ordem de centenas; (v) A rede sem fio deve possuir cobertura total e sem oscilações, devido à importância da aplicação industrial. Todos estes aspectos citados se diferenciam quando comparados à telefonia móvel ou à internet.

2.3. O problema de posicionamento de nós em redes de automação

O que se espera de transmissão de sinais sem fio em um sistema de controle industrial? Que ele seja tão robusto quanto um sinal que seja transmitido através de cabeamento, que ele tenha baixos atrasos na transmissão da informação (menor que 5ms), que ele tenha comportamento determinístico, que a configuração da comunicação seja automática, que qualquer interrupção na comunicação seja detectada rapidamente para que não se tenha perda de dados, que a rede tenha capacidade para suportar alta densidade de dispositivos de comunicação e que os mesmos sejam independentes entre si, que o custo seja atrativo, que tenha segurança no tráfego das informações e seja livre de acessos indevidos e que tenha fácil manuseio. Todas essas características servem para resumir que uma solução de comunicação sem fio será tão boa quanto mais ela for compatível, por estes aspectos, com uma solução cabeada. Dentre os fatores enunciados anteriormente, quase todos (se não todos), tem correlação com posicionamentos de nós da rede. Posicionar de forma correta os nós tem impactos diretos em vários aspectos da rede e no sucesso da aplicação. Nos ambientes industriais, realizar o posicionamento dos nós normalmente não é uma tarefa fácil, considerando todos os obstáculos e interferências existentes nesses cenários. Na maioria dos casos, os pontos de medição de processo onde são instalados os transmissores são também os locais onde ficarão posicionados os dispositivos de transmissão de rede sem fio. Nesses casos, não há flexibilidade para escolha do local mais apropriado para posicionar os nós, então, parte da rede já se torna estabelecida. Então, levando em consideração esse aspecto, o desafio é tornar a rede totalmente conectada, e da forma mais eficiente possível, seja em relação à quantidade de roteadores adicionais, à confiabilidade, à latência, à tolerância a falhas, à disponibilidade e a outros fatores que estão relacionados a uma comunicação sem fio. Como adicionar roteadores à rede para torná-la totalmente conectada? Quantos desses roteadores adicionais serão suficientes? Como saber a posição adequada para garantir os melhores resultados? Essas são algumas perguntas que são feitas em qualquer instalação de rede sem fio em ambientes industriais. Sem o auxílio de um mecanismo, essas questões são mais difíceis de serem equacionadas. Essas dificuldades motivaram a elaboração dessa ferramenta para auxiliar o usuário da rede a posicionar de forma mais adequada esses roteadores adicionais.

Existem semelhantes e diferenças entre a as redes de sensores tradicionais e as redes de automação sem fio. A tabela 4 abaixo demonstra os principais aspectos quanto a esses pontos.

Tabela 4 – Semelhanças x Diferenças

	Redes de Sensores	***Redes de Automação s/ fio***
Quantidade de Sensores	Na ordem de dezenas, milhares ou milhões	Na ordem de dezenas
Densidade	Nós sensores são colocados densamente	Densidade é bem menor
Tolerância a Falhas	Maior tolerância	Menor tolerância
Topologia dos sensores	Pode variar freqüentemente	Não variam
Topologia da rede	Mobilidade (Aleatória)	Fixa (*mesh*)
Tipo de comunicação	Por difusão	Por difusão
Nós sensores em termos de energia, capacidade computacional e memória	São mais limitados	São mais eficientes
Função colaborativa (Roteamento)	Sim	Sim
Robustez dos sensores	Menos robustos	Mais robustos
Custo dos sensores	Mais baratos	Mais caros
Confiabilidade da rede	Importante	Imprescindível
Latência	Pode ser tolerável	Fator fundamental
Manutenção da rede	Menos acessível	Totalmente acessível
Grau de criticidade	Menor	Maior
Posicionamento do nós	De forma densa e aleatória	De forma calculada e precisa

3 POSICIONAMENTO VISTO COMO UM PROBLEMA DE OTIMIZAÇÃO

Realizar o posicionamento de sensores em redes sem fio não é uma tarefa simples, tendo em vista os diversos aspectos envolvidos com cada aplicação. Embora aspectos como a cobertura de rede sejam mandatórios em qualquer projeto, cada aplicação tem suas particularidades que podem demandar definições específicas com relação ao posicionamento dos nós. Seja qual for a demanda exigida, a estratégia de posicionamento dos sensores estará relacionada a diferentes critérios que pode ser visto como um problema de otimização. Esta ferramenta propõe um método para auxiliar o usuário a encontrar as melhores configurações para a sua rede, onde os parâmetros de entrada são o número de nós roteadores adicionais e as suas coordenadas e a função de custo leva em conta diferentes critérios que serão descritos nos tópicos a seguir.

3.1. Técnica de otimização utilizada

A técnica de otimização utilizada no desenvolvimento do trabalho são os Algoritmos Genéticos (AGs). Os AGs constituem uma técnica de busca e otimização, altamente paralela, inspirada nos mecanismos de evolução natural e recombinação genética (Davis, 1990). O princípio Darwiniano da seleção natural diz que indivíduos que possuem características favoráveis a se adaptar a um determinado ambiente, têm maiores chances de sobreviver e reproduzir-se do que aqueles com características menos favoráveis. Se estas características favoráveis estiverem associadas aos códigos genéticos dos indivíduos (que são armazenados nos cromossomos), então, estes códigos se tornarão cada vez mais comuns nas gerações seguintes da população, enquanto que aqueles que forem desfavoráveis se tornarão cada vez mais raros. Usando os aspectos fundamentais destes princípios como inspiração, é possível construir algoritmos computacionais iterativos em que uma população de representações abstratas de possíveis soluções evolui na busca de melhores soluções para um determinado problema. O fluxograma da Figura 9 mostra o procedimento básico de otimização por AGs. A evolução ocorre durante um determinado número de ciclos, que são chamados de gerações, e geralmente é iniciada a partir de um conjunto de soluções criado aleatoriamente (população inicial). A cada geração, avalia-se o grau de adaptação (grau de aptidão) de cada indivíduo da população em relação ao problema, classificando cada indivíduo segundo o seu grau de adaptação. A seguir, de acordo com a estratégia de seleção adotada, escolhem-se os indivíduos mais aptos. Então, serão aplicados sobre os escolhidos os operadores genéticos de cruzamento (*crossover*) e mutação para

obter uma nova população. Este procedimento é realizado até que o critério de parada seja alcançado. Segundo Michalewick (1994), os algoritmos genéticos devem ser caracterizados através dos seguintes componentes: Uma representação genética para as possíveis soluções do problema; uma forma de criar a população inicial; uma função de avaliação que desempenha o papel do ambiente, classificando soluções de acordo com sua aptidão; operadores genéticos que modificam a composição dos descendentes (seleção, *crossover* e mutação), e valores para os vários parâmetros que o algoritmo genético utiliza (tamanho da população, probabilidades de aplicação dos operadores genéticos, etc.).

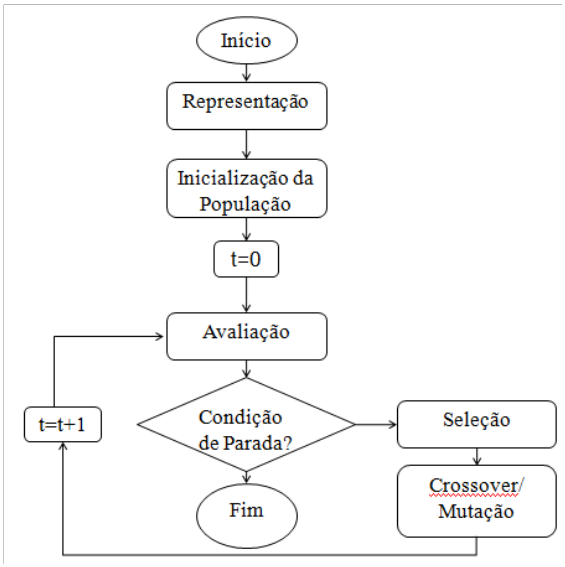

Figura 9 - Fluxograma de um Algoritmo Genético

3.2. Modelagem do problema

Primeiramente, uma vez se tratando de um ambiente industrial, os nós que fazem parte da rede estão posicionados nos locais onde o processo determina que devam ser instrumentados para realizarem as devidas medições a que se destinam e que, sendo assim, a conectividade destes dispositivos sensores com o nó central (gateway) localizado, em geral, na sala de controle é absolutamente necessária para um adequado funcionamento da rede sem fio e da operacionalidade da unidade industrial. Esta situação se configura de forma diferente de uma rede sem fio para acesso a internet, onde é admissível a perda de conectividade e posterior retomada sem grandes prejuízos para o usuário, pelo fato que o interesse maior da rede está em

se obter uma alta vazão de dados. Em seguida, neste trabalho, se apresenta uma estratégia própria para aplicações de rede sem fio em instalações industriais, levando em conta os obstáculos reais e presentes nestes ambientes, onde normalmente, outros artigos tratam de forma diferente, considerando o cenário em que a rede está presente como um local aberto. Por último, essa ferramenta disponibiliza para o usuário um conjunto de critérios que pode ser selecionado de acordo com as necessidades da aplicação, para realização do posicionamento adequado dos nós adicionais. Outros artigos relacionados a este tema, em geral, utilizam poucos ou apenas um critério para realizar desta tarefa de posicionamento, como por exemplo, a vazão de dados. Como será apresentado adiante, para aplicações destinadas a rede sem fio em ambientes industriais, existe um conjunto de critérios que devem ser trabalhados em conjunto e que influenciam diretamente no comportamento da rede.

Esta seção descreve o método utilizado pela ferramenta para auxiliar o usuário a encontrar as melhores configurações para a sua rede. Conforme foi dito anteriormente, este problema é visto como um problema de otimização,onde se deseja:

- Minimização do número de nós roteadores a serem adicionados com as respectivas coordenadas
- Minimização de retransmissões por cada dispositivo
- Minimização do maior número de *hops* permitido para mensagens
- Maximização do número de nós vizinhos por dispositivos
- Maximização do número de conexão direta com gateway
- Maximização da tolerância de falha da rede a perda de um nó

O número máximo de nós roteadores a serem adicionados na rede tem como objetivo encontrar a menor quantidade de nós excedentes que um usuário deverá colocar na sua rede, garantindo que todos os nós estarão conectados para formação da cobertura total da rede, que é o principal objetivo de qualquer aplicação desse gênero, reduzindo também os custos relacionados a roteadores adicionais desnecessários que viessem a ser adicionados sem o uso da ferramenta. Essa quantidade inicial de dispositivos é posicionada dentro da área de cobertura onde se pretende instalar a rede. As coordenadas desses nós roteadores a serem adicionados também são calculadas pelo algoritmo, que informa os valores das coordenadas X e Y no plano cartesiano e

também informa a coordenada Z na necessidade de se posicionar os roteadores quanto a sua altura do chão.

A minimização do número de retransmissões de cada dispositivo tem o objetivo de reduzir o número de mensagens que um único dispositivo pode efetuar. Quanto maior o número de mensagens que passam por um dispositivo para retransmissão de pacotes por força da função de roteamento em uma rede em malha, mais crítico será este dispositivo na rede. Ao minimizar o número de mensagens por dispositivos, menor será a quantidade de caminhos passando por ele, e consequentemente menos crítico será este dispositivo, evitando situações de congestionamento e pontos críticos de falhas. À medida que as mensagens retransmitidas sejam distribuídas o mais uniformemente possível entre outros nós roteadores da rede, maior será a existência de caminhos alternativos, contribuindo para aumentar a confiabilidade da rede e a redução de latência de transmissão.

A minimização do número máximo de *hops* (saltos) permitido para as mensagens visa limitar a quantidade de retransmissões feitas pelos dispositivos intermediários durante o encaminhamento fim a fim do pacote, assegurando com isso uma baixa latência de transmissão, tendo em vista que em cada tempo de transmissão fim a fim são adicionados os tempos de processamento dos nós intermediários. Logo, quanto mais *hops* existirem em um determinado caminho, maior será a latência de transmissão. O objetivo de se ter a menor quantidade de saltos (*hops*) das mensagens é buscar a otimização do caminho mais curto para as mensagens em termos de retransmissões. Com dito anteriormente, quanto maior for a quantidade de *hops* de uma mensagem em um determinado caminho, maior será sua latência de transmissão, considerando que o tempo gasto em retransmissões são bem relevantes. O *WirelessHart* utiliza como método de acesso o TDMA (*Time Division Multiple Access*) com *slots* de tempo de 10ms, o que faz com que cada dispositivo saiba exatamente quando tem que transmitir ou receber mensagens. Cada mensagem no *WirelessHART* leva aproximadamente 4ms para transferir 250kbit/s (considerando que o *baudrate* é fixo no *WirelessHART*). Essa retransmissão precisa ser feita dentro dos 10ms do *time slot*, e ainda assim sobrará um tempo para processamento de hardware. Dessa forma, considerando uma latência de 10ms por *hop*, pode-se tem uma boa estimativa do que acontece na rede em termos de tempo de transmissão quando se acrescenta cada *hop*. Além disso, do ponto de vista de confiabilidade, quanto mais nós intermediários estiverem entre o dispositivo de origem e o de destino, maiores são as chances de perda de dados causados por falhas nos dispositivos ou interferências, fazendo com que as mensagens não cheguem aos seus destinos finais. A retransmissão também afeta a vida útil da bateria dos nós

intermediários, pois os nós passam a permanecerem mais tempo ativos realizando o processamento de retransmissão, comparados aos nós que simplesmente publicam seus dados de processo e ficam mais tempo hibernando. Embora existam aspectos negativos relacionados à retransmissão, ela é um recurso fundamental para a conectividade e auto-organização da rede, pois é através de retransmissão que se alcançam os nós mais distantes sem visada direta e que também possibilitam a reorganização através de novos caminhos em caso que falhas em dispositivos intermediários

Maximizar um número mínimo de dispositivos vizinhos por cada nó tem o objetivo de garantir caminhos alternativos para as mensagens que utilizam múltiplos saltos entre dispositivos origem e destino. Uma configuração ideal teria uma rede totalmente conectada, com cada dispositivo contendo no mínimo três vizinhos, segundo a recomendação da HART *Foundation*, Pois esta situação estabelece redundância de caminhos para todos os pacotes e aumenta a confiabilidade da rede em caso de perdas de dispositivos. Entretanto, nem sempre é possível obedecer esta recomendação, devido aos custos envolvidos. A otimização deste objetivo verifica a quantidade de vizinhos existentes para cada nó e, procura maximizar o menor número de vizinhos existentes, adicionando outros nós roteadores de forma apropriada.

O número máximo de conexões diretas com gateway é uma recomendação da organização HART *Foundation* para garantir caminhos alternativos para todos os dispositivos da rede. Trata-se de uma boa prática que, segundo estudos, com o mínimo de três nós conectados diretamente com o gateway a rede chega a um grau de confiabilidade de 99%, que é o mesmo índice de uma solução cabeada. Sendo o gateway o dispositivo central de controle da rede por onde todas as mensagens são encaminhadas, torna-se claro que quanto mais caminhos existirem, mais confiável e versátil será a rede.

