UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS ARARANGUÁ

Marcelo Seibt de Oliveira

SISTEMA DE ILUMINAÇÃO PÚBLICA INTELIGENTE

Araranguá

2018

Marcelo Seibt de Oliveira

SISTEMA DE ILUMINAÇÃO PÚBLICA INTELIGENTE

Trabalho de Conclusão de Curso submetido à Universidade Federal de Santa Catarina como parte dos requisitos necessários para obtenção de grau de Bacharel em Engenharia de Computação.
Orientador: Prof. Dr. Fábio Rodrigues de La Rocha

Araranguá

2018

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

de Oliveira, Marcelo Seibt
Sistema de Iluminação Pública Inteligente / Marcelo Seibt de Oliveira ; orientador, Fábio Rodrigues de La Rocha, 2018.
168 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Araranguá, Graduação em Engenharia de Computação, Araranguá, 2018.

Inclui referências.

1. Engenharia de Computação. 2. Iluminação Pública. 3. Cidades Inteligentes. 4. Internet das Coisas. 5. Redes de Sensores Sem Fio. I. Rodrigues de La Rocha, Fábio . II. Universidade Federal de Santa Catarina. Graduação em Engenharia de Computação. III. Título.

Marcelo Seibt de Oliveira

SISTEMA DE ILUMINAÇÃO PÚBLICA INTELIGENTE

Este Trabalho de Conclusão de Curso foi julgado aprovado para a obtenção do Título de "Bacharel em Engenharia de Computação" e aprovado em sua forma final pela Universidade Federal de Santa Catarina.

Araranguá, 30 de Novembro 2018.

Prof. Drª. Eliane Pozzebon
Coordenadora

Prof. Dr. Fábio Rodrigues de La Rocha
Orientador

Banca Examinadora:

Prof. Dr. Anderson Luiz Fernandes Perez

Prof. Dr. Tiago Oliveira Weber

AGRADECIMENTOS

Ao meu orientador, prof. Fábio, foi uma honra tê-lo como professor durante a graduação e, neste trabalho, como orientador. Uma pessoa que admiro por ser apaixonado pela profissão, comprometido com o ensino, humano e extremamente inteligente. Agradeço pela contribuição e interesse neste trabalho.

Aos meus familiares Hélio, Sônia, Camila, Juliano, André, Marcus, Elsa (in memorian), Luzia, Nicolas e Adriana, pelo amor e carinho incondicional.

Aos meus colegas e amigos pela amizade e vivência durante o período de graduação.

Aos demais professores, servidores e colaboradores da Universidade Federal de Santa Catarina.

Muito obrigado!

" Opte por aquilo que faz o seu coração vibrar... Apesar de todas as consequências "

Osho

RESUMO

A Internet das Coisas é a tendência de termos cada vez mais equipamentos eletrônicos ligados à Internet, trocando informações com pessoas e outros equipamentos eletrônicos para a comodidade dos consumidores. Neste trabalho de desenvolvimento tecnológico, utiliza-se a Internet das Coisas para criar um sistema de monitoramento e controle da iluminação pública de uma cidade. O sistema é benéfico pois reduz os custos com manutenção, bem como o tempo de detecção de problemas nos postes de luz, contribuindo assim para o uso racional da energia elétrica. Além destes, o sistema coleta informações estratégicas para construir um mapa de falhas da rede de iluminação, e assim detectar problemas que levam à queima prematura das lâmpadas.

Palavras-chave: Cidades Inteligentes, Internet das Coisas, Iluminação Pública, Microcontrolador, Redes de Sensores Sem Fio

ABSTRACT

Internet of Things is the trend of having an increasingly number of electronic devices connected to the internet, sharing information with people and other devices for the consumers convenience. In this work, the Internet of Things is used to create a system to control and monitor a city's lighting system. This system is important because it reduces maintainance expenses, time for problem detection in the light poles and improves rational use of electrical energy. Besides, the system collects strategic information in order to engineer a failure map of the lighting mesh and then identifies problems which may cause premature failure of the lamps.

Keywords: Smart Cities, Internet of Things, Public Lightning, Microcontroller, Wireless Network Sensors

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

IoT Internet of Things

MIT Massachusetts Institute of Technology

IEEE Institute of Electrical and Electronics Engineers

BLE Bluetooth Low Energy

AFH Adaptative Frequency Hopping

Wi-Fi Wireless Fidelity

Voip Voice Over IP

P2P Peer-to-peer

UNB Ultra Narrow Band

ISM Industrial Sientific and Medical

DAG Directed Acyclic Graph

DHSS Direct-Sequence Spread Spectrum

FHSS Frequency-Hopping Spread Spectrum

LPWAN Low-Power Wide-Area Networks

CSS Chirp Spread Spectrum

FSK Frequency-shift keying

MPR Multipoint Relay

BWA Broadband Wireless Access

MAC Medium Access Control

BSS Basic Service Set

IBSS Independent Basic Service Set

PCF Point Coordination Function

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

DIFS DCF Interframe Spacing

SIFS Short Interframe Spacing

CTS Clear-to-Send

NAV Network Allocation Vector

WPAN Wireless Personal Area Networks

DCF Distributed Coordination Function

RTS/CTS Request to Send and Clear to Send

RTS Request to Send

CTS Clear to Send

WiMAX Worldwide Interoperability for Microwave Access

OFDM Orthogonal Frequency Division Multiplexing

WMAN Wireless Metropolitan Area Network

RREQ Route Request Package

RREP Route Reply Package

NS Network Simulator

SUMÁRIO

1 INTRODUÇÃO

1.1 CARACTERIZAÇÃO DO PROBLEMA

Internet das coisas (Internet of Things (IoT)) é o termo criado em 1999 por Kevin Ashton, do Massachusetts Institute of Technology (MIT), para descrever a ideia de conectar os itens utilizados no dia a dia (coisas) à rede mundial de computadores (OLSON, 2016; ATZORI; IERA; MORABITO, 2010). Até então pensava-se na Internet como uma rede que conectava apenas pessoas. Hoje o cenário é tal que há mais dispositivos eletrônicos do dia a dia acessando a rede que pessoas. Um bom exemplo disso é a constatação que em 2011, a população da Terra atingiu 7 bilhões de pessoas e o número de dispositivos na rede atingiu 13 bilhões. A expectativa para 2015 era de três vezes mais dispositivos conectados à Internet do que a população mundial. Calcula-se que em 2020 existirão 50 bilhões de dispositivos na rede, e a expectativa é que a população mundial esteja em apenas 7,6 bilhões (EVANS, 2011).

Existem diversas aplicações para a IoT que podem ser utilizadas para resolver problemas do mundo real. Um destes problemas é o gerenciamento racional da iluminação pública em uma cidade.

Figura 1 – Iluminação pública (MARQUES, 2017)

Numa cidade, a iluminação pública é composta de postes de luz com lâmpadas (tipicamente lâmpadas de sódio) e um sensor fotoelétrico para detectar ausência de luz e ligar a lâmpada. A iluminação pública é de responsabilidade da prefeitura, e esta deve realizar as trocas de lâmpadas quando as mesmas queimam ou apresentam quaisquer defeitos de funcionamento (AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA - ANEEL, 2010). Conforme levantamento realizado através de contato com diversas prefeituras, existem, atualmente, duas formas de identificar o momento de substituição de uma lâmpada:

- Reclamações da população: a população entra em contato com a prefeitura, alertando mau funcionamento da lâmpada do poste público. Como ponto negativo, tem-se a existência de um intervalo de tempo em que a lâmpada permanece queimada até que um cidadão entre em contato com a prefeitura (que em muitos casos só pode ocorrer em horário comercial) para reclamar do fato. Isso causa transtornos à população em geral.
- Varreduras de caminhão: funcionários da prefeitura dirigem a noite pela cidade, verificando os postes de luz para detectar se os mesmos estão apagados. Como a operação de troca da lâmpada seria dificultada se realizada à noite, os funcionários tipicamente marcam o poste com algum símbolo (e.g. pano pendurado, placa, etc.) e anotam o endereço próximo. No dia seguinte, à luz do sol, a prefeitura retorna aos locais marcados e efetua a troca da lâmpada. Como ponto negativo, tem-se o custo envolvido em termos de recursos e tempo nesta atividade de varredura e troca das lâmpadas.

Percebe-se, portanto, que a iluminação pública apresenta-se como um cenário passível de melhorias através da aplicação de tecnologias embarcadas.

Neste trabalho propomos um sistema embarcado para monitorar o status das lâmpadas de postes de uma cidade. O sistema detecta se as lâmpadas estão funcionando ou estão queimadas e envia o status para a prefeitura. Além do monitoramento, pretende-se permitir que a prefeitura tenha capacidade de controlar a ativação das lâmpadas.

A figura 2 introduz os componentes do sistema proposto, conforme a disposição estrutural da rede. Os nós representam o arranjo composto pelo sistema embarcado e o poste ao qual o mesmo está instalado.

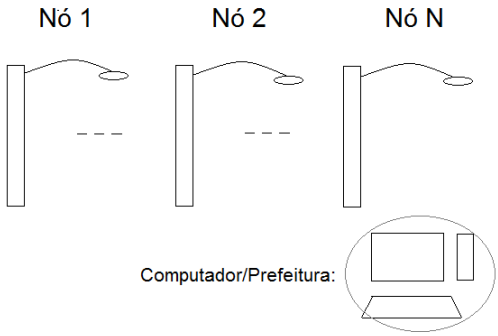


Figura 2 – Representação do sistema de iluminação pública

A transmissão de dados é a parte central desse sistema e poderia ser implementada por diferentes infraestruturas de rede:

- Transmissão por Wi-Fi (Institute of Electrical and Electronics Engineers (IEEE) 802.11) municipal (MILLAN et al., 2009): um dispositivo instalado no poste de luz é capaz de conectar-se à rede sem fio municipal. Essa alternativa seria de difícil implementação, pois demanda uma cobertura Wi-Fi em toda a cidade, gerando custos muito altos para instalar e manter;

- Uso de transmissão de dados por rede elétrica (LI et al., 2010): um dispositivo eletrônico envia e recebe as mensagens, usando como meio a própria rede elétrica dos postes, tal como um barramento comum. Este seria um sistema ideal, mas ainda possui problemas como o fato que, ao passar por transformadores, o sinal de rede provavelmente seria deturpado, necessitando de outros dispositivos instalados nos transformadores para propagar as mensagens daquele ponto em diante, o custo do dispositivo de rede em cada poste e a fragmentação de rede quando um poste falha;

- Uso de redes MESH (YI et al., 2015; LIU et al., 2008): utiliza um dispositivo sem fio instalado no poste, capaz de transmitir mensagens para os dispositivos próximos (postes de luz próximos). Os receptores das mensagens enviam as mensagens para os demais e assim por diante, propagando as mensagens por toda a rede MESH até que cheguem no equipamento instalado na prefeitura. Como ponto negativo, há a necessidade de verificar se existem postes de luz instalados numa distância máxima d entre si (onde

d precisa ser menor que o raio de alcance do Wi-Fi) e se eles formam um caminho até a sede da prefeitura. Nesta abordagem já existem algumas alternativas em uso, sendo uma bem conhecida, a *Zigbee*, embora ainda tenha um custo alto por unidade;

- Uso de infraestruturas de rede de longo alcance (LoRa e Sigfox): essas tecnologias seriam benéficas a este tipo de problema mas teriam também pontos negativos, como: instalação de *transceivers* nos postes de luz e *gateways* espalhados pela cidade para receber as mensagens e propagá-las pela internet, no caso da LoRa. Já no caso da Sigfox, os custos além do *transceiver* Sigfox nos postes, seria o custo de assinatura/unidade de um serviço de dados Sigfox, bem como problemas de pontos cegos de cobertura.

Alheio a tecnologia de transmissão coexiste a necessidade de escolha de um algoritmo de comunicação que otimize a transmissão e recebimento de dados neste sistema. Para que os microcontroladores consigam trafegar dados de ponta-a-ponta na rede, assegurando, para tal, que o tráfego de dados entre a central de gerenciamento e os dispositivos ocorra de modo mais conveniente possível, em um menor período de tempo e sem perda de informações entre o destino e a origem. Para isso, é preciso analisar os modelos existentes e, caso haja necessidade, propor um modelo de comunicação idealizado.

1.2 JUSTIFICATIVA E RELEVÂNCIA

O desenvolvimento do presente trabalho, em um sistema de iluminação pública, essencialmente permite automatizar procedimentos e otimizar o máximo de variáveis possíveis relacionadas a esse sistema, tornando-o mais funcional, eficiente, econômico e, principalmente, gerenciável.

Este sistema, cuja abordagem individual de seus elementos ainda é feita presencialmente e com pouca extração de dados inerentes ao seu funcionamento, conduz-se, de tal maneira, a uma incapacidade desejável de gerência das suas variáveis, havendo assim um considerável déficit de controle provocado pela ausência de dados pertinentes e assertivos.

Ciente destas deficiências, o presente trabalho visa aproveitar-se da redução do custo de tecnologias - especialmente as que integram microcontroladores e seus periféricos -, para propor uma alternativa

de aprimoramento do sistema de iluminação pública, através de um dispositivo de baixo custo, com expertise tecnológica autônoma e suficiente e da apresentação de um modelo de comunicação que otimize o funcionamento deste sistema.

1.2.1 Vantagens

A seguir são listadas as principais vantagens resultantes da implementação deste trabalho:

- Monitoramento online: monitoramento 24h, possibilitando a detecção mais rápida de problemas nas lâmpadas, reduzindo também os custos envolvidos. Uma redução do custo se daria na eliminação do sensor de acionamento da lâmpada que existe em alguns postes, visto que agora os postes são avisados quando devem acionar a lâmpada. Mais do que isso, a prefeitura não precisaria mais varrer os postes de luz para saber seu estado, os próprios postes de luz comunicam o problema à prefeitura;

- Mapa geral: mm mapa dos postes de iluminação pode ser desenvolvido, e num dado momento saber quantos são os postes que apresentam problema e qual a localização destes. Pode ainda manter um histórico de falhas periódicas e assim identificar zonas de falhas na rede elétrica, que causam queimas prematuras nas lâmpadas;

- Uso racional da energia: como agora os postes são inteligentes, seria razoável imaginar um cenário em que alguns dos postes tenham outros sensores (e.g. sensor de movimento, onde a cada dois postes, um deles tem sensor de movimento). Assim, numa rodovia em que não existem carros trafegando (tipicamente de madrugada) nem todos os postes de luz precisam ficar ativos, desperdiçando energia. Um poste de luz com sensor de movimento detecta que não existe movimento recente nas proximidades e envia mensagens para os postes próximos, para que alguns deles fiquem apagados. Quando eventualmente detecta movimento, envia mensagem para que todos sejam ativados.

1.2.2 Aplicações

Existe uma grande quantidade de aplicações que podem usar a rede de comunicação criada pelos postes de luz para outros propósitos, fomentando assim uma série de trabalhos:

- Monitoramento de trânsito: com a redução de preço da eletrônica embarcada, torna-se possível, a um baixo custo, criar um sistema eletrônico que, usando uma câmera, capture imagens dos carros numa rua/avenida e, executando uma aplicação de captura de imagens, verifica a placa dos carros e reconhece as letras e números. Com posse dessas informações, seria possível, para um sistema conectado ao DETRAN, detectar se um carro está com IPVA/licenciamento atrasado, ou mesmo se foi roubado. O sistema poderia enviar um alerta aos carros de polícia nas proximidades, já que a posição do poste de luz é conhecida. Sistemas como esse poderiam ser espalhados pela cidade, em virtude de seu custo reduzido.

- Lixeiras públicas: lixeiras públicas são esvaziadas diariamente ou a cada 2 ou 3 dias. O custo para manter a logística de recolhimento de lixo diariamente é muito alto. Mas há dias que a quantidade de lixo é maior e justificaria uma coleta. Uma lixeira eletrônica capaz de detectar se a sua tampa foi aberta (para adicionar lixo) e com sensor de carga para detectar se existe lixo dentro pode ser de grande ajuda. A lixeira eletrônica conectada à prefeitura avisa quando precisa ser esvaziada, ajudando a manter a cidade limpa, livre de pragas, e ajuda a minimizar o custo da coleta.

- Máquina de bilhetes de estacionamento: neste sistema, em alguns pontos da cidade existiriam máquinas de validação de estacionamento. O cliente que deseja estacionar o seu carro deve cadastrar a placa do seu veículo e informar o período de carência desejado. A máquina acessa a rede dos postes de luz para registrar o pagamento para a placa do carro. Os fiscais podem, através de uma aplicação móvel, reconhecer as placas dos carros e acessar a rede para verificar se estão com o estacionamento válido. Seria possível imaginar o mesmo sistema utilizando o padrão de telefonia móvel 3G, mas pontos cegos da cobertura tornariam o sistema inviável. Em um sistema com acesso à rede municipal pelos postes de luz, a cobertura seria contínua e ainda não incorreria em custos de

operadora de telefonia para cada um dos fiscais.

1.3 OBJETIVO

1.3.1 Objetivo Geral

Este é um trabalho de investigação que visa analisar as tecnologias de redes sem fio e os algoritmos de roteamento em redes sem fio que melhor se adaptam ao cenário disposto em um sistema de iluminação pública. Além disso, deseja-se aproveitar-se deste estudo científico, dos conhecimentos adquiridos sobre desenvolvimento de sistemas embarcados e da arquitetura da Internet das Coisas para implementar um sistema de iluminação pública inteligente que solucione os problemas pertinentes ao atual sistema de iluminação pública brasileiro, com o incremento da possibilidade de adição de novas funcionalidades ao mesmo.

1.3.2 Objetivos Específicos

Considerando o desenvolvimento do trabalho e o objetivo geral apresentado, destacam-se os seguintes objetivos específicos:

- Investigar e validar a capacidade de implementação de um sistema de iluminação pública inteligente através da aplicação de um modelo de comunicação de redes distribuídas e da utilização de um microcontrolador de baixo custo com capacidade de acesso Wireless Fidelity (Wi-Fi) 802.11. A investigação deve levar em conta o raio de alcance destes dispositivos e o mapa de instalação de postes de luz de uma cidade, para verificar a viabilidade do projeto;
- Criar um dispositivo de baixo custo capaz de ligar/desligar e informar o estado de uma lâmpada de iluminação pública através de mensagens enviadas por Wi-Fi;
- Este dispositivo deve ser capaz de ser expandido com a adição de alguns sensores de interesse, como, por exemplo: detector de movimento (para ser capaz de detectar que é possível desativar alguns postes de luz), detector de chuva, temperatura, poluição, trânsito (quantidade de carros passando por minuto), detector de transbordamento em determinado rio próximo, etc;

- Propor um modelo de comunicação entre os microcontroladores que atenda os requisitos do projeto;
- Implementar um modelo de comunicação minimamente satisfatório para o sistema de iluminação pública, implementando as funcionalidades de comunicação conforme sua característica topológica;
- Analisar os resultados obtidos e a viabilidade de implementação do projeto proposto.

1.4 ORGANIZAÇÃO

O presente trabalho está organizado da seguinte forma:

O **Capítulo 2** traz considerações a respeito das tecnologias existentes e potenciais para implementação do sistema. E, fundamentalmente para esta aplicação, considera os algoritmos de comunicação de dados através de uma revisão bibliográfica, comparando o funcionamento de modelos de comunicação compatíveis aos preceitos de funcionamento topológicos de um sistema de iluminação pública.

O **Capítulo 3** apresenta detalhes sobre o modelo de comunicação e o sistema embarcado desenvolvido.

O **Capítulo 4** exibe os resultados obtidos na execução do projeto e os dados pertinentes aos testes efetuados para avaliar o trabalho.

O **Capítulo 5** retrata as considerações após a conclusão do projeto acerca da experiência, dos resultados e das projeções futuras em relação ao contexto deste trabalho.

2 TECNOLOGIAS DE REDES SEM FIO

A escolha de uma tecnologia de redes sem fio adequada é fundamental para que o sistema funcione conforme a necessidade do projeto. Esta etapa irá impactar de diferentes formas na execução, sendo assim necessário levantar o máximo de parâmetros possíveis acerca de seu funcionamento: suas potencialidades, características, limitações, aplicabilidade, etc.

Deve-se, posteriormente, traçar um paralelo entre os requisitos de implementação do projeto e os recursos disponíveis em cada tecnologia. A escolha deve ser coerente à demanda de funcionamento e, adicionalmente, evidenciar as tecnologias que isolam a incompatibilidade, minimizam fatores que possam implicar em necessidade constante de manutenção e asseguram o pleno funcionamento do sistema em condições de instabilidade.

Especialmente para este projeto, algumas especificações possuem ênfase em relação a opção adotada: e.g. alcance do sinal, custo de aquisição, suporte ao desenvolvimento, taxa de transferência de dados, escalabilidade, configuração da topologia e custo de implementação. Este capítulo visa abstrair estas especificações, para cada tecnologia, através de uma breve descrição de cada uma delas.

Permite-se, de acordo com estas especificações, referenciar estas tecnologias associadas à atuação de sensores, sendo classificadas, de tal maneira, através de duas classes principais de atuação: monitoramento indoor e monitoramento outdoor.

2.1 TECNOLOGIAS DE MONITORAMENTO INDOOR

Pode-se utilizar, como exemplo, o caso de automações residenciais, onde a ocorre a interação com módulos sensores espalhados pela casa. Cada um desses módulos sensores possui uma unidade de processamento (microcontrolador), um sensor eletrônico e um *transceiver* de rádio para enviar os dados sem fio para um dispositivo *gateway*, onde ficarão disponiveis.

O gateway pode estar conectado a um servidor ou ser o próprio

servidor onde os dados oriundos dos sensores são processados e ações serão tomadas. Assim, o *gateway* pode, além de fazer um histórico dos valores dos sensores na nuvem, disparar um alarme de invasão, alarme de vazamento de gás, etc. A quantidade e capacidade dos sensores está limitada apenas pelo custo de implantação da aplicação.

A partir disto é possível monitorar estados das janelas (abertas/fechadas), estado das portas (abertas/fechadas), consumo de energia elétrica da residência, consumo da água da residência, sensor de gás GLP, etc.

Neste cenário, as tecnologias tipicamente empregadas são Bluetooth/BLE ou IEEE 802.11 e, assim, os módulos sensores precisam de *transceivers* dessas tecnologias.

2.1.1 Bluetooth Low Energy (IEEE 802.15.1)

2.1.1.1 Definição

A tecnologia bluetooth clássica surgiu em 1997, após técnicos suecos desenvolverem o primeiro padrão para um dispositivo de comunicação, de alcance restrito, via rádio. Hoje seu uso é disseminado e a tecnologia está disponível para uso em celulares, tablets, computadores, palmtops, fones de ouvido, televisores e diversos outros dispositivos (COSTAUR; MENDES, 2014).

Pode-se resumir a tecnologia bluetooth, de forma concisa e clara, da seguinte forma: é uma tecnologia que utiliza sinais de frequência de rádio, possui baixo custo, baixo consumo de energia, baixa potência, atua em curta distância e é utilizada para desempenhar a comunicação de dados e voz por vários dispositivos eletrônicos.

Em relação a banda, utiliza a ISM (Industrial, Científica e Médica), que é livre para utilização em quaisquer finalidades. Opera em uma faixa de frequência delimitada entre 2,4GHz e 2,48GHz. Caso vários dispositivos a utilizem há a possibilidade de congestionamento no tráfego de dados e pode, inclusive, haver interferência mútua entre os dispositivos. Devido a isso, para minimizar este efeito, os rádios bluetooth utilizam técnicas como alternar a frequência durante o uso (SAIRAM; GUNASEKARAN; REDD, 2002).

É projetada para utilizar técnicas objetivando atender as demandas das aplicações e requisições de comunicação de dados e voz com eficiência, controlando as perdas de sinais. Em função disso, o sinal de dados usualmente utiliza a técnica de comutação de pacotes - tecnologia que divide os dados, segmentando-os em pequenos pacotes antes da transmissão. Estes pacotes podem ser transmitidos por frequências, rotas e ordem diferentes da original. Quando recebidos, no entanto, são organizados e recompilados na sua forma original. Já o sinal de voz, utiliza a tecnologia de comutação de circuito, onde um canal dedicado (circuito dedicado) é estabelecido entre o receptor e o emissor para a transmissão de dados (BISDIKIAN, 2002).

Em termos de prospecção, bluetooth é uma tecnologia que pode ser largamente expandida e otimizada, haja vista que as aplicações pessoais, as quais requerem, cada vez mais, suporte à mobilidade, crescem em larga escala. As praticidades das aplicações que utilizam esta tecnologia nos próximos anos tendem a revolucionar não apenas o mercado de tecnologia, assim como atividades e tarefas mais variadas possíveis - desde as criticamente complexas tais como as aplicações de medicina até as tecnologias usadas corriqueiramente no dia a dia das pessoas.

Bluetooth Low Energy BLE ou Bluetooth Smart iniciou sendo parte das especificações do bluetooth 4.0 e, assim como a tecnologia clássica bluetooth, seu crescimento está intimamente associado ao crescimento de dispositivos móveis, smartphones, tablets e computação móvel. A tendência é que muitas aplicações tornem à aderi-la conforme sua expectativa crescente de aprimoramento (ARAUJO; VASCONCELLOS, 2012).

A atratividade desta tecnologia provém, principalmente, do seu demasiado baixo consumo de energia. Segundo Gomez, Oller e Paradells (2012), de acordo com resultados teóricos, verificou-se que:

- A duração da bateria de um dispositivo que utilize uma bateria *coin cell* varia de 2 dias a 14.1 anos;
- A quantidade de dispositivos terminais que podem estar simultaneamente conectados a cada dispositivo master varia de 2 à 5.917;
- A latência miníma para a obtenção de dados pelo master, a partir de uma leitura de sensor, é de 676 us (em redes com alta taxa de

bits errados essa latência pode ser aumentada em até 3x).

Apesar da derivação, BLE é considerada uma versão menor, otimizada e com objetivos de implementação distintos ao bluetooth (TOWNSEND; CUFÍ; DAVIDSON, 2014). Ainda segundo o autor, alguns destes objetivos são atender, de forma otimizada, às especificações de redes que contemplam as seguintes características:

- Baixo custo;
- Baixa largura de banda;
- Baixo consumo em todos os modos de utilização (pico de consumo, consumo médio e modo ocioso);
- Baixa complexidade;
- Alcance melhorado em relação ao bluetooth clássico;
- Suporte à tecnologia e disponibilização por múltiplos fabricantes.

Projetado para transmitir quantidades inferiores de dados, porém com menor latência, o BLE consegue ser até quinze vezes mais eficiente comparado ao bluetooth na entrega de dados. Segundo (CHO et al., 2016), essa eficiência é obtida através da otimização de três áreas funcionais:

1. Modo de descoberta e conectividade entre os dispositivos;
2. Número de pacotes transmitidos durante as conexões;
3. Tamanho individual dos pacotes.

No método de transmissão de sinal de rádio *two frequency hopping*, os dispositivos necessitam estar na mesma frequência ou canal, ao mesmo tempo, para se comunicarem. Quando os dispositivos iniciam a comunicação, não possuem sincronização mútua, e então iniciam um processo de descoberta de canal onde ocorre reciprocamente o reconhecimento entre os dispositivos. Este procedimento é demasiadamente custoso, na tecnologia bluetooth, devido ao número de canais ser elevado. Os dispositivos levam um tempo considerável para se conectarem, o que implica em consumo de energia relativamente excessivo. Na tecnologia BLE, a quantidade minimizada de canais associa um ganho de eficiência significativo em termos de tempo de estabelecimento da comunicação e consumo de energia (CHO et al., 2016).

Possui um mecanismo adaptativo baseado em saltos de frequência Adaptative Frequency Hopping (AFH), que evita as frequências ocupadas, sendo útil para evitar colisões com sinais Wi-Fi operantes na sua região de atuação. Isto é necessário, já que ambos ocupam o espectro de frequência gratuito 2.4GHz (GOMEZ; OLLER; PARADELLS, 2012).

BLE foi projetado para transmitir pequenas quantidades de dados através dos beacons. Um beacon BLE é um pequeno dispositivo, alimentado geralmente por bateria ou USB, que emite um sinal. Smartphones, que oferecem suporte, e que estejam na região de alcance do sinal (efetivamente 50m), podem captar este sinal e utilizá-lo, através de seus aplicativos.

As empresas como a Apple possuem seu próprio core de implementação, podendo definir o que é transmitido em dado intervado, definido também por si. A especificação BLE apenas define como o dado é transmitido, nas camadas físicas e de enlace.

Um exemplo bastante interessante da aplicação desta tecnologia é o acesso às promoções ou quaisquer outras informações relevantes, de uma loja, ao aproximar-se dela com seu smartphone, possuindo um aplicativo leitor de beacons.

2.1.1.2 Aplicações

Deve-se levar em consideração à aplicação para escolha de cada tecnologia. Ambas as tecnologias descritas anteriormente possuem características funcionais que visam atingir os requisitos de diferentes aplicações. São aplicações da tecnologia BLE:

- Monitoramento de batimento cardíaco utilizando sensores BLE;
- Monitoramento de temperatura, umidade através de sensores BLE;
- Fornecimento de informações estratégicas organizacionais dada proximidade do cliente com o estabelecimento;
- APP de cumpons;
- APP guia turistico baseado em beacons.

Pode ser utilizado nas seguintes áreas:

- Agricultura;
- Indústria;
- Cidades inteligentes;
- Indústria automotiva;
- Automação residencial;
- Serviços Médicos;
- Comunicações;
- Educação;

Observa-se, portanto, que em aplicações que demandam transferência de uma baixa quantia de dados (o que exclui streaming de vídeo, Voice Over IP (Voip), etc.), baixo consumo de energia e baixo custo associado, pode-se considerar a utilização desta tecnologia.

2.1.1.3 Topologia

A tecnologia BLE pode ser utilizada em topologias Peer-to-peer (P2P) (onde dois dispositivos comunicam-se através de uma conexão ponto-a-ponto), estrela ou redes Mesh. A topologia Mesh, tratando-se de redes de sensores, é a topologia mais utilizada na tecnologia BLE. Em decorrência do aumento de 3 para 48 bits em seu espaço reservado para endereços, agora é possível ter bilhões de dispositivos associados a um único dispositivo mestre nas redes Mesh (PESSOA, 2016).

Adicionalmente, na tecnologia BLE, o dispositivo *slave* permanece no modo de menor consumo por um período que compreende o máximo de tempo possível. Ele só estará apto para ouvir pacotes de eventos de comunicação, enviados pelo dispositivo *master*, quando desejar transmitir algum dado. Com excessão disso, permanece em modo *sleep*, economizando consumo de energia. Nesse modo, a média de consumo é de 1uA e, mesmo em pico, seu consumo não ultrapassa 6uA (PESSOA, 2016).

2.1.1.4 Especificações Técnicas

A tecnologia bluetooth considera uma taxa de transferência de dados máxima teórica de 1 Mbps (megabit por segundo). Essa taxa diverge de dispositivo para dispositivo conforme o tipo de comunicação, sendo, na prática, relativamente mais baixa que o referido valor teórico. Por exemplo, na comunicação *full-duplex*, na qual os dados trafegam em ambos os sentidos simultaneamente, a taxa de transferência de dados é realizada à 432,6 Kbps. E na assimétrica, na qual a transmissão é mais rápida em um dos sentidos, a taxa de transmissão de envio é de 721 Kbps e a de recepção é limitada à 56 Kbps (BISDIKIAN, 2002).

Para as transmissões de voz, a especificação da tecnologia determina a disposição de 3 canais de voz síncronos, com taxa de transferência de 64Kbps. O bluetooth suporta até 3 canais de voz síncronos e um canal de dados assíncrono; ou um único canal que suporte dados assíncronos e voz síncrono paralelamente (COSTAUR; MENDES, 2014).

De acordo com a tabela a seguir, são apresentadas as especificações técnicas de funcionamento das tecnologias bluetooth clássica e bluetooth low energy (LITEPOINT, 2012).

Tabela 1 – Tabela comparativa entre as tecnologias Bluetooth e BLE

Especificações Técnicas	**Bluetooth Clássico**	**Bluetooth Low Energy**
Frequência	2400 até 2483.5 MHz	2400 até 2483.5 MHz
Técnica de Modulação	Salto de Frequência	Salto de Frequência
Esquema de Modulação	GFSK	GFSK
Indíce de Modulação	0.35	0.5
Número de Canais	79	40
Largura de Banda do Canal	1 MHz	2 MHz
Taxa de Dados (nominal)	1-3 Mbps	1 Mbps
Taxa de Transferência	0.7 até 2.1 Mbps	<0.3 Mbps
nós	7	Ilimitado
Segurança	56 até 128 bits	128 bits AES
Robustez	FHSS	FHSS
Voz	Apto	Não Apto

2.1.2 WiFi (IEEE 802.11)

2.1.2.1 Definição

As WLANs dominam a concentração de uso pelos usuários através do seu padrão de comunicação mais difundido e utilizado: o padrão 802.11 ou WiFi (Wireless Fidelity). Fundado em 1999 pela Wireless Ethernet Compatibility Alliance, aliança composta pelas empresas Nokia, 3Com, Alcatel-Lucent e Symbol, esse padrão se destaca pelo seu considerável alcance, custo consideravelmente baixo e maturidade da tecnologia no mercado (HIERTZ et al., 2010).