Maximização da tolerância de falha da rede a perda de um nó tem por objetivo minimizar os nós potencialmente críticos que compõe a rede. Um dispositivo é considerado crítico quando, se por alguma razão, for retirado da rede, ele causar a interrupção de comunicação de outros nós com o gateway. Quanto maior for a quantidade de nós que dependerem do nó crítico, maior será a queda de desempenho da rede. Para cada solução proposta de configuração de rede, essa função retira um dispositivo de cada vez, simulando a perda deste nó, e verifica o quanto do restante da rede ainda está funcionando, isto é, quantos nós ainda conseguem se comunicar com o *gateway*. Para cada nó, a função retorna um índice de tolerância a falha, que varia entre 0 e 1,

que é atribuído ao nó que foi retirado, e que representa a porcentagem da rede que ainda funciona. Quanto menor o índice, menos tolerante a falha do nó será a rede. Após calcular este índice para todos, os nós, o GA vai procurar maximizar o menor índice de tolerância encontrado, com o intuito de obter uma rede mais confiável. Esta função apresenta um custo computacional alto que aumenta com o número de nós presentes na rede.

O algoritmo também permite que o usuário estabeleça algumas restrições. Neste caso, o programa irá procurar soluções onde as restrições sejam satisfeitas. As restrições estão relacionadas a seguir:

- Garantir a total conectividade de todos os dispositivos da rede
- Garantir uma quantidade mínima de nós vizinhos para cada dispositivo
- Garantir a existência de uma quantidade mínima de dispositivos conectados diretamente ao nó central (*gateway*)
- Garantir uma limitação para o número máximo de *hops* por dispositivo
- Garantir uma quantidade máxima de mensagens retransmitidas por dispositivos

Garantir a cobertura total da rede torna-se uma necessidade para qualquer aplicação, e para cumprir esta restrição o algoritmo aplica uma penalidade de acordo com o percentual de nós não alcançados pelo programa, a relação estabelece que quanto maior for o percentual maior será a penalidade.

Como dito anteriormente, a quantidade mínima de nós vizinhos se faz necessária para garantir caminhos alternativos para as mensagens, premissa fundamental para aumentar a confiabilidade e a disponibilidade da rede. Neste caso, o programa analisa todos os nós da rede de uma determinada solução e aplica penalidades nos casos em que cada nó apresentar uma quantidade menor de vizinhos do que a estabelecida pelo parâmetro definido para esta restrição.

A existência de uma quantidade mínima de dispositivos conectados diretamente ao *gateway* tem o intuito de garantir caminhos alternativos para as mensagens trafegarem por todos os nós da rede. A recomendação da HART *Foundation* é de que se tenha no mínimo 5 dispositivos conectados diretamente ao gateway de modo a aumentar a confiabilidade e a disponibilidade da rede, embora este valor seja um parâmetro de entrada do programa que pode ser definido de acordo com a necessidade da aplicação. O algoritmo está preparado para aplicar penalidades quando não for atendido este limite de conexões com o *gateway*.

A restrição para estabelecer um limite para o número máximo de *hops* por dispositivo tem o propósito de garantir que uma penalidade seja aplicada e não permita que existam mais de N saltos para as mensagens, independente da função de otimização de *hops*. O valor de N é um parâmetro de entrada do programa que pode ser definido pelo usuário.

A restrição para garantir uma quantidade máxima de mensagens retransmitidas por dispositivos visa limitar que um dispositivo seja sobrecarregado com mensagens de retransmissão e se torne um ponto crítico de falhas ou de atrasos na rede. Esta restrição limita em um número N de caminhos que podem passar por um nó, independentemente da função objetivo do mesmo assunto. O valor de N é um parâmetro de entrada do programa que pode ser definido pelo usuário.

A principal diferença entre uma restrição e um objetivo é que, a primeira estabelece um valor definido que deve ser alcançado. Por exemplo, se for definido como restrição que o número máximo de *hops* deve ser igual a quatro, o programa irá procurar uma solução onde nenhum nó usasse mais do que quatro *hops* para se comunicar com o *gateway*.Uma vez que a restrição fosse atendida, o programa não procuraria mais diminuir o número de *hops*. Se a minimização do número de *hop*s fosse definida como um objetivo, o programa procuraria atender esse objetivo de melhor forma possível, mas sem definir um valor específico determinado.

3.2.1 Descrição da Representação (cromossomo)

A representação do cromossomo é dada pelas coordenadas dos *n* roteadores, que devem ser colocados para fazer com que a rede atenda as especificações determinadas pelo usuário. A Figura 10 mostra a representação do cromossomo. O número *n* de roteadores determina o número máximo de roteadores que o usuário aceita colocar na sua rede para que esta atenda as suas especificações. Uma vez que o toolbox utilizado para algoritmos genéticos no Matlab, GAOT (Houck, 1995) não admite a utilização de cromossomos de tamanho variável, foi utilizado um artifício para que se pudesse obter o número mínimo de roteadores (um número entre 0 e *n*). A figura 11a mostra uma região demarcada pelas coordenadas (0,0), (0,x2), (0,y2) e (x2,y2) e cuja a área é dada por (A1 + A2). Esta é a região na qual o AG pode posicionar os roteadores. Entretanto, somente serão utilizados na solução final os roteadores que estiverem dentro da região cuja área é A1, que é a região onde se encontra a instalação industrial de fato. Deste modo dependendo de onde o AG coloca os roteadores, eles são contabilizados ou não. Por exemplo, a figura 11b mostra a situação na qual o número máximo de roteadores é igual a 5, mas

apenas 3 são contabilizados (aqueles que estão na área A1). Para que não haja uma tendência para que o AG coloque os roteadores na área A1 ou na área A2, elas possuem o mesmo valor.

x_1	y_1	x_2	y_2	x_3	y_3	.....	x_n	y_n

Figura 10 Representação Utilizada

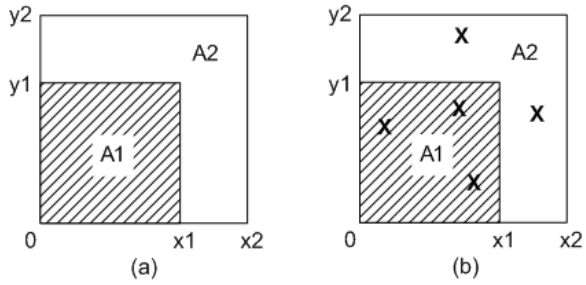

Figura11 Contabilização de Roteadores

3.2.2 Descrição da função de avaliação para o GA

A função de avaliação (F_{aval}), mostrada na equação 1 é composta por duas parcelas: a primeira corresponde a uma soma ponderada de diferentes funções a serem otimizadas (F_{spobj}) e a segunda corresponde às restrições ao qual o problema está sujeito (F_R).

$$F_{aval} = F_{spobj} - F_R \qquad (1)$$

Na primeira parcela, diferentes objetivos que se desejam alcançar são representados como funções individuais, para depois serem combinadas em uma única avaliação através de uma soma ponderada conforme visto na equação (2).

$$F_{spobj} = w_1 f_{obj1} + w_2 f_{obj2} + \cdots + w_m f_{objm} \qquad (2)$$

Dessa forma o usuário pode definir através dos pesos quais os objetivos são mais importantes. De acordo com a equação (2) se o usuário tivesse interesse apenas no objetivo 1, ele faria $w_1 = 1$ e todos os outros iguais a 0. Por outro lado, se ele considerasse todos os objetivos igualmente importantes, os valores dos pesos w_1, w_2, ..., w_n seria igual $1/m$. Esta forma de agregação para atender múltiplos objetivos necessita que todas as funções correspondentes aos objetivos individuais sejam normalizadas. As equações (3) e (4) mostram exemplos de funções objetivos individuais que podem ser utilizadas. A equação (3) mostra a função objetivo utilizada para minimizar o número de roteadores adicionais e a equação (4) mostra a função utilizada para minimizar o número máximo de hops. Uma vez que o pacote gaot admite apenas maximização, é importante observar que as funções objetivos individuais devem ser escritas de forma que, quando maior for o grau de atendimento do objetivo, maior será o seu valor. Por exemplo, a equação (3) representa o objetivo de minimizar o número de roteadores. Ela está escrita de tal forma que quanto menor for o número de roteadores adicionais, maior será o seu valor. Além disso, é importante que o valor de saída das funções objetivo individuais estejam normalizadas entre 0 e 1 para permitir a agregação de objetivos sem que haja uma preponderância de um objetivo sobre o outro. Se todas as funções objetivos estão normalizadas, então o usuário pode determinar quais serão as mais relevantes para a sua aplicação, atribuindo a elas pesos diferentes.

$$f_{obj1} = \frac{NumMaxRot - NumRotUsados}{NumMaxRot} \qquad (3)$$

$$f_{obj2} = \frac{1}{1 + NumMaxHops} \qquad (4)$$

A segunda parcela (F_R) e refere às penalidades impostas à função de avaliação. O objetivo de utilizar penalidades é fazer com que soluções que não atendam as restrições impostas pelo problema tenham uma avaliação menor, diminuindo a probabilidade de serem escolhidas para gerar novas soluções. O problema em questão pode estar sujeito a uma série de restrições que podem ser impostas de acordo com o desejo do usuário. Normalmente, são mais comuns as restrições que obrigam que a rede esteja totalmente conectada, isto é, que todo nó possa se comunicar com o nó central, e a restrição que limita o número de saltos (hops) usados para transmitir uma mensagem de um nó para outro. A função que calcula a penalidade é mostrada na

equação (5), e é formada pela soma de restrições individuais (p_1 a p_k). A equação (6) mostra o cálculo das restrições individuais que é feito seguindo dois critérios: o primeiro é que uma solução que não obedeça à restrição imposta deve ter uma avaliação pior do que uma solução que respeita a restrição e segundo; o valor da penalidade (p) deve ser proporcional ao grau de infração da restrição (u) (Molina et al, 2008).

Para que o cálculo da função de avaliação possa ser realizado, primeiro se obtém uma rede que é formada por nós e segmentos. Os nós são dados pelos pontos que o usuário deseja instrumentar e pelos roteadores adicionais, cujas coordenadas estão no cromossomo. Os segmentos indicarão se existe uma ligação entre dois nós, isto é, se existir um segmento entre o no *i* e o nó *j*, então será possível enviar uma mensagem de *i* para *j*.

$$F_R = p_1 + \ldots + p_k \qquad (5)$$

$$\begin{cases} (u == 0),\ p = 0, \\ (u > 0.001) \,\&\, (u <= 0.01),\ p = 2 * N \\ (u > 0.01) \,\&\, (u <= 0.1),\ p = 3 * N \\ (u > 0.1) \,\&\, (u <= 0.2),\ p = 4 * N \\ (u > 0.2) \,\&\, (u <= 0.4),\ p = 5 * N \\ (u > 0.4) \,\&\, (u <= 0.6),\ p = 6 * N \\ (u > 0.6) \,\&\, (u <= 0.8),\ p = 7 * N \\ (u > 0.8),\ p = 8 * N \end{cases} \qquad (6)$$

A existência de um segmento entre o nó *i* e o nó *j* é dada por: Os nós *i* e *j* devem estar em visada direta. Isto minimiza o problema de interferências causadas por obstáculos (reflexões, interferência por *multi-path*, etc). Além disso, a distância máxima permitida entre os nós *i* e *j* devem ser menor ou igual a d_{max}, que é a distância máxima permitida para que uma mensagem possa ser transmitida e chegue no receptor com potência suficiente para ser corretamente compreendida.

4 ESTUDOS DE CASOS

Os testes de simulação foram realizados em um cenário com área útil da rede na forma quadrangular, com 200m de lado. Foi considerada a distância máxima de conexão ponto a ponto entre nós com visada direta de 200m. Foram realizados 10 experimentos para cada estudo de caso, em uma simulação simplificada e outra completa. Isto foi feito para demonstrar se o GA é capaz de encontrar soluções satisfatórias de modo consistente.

4.1. Simulação de Cenário Simplificado

Um cenário simplificado foi elaborado para facilitar a avaliação das funcionalidades propostas pela ferramenta desenvolvida. Foi realizada uma seqüência de testes com o mesmo cenário variando-se cada objetivo do algoritmo. O cenário simplificado possui 8 obstáculos fixos com 8 nós de rede, sendo o nó 1 como *gateway*. No momento inicial do cenário simplificado, o gateway não está conectado ao restante da rede, pois não possui visada direta com algum nó, somente os nós 3-4-5-7 possuem visada direta entre si, conforme apresentado na figura 12. Na simulação do cenário simplificado foram considerados 5 estudos de caso, descritos na tabela 5

.

Tabela 5 – Estudo de caso cenário simplificado

Estudo Caso	Objetivo	Restrição
1	Minimização roteadores	Cobertura total (100%)
2	Minimização roteadores Minimização do maior número de *hops* para mensagens Minimização de retransmissões por cada dispositivo (pesos iguais)	Cobertura total (100%)
3	Minimização roteadores, Minimização do maior número de *hops* para mensagens Minimização de retransmissões por cada dispositivo (pesos diferentes)	Cobertura total (100%)
4	Minimização roteadores, Minimização do maior número de *hops* para mensagens Minimização de retransmissões por cada dispositivo Maximização da tolerância de falha da rede a perda de um nó (pesos iguais)	Cobertura total (100%)
5	Minimização roteadores, Minimização do maior número de *hops* para mensagens Minimização de retransmissões por cada dispositivo Maximização da tolerância de falha da rede a perda de um nó (pesos diferentes)	Cobertura total (100%)

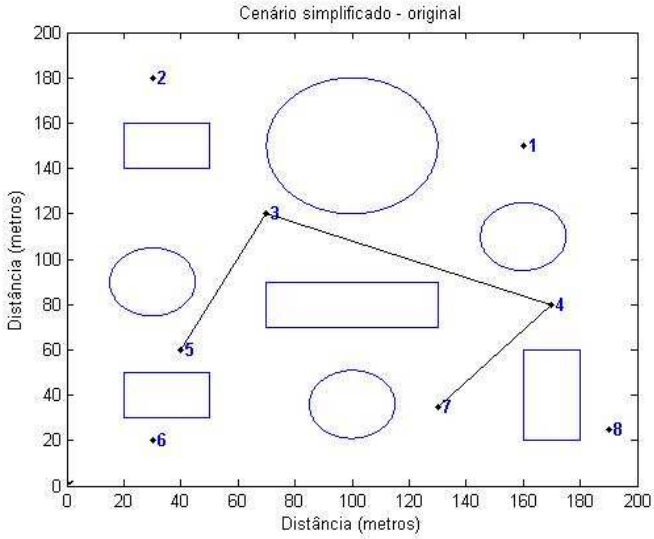

Figura 12 – Cenário Simplificado – Original

Foram realizados alguns experimentos iniciais para encontrar um bom conjunto de parâmetros para o GA para que este tivesse um bom desempenho nesta aplicação. Os parâmetros escolhidos para as simulações do cenário simplificado são apresentados na tabela 6.

Tabela 6 – Cenário Simplificado – Parâmetros

Parâmetros GA	Valores
Operador de cruzamento	0,9
Operador de Mutação	0,08
Número de gerações	100
Método de Seleção	Normalização geométrica
População inicial	100

4.1.1 Estudo de caso 1 – Cenário Simplificado - Minimização roteadores

Nesta simulação foi habilitada apenas a restrição de cobertura total da rede e o objetivo de minimização dos roteadores adicionais para conectividade da rede. A melhor configuração encontrada nos dez experimentos pode ser vista na figura 13. Os dados consolidados resultantes dos 10 experimentos são apresentados na tabela 7. O algoritmo atendeu propósito do teste de conectar toda rede com o mínimo de roteadores adicionais, pois adicionou apenas os roteadores 9 e 10 para conexão total dos nós.

Tabela 7 Estudo de caso 1 - Quadro consolidado

Critério	Original	Mínimo	Médio	Máximo
Nós Não Alcançados pelo Gateway	7	0	0	0
Número de Roteadores adicionados	0	**2**	2	2
Número de Vizinhos < (2)	6	4	4,5	**5**
Conexão Direta com Gateway	0	**1**	1,5	2
Nós com Hops > (4)	7	**0**	0,5	1
Máximo Hops	inf	**4**	4,5	5
Nós com Retransmissões > (4)	0	1	1,5	**2**
Máximo de Retransmissões por Nó	0	6	7	**8**
Menor Índice Tolerância Rede a falhas Nós	0	**0**	0,12	0,25

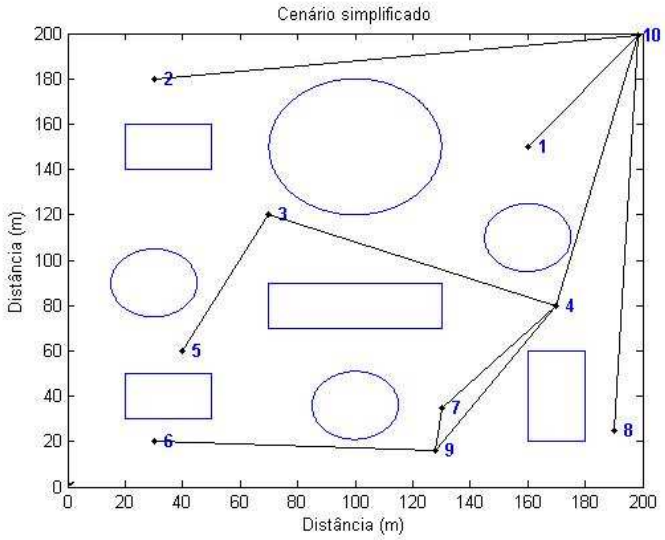

Figura 13 Estudo de caso 1 – Cenário

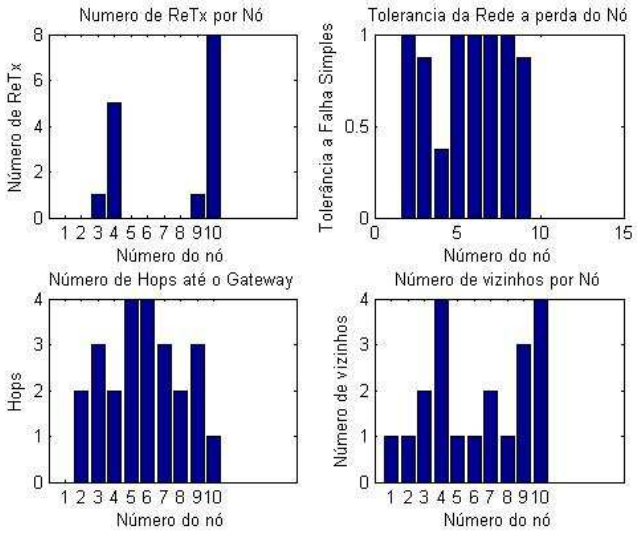

Figura 14 Estudo de caso 1 - Gráficos

Pode-se observar pelos resultados apresentados na tabela 7, os seguintes pontos positivos: (i) Foram adicionados apenas 2 roteadores para que a rede fosse totalmente conectada; (ii) Baixo número de nós com saltos (*hops*) acima de 4; e (iii) Poucos nós com retransmissões acima de 4. Quanto aos pontos negativos podemos ressaltar: (i) Baixa quantidade de nós com mais de 2 vizinhos; (ii) Poucos nós conectados diretamente com *gateway*; (iii) Alto número de retransmissões por nó; e (iv) Baixo índice de tolerância da rede à falha de nós.

Os gráficos da figura 14 apresentam os melhores resultados encontrados nos 10 experimentos. Pode-se ressaltar, com relação ao número de retransmissões, que o nó 10 está sobrecarregado. Isto significa que a bateria do nó 10 vai se esgotar mais rapidamente, o que fará com que este nó pare de funcionar e seja desligado da rede. Além disso, apesar da rede apresentar uma boa tolerância a perda de um nó, com exceção apenas dos nós 4 e 10, este último apresentou tolerância zero, sendo um ponto de falha altamente crítico, pois é responsáveis por conectar todos os outros nós da rede ao gateway. É importante destacar que se o nó 10 for retirado, a rede irá parar de funcionar, pois ele é o único nó em visada direta para o gateway. Com relação ao número de *hops* até o *Gateway*, as mensagens dos nós 5 e 6 precisam de 4 saltos para chegar ao *gateway*, que representa um atraso maior na atualização dos dados vindos destes dispositivos, já que a mensagem precisa passar por 3 nós intermediários antes de chegar ao gateway. Com relação ao número de nós vizinhos, os nós 4 e 10 apresentam os melhores resultados, devido as necessidades de conectividade da rede e não por aspectos de redundância de caminhos alternativos.

4.1.2 Estudo de caso 2 – Cenário Simplificado - Minimização roteadores, Minimização do maior número de *hops* para mensagens e Minimização de retransmissões por dispositivo (pesos iguais)

Nesta simulação foram habilitadas a restrição de cobertura total da rede e os objetivos de minimização dos roteadores adicionais, de minimização do maior número de *hops* para mensagens e da minimização de retransmissões por dispositivo. Nesta simulação os pesos dos objetivos foram colocados com os valores proporcionais e iguais (p=1/3). A melhor configuração encontrada nos dez experimentos pode ser vista na figura 15. Os dados consolidados resultantes dos 10 experimentos são apresentados na tabela 8. O propósito desse teste foi verificar o comportamento do algoritmo adicionando os dois objetivos de minimização do maior número de *hops* para mensagens e da minimização de retransmissões por dispositivo ao estudo de caso 1. Comparado ao estudo de caso 1, o algoritmo adicionou 3 roteadores (9, 10 e 11), um a mais do que o estudo 1.

Comparando os resultados apresentados na tabela 8 com os testes do estudo de caso 1, pode-se ressaltar os seguintes pontos positivos; (i) Não houve ocorrência de nós com saltos (*hops*) acima de 4; e (ii) Reduziu o número de nós com retransmissões acima de 4; (iii) Reduziu o número de retransmissões por nó; (iv) Aumentou a quantidade de nós com mais de 2 vizinhos, (v) O índice de tolerância da rede à falha de nós aumentou ; (vi) Aumentou a quantidade de nós conectados diretamente com *gateway*. Quanto aos pontos negativos podemos ressaltar que algumas soluções tiveram adição de até quatro roteadores.

Tabela 8 Estudo de caso 2 - Quadro consolidado

Critério	Original	Mínimo	Médio	Máximo
Nós Não Alcançados pelo Gateway	7	0	0	0
Número de Roteadores adicionados	0	**2**	3	4
Número de Vizinhos < (2)	6	**2**	2,5	3
Conexão Direta com Gateway	0	2	**3**	4
Nós com Hops > (4)	7	**0**	0	0
Máximo Hops	inf	**2**	2,5	3
Nós com Retransmissões > (4)	0	**0**	0,5	1
Máximo de Retransmissões por Nó	0	2	**3,5**	5
Menor Índice Tolerância Rede a falhas Nós	0	0,75	**0,82**	0,9

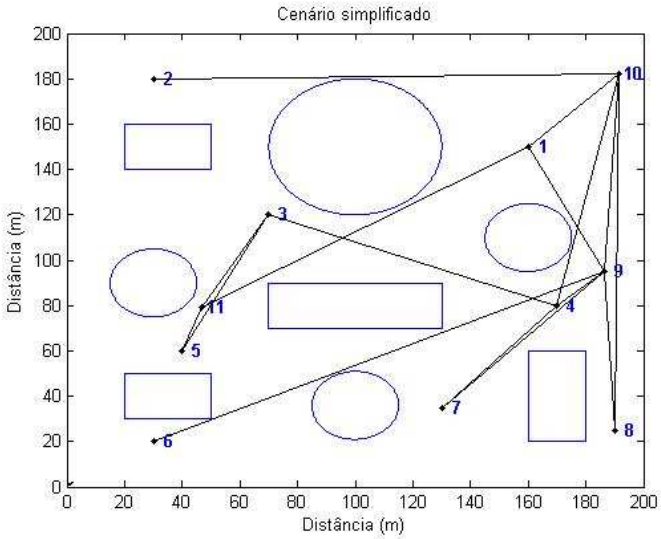

Figura 15 Estudo de caso 2 – Cenário

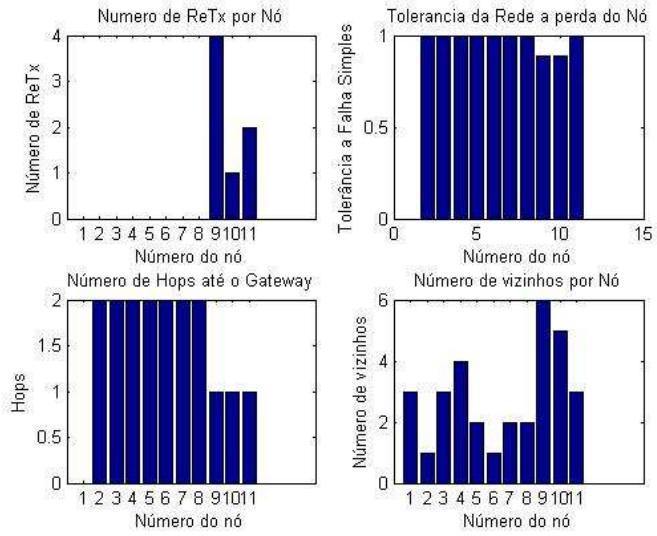

Figura 16 Estudo de caso 2 - Gráficos

Os gráficos da figura 16 apresentam os melhores resultados encontrados nos 10 experimentos. Pode-se ressaltar que o nó 9 apresentou os maiores números de retransmissões, a rede apresentou tolerância máxima a perda de um nó, com exceção dos nós 9 e 10, com relação ao número de *hops* até o *Gateway*, os nós apresentam no máximo até 2 saltos e com relação ao número de nós vizinhos, a maioria dos nós apresentaram pelo menos de 2 a 3 conexões com nós vizinhos.

Como o intuito desse estudo de caso foi observar a evolução da solução proposta pelo algoritmo pelo acréscimo dos objetivos citados acima, pode-se observar no gráfico da figura 17 que o valor médio do número máximo de *hops* do estudo 2 foi reduzido em 45% e o valor médio do número máximo de retransmissões foi reduzido em 50%, ambos em relação ao estudo 1. No gráfico da figura 18, pode-se observar que o valor médio do número de nós com *hops* acima de 4, foi reduzido a zero, e o valor médio do número de nós com retransmissões acima de 4 foi reduzida em 30%. Isso demonstra a solução satisfatória dada pelo algoritmo devido à redução tanto no número de *hops* quanto em retransmissões.

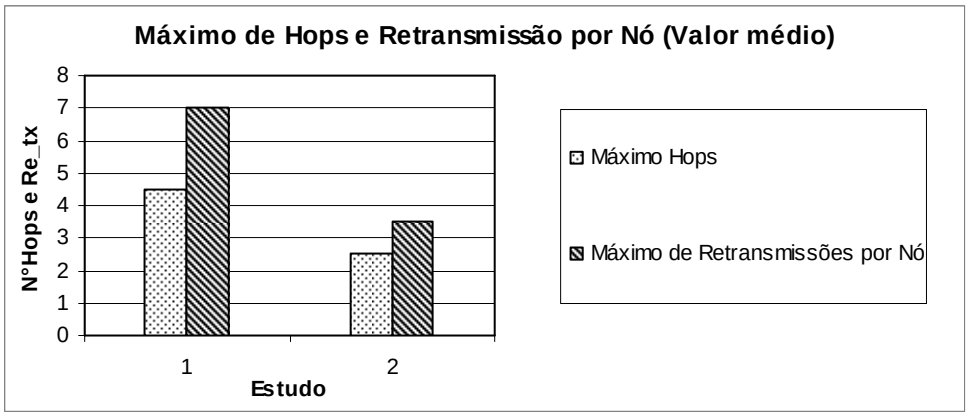

Figura 17 Máx. Retransmissões X Max. Hops (Estudo de caso 2)

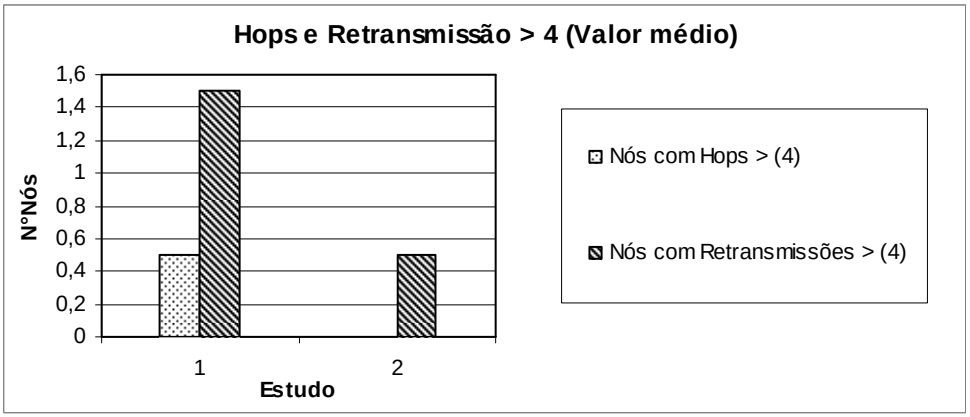

Figura 18 Retransmissões > 4 X Hops > 4 (Estudo de caso 2)

4.1.3 Estudo de caso 3 – Cenário Simplificado - Minimização roteadores, Minimização do maior número de *hops* para mensagens e Minimização de retransmissões por dispositivo (pesos diferentes)

Nesta simulação foram habilitadas a restrição de cobertura total da rede e os objetivos de minimização dos roteadores adicionais, de minimização do maior número de *hops* para mensagens e da minimização de retransmissões por dispositivo. Os pesos dos objetivos para minimização dos roteadores e minimização do maior número de *hops* foram de 0,1, enquanto para retransmissões por dispositivos foi de 0,8. A finalidade dessa diferença é priorizar o objetivo com maior peso para analise do resultado proposto pelo algoritmo. Após executada, a melhor configuração encontrada nos dez experimentos pode ser vista na figura 19 Os dados consolidados resultantes dos 10 experimentos são apresentados na tabela 9. O propósito deste estudo foi verificar a evolução das soluções propostas entre os estudos de casos 2 e 3, priorizando a minimização de retransmissões por dispositivos. Comparado ao estudo de caso 2, o algoritmo adicionou 4 roteadores (9, 10, 11 e 12), que possibilitou a conexão total dos nós da rede.