Os padrões 802.11 atuam especificando as camadas física e de controle de acesso ao meio (MAC - Medium Access Control) da pilha de protocolos das WLANs (ALABADY; SALLEH; HASIB, 2014).

2.1.2.2 Camada Física

2.1.2.2.1 DSSS (Direct Squence Spread Spectrum)

A técnica de comunicação por espalhamento de espectro tem se tornado cada vez mais popular e utilizada devido capacidade de atenuar a interferência dos sinais transmitidos. Algumas de suas aplicações incluem: sistemas anti-jamming (interferência causada propositalemente), *Code Division Multiple Access* (Acesso Multiplo por Divisão de Código) e sistemas projetados para coibir *multipath* (DESHMUKH; BHOSLE, 2016).

Sinais que utilizam a técnica de espalhamento de espectro para transmitir informações digitais são caracterizados pela grande largura de banda em relação à taxa de informação em bits/s. Isto ocorre de tal modo que a densidade espectral de potência torna-se muito baixa e a potência do sinal é espalhada sobre uma faixa de frequência ampla. A grande redundância existente nos sinais de espalhamento de espectro superam os níveis acentuados de interferência encontrados na transmissão do sinal (STEPHENS; NORMAN, 1991).

Uma segunda característica interessante projetada para esta técnica de comunicação é a pseudoaleatoriedade, que faz com que o sinal

assemelhe-se ao ruído aleatório, porém difícil de ser demodulado por receptores exceto os pretendidos. Isto torna o sinal menos suscetível a interceptações (DESHMUKH; BHOSLE, 2016).

Segundo Deshmukh e Bhosle (2016), algumas aplicações frequentes desta técnica de comunicação incluem: WLANs (802.11b, 802.11g 802.11n) e Bluetooth. Estas tecnologias utilizam a banda ISM (2.4 GHz), que não possui controle sobre o uso indevido de seus recursos e acessos alheios indevidos, de forma proposital. DSSS é uma técnica restringe a facilidade de ocorrência destas particularidades. Também implementa as seguintes funcionalidades:

- Criptografia por salto pseudo aleatório de frequência;
- Resistência a interferência provocada por ruídos
- Escalabilidade superior em relação a técnica *Time Division Multiple Access*.

Esta técnica é adicionalmente composta por um arranjo de dados que inclui o sinal de dados enviado pelo transmissor associado a uma alta taxa de sequência de bit rate. O emissor gera um código de chip (*PN code sequence*) que garante a decifragem do sinal apenas aos receptores que conheçam esta código (STEPHENS; NORMAN, 1991).

2.1.2.2.2 OFDM (Orthogonal Frequency Division Multiplexing)

Recentemente utilizada nas redes Wireless, esta técnica é uma otimização da FDM (Multiplexação por Divisão de Frequência) e consiste em dividir um fluxo digital de alta taxa de bits em vários canais, através de taxas de bits menos elevadas, utilizando para isto a transmissão paralela de subportadoras (AUGUSTO et al., 2006).

Na técnica FDM, é necessário esperar que ocorra a transmissão íntegra de um sinal para posteriormente enviar o próximo. Isto ocasiona um mal aproveitamento da largura dos canais disponíveis para a transmissão de dados (AUGUSTO et al., 2006).

Na técnica OFDM, a resolução deste problema dá-se pela técnica de transmissão que utiliza meios de modulação que permitam a superposição das bandas laterais dos sinais consecutivamente enviados. Na OFDM, estas portadoras se sobrepõe sem que haja interferência mutua

entre elas. Isso torna desnecessária a utilização de bandas de guarda entre as subportadoras para separamento na recepção, originando um ganho de até 50% em relação a FDM (PINHEIRO, 2005).

Figura 3 – OFDM x FDM (AUGUSTO et al., 2006)

É uma técnica vantajosa que proporciona uma maior taxa de transmissão de dados e é benéfica em ambientes que requerem a resolução de problemas de interferência entre as frequências e de ruído impulsivo. Esta esta técnica também apresenta-se robusta em ambientes onde a transmissão é vulnerável a desvanecimento seletivo em frequência (PINHEIRO, 2005).

As dificuldades encontradas na utilização desta técnica de modulação de dados são o sincronismo das portadoras, a sensibilidade aos desvios de frequência e a contínua necessidade de amplificação do sinal (PINHEIRO, 2005).

2.1.2.3 Controle de Acesso ao Meio

Um dos principais quesitos na comunicação sem fio é o compartilhamento de acesso ao meio. No padrão 802.11, os protocolos usados para gerenciar esta função são chamados de funções coordenadoras de acesso ao meio e pertencem a camada Medium Access Control (MAC). Existem três protocolos principais responsáveis pelo controle de acesso ao meio: Distributed Coordination Function (DCF) Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), DCF Request to Send and Clear to Send (RTS/CTS) e Point Coordination Function (PCF).

Segundo (YOUSSEF; MILLER, 2012), pode-se dividir estes proto-

colos de acordo com a seguinte estrutura de funcionamento das redes.

1. Modo Basic Service Set (BSS): Refere-se ao conjunto de dispositivos wireless que se comunicam entre si e com outras redes através de um intermediário (*Access Point*). Neste modo apenas o intermediário roda o algoritmo de controle de acesso ao meio.

2. Modo Independent Basic Service Set (IBSS): Refere-se ao conjunto de dispositivos que se comunicam entre si sem a presença de um agente intermediário na comunicação (*Access Point*). Neste modo todos os dispositivos rodam o algoritmo de controle de acesso ao meio.

As redes inseridas no modelo de comunicação BSS (baseadas no modelo infraestruturado) utilizam o protocolo PCF e seu esquema de funcionamento será desconsiderado devido a incompatibilidade com o projeto (ALABADY; SALLEH; HASIB, 2014)‘

No contexto do modelo de comunicação distribuída IBSS, onde estão inseridas as redes Ad hoc, tema de estudo do presente trabalho, encontram-se os protocolos com função de coordenação distribuída DCF (CSMA/CA) e DCF (RTS/CTS).

2.1.2.3.1 DCF (CSMA/CA)

Este método de acesso ao meio é definido pelas seguintes características (YU; QIN, 2008):

- Evita-se a colisão através do mecânismo denominado *backoff*;
- Período de tempo mínimo entre pacotes consecutivos.

Em uma rede com controle de acesso ao meio definido pela implementação do modelo CSMA/CA, o funcionamento ocorre da seguinte maneira: a partir do momento que um nó transmite através da rede, qualquer outro nó que perceba esta transmissão deverá permanecer em silêncio e aguardar a transmissão encerrar-se para tentar o acesso ao meio (HARGREAVES, 2017).

Esta sensibilidade de perceber as transmissões na rede pode ocorrer tanto fisicamente como virtualmente, através de mecanismos físicos e virtuais. No mecanismo físico, adotado pelo modelo CSMA/CA, o dispositivo verifica se a rede está sendo utilizada. No virtual, esta

verificação é dada através da distribuição de informações reservadas utilizando-se do método RTS/CTS. Os dispositivos podem operar simultâneamente em ambos os modos (HARGREAVES, 2017).

O CSMA/CA é o modo básico de operação do 802.11. Nele, os dispositivos monitoram o canal de transmissão quando desejam enviar dados e, segundo (YOUSSEF; MILLER, 2012), procedem da seguinte forma em relação ao estado de atividade do meio:

1. Meio desocupado: Dispositivo monitora o canal por um período de tempo denominado DCF Interframe Spacing (DIFS) e então, após monitorar o canal, caso este estado de ociosidade do meio persista após este intervalo de tempo, o dispositivo transmitirá o *DATA frame*.

2. Meio ocupado: Dispositivo monitora o canal e aguarda o término da transmissão. Após o término, o dispositivo monitora o canal pelo intervalo de tempo DIFS. Se o meio vir a ser desocupado durante este intervalo de tempo, inicia-se um temporizador denominado *backoff*, sendo este um mecânismo cuja atribuição é aguardar adicionalmente um intervalo de tempo aleatório para minimizar a probabilidade de uma nova colisão. Caso o meio permaneça livre durante este intervalo adicional *backoff*, o dispositivo, então, transmite o *DATA frame*. Caso o meio venha a ser ocupado durante o intervalo de *backoff* o temporizador é pausado e não resetado. O dispositivo aguarda o meio tornar-se livre novamente, espera pela ociosidade do meio durante um intervalo DIFS e inicia o *backoff* novamente, porém decrementando-o à partir do instante em que ele foi pausado. O dado só será enviado após o intervalo de *backoff* ser expirado.

Para evitar que um dispositivo específico monopolize a utilização do canal, cada dispositivo inicia um contador sempre que enviar dois ou mais pacotes consecutivos (HARGREAVES, 2017).

No processo de recebimento, quando dado dispositivo recebe um *DATA frame*, ele aguarda por um intervalo de tempo Short Interframe Spacing (SIFS). Após este intervalo, transmite um ACK ao emissor para confirmar o recebimento do *DATA frame*. Este procedimento de confirmação de recepção é necessário pois o emissor não consegue identificar colisões na transmissão. É impossível o emissor enviar e escutar

o meio ao mesmo tempo (HARGREAVES, 2017).

Não há algoritmo de *backoff* ou verificação do meio no processo de envio de ACKs. O emissor passará a retransmitir caso nenhum ACK tenha sido recebido durante um período específico de tempo (HARGREAVES, 2017).

2.1.2.3.2 DCF (RTS/CTS)

Neste modo de operação, o processo de transmissão é semelhante até certo ponto. Após o dispositivo verificar que o meio está ocioso durante o intervalo de tempo DIFS e executar o algoritmo de *backoff*, ainda envia um quadro de reserva Request to Send (RTS) ao emissor, antes de iniciar a transmissão do *DATA frame*, contendo a duração de envio do pacote.
Após o emissor receber o pedido de reserva do canal (através do RTS) e conhecer a duração da transmissão, ele aguarda um período de tempo SIFS e envia um quadro de confirmação denominado de Clear to Send (CTS), notificando ao dispositivo emissor que ele poderá iniciar a transmissão do *DATA frame*. O dispositivo, após receber o CTS, aguarda um intervalo de tempo SIFS e inicia a transmissão (YU; QIN, 2008).

Os demais dispositivos que não participam diretamente da transmissão também recebem o RTS/CTS e utilizam-se destas informações para atualizarem seus vetores de alocação da rede Network Allocation Vector (NAV). Através disto, os dispositivos que não participam da transmissão não necessitam monitorar constantemente o meio, apenas quando este vetor estourar. Esse monitoramento do vetor de alocação da rede é o método virtual de percepção do meio (YOUSSEF; MILLER, 2012).

O mecânismo RTS/CTS reduz o número de colisões e resolve o problema de terminal escondido. Sendo assim, seu desempenho é considerado superior ao do modo básico CSMA/CA (YOUSSEF; MILLER, 2012).

2.1.2.4 Especificações Técnicas

Segue um comparativo entre as especificações técnicas de diferentes padrões do protocolo 802.11 de interesse (SHARMA; SAXENA, 2013).

Característica	**802.11 a**	**802.11 b**	**802.11 g**	**802.11 n**
Espectro (GHz)	5	2.4	2.4	5/2.4
Taxa de dados (Mbps)	54	11	54	600
Modulação	OFDM	DSSS	OFDM	OFDM
Compatível (802.11 x)	nenhum	a	b	b/g/n
Desvantagem	Alcance baixo	Taxa de dados baixa	Número de redes Limitadas	Dificuldade de Implem.
Vantagem	Alta taxa de dados	Alto alcance Maturidade	Alta taxa de dados	Muito alta taxa de dados

2.2 TECNOLOGIAS DE MONITORAMENTO HÍBRIDAS

São tecnologias que possuem capacidade de atender as especificações de aplicações de monitoramento *indoor* e *outdoor*, sendo projetadas para coexistir entre estas delimitações referenciais.

A tecnologia Zigbee possui resultados experimentais inferiores em termos de alcance do sinal. Devido a isso, é limitada à aplicações *outdoor* de curto alcance e aplicações *indoor*, sendo amplamente utilizada no monitoramento de sensores.

A tecnologia WiMAX, por sua vez, possui longo alcance e pode atender os requisitos de comunicações *outdoor*, desde que exista a infraestrutura necessária ao seu uso. Entretanto, sua concepção de característica híbrida provém das pretensões advindas de sua implementação, cujo foco são aplicações de usuários *indoor*.

2.2.1 ZigBee (IEEE 802.15.4)

2.2.1.1 Definição

A tecnologia Zigbee é o padrão industrial mais popular de redes Mesh sem fio para conectividade de sensores, instrumentação e controle de sistemas. A tecnologia *Zigbee* especifica as camadas físicas e

de controle de acesso ao meio para prover a comunicação de dados nas Wireless Personal Area Networks (WPAN) através de uma arquitetura de fácil utilização, segura e confiável (KINNEY, 2009).

Sua existência deve-se à necessidade explicita de um padrão de comunicação que atendesse às especificações estritamente associadas as redes de sensores. Sensores e aplicações de controle e monitoramento de dados não necessitam alta largura de banda, porém possuem algumas necessidades fundamentais para sua operação.

Segundo (TOMAR, 2011), a tecnologia Zigbee é o padrão global referência em redes de sensores através da provisão dos seguintes recursos:

- Baixo consumo de energia (bateria dura período compreendido entre meses e anos);
- Facilidade de Implementação;
- Simplicidade operacional (o que implica em facilidade de implementação e baixo consumo);
- Alta escalabilidade (praticamente não há restrição quanto ao número de dispositivos);
- Protocolo simples (o que implica em custo reduzido, interoperabilidade e facilidade de manutenção);
- Implementação global (maior produção/investimento e portabilidade global dos dispositivos).

A Zigbee ganhou espaço pela sua viabilidade em redes com baixa taxa de dados através do seu baixo custo de aquisição da infraestrutura, instalação e manutenção. Essas características voltadas às redes de sensores ganham ainda mais expressão em comparação as redes cabeadas, as quais requerem um maior investimento para implementação e manutenção, possuem maior exposição e risco de danificação em relação a estrutura física (cabeamento de dados) e nenhuma portabilidade (C et al., 2011).

2.2.1.2 Aplicações

Segundo Tomar (2011), algumas aplicações da tecnologia Zigbee incluem:

- Automação residencial e industrial;
- Monitoramento em aplicações da medicina;
- Serviços de telecomunicação;
- HVAC (aquecimento, ventilação e sistemas ar-condicionados);
- Periféricos eletrônicos;
- Controle e monitoramento de processos;
- Aplicações de segurança.

2.2.1.3 Topologia

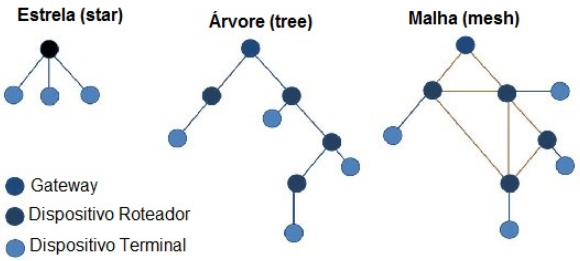


Figura 4 – Topologias Zigbee

Segue a descrição de cada topologia, segundo C et al. (2011).

2.2.1.3.1 Estrela

Consiste em um coordenador e um número arbitrário de dispositivos terminais. Nesta topologia, o modelo mestre-escravo (*master-slave*) é adotado, sendo o dispositivo master o coordenador que possuí função completa e o *slave* o dispositivo terminal, que possuí suporte à ambas as funções (função reduzida ou função completa). Nesta topologia os dispositivos terminais só se comunicam na rede através do coordenador. Isso limita a rede a não prover comunicação em múltiplos saltos e comunicação em malha (*Mesh Networking*).

2.2.1.3.2 Árvore

É similar à topologia estrela com exceção à comunicação entre os dispositivos terminais, que podem comunicar-se entre si. Esta topologia facilita a expansão geográfica da rede.

2.2.1.3.3 Malha

Nesta topologia, todos os nós podem estabelecer comunicação com os demais nós que estiverem dentro de seu alcance. É mais robusta e tolerante a erros, porém complexa em termos de manutenção.

2.2.1.4 Especificações Técnicas

Segue a tabela de especificações da tecnologia Zigbee (TOMAR, 2011).

Parâmetros	**Zigbee**
Frequência (GHz)	2.4
Padrão (IEEE)	802.15.4
Alcance (m)	Ambiente Interno: ∼30 Ambiente Externo: ∼100
Consumo de Corrente	25-35mA (Tx) 3uA (modo ocioso)
Taxa de Dados	250kbps
Tamanho da Pilha do Protocolo	32kb 4kb (funções limitadas)
Tempo Estimado de Conexão	30ms (tipicamente)
Técnica de Modulação	DSSS
Largura de Banda (mínimo requerido)	3 MHz (estática)
nós (máximo por rede)	64K
Número de Canais	16

Tabela 2 – Tabela de especificações do padrão 802.15.4

2.2.2 WiMAX (IEEE 802.16)

2.2.2.1 Definição

A tecnologia Worldwide Interoperability for Microwave Access (WiMAX) faz parte do conjunto de tecnologias Broadband Wireless Access (BWA), que são tecnologias banda larga sem fio. Tem como propósito expandir a internet globalmente para dispositivos portáteis, promovendo conectividade à internet e compatibilidade/interoperabilidade aos dispositivos através de um padrão que promete ser muito difundido e capacitado em pouco tempo.

Prospecta-se que esta tecnologia possibilite a utilização da internet e seus serviços, com alta taxa de dados, e abrangendo localizações, até então, consideradas remotas, como as últimas milhas, que são caracterizadas pela existência de pontos distantes, difíceis de serem interligados.

O objetivo da WiMAX é proporcionar acesso à internet em qualquer localização e resolver o problemas da inacessibilidade em pontos distantes das infraestruturas de telecomunicação, em cujos quais, as operadoras acabam ignorando a prestação de serviço pela incapacidade ou inviabilidade de estabelecimento de conexão entre estes pontos e seus links de acesso à internet. Destaca-se, neste cenário, pela sua capacidade de cobertura de longas distâncias e baixo custo de implementação da infraestrutura necessária para prover a conectividade entre estes pontos e a internet (SEYEDZADEGAN; OTHMAN, 2013).

2.2.2.1.1 Propostas e desafios

Na WiMAX, o acesso é permitido, assim como nas demais Wireless Metropolitan Area Network (WMAN), através de antenas externas nas estações rádio base. Este acesso ainda possui desafios a serem enfrentados, assim como outros parâmetros que afetam diretamente a qualidade e desempenho da tecnologia. Segundo (LIMA et al., 2004), em consequência dessas problemáticas, o 802.16 (através do IEEE) apresenta algumas propostas e desafios, que são descritos abaixo.

Usualmente 50% a 70% dos usuários em áreas urbanas, nas redes metropolitanas, não possuem visada direta ao ponto de acesso da rede sem fio. Isto ocorre devido a enorme quantidade de edifícios, árvores, pontes e construções que se concentram nestas regiões. Nestas condições, a qualidade na transmissão do sinal é severamente afetada. Apesar de os prédios refletirem uma parte do sinal, contribuindo para alcançar pontos diretamente inacessíveis, estas reflexões causam atenuação do sinal em certas faixas imprevisíveis de frequência. Diante disto e dessas dificuldades, o protocolo deve conseguir contornar estas perdas devido à atenuação.

Os protocolos da camada física Direct-Sequence Spread Spectrum (DHSS) e Frequency-Hopping Spread Spectrum (FHSS) necessitam de visada direta para funcionarem corretamente. Portanto, o WiMAX utiliza o protocolo Orthogonal Frequency Division Multiplexing (OFDM), que diferentemente dos anteriores, transmite mais de uma portadora, ele transmite centenas de portadoras simultâneamente. Essa técnica é positiva, pois somente necessita-se que uma fração dessas portadoras atinja o receptor para que a informação possa ser recuperada e permite comunicar-se, sem visada, em distâncias de até 6km, apenas beneficiando-se das reflexões.

Aplicações WMAN podem conectar milhares de usuários, principalmente tratando-se de regiões metropolitanas, em grandes cidades. Ao fornecer acesso a esta enorme quantidade de usuário várias variáveis precisam ser consideradas: desempenho, segurança, qualidade de serviço, etc. A escalabilidade e o real dimensionamento destas redes implicam em maior dificuldade de manutenção da qualidade do serviço oferecido.

Uma das medidas de desempenho essenciais é a relação entre a banda obtida para cada Hz utilizado. Esta medida traz informações acerca do tráfego em Bps (bits por segundo) permitido na rede, devido a limitação de uso existente na faixa de frequência. O WiMAX fornece 5 Bps/Hz, praticamente o dobro do aproveitamento do espaço de frequências em comparação ao padrão 802.11 (a/g).

Devido a projeção de tráfego de voz e vídeo e, para manter a qualidade de operadora para estas finalidades, o WiMAX foi projetado com recursos de priorização, controle/garantia de banda e qualidade de serviço em todos seus elementos.

Inclui os protocolos criptográficos Triple-DES (128bits), RSA (1.024 bits) e recurso à certificação digital, proporcionando segurança ás informações transmitidas.

2.2.2.2 Aplicações

Conforme Guainella et al. (2007), algumas aplicações da tecnologia WiMAX incluem:

- Backhaul móvel;
- Segurança pública;
- Redes 4G;
- Monitoramento de ambientes;
- Prevenção de incêndios;
- Telemedicina;
- Promover conectividade em áreas remotas.

2.2.2.3 Topologia

Segundo Andrews, Ghosh e Muhamed (2007), seguem as topologias suportadas pela arquitetura WiMAX:

Topologia estrela: Consiste em um coordenador e vários dispositivos terminais. Nesta topologia, os dispositivos terminais comunicam-se apenas com o coordenador e qualquer comunicação entre os dispositivos terminais deve passar pelo coordenador. É uma topologia simples, de fácil implementação, porém com a desvantagem de a comunicação estar condicionada ao funcionamento dos coordenadores.

Topologia árvore: Consiste em um nó central, coordenador e diversos roteadores interligados aos dispositivos terminais. Os dispositivos terminais podem apenas conectar-se aos roteadores ou coordenadores.

2.2.2.4 Especificações Técnicas

Esta tecnologia promete superar a tecnologia 3G por oferecer os seguintes parâmetros otimizados: agilidade na transmissão de dados, flexibilidade, cobertura e taxa de transferência de dados. Sendo considerada, por estes aspectos e pela sua viabilidade, uma evolução da tecnologia Wi-Fi e 3G (LIMA et al., 2004).

Seguem as especificações do padrão WiMAX (MOHAMED; ZAKI; MOSBEH, 2010).

Tabela 3 – Tabela de especificações do padrão 802.16

Parâmetros	WiMAX
Padrão (IEEE)	802.16
Largura do Canal	Variável <= 28 Mbps
Faixa de Espectro	10-66 GHz
Taxa de Dados	240 Mbps
Alcance	12-15 Km
Multiplexação	FDM/TDM
Transmissão	SC
Mobilidade	Veícular (802.16e)
Vantagens	Taxa de transferência/Alcance

2.3 TECNOLOGIAS DE MONITORAMENTO OUTDOOR

Até pouco tempo, a tecnologia mais adequada seria a utilização de módulos GSM/GPRS. Assim, cada módulo sensor estaria conectado a um módulo GSM/GPRS, habilitado em uma operadora de telefonia e, através deste, seria capaz de enviar dados por 3G/2G/Edge para um servidor na Internet. O problema destes módulos é o custo individual da unidade GSM, do chip da operadora de telefonia (custo mensal) e da necessidade de cobertura em toda a área de operação. Em aplicações (como no rastreamento de rebanho) em que o sistema deve operar com baterias, o uso de GSM/GPRS tem mais um ponto negativo, que é o alto consumo de energia do mesmo.

No caso de sistemas outdoor, existem duas tecnologias recentes que despertam atenção: LoRa e SigFox. Essas tecnologias são diferentes em vários aspectos mas tem como semelhança a característica de apresentar um baixo consumo de energia e, também, uma pequena largura de banda.

Aplicações típicas dessas tecnologias seriam para monitoramento de sensores com transmissão de dados a longas distãncias (na ordem de quilômetros), sendo que a transmissão de dados é pouco frequente (digamos uma amostra a cada 10 minutos) e ocorre a poucos bits por segundo (250bps até 21.9Kbps) (SOARES; BARRIQUELLO, 2017).

2.3.1 LPWAN (Low-Power Wide-Area Networks)

As conexões entre dispositivos podem estar sujeitas, frequentemente, à locais inacessíveis por certas tecnologias previamente difundidas (bluetooth, zigbee e BLE). Além disso, diversas aplicações requerem ampla cobertura de sinal e baixo consumo de energia para sua concepção. A demanda elevada em função destas aplicações vinculou a pronta necessidade de surgimento de tecnologias capazes de prover a transferência de um conjunto limitado de dados, em links de longa distância, entre dispositivos IoT, à baixo custo. Este conjunto de tecnologias são classificados como Low-Power Wide-Area Networks (LPWAN).

As tecnologias, LPWAN, baseiam-se na otimização dos seguintes parâmetros: consumo de energia entre dispositivos terminais, volume de dados enviados por unidade de tempo, maximização da área de cobertura e custo dos dispositivos terminais.

Segundo Raza, Kulkarni e Sooriyabandara (2017), os fatores mais críticos nas LPWAN são:

- Arquitetura da rede;
- Alcance da comunicação;
- Tempo da vida da bateria;
- Robustez a interferência;
- Capacidade da rede (números de nós);
- Segurança da rede;

- Comunicação unidirecional vs bidirecional;
- Variedade de aplicações oferecidas.

As tecnologias LPWAN possuem, em comum, a necessidade de contornar as restrições encontradas pelo uso destas bandas. Fatores como a resiliência à interferência e todos os demais citados são constantemente aprimorados por estas tecnologias através da otimização técnica das suas funcionalidades.

Além destas comparações técnicas, que obviamente são fatores críticos importantes ao diferenciar as tecnologias existentes, há outros fatores que exercem forte impacto entre estas tecnologias. Pode-se destacar o modelo comercial peculiar à cada uma delas. É sobre esse prisma que as empresas buscam diferenciar estas tecnologias que possuem muito em comum, por pertencerem à uma mesma classe de interesse tecnológico. É fundamental, tendo ciência disto, analisar as tecnologias LPWAN sobre a perspectiva de modelo comercial.

As LPWAN estão tendo um crescimento vertiginoso graças ao modelo comercial empregado, que facilita o desenvolvimento imediato das tecnologias, oferecendo suporte à massiva adesão dos usuários através de seus modelos comerciais distintos. Um provável segundo fator preponderante para o desenvolvimento das LPWAN é o custo extremamente acessível para desenvolvimentos das redes em bandas não licenciadas.

Esta seção visa abordar algumas das principais questões que devem ser levadas em consideração na diferenciação destas tecnologias, como as citadas abaixo (PETAJAJARVI et al., 2016):

- Flexibilidade de uso (variedade de aplicações existentes);
- Segurança do protocolo de comunicação;
- Aspectos técnicos (anteriormente citados);
- Custos (implantação da rede, nós terminais e bateria);
- Ecossistema de soluções oferecidas para modelos comerciais flexíveis;
- Disponibilidade da tecnologia e produtos terminais (produtos de prateleira);

- Potencial do ecossistema para garantir qualidade e longevidade a solução implementada.

Conforme Sigfox (2017), segue um panorama da estimativa feita, sobre as conexões LPWAN, para o ano de 2024:

Figura 5 – Estimativa LPWAN

2.3.2 LoRaWAN (IEEE 802.11ah)

2.3.2.1 Definição

LoRaWAN é um protocolo de comunicação que utiliza-se da tecnologia LoRa e surgiu como solução potencial em aplicações para a Internet das Coisas IoT, em redes sem fio. Suas especificações de longo alcance, simplicidade estrutural e o consumo de energia extremamente reduzido (duração estimada superior a 10 anos) possibilitam a implementação de diversos tipos de serviços em locais amplos e variados (ADELANTADO et al., 2017).

Utiliza LoRa Radio/Chipset e aproveita-se dos benefícios de sua camada física, que permite a comunicação em links de longas distâncias. As funcionalidades adicionadas pelo protocolo LoRaWAN compreendem serviços da camada de rede, sendo assim um complemento à tecnologia LoRa (ADELANTADO et al., 2017; AUGUSTIN et al., 2016).

A robustez de seu protocolo/arquitetura de rede determinam o longo período de duração da bateria, segurança e a variedade de aplicações de rede suportadas (AUGUSTIN et al., 2016).

2.3.2.1.1 LoRa

Existe uma grande variedade de tecnologias *wireless* que utilizam a modulação Frequency-shift keying (FSK) na camada física. Isto deve-se à sua eficiência na modulação de sinais atingindo baixo consumo, utilizando a minima potência possível para envio dos dados. LoRa é baseada na modulação Chirp Spread Spectrum (CSS), a qual mantém a mesma característica em relação a potência do sinal da modulação FSK, porém com aumento significativo da distância de alcance do sinal na comunicação (PETAJAJARVI et al., 2015; INFO, 2017).

A tecnologia CSS tem sido usada há décadas na comunicação espacial e na comunicação militar devido ao alcance longo do sinal e também a alta imunidade à interferências. Entretanto, LoRa é o primeiro registro de utilização desta tecnologia, à baixo custo, em escala comercial (KHUTSOANE et al., 2017).

A sua arquitetura é projetada para prover um equilíbrio entre o alcance do seu sinal e a consequente cobertura oferecida, consumo de energia e taxa de dados. Assim como nos demais métodos de espelhamento espectral, o CSS utiliza toda a largura de banda alocada na transmissão de um sinal, o que torna-o robusto em relação à presença de ruídos no canal. A utilização de uma faixa ampla do espectro de transmissão também o permite ser mais resistente à ocorrência de desvanecimento de múltiplos caminhos, mesmo operando em potências baixas (KHUTSOANE et al., 2017).

A capacidade de cobertura do sinal é o seu grande diferencial. Através dela, um único *gateway* (estação base) pode cobrir zonas muito extensas, como cidades inteiras ou centenas de quilômetros quadrados (VEJLGAARD et al., 2017).

LoRa possui a melhor média de potência fornecida através do meio de comunicação utilizado, considerando-se os ganhos e perdas de potência entre o percurso transmissor-receptor (TX e RX). Isto condiciona a tecnologia a cobrir países com um custo ínfimo de infra-estrutura (ALLIANCE, 2015).

2.3.2.1.2 Protocolo LoRaWAN

O protocolo LoRaWAN foi projetado com o objetivo de otimizar as LPWAN em suas seguintes atribuições: tempo de vida da bateria, capacidade de nós, alcance e custo.

Enquanto LoRa especifica as atribuições da camada física, propiciando, por exemplo, o alcance da comunicação, como previamente descrito, LoRaWAN refere-se às especificidades do protocolo de comunicação e arquitetura desenvolvidas para as aplicações. Possui maior influência no tempo de vida da bateria, capacidade da rede, qualidade do serviço, segurança, leque de aplicações suportadas, etc.

A faixa de frequência utilizada pelo LoRaWAN (excepcionalmente nas Américas) varia de 902MHz a 928MHz. Apesar dessa regulamentação, a tecnologia LoRa opera em um considerado amplo espectro de frequências sobre as faixas de frequência não licenciadas. Havendo, assim, mais opções para evitar a utilização excessiva de uma mesma frequência por vários dispositivos (ADELANTADO et al., 2017; SILVA et al., 2017).

Isso é importante no monitoramento da interferência por dispositivos vizinhos. Existe a possibilidade de várias redes LoRaWAN particulares estarem operando em uma mesma localidade, ocasionando uma região concentrada de sobreposição de sinais. Já na Sigfox, apenas haverá uma rede por localidade, o que minimiza esta interferência.

2.3.2.2 Modulos LoRaWAN

Em relação aos módulos de desenvolvimento, a tecnologia LoRaWAN possuia módulos exclusivos de sua proprietária, a empresa francesa Semtech. Porém, recentemente, as fabricantes STMicro e Atmel ingressaram neste mercado como parceiras da Semtech e a tecnologia deixou de ser exclusivamente fabricada pela empresa detentora da tecnologia.

Em termos de desenvolvimento, a LoRa oferece uma API baixo-nível altamente configurável, possibilitando uma escala maior de otimizações. Isso é excelente, porém torna mais complicada a integração dos módulos LoRa por possivelmente possuírem implementação distinta em

determinado nível.

2.3.2.3 Modelo Comercial

Sobre o modelo comercial, como a Sigfox é uma operadora de rede, deve-se esperar a sua implantação e pagar uma taxa de assinatura para utilizá-la. Já com a LoRa, há a possibilidade de implantação de sua própria rede, de forma imediata, sem taxa de inscrição. Há vantagens em implantar uma rede própria, a principal delas é definir a área de cobertura de acordo com o seu interesse.

Em relação aos serviços disponíveis, na tecnologia LoRa existêm diversos provedores, enquanto na tecnologia Sigfox existem apenas a Sigfox e os parceiros licenciados.

Apesar de existirem empresas construindo redes LoRa, com a possibilidade de integração de regiões mais amplas, não há a necessidade de aguardar esta alternativa - a menos que a aplicação demande de uma cobertura amplamente interligada, tal como uma rede municipal, regional ou até nacional.

2.3.2.4 Arquitetura/Topologia LoRaWAN

Na arquitetura Mesh, os nós terminais individualmente propagam as mensagens. Atuam como roteadores, difundindo a rede, disseminando as mensagens aos demais nós de forma a aumentar o alcance da comunicação e expandir a topologia da rede.

Essas redes alcançam longas distâncias, porém isso adiciona complexidade à rede, reduz a capacidade da rede e o tempo de vida das baterias, pois os nós recebem mensagens dos demais nós que são, tipicamente, irrelevantes para si. Eles atuam, invariavelmente, na comunicação sem necessariamente estarem associados a ela, o que faz-se necessário em comunicações de curto alcance.

No caso de comunicações de longo alcance, como a LoRaWAN, a topologia estrela, de longo alcance, faz mais sentido, afim de preservar o uso de bateria dos nós, comunicando-se de forma mais direta.

Para este tipo de topologia ser viável, o *gateway* deve possuir uma capacidade de recebimento de mensagens considerável (irá receber mensagem de uma quantidade alta de nós). Para isso, os *gateways* utilizam transceptores multicanal multi-modem, fazendo com que as mensagens simultâneas sejam recebidas em múltiplos canais (LORIOT; ALJER; SHAHROUR, 2017).

Alguns fatores críticos para esta capacidade são: taxa de dados, frequência de envio e número de canais simultâneos. O *gateway* utiliza-se da técnica de modulação por espalhamento espectral, na qual os sinais são praticamente ortogonais entre si, para adotar fatores de espelhamento como o fator de propagação. À medida em que este fator é alterado, a taxa de dados é alterada proporcionalmente. Desta forma, o *gateway* consegue receber várias taxas de dados, no mesmo canal, ao mesmo tempo, otimizando a capacidade de recebimento de mensagens (LORIOT; ALJER; SHAHROUR, 2017).

Há uma adaptação na taxa de dados, encurtando-se o tempo de vida de certas mensagens no ar, permitindo outros nós transmitirem simultaneamente e aumentando o tempo de vida útil da bateria dos nós.

Segue a ilustração da arquitetura LoRaWAN:

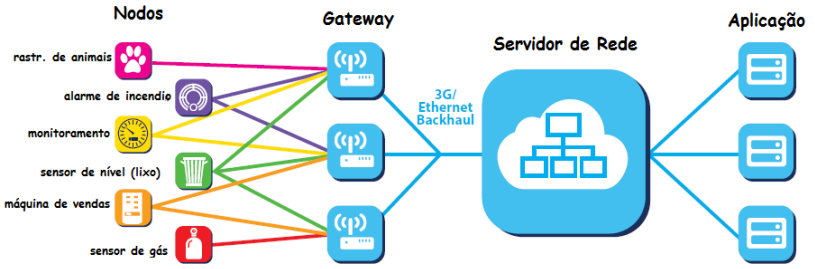


Figura 6 – Arquitetura LoRaWAN (ALLIANCE, 2015)

Na arquitetura LoRaWAN, os nós não estão associados a um único *gateway*. Ao enviar um dado, o nó o envia para múltiplos *gateways*. Estes *gateways*, cada um deles, propagam a mensagem recebida dos nós para o servidor de rede, geralmente hospedado na núvem, utilizando-se, como *link*, os backhauls, que podem ser compostos por Wi-Fi, Ethernet, satélite ou antenas celulares e interligam o núcleo da

rede às sub-redes periféricas.

A complexidade envolvida no gerenciamento da rede é atribuída ao servidores de rede, que atuam na camada de rede verificando a redundância de pacotes, assegurando a segurança na comunicação, adaptando a taxa de dados e demais funções lógicas que otimizam a performance da rede.

2.3.2.5 Comunicação e troca de mensagens

Neste protocolo, os *gateways* comunicam-se com os nós e os nós comunicam-se com as redes WMAN, diretamente. O protocolo LoRaWAN possui múltiplos canais de recebimento, podendo receber 8 (oito) mensagens simultâneas através de múltiplos canais de frequência. A rede opera em um modo de transmissão assíncrona e possivelmente o *gateway* pode não estar apto a receber todas as mensagens (ADELANTADO et al., 2017; AUGUSTIN et al., 2016).

Os módulos LoRa podem operar de modo bi-direcional, diferentemente dos módulos Sigfox, o que lhe fornece uma vantagem competitiva em certos cenários. Usando o mesmo módulo de rádio, o receptor pode passar a transmitir dados e vice-versa, a qualquer momento. Isso lhe propicia a flexibilidade de se adaptar e controlar a transmissão, se adaptando a cenários onde esta situação é conveniente.

A respeito da transmissão de mensagens na rede, segundo o autor Augustin et al. (2016), os nós possuem três classes:

Figura 7 – Classes de comunicação LoRaWAN (ALLIANCE, 2015)

LORAWAN CLASSE A Os nós terminais não esperam um evento ou determinado período para enviar as mensagens, eles comunicam quando há necessidade. A capacidade teórica de transmissão em uma rede classe A (Aloha pura) é de 18,4%, devido as colisões que ocorrem quando mais de um nó decide transmitir ao mesmo tempo, no mesmo canal de frequência, e com as mesmas configurações de rádio.

LORAWAN CLASSE B A cada 128 segundos, o *gateway* transmite um *beacon* e os nós recebem um intervalo de tempo de 129 segundos, dentro deste intervalo - eles também são informados quando devem ouvir as mensagens transmitidas pelo *gateway*. Neste intervalo concedido ao nó ocorre a permissão de uma transmissão de mensagem *downlink*.

LORAWAN CLASSE C Esta classe permite que os nós enviem uma mensagem de *downlink*, a qualquer momento, e os nós, por sua vez, escutam constantemente. É necessário muita energia para permitir que os nós executem a função de recepção de mensagens constantemente e, por isso, necessita-se de alimentação privilegiada.

2.3.2.6 Limitação da Razão Cíclica

É uma limitação inerente às bandas de frequência utilizadas que possui amplo impacto em relação à operação destas redes à medida que cresce o número de nós (ADELANTADO et al., 2017).

Em termos de interferência, existe a possibilidade de várias redes LoRa particulares estarem operando em uma mesma localidade, ocasionando uma região concentrada de sobreposição de sinais. Já na Sigfox, apenas haverá uma rede por localidade, o que minimiza a interferência.

Na Europa, por exemplo, há a limitação de transmissão de mensagens pelo gateway em 99% do tempo. Ou seja, apenas 1% do tempo o gateway poderá transmitir mensagens. Nos Estados Unidos não há essa limitação e, no Brasil, ainda está em processo de elaboração sua regulamentação(ADELANTADO et al., 2017).

2.3.2.7 Aplicações

São cenários recorrentes de aplicações desta tecnologia (ADELANTADO et al., 2017):

- Agricultura Inteligente
  - Monitoramento de umidade do solo;
  - Monitoramento da saúde do gado;
  - Sensores inteligentes do solo;
  - Irrigação Autônoma.
- Cidades Inteligentes
  - Sensores de Inundação;
  - Sistema viário coletivo inteligente;
  - Iluminação de rua inteligente;
  - Gestão Inteligente de Resíduos;
  - Redes comunitárias residenciais.
- Ecossistemas Inteligentes
  - Comunicação sobre desastres naturais;
  - Proteção de espécies ameaçadas;
  - Monitoramento do sistema de água.
- Inteligência associada a saúde
  - Acompanhamento de pacientes com Alzheimer;
  - Localização de pacientes com demência;
  - Vestimentos inteligentes para crianças e idosos;
  - Detecção de queda;
  - Geladeira médica.
- Edificações inteligentes
  - Evacuação de incêndio;
  - Gestão doméstica inteligente;
  - Monitoramento de eletrônicos e dispositivos;

  - Monitoramento da energia;
  - Segurança residencial.

- Monitoramento inteligente
  - Gestão inteligente de água e gás;
  - Rede elétrica urbana inteligente;
  - Monitoramento industrial;
  - Monitoramento de áreas rurais.

- Logística inteligente
  - Recuperação de veículo furtado;
  - Monitoramento de containers;
  - Rastreamento de cargas.

A tecnologia LoRaWAN possui algumas limitações, no entanto, que a impedem de ser aplicada em certos casos, sendo a principal delas a baixa taxa de transferência de dados. Devido a isso, desconsidera-se seu uso, por hora, em implementações de aplicações em tempo real e monitoramentos determinísticos (ADELANTADO et al., 2017).

2.3.2.8 Segurança

Existem duas camadas de segurança: a camada de rede e a da aplicação. A camada de segurança de rede é responsável pela autenticação dos nós na rede. A camada de aplicação é responsável por assegurar que o usuário da rede não tenha acesso aos dados da aplicação dos usuários.

Para assegurar a integridade dos dados utiliza-se chave criptográfica AES-128 bits. Todos os dispositivos precisam criptografar as mensagens utilizando este protocolo de segurança para o envio das mensagens (ALLIANCE, 2015).

Conforme Alliance (2015), segue abaixo a figura que ilustra o esquema de segurança implementado pela tecnologia LoRaWAN:

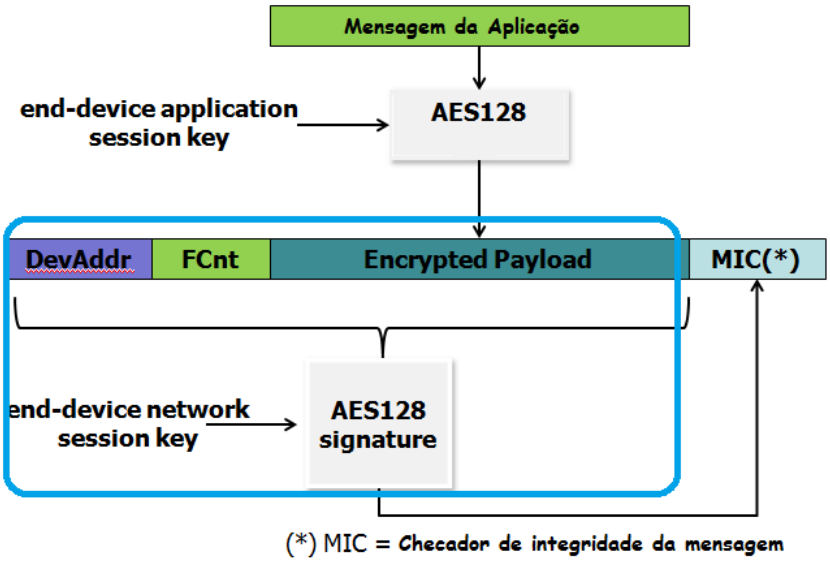


Figura 8 – Segurança LoRaWAN (JUNIOR, 2016)

2.3.2.9 Especificações Técnicas

Segundo Alliance (2015), seguem as especificações técnicas da tecnologia LoRaWAN:

Característica	LoRaWAN
Modulação	SS Chirp
Largura de banda Rx	500-125 KHz
Taxa de Dados	290bps - 50Kbps
Max.# msgs/dia	Ilimitado
Max Potência de Saída	20 dBm
Link Budget	154 dB
Duração da bateria	105 meses
Eficiência (energia)	Muito alta
Imunidade à interferência	Muito alta
Coexistência	Sim
Segurança	Sim
Mobilidade/Localização	Sim

2.3.3 SigFox

2.3.3.1 Definição

Sigfox foi desenvolvida especialmente para dispositivos com baixa taxa de transferência de dados, sendo excelente para situações onde a transmissão é pouco frequente. As mensagens Sigfox são limitadas em 12 bytes, enquanto na tecnologia LoRa, o usuário pode definir arbitrariamente o tamanho da mensagem. A única imposição é devido a restrição em relação ao tempo de permanência no ar, para cada mensagem, especificado em 5 segundos, via regulamentação - o que restringe o tamanho das mensagens (RIBEIRO et al., 2018).

Sigfox caracteriza-se por ser uma tecnologia de longo alcance que possui proposta relevante para os dispositivos IoT, principalmente pela sua capacidade de cobertura, que abrange longas distâncias. Contudo, esta tecnologia, deveras recente, apresenta limitações severas, devido, principalmente, a sua incapacidade de transmitir dados com frequência. Apesar destas limitações de utilização, seus benefícios vem a calhar com os interesses de um conjunto extenso de aplicações onde a necessidade de transmitir pequenas quantidades de dados, ocasionalmente, por longas distancias, se faz presente.

Sua tecnologia de rádio Ultra Narrow Band (UNB) utiliza-se de um espectro amplamente estreito (<1KHz) para transmitir dados a longa distância, otimizando a potência de transmissão disponível e, sobretudo, assegurando uma comunicação confiável, até mesmo em canais com presença de ruídos e interferência, devido à sua intrínseca baixa sobreposição ao ruído (SIGFOX, 2017).

Esta característica de transmissão, resiliente às intempéries próprias dos canais de comunicação, torna ainda mais relevante a escolha da tecnologia de transmissão UNB - já que a transmissão é feita através da Industrial Sientific and Medical (ISM), que é uma banda livre e passível de interferência em larga escala (SIGFOX, 2017).

Em relação ao alcance de seu sinal, apresenta uma excelente cobertura em áreas externas e mesmo nas internas. Em uma região de 8000km2, o estudo realizado resultou na cobertura de mais de 99% dos usuários nas áreas externas e 95% nas áreas internas, com 20dB de

perda por penetração nas áreas internas (VEJLGAARD et al., 2017).

Outra consideração relevante deste estudo é a probabilidade de bloqueio de uso da tecnologia Sigfox, que ocorre quando o serviço é negado devido a falta de recursos para sua efetivação, a qual apresentou-se elevada. A tecnologia apresenta 2% de probabilidade de bloqueio para um dispositivo IoT por usuário e esta taxa cresce para mais de 20% para a quantidade de dez dispositivos por usuário. A probabilidade de violar a taxa de *duty cicle* para até dois dispositivos por usuários é inferior a 1%, porém cresce para 15% para dez dispositivos por usuário (VEJLGAARD et al., 2017).

A principal limitação envolvendo a utilização da tecnologia é o seu ciclo de operação (*duty cicle*), cujo termo corresponde a fração de tempo em que o dispositivo estará ativo. Esta tecnologia possui restrições na disponibilidade temporal de uso do seu meio de comunicação (ar). Na Europa, por exemplo, o uso do meio de transmissão utilizando a frequência de 868MHz (banda ISM) está restrito à fração de 1% do tempo. Esta restrição pode variar de 0.1% a 10%, por hora, na banda ISM, de acordo com a região de utilização. Nestas condições (1%), o dispositivo Sigfox poderá transmitir dados por apenas 36 segundos a cada hora. Como a tecnologia possui uma média de tempo no ar, para cada pacote, equivalente a 6 segundos, isso resultaria em um máximo de seis mensagens com carga de 4, 8 ou 12 bytes, por hora, o que limita a viabilidade de diversas aplicações, restringindo sua utilização a conjuntos específicos de atividades (VEJLGAARD et al., 2017).

2.3.3.1.1 Acesso Aleatório

É um dos pontos principais para a tecnologia atingir a qualidade de seu serviço. A transmissão é assíncrona entre o *gateway* e o dispositivo. O dispositivo emite uma mensagem em uma frequência aleatória e, após isso, emite duas réplicas dessa mensagem em frequências e tempos diferentes (SIGFOX, 2017).

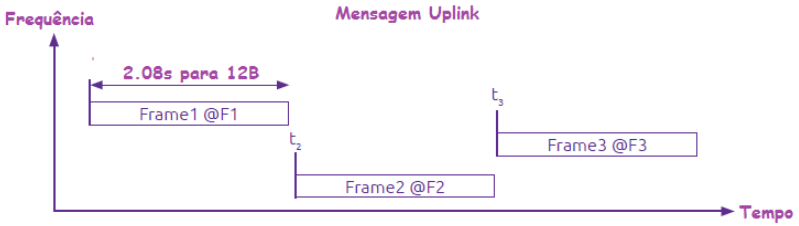


Figura 9 – Esquema do acesso aleatório na Sigfox (BRASIL, 2017)

2.3.3.1.2 Recepção Cooperativa

Um nó não está associado, unicamente, a uma única estação base, diferente dos protocolos celulares. As mensagens são recebidas por quaisquer estações bases dentro do alcance do nó. Em média, nas redes Sigfox, há três estações bases próximas para cada nó, havendo, de tal maneira, uma diversidade de receptores para cada transmissão (SIGFOX, 2017).

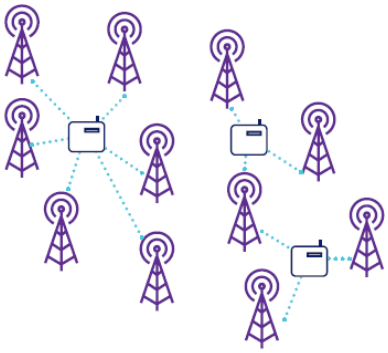


Figura 10 – Ilustração da Recepção Cooperativa na Sigfox (BRASIL, 2017)

2.3.3.2 Arquitetura/Topologia Sigfox

Nesta tecnologia, os nós enviam os dados às estações bases. As estações bases utilizam o *backhaul*, geralmente constituído por um link

primário DSL e um link secundário 3G ou 4G como alternativa para enviar as mensagens aos servidores que estão concentrados no núcleo da rede. Estes servidores processam as mensagens, descartando as réplicas recebidas. Uma interface web e a API permitem aos usuários acessar estas mensagens (SIGFOX, 2017).

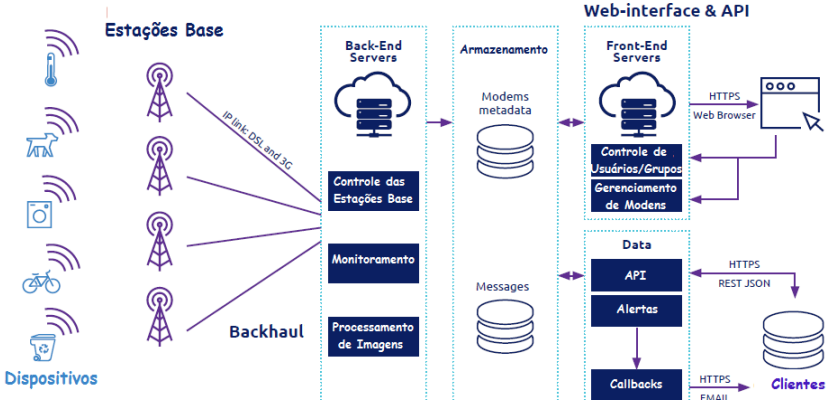


Figura 11 – Arquitetura na Sigfox (BRASIL, 2017)

2.3.3.2.1 Modelo Comercial Sigfox

Atualmente, a escolha é amplamente pautada em termos do modelo comercial distinto entre as tecnologias e a área de cobertura, porém ambas as tecnologias devem evoluir suas propriedades visando buscar diferenciais que possibilitem o estabelecimento do domínio no cenário IoT.

Devido a diferentes estratégias de mercado, a tecnologia Sigfox fornece uma API simples para integrar ao módulo rádio, sendo assim bastante estrita sua otimização. Já a tecnologia LoRa oferece uma API baixo-nível altamente configurável, possibilitando uma escala maior de otimizações. Isso é excelente, porém torna mais complicada a integração dos módulos LoRa por possivelmente possuírem implementação distinta em determinado nível.

2.3.3.3 Módulos Sigfox

Em relação aos módulos de desenvolvimento, a Sigfox, desde o princípio, após compartilhar o seu *design* de referência, optou pela política de conferir aos fornecedores de *chips* a possibilidade de expandir a tecnologia e participar do desenvolvimento da mesma. É possível encontrar vários fabricantes de *chips* Sigfox.

2.3.3.4 Aplicações

- Cidades inteligentes (Smart Cities);
- Construções inteligentes (Smart Buildings);
- Agricultura;
- Indústria;
- Segurança;
- Monitoramento;
- Energia e utilidades afins.

2.3.3.5 Especificações Técnicas

Segundo Sigfox (2017), seguem as especificações técnicas da tecnologia Sigfox.

Característica	**Sigfox**
Frequência	**SS Chirp**
Alcance	**30 a 50 Km (Áreas rurais)** **3 a 10 Km (Áreas urbanas)**
Taxa de transferência	**100 bps**
Tamanho do pacote	**12 bytes**
Consumo de energia	**Muito baixo**
Duração (bateria de 2.5Ah)	**20 anos**
Uplink/Downlink	**mono/bi-direcional**
Frequency Hopping	**Suporta**
Segurança/Privacidade	**Alta**

3 ALGORITMOS DE ROTEAMENTO EM REDES AD HOC

3.1 REDES AD HOC

As redes Ad hoc são conceitualmente conhecidas e pesquisadas há muito tempo. Anteriormente conhecidas como redes de múltiplos saltos, assim como diversas outras áreas de pesquisa, sua difusão progrediu em consonância com a intensidade de interesse da sociedade e das tecnologias associadas ao seu desenvolvimento.

Apesar de sua peculiaridade, por flutuar em meio à áreas correlacionadas e ser dependente da demanda de implementação de tecnologias paralelas, sobretudo as que permitiram a proliferação das redes sem fio e sua competitividade com as redes ethernet, sua visibilidade e pesquisas tornaram-se proeminentes nos últimos anos com o avanço das redes sem fio e suas tecnologias.

As redes Ad hoc surgiram através da necessidade de prover comunicação a um conjunto de dispositivos (possivelmente móveis) em ambientes sem infraestrutura de comunicação disponível e sem predeterminação da organização dos links de comunicação. Nestas redes não há um elemento central de comunicação tampouco uma topologia fixa existente que possa ser pré-determinada sem necessidade de alterações constantes (KAUR; SALUJA, 2014).

Coexistem em uma rede Ad hoc a eventual necessidade de os dados serem propagados de ponta a ponta na rede, independentemente da quantidade de dispositivos existentes na rede e a presunção de impossibilidade de comunicação direta entre todos os nós pertencentes. A estas atribuições de funcionamento nas redes Ad hoc e em decorrência destas características intrínsecas do modelo de comunicação existente fundamenta-se seu estudo (RAMANATHAN; REDI, 2002).

Nas redes Ad hoc, os dispositivos são os próprios responsáveis pelo roteamento dos dados e devem ser capazes de propagar as mensagens entre si alcançando qualquer nó da rede. Eles estabelecem a conectividade entre os dispositivos através da descoberta dinâmica de nós aos quais possam comunicar-se diretamente, criando-se assim links (rotas) de comunicação que associadamente constituem a rede de co-

municação em sua disposição integral. Também são agentes quanto ao reconhecimento de alterações na topologia da rede e verificação/seleção de rotas (RAMANATHAN; REDI, 2002; WU; STOJMENOVIC, 2004).

3.2 ALGORITMOS DE ROTEAMENTO EM REDES AD HOC

O objetivo principal deste capítulo é abstrair as funcionalidades e entender os mecânismos dos principais algoritmos de comunicação em redes sem fio Ad hoc.

A escolha de privilegiar o estudo de algoritmos de redes Ad hoc deu-se devido à sua característica funcional, baseando-se nas seguintes premissas identificadas: não possuírem elementos centrais de gerenciamento (cada nó atua como um roteador), independer de uma infraestrutura prévia que possibilite o compartilhamento de dados na rede, serem algoritmos bases de redes de sensores, etc.

Essas características referenciadas foram de encontro ao interesse de aplicação do projeto. Isso motivou o interesse em conhecer os principais algoritmos da área, suas métricas, funcionamentos, abordagem, etc.

Este capítulo busca identificar os conceitos fundamentais de implementação de algoritmos em redes Ad hoc e o levantamento do conhecimento necessário para o desenvolvimento de um modelo de comunicação conveniente ao sugerido pelo projeto, atingindo as características pretendidas para o roteamento dos dados na rede.

A função crítica da camada de rede é o roteamento. É a principal função desta camada e sua descrição pode ser sintetizada pela sua finalidade: a atribuição de rotear pacotes da máquina de origem para a máquina de destino através de boas rotas (KUROSE; ROSS, 2010; TANENBAUM, 2003).

Um algoritmo de roteamento atua como agente responsável por prover o melhor roteamento disponível e fornecer diretrizes, políticas e critérios para o estabelecimento destas rotas e as demais rotinas lógicas que envolvem o alcance de sua finalidade. É a parte do software da camada de rede responsável pela decisão sobre a linha de saída a ser

usada na transmissão do pacote de entrada (TANENBAUM, 2003).

Segundo Tanenbaum (2003), o algoritmo de roteamento deve ser capaz de aceitar as alterações na topologia e no tráfego sem exigir que todas as tarefas de todos os *hosts* sejam interrompidas e que a rede seja reinicializada sempre que algum roteador apresentar falha.

Além de tornar a rede ininterrupta e resiliente às alterações no tráfego, os algoritmos devem condicionar a otimização dos parâmetros que envolvem a comunicação entre os dispositivos na rede.

Neste sentindo, Tanenbaum (2003) descreve seis propriedades que são desejáveis em um algoritmo de roteamento: correção, simplicidade, robustez, estabilidade, equidade e otimização.

Pode-se exemplificar à partir destes parâmetros:

- Suporte a escalabilidade (robustez);
- Identificação e correção na quebra de links entre as rotas (correção);
- Convergência no funcionamento independente do tempo de operação. Tem-se como exemplo evitar que ocorra sobrecarga de processamento em função do tempo de funcionamento da rede (estabilidade);
- Controle na perda de pacote, melhoria no tempo estimado para obtenção das melhores rotas, encaminhamento dos pacotes em menor prazo, etc. (otimização);
- Consideração lógica eficiente na escolha das melhores rotas (equidade).

3.3 ALGORITMOS DE ROTEAMENTO REATIVOS EM REDES AD HOC

Os protocolos reativos têm a característica comum de apenas iniciar o processo de descobrimento de rota quando necessário. Imediatamente após determinado nó da rede necessitar enviar um pacote até o destino inicia-se o processo de descobrimento de rota. Este nó requisita a rota até o destino aos nós intermediários entre a origem e o

destino, quando existentes (ROYER; TOH, 1999).

Este processo só terminará quando:

1. O pacote é entregue ao destinatário;
2. O pacote é entregue até um nó que conhece a rota até o destino;
3. Todas as permutações de rota possíveis terem sido percorridas.

Uma vez descoberta a rota até o destino, estes algoritmos a mantém para possíveis futuros envios até este mesmo destinatário. Esta rota só será descartada ou alterada caso algum dos nós torne-se inacessível a partir de todas as rotas de envio mantidas pelo nó emissário.

A implementação deste modelo gera uma maior latência na resposta instantânea à requisição quando os destinos são desconhecidos, entretanto gera uma menor sobrecarga (*overhead*) na rede - haja vista que a rede só é inundada por pacotes de manutenção de rotas à partir de requisições. Essa propriedade os caracteriza como algoritmos que atuam sob demanda (RAUT; AMBULGEKAR, 2013).

3.3.1 DSR (*Dynamic Source Routing*)

3.3.1.1 Definição

É um protocolo *on-demand* de roteamento de dados simples e eficiente projetado para suportar ambientes com alta taxa de mobilidade entre os nós e, preferencialmente, ser utilizado em redes com aproximadamente 200 (duzentos) nós (JOHNSON; MALTZ; BROCH, 2001a).

Fornece mecânismos de descoberta e manutenção de rotas em redes de múltiplos saltos, conforme seu modelo de roteamento reativo, possibilitando a autonomia na organização e configuração do roteamento na rede. Sua configuração permite ainda que os nós mantenham múltiplas rotas até os destinos, sendo estes responsáveis pelo controle e seleção do uso e armazenamento destas rotas (JOHNSON; HU; MALTZ, 2007).

Deve-se atentar a relevantes considerações na escolha do protocolo de rede DSR:

- Concentra-se bastante no uso das rotas a partir da origem e nas rotas armazenadas em cache.
- É possível observar que a comunicação vai ganhando consistência e torna-se otimizada à medida em que a rede atinge um elevado grau de utilização, com um maior número de rotas definidas pelos nós.
- A rede não deve falhar constantemente e/ou os nós precisam ser geograficamente estáticos, pouco alterados, já que isso provocaria uma maior ocorrência de rotas incompatíveis e inacessíveis, forçando os nós a utilizarem a varredura e descoberta de rotas, gerando um aumento de *overhead* na rede. Este problema ganha representatividade e complexidade maior de ser administrado em redes maiores, com muitos nós, já que as rotas possuem um maior número de nós e, portanto, há maior chance de uma falha ocorrer durante o percurso do trajeto.

Conforme Johnson, Maltz e Broch (2001b), cada tipo de mensagem carrega conjuntos de informações chave distintos, tais como limite de saltos/TTL (RREQ) na busca por rotas, endereço de *broadcast* para solicitação de rotas, tipo de erro, etc. E alguns campos elementares:

- Unique ID (identificação exclusiva do pacote);
- Endereço do nó de origem;
- Endereço do nó destino;
- Endereço dos nós pertencentes a rota percorrida;
- Rota a ser percorrida.

A característica funcional principal do protocolo DSR é o uso do roteamento na origem (JOHNSON; HU; MALTZ, 2007).

3.3.1.2 Funcionamento

3.3.1.2.1 Processo de Descobrimento de Rotas

Quando um nó na rede pretende enviar um pacote de dados a um nó destinatário, cujo mesmo possui sua rota desconhecida pelo nó

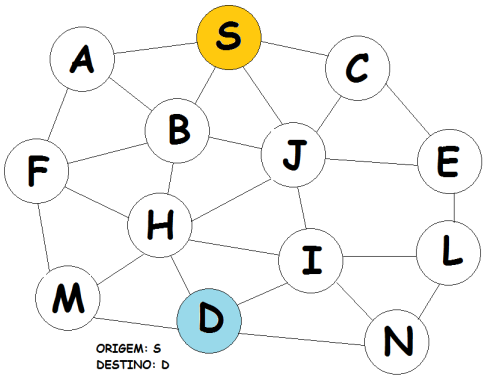


Figura 12 – Configuração Inicial da Rede

emissor, conforme ilustra a figura 12, ele inicia um processo de descobrimento de rota para determinar dinamicamente a rota até o mesmo.

Este processo funciona através de uma inundação de pacotes de requisição de rota Route Request Package (RREQ) na rede. A figura 13 ilustra o envio do pacote RREQ para os nós adjacentes ao nó de origem (nós [A,B,J,C]), requisitando conhecimento acerca do caminho até o nó D.

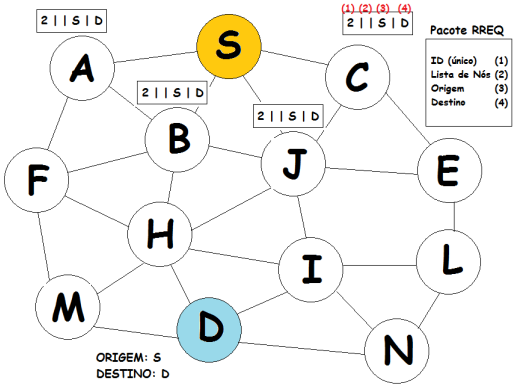


Figura 13 – Inundação dos pacotes RREQ

Os nós, que ainda não conhecem o caminho até o nó D (figura 14) dão continuidade ao processo de descobrimento de rota, transmitindo o pacote RREQ para os seus nós adjacentes.

A figura 14 apresenta o cenário final de envio de requisição aos nós adjacentes ao nó de origem, onde os nós próximos à origem, por não saberem o caminho até o nó D, propagam o pacote de requisição os nós adjacentes a si. O nó de origem também recebe os pacotes de requisição dos nós adjacentes a ele, porém estes são posteriormente descartados - justifica-se isto pelo fato de o envio ser feito por *broadcast*.