Comparando os resultados apresentados na tabela 9 com os testes do estudo de caso 2, pode-se ressaltar os seguintes pontos positivos: (i) O número máximo de retransmissões por nó reduziu; (ii) O índice de tolerância da rede a falhas aumentou; (iii) O número de conexões direta com gateway também aumentou; (iv) Não houve ocorrência de nós com retransmissões maior de 4. Quanto aos pontos negativos podemos destacar: (i) O uso de maior número de roteadores pelo programa; (ii) Aumentou o número de dispositivos com menos de 2 vizinhos; (iii) o número médio máximo de *hops* entre dispositivos e o gateway também aumentou.

Tabela 9 Estudo de caso 3 - Quadro consolidado

Critério	Original	Mínimo	Médio	Máximo
Nós Não Alcançados pelo Gateway	7	0	0	0
Número de Roteadores adicionados	0	4	5	6
Número de Vizinhos < (2)	6	2	3	4
Conexão Direta com Gateway	0	2	3	5
Nós com Hops > (4)	7	0	0	0
Máximo Hops	inf	3	3	3
Nós com Retransmissões > (4)	0	0	0	0
Máximo de Retransmissões por Nó	0	2	2,5	3
Menor Índice Tolerância Rede a falhas Nós	0	0,8	0,86	0,92

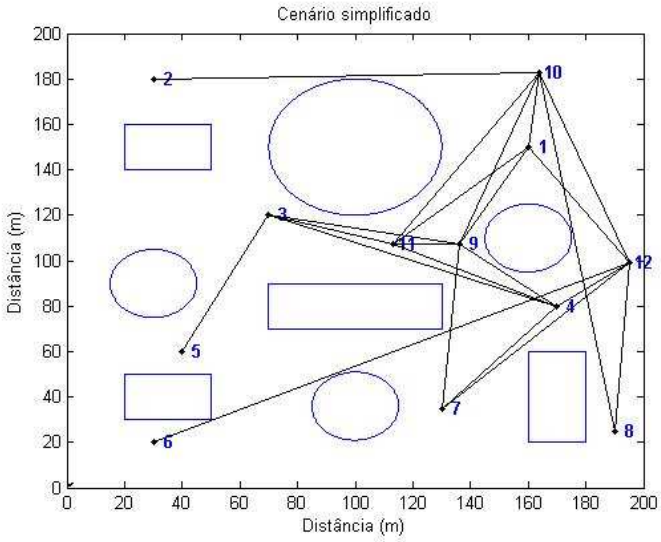

Figura 19 Estudo de caso 3 – Cenário

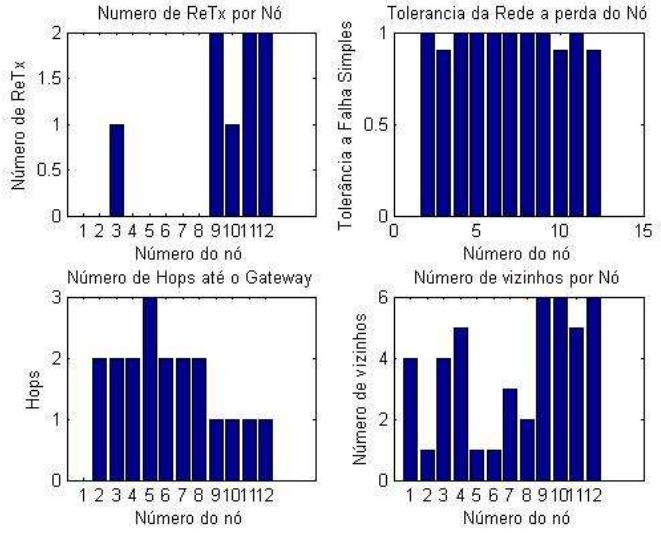

Figura 20 Estudo de caso 3 – Gráficos

Com pode ser observado nos gráficos da figura 20, com relação ao número de retransmissões, os nós 9, 11 e 12 apresentam os maiores números de retransmissões (2 retransmissões). A rede apresenta uma tolerância máxima a perda de um nó, com exceção dos nós 3, 10 e 12. Com relação ao número de *hops* até o *Gateway*, os nós 9, 10, 11 e 12 estão conectados diretamente com *Gateway*, o nó 5 possui 3 conexões até o *Gateway* e outros nós da rede apresentaram 2 saltos até chegar o *Gateway*. Com relação ao número de nós vizinhos, 8 nós possuem pelo menos 3 conexões com nós vizinhos e 4 nós possuem menos de 3 conexões.

O propósito do estudo 3 foi avaliar a variação da solução dada, comparada com o estudo 2, em função da prioridade dada ao objetivo Número de Retransmissões por Nó. Pode-se observar no gráfico da figura 21 que o valor médio do número máximo de retransmissões por nós foi reduzido de 3,5 para 2,5 , que demonstra que o algoritmo buscou dar prioridade a este objetivo, obtendo melhores valores, mesmo em detrimento aos outros, que pode ser comprovado pelo valor médio do número máximo de *hops* do estudo 2 que se elevou de 2,5 para 3, ambos em relação ao estudo 2. A mesma analogia pode ser feita para o valor médio do número de nós com retransmissões acima de 4, que foi zerada no estudo 2, e o valor médio do número de nós com *hops* acima de 4 se manteve em zero, conforme apresentado na figura 22.

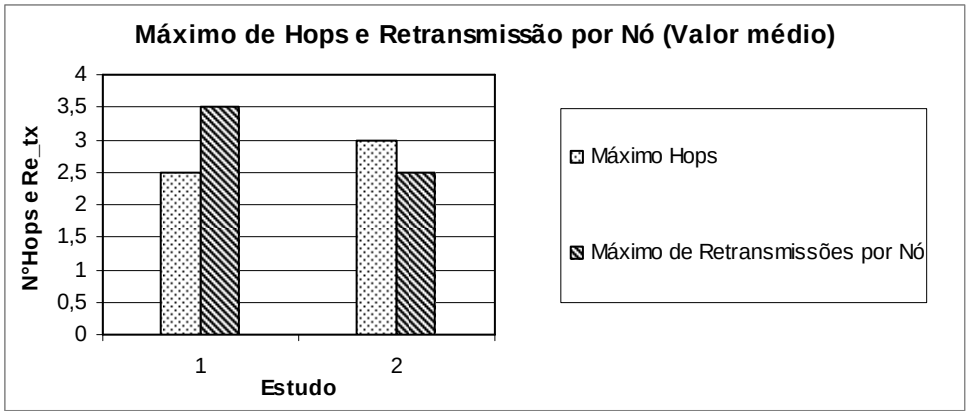

Figura 21 Máx. Retransmissões X Max. Hops (Estudo de caso 3)

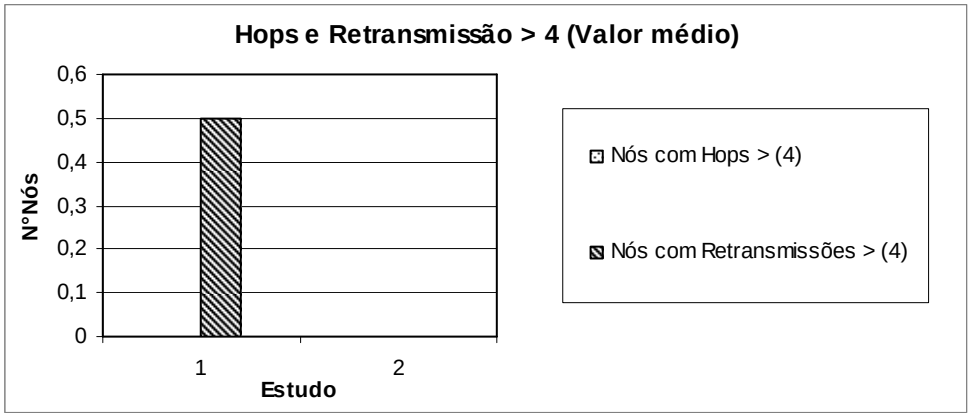

Figura 22 Máx. Retransmissões X Max. Hops (Estudo de caso 3)

4.1.4 Estudo de caso 4 – Cenário Simplificado - Minimização roteadores, Minimização do maior número de *hops* para mensagens, Minimização de retransmissões por dispositivo e Índice de Tolerância a falha da rede (pesos iguais)

Nesta simulação foram habilitadas a restrição de cobertura total da rede e os objetivos de minimização dos roteadores adicionais, de minimização do maior número de *hops* para mensagens, da minimização de retransmissões por dispositivo e do índice de tolerância a falha da rede a perda de um nó, considerando pesos iguais de valor 0,25 para todos os objetivos. A melhor configuração encontrada nos dez experimentos pode ser vista na figura 23. Os dados consolidados resultantes dos 10 experimentos são apresentados na tabela 10. O propósito do teste deste estudo 4 foi avaliar a solução dada pelo algoritmo com a inclusão do objetivo índice de tolerância a falha da rede, comparado com o estudo de caso 2, onde este objetivo não tinha sido habilitado. Neste cenário, o algoritmo adicionou 3 roteadores (9, 10 e 11), que possibilitou a conexão total dos nós da rede.

Comparando os resultados apresentados na tabela 10 com os testes do estudo de caso 3, pode-se ressaltar os seguintes pontos positivos: (i) Elevou o índice de tolerância da rede a falhas; (ii) O número médio de dispositivos com menos de 2 vizinhos se manteve constante; (iii) O número máximo de hops das mensagens dos dispositivos se manteve constante; (iv) Também não houve ocorrência de nós com retransmissões maior de 4; (v) O número de conexões direta com *gateway* se manteve constante; (vi) O número máximo e retransmissões por nó reduziu;. Quanto aos pontos negativos podemos ressaltar: (ii) Aumentou o uso de roteadores pelo programa;

Tabela 10 Estudo de caso 4 - Quadro consolidado

Critério	Original	Mínimo	Médio	Máximo
Nós Não Alcançados pelo Gateway	7	0	0	0
Número de Roteadores adicionados	0	3	3	4
Número de Vizinhos < (2)	6	2	2,5	3
Conexão Direta com Gateway	0	2	3	4
Nós com Hops > (4)	7	0	0	0
Máximo Hops	inf	2	2,5	3
Nós com Retransmissões > (4)	0	0	0	0
Máximo de Retransmissões por Nó	0	2	3	4
Menor Índice Tolerância Rede a falhas Nós	0	0,89	0,9	0,9

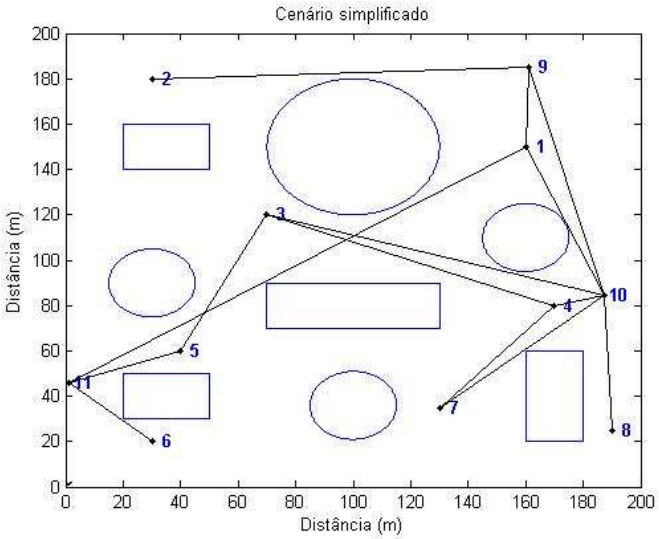

Figura 23 Estudo de caso 4 – Cenário

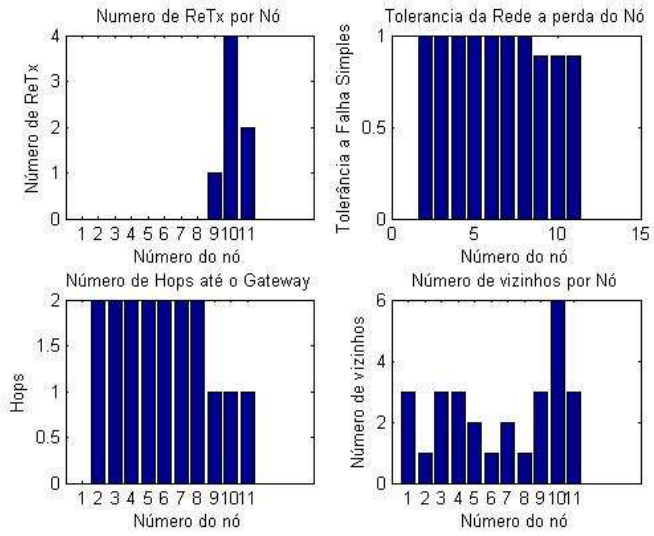

Figura 24 Estudo de caso 4 - Gráficos

Como mostrado nos gráficos da figura 24, nos melhores resultados encontrados nos 10 experimentos, com relação ao número de retransmissões, os nós 9, 10 e 11 apresentam valores que variam de 1 a 4 retransmissões. A rede apresenta uma tolerância máxima a perda de um nó, com exceção dos nós 9, 10 e 11, por também estarem associados à função de nós que fazem papel de repetidores. Com relação ao número de *hops* até o *Gateway*, os nós 9, 10 e 11 estão conectados diretamente com *Gateway*, e os outros nós possuem 2 conexões. Com relação ao número de nós vizinhos, o valor médio está entre 2 e 3 nós, que é um bom valor para este requisito, enquanto o nó 10 apresenta 6 conexões por exercer a função de repetidor de vários nós até o *gateway*.

No estudo 4, avaliou-se a solução dada em comparação ao estudo 2, onde a diferença foi a inclusão do objetivo de tolerância a falha da rede, mantendo-se pesos iguais e proporcionais para os objetivos. Pode-se observar no gráfico da figura 25 que o valor médio do índice de tolerância a falha da rede se elevou quase 10%, que demonstra que o algoritmo conseguiu melhorar o valor desse objetivo em relação ao estudo 2.

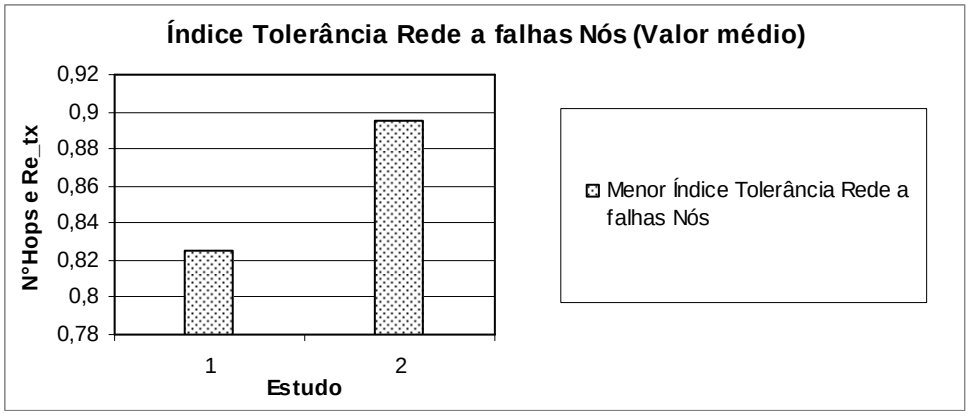

Figura 25 Tolerância a falha da rede (Estudo de caso 4)

4.1.5 Estudo de caso 5 – Cenário Simplificado - Minimização roteadores, Minimização do maior número de *hops* para mensagens, Minimização de retransmissões por dispositivo e Índice de Tolerância a falha da rede (pesos diferentes)

Nesta simulação foram habilitadas a restrição de cobertura total da rede e os objetivos de minimização dos roteadores adicionais, de minimização do maior número de *hops* para mensagens, da minimização de retransmissões por dispositivo e a maximização do índice de tolerância a falha da rede, considerando peso de valor 0,7 para tolerância a falha e pesos iguais de valor 0,1 para os outros objetivos. A finalidade dessa diferença é priorizar o objetivo com maior peso para analise do resultado proposto pelo algoritmo. Após executada, a melhor configuração encontrada nos dez experimentos pode ser vista na figura 26. Os dados consolidados resultantes dos 10 experimentos são apresentados na tabela 11. O propósito deste estudo foi verificar o resultado das soluções propostas entre os estudos de casos 4 e 5, priorizando a maximização de tolerância a falha da rede. Comparado ao estudo de caso 4, o algoritmo adicionou 4 roteadores (9, 10, 11 e 12), que possibilitou a conexão total dos nós da rede.