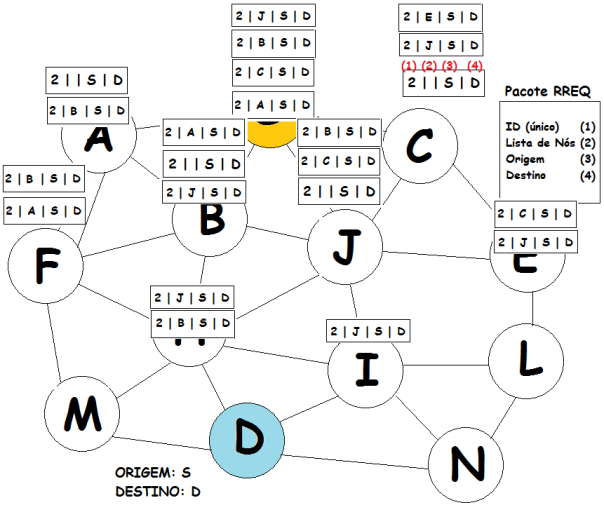


Figura 14 – Propagação dos pacotes RREQ

3.3.1.2.2 Descarte de Pacotes

Verifica-se, após o cenário inicial, que há uma inundação de pacotes RREQ e que os nós precisam descartar os desnecessários para evitar a propagação de pacotes redundantes na rede. Para isso, existe o item ID (único), para que os nós possam identificar a unicidade do pacote e, à partir disso, consigam excluir os pacotes redundantes. É o que ocorre na próxima etapa. De acordo com a figura 15, os nós descartam os pacotes repetidos propagando os que chegaram de forma antecedente.

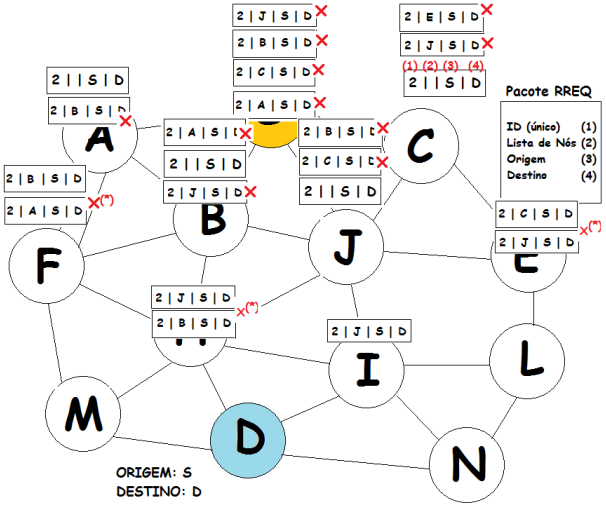


Figura 15 – Descarte dos pacotes redundantes

Esse processo de inundação e descarte dos pacotes RREQ segue até que o nó encontre o destinatário, conforme a figura 16.

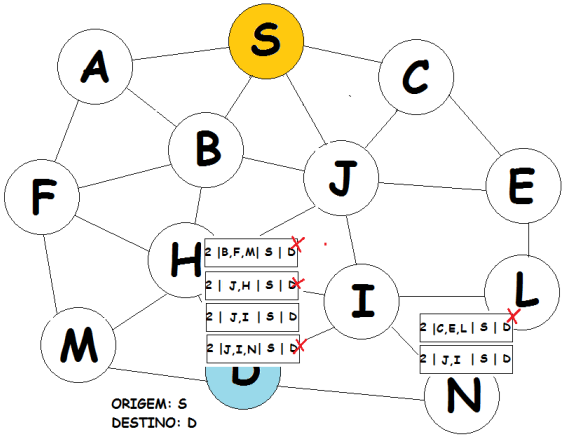


Figura 16 – Cenário final de RREQ

3.3.1.2.3 Casos Especiais

1. nó é o próprio destinatário

Neste caso não há porque retransmitir o pacote, haja vista que o mesmo já chegou ao seu destino. Ele, então, transmite a resposta à requisição de rota através do pacote RREP (*Route Reply Package*), contendo a rota até si.

Essa rota retransmitida é armazenada durante o processo de requisição de rotas. O RREQ constrói o caminho percorrido através da rede até chegar ao destinatário. A resposta a requisição de rotas RREP utiliza-se desse caminho percorrido e armazenado no conjunto de informações do pacote RREQ para transmitir a si próprio até a origem, atravessando esse caminho construído de forma reversa. Essa rota, fornecida agora pelo RREP, é armazenada no cache do nó de origem para uso futuro, quando necessário percorrê-la novamente.

2. nó possui a rota até o destinatário

A rota a partir deste nó é conhecida. Consequentemente, torna-se desnecessário o prosseguimento do processo de descoberta de rotas. Neste caso, os nós respondem a requisição ao nó de origem enviando a rota através do RREP.

3. nó de origem conhece a rota até o nó destinatário (situação optimizada)

O nó emissor (origem) já conhece o caminho de múltiplos saltos, completo, até o destino. Este caminho, por sua vez, já está armazenado no cache de rotas do nó emissor, não sendo necessário efetuar a descoberta da rota.

Assim que as comunicações na rede vão ocorrendo com diferentes nós origem, os nós vão ganhando inteligência na rede e conhecendo as diferentes rotas – à medida em que as descobertas na rede vão aumentando, os nós vão incorporando conhecimento sobre as rotas na rede.

4. Algum nó pertencente a rota deixou a rede temporariamente ou permanentemente

Se ao enviar a mensagem através de uma rota algum nó pertencente a esta rota predefinida se torne intrafegável e, por consequência disto, a

ligação deste caminho "origem-destino" estiver corrompida, o nó emissor (nó de origem) é notificado através de um pacote chamado: *Route Error Package* (RERR).

A origem, à partir da etapa anterior, remove todas as rotas que utilizam este caminho corrompido armazenadas em seu cache. A partir disto, um novo processo de descobrimento de rotas deve ser iniciado pela origem, assim que as rotas excluídas forem necessárias.

3.3.2 AODV (*Ad-hoc On-Demand Distance Vector*)

3.3.2.1 Definição

Foi projetado para prover escalabilidade e desempenho através da redução da disseminação do controle de rotas e eliminação da sobrecarga de processamento na rede (WU; STOJMENOVIC, 2004).

Estas redes, por vezes, demandam alta escalabilidade e podem atingir milhares de nós, sendo este um algoritmo melhor apropriado para uso nestes casos. Uma das principais vantagens sobre a utilização do AODV é a facilidade de inserção/remoção de nós sem praticamente afetar a manutenção das rotas dos demais nós da rede, exceto seus adjacentes. Isto gera uma menor dependência entre os nós em relação a manutenção das rotas. Em função desta característica, este algoritmo consegue lidar bem com a mobilidade dos nós suportando baixas, médias e relativamente as altas taxas de mobilidade (AGGARWAL et al., 2016).

No algoritmo AODV, cada nó mantém uma tabela de rotas contendo informações sobre como chegar até o destino à partir de seus vizinhos. Este mecanismo de descoberta de transmissão estabelece entradas na tabela de rotas de nós contendo informação de roteamento a partir de seus nós adjacentes e se baseia nessa tabela para percorrer a rede (ROYER; PERKINS, 2000).

Diferente do DSR, que armazena em cada nó a rota completa desde a origem até o destino, o AODV armazena informações de rota até o destino somente em relação ao próximo nó adjacente, ou seja, armazena apenas a informação necessária para o próximo deslocamento. Isso gera uma resposta mais rápida à quebra de links em rotas ativas,

além de minimizar os requerimentos de memória necessários à manutenção das rotas da rede (ROYER; PERKINS, 2000)

Segundo (RAMANATHAN; REDI, 2002), são características principais do protocolo AODV:

- Nós armazenam apenas as rotas necessárias;
- Necessidade de *broadcast* é minimizada;
- Reduz requerimentos de memória
- Rápida resposta a quebra de link em rotas ativas;
- Rotas livres de *loops* mantidas pelo uso de número de sequência para o destino;
- Alta escalabilidade.

3.3.2.1.1 Número de sequência

A principal diferença em relação ao DSR é o uso de números de sequência para determinar a atualização do caminho até o destino. Esse número de sequência atua como um *timestamp* (ponto especifico na linha do tempo) assegurando que a melhor rota utilizada esteja sempre atualizada (MAURYA et al.,).

Assim que um nó intermediário recebe um pacote de requisição de rota, ele compara seu número de sequência com o número de sequência do pacote. Caso o seu número de sequência seja maior em relação ao número de sequência do pacote, a rota existente está atualizada e, por consequência disto, a rota do pacote é desconsiderada (AGGARWAL et al., 2016).

Este mecanismo de número de sequência atribuído a cada rota evita que ocorra a situação em que os nós se atualizam entre si em um *loop* infinito, permitindo o reconhecimento deste evento (RAMANATHAN; REDI, 2002).

Todas estas técnicas conjuntas resultam em um algoritmo capaz de responder rapidamente as mudanças de topologia na rede e utilizar a largura de banda de forma eficiente, minimizando o *overhead* da rede referente ao controle e tráfego dos pacotes de dados.

3.3.2.1.2 Gerenciamento da Tabela de Roteamento

Segundo (MANTORO; REZA, 2016), as seguintes variáveis são armazenadas na tabela de roteamento para manutenção e gerenciamento das rotas:

- Endereço IP do nó de destino;
- Numéro de saltos até o nó de destino;
- Próximo salto (informação a respeito dos nós vizinhos pertencentes a rota e que são utilizados para propagar os pacotes de dados);
- Numero de sequência do nó de destino;
- Vizinhos ativos (nós que pertencem à rota ativa);
- Tempo de expiração.

Há dois parâmetros importantes em relação ao tempo de expiração utilizados no protocolo AODV. São eles os temporizadores *route request expiration timer* e *route caching timeout*. O objetivo deste primeiro temporizador é eliminar a manutenção de rotas reversas em nós que não estejam na rota entre a origem e o destino. O valor desse temporizador depende do tamanho da rede Ad hoc. Já o segundo temporizador, é responsável por definir o tempo máximo para uma rota ser considerada válida (ROYER; TOH, 1999).

Cada vez que uma rota é utilizada para transmitir dados de uma origem a determinado destino, o valor de *timeout* da tabela de entrada de rotas é *resetado* para um $valor = tempoatual + tempolimitedarotaativa$ (ROYER; TOH, 1999).

3.3.2.2 Funcionamento

3.3.2.2.1 Processo de descoberta de rota

Seu funcionamento é basicamente semelhante ao do DSR: quando um nó rodando o algoritmo AODV deseja enviar uma mensagem, caso não exista em sua tabela de roteamento nenhuma informação referente ao destino requisitado, ele dá início ao processo de descobrimento de

rotas. Assim como no DSR, esse processo parte da origem de requisição.

Quando o nó da origem não possui informação de rotas sobre o nó destinatário, ele envia um pacote de requisição RREQ através uma mensagem *broadcast* a todos os seus nós adjacentes. Este processo, semelhante ao que ocorre no DSR, é também feito pelos nós intermediários entre o nó de origem e o destinatário e repete-se até que algum deles cheque uma rota válida em sua tabela de roteamento ou atinja o destino pretendido.

Cada nó intermediário que retransmite o RREQ insere sua identificação, de modo a identificar por quais nós o RREQ passou. Se houver uma rota válida, o nó que a pertence envia um pacote RREP de volta a origem, com a rota requisitada. Caso nenhum deles conheça uma rota válida até o destinatário, eles irão repetir o processo de envio de pacotes de requisição aos seus vizinhos, até que o nó destinatário seja alcançado. Assim que o nó destinatário é alcançado, ele retorna um pacote RREP ao nó origem - através do caminho percorrido pelo pacote RREQ até si mesmo.

REVERSE PATH SETUP Conforme o pacote RREQ avança em sentido ao destinatário, através dos nós intermediários entre a origem e o destino, a rota de volta à origem é armazenada em cada nó intermediário.

Na figura 17, pode-se visualizar o envio do pacote de requisição de rotas a partir de A aos nós adjacentes e a propagação deste pacote RREQ até encontrar o destino (nó F). Percebe-se que, conforme os nós propagam o pacote de requisição de rotas ao nó F, eles armazenam a rota percorrida por esse pacote de requisição em sua tabela de entrada de rotas.

Cada nó adjacente responde ao RREQ através de um pacote de resposta à requisição de rota RREP ou retransmitindo a mensagem aos seus nós adjacentes, após incrementar o atributo hop_cnt (contador de saltos).

Caso um nó intermediário não saiba a resposta até o destino ele guarda informações para implementação da rota em direção a origem (*Reverse Path Setup*) e da rota em direção ao destino (*Forward Path Setup*).

Para construir a rota reversa à origem, os nós armazenam o endereço do nó adjacente responsável pelo envio da primeira cópia do pacote RREQ. Esse caminho reverso é mantido por tempo suficiente maior ou igual ao tempo levado para o RREQ atravessar a rede e o RREP ser concebido pelo nó destinatário.

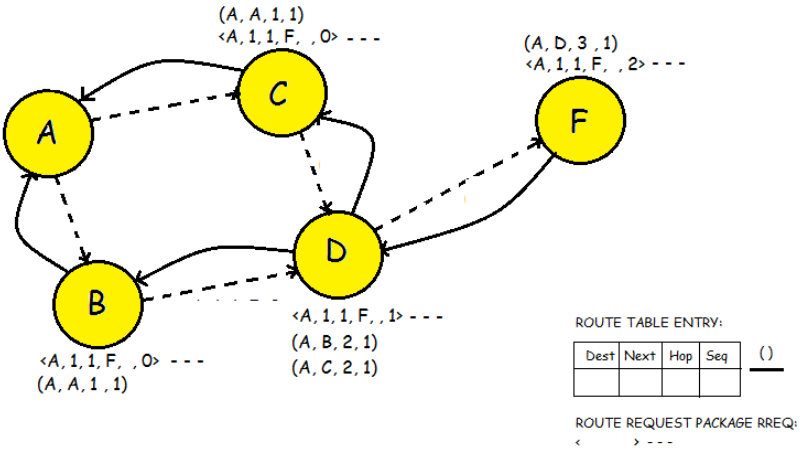


Figura 17 – Esquemático para ilustração do funcionamento do RREQ no protocolo AODV

FORWARD PATH SETUP Possivelmente, um pacote de requisição de rota chegará a um nó que possui a rota até o destinatário antes de atingir ele mesmo. Caso o nó tenha uma entrada de rota para o referido destino, ele irá analisar o número de sequência de destino do RREQ e comparar com o número de sequência de destino que possui em sua tabela de entrada de rotas.

Se o número de sequência de destino do RREQ for maior que o mantido pelo nó intermediário, o nó não deverá usar sua rota para responder ao RREQ e deverá apenas propagar o RREQ, ignorando sua própria informação. Este nó apenas poderá responder à solicitação de rota quando houver em sua tabela de entrada de rotas alguma rota com um número de sequência maior ou igual ao contido no pacote RREQ.

Neste último caso, o nó envia um pacote Route Reply Pac-

kage (RREP) de resposta à solicitação de rota, contendo nele a rota até o destinatário. O envio é feito através de mensagem *unicast* ao nó adjacente que enviou o pacote RREQ solicitando a rota.

No momento em que o pacote RREQ chega até um nó que possui a rota até o nó de destino, há um caminho reverso até a origem mantido na tabela de rotas de cada nó pertencente a rota. De tal maneira, a mensagem poderá ser entregue de volta à origem.

Conforme o pacote RREP trafega a rota de volta à origem, cada nó pertencente a esta rota armazena uma referência do nó que enviou o RREP. Isto é feito através de um *forward pointer*, cuja função é estabelecer a ligação entre os nós. Em caso de futura reutilização desta rota, até este mesmo destino, o nó já possuirá conhecimento sobre o nó adjacente ao qual será enviado o pacote RREQ.

Além da referência armazenada, o nó atualiza a informação própria de *timeout* para atualização das tabelas de entrada de rotas e grava o último número de sequência do destino, para o destino requisitado.

Os nós que não estiverem no caminho percorrido pelo RREP irão acabar estourando os seus valores de *timeout* e deletarão seus *reverse pointers*, de forma a desconstituir-se da rota.

Assim que um nó recebe o primeiro RREP, ele irá propagá-lo à origem que solicitou a requisição de rota. Caso ele receba novamente pacotes RREP para esta rota, ele apenas atualizará a informação a respeito da rota e propagará este pacote RREP se o pacote possuir número de sequência de destino maior que o antigo RREP possuía ou o mesmo número de sequência de destino (*destination sequence number*) e menor valor de número de saltos (*hopcount*).

Este mecanismo diminui a quantidade de pacotes RREP propagados à origem e torna as informações de roteamento mais rapidamente obtidas e atualizadas.

Na figura 18, após o envio do pacote de resposta a requisição, percebe-se que os nós que recebem os pacotes RREP salvam em sua tabela de roteamento a rota até o destino F através da informação do nó adjacente pelo qual o pacote deve ser enviado para atingir o destino F. Ou seja, ele não armazena a rota inteira, porém ele conhece o nó

próximo a si para enviar o pacote quando o destino for requisitado. Os nós também armazenam a informação sobre os nós adjacentes a serem requisitados para atingir o nó A, que requisitou a rota até o destino F.

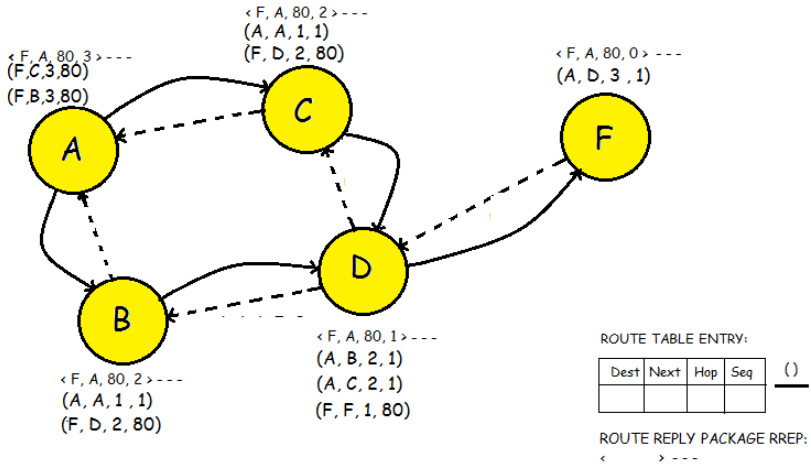


Figura 18 – Esquemático para ilustração do funcionamento do RREP no protocolo AODV

Percebe-se então, que à medida que as rotas vão sendo requisitadas, os nós vão aumentando o conhecimento sobre quais nós próximos a si são responsáveis pela propagação dos pacotes a todos os nós na topologia da rede.

3.3.2.2.2 Quebra de link

Assim como no protocolo DSR, quando há uma quebra de link por algum nó pertencente a rota (seja por mudança em seu posicionamento ou por estar inativo), é iniciado o processo de busca por rotas alternativas. O nó adjacente ao nó que está inacessível, emissor da mensagem, cujo qual detectou a ausência e a impossibilidade de envio, é o nó responsável por enviar pacotes RERR (pacote de erro de mensagem) aos seus vizinhos (nós adjacentes). As rotas serão redefinidas, em consequência disto, a partir do ponto onde houve a quebra de rota.

3.3.2.2.3 Descarte de Pacotes

Cada nó no protocolo AODV possui dois contadores distintos: número de sequência do nó e $broadcast_id$.

A unicidade do pacote RREQ é verificada através dos atributos: $source_address$ (endereço de origem) e $broadcast_id$ (id da mensagem de broadcast). Este atributo $broadcast_id$ é incrementado a cada vez que a origem envia um pacote de requisição de rotas (pacote RREQ).

Assim que os nós recebem pacotes RREQ, eles analisam o atributo $broadcast_id$ e o endereço de origem e, caso o pacote possua o mesmo valor para esses atributos, em comparação aos já recebidos, o pacote é classificado como redundante e é automaticamente descartado pelo nó, evitando a propagação de pacotes redundantes na rede.

3.4 ALGORITMOS DE ROTEAMENTO PROATIVOS EM REDES AD HOC

Algoritmos proativos são *table driven alghoritms*, pois seu funcionamento é conduzido fortemente pela utilização das tabelas de roteamento. Estes algoritmos utilizam mecanismos que visam elevar o conhecimento e a quantidade de informações armazenadas em cada nó a respeito da topologia da rede (VENKATESAN; RAJAKUMAR; PITCHAIKKANNU, 2014).

Nos algoritmos proativos, cada nó é capaz de construir sua própria tabela de roteamento ao adquirir informações da rede e conhece-la à partir do intercâmbio de informação com os demais nós da rede. Eles trocam informação de atualizações de rota entre si de forma regular, desta maneira, possuem suas tabelas de roteamento sempre atualizadas (ALOTAIBI; MUKHERJEE, 2012).

Estes algoritmos possuem algumas definições que precisam ser implementadas para prover atualização/obtenção precisa e frequente de informações da topologia e configuração da rede. São estas:

- Aumento do volume de informações referentes a topologia da rede armazenadas em cada nó da rede;
- Variação dinâmica na quantidade e frequência de atualizações de rotas na rede;

- Otimização da inundação de pacotes na rede.

A ideia central de possuir informação prévia a respeito da topologia da rede armazenada em cada nó é agilizar o processo de envio, pois, nesse cenário, os nós já possuem a rota até o destino de forma imediata, eliminando o *delay* referente ao processo de descoberta de rotas.

A segunda função deste mecanismo é evitar a pronta ocorrência de *loops*, já que estes, caso existam, são detectados e contornados no prévio processo de busca.

A necessidade de implementação de protocolos de roteamento proativos ganha ainda mais evidência em aplicações interativas, cujas quais demandam agilidade na troca de informações entre os nós, tornando os dados da comunicação aproximadamente acessíveis em tempo real.

A atribuição de envio instantâneo deve-se ao mecanismo de cooperação que é utilizado nestes algoritmos. Cada nó pertencente a rede faz atualizações periódicas de rota aos nós alcançáveis por si através do envio frequente de *broadcast* feito pelos outros nós da rede.

Esta otimização possui um preço: a inundação de pacotes de atualização de rotas trocados pelos nós gera um alto *overhead* (sobrecarga de processamento) na rede e requer uma alta largura de banda, de modo a tornar este processo factível e passível de ser implementado.

Além disso, este processo de manutenção das rotas na rede é contínuo, independe da utilização momentânea do nó ou da pronta necessidade de troca de mensagens. Essa continuidade implica em maior consumo de energia em cada nó.

3.4.1 DSDV *(Destination Sequenced Distance Vector Routing)*

3.4.1.1 Definição

É um algoritmo que é baseado no destino e não possui uma visão global sobre a estrutura da topologia. Fácil de implementar, porém só funciona bem quando a rede possuí poucos nós (*overhead* cresce a uma

taxa de O(n2) limitando a escalabiliade) e baixa taxa de mobilidade (HE, 2002).

Por ser proativo, requer atenção quanto ao consumo de energia, que é bastante requisitado. Mesmo estando ocioso os nós executam atualizações frequentes das tabelas de roteamento e, devido a isto, demandam largura de banda e suporte ao consumo quase que ininterrupto de energia (JUN, 2011).

No protocolo DSDV, cada nó possui uma tabela de roteamento que contém endereço IP de todos os destinos disponíveis, endereço IP do próximo salto, o número de sequência gerado pelo nó de destino e as métricas até cada destino - como o *settling time*, que é o tempo de conclusão. Esta tabela contém a menor distância a cada destino e a rota a ser percorrida para atingir o destino (MAHDIPOUR; RAHMANI; AMINIAN, 2009).

Cada nó deve conhecer as seguintes informações através de sua tabela de roteamento (JUN, 2011):

- Todos os destinos disponíveis;
- Próximo nó até o destino;
- Número de saltos até o destino.

Por armazenar rotas em relação a todos os destinos possíveis, ele mantém rotas em sua tabela de roteamento que possivelmente serão desnecessárias por não serem nunca utilizadas.

Seu principal propósito é tratar o problema de *looping* do protocolo de roteamento vetor-distância e adaptá-lo a redes Ad hoc.

3.4.1.1.1 Atualização de Rotas

Cada nó da rede atualiza a tabela de roteamento periodicamente ou imediatamente após uma alteração na topologia ser detectada pela rede. Esta alteração pode ocorrer tanto por quebra de link ou devido a inserção de novos nós.

Apesar de ser um algoritmo que possuí reação imediata a mudanças na topologia, ele demanda um tempo de espera caso as rotas

sejam consideradas instáveis - problema genericamente conhecido como *damping fluctuations*. Este problema de flutuação dá-se pelo critério de atualização de rotas. As mensagem *broadcast* são representadas por um evento assíncrono e, embora espere-se regularidade na ocorrência das mensagens, quando estes eventos são feitos por um número elevado de nós que possuem intervalos diferentes de transmissões, pode haver flutuação no reconhecimento e atualização das rotas (HE, 2002).

Estes nós atualizam a tabela de roteamento após receber um anúncio de que a rede foi modificada. A forma da mensagem pode ser *broadcast* ou *multicast* e propaga-se através de um pacote de atualização da tabela de roteamento, cujo envio dá-se pelos nós que detectam a atualização na topologia.

A atualização da tabela de roteamento inicia com o valor de *hop* (salto) em relação aos nós conectados diretamente ao nó que detecta a alteração na topologia igual a 1 (um). Os nós, que recebem o pacote, incrementam esse valor e este processo é continuado até que todos os nós da rede tenham uma cópia deste pacote, conforme o pacote é disseminado pela rede (HE, 2002).

Este dado de atualização é preservado por um tempo suficiente antes que o nó atualize a rota e a retransmita para os demais nós da rede. Isto é feito para assegurar que o nó receberá várias rotas e certifique-se de que escolherá a melhor rota para cada nó de destino particular, para cada nó da rede.

Caso o nó receba vários pacotes para o mesmo destino, durante o período de espera, ele avaliará os números de sequência de cada pacote e optará pelo que possuir o número de sequência mais recente. Este número de sequência é o parâmetro primordial para a decisão de propagação do pacote.

Caso o nó receba pacotes com mesmo número de sequência para o mesmo nó de destino, a rota que possuir a menor métrica será utilizada e a atual rota existente é automaticamente descartada ou salva como rota alternativa, com menor precedência de utilização.

Assim como no protocolo AODV, no protocolo DSDV ocorre, no processo de atualização da tabela de roteamento, a utilização do artifício de atribuir um número de sequência para verificar se a rota é atual

ou antiga. Este número de sequência é atribuído pelo nó que origina a atualização de rota e serve como identificador único para identificar se a atualização de rota deste nó de origem é atual ou antiga.

Há três casos a ser considerados novamente em relação ao número de sequência:

1. Em caso especifico de um nó qualquer da rede receber um pacote de atualização desta rota de outro nó, que não seja o de origem, o número de sequência deve ser igual ou maior o número de sequência em relação ao mantido na tabela de roteamento.

2. Caso seja menor, esta nova informação de atualização de rota é antiga e deve ser desconsiderada pelo nó receptor.

3. Caso o número de sequência seja igual, a métrica (*settling time*) é comparada para decidir se a atualização é conveniente.

Além das informações métrica e número de sequência, os pacotes de atualização de rota contém ainda o endereço do nó destinatário e o endereço do nó correspondente ao próximo salto.

3.4.1.2 Funcionamento

Conforme He (2002), Jun (2011), Mahdipour, Rahmani e Aminian (2009), segue a descrição do funcionamento do protocolo DSDV:

Na figura 19, os nós apenas tem conhecimento da distância em relação aos nós adjacentes.

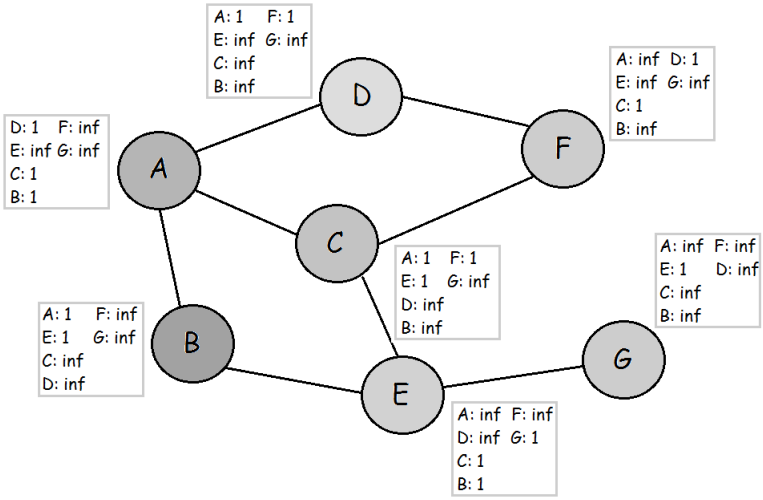


Figura 19 – Rede esquemática para ilustração do AODV

A figura 20 ilustra como ocorre o processo de atualização da tabela de roteamento. O nó A envia a sua tabela contendo informação dos nós adjacentes a si para todos os seus nós adjacentes.

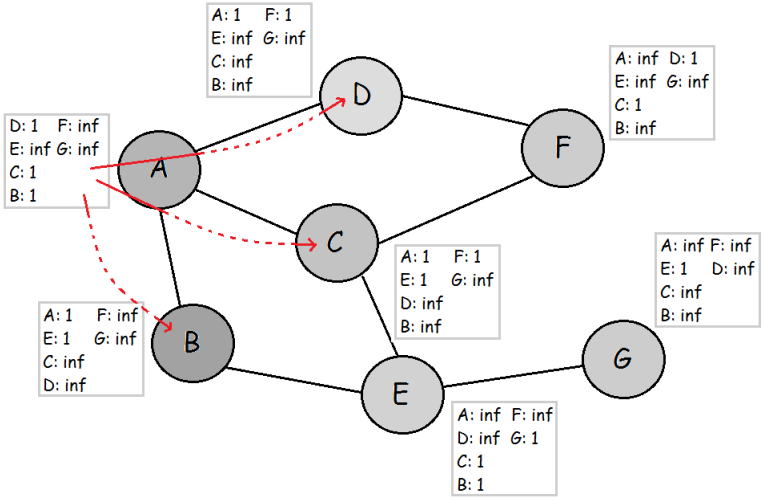


Figura 20 – Envio da tabela para os nós adjacentes

Percebe-se que o nó D não conhece o nó B e C. Assim como o nó C não conhece o nó B e D e o nó B não conhece os nós C e D. A partir do envio da tabela de roteamento do nó A eles passarão a conhecer uns aos outros e cada nó atualizará sua tabela com as novas informações obtidas, conforme a figura 21. Este processo é feito por todos os nós na rede.

Segue a configuração final, conforme ilustra a figura 22.

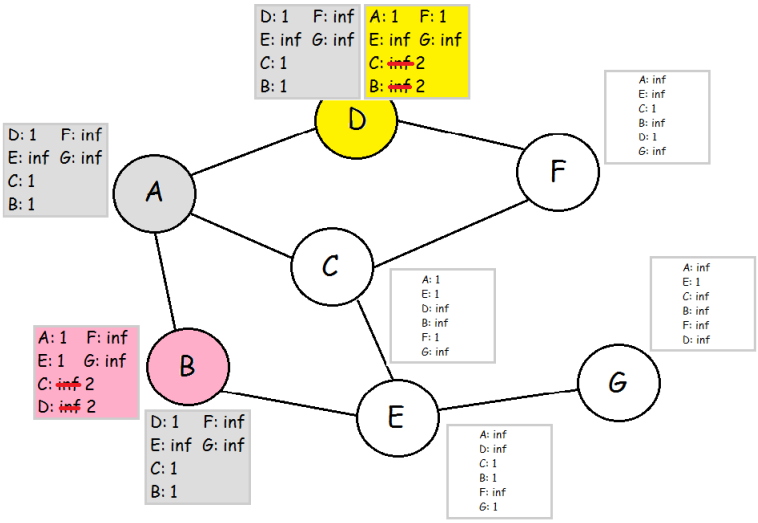


Figura 21 – Considerações após informações obtidas a respeitos dos nós adjacentes

Este processo de difusão de conhecimento é efetuado por todos os nós, através do envio de suas próprias tabelas de roteamento aos nós adjacentes, até que a topologia da rede como um todo seja constituída, de forma cooperativa. A figura 22 ilustra a configuração final da rede, após o compartilhamento das tabelas pelos demais nós da rede.

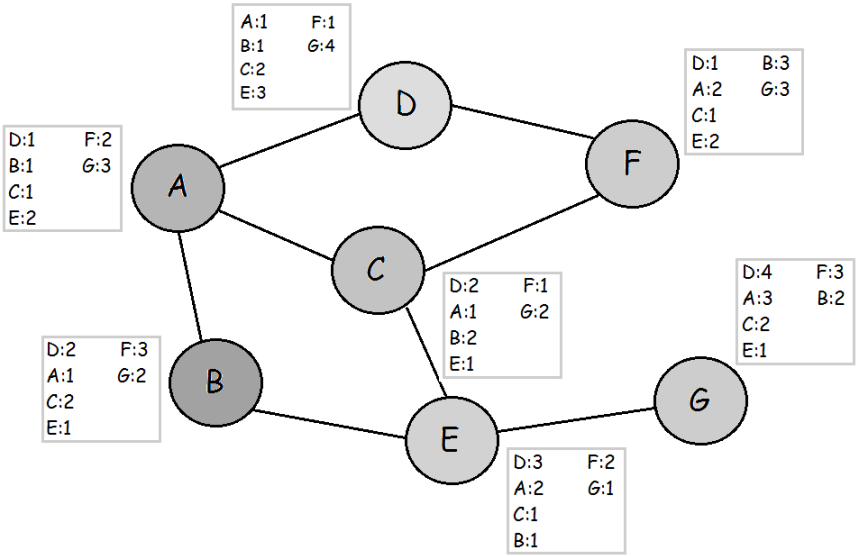


Figura 22 – nós conhecendo a quantidade de múltiplos saltos até cada nó pertencente a rede

Como esperado, todos os nós conhecem todos os nós pertencentes a rede, isso graças a esse processo de cooperação na difusão de conhecimento da topologia da rede.

3.4.2 OLSR (*Optimized Link State Routing Protocol*)

3.4.2.1 Definição

É um protocolo proativo, *table driven*, que possui alta escalabilidade e pode ser utilizado em redes grandes e densas. Essa escalabilidade é possível devido ao seu mecanismo de controle de propagação de tráfego. Apesar de os nós trocarem dados entre si com regularidade, conforme sua característica, de atualização constante de rotas, ele possui um mecanismo que agrega inteligência à este procedimento (JACQUET et al., 2001).

É um protocolo que se adapta bem em redes cujo tráfego de informações é randômico, aleatório e esporádico. Além de transmissões

pouco frequentes prospecta-se, na avaliação de sua implementação, que a rede possua um conjunto grande de nós e que a comunicação não ocorra restritamente a um conjunto pequeno de nós (CLAUSEN; JACQUET, 2003).

Neste protocolo, os nós recebem pacotes de controle contendo dados responsáveis por prover atualização da rede. Há uma inundação, contudo, destes pacotes na rede, isto gera uma sobrecarga na rede, além de consumir muita bateria dos nós, já que cada nó, ao receber estes pacotes de controle, o retransmitem aos seus vizinhos.

Cada nó recebe o mesmo pacote, várias vezes, desnecessariamente, gerando um *overhead* sem sentido na rede. Como o OLSR é um protocolo proativo, este problema é agravado em decorrência da frequente troca de informações à respeito da rede executada pelos nós. As rotas são mantidas, em cada nó, para todos os destinos possíveis, semelhantemente ao protocolo DSDV (CLAUSEN; JACQUET, 2003).

O protocolo OLSR diferencia-se dos demais protocolos proativos pois utiliza Multipoint Relay (MPR) para reduzir este possível *overhead* na rede, reduzindo a quantidade de transmissões necessárias para obtenção de dados na rede. O objetivo deste mecanismo é reduzir a inundação de *broadcasts* através da redução de ocorrência destes nas regiões da rede (JACQUET et al., 2001).

O MPR tem a função de evitar o excesso de pacotes na rede, buscando a minimização desta ocorrência através da seleção dos nós que serão responsáveis por essa inundação. Tem-se, a partir disto, apenas um conjunto de nós selecionados na rede com este propósito, em contraste à situação anterior, onde todos os nós eram emissores.

Cada nó seleciona um conjunto de nós adjacentes para efetuar a transmissão dos dados. Somente estes nós selecionados são responsáveis por trafegar as informações na rede, pelo controle do tráfego de propagação de dados na rede. Nós que tenham sido selecionados como MPR anunciam periodicamente sua função através de suas mensagens de controle (NGUYEN; MINET, 2007).

Este protocolo também utiliza a técnica de atribuição de números de sequência aos pacotes, sendo este o parâmetro para seleção as rotas, provendo a manutenção de rotas atuais no fluxo de mensagem

do algoritmo (CLAUSEN; JACQUET, 2003).

3.4.2.2 Funcionamento

Conforme os autores Nguyen e Minet (2007), Clausen e Jacquet (2003), segue a descrição do funcionamento do protocolo OLSR.

3.4.2.2.1 Escolha dos nós MPR de difusão de mensagens

A escolha dos nós MPR é baseada na premissa de que eles consigam alcançar todos os nós de segunda ordem, de forma a percorrer o menor número de nós possíveis para tal. Através dos MPR, o nó de origem deve alcançar qualquer nó a dois enlaces de distância (NGUYEN; MINET, 2007).

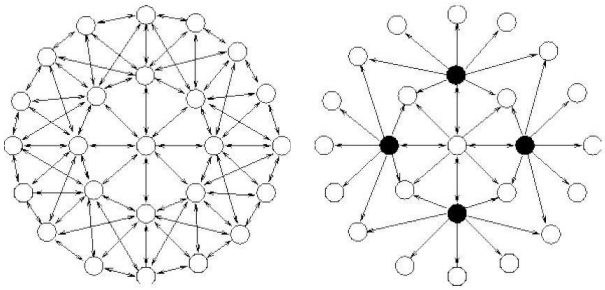


Figura 23 – Propagação no protocolo OLSR sem MPR e com MPR (FLICKENGER, 2006)

3.4.2.2.2 Processo de descoberta de rota

Nesta primeira etapa, conforme ilustra a figura 24, o nó B envia a topologia vista a partir de si para os nós que são adjacentes a ele. Isso é feito através da informações de link que cada nó possui em relação aos nós próximos a si.

A figura 25 ilustra a representação da rede após a propagação da topologia, vista a partir de B, para os nós adjacentes aos nós adjacentes à B. Percebe-se, então, que à partir deste mecanismo, a topologia vista

pelo nó B é, também, conhecida pelos nós que receberam esta informação.

Conforme ilustra a figura 26, o nó A também envia seu conhecimento à respeito da topologia para os nós adjacentes a ele.

A figura 27 apresenta a atualização dos nós à partir dos pacotes enviados. Isso ocorre de modo complementar na figura 28.

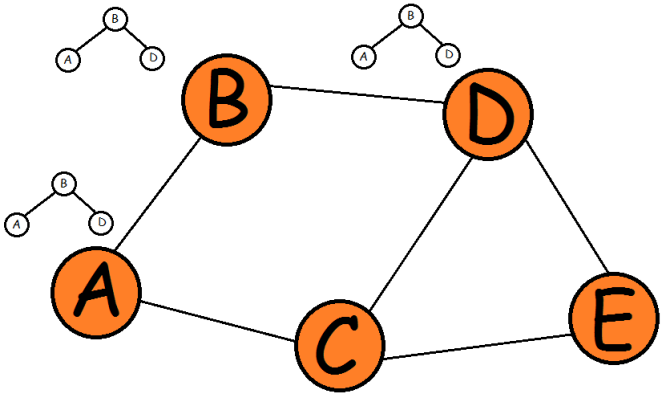


Figura 24 – Envio da topologia vista a partir do nó B

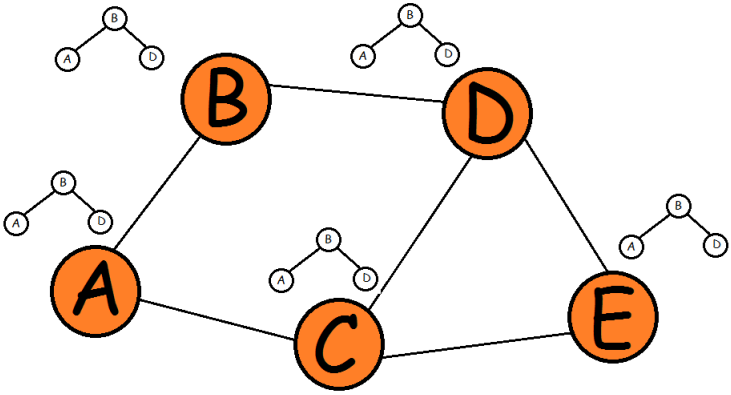


Figura 25 – Retransmissão feita pelos seus vizinhos

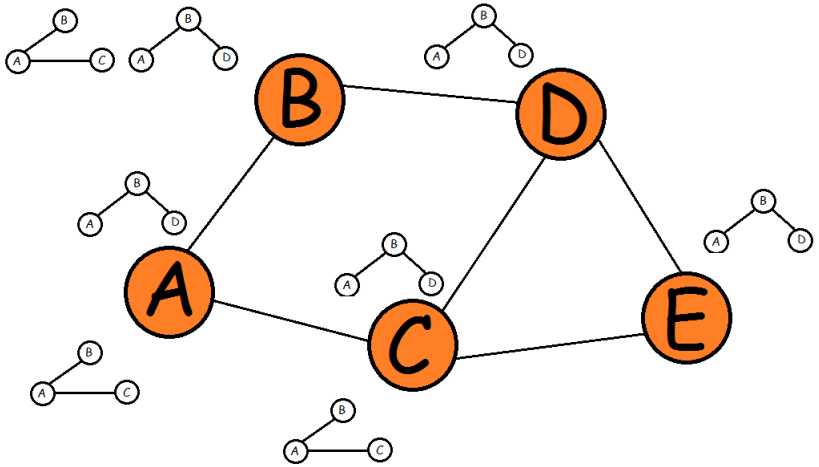


Figura 26 – Envio da topologia da rede vista pelo nó A

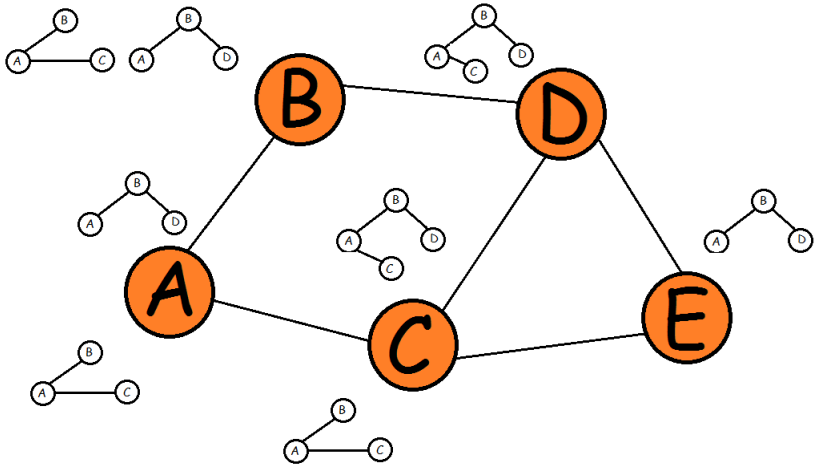


Figura 27 – Atualização da topologia da rede pelos nós C e D

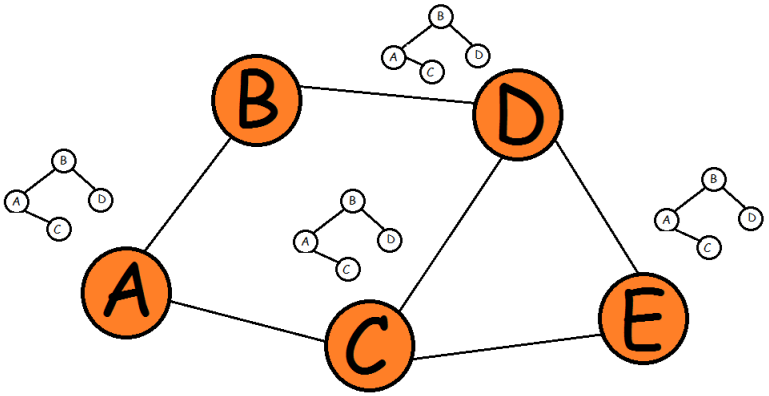


Figura 28 – Atualização da rede pelos nós A, B e E após os pacotes de C e D

Finalmente, após a troca de informação a respeito das topologias vistas à partir de cada nó, todos os nós da rede passam a conhecer a topologia completa da rede, conforme ilustra a figura 29.

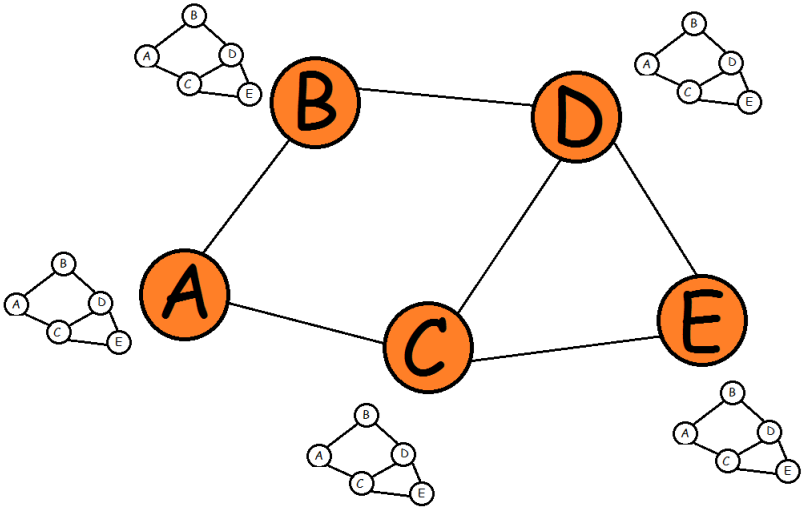


Figura 29 – Esquema final da rede

3.5 ALGORITMOS DE ROTEAMENTO HÍBRIDOS EM REDES AD HOC

É a classe de algoritmos Ad hoc que se adequa a redes maiores. Apresentam-se eficientes nestas redes quando comparados aos algoritmos de roteamento proativos e reativos (KHATKAR; SINGH, 2012; BIRADAR et al., 2008).

As redes com um número muito elevado de nós funcionam melhor quando divididas em grupos (*clusters*) e submetidas a algoritmos diferentes para o roteamento dentro e entre os grupos.

A justificativa para tal afirmação é que, quando bem divididos, um número reduzido de nós saíra do grupo. À partir desta constatação, pode-se simplificar o algoritmo da rede repassando as alterações de topologia dentro de um grupo apenas para o nós pertencentes ao próprio grupo, sendo estas alterações internas transparentes para os nós externos ao grupo.

Em algoritmos de roteamento híbridos, apenas uma parte dos nós fará atualização periódica em função do nó de destino, os chamados coordenadores. Estes nós são responsáveis pelos dados que entram e saem dos grupos (RAJU; RUNKANA; MUNGARA, 2010).

3.5.1 TORA (*Temporally Ordered Routing Algorithm*)

3.5.1.1 Definição

É um algoritmo eficiente, altamente adaptativo e muito hábil em termos de escalabilidade. Atua sob demanda, como seu próprio nome sugere (algoritmo de roteamento solicitado temporariamente). Tem por definição seu ímpeto de funcionamento sendo executado à partir da origem (KUPPUSAMY; THIRUNAVUKKARASU; KALAAVATHI, 2011).

Utiliza a técnica de algoritmos de sistemas distribuídos *link reversal*, a qual atribui ao link a característica de livrar-se da ocorrência de *loops*. Quando um nó está impossibilitado de propagar as mensagens, devido ao fato de não possuir algum nó (exceto os adjacentes de origem) em seu alcance, o algoritmo consegue contornar através desta

técnica. Desta forma, não ocorre transmissão contínua em laços fechados (KUPPUSAMY; THIRUNAVUKKARASU; KALAAVATHI, 2011).

Foi modelado com o propósito de reduzir o *overhead* na comunicação através da capacidade de efetuar mudanças adaptativas sobre a topologia local na rede, adaptando as rotas quando necessário. Fornece múltiplas "melhores" rotas para os dados serem transmitidos, desde o nó da origem até o nó destino. Assegura-se isto através da técnica *multi-path routing*, que considera múltiplos caminhos seletivos alternativos em uma rede (GIANNOULIS et al., 2005).

É um protocolo de roteamento essencialmente adaptativo, para redes de múltiplos saltos, pois possui execução distribuída. Possui a característica de manter pacotes de controle em conjuntos de nós próximos às ocorrências de alteração na topologia - que ocorrem, usualmente, em função da quebra de link. Para isso, cada nó precisa conter sua própria informação de roteamento e, também, informações sobre a topologia de rede pertencente aos nós adjacentes, que estão a um salto de sua localização.

Foi projetado para suavizar o impacto das alterações topológicas sobre a atualização das tabelas de rota em uma comunicação. Faz isso restringindo as mensagens relativas sobre a situação de roteamento local aos nós próximos ao evento (PIRZADA; MCDONALD, 2004).

Atua de forma independente em cada nó, que apenas possuem informações referentes aos seus adjacentes. Para este algoritmo, o roteamento otimizado não é o fundamento mais importante, e sim, o desempenho da rede como um todo. Ele leva em consideração o seguinte princípio: manter informações otimizadas, na tabela de roteamento, é desvantajoso em função da quantidade de mensagens necessárias para tal.

Quando ocorrem mudanças topológicas com frequência na rede, o controle do *overhead*, causado pelas mensagens estritamente de manutenção de rotas otimizadas, pode causar atraso na entrega de pacotes e ser inviável.

Desta forma, conforme Giannoulis et al. (2005), o algoritmo TORA oferece as seguintes características de roteamento:

- Execução distribuida;

- Assegura a não ocorrência de *loops*;
- Roteamento que assegura múltiplos caminhos;
- Estabelecimento e manutenção das rotas reativo ou proativo;
- Minimiza *overhead*.

3.5.1.2 Funcionamento

Segue o funcionamento do algoritmo de roteamento TORA, conforme descrevem os autores Giannoulis et al. (2005), Thiagarajan e Moorthi (2017), Pirzada e McDonald (2004):

3.5.1.2.1 Estabelecimento de Rotas

O processo de estabelecimento de rotas inicia-se à partir do momento em que um nó de origem deseja enviar um dado a determinado nó destino e complementarmente não possui informação sobre a rota até este. O estabelecimento da rota entre o nó de origem e o nó de destino é designado através de dois principais pacotes: *QUERY* (QRY) e *UPDATE* (UPD).

Para o estabelecimento da rota, o TORA estabelece um grafo direcionado e orientado acíclico até o destino Directed Acyclic Graph (DAG), criando caminhos direcionados na rede, que são fundamentados em relação ao destino. Denota valores de "altura direcional", cuja interpretação dá-se como a distância relativa entre dois pontos. Utiliza, posteriormente, essa referência para a transmissão de dados, transmitindo os pacotes de dados conforme o seu sentido atribuído: de um nó mais alto (nó de origem) para um nó mais baixo (nó de destino).

Este algoritmo estabelece múltiplas rotas até o destino rapidamente. Para o estabelecimento de uma determinada rota, o nó de origem envia um pacote QRY através de uma mensagem *broadcast* para os nós adjacentes. O pacote QRY contém o endereço do nó de destino e é propagado de forma semelhante ao algoritmo DSR (até atingir o destinatário ou algum nó intermediário que contenha a rota até ele).

Cada nó na rede possui um valor de altura que é calculado pelo próprio algoritmo de roteamento TORA. Os nós intermediários, quando

enviam o pacote QRY, incrementam a variável altura com um valor maior do que o recebido pelos nós adjacentes de origem e, em sequência, enviam esta informação através do pacote UPD. Esse mecanismo é o responsável por criar o grafo diretamente orientado até o destino.

Cada nó é capaz de conter conhecimento estrutural da rede através da manutenção das variáveis altura e status de todos os nós/caminhos (links) existentes. A relevância dessa variável altura no funcionamento deste algoritmo é que os nós da rede só deverão propagar pacotes de dados de forma descendente, ou seja, em um mesmo sentido.

Conforme ilustra a figura 30, em um primeiro momento, quando o nó não conhece o nó destinatário, inicia-se o processo de requisição da rota através da inundação do pacote de requisição de rotas (QRY). Em seguida, a figura 31 representa a continuação deste processo de descobrimento de rota pelos nós adjacentes. Percebe-se a existência da *flag* RRd, que é utilizada para os nós saberem que o pacote já foi inundado por si e, desta maneira, não repropagá-lo novamente, evitando a inundação excessiva de pacotes na rede.

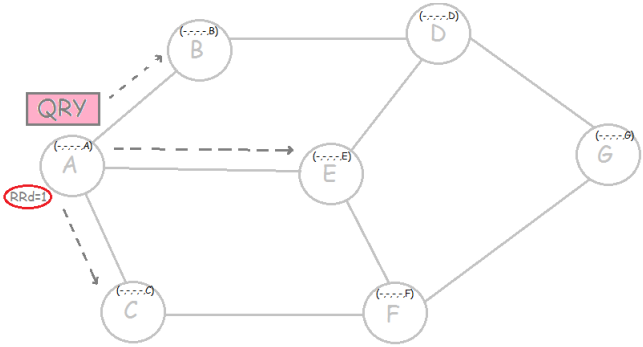


Figura 30 – Inicio do processo de descoberta de rotas através de *broadcast* do pacote QRY

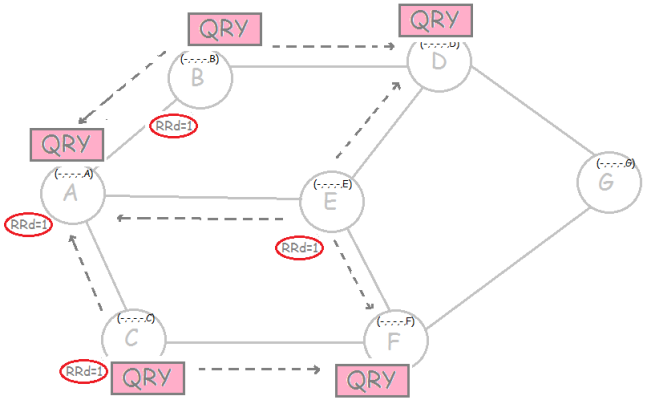


Figura 31 – Continuação do processo anterior

Este processo é efetuado até que algum nó adjacente ao nó de destino seja encontrado (32). Ao reconhecer o nó de destino, o nó F atualiza sua altura em relação ao nó de destino G e o primeiro segmento de link é constituído.

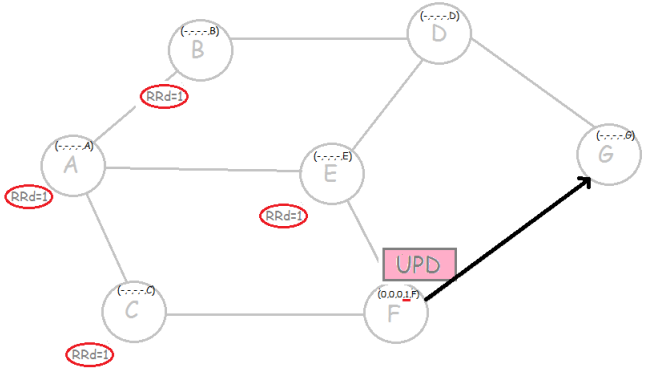


Figura 32 – nó adjacente ao destino estabelece o primeiro link e atualiza sua altura

Uma vez alcançado o destino pretendido, inicia-se o processo de atualização e resposta à requisição de rota. O nó destino envia um pacote UPD no sentindo inverso, em direção à origem, conforme ilustra a figura 33. Feito isto, obtém-se a formação do link entre a origem e o destino (figura 34).

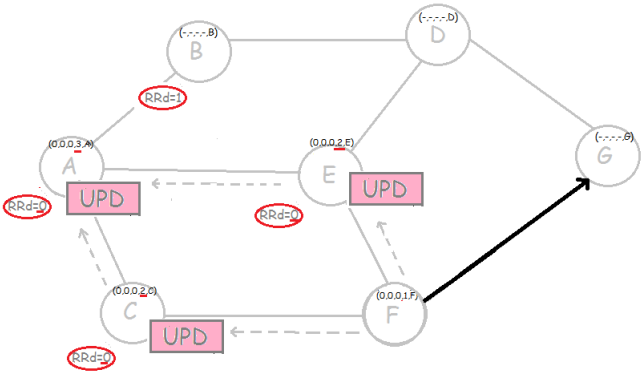


Figura 33 – nó adjacente ao destinatário envia pacote UPD aos seus adjacentes até a origem

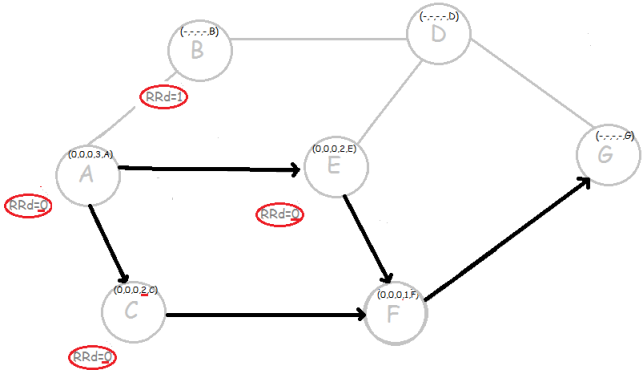


Figura 34 – Link origem-destino formado

As figuras 35, 36 e 37 apresentam o processo de difusão do conhecimento da rede aos demais nós da rede e consequente constituição da topologia da rede.

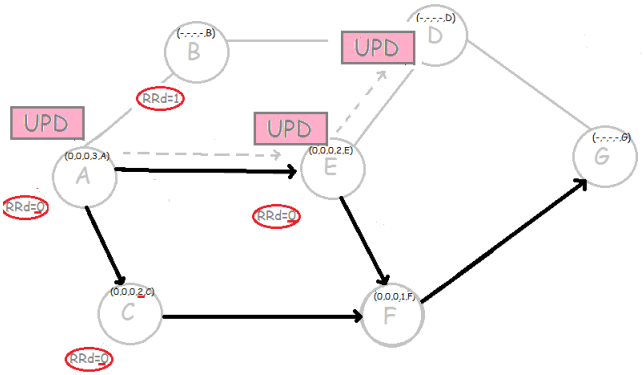


Figura 35 – Processo de aviso aos nós adjacentes aos que conhecem a rota

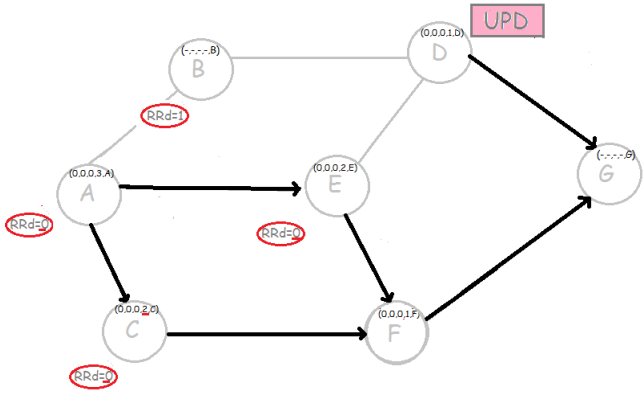


Figura 36 – nó que recebe o pacote é adjacente a rota e a complementa adicionando o link que passa por ele

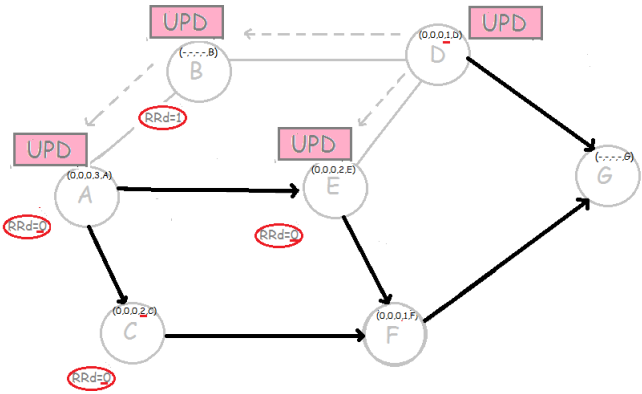


Figura 37 – nó informa aos adjacentes sua altura em relação ao destino

Finalmente. a figura 38 apresenta a rede com a topologia completa, conhecida por todos os nós da rede, após os prévios processos descritos.

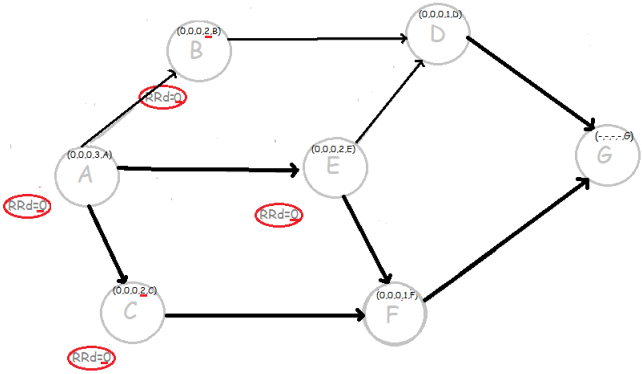


Figura 38 – Grafo total é conhecido pelos nós pertencentes a rede

3.5.1.2.2 Manutenção de Rotas

Quando uma rota não está disponível para comunicação, devido à quebra no link ou inserção de novos nós, o algoritmo TORA precisa reestabelecer a rota até o destino. Quando um link é quebrado, a altura do nó em que o link está indisponível recebe atualização. A ela é atribuída um valor maior do que qualquer nó adjacente a estes nós.

Eles irão enviar o pacote percorrendo o sentido contrário e procurarão uma rota alternativa até o destino.

É enviado, paralelamente a esta execução, um pacote UPD ao nó de origem, informando o rompimento do link. Se o nó de origem contém informação sobre rotas alternativas ao destino, ele selecionará alguma delas e irá propagar o pacote. Em caso contrário, inicia-se um novo processo de descoberta de rota através do procedimento QRY/UPD.

No primeiro caso, conforme a figura 39, o link está quebrado mas a rede possui um caminho alternativo até o destino e, portanto, não há necessidade de fazer algo. No segundo caso (40), o link está quebrado e o nó não possui caminho alternativo até o destino. Sendo assim, ele atualiza sua altura para um valor maior que seus adjacentes, de modo a forçar os pacotes de requisição de rota à não passarem mais por ele, já que o destino passou a ser inacessível por esse link.

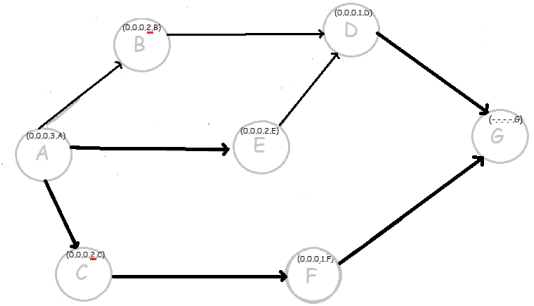


Figura 39 – Quebra de link: caso 1

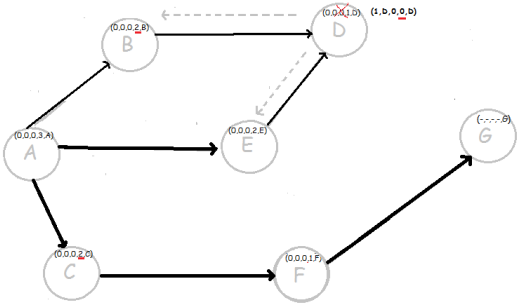


Figura 40 – Quebra de link: caso 2

Na sequência, o nó comunica aos seus nós adjacentes sobre a atualização através do pacote de atualização de rotas UPD (41). Os nós ao receberem o pacote UPD atualizam estas informações e passam a desconsiderar aquela rota como uma rota válida permanente.

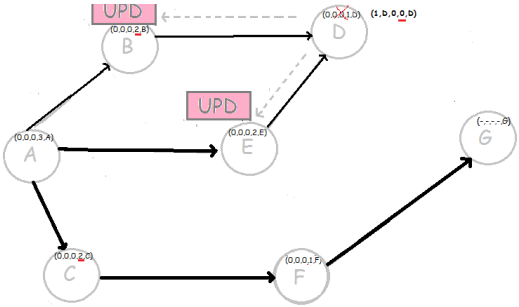


Figura 41 – Quebra de link: caso 2 (UPD)

3.5.1.2.3 Remoção de Rotas

Este processo é iniciado quando se percebe uma divisão na rede, conforme a figura 42. Ao perceber essa divisão, o nó atualiza os valores de altura dos nós adjacentes e dele próprio para o valor nulo. Feito isto, gera um pacote CLR (clear packet) que restaura o estado das rotas e remove as rotas inválidas da rede. Este algoritmo é denominado link reversal e é utilizado para resetar a configuração dos nós.

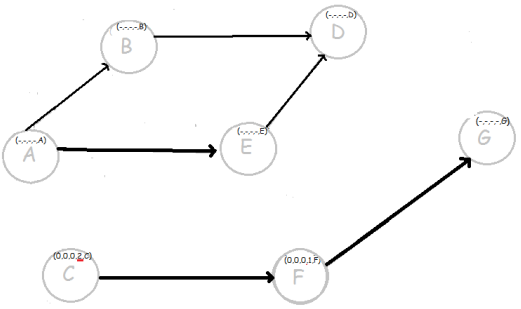


Figura 42 – Divisão da rede

3.5.2 ZRP (*Zone Routing Protocol*)

3.5.2.1 Definição

Baseia-se na definição de zonas, onde cada nó define uma zona. Neste algoritmo os nós conhecem estritamente as informações referentes à sua zona de roteamento. Neste modelo, as informações de roteamento podem ser propagadas apenas localmente (RAJU; RUNKANA; MUNGARA, 2010).

Protocolos de roteamento para redes móveis possuem diversos empecilhos a serem superados em sua implementação: alterações na topologia com frequência, baixa intensidade de transmissão dos nós e links assimétricos.