Comparando os resultados apresentados na tabela 11 com os testes do estudo de caso 4, pode-se ressaltar os seguintes pontos positivos: (i) O índice de tolerância da rede a falhas aumentou; (ii) Reduziu o número de dispositivos com menos de 2 vizinhos; Quanto aos pontos negativos podemos destacar: (i) O número máximo de retransmissões por nó aumentou; (ii) O número de conexões direta com gateway reduziu; (iii) O número de nós com retransmissões maior de 4 aumentou; (iv) O uso de maior número de roteadores pelo programa; (iii) o número máximo de *hops* entre dispositivos e o gateway também aumentou.

Tabela 11 Estudo de caso 5 - Quadro consolidado

Critério	Original	Mínimo	Médio	Máximo
Nós Não Alcançados pelo Gateway	7	0	0	0
Número de Roteadores adicionados	0	4	4	4
Número de Vizinhos < (2)	6	0	0	0
Conexão Direta com Gateway	0	2	2	2
Nós com Hops > (4)	7	0	0	0
Máximo Hops	inf	4	4	4
Nós com Retransmissões > (4)	0	1	1	1
Máximo de Retransmissões por Nó	0	5	6	7
Menor Índice Tolerância Rede a falhas Nós	0	1	1	1

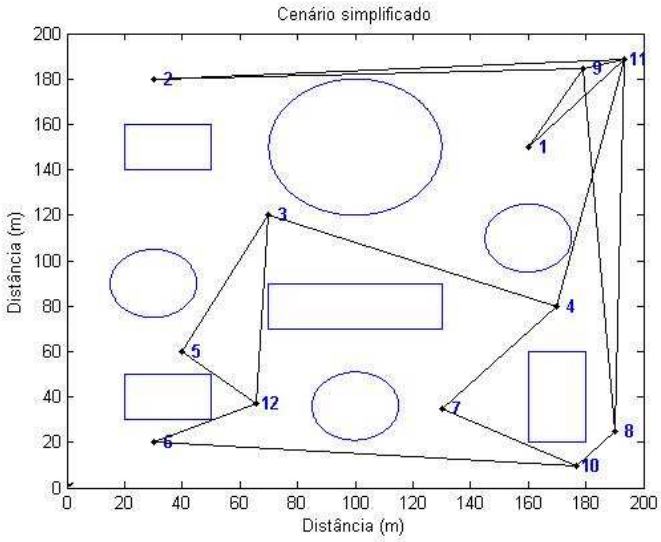

Figura 26 Estudo de caso 5 – Cenário

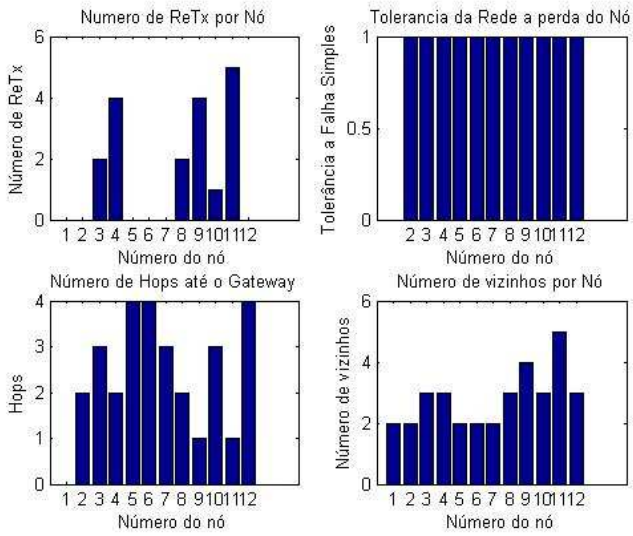

Figura 27 Estudo de caso 5 - Gráficos

Com pode ser observado nos gráficos da figura 27, com relação ao número de retransmissões, os nós 4, 9 e 11 apresentam os maiores números de retransmissões (4 retransmissões), caso que se justifica pelo fato desses nós estarem em posições estratégicas para conectividade da rede e redundância de caminhos de comunicação com nó 1 (*gateway*). Neste teste a rede apresentou valor máximo para índice de tolerância a falha de rede para todos os nós. Com relação ao número de *hops* até o *gateway,* os nós 9 e 11 estão conectados diretamente com *gateway*, e os outros nós com conexões entre 2 e 4 *hops* até o *gateway*, fato que também é explicado pelo aumento de caminhos redundantes da rede. Com relação ao número de nós vizinhos, todos os nós apresentaram pelo menos dois vizinhos, também influenciado pelo aumento de caminhos alternativos da rede.

O propósito do estudo 5 foi avaliar a diferença da solução dada, comparada com o estudo 4, em função da prioridade dada ao objetivo de tolerância a falha de rede. Pode-se observar no gráfico da figura 28 que o valor médio do Índice de Tolerância a falha da rede obteve o valor 1 para todos os nós, que é o valor máximo para o índice, em relação ao valor 0,89 do estudo de caso 4. Fato que demonstra que o algoritmo atingiu o seu propósito, obtendo os melhores valores, mesmo em detrimento aos outros objetivos configurados. Observa-se também que alguns outros objetivos tiveram pior desempenho comparado com o estudo 4, como número máximo de *hops* e número máximo de retransmissões. O valor médio do máximo de *hops* passou de 2,5 para 4 e o valor médio do máximo de retransmissões passou de 3 para 6, como mostra a figura 29.

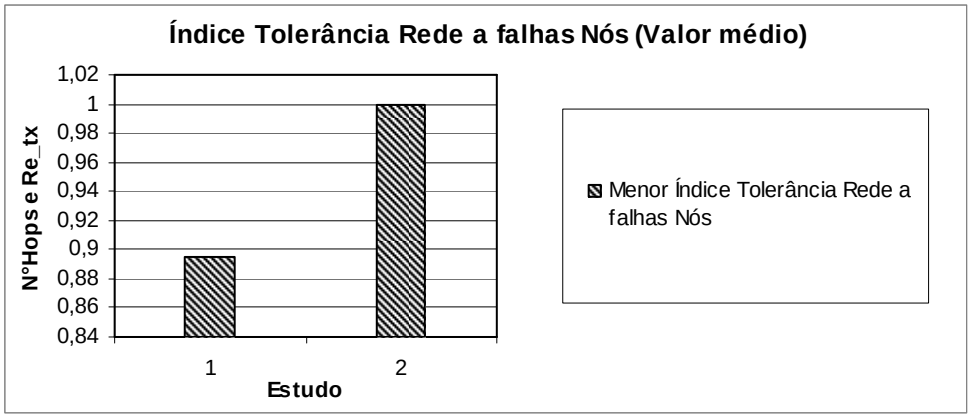

Figura 28 Tolerância a falha da rede (Estudo de caso 5)

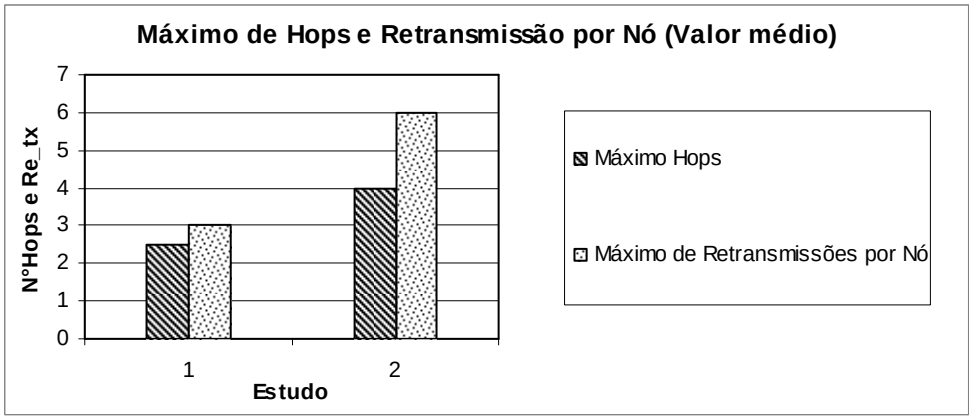

Figura 29 Tolerância a falha da rede (Estudo de caso 5)

4.2. Simulação de Cenário Completo

Um cenário completo, hipotético, foi elaborado para testar a eficiência da ferramenta desenvolvida, com características semelhantes a uma unidade industrial com prédio e tanques, onde se realizou uma seqüência de testes variando-se os objetivos do algoritmo. O cenário completo possui vários obstáculos fixos com 35 nós de rede, sendo o nó 1 o *gateway*. Além disso, foram adicionadas algumas ruas que funcionam como obstáculos passíveis de visada direta entre nós, porém não permitem que sejam posicionados roteadores sobre estas áreas. No momento inicial do cenário completo, conforme apresentado na figura 30, a rede aparece parcialmente conectada, tendo o gateway alcançado apenas 14 nós, devido à dificuldade imposta pelos obstáculos, dificultando a visada direta entre os nós. Um aspecto importante a ser observado é a grande quantidade de hops para as mensagens dado pelas ligações dos nós. Nesta simulação do cenário completo foram considerados 5 estudos de caso, descritos na tabela 12.

Tabela 12 – Estudo de caso cenário completo

Estudo Caso	Objetivo	Restrição
1	Minimização roteadores	Cobertura total (100%)
2	Minimização roteadores Minimização do maior número de *hops* para mensagens Minimização de retransmissões de cada dispositivo (pesos iguais)	Cobertura total (100%)
3	Minimização roteadores, Minimização do maior número de *hops* para mensagens Minimização de retransmissões por cada dispositivo (pesos diferentes)	Cobertura total (100%)
4	Minimização roteadores, Minimização do maior número de *hops* para mensagens Minimização de retransmissões por cada dispositivo Maximização da tolerância de falha da rede a perda de um nó (pesos iguais)	Cobertura total (100%)
5	Minimização roteadores, Minimização do maior número de *hops* para mensagens Minimização de retransmissões por cada dispositivo Maximização da tolerância de falha da rede a perda de um nó (pesos diferentes)	Cobertura total (100%)

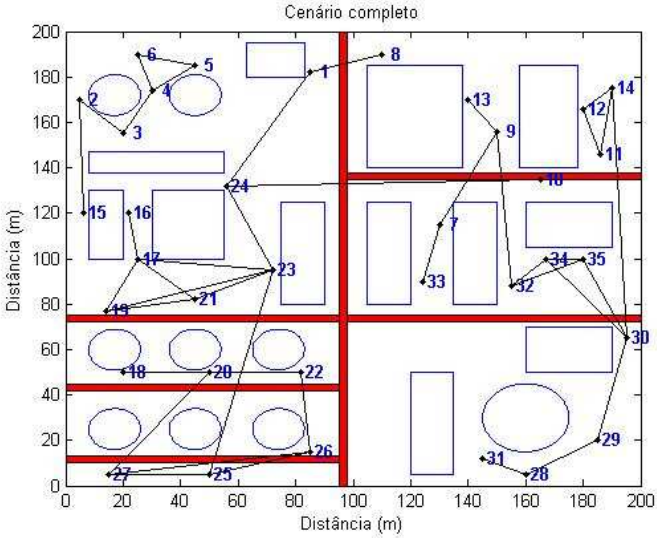

Figura 30 – Cenário Completo – Original

Da mesma forma que foi feito no cenário simplificado, foram realizados alguns experimentos iniciais para encontrar um bom conjunto de parâmetros para o GA para que este tivesse um bom desempenho nesta aplicação. Os parâmetros escolhidos para as simulações do cenário simplificado são apresentados na tabela 13.

Tabela 13 – Cenário Completo – Parâmetros

Parâmetros GA	Valores
Operador de cruzamento	0,9
Operador de Mutação	0,08
Número de gerações	50
Método de Seleção	Normalização geométrica
População inicial	50

4.2.1 Estudo de caso 1 – Cenário Completo - Minimização roteadores

Nesta simulação foi habilitada apenas a restrição de cobertura total da rede e o objetivo de minimização dos roteadores adicionais para conectividade da rede. A melhor configuração encontrada nos dez experimentos pode ser vista na figura 31. Os dados consolidados resultantes dos 10 experimentos são apresentados na tabela 14. O algoritmo atendeu o propósito de conectar toda rede com o mínimo de roteadores adicionais, adicionando na maioria dos experimentos apenas um roteador. Pelo cenário da figura 31, pode-se considerar que, sem o auxílio de uma ferramenta como esta, concluir que apenas um roteador seria suficiente para conectar toda rede e posicioná-lo de forma correta, não é uma tarefa fácil.

Tabela 14 Estudo de caso 1 - Quadro consolidado

Critério	Original	Mínimo	Médio	Máximo
Nós Não Alcançados pelo Gateway	20	0	0	0
Número de Roteadores adicionados	0	1	1	1
Número de Vizinhos < (2)	7	5	5,5	6
Conexão Direta com Gateway	2	2	2	2
Nós com Hops > (4)	23	16	19,5	23
Máximo Hops	Inf	9	10,5	12
Nós com Retransmissões > (4)	3	8	8,5	9
Máximo de Retransmissões por Nó	12	33	33	33
Menor Índice Tolerância Rede a falhas Nós	0.0303	0,0294	0,0294	0,0294

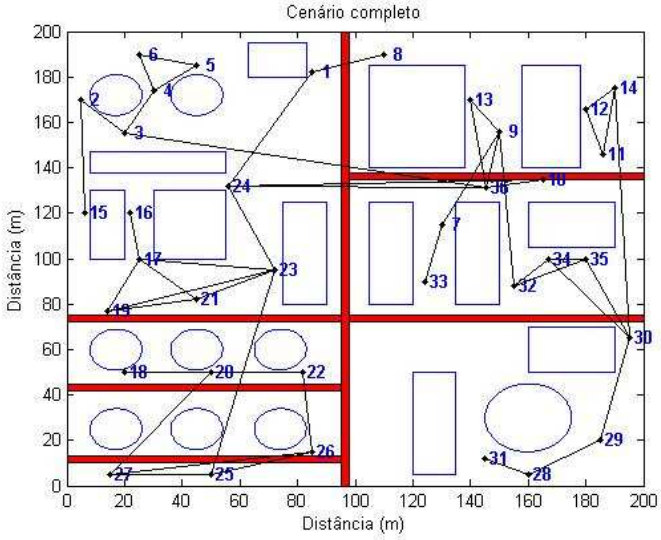

Figura 31 Estudo de caso 1 – Cenário

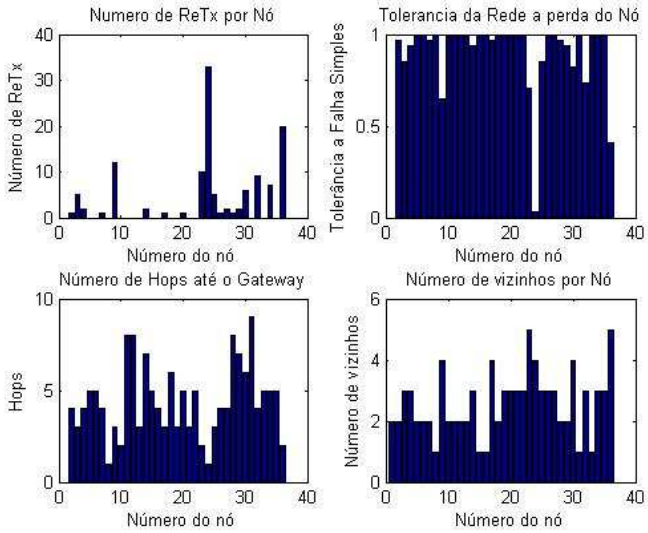

Figura 32 Estudo de caso 1 - Gráficos

Pode-se observar pelos resultados apresentados na tabela 14, os seguintes pontos positivos: (i) Foi adicionado apenas 1 roteador para que a rede fosse totalmente conectada; e (ii) Poucos nós com menos de 2 vizinhos. Quanto aos pontos negativos podemos ressaltar: (i) Grande número de nós com saltos (*hops*) acima de 4; (ii) Poucos nós conectados diretamente com *gateway*; (iii) Número razoável de nós com retransmissões acima de 4; (iv) Alto número de retransmissões por nó; e (v) Baixo índice de tolerância da rede à falha de nós.