Ao visualizar as técnicas e a concepção dos algoritmos existentes, nas redes Ad hoc, no sentido de tratar estas limitações, ambos os protocolos puramente reativos ou proativos são incapazes e ineficientes. Os protocolos proativos utilizam a largura de banda em demasia para manter as informações de roteamento atualizadas, enquanto os algoritmos de roteamento reativos possuem um longo tempo de resposta sobre a requisição de rotas na rede, além de inundar, de forma não precisamente eficiente, a rede, para determinar as rotas desejáveis (KHATKAR; SINGH, 2012; BIRADAR et al., 2008).

O algoritmo ZRP idealiza tratar estas ocorrências através da união das vantagens dos algoritmos proativo e reativos, buscando uma

resposta conveniente através de sua aplicação sobre estas circunstâncias.

A metodologia adotada pelo algoritmo visa manter um mapa topológico atualizado das zonas centralizadas em cada nó. A ideia é ter as rotas imediatamente disponíveis, para cada zona, dentro do seu perímetro de alcance. Fora destas zonas, o algoritmo utiliza o procedimento de busca por rotas, beneficiando-se das informações locais de roteamento existentes nas zonas.

Desta forma, limitando-se a rede em zonas, a manutenção das informações de roteamento é simplificada, minimiza-se a quantidade de informações de roteamento que nunca são utilizadas e, como os nós armazenam as informações das zonas locais de maneira proativa, as requisições de rota aos nós mais distantes será desempenhada com maior performance, diminuindo a quantidade de requisições de rotas necessárias para alcançar os nós da rede (LOUTFI; ELKOUTBI, 2011).

Outra vantagem na atribuição deste protocolo é a redução da sobrecarga relacionada aos protocolos hierárquicos. Nestes protocolos, todos os nós devem conseguir acessar o níveis superiores da rede através do posicionamento estratégico dos *gateways*. Nós pertencentes a diferentes sub-redes, que desejam enviar mensagens a nós pertencentes à camadas superiores da rede, devem enviar as mensagens para um nó pertencente a uma sub-rede comum entre estes nós. Isso gera um indesejável congestionamento em regiões específicas da rede. O ZRP é considerado um algoritmo plano, as zonas se sobrepõem, há um conhecimento plano da rede e o congestionamento hierárquico é reduzido (GIANNOULIS et al., 2005).

O protocolo ZRP é eficiente em redes grandes. Como as atualizações de rota proativas são feitas apenas localmente, nas zonas internas, a quantidade de trafego de informações independe do tamanho da rede. Pode-se reduzir, adicionalmente, a quantidade de trafego reativo através do aumento do tamanho das zonas. Ajustando-se o raio destas zonas pode-se otimizar a performance do protocolo (LOUTFI; ELKOUTBI, 2011).

A dimensão ideal de uma zona depende de um conjunto de fatores: velocidade de alteração da topologia, quantidade dos nós, taxa de transmissão e extensão da rede. Conforme estes parâmetros são altera-

dos, a zona deve ser ajustada, visando a manutenção da performance pretendida (RAJU; RUNKANA; MUNGARA, 2010).

3.5.2.2 Funcionamento

Conforme os autores Raju, Runkana e Mungara (2010), Giannoulis et al. (2005), Loutfi e Elkoutbi (2011), segue a descrição do funcionamento do algoritmo ZRP:

As zonas de roteamento são definidas separadamente para cada nó e as zonas dos nós adjacentes as zonas vizinhas se sobrepõem. As zonas de roteamento são dadas pelo raio entre os nós, sendo este raio equivalente a quantidade de saltos "n"e não a uma grandeza física estática. As zonas particularmente incluem todos os nós que estão inclusos neste perímetro de "n"saltos.

Os nós de uma zona são divididos em nós periféricos e nós interiores. Os nós periféricos são os nós cuja distância mínima é exatamente igual ao raio da zona. os nós cuja distância é inferior ao raio da zona são nós interiores à zona. E os nós cuja distância é maior que o raio são considerados nós externos a zona de roteamento do nó em questão.

O número de nós na zona de roteamento pode ser ajustado através da potência de transmissão dos nós. Aumentando-se a potência de transmissão têm-se um aumento na quantidade de nós com alcance direto. Reduzindo-se a potência de transmissão, têm-se uma redução na quantidade de nós com alcance direto.

Deve-se atentar em relação a quantidade de nós dentro de uma zona, já que uma cobertura muito grande pode ser traduzida em tráfegos de atualização de forma excessiva.

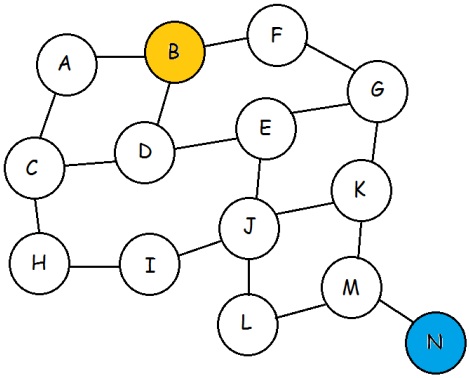


Figura 43 – Configuração inicial da rede

A figura 44 apresenta o conjuntos de nós pertencentes a zona do nó B. O critério utilizado para definição da zona é o número de adjacência igual a dois, ao nó em questão. Ou seja, os nós que estão até dois saltos distantes do referido nó. No caso da figura 44, os nós [A,C,D,E,F e G] estão inseridos na mesma zona que o nó B.

A figura 45 destaca os nós periféricos, que são os nós que estão exatamente há dois saltos de distância em relação ao nó emissor. Estes nós são os responsáveis pela propagação da mensagens nas zonas externas à zona local.

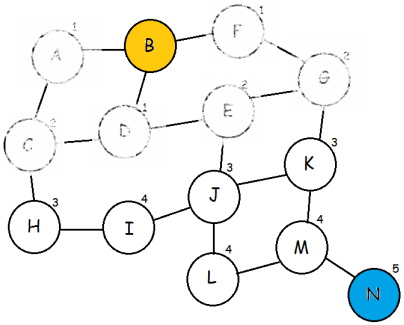


Figura 44 – Delimitação da zona do nó B

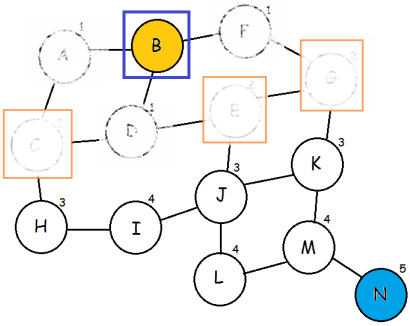


Figura 45 – nós periféricos

A figura 46 apresenta o conjuntos de nós pertencentes a zona dos nós periféricos ao nó B.

Este processo conclui-se na figura 47, pois um nó periférico é adjacente ao nó de destino da mensagem, alcançando-se, assim, o destino pretendido através das sub-divisão da rede em zonas.

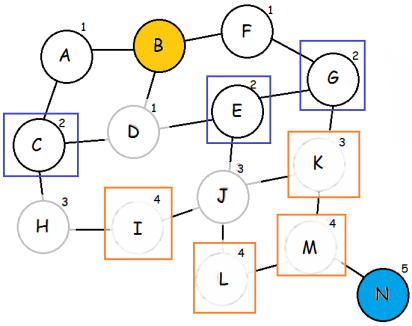


Figura 46 – Delimitação da zona pelos nós periféricos

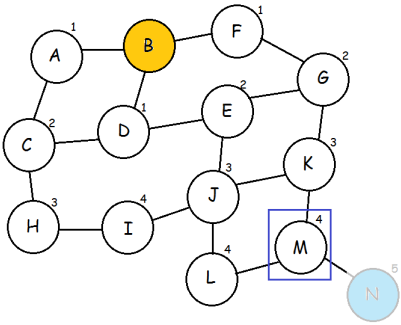


Figura 47 – Conclusão do processo

4 DESENVOLVIMENTO DO SISTEMA EMBARCADO

4.1 HARDWARE

4.1.1 Tecnologia Wireless Escolhida

Dentre as tecnologias pesquisadas LoRa e Sigfox destacam-se como escolhas principais para solucionar o problema de monitoramento das lâmpadas dos postes. Diferentemente da Sigfox, a Lora permite mensagens nos dois sentidos e assim, caso esta fosse utilizada, seria possível implementar o controle das lâmpadas além do simples monitoramento das mesmas.

Ainda assim, essas tecnologias são custosas para avaliação prática neste trabalho de conclusão de curso. O custo dos módulos *transceivers* em adição ao custo de um *gateway* LoRa equivalem a cerca de 300 dólares (no exterior) e, na tecnologia Sigfox, há o custo dos módulos Sigfox mais o custo da assinatura. Desta forma, buscamos realizar uma implementação prática utilizando módulos de baixo custo, já disponíveis e acessíveis.

Esses módulos são compatíveis com o padrão IEEE 802.11, mas possuem um consumo de energia muito superior aos módulos LoRa e Sigfox e um alcance menor (cerca de 60 metros na versão mais simples).

A escolha do módulo compatível ao padrão 802.11 deu-se em função das seguintes considerações:

- Custo: disponibilidade de um microcontrolador com suporte à tecnologia 802.11, com custo acessível, que viabilizasse a implementação do sistema em termos de sua escalabilidade - a qual pode requisitar a instalação de centenas de milhares de dispositivos (1 unidade/poste), conforme dados da Centrais Elétricas de Santa Catarina S.A (figura 48).

Relatório de Itens Cadastrados - Postes

Celesc Distribuição S.A.

Data de 19/07/2018 10:07 **Matrícula:** e016726 **Banco de Dados:** GENCEL

	Total
BLUMENAU	149990
CHAPECÓ	136847
CONCÓRDIA	88745
CRICIÚMA	85991
FLORIANÓPOLIS	171534
INDEFINIDA	133
ITAJAÍ	99543
JARAGUÁ DO SUL	47680
JOAÇABA	97127
JOINVILLE	103568
LAGES	149507
MAFRA	120101
RIO DO SUL	123359
S MIGUEL OESTE	137883
SÃO BENTO SUL	41200
TUBARÃO	73120
VIDEIRA	84026
Total	1710354

Figura 48 – Relatório da quantidade de postes em SC

- Alcance de transmissão: alcance de transmissão do sinal de acordo com a delimitação pertinente à constituição do sistema de iluminação pública e seus elementos. Segundo as normas técnicas de distribuição (NTD - 001/2008), a distância (vão) média entre os postes deverá ser de 35m e respeitar o limite máximo de 40m nas vias públicas, sendo admitidos vãos médios menores que 35m nos centros comerciais das cidades. Distâncias dentro do alcance da tecnologia 802.11, com considerável margem de segurança;

- Arquitetura da rede: possibilidade de implementação do sistema sem depender de uma infraestrutura privada ou previamente existente para funcionamento do sistema, como seriam os casos das tecnologias SigFox, WiMAX e LoRa. A última, apesar de permitir a incorporação de uma rede particular, demanda investimento em infraestrutura (antenas, backhauls, gateways) e carece de uma maturidade de utilização maior. Sabe-se pouco à respeito dos desafios existentes em sua utilização, principalmente no Brasil, onde a tecnologia está em estado de experimentação, havendo assim um maior risco envolvido em sua implementação.

A tabela 4 apresenta informações relevantes sobre a atribuição do

protocolo 802.11 e foram consideradas no desenvolvimento do mesmo, buscando evidenciar a compatibilidade entre o projeto e as especificações do 802.11 no microcontrolador adotado. Seguem as especificações técnicas detalhadas, como potência de transmissão de envio do sinal, sensibilidade de recepção, característica da antena, faixa de frequência e protocolos suportados.

Tabela 4 – Wi-Fi (ESPRESSIF, 2018)

Itens	Parâmetros
Certificação	Wi-Fi Alliance
Protocolos	802.11 b/g/n
Faixa de Frequência	2.4G ∼2.5G (2400M - 2483.5M)
Potência de Transmissão (Tx)	802.11 b: +20 dBm 802.11 g: +17 dBm 802.11 n: +14 dBm
Sensibilidade de Recepção (Rx)	802.11 b: -91 dbm (11 Mbps) 802.11 g: -75 dbm (54 Mbps) 802.11 n: -72 dbm (MCS7)
Antena	PCB Trace, Externa, Conector IPEX, Chip Ceramico

4.1.2 Módulo ESP8266

É um microcontrolador projetado para ser capaz de atender as especificações de projetos que integram um novo paradigma de aplicações: a Internet das Coisas (*Internet of Things*). Fabricado na China e considerado acessível pelo seu considerável baixo custo, dispõe de uma interface Wi-Fi, sendo este seu núcleo diferencial.

Suas dimensões ainda não são tão reduzidas quanto demanda os produtos comerciais, portanto seu uso ainda não está associado a produtos comerciais em larga escala, sendo seu propósito principal o suporte ao desenvolvimento de projetos pessoais.

Considerando-se o projeto desenvolvido, o preço, o tamanho e as características fornecidas pelo microcontrolador ESP8266 são suficientes e satisfatórias. Sendo, por tal motivo, o microcontrolador escolhido para implementação do sistema de iluminação pública. A figura 49 apresenta o ESP8266 NodeMCU, uma plataforma open source com suporte ao desenvolvimento integrada ao microcontrolador ESP8266.

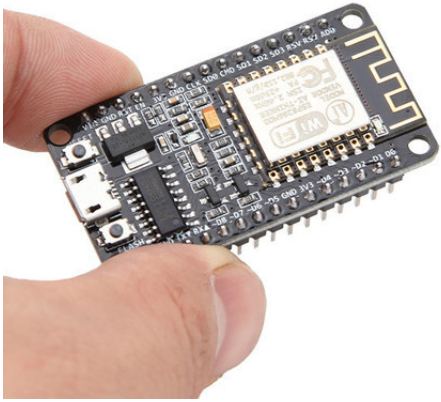


Figura 49 – ESP8266 NodeMCU

O microcontrolador ESP8266 possui um conjunto de recursos que promovem sua aplicabilidade à uma gama ampla de projetos: dispositivos móveis, eletrônicos *wearables* (eletrônicos vestíveis ou utilizáveis que são comuns no cotidiano das pessoas), aplicativos IoT, redes de sensores, *Smart Grids* e diversos outros que partilham a mesma demanda de recursos proporcionados pelo microcontrolador ESP8266.

Particularmente para este projeto, ele foi escolhido pelos seguintes recursos:

- Baixo custo;
- Arquitetura de baixo consumo de energia;
- Alance de RF satisfatório;
- Maturidade no mercado;
- Confiabilidade;
- Versatilidade de operação (AP/Cliente);
- Capacidade considerável de armazenamento de dados em memória flash;
- Processador de 32 bits otimizado para este tipo de aplicação;

- Segurança AEK, TKIP e AES integradas;
- Interface serial para atualização de software;
- Suporte ao desenvolvimento;
- Dispositivo compacto.

Tais recursos promovem as funcionalidades características exigentes em uma comunicação de dispositivos distribuídos que possuem o objetivo de coletar, transmitir e processar dados através da atuação de sensores.

4.1.2.1 Consumo de Energia

É um dos parâmetros primordiais na modelagem do sistema de iluminação pública e escolha do microcontrolador utilizado. A propriedade de baixo consumo de energia propicia uma vida útil maior à bateria dos dispositivos, se alimentados desta forma.

Deve-se adotar um microcontrolador que esteja sujeito a minima intervenção possível, evitando necessidade de manutenção das baterias, condição esta inerentemente determinante na viabilidade do projeto.

Apesar de haver alternativas superiores neste quesito, o módulo ESP8266 foi projetado para atender as aplicações IoT, onde as especificações de baixo consumo encontram-se intrinsecamente presentes e se fazem imprescindíveis. De tal maneira, este módulo é considerado hábil para a aplicação do sistema de iluminação pública.

A principal alternativa considerada em relação ao consumo de energia, na implementação deste trabalho, é aproveitar-se da rede elétrica e obter a alimentação à partir dos próprios postes, excluindo a necessidade do uso de baterias para alimentação dos nós. Sendo esta alternativa mais viável economicamente e atrativa por prover longevidade a manutenção dos nós sem necessidade de interferência para a troca das baterias.

Segue a tabela descritiva, contendo informações acerca do consumo de energia requisitado pelo nó em seus diferentes estados de funcionamento (modo cliente (Tx), modo Access Point (Rx) e modo ocioso (*sleep*)):

Tabela 5 – Consumo (ESPRESSIF, 2018)

Parâmetros	Média	Unidade
Tx802.11b, CCK 11Mbps, POUT=+17 dBm	170	mA
Tx 802.11g, OFDM 54Mbps, POUT=+15 dBm	140	mA
Tx 802.11n, MCS7, POUT=+13dBm	120	mA
Rx 802.11b, 1024 bytes, –80 dBm	50	mA
Rx 802.11g, 1024 bytes, –70 dBm	56	mA
Rx 802.11n, 1024 bytes, –65 dBm	56	mA
Modem-Sleep	15	mA
Light-sleep	0.9	mA
Deep-sleep	20	uA
Power Off	0.5	uA

Na figura 50 é possível identificar o critério de *sleep* adotado no microcontrolador ESP8266. Verifica-se, através da máquina de estados descrita, que o módulo entra em estado de *sleep* (estado ocioso de baixo consumo de energia), havendo para tal três estados de *sleep*: *modem-sleep*, *light-sleep* e *deep-sleep*, com respectivos consumos de 15mA, 0,9mA e 20uA, como visto na tabela 5. Este microcontrolador apenas recebe estímulo de energia para receber e transmitir dados - atividades que requerem um consumo maior de energia -, periodicamente, segundo o critério de sleep adotado.

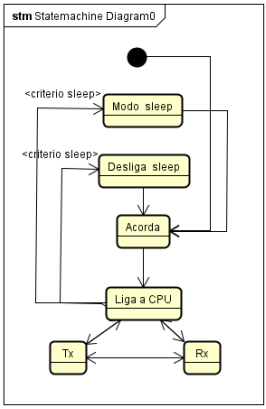


Figura 50 – Máquina de estados esquemática do modo de operação do ESP8266

4.1.3 Especificações Técnicas

As especificações técnicas adicionais com relação ao hardware estão dispostas na tabela 6. Estas informações são extremamente importante para dimensionar a capacidade de utilização do referido hardware neste projeto e também conhecer os limite de utilização.

Destaca-se a capacidade de processamento formidável para um microcontrolador com baixo custo, com tamanho da palavra de 32 bits e frequências de clock de 24MHz/52MHz.

Outro diferencial é a presença de uma memória flash externa de 16MB, capacitando o dispositivo a atualizar dados com maior agilidade, se necessário.

Tratando-se de um sistema de iluminação pública, como os microcontroladores são expostos a uma ampla faixa de temperatura distinta, é importante também reconhecer a sua capacidade de operação nestas condições.

Tabela 6 – Hardware (ESPRESSIF, 2018)

Itens	Parâmetros
CPU	Tensilica L106 32-bit
Frequência de Clock Tx/Rx (Min/Max)	24/52 MHz
Memória Flash Externa	16MB
Interface Periférica	UART/SDIO/SPI/I2C/I2S/IR Controle Remoto
	GPIO/ADC/PMW/LUZ E BOTAO LED
Voltagem de Operação	2.5V ∼3.6V
Corrente de Operação	80mA (média)
Faixa de Temperatura (Operação)	-40°C ∼125°C
Faixa de Temperatura (Armazenamento)	-40°C ∼125°C

Entre as características de software que facultaram a escolha do microcontrolador EPS8266 destacam-se o modo de operação presente compatível ao modelo de um sistema de iluminação pública desejado, havendo recursos de software disponíveis para as aplicações Cliente/AP/AP+Cliente, conforme apresenta a tabela 7.

Em complemento a isto, há os demais recursos de software essenciais para o desenvolvimento do projeto: a presença de um SDK (Software Kit Development), que é um kit de desenvolvimento de software; a possibilidade de atualizar o firmware, o suporte ao protocolo

IP de rede TCP/IP v4, protocolos de comunicação de rede TCP/UDP, protocolos de comunicação HTTP e transferência de arquivos FTP.

Em termos de segurança disponível na transmissão das mensagens e acesso indevido ao dispositivo microcontrolador, há suporte aos protocolos de segurança WPA/WPA2 e aos protocolos criptográficos WEP/TKIP/AES, como referencia a tabela 7.

Tabela 7 – Software (ESPRESSIF, 2018)

Itens	Parâmetros
Modo Wi-Fi	Cliente/AP/AP+Cliente
Segurança	WPA/WPA2
Criptografia	WEP/TKIP/AES
Atualização do Firmware	UART Download / OTA (via rede)
Desenvolvimento	Cloud Server Development / Firmware e SDK
Protocolos de Rde	IPV4, TCP/UDP/HTTP/FTP
Configuração de Usuário	Conjunto de Instruções AT, Cloud Server, Android/iOS App

4.1.4 Sensor AC5712

Para descobrir se a lâmpada dos postes queimou optou-se pela escolha do sensor de corrente ACS712 51. Este sensor de corrente, da empresa Allegro MicroSystems, é invasivo e capaz de medir valores de correntes contínua e alternada com alta sensibilidade de aferição e baixo custo.

Utilizou-se um relé 5V para controlar o acionamento das lâmpadas dos postes, podendo este componente ser substituído por um transistor de potência.

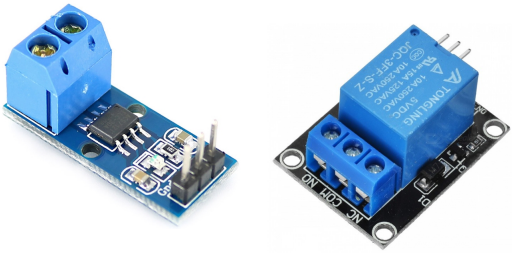


Figura 51 – Sensor ACS712 (AMARAL, 2017a)

O sensor ACS712 é um sensor de efeito Hall que beneficia-se deste efeito para medir a corrente, gerando uma saída de tensão proporcional a corrente que flui entre os seus pinos IP+ e IP-. A corrente aplicada que flui através do condutor de cobre gera um campo magnetico que é detectado pelo circuito integrado Hall IC e é convertida em uma tensão proporcional.

Ele é invasivo pois há a necessidade de colocá-lo entre o circuito para realizar aferições, ou seja, abrir e interromper o circuito para que este sensor seja instalado, forçando a corrente à passar por ele.

Algumas informações relevantes presentes no datasheet do sensor ACS712 que devem ser consideradas na utilização: identificação do modelo (part number), a temperatura de operação (TA), a faixa de amplitude da corrente elétrica suportada pelo sensor, que basicamente define a corrente máxima a ser medida no circuito (em Ampéres) e a relação de sensibilidade (mV/A) entre a tensão e a corrente.

Part Number	Packing*	T_A (°C)	Optimized Range, I_P (A)	Sensitivity, Sens (Typ) (mV/A)
ACS712ELCTR-05B-T	Tape and reel, 3000 pieces/reel	–40 to 85	±5	185
ACS712ELCTR-20A-T	Tape and reel, 3000 pieces/reel	–40 to 85	±20	100
ACS712ELCTR-30A-T	Tape and reel, 3000 pieces/reel	–40 to 85	±30	66

Figura 52 – Datasheet (AMARAL, 2017b)

Pode-se perceber, através da figura 52, que este componente possui três modelos que diferenciam-se pela capacidade máxima de medição da corrente elétrica: 5A, 20A e 30A. Estes valores referem-se a corrente DC suportada pelo sensor (i.e. o modelo ACS712-30A pode suportar até 30A (bidirecional)). Este é um sensor que mede correntes contínuas CC, através do efeito Hall, por intermédio do campo elétrico produzido pela corrente.

Para verificar a corrente AC suportada, considera-se um parâmetro razoável a divisão entre o valor de pico e a raíz quadrada de 2. Para correntes alternadas AC, considerando este modelo e a equação descrita como referência, em regime senoidal, a corrente máxima suportada é de, aproximadamente, 21.2A.

4.2 COMUNICAÇÃO EM REDE

Ao desenvolver o sistema levou-se em consideração um conjunto de premissas desejáveis. Entre estas destacam-se as características fundamentais do sistema projetado e outras agregadas para o melhor funcionamento do mesmo. É de suma importância para o projeto a validação destas premissas, descritas a seguir.

O modelo de comunicação deve levar em consideração que o sistema de iluminação pública é composto por postes distribuídos geograficamente, em ambientes sem infraestrutura de rede previamente disponível. Portanto, deve ser capacitado à funcionar em redes Ad hoc com a restrição de ser flexível e dinamicamente funcional. Para isso, os nós devem funcionar como roteadores sendo capazes de estabelecer a comunicação e adaptação autônoma às intempéries características da comunicação em redes Ad hoc.

O sistema funciona através de múltiplos saltos e, portanto, os dispositivos devem estar localizados em regiões de alcance mútuas, nunca isolados, sendo capazes de comunicar-se com outros dispositivos, havendo, sempre que possível, um link entre a origem de comunicação e o destino.

Deve ser tolerante a ocorrência de falhas ou alterações na configuração da rede. Essas alterações representam-se pela inserção/remoção de nós, falhas na comunicação, perda de conectividade, etc. O sistema deve ser capaz de contornar as falhas, sendo tolerante às mesmas e possuindo autonomia para reconfigurar as rotas sempre que necessário.

O modelo proposto deve ser adaptável e autoconfigurável para ser alocado em qualquer lugar, por qualquer pessoa. Deve apresentar-se permanentemente apto à instalação e isentando a necessidade de configuração para seu funcionamento. O dispositivo deve reconhecer a rede e configurar-se adequadamente para a adequação homogênea ao sistema.

O modelo deve promover o envio e recepção de mensagens entre os nós, habilitando a condição de detecção e troca de mensagens entre quaisquer dois dispositivos que estejam na mesma área de cobertura do alcance de seus sinais. Estes devem estar aptos a comunicar-se, viabilizando a execução do algoritmo. Os dispositivos devem trocar in-

formação entre si afim de reconhecer a rede, mesmo que parcialmente, de modo a selecionar a melhor rota disponível.

O modelo de comunicação deve maximizar o desempenho e adequar-se à mobilidade dos nós e alterações na topologia da rede, minimizando o efeito negativo da ocorrência destes eventos.

4.3 MODELO IMPLEMENTADO

A implementação do modelo baseou-se através das suas características de comunicação distintas. A comunicação divide-se em dois modos:

- Baseado em zonas e orientado ao destino;
- Baseado em busca pelas rotas.

Considerou-se o desenvolvimento de um modelo de comunicação otimizado à estas características e considerando-se as propriedades desejáveis em um algoritmo de roteamento: correção, simplicidade, robustez, estabilidade, equidade e otimização.

Buscou-se a realização do modelo de comunicação através de um algoritmo que atendesse os requisitos impostos pela restrições estruturais da rede e que maximizasse o desempenho da rede conforme sua topologia e configuração.

4.3.1 Arquitetura

A arquitetura da rede destaca-se pela isenção de roteadores exclusivos, antenas ou qualquer meio de comunicação, exceto o ar, como cabeamento disponível para transferência de dados, etc.

É essencialmente uma arquitetura Ad hoc, composta pelos nós que atuam tanto como roteadores como Access Points, graças a autonomia do dispositivo escolhido que possui a flexibilidade de transmitir e receber dados, permitindo a configuração dessa comunicação par-a-par nos dois sentidos de transmissão de dados.

O servidor web, onde está alocada a aplicação e o servidor do banco de dados completam a arquitetura da rede, sendo estes os com-

ponentes da camada de gerenciamento da rede, onde ocorre o disparo dos eventos e monitoramento do status dos nós, de modo geral.

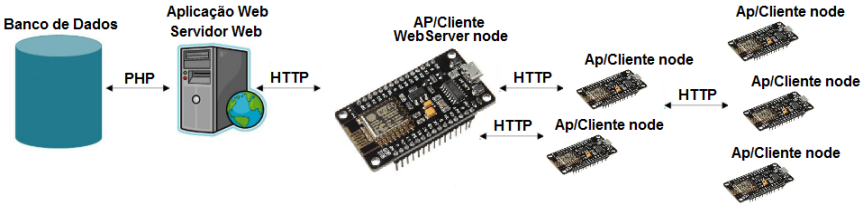


Figura 53 – Arquitetura da Rede

4.3.2 Comunicação Nós-Prefeitura

4.3.2.1 Configuração da Rede

Em cada poste existe um sistema embarcado para monitoramento e controle do status da lâmpada do poste, denominado nó. Os nós são alimentados pela rede elétrica do próprio poste e, caso a mesma seja interrompida, ele será desligado.

Ao ser energizado, um nó faz um "scan"da rede no seu raio de alcance e detecta se ele detectou o computador da prefeitura através da informação resultante do processo de scan.

A rede se configura à partir da prefeitura, este é o ponto inicial de estabelecimento da topologia da rede. Ao perceber a prefeitura através de varredura periódica, os nós que estão em seu alcance e a percebem incrementam a informação sobre a quantidade de saltos n até ela (sendo n=0 inicialmente), conforme apresenta a figura 54.

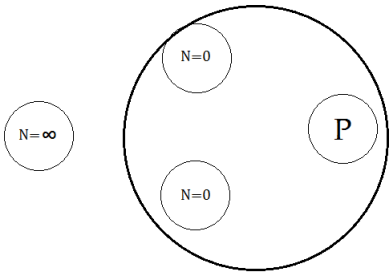


Figura 54 – Configuração inicial

A partir da configuração inicial, o conjunto de nós que está próximo aos nós adjacentes à prefeitura irá detectar, através do escaneamento periódico, que os nós próximos a si possuem link direto (n=0) com a prefeitura. A partir desta constatação eles irão incrementar a informação própria sobre a quantidade de saltos até a prefeitura para (n=n+1=1).

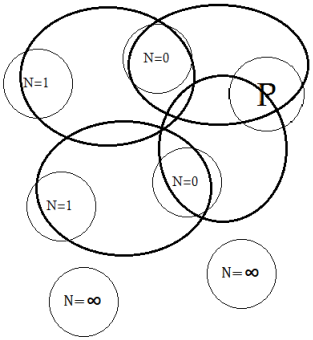


Figura 55 – Continuidade da configuração da rede à partir do escaneamento da zona local

Este processo de escaneamento é realizado periodicamente por todos os nós da rede. Deste modo, conforme os nós vão percebendo os nós próximos a si, eles vão atualizando a sua distância até a prefeitura.

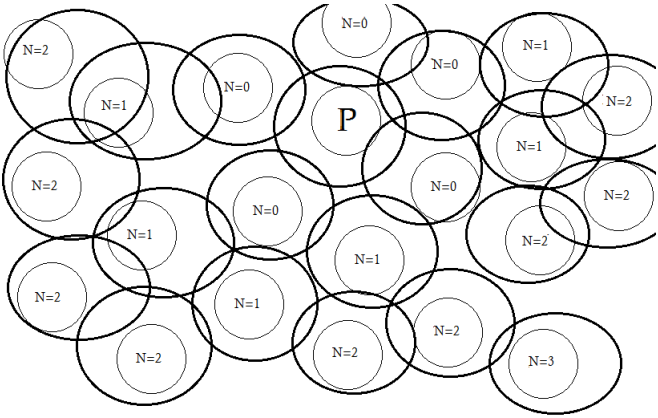


Figura 56 – Configuração completa da rede orientada á prefeitura

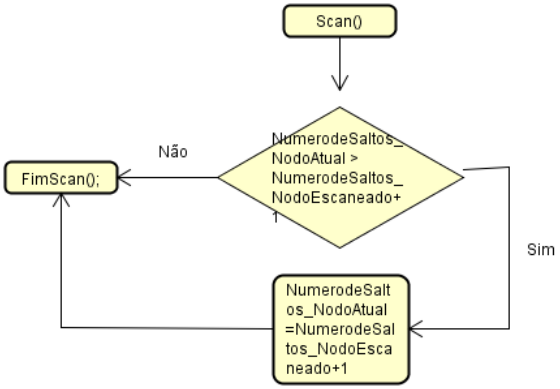


Figura 57 – Processo de Escaneamento

A propagação de dados é sempre orientada à topologia local, ou seja, até o próximo salto. Na verificação periódica, os nós verificam qual nó próximo a si possui a variável de menor quantidade de saltos até a prefeitura. Após a verificação, os nós armazenam esta configuração em sua tabela de roteamento.

Na propagação de dados, os dados serão enviados localmente

para o nó que possui a menor quantidade saltos até a prefeitura. Isto ocorre de modo sucessivo até que os dados sejam entregues ao destino.

4.3.2.2 Definição de Rotas

Neste modelo proposto, os nós dispensam a necessidade de manter rotas completas até a prefeitura. Conforme apresentado anteriormente, os nós mantem informação de saltos em relação à prefeitura e, portanto, os nós definem a rota somente até o próximo nó.

Isso evita a inundação de pacotes com atribuição de definição de rotas, diminuindo o *overhead* gerado por esse mecanismo de busca.

Em termos de escalabilidade, que é uma característica predominante em um sistema de iluminação pública, este modelo apresenta-se extremamente vantajoso pelas seguintes definições:

1. Simplicidade na manutenção de rotas;
2. Redução na interdependência de comunicação entre os nós;
3. Exclusão de armazenamento de rotas longas;
4. Redução da necessidade de processamento gerado pela manutenção de rotas longas;
5. Exclusão da existência de algoritmos complexos para determinação de rotas de ponta-a-ponta;
6. Agilidade na descoberta de rotas;
7. Facilidade de inserção ou remoção de um novo nó;
8. Exclusão da necessidade de manutenção de informação sobre os nós fora da zona de alcance;
9. Alteração na rede só requer correção local (intrazonal).

Este modelo dispensa a curva de tempo necessária à descoberta de rotas dos algoritmos *on-demand*, por estabelecer periodicamente rotas à partir dos nós próximos a si e armazenar a melhor rota até o próximo nó para uso instantâneo. Exclui a necessidade de atualização frequente de rotas e dependência destas no fluxo de dados da rede, que são características intrínsecas de algoritmos proativos, os quais predominantemente baseiam-se nas informações de sua própria tabela de roteamento.

4.3.2.3 Atualização das Rotas

As rotas são atualizadas por cada nó periodicamente. Este procedimento tem o propósito de averiguar se houve, na topologia local (área de cobertura de sinal de cada nó), alguma alteração que implique em mudança nas rotas ou na ordem de precedência de rotas. Cada nó realiza o escaneamento periódico na região de alcance de cobertura do seu sinal de transmissão com o propósito de verificar as seguintes possibilidades:

- Se algum nó novo foi inserido e se esta inserção promoveu alterações em sua rota;
- Se houve falha e esta promoveu a exclusão de algum nó que pertencia a sua rota;

De modo geral, os nós utilizam este mecanismo para verificar se dentre os nós que estão próximos a si, após comparar, em cada nó, a variável de número de saltos até o nó destino (prefeitura), existe a necessidade de atualizar a sua rota até o destino.

4.3.2.4 Vantagens da Implementação deste Modelo

- Nós não necessitam armazenar a rota completa até a prefeitura;
- Evita inundação de pacotes na rede;
- Otimiza o envio de pacotes;
- Utiliza menos espaço de armazenamento nos nós;
- Simplifica processos de descoberta de rota;
- Torna a rede autoconfigurável;
- As rotas mantidas pelos nós não estão mais em função de uma sequência grande de nós e, sim, em função apenas dos nós mais próximos. Isso gera menor dependência entre os nós na integridade das rotas;
- Diminui drasticamente a quantidade de espaço ocupado nos nós para manutenção de rotas;
- Diminui o processamento gerado pelos nós para manutenção das rotas;

- Dispensa a necessidade de processamento de algoritmos responsáveis pela eleição de melhores rotas;
- Facilita a inserção de um nó - já que ele apenas necessitará executar a função de escaneamento para perceber e atualizar sua localização na rede.

A figura 58 apresenta o diagrama de atividade referente a comunicação entre os nós e a prefeitura.

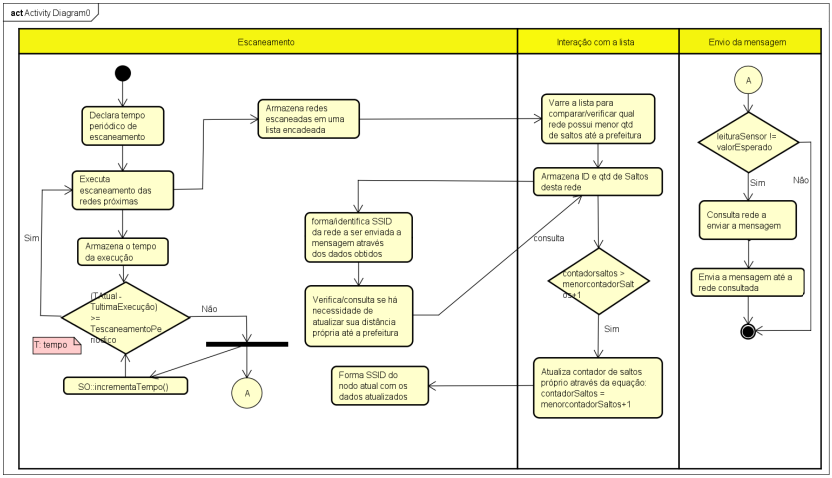


Figura 58 – Diagrama de atividade: funcionamento do comunicação nó-prefeitura

4.3.3 Comunicação Prefeitura-Nós

A comunicação originada na prefeitura e com sentido de transmissão conforme descrito nesta seção, encerrando-se ao atingir o nó desejado, é feita com o intuito de acionar ou desligar uma lâmpada. Ela inicia-se no sistema à partir da seleção de determinado nó pelo admnistrador, para que este receba a mensagem de controle de acionamento da lâmpada.

O admnistrador envia a mensagem pela aplicação e esta gera um link contendo os dados da mensagem e o ID identificador do nó ao qual a mensagem tem destino. Esse link, gerado pela aplicação, é consul-

tado periodicamente pelo nó *webserver* ligado à prefeitura. Após obter os dados provenientes deste link, o nó *webserver* propaga a mensagem (obtida através do link) ao nó desejado (também obtido por intermédio das informações contidas no link). Observa-se, como exemplo, um link retornado pela aplicação contendo informações que são subtraídas para envio da mensagem.

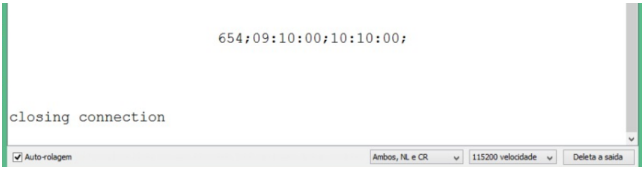


Figura 59 – Exemplo de link retornado

Para a aplicação, no entanto, o link submetido pela aplicação ao ESP é: http://localhost/ESP/esp.php?id=5&ip=123.123.123.21&msg=TesteMarcelo. Do qual são extraídas informações fundamentais para identificação do nó de destino da mensagem e da própria mensagem.

A propagação da mensagem é feita por *broadcast* aos nós que estão dentro da região de alcance da cobertura do sinal do nó emissor. Esta técnica de difusão de mensagens foi escolhida devido a alta escalabilidade da rede, havendo substancialmente mais de 100 mil nós existentes na rede, o que resulta na incompatibilidade das demais técnicas e, adicionalmente, ao fato de a mensagem neste sentido não ser enviada exclusivamente a um único nó, havendo vários possíveis diferentes destinos para este sentido de comunicação, favorecendo a técnica de difusão de mensagens.

A metodologia de armazenamento de rota também não se aplica neste caso, devido a extensidade das rotas e a quantidade ampla de rotas, inviabilizando a manutenção destas pelos dispositivos microcontroladores. Portanto, a busca por difusão é a metodologia prioritária a ser aplicada nesta situação.

Basicamente, para este sentido de comunicação, o modelo implementado baseado em um nó de destino é inadequado e improcedente. É necessário adotar um modelo de comunicação distinto haja vista que o destino da mensagem poderá ser qualquer um dos nós pertencentes

à rede.

Como a rede é muito grande, podendo ter mais de 100 mil nós, armazenar a tabela de roteamento até cada um destes nós seria uma metodologia utópica e impossível, seria incoerente, todavia, em termos de performance. Como a rede possui certa dinamicidade, ainda que baixa, porém existente devido a susceptibilidade que os nós possuem a falha de comunicação e as eventuais inclusões/remoções de nós na rede e a possível necessidade de troca de dispositivos e demais manutenções que possam ocorrer, estes eventos gerariam uma necessidade periódica de correção na tabela de roteamento, desvalidando esta alternativa.

Levando isto em consideração, atualizar a tabela de roteamento em uma rede com uma quantidade enorme de nós seria impraticável, como mensurado nos parágrafos anteriores. A escalabilidade é um fator que sugere metodologias de roteamento baseadas em zonas, na melhor das hipóteses. Sendo a manutenção de rotas em tabelas a última hipótese a ser considerada, implementando-a apenas em situações onde a relação temporal entre a requisição e o envio da mensagem até o destino é iminentemente a mais curta possível, para viabilizar a aplicação. E, nestes casos, os microcontroladores devem suportar a manutenção de tamanha quantidade de dados.

A aplicação de um sistema de iluminação pública é considerada uma aplicação que, embora o presente trabalho busque minimizar o tempo relativo ao envio e recebimento de mensagens, sugere fortemente a consideração do custo benefício e a capacidade dos dispositivos de interesse, dispondo de tempo suficiente para avaliar as ponderações a respeito do algoritmo implementado.

Sendo assim, para o envio até os nós considerou-se como melhor opção a implementação de um algoritmo baseado em requisição de rotas associado a técnicas que objetivam maximizar a performance dessa metodologia.

A comunicação neste sentido tem origem na aplicação do sistema, onde o administrador ou o usuário do sistema associam uma determinada mensagem referente a execução de um evento a um nó qualquer existente no banco de dados. Desta maneira, ocorre o envio da mensagem à partir da aplicação. Esta mensagem terá o formato de uma String característica detonada por: prefixo|id|mensagem.

Esta mensagem é composta dessa forma para facilitar a identificação dos nós na rede. A identificação ocorre através da comparação entre SSID dos nós e o id extraído da mensagem enviada pela aplicação. Ao escanear as redes, o nó que as escaneia obtém o SSID das redes, formadas também pela String característica descrita anteriormente. Os nós conseguem, então, separar os dados separados pelo identificador "e obtê-los separadamente, possuindo assim o ID das redes escaneadas.

Essa obtenção de dados permite, por exemplo, que o nó compare o ID do nó de destino da mensagem com o ID do nó a que se pretende enviar a mesma. Casos os IDs sejam equivalentes, o nó envia a mensagem ao nó desejado.

Assim que enviada a mensagem pela aplicação, o nó webserver, conectado diretamente ao servidor web, interpreta a mensagem recebida e inicia o processo de requisição de rota, através do processo de difusão de mensagens na rede, até que o nó que receba a mensagem seja o nó de destino desta. É evidente nesta metodologia que há uma decorrente inundação de mensagens até que o nó de destino da mensagem a receba.

Um dos recursos utilizados para minimizar a inundação de pacotes na rede foi a implementação de um identificador através de um número de sequência, sendo este exclusivo para cada pacote.

Estas técnicas implementadas no processo de envio da mensagem por inundação baseiam-se no seguinte objetivo: visam evitar a propagação de um mesmo pacote, recebido por nós diferentes, através de rotas distintas, evitando, assim, a réplica desnecessária de pacotes idênticos na rede e a consequente multiplicação destes na propagação das mensagens.

A figura 60 apresenta o diagrama de atividade referente a comunicação entre a prefeitura e os nós do sistema.

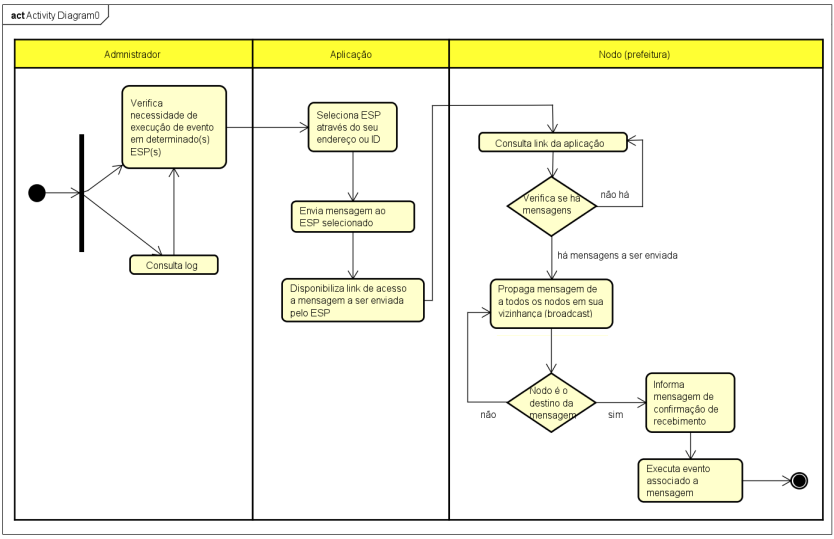


Figura 60 – Diagrama de atividade: funcionamento do comunicação prefeitura-nós

4.4 SISTEMA DE GERENCIAMENTO DOS DADOS

É o componente da arquitetura da rede responsável pela tarefa de gerenciar as informações do sistema de iluminação pública através do monitoramento do status das lâmpadas dos postes, sendo este sistema capaz de enviar mensagens a todos os postes cadastrados, bem como receber mensagem, atuando de modo bidirecional na comunicação com os nós microcontroladores.

As informações recebidas pelo sistema são prontamente armazenadas em um log onde os admnistradores da rede podem acompanhar e detectar eventuais falhas no acionamento das lãmpadas. Expondo genericamente esta atuação, extendendo a funcionalidade do sistema para outros sensores, é possível verificar o retorno da atuação dos sensores em decorrência do acontecimento de eventos.

Este log é muito importante para o monitoramento do sistema, porém, para monitorar o sistema em tempo real, devido a pouca ocorrência de mensagens, deve-se inserir um alerta como funcionalidade complementar ou envio de uma mensagem de notificação para o celular

do admnistrador.

Possui também a função de controlar o acionamento dos postes por meio do envio de mensagens aos nós da rede. Esta ação é executada por intermédio do admnistrador do sistema, podendo este requisitar o acionamento da lâmpada dos postes através do painel de controle do sistema.

Para enviar a mensagem a qualquer nó existente na rede, o sistema precisa obter conhecimento com relação aos nós da rede. Este processo é feito através do cadastro destes nós no sistema de gerenciamento da iluminação pública. Assim que o microcontrolador ESP8266 é instalado em um poste, este envia uma mensagem de notificação ao sistema contendo data, hora e minuto da instalação. Com base nessas informações, o admnistrador consegue contatar os instaladores e identificar o endereço da instalação, que deve ser catalogada pelos mesmos.

Com posse dessas informações, o admnistrador consegue realizar o cadastro do nó microcontrolador no sistema e associar o cadastro ao respectivo endereço de instalação, onde está alocado o poste na rede municipal.

Esta informação de endereço é interessante para filtrar o envio das mensagens de acionamento das lâmpadas para determinado endereço específico, em caso de futuras aplicações neste âmbito.

A figura 61 detalha os casos de uso do sistema de gerenciamento da iluminação pública e a interação deste com os principais atores: usuário e admnistrador. Este diagrama fornece, de tal modo, uma visão intuitiva das tarefas associadas ao sistema.

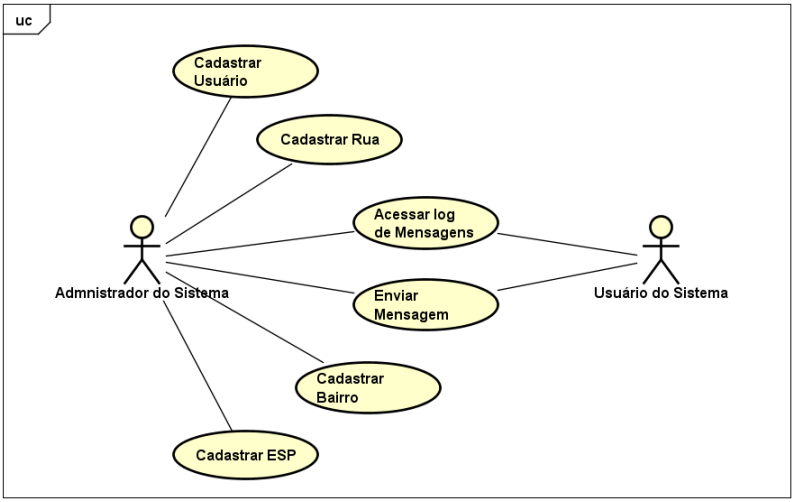


Figura 61 – Diagrama de casos de uso do sistema

Os processos referentes ao diagrama de caso de uso do sistema são melhores detalhados nos diagramas de sequência apresentados a seguir. Primeiramente observa-se o processo de envio de mensagens, na figura 62. Ele depende do cadastro dos nós na rede e percebe-se a opção de filtragem por endereço na busca por associação de filtros e a interação deste processo com o banco de dados.

Assim que o admnistrador seleciona o nó, à partir do endereço do mesmo, o sistema disponibiliza um link com o conteúdo da mensagem a ser enviada e o ID do nó de destino. O nó ligado à prefeitura coleta estes dados através de consulta periódica ao link da mensagem e propaga a mensagem até o nó de origem.

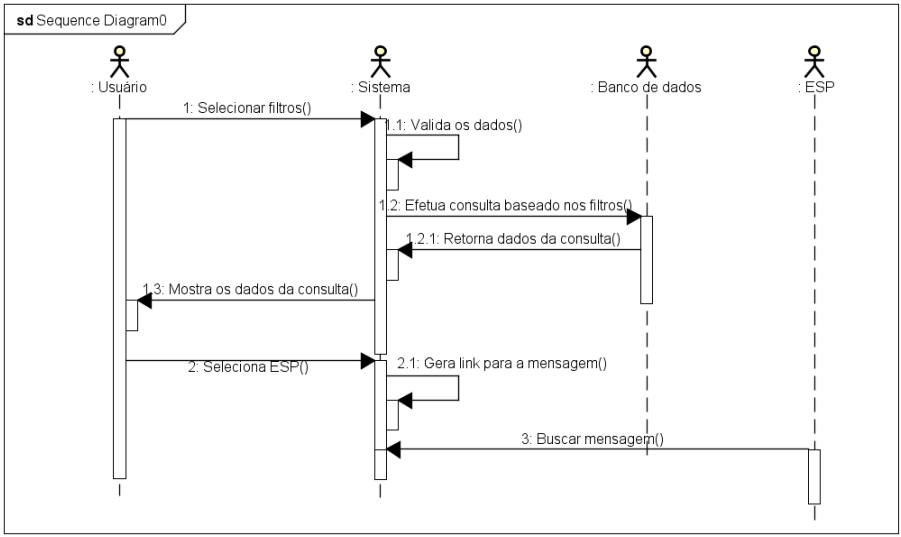


Figura 62 – Diagrama de sequência: envio de mensagens

Na figura 63, é possível visualizar como ocorre o processo de cadastro no sistema. Este caso de uso é genérico pois o procedimento dos cadastros são similares, sendo, portanto, representados pelo mesmo diagrama.

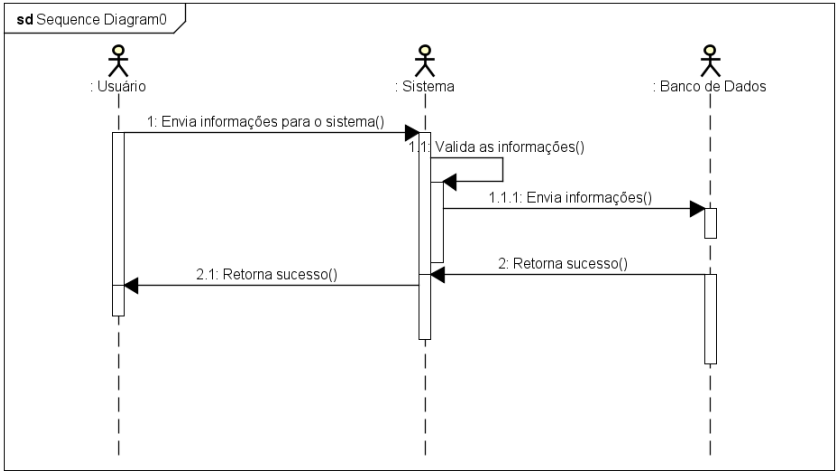


Figura 63 – Diagrama de sequência: diagrama de cadastros

O diagrama apresentado pela figura 64 representa a interação dos principais atores deste sistema e a ordem em que a interação é feita para acesso ao log do sistema.

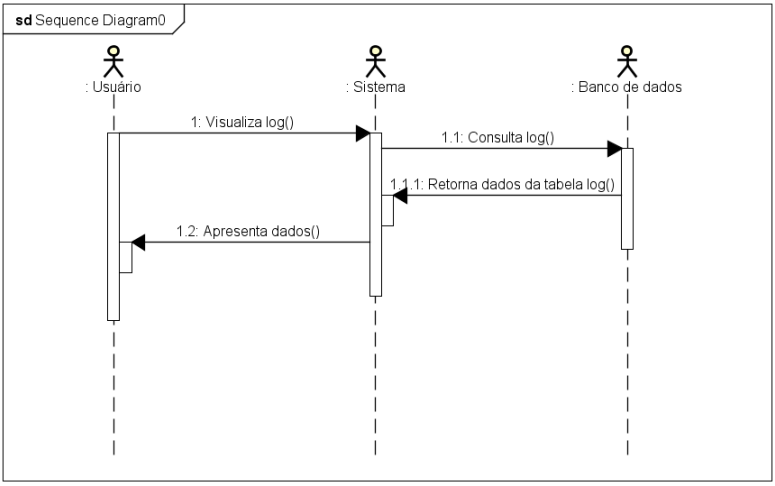


Figura 64 – Diagrama de sequência: acesso ao log do sistema

A critério de informação, a maneira como estes dados estão dispostos no banco de dados e a interação entre as tabelas são apresentados pelo diagrama de classes da figura 65.

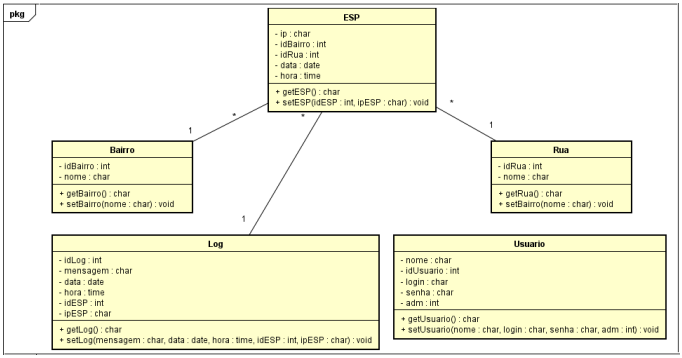


Figura 65 – Diagrama de classes do sistema

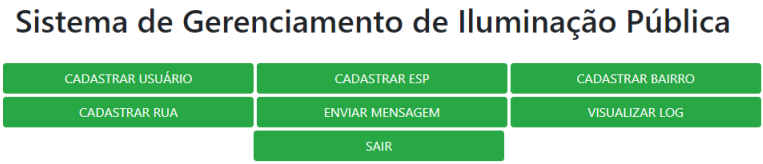


Figura 66 – Tela do admnistrador do sistema

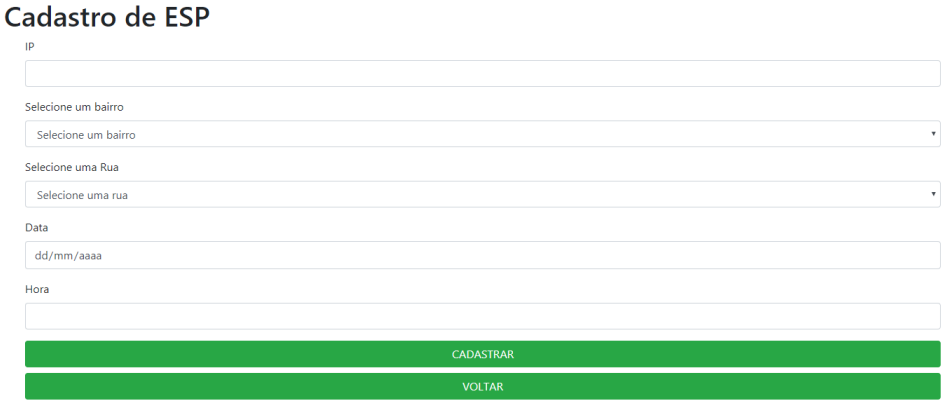


Figura 67 – Tela de cadastro do microcontrolador ESP8266 no sistema

Figura 68 – Tela de cadastro do bairro aonde o nó foi instalado

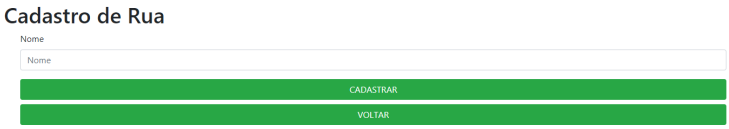
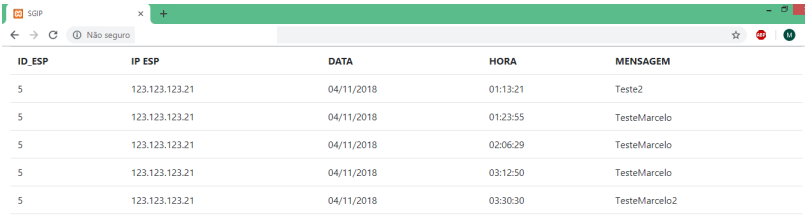


Figura 69 – Tela de cadastro da rua aonde o nó foi instalado

Figura 70 – Tela de envio de mensagens do sistema



ID_ESP	IP ESP	DATA	HORA	MENSAGEM
5	123.123.123.21	04/11/2018	01:13:21	Teste2
5	123.123.123.21	04/11/2018	01:23:55	TesteMarcelo
5	123.123.123.21	04/11/2018	02:06:29	TesteMarcelo
5	123.123.123.21	04/11/2018	03:12:50	TesteMarcelo
5	123.123.123.21	04/11/2018	03:30:30	TesteMarcelo2

Figura 71 – Tela de verificação de mensagens recebidas no sistema

5 RESULTADOS E TESTES

Os resultados do modelo de comunicação desenvolvido podem ser evidenciados através das ocorrências possíveis em sua execução, apresentando sua metodologia de tratamento e comparando-a com outros modelos.

O uso de um simulador seria uma alternativa otimizada e foi, à princípio, a primeira opção, através dos simulador Network Simulator (NS). Contudo, a curva de tempo estimada para incorporar o algoritmo ao simulador e a dificuldade inerente a esta tarefa excederia o escopo deste trabalho.

Ademais, é possível visualizar, com clareza, os seus fundamentos em um modelo em menor escala, conforme suas concepções, transpondo-as posteriormente à um modelo em maior escala com manutenção de suas características, preservando-se as variáveis de desempenho peculiares ao modelo desenvolvido neste trabalho.

Preocupou-se, em todos os sentidos, em delinear o modelo em função de sua aplicabilidade e compatibilidade com o sistema de iluminação pública, em sua disposição genérica.

Observa-se à partir destas constatações, em analise feita a seguir, o paralelo entre o desempenho particular de cada modelo, analisando-se os parâmetros envolvidos em cada situação.

A figura 72 apresenta a rede de nós conectados à prefeitura, similar á arquitetura do modelo de um sistema de iluminação pública designado pelo presente trabalho. Apesar da escalabilidade limitada, é um modelo capaz de retratar a aplicabilidade do algoritmo e os devidos resultados obtidos através de sua implementação. Representa-se, a seguir, nesta rede, as ocorrências e os respectivos tratamentos.

Na figura 73 verifica-se a rede e sua representação após a aplicação do algoritmo desenvolvido. Vê-se a formação da rede à partir da prefeitura, onde os nós vizinhos ao nó P a identificam através da função Scan() e, seguindo a metodologia do algoritmo, ocorre a progressão da configuração da rede.

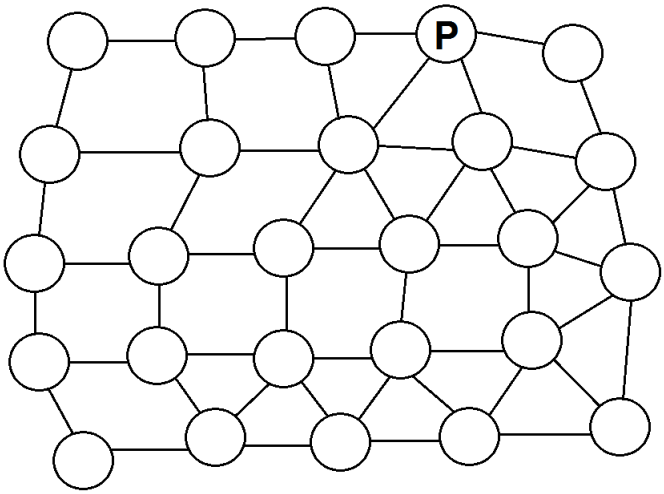


Figura 72 – Rede antes da aplicação do algoritmo

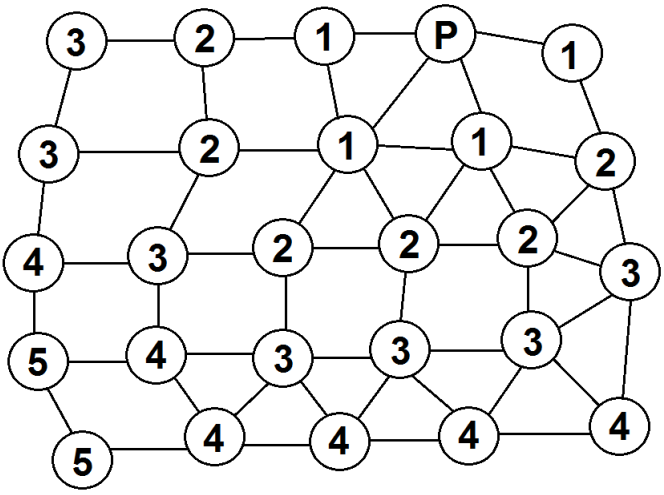


Figura 73 – Rede após a aplicação do algoritmo

5.0.1 Inserção de um nó

A analise da primeira ocorrência dá-se pela inserção de um novo nó na rede, conforme apresenta a figura 74.

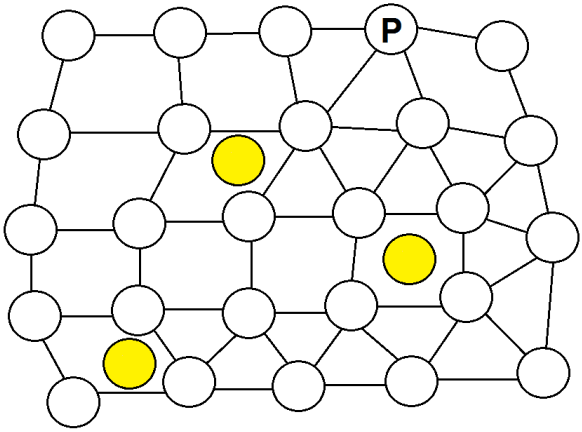


Figura 74 – Inserção de novos nós na rede

Esta inserção provoca alteração na configuração da rede, impactando o arranjo posicional dos nós e requisitando atualização/readequação das informações de percurso entre o nó de origem e o nó P para o envio correto da mensagem entre estes nós.

No caso dos algoritmos reativos, o efeito desta alteração não é perceptível em situações onde o percurso é desconhecido. Porém, a inclusão de um novo nó, na metodologia de algoritmos reativos, implica em possível alteração na informação de roteamento preexistente sobre percursos já contidos em sua tabela de rotas percorridas.

Esta constatação torna imprescindível o tratamento iminente à partir do escaneamento periódico, sendo esta metodologia uma medida corretiva para amparar as situações em que as alterações envolvam nós pertencentes aos possíveis percursos até a prefeitura. Este tratamento periódico inunda a rede de mensagens de requisição de rota, o que implica em consumo excessivo de energia e maior uso da largura de banda.

Como é uma abordagem metodológica, na qual o conhecimento

da rede aumenta conforme sua utilização, supõe-se que ao decorrer do tempo uma quantidade superior de nós possuam informação de roteamento ponta-a-ponta até o nó P, nó de destino da mensagem, armazenada em sua tabela de roteamento.

O efeito da inclusão de um novo nó na alteração da configuração da rede acentua-se neste caso, pois os percursos seriam alterados e os nós, ao detectarem falha na tentativa de envio pela rota preexistente, iniciariam uma nova requisição de rota para corrigir a alteração na rede, ocasionando uma latência de envio, que já é peculiarmente alta devido a metodologia reativa de inundação de mensagens, ainda maior.

Os algoritmos proativos, por sua vez, são os mais afetados por essa ocorrência. Por serem *table-driven*, conduzidos fortemente pelas informações associadas ao armazenamento de rotas na tabela de roteamentos dos nós, seu comportamento é intrinsecamente inconveniente a este modelo.

As ocorrências de alteração topológicas afetam a configuração dos percursos e, consequentemente, implicam em necessidade constante de verificação/aplicação de correção nas rotas, por todos os nós na rede.

O modelo proposto neste trabalho apresenta singularidades. Como a comunicação é orientada a um nó específico, nesta configuração apresentada, conforme as mensagens são disseminadas na rede, os algoritmos reativos passam a assumir equitativamente essa propriedade, pois passam a basear-se prioritariamente na informação de roteamento já existente na tabela de roteamento dos nós.