Os gráficos da figura 32 apresentam os melhores resultados encontrados nos 10 experimentos. Pode-se ressaltar que os nós 24 e 36 apresentam os maiores números de retransmissões, pois são os principais nós de interligação da rede. As baterias desses nós vão se esgotar mais rapidamente devido às retransmissões, o que poderá comprometer todo o funcionamento da rede. Por estes motivos, estes nós 24 e 36, também apresentam os mais baixos índices de tolerância à falha da rede, o que representam pontos crítico de falha, pois são os principais responsáveis por conectar todos os outros nós da rede ao gateway. Com relação ao nó 24, é importante destacar que toda rede será interrompida caso o mesmo pare de funcionar, pois ele é o único nó em visada direta para o gateway. Com relação ao número de *hops*, dezesseis nós precisam ter mais de 4 saltos (*hops*) para chegar ao *gateway*, sendo que os nós 11, 12 e 28 utilizam 8 saltos e o nó 31 com nove saltos. Isso representa um grande atraso nos pacotes de dados desses dispositivos, já que a mensagem precisa passar por vários nós intermediários antes de chegar ao gateway. Com relação ao número de nós vizinhos, a alta densidade da própria rede facilita a conexão entre nós vizinhos, que faz com que apenas cinco nós tenham menos de 2 vizinhos cada um. Os nós 23 e 36 são os que possuem os maiores números, sendo cada um com cinco vizinhos.

4.2.2 Estudo de caso 2 – Cenário Completo - Minimização roteadores, Minimização do maior número de *hops* para mensagens e Minimização de retransmissões por dispositivo (pesos iguais)

Nesta simulação foram habilitadas a restrição de cobertura total da rede e os objetivos de minimização dos roteadores adicionais, de minimização do maior número de *hops* para mensagens e da minimização de retransmissões por dispositivo. Os pesos dos objetivos foram colocados com os valores proporcionais e iguais (p=1/3). A melhor configuração encontrada nos dez experimentos pode ser vista na figura 33. Os dados consolidados resultantes dos 10 experimentos são apresentados na tabela 15. O propósito desse teste foi verificar o comportamento do algoritmo adicionando os dois objetivos de minimização do maior número de *hops* para mensagens e da minimização de retransmissões por dispositivo ao estudo de caso 1. Comparado ao estudo de caso 1, o algoritmo adicionou apenas um roteador, igualmente ao estudo de caso.

Comparando os resultados apresentados na tabela 15 com os testes do estudo de caso 1, pode-se ressaltar os seguintes pontos positivos; (i) Reduziu bastante o número de nós com saltos (*hops*) acima de 4; (ii) Reduziu o número de nós com retransmissões acima de 4; (iii) Não houve aumento na quantidade de nós com mais de 2 vizinhos. Quanto aos pontos negativos podemos ressaltar: (i) Manteve o número de retransmissões por nó; (ii) Manteve baixo o índice de tolerância da rede à falha de nós; (iii) Manteve a quantidade de nós conectados diretamente com *gateway*.

Tabela 15 Estudo de caso 2 - Quadro consolidado

Critério	Original	Mínimo	Médio	Máximo
Nós Não Alcançados pelo Gateway	20	0	0	0
Número de Roteadores adicionados	0	1	1	1
Número de Vizinhos < (2)	7	5	5	5
Conexão Direta com Gateway	2	2	2	2
Nós com Hops > (4)	23	11	12,5	14
Máximo Hops	Inf	8	8	8
Nós com Retransmissões > (4)	3	6	7	8
Máximo de Retransmissões por Nó	12	33	33	33
Menor Índice Tolerância Rede a falhas Nós	0.0303	0,029	0,029	0,029

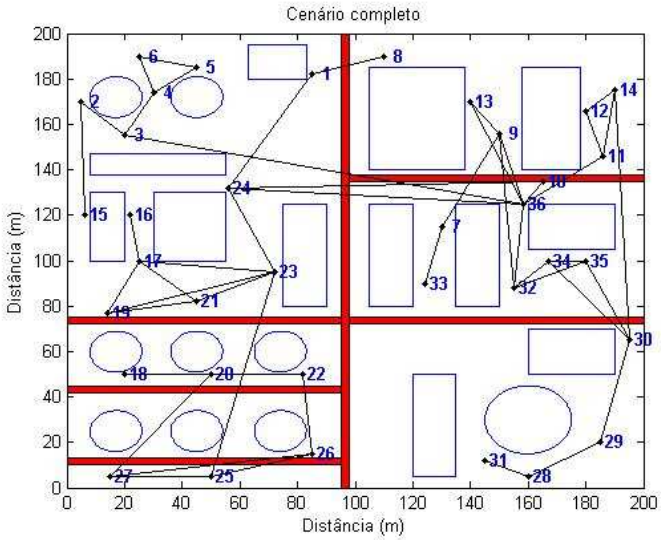

Figura 33 Estudo de caso 2 – Cenário

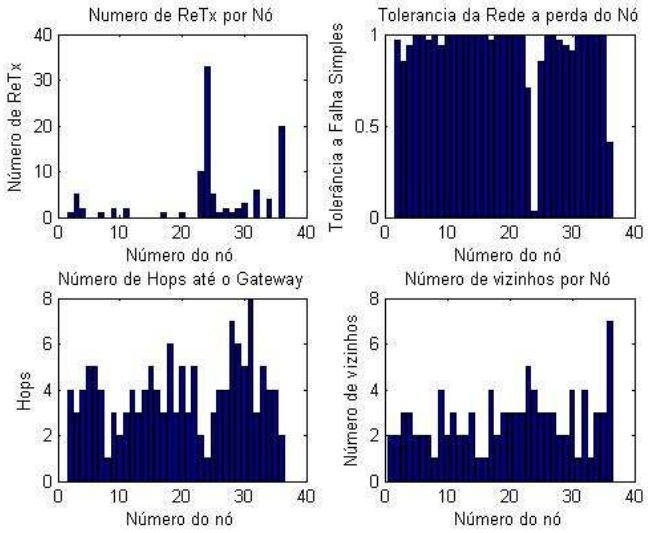

Figura 34 Estudo de caso 2 - Gráficos

Os gráficos da figura 34 apresentam os melhores resultados encontrados nos 10 experimentos. Pode-se ressaltar que o nó 24 apresentou os maiores números de retransmissões, a rede apresentou boa tolerância à perda de um nó, com exceção deste mesmo nó, por ser o principal ponto de ligação dos outros nós da rede com o gateway. Com relação ao número de *hops* até o *Gateway*, o nó 31 apresentou o maior valor de 8 saltos e com relação ao número de nós vizinhos, a maioria dos nós apresentaram pelo menos de 2 a 3 conexões com nós vizinhos, com exceção dos nós 8, 15, 16, 31 e 33.

Como o intuito desse estudo de caso foi observar a evolução da solução proposta pelo algoritmo com a inclusão dos objetivos citados acima, pode-se observar no gráfico da figura 35 que o valor médio do número máximo de *hops* do estudo 2 foi reduzido em 24%. O valor médio do número máximo de retransmissões se manteve com o mesmo valor, ambos em relação ao estudo 1. No gráfico da figura 36, pode-se observar que o valor médio do número de nós com *hops* acima de 4, foi reduzida em 36%, e o valor médio do número de nós com retransmissões acima de 4 foi reduzido em torno de 18%. Isso demonstra a solução satisfatória dada pelo algoritmo devido à redução tanto no número de *hops* quanto em retransmissões.

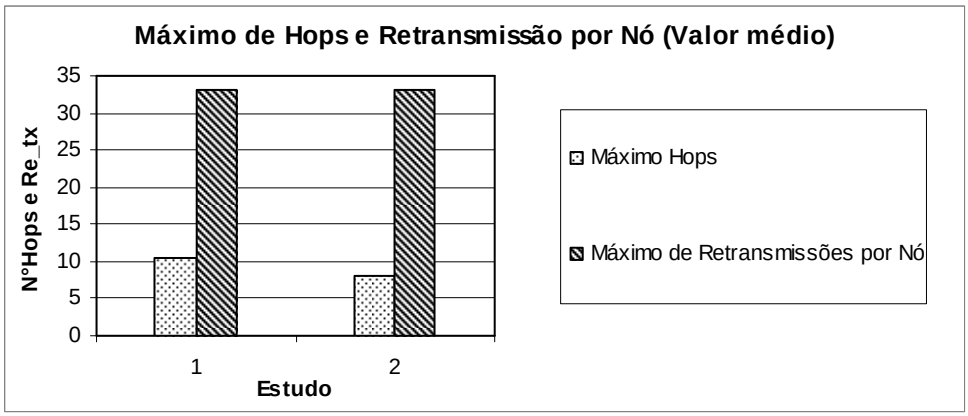

Figura 35 Máx. Retransmissões X Max. Hops (Estudo de caso 2)

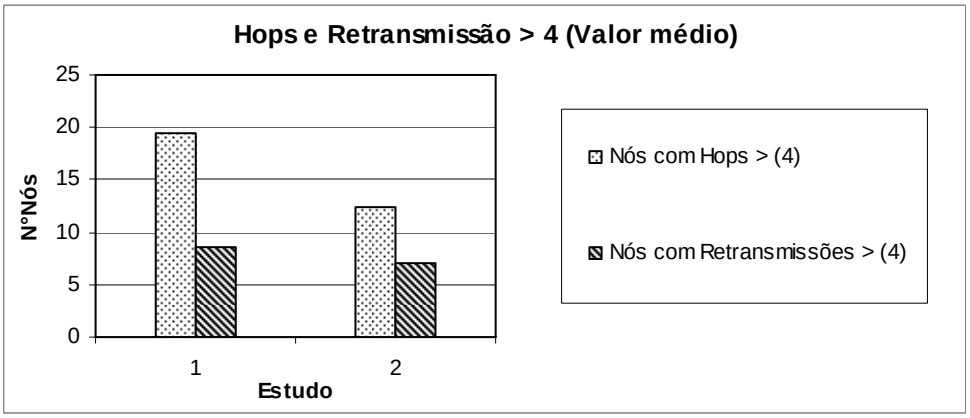

Figura 36 Retransmissões > 4 X Hops > 4 (Estudo de caso 2)

4.2.3 Estudo de caso 3 – Cenário Completo - Minimização roteadores, Minimização do maior número de *hops* para mensagens e Minimização de retransmissões por dispositivo (pesos diferentes)

Nesta simulação foram habilitadas a restrição de cobertura total da rede e os objetivos de minimização dos roteadores adicionais, de minimização do maior número de *hops* para mensagens e da minimização de retransmissões por dispositivo. Os pesos dos objetivos para minimização dos roteadores e minimização do maior número de *hops* foram de 0,1, enquanto para retransmissões por dispositivos foi de 0,8. A finalidade dessa diferença é priorizar o objetivo com maior peso para analise do resultado proposto pelo algoritmo. Após executada, a melhor configuração encontrada nos dez experimentos pode ser vista na figura 37. Os dados consolidados resultantes dos 10 experimentos são apresentados na tabela 16. O propósito deste estudo foi verificar a evolução das soluções propostas entre os estudos de casos 2 e 3, priorizando a minimização de retransmissões por dispositivos. Comparado ao estudo de caso 2, o algoritmo adicionou 4 roteadores (36, 37, 38 e 39), que possibilitou a conexão total dos nós da rede.

Comparando os resultados apresentados na tabela 16 com os testes do estudo de caso 2, pode-se ressaltar os seguintes pontos positivos: (i) O número máximo de retransmissões por nó reduziu de 33 para 7; (ii) O índice de tolerância da rede a falhas aumentou bastante; (iii) O número de conexões direta com gateway também aumentou; (iv) Não houve alteração significativa de nós com retransmissões maior de 4; (v) Reduziu o número de dispositivos com menos de 2 vizinhos; e (vi) O número máximo de *hops* entre dispositivos e o gateway diminuiu. Quanto aos pontos negativos podemos destacar: (i) O uso de maior número de roteadores pelo programa;

Tabela 16 Estudo de caso 3 - Quadro consolidado

Critério	Original	Mínimo	Médio	Máximo
Nós Não Alcançados pelo Gateway	20	0	0	0
Número de Roteadores adicionados	0	3	3,5	4
Número de Vizinhos < (2)	7	3	4,5	6
Conexão Direta com Gateway	2	4	5	6
Nós com Hops > (4)	23	2	4,5	7
Máximo Hops	Inf	5	5,5	6
Nós com Retransmissões > (4)	3	6	7,5	9
Máximo de Retransmissões por Nó	12	7	9	11
Menor Índice Tolerância Rede a falhas Nós	0.0303	0,833	0,835	0,837

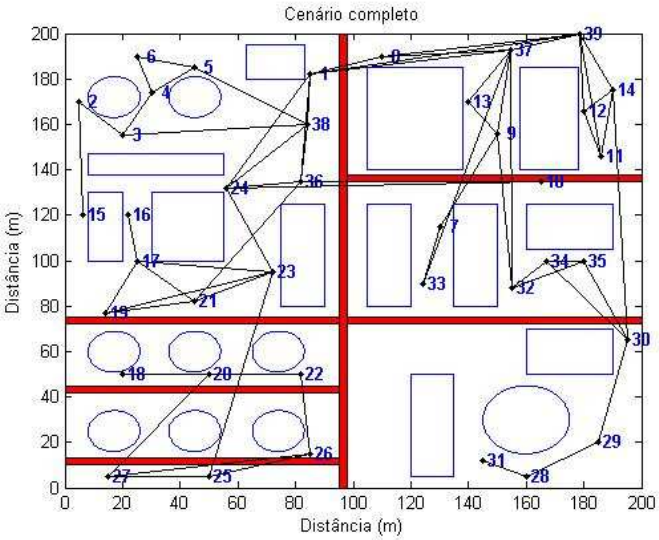

Figura 37 Estudo de caso 3 – Cenário

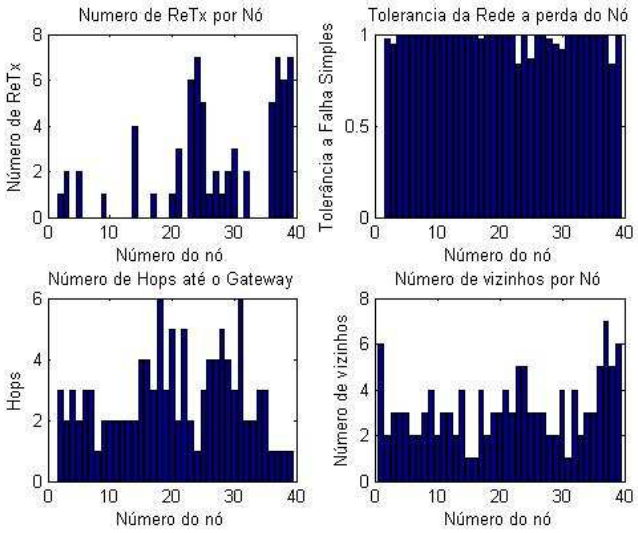

Figura 38 Estudo de caso 3 - Gráficos

Com pode ser observado nos gráficos da figura 38, com relação ao número de retransmissões, os nós 24, 37 e 39 apresentaram os maiores números de retransmissões (7 retransmissões). A rede apresenta uma boa tolerância a perda de um nó, com os menores valores para os nós 23 e 38. Com relação ao número de *hops* até o *gateway*, os nós 18, 20, 22, 28 e 31 apresentam mais de quatro saltos, sendo os nós mais distantes, 18 e 31, que apresentam 6 saltos até chegar o *gateway*. Com relação ao número de nós vizinhos, apenas os nós 15, 16 e 31 possuem menos de duas conexões com outros nós, o restante possuem pelos menos duas ou mais conexões com nós vizinhos.