Percebe-se, após estas constatações, que ambas as metodologias de roteamento reativas e proativas apresentam um fundamentos funcionais inadequados ao modelo proposto, no sentido de comunicação à partir dos nós até a prefeitura. Isto deve-se a particularidade de a comunicação ser orientada a um único destino específico.

Nesta configuração, que é a apresentada pelo modelo do sistema de iluminação pública inteligente, o modelo de comunicação proposto apresentou-se eficiente no tratamento dos desvios funcionais presentes nas abordagens reativas e proativas.

Ainda sobre este sentido de comunicação, em que os nós enviam

mensagens até a prefeitura, considerou-se a utilização de algoritmos com metodologias híbridas. Verificou-se que o impacto gerado pelos algoritmos de roteamento híbridos, baseados em zonas, dá-se pela necessidade inevitável de recalcular e realocar as zonas. Conforme alteração na configuração dos nós na rede, gera-se a imposição de definir novamente os nós responsáveis pela propagação das mensagens.

Esta alteração na configuração da rede ao inserir novos nós pode ocasionar, em todos os nós, o efeito da remoção/inserção em novas zonas e estes poderão assumir o papel de difusores de mensagem de roteamento, bem como deixar de assumir este papel na rede.

Associadamente, por serem algoritmos de roteamento híbridos, existe a difusão de mensagens na rede e a interação com a tabela de roteamento intrínseca, de modo ainda contundente, havendo, portanto, os mesmos agravantes mesmo que minimizados pelas técnicas dispostas nos algoritmos.

Após a analise dos algoritmos existentes nas diferentes classificações existentes e da abstração dos seus métodos de implementação, decidimos implementar um modelo característico ao sistema proposto, aproveitando-se do conhecimento teórico adquirido para desenvolver a que consideramos a melhor abordagem para o sistema de iluminação pública no referido sentido de comunicação de mensagens nós-prefeitura.

Esta decisão veio após analisar as ocorrências já defasados pelos anteriores protocolos de comunicação. Percebe-se a seguir como as ocorrências são minimizadas através do modelo proposto.

A figura 76 apresenta a configuração da rede após a execução do algoritmo desenvolvido, conforme visto no capítulo anterior.

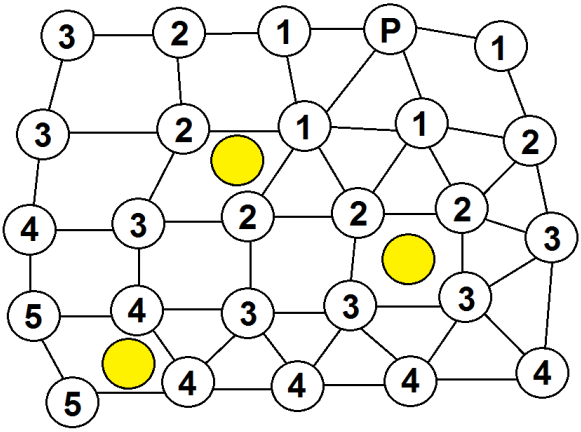


Figura 75 – nós inseridos no modelo proposto

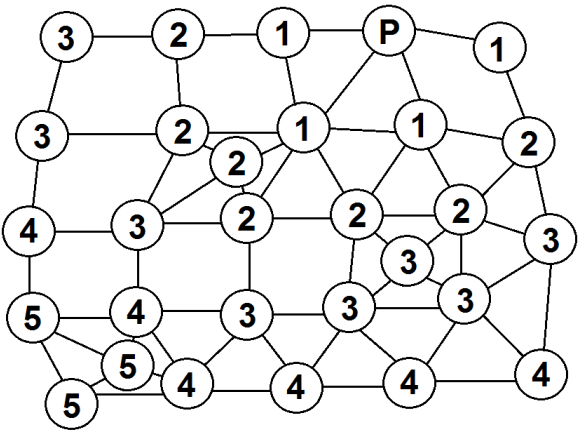


Figura 76 – Resultado após a inserção

Percebe-se, a partir da figura 76 que a inclusão destes nós minimizou severamente o efeito da ocorrências sobre os demais nós. A alteração não afetou os demais nós da rede, tampouco houve necessidade alguma de alteração na configuração em algum destes. O próprio nó, ao detectar os nós em sua vizinhança, segundo definição de sua implementação, atualiza a sua posição na rede.

Nesta metodologia a comunicação não fica refém da atualização

dos dados, já que a inserção do nó não obstrui nenhuma rota preexistente pela descaracterização dos vínculos entre rotas e percursos das mensagens. O modelo proposto desvincula a comunicação com as rotas. A inserção de um novo nó irá apenas gerar uma nova alternativa de percurso ou contribuir para a redução de saltos até o nó de destino P.

No modelo proposto não há a pronta ou periódica necessidade de inundar a rede com pacotes de requisição de rota ou de manter informações de rotas ponta-a-ponta. Os nós inseridos adequam-se a rede e aos demais nós.

5.0.1.1 Falhas ou remoção de nós

A ocorrência de falha de comunicação entre os nós é o resultado proveniente da tentativa insucedida de envio e recebimento de mensagens por um dos nós envolvidos na comunicação, seja esta por falha propriamente dita no funcionamento de pelo menos um dos nós envolvidos na comunicação ou por remoção do nó, que também irá configurar uma falha na comunicação.

Assim como a introdução de um novo nó na rede, a falha irá gerar uma alteração na configuração da rede e deve ser contornada pelo algoritmo com o mínimo de interferência possível sobre o seu funcionamento regular.

Nos algoritmos reativos, a falha é contornada de maneira similar à inserção de um novo nó, quanto este altera o percurso de envio da mensagem enviada. Sendo esta ocorrência nula, nos protocolos reativos, em situações onde a comunicação é inédita entre o nó de origem e o nó de destino. Nestas situações, os algoritmos reativos implementam sua rotina de difusão de mensagens de requisição de rota e esta alteração será contornada de antemão. Todavia, como a comunicação no modelo de estudo é orientada ao destino, há a particularidade de os nós adquirirem conhecimento sobre esta rota ao passar do tempo, descaracterizando sua busca por novas rotas - como descrito em capítulos anteriores, os modelos reativos armazenam a rota de envio percorrida no nó de origem, em sua tabela de roteamento, sempre que uma mensagem é enviada.

Em caso de falhas de comunicação, nos protocolos reativos, no

modelo proposto, devido a característica observada de aquisição de conhecimento sobre as rotas, essa busca será feita predominantemente através do reenvio de mensagens de requisição de rota, após a verificação de que a falha afetou o percurso de envio preexistente, gerando um *delay* indesejável em função necessidade de reenvio.

Esse evento de falha irá gerar uma quebra de link entre os nós e é passível de correção apenas após o diagnóstico, haja vista que os nós necessitam tentar interagir entre si para que tal alteração na configuração da rede seja reconhecida.

Em situações onde a quebra de link está distante, a dificuldade verificada em alguns algoritmos para realizar essa correção é notória e crítica, pois há a necessidade de varrer a rede periodicamente de ponta-a-ponta, havendo um excesso de mensagens e utilização da largura de banda incrementados ao funcionamento da rede.

Nos protocolos proativos, a atuação dos algoritmos evidenciam um forte comprometimento da performance em caso de falhas. As falhas alteram as rotas que, por sua vez, são fatores críticos para a performance da comunicação, pois as rotas são elementos inassociáveis e exclusivos ao envio e recebimento das mensagens neste protocolo de comunicação.

No modelo proposto, conforme apresenta a figura 78, a ocorrência de falhas representa alterações locais aos nós dentro das zonas de alcance, onde as falhas estão contidas, afetando apenas os nós adjacentes ao ponto de falha e em casos extraordinários. Algum nó nesta zona será afetado apenas se não há um outro nó interligado com a mesma quantidade de saltos até a prefeitura.

Mesmo quando há alteração na configuração da rede, os nós a corrigem prontamente, após a varredura periódica. Esta eleição dará-se pela nova eleição de nós com o menor número de saltos até a prefeitura e consequentemente descarte do nó alvo de falha.

Através do procedimento de eleição de nós com menor número de saltos até a prefeitura, cujo qual é parâmetro para configuração própria, em função da atualização da quantidade de saltos particular até a prefeitura, define-se a nova configuração particular de cada nó na rede. Sendo esta alterada apenas caso o novo nó eleito possua parâmetro

(quantidade de saltos até a prefeitura) diferente dos anteriores, alvos de falha.

As figura 77 apresenta a simulação da ocorrência de falha em determinadas regiões diferentes da rede, sobre os nós na rede.

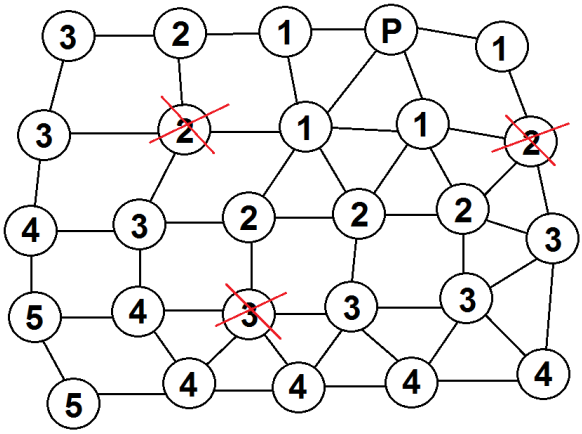


Figura 77 – Ocorrência de falhas no modelo proposto

As figura 78 apresenta o resultado após a ocorrência de falhas na rede. E a figura a seguir, figura 79 apresenta a rede após a execução do modelo proposto.

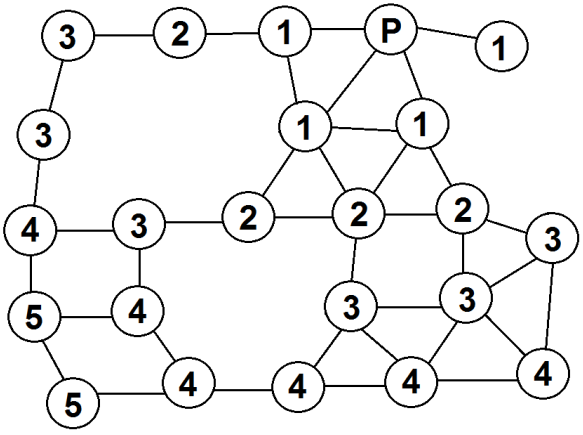


Figura 78 – Resultado após a falha no modelo proposto

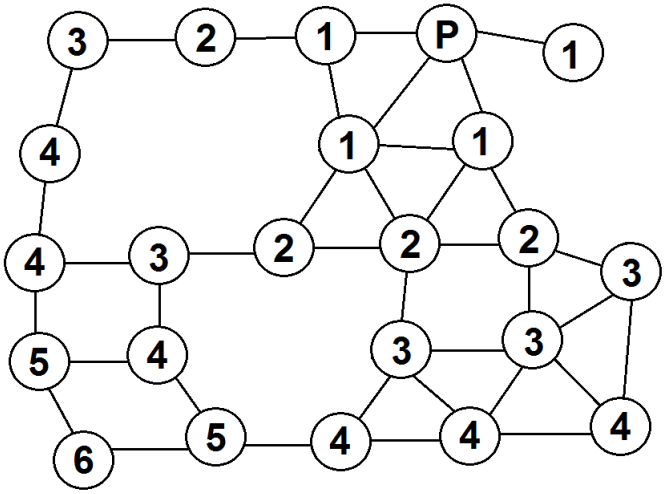


Figura 79 – Resultado após a falha no modelo proposto

É possível identificar na figura 79 que esta ocorrência afetou minimamente a configuração da rede, como esperado pela metodologia adotada no desenvolvimento do modelo proposto.

5.0.1.2 Tempo de envio das mensagens

O tempo de envio das mensagens, neste modelo, pode ser representado pela quantidade de arestas percorridas pela mensagem em função do tempo de comunicação entre os nós situados nas extremidades destas arestas. Somando-se assim a quantidade de arestas percorridas pela mensagem.

Esse cálculo é razoável e pode ser considerado já que a distância entre os postes em um sistema de iluminação pública é aproximadamente constante.

Para o modelo proposto, representado na figura 73, o tempo T de envio das mensagem para percorrer a rede de ponta-a-ponta, na pior das hipóteses é 5*T.

Este tempo é, teoricamente, o mínimo possível pois a comunicação é feita ponto-a-ponto entre os nós dentro da zona de alcance do

sinal, restringindo-se o envio ao nó que possui a menor quantidade de saltos até o nó de destino da mensagem. As demais metodologias de envio, considerando-se o uso da tecnologia 802.11 e seu alcance limitado, foram pautadas e refutadas por serem consideradas indiretas em relação a esta.

5.0.1.3 Quantidade de nós envolvidos na mensagem

A quantidade de nós envolvidos na troca de mensagens é função das metodologias existentes no algoritmo, sejam estas para descoberta de rota, comunicação efetivamente dita ou quaisquer correções necessárias.

A dimensão deste parâmetro está diretamente atrelada ao uso da largura de banda da rede, possível sobrecarga de processamento sobre os nós, ativação excessiva dos nós, consumo maior de energia e diminuição da vida útil do dispositivo.

A descoberta por novas rota só ocorre diretamente entre os nós adjacentes entre si, os quais estão dentro da região de alcance do sinal WiFi, não envolvendo os demais nós no processo.

Este procedimento atualiza a configuração para todos os nós da rede, diferentemente dos modelos onde a requisição é difundida na rede, afetando vários nós até que se atinja o nó de destino, nos quais atualiza-se apenas a rota específica entre a origem e o destino para aquele nó que requisitou a rota.

As zonas da rede se sobrepõe umas às outras 80, havendo convergência no sentido de transmissão entre os nós, facilitando o mecanismo de envio da mensagem até o destino (nó P).

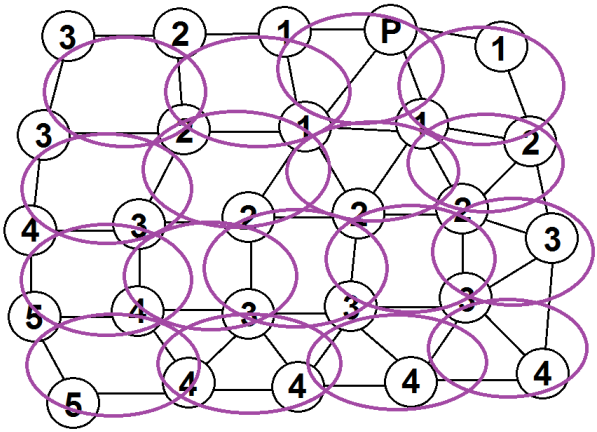


Figura 80 – Sobreposição das zonas na rede

Percebe-se que o modelo desenvolvido tem como propósito minimizar a multiplicação de mensagens na rede e o número de nós envolvidos. Todos os processos de comunicação foram desenvolvidos otimizando a interação entre os nós. Seja no envio, conhecimento da rede, atualização do conhecimento da rede, contorno à falhas, inserção de novos nós, etc.

6 CONSIDERAÇÕES FINAIS

Este trabalho possibilitou entender melhor o que considera-se um novo paradigma para a arquitetura de informação: a Internet das Coisas. Nele avaliou-se, no contexto das Cidades Inteligentes e Indústria 4.0, a implementação de um sistema de iluminação pública inteligente.

A revisão bibliográfica, através de artigos científicos produzidos na área, permitiu abstrair conceitos e prospecções sobre aspectos técnico-econômicos, tecnologias disponíveis, os modelos de comunicação utilizados e as inovações que prometem promover, através da informação, a interação entre os objetos sem a necessidade de intervenção humana. Acredita-se que a Engenharia de Computação tenha uma representatividade muito significativa nesta área, através das tecnologias embarcadas.

Ao concluir o presente trabalho constatou-se que o sistema embarcado proposto atende os requisitos desejáveis, mesmo que parcialmente, para a implementação de um sistema de iluminação pública inteligente.

Considera-se que, embora haja margens para melhorias e otimização no sistema proposto, o sistema elaborado vai de encontro às necessidades da aplicação e alcançaram-se os resultados esperados na pesquisa, tais como: avaliação das tecnologias sem fio e respectivos protocolos de comunicação, escolha de um microcontrolador apropriado, analise dos algoritmos de redes sem fio Ad hoc e projeto e implementação de um modelo de comunicação otimizado para o funcionamento de um sistema de iluminação pública.

Validou-se a proposta de desenvolver um modelo de gerenciamento do sistema de iluminação pública que contemplasse a atuação de um sensor e a comunicação bi-direcional entre os nós.

Esta atividade, representada através do controle do acionamento das lâmpadas dos postes e do envio do status das lâmpadas ao sistema de gerenciamento identificou a capacidade de agregar tecnologia embarcada ao sistema de iluminação pública, tornando-o mais eficiente, gerenciável e autônomo.

Verificou-se que este sistema embarcado pode abranger diversas aplicações além da apresentada neste trabalho, havendo real potencial de incorporação do sistema pelas prefeituras.

6.1 TRABALHOS FUTUROS

Possíveis trabalhos futuros relacionados ao Sistema de Iluminação Pública Inteligente:

- Implementar o modelo de comunicação desenvolvido para funcionamento com outras tecnologias;
- Otimizar o modelo de propagação das mensagens da prefeitura até os nós;
- Implementar as funcionalidades citadas como passíveis de aplicação;
- Transpor o algoritmo desenvolvido, do modelo de comunicação, para um simulador, com o propósito de verificar as taxas de probabilidade de ocorrência de erros associados ao funcionamento do sistema com um número elevado de nós, na ordem existente em um sistema de iluminação pública;
- Aumentar as funcionalidades da aplicação;
- Descobrir novas aplicações, derivadas da implementação do presente trabalho, que possam viabilizar cada vez mais a sua implementação.

REFERĘNCIAS

ADELANTADO, F. et al. Understanding the limits of lorawan. v. 55, 06 2017.

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA - ANEEL. Resolucão normativa nº 414, artigo 218. p. 133, 2010.

AGGARWAL, N. et al. Relative analysis of aodv & dsdv routing protocols for manet based on ns2. p. 3500–3503, 03 2016.

ALABADY, S.; SALLEH, M. F. M.; HASIB, A. Throughput and delay analysis of ieee 802.11 dcf in the presence of hidden nodes for multi-hop wireless networks. v. 79, p. 907–927, 11 2014.

ALLIANCE, L. Lorawan: what is it. 2015.

ALOTAIBI, E.; MUKHERJEE, B. A survey on routing algorithms for wireless ad-hoc and mesh networks. *Computer Networks*, v. 56, n. 2, p. 940 – 965, 2012. ISSN 1389-1286. <http://www.sciencedirect.com/science/article/pii/S138912861100377X>.

AMARAL, H. *Medidor de corrente AC com ACS712 e Emonlib*. 2017.

AMARAL, H. *Medidor de corrente AC com ACS712 e Emonlib*. 2017.

ANDREWS, J. G.; GHOSH, A.; MUHAMED, R. Fundamentals of wimax. v. 5, 02 2007.

ARAUJO, A. S. de; VASCONCELLOS, P. de. *Bluetooth Low Energy*. 2012. $<https : //www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2012_2/bluetooth/index.htm>$.

ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: A survey. *Computer Networks*, n. 54(15), p. 2787–2805, 2010.

AUGUSTIN, A. et al. A study of lora: Long range and low power networks for the internet of things. *Sensors*, v. 16, n. 9, 2016. ISSN 1424-8220.

AUGUSTO, E. et al. *OFDMA e WCDMA*. 2006.

BIRADAR, S. R. et al. Hybrid (day-night) routing protocol for mobile ad-hoc networks. In: *2008 International Conference on Recent Advances in Microwave Theory and Applications*. [S.l.: s.n.], 2008. p. 875–877.

BISDIKIAN, C. An overview of the bluetooth wireless technology. v. 39, p. 86 – 94, 01 2002.

BRASIL, W. *Uma visão técnica da Rede Sigfox*. 2017. $<https://www.embarcados.com.br/uma-visao-tecnica-da-rede-sigfox/>$.

C, M. R. et al. Study on zigbee technology. p. 297–301, 04 2011.

CHO, K. et al. Performance analysis of device discovery of bluetooth low energy (ble) networks. *Computer Communications*, v. 81, p. 72 – 85, 2016. ISSN 0140-3664. <http://www.sciencedirect.com/science/article/pii/S0140366415003886>.

CLAUSEN, E. T.; JACQUET, E. P. Optimized link state routing protocol (olsr). 10 2003.

COSTAUR, K. A. A.; MENDES, L. A. M. Evolução das redes sem fio: Um estudo comparativo entre bluetooth e zigbe. 2014.

DESHMUKH, S.; BHOSLE, U. Performance evaluation of spread spectrum system using different modulation schemes. *Procedia Computer Science*, v. 85, p. 176 – 182, 2016. ISSN 1877-0509. International Conference on Computational Modelling and Security (CMS 2016). <http://www.sciencedirect.com/science/article/pii/S1877050916305555>.

ESPRESSIF. *ESP8266 datasheet*. 2018. $<https://www.espressif.com/sites/default/files/documentation/0a-esp8266ex_datasheet_en.pdf>$.

EVANS, D. The internet of things: How the next evolution of the internet is changing everything. p. 2–3, 2011.

FLICKENGER, R. *Wireless Networking in the Developing World*. Limehouse Book Sprint Team, 2006. ISBN 9781411678378. <https://books.google.com.br/books?id=BSmcUJo_qIIC>.

GIANNOULIS, S. et al. Zrp versus dsr and tora: a comprehensive survey on zrp performance. In: *2005 IEEE Conference on Emerging Technologies and Factory Automation*. [S.l.: s.n.], 2005. v. 1, p. 8 pp.–1024. ISSN 1946-0740.

GOMEZ, C.; OLLER, J.; PARADELLS, J. *Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology*. 2012.

GUAINELLA, E. et al. Wimax technology support for applications in environmental monitoring, fire prevention and telemedicine. In: *2007 IEEE Mobile WiMAX Symposium*. [S.l.: s.n.], 2007. p. 125–131.

HARGREAVES, E. O protocolo csma-ca e o padrão ieee 802.11. 2017.

HE, G. Destination-sequenced distance vector (dsdv) protocol. 06 2002.

HIERTZ, G. R. et al. The ieee 802.11 universe. *IEEE Communications Magazine*, v. 48, 2010.

INFO, G. *LoRa Tutorial – What is LoRa Wireless for IoT?* 2017. $<http://www.3glteinfo.com/lora/lora-architecture/>$.

JACQUET, P. et al. Optimized link state routing protocol for ad hoc networks. In: *Proceedings. IEEE International Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century.* [S.l.: s.n.], 2001. p. 62–68.

JOHNSON, D. B.; HU, Y.-C.; MALTZ, D. A. The dynamic source routing protocol (dsr) for mobile ad hoc networks for ipv4. *RFC*, v. 4728, p. 1–107, 2007.

JOHNSON, D. B.; MALTZ, D. A.; BROCH, J. Ad hoc networking. In: . Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2001. cap. DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks, p. 139–172. ISBN 0-201-30976-9. <http://dl.acm.org/citation.cfm?id=374547.374552>.

JOHNSON, D. B.; MALTZ, D. A.; BROCH, J. Ad hoc networking. In: . Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2001. cap. DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks, p. 139–172. ISBN 0-201-30976-9. <http://dl.acm.org/citation.cfm?id=374547.374552>.

JUN, M. The study on multi-path dsdv in ad hoc. In: *2011 IEEE 3rd International Conference on Communication Software and Networks*. [S.l.: s.n.], 2011. p. 299–303.

JUNIOR, V. P. da S. *Conheça a tecnologia LoRa e o protocolo LoRaWAN*. 2016. <*https* : *//www.embarcados.com.br/conheca − tecnologia − lora − e − o − protocolo − lorawan/*>.

KAUR, M.; SALUJA, K. Performance comparison of mobile ad hoc network routing protocols. v. 6, p. 127–142, 03 2014.

KHATKAR, A.; SINGH, Y. Performance evaluation of hybrid routing protocols in mobile ad hoc networks. In: *2012 Second International Conference on Advanced Computing Communication Technologies*. [S.l.: s.n.], 2012. p. 542–545. ISSN 2327-0632.

KHUTSOANE, O. et al. Iot devices and applications based on lora/lorawan. 2017.

KINNEY, P. *ZigBee Technology: Wireless Control that Simply Works*. 2009. <*https* : *//www.hometoys.com/htinews/oct*03/*articles/kinney/zigbee.html*>.

KUPPUSAMY, P.; THIRUNAVUKKARASU, K.; KALAAVATHI, B. A study and comparison of olsr, aodv and tora routing protocols in ad hoc networks. In: *2011 3rd International Conference on Electronics Computer Technology*. [S.l.: s.n.], 2011. v. 5, p. 143–147.

KUROSE, J.; ROSS, K. *Redes de computadores e a internet: uma abordagem top-down*. ADDISON WESLEY BRA, 2010. ISBN 9788588639973. <https://books.google.com.br/books?id=raZtQwAACAAJ>.

LI, F. et al. Smart transmission grid: Vision and framework. *IEEE Transactions on Smart Grid*, v. 1, n. 2, p. 168–177, Sept 2010. ISSN 1949-3053.

LIMA, L. S. et al. Wimax: Padrão ieee 802.16 para banda larga sem fio. In: . [S.l.: s.n.], 2004. ISSN 0103-9741.

LITEPOINT. *Tabela Comparativa entre as tecnologias Bluetooth e BLE*. 2012. <https://www.litepoint.com/company/white-papers>.

LIU, H. et al. Heterogeneous wireless access in large mesh networks. In: *2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*. [S.l.: s.n.], 2008. p. 233–242. ISSN 2155-6806.

LORIOT, M.; ALJER, A.; SHAHROUR, I. Analysis of the use of lorawan technology in a large-scale smart city demonstrator. In: *2017*

Sensors Networks Smart and Emerging Technologies (SENSET). [S.l.: s.n.], 2017. p. 1–4.

LOUTFI, A.; ELKOUTBI, M. Evaluation and enhancement of zrp performances. In: *2011 International Conference on Multimedia Computing and Systems*. [S.l.: s.n.], 2011. p. 1–6.

MAHDIPOUR, E.; RAHMANI, A. M.; AMINIAN, E. Performance evaluation of destination-sequenced distance-vector (dsdv) routing protocol. In: *2009 International Conference on Future Networks*. [S.l.: s.n.], 2009. p. 186–190.

MANTORO, T.; REZA, M. Performance analysis of aodv and dsdv using sumo, move and ns2. In: *2016 International Conference on Informatics and Computing (ICIC)*. [S.l.: s.n.], 2016. p. 372–376.

MARQUES, E. *Iluminação Pública é porta de entrada para sistemas inteligentes*. 2017. *<https : //www.gazetadopovo.com.br/blogs/cidades − inteligentes/iluminacao − publica>*.

MAURYA, P. K. et al. *An Overview of AODV Routing Protocol*.

MILLAN, A. F. et al. Technological models of municipal wireless networks based on hybrid wifi/wimax mesh networks: a proposal to colombian municipalities. In: *2009 IEEE Latin-American Conference on Communications*. [S.l.: s.n.], 2009. p. 1–6. ISSN 2330-989X.

MOHAMED, M. A.; ZAKI, F. W.; MOSBEH, R. H. Simulation of wimax physical layer: Ieee 802.16e. In: . [S.l.: s.n.], 2010.

NGUYEN, D.; MINET, P. Analysis of mpr selection in the olsr protocol. In: *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*. [S.l.: s.n.], 2007. v. 2, p. 887–892.

OLSON, N. The internet of things. *New Media & Society*, n. 18(4), p. 680–682, 2016.

PESSOA, L. *Introdução ao Bluetooth Smart (BLE)*. 2016. *<https : //www.embarcados.com.br/bluetooth − smart − ble>*.

PETAJAJARVI, J. et al. Evaluation of lora lpwan technology for remote health and wellbeing monitoring. In: *2016 10th International Symposium on Medical Information and Communication Technology (ISMICT)*. [S.l.: s.n.], 2016. p. 1–5. ISSN 2326-8301.

PETAJAJARVI, J. et al. On the coverage of lpwans: range evaluation and channel attenuation model for lora technology. In: *2015 14th International Conference on ITS Telecommunications (ITST)*. [S.l.: s.n.], 2015. p. 55–59.

PINHEIRO, J. M. S. *Multiplexação Ortogonal por Divisão de Freqüência*. 2005. <*http* : *//www.projetoderedes.com.br/artigos/artigo*$_m$*ultiplexacao*$_o$*rtogonal*$_p$*or*$_d$*ivisao*$_d$*e*$_f$*re*

PIRZADA, A. A.; MCDONALD, C. Trusted route discovery with tora protocol. In: *Proceedings. Second Annual Conference on Communication Networks and Services Research, 2004.* [S.l.: s.n.], 2004. p. 121–130.

RAJU, S. R.; RUNKANA, K.; MUNGARA, J. Zrp versus aodv and dsr: A comprehensive study on zrp performance on manets. In: *2010 International Conference on Computational Intelligence and Communication Networks*. [S.l.: s.n.], 2010. p. 194–199.

RAMANATHAN, R.; REDI, J. A brief overview of ad hoc networks: Challenges and directions. v. 40, p. 20–22, 06 2002.

RAUT, S. H.; AMBULGEKAR, H. P. Proactive and reactive routing protocols in multihop mobile ad hoc network. *International Journal of Advanced Research in Computer Science and Software Engineering*, n. 3(4), p. 152, 2013.

RAZA, U.; KULKARNI, P.; SOORIYABANDARA, M. Low power wide area networks: An overview. *IEEE Communications Surveys Tutorials*, v. 19, n. 2, p. 855–873, Secondquarter 2017. ISSN 1553-877X.

RIBEIRO, G. G. L. et al. An outdoor localization system based on sigfox. In: *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. [S.l.: s.n.], 2018. p. 1–5. ISSN 2577-2465.

ROYER, E. M.; PERKINS, C. An implementation study of the aodv routing protocol. v. 3, p. 1003 – 1008 vol.3, 02 2000.

ROYER, E. M.; TOH, C.-K. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications*, n. 1070-9916/99, p. 46–53, 1999.

SAIRAM, K.; GUNASEKARAN, N.; REDD, S. Bluetooth in wireless communication. v. 40, p. 90 – 96, 07 2002.

SEYEDZADEGAN, M.; OTHMAN, M. Ieee 802.16: Wimax overview, wimax architecture. v. 5, p. 784–787, 01 2013.

SHARMA, P. K.; SAXENA, A. S. Comparison analysis between ieee 802.11a/b/g/n. In: . [S.l.: s.n.], 2013.

SIGFOX. Sigfox tecnhical overview. In: . [S.l.: s.n.], 2017.

SILVA, J. de C. et al. Lorawan - a low power wan protocol for internet of things: a review and opportunities. 07 2017.

SOARES, F. E.; BARRIQUELLO, C. ComunicaçÃo sem fio com ampla cobertura para redes elÉtricas inteligentes em meio rural. p. 7, 2017.

STEPHENS, J.; NORMAN, D. Direct-sequence spread spectrum system. 1991. Proceedings of the IEEE 1991 National Aerospace and Electronics Conference (NAECON). <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=165790>.

TANENBAUM, A. *Redes de computadores.* CAMPUS - RJ, 2003. ISBN 9788535211856. <https://books.google.com.br/books?id=0tjB8FbV590C>.

THIAGARAJAN, R.; MOORTHI, M. Efficient routing protocols for mobile ad hoc network. In: *2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*. [S.l.: s.n.], 2017. p. 427–431.

TOMAR, A. Introduction to zigbee technology. *element14*, v. 1, 2011.

TOWNSEND, K.; CUFÍ, C.; DAVIDSON, R. *Getting Started with Bluetooth Low Energy: Tools and Techniques for Low-Power Networking.* O'Reilly Media, 2014. (EBSCOhost ebooks online). ISBN 9781491900581. <https://books.google.com.br/books?id=AIR7AwAAQBAJ>.

VEJLGAARD, B. et al. Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot. In: *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*. [S.l.: s.n.], 2017. p. 1–5.

VENKATESAN, T. P.; RAJAKUMAR, P.; PITCHAIKKANNU, A. Overview of proactive routing protocols in manet. p. 173–177, 04 2014.

WU, J.; STOJMENOVIC, I. Guest editors' introduction: Ad hoc networks. *Computer*, v. 37, p. 29–31, 02 2004. ISSN 0018-9162. <doi.ieeecomputersociety.org/10.1109/MC.2004.1266292>.

YI, Z. et al. Zigbee technology application in wireless communication mesh network of ice disaster. *Procedia Computer Science*, v. 52, p. 1206 – 1211, 2015. ISSN 1877-0509. The 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015). <http://www.sciencedirect.com/science/article/pii/S187705091500959X>.

YOUSSEF, A. V. M.; MILLER, R. Specification and analysis of the dcf and pcf protocols in the 802.11 standard using systems of communicating machines. 11 2012. ISSN 1092-1648.

YU, Y. M. Q.; QIN, Z. Researches on ieee 802.11 access mechanism. 2008.