O propósito do estudo 3 foi avaliar a variação da solução dada, comparada com o estudo 2, em função da prioridade dada ao objetivo Número de Retransmissões por Nó. Pode-se observar no gráfico da figura 39 que o valor médio do número máximo de retransmissões por nós foi bastante reduzido de 33 para 9, que demonstra que o algoritmo buscou dar prioridade a este objetivo, obtendo melhores valores. O valor médio do número máximo de *hops* do estudo 2 também foi bem reduzido de 8 para 5,5. A mesma analogia pode ser feita para o valor médio do número de nós com *hops* acima de 4, que foi reduzida 64% no estudo 2. O valor médio do número de nós com retransmissões acima de 4 teve uma pequena elevação em torno de 6%, conforme apresentado na figura 40.

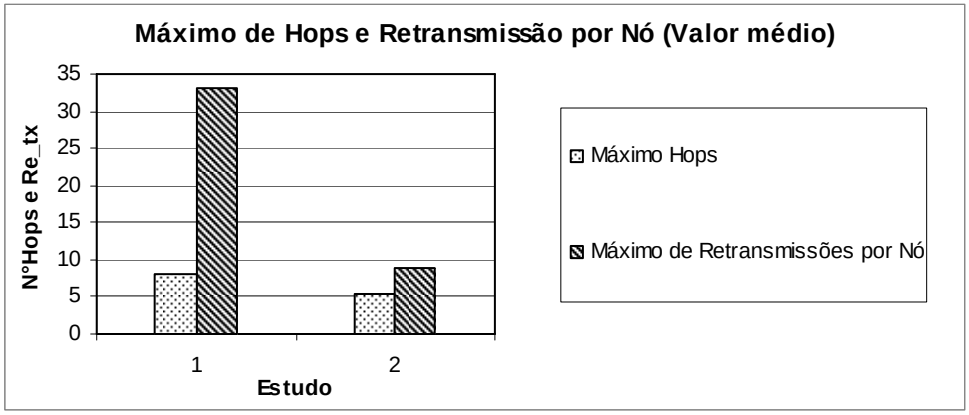

Figura 39 Máx. Retransmissões X Max. Hops (Estudo de caso 3)

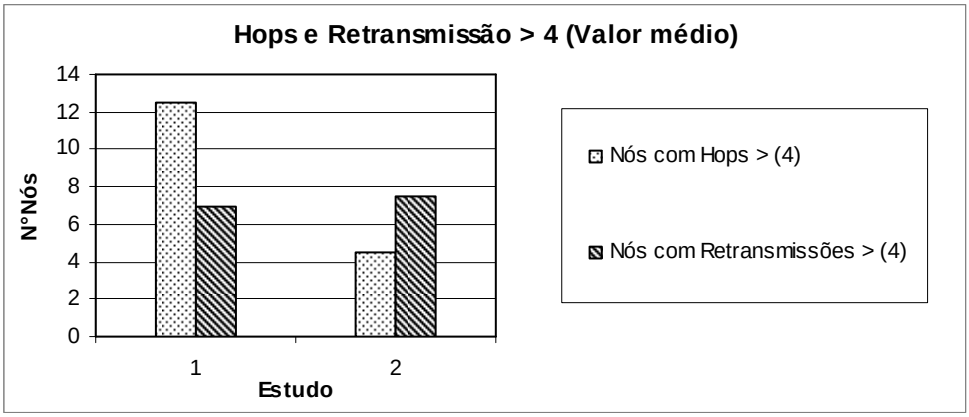

Figura 40 Máx. Retransmissões X Max. Hops (Estudo de caso 3)

4.2.4 Estudo de caso 4 – Completo - Minimização roteadores, Minimização do maior número de *hops* para mensagens, Minimização de retransmissões por dispositivo e Índice de Tolerância a falha da rede (pesos iguais)

Nesta simulação foram habilitadas a restrição de cobertura total da rede e os objetivos de minimização dos roteadores adicionais, de minimização do maior número de *hops* para mensagens, da minimização de retransmissões por dispositivo e da maximização do índice de tolerância a falha da rede a perda de um nó, considerando pesos iguais de valor 0,25 para todos os objetivos. A melhor configuração encontrada nos dez experimentos pode ser vista na figura 41. Os dados consolidados resultantes dos 10 experimentos são apresentados na tabela 17. O propósito do teste do estudo 4 foi avaliar a solução dada pelo algoritmo com a inclusão do objetivo índice de tolerância a falha da rede, comparado com o estudo de caso 2, onde este objetivo não tinha sido habilitado. Neste cenário, o algoritmo adicionou 3 roteadores (36, 37 e 38), que possibilitou a conexão total dos nós da rede.

Comparando os resultados apresentados na tabela 17 com os testes do estudo de caso 2, pode-se ressaltar os seguintes pontos positivos: (i) Elevou bastante o índice de tolerância da rede a falhas; (ii) O número de dispositivos com menos de 2 vizinhos reduziu; (iii) O número máximo de hops das mensagens dos dispositivos também reduziu; (iv) Manteve constante a ocorrência de nós com retransmissões maior de 4; (v) O número de conexões direta com *gateway* reduziu; (vi) O número máximo e retransmissões por nó reduziu bastante. Quanto aos pontos negativos podemos ressaltar: (i) Aumentou o uso de roteadores pelo programa;

Tabela 17 Estudo de caso 4 - Quadro consolidado

Critério	Original	Mínimo	Médio	Máximo
Nós Não Alcançados pelo Gateway	20	0	0	0
Número de Roteadores adicionados	0	2	2,5	3
Número de Vizinhos < (2)	7	3	4	5
Conexão Direta com Gateway	2	3	3,5	4
Nós com Hops > (4)	23	5	8,5	12
Máximo Hops	Inf	5	7	9
Nós com Retransmissões > (4)	3	6	6,5	7
Máximo de Retransmissões por Nó	12	15	22	29
Menor Índice Tolerância Rede a falhas Nós	0.0303	0,828	0,858	0,888

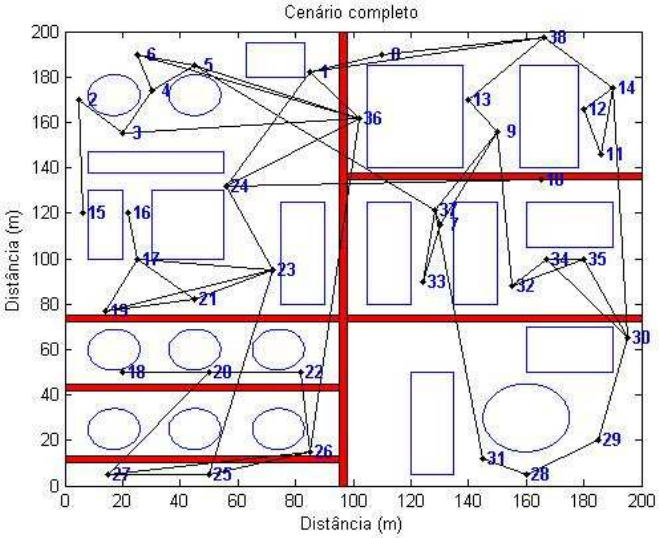

Figura 41 Estudo de caso 4 – Cenário

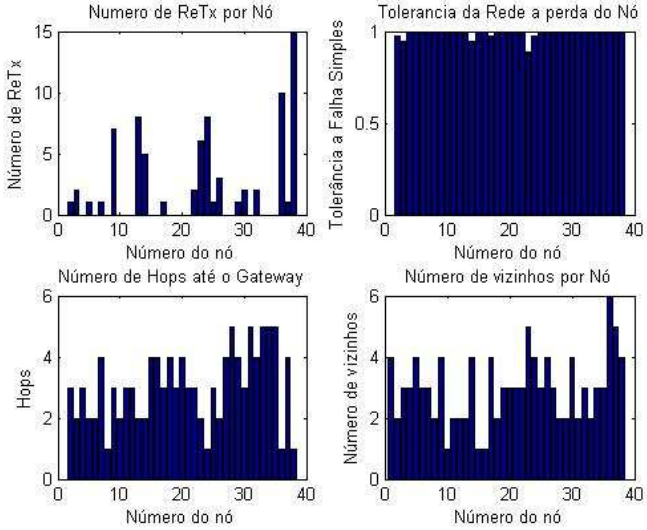

Figura 42 Estudo de caso 4 - Gráficos

Como mostrado nos gráficos da figura 42, nos melhores resultados encontrados nos 10 experimentos, com relação ao número de retransmissões, os nós 36 e 38 apresentam os maiores valores, acima de 10 de retransmissões. A rede apresenta uma boa tolerância à perda de um nó, com pequenas exceções, que representam um pequeno número em relação a toda rede. Com relação ao número de *hops* até o *Gateway*, apenas 5 nós apresentaram acima de 4 hops, que é um valor baixo dada a complexidade da rede e o baixo número de roteadores adicionados. Com relação ao número de nós vizinhos, apenas os nós 10, 15 e 16 apresentaram menos de dois vizinhos, que é um bom valor para este requisito, dado a quantidade de nós e a disposição da rede.

No estudo 4, avaliou-se a solução dada em comparação ao estudo 2, onde a diferença foi a inclusão do objetivo de tolerância a falha da rede, mantendo-se pesos iguais e proporcionais para os objetivos. Pode-se observar no gráfico da figura 43 que o valor médio do índice de tolerância a falha da rede se elevou significativamente de 0,029 para 0,858, que demonstra que o algoritmo conseguiu melhorar muito o valor desse objetivo em relação ao estudo 2.

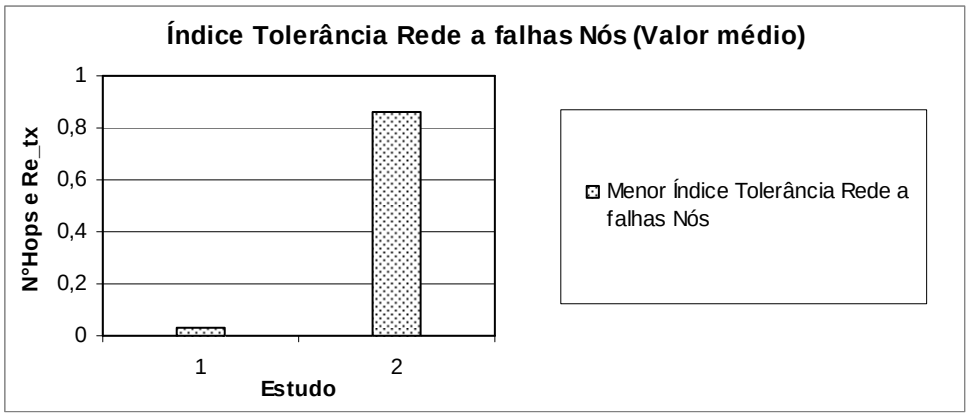

Figura 43 Tolerância a falha da rede (Estudo de caso 4)

4.2.5 Estudo de caso 5 – Cenário Completo - Minimização roteadores, Minimização do maior número de *hops* para mensagens, Minimização de retransmissões por dispositivo e Maximização do Índice de Tolerância a falha da rede (pesos diferentes)

Nesta simulação foram habilitadas a restrição de cobertura total da rede e os objetivos de minimização dos roteadores adicionais, de minimização do maior número de *hops* para mensagens, da minimização de retransmissões por dispositivo e do maximização do índice de tolerância a falha da rede, considerando peso de valor 0,7 para tolerância a falha e pesos iguais de valor 0,1 para os outros objetivos. A finalidade dessa diferença é priorizar o objetivo com maior peso para análise do resultado proposto pelo algoritmo. Após executada, a melhor configuração encontrada nos dez experimentos pode ser vista na figura 44. Os dados consolidados resultantes dos 10 experimentos são apresentados na tabela 18. O propósito deste estudo foi verificar o resultado das soluções propostas entre os estudos de casos 4 e 5, priorizando a minimização de tolerância a falha da rede. Comparado ao estudo de caso 4, o algoritmo adicionou 4 roteadores (36, 37, 38 e 39), que possibilitou a conexão total dos nós da rede.

Comparando os resultados apresentados na tabela 18 com os testes do estudo de caso 4, pode-se ressaltar os seguintes pontos positivos: (i) O índice de tolerância da rede a falhas aumentou; (ii) Reduziu o número de dispositivos com menos de 2 vizinhos; (iii) O número máximo de retransmissões por nó reduziu; (iv) Manteve o número de conexões direta com gateway; (v) Reduziu o número de nós com retransmissões acima de 4; (vi) o número máximo de *hops* entre dispositivos e o gateway também reduziu. Quanto aos pontos negativos podemos destacar: (i) O uso de maior número de roteadores pelo programa.

Tabela 18 Estudo de caso 5 - Quadro consolidado

Critério	Original	Mínimo	Médio	Máximo
Nós Não Alcançados pelo Gateway	20	0	0	0
Número de Roteadores adicionados	0	4	4,5	5
Número de Vizinhos < (2)	7	2	3	4
Conexão Direta com Gateway	2	3	4	5
Nós com Hops > (4)	23	0	5	10
Máximo Hops	Inf	4	5,5	7
Nós com Retransmissões > (4)	3	3	5,5	8
Máximo de Retransmissões por Nó	12	12	20,5	29
Menor Índice Tolerância Rede a falhas Nós	0.0303	0,972	0,973	0,974

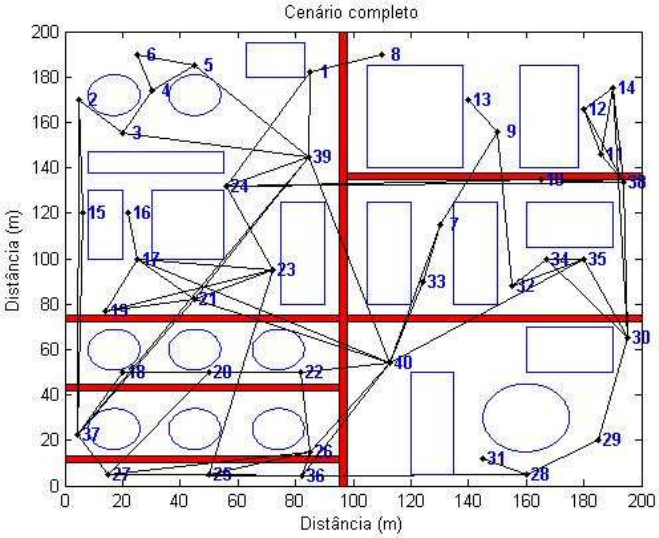

Figura 44 Estudo de caso 5 – Cenário

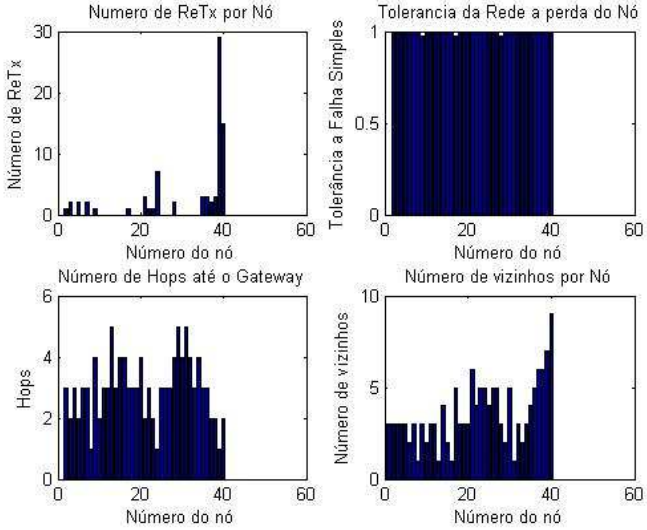

Figura 45 Estudo de caso 5 – Gráficos

Com pode ser observado nos gráficos da figura 45, com relação ao número de retransmissões, os nós 39 e 40 apresentam os maiores números de retransmissões por estarem em locais estratégicos que interligam vários nós da rede, além de servirem como redundância de caminhos de comunicação com nó 1 (*gateway*). Neste teste a rede apresentou praticamente valor máximo para índice de tolerância a falha de rede para todos os nós. Com relação ao número de *hops* até o *Gateway*, os nós 8, 24 e 31 estão conectados diretamente com *Gateway*, os nós 13, 29 e 31, pelo isolamento, apresentam mais de 4 saltos até o *Gateway*, e os outros nós apresentam até 4 saltos. Com relação ao número de nós vizinhos, apenas os nós 8, 13, 16 e 31 não apresentaram pelo menos dois vizinhos, também influenciado pelo seu posicionamento na rede.

O propósito do estudo 5 foi avaliar a diferença da solução dada, comparada com o estudo 4, em função da prioridade dada ao objetivo de tolerância a falha de rede. Pode-se observar no gráfico da figura 46 que o valor médio do Índice de Tolerância a falha da rede teve um acréscimo de valor em torno de 12%, em relação ao valor 0,858 do estudo de caso 4. Fato que demonstra que o algoritmo atingiu o seu propósito, obtendo os melhores valores, mesmo em detrimento aos outros objetivos configurados. Observa-se também que alguns outros objetivos tiveram redução de valor comparado com o estudo 4, como número máximo de *hops* e número máximo de retransmissões. O valor médio do máximo de *hops* passou de 7 para 5,5 e o valor médio do máximo de retransmissões passou de 22 para 20,5, como mostra a figura 47.

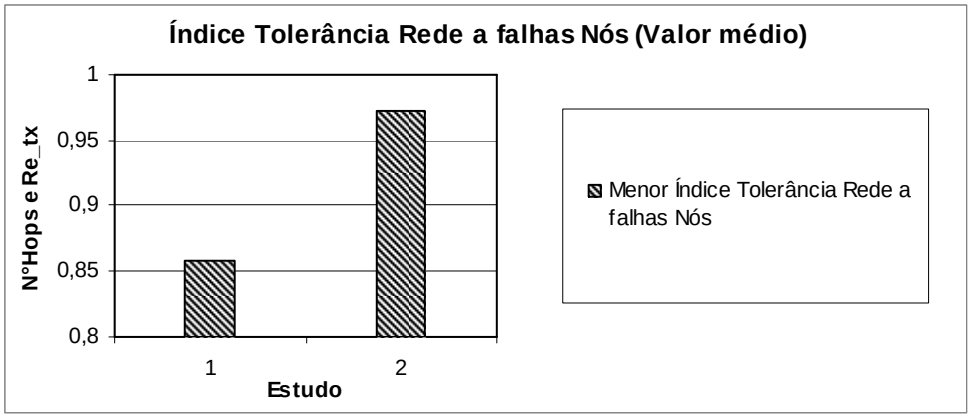

Figura 46 Tolerância a falha da rede (Estudo de caso 5)

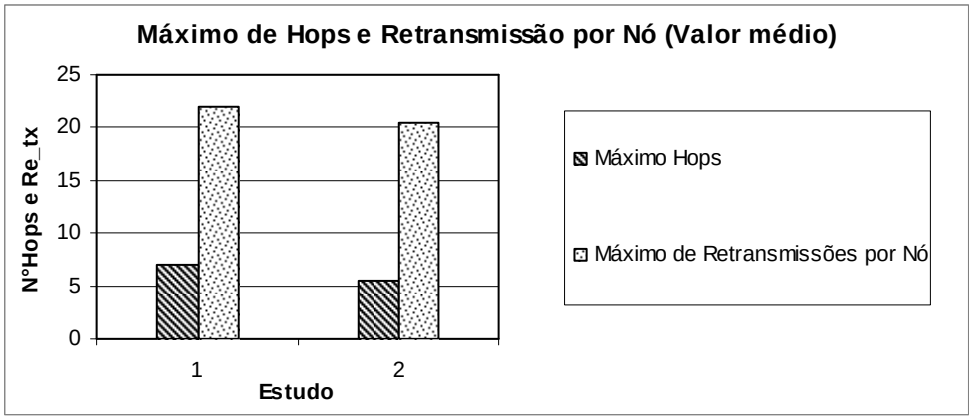

Figura 47 Tolerância a falha da rede (Estudo de caso 5)

CONCLUSÃO

Este trabalho apresentou o desenvolvimento de uma ferramenta para análise do posicionamento de nós em redes sem fio. A partir dos estudos realizados nos protocolos utilizados, determinou-se um conjunto de critérios utilizados para avaliar a rede formada. Os critérios escolhidos foram: minimização do número de roteadores adicionais, minimização do número de Hops, minimização do número de retransmissões e maximização do índice de tolerância a rede. Além destes critérios, a ferramenta também fornece informações relativas ao número de vizinhos de cada nó, a cobertura da rede e ao número de nós em conexão direta com o *gateway*.Nos estudos de casos realizados, ela foi capaz de analisar um cenário inicial de uma rede sem fio, e propor a inclusão do menor número de nós adicionais com o objetivo de otimizar os critérios estabelecidos pelo usuário. A ferramenta também permite que sejam dados diferentes pesos para os diferentes critérios, possibilitando que o usuário defina quais são os critérios mais relevantes para a sua aplicação. Os estudos de casos mostraram que a otimização dos critérios estabelecidos levou ao aumento do número de vizinhos e ao aumento do número de nós em conexão direta com o gateway, o que significa que as soluções propostas pela ferramenta encontram-se em concordância com as boas práticas de projeto sugeridas pela HART FOUNDATION para redes *WirelessHart*. Na simulação completa, onde se tem cenário mais complexo, pode-se observar diferentes soluções dada pelo algoritmo que dificilmente seria obtida por um usuário sem o auxílio de uma ferramenta desse gênero. Nos próximos passos do trabalho pretende-se incluir outros modelos de propagação para a determinação da conexão entre nós investigar a implementação de funções objetivo que sejam menos computacionalmente custosas, especialmente no que se refere a tolerância a falhas e comparar os resultados obtidos com agregação de objetivos com aqueles obtidos por algoritmos de otimização multiobjetivo baseados na obtenção do Conjunto ótimo de Pareto (Coello & Lamont, 2004). A seguir será feita uma avaliação da contribuição de cada uma destas parcelas na formação da rede final e comparar os resultados obtidos por agregação com aqueles obtidos por algoritmos de otimização multiobjetivo baseados na obtenção do Conjunto ótimo de Pareto (Coello & Lamont, 2004).

5. Referências Bibliográficas

COELLO, C.A.C and Lamont,G.B. (2004) “Applications of Multi-objective Evolutionary Algortihms”, World Scientific Books Publishing Co, Singapore.

CONTROLGLOBAL (2007). Disponível em http://www.controlglobal.com/Media/MediaManager/CT0708_wirelessGraphs.pdf. Acesso em 01 de fevereiro de 2010.

DAVIS, L., Handbook of Genetic Algorithms,VNR Comp. Library, 1990.

HOFFERT, J., Klues and Orjih O. (2007) “Configuring the IEEE 802.15.4 MAC Layer for Single-sinkWireless Sensor Network Applications. Technical Report. Disponível em: http://www.cs.wustl.edu/~joeh/802_15_4_Eval_Report.pdf. Acesso em 12 de dezembro de 2009.

HOUCK C. , Joines, J. and Kay, M. (1995). A Genetic Algorithm for Function Optimization: A Matlab Implementation NCSU-IE TR 95-09.

ISA-SP100.11a (2007). Disponível em: http://tinyos.stanford.edu/ttx/2007/viewgraphs/standards-sp100.pdf. Acesso em 01 de fevereiro de 2010.

MICHALEWICZ, Z. (1994) Genetic Algorithms+Data Structures=Evolution Programs, Springer-Verlag.

MOLINA, G. and Alba, E. and Talbi,E.G., 2008, “Optimal Sensor Network Layout Using Multi-Objective Metaheuristics”- Journal of Universal Computer Science, vol.14 , n^{o} 15, pp. 2549-2565.

MUTHAIAH, S. N. and Rosenberg, C. P. (2008). Single Gateway Placement in Wireless Mesh Networks. Disponível em http:// www.ece.uwaterloo.ca/ ~cath/iscn08.pdf. Acesso em 26 de janeiro de 2010.

WANG, J., Xie, B., Cai, K. and Agrawal, D. P. (2007). Intelligent Gateways Placement for Reduced Data Latency in Wireless Sensor Networks, *IEEE International Conference on Mobile Adhoc and Sensor Systems*, Pisa, pp. 1-9.

WHITAKER, R. M., Raisanen, L., and Hurley, S. 2004. A Model for Conflict Resolution between Coverage and Cost in Cellular Wireless Networks. In *Proceedings of the Proceedings of the 37th Annual Hawaii international Conference on System Sciences (Hicss'04) - Track 9 - Volume 9* (January 05 - 08, 2004). HICSS. IEEE Computer Society, Washington, DC, 90287.1.

YOUSSEF, W. and Younis, M. (2007). Intelligent Gateways Placement for Reduced Data Latency in Wireless Sensor Networks, *ICC’ 07 International Conference on Communications*, Glasgow, pp. 3805-3810.

PACHECO M. A. C., Algoritmos Genéticos: Princípios e Aplicações, Laboratório de Inteligência Computacional Aplicada, Pontifícia Universidade Católica do Rio de Janeiro, 1999.

Zheng J. and Myung J. L,(2006) "A Comprehensive Performance Study of IEEE 802.15.4, "Sensor Network Operations, IEEE Press, Wiley InterScience, Chapter 4, pp. 218-237.

IEEE 802.15.4. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks(LR-WPAN), maio de 2003.

ZIGBEE ALLIANCE. ZigBee Specification version 1.0, dezembro de 2004. Página: http://www.zigbee.org

IEEE 802.11. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPAN)*, 1999.

Antonio A.F. Loureiro, José M. S. Nogueira, Linnyer B. Ruiz, Raquel A. F. Mini, Eduardo F. Nakamura, Carlos M. S. Figueiredo "*Redes de Sensores Sem Fio*", XXI Simpósio Brasileiro de Redes de Computadores (2003).

PEREIRA Marluce R., AMORIM Cláudio L., Maria Clicia Stelling de Castro "Tutorial sobre Redes de Sensores" disponível em http://magnum.ime.uerj.br/cadernos/cadinf/vol14/3-clicia.pdf**,** acesso em 10/2/2010.

L. Hu e D. Evans, "Secure aggregation for wireless networks", In Workshop on Security and Assurance in Ad hoc Networks, January 2003, disponível em http://www.cs.virginia.edu/~evans/pubs/wsaan-abstract.html.

A. Lim, "Self-configurable sensor networks", Computer Science and Engineering, Auburn University, disponível em (2003) http://www.eng.auburn.edu/users/lim/sensit.html.

IEEE Std. 802.15.4-2006, IEEE Standard for Information Technology – *Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)*. Institute of Electrical and Electronics Engineers, Inc., New York, 2006.

Joe Hoffert, Kevin Klues, Obi Orjih Washington University in St. Louis "Configuring the IEEE 802.15.4 MAC Layer for Single-sink Wireless Sensor Network Applications".

SINEM COLERI ERGEN, "ZigBee / IEEE 802.15.4 Summary", Email: csinem@eecs.berkeley.edu, September, 2004

RICARDO RENAN FONTÃO, "REDES WIRELESS - Monografia apresentada ao Curso de Especialização em Redes de Computadores e Comunicação de Dados", Departamento de Computação da Universidade Estadual de Londrina, 2008

RICARDO BARBOSA RORIZ, GABRIEL MEDINA PEGORARO, SHOU MATSUMOTO, “Antenas Inteligentes”, Universidade de Brasília / Departamento de Ciência da Computação, 2006

Santos, S. T, Redes de Sensores Sem Fio em Monitoramento e Controle. Dissertação de Mestrado - Universidade Federal do Rio de Janeiro, COPPE/UFRJ , (2007)

HART Communication Foundation. Disponível em: http://www.hartcomm.org/protocol/wihart/wireless_technology.html. Acesso em 30 de março de 2011.

IEC/PAS 62591, *Industrial communication networks – Fieldbus specifications – WirelessHART™ communication network and communication profile*, International Electrotechnical Commission, Edition 1.0, 2009

Raymond S. Wagner (2010), *Standards-Based Wireless Sensor Networking Protocols for Spaceflight Applications*, NASA Johnson Space Center - 2101 NASA Parkway, Houston TX, rayniond.s.Wagner@.nasa.gov, (2010)

ZigBee Alliance. Disponível em http://www.zigbee.org/Home.aspx. Acesso em 04 de abril de 2011.