GUILHERME NUNES NASSEH BARBOSA

MONITORAÇÃO DE TRANSFORMADORES DE POTÊNCIA UTILIZANDO TECNOLOGIA WIRELESS NA DETECÇÃO DE FRAUDES

Niterói
2016

GUILHERME NUNES NASSEH BARBOSA

MONITORAÇÃO DE TRANSFORMADORES DE POTÊNCIA UTILIZANDO TECNOLOGIA WIRELESS NA DETECÇÃO DE FRAUDES

Trabalho de Conclusão de Curso Apresentado ao Curso de Graduação em Engenharia de Telecomunicações da Universidade Federal Fluminense para obtenção do Grau Engenheiro de Telecomunicações.

Universidade Federal Fluminense – UFF
Centro Tecnológico
Escola de Engenharia

Orientador: Prof. Dr. João Marcos Meirelles da Silva

Niterói
2016

GUILHERME NUNES NASSEH BARBOSA

MONITORAÇÃO DE TRANSFORMADORES DE POTÊNCIA UTILIZANDO TECNOLOGIA WIRELESS NA DETECÇÃO DE FRAUDES

Trabalho de Conclusão de Curso Apresentado ao Curso de Graduação em Engenharia de Telecomunicações da Universidade Federal Fluminense para obtenção do Grau Engenheiro de Telecomunicações.

Trabalho aprovado. Niterói, XX de XXX de 2016:

Prof. Dr. João Marcos Meirelles da Silva
Orientador

Profª. Drª. Natália Castro Fernandes
UFF

Prof. Dr. Ricardo Campanha Carrano
UFF

Niterói
2016

Agradecimentos

Resumo

O furto e a fraude de energia elétrica são fatos que causam grandes prejuízos e, consequentemente, a deteriorização do serviço prestado. Tais práticas podem ser facilmente detectadas atráves da implementação e da utilização de sensores na rede elétrica, de modo a monitorar a energia a ser entregue pelos transformadores de tensão. Este trabalho tem como objetivo o desenvolvimento de um modelo capaz de detectar e monitorar tanto o furto quanto a fraude, sem intervenção humana, através de uma rede mesh. Com a utilização de plataformas opensource, é possível elaborar uma infraestrutura para a aquisição e transmissão dos dados referentes ao valor de potência entregue pelo transformador. Esse valor seria comparado com a soma da potência entregue a todos os estabelecimentos em que atua o transformador em questão. Caso o valor obtido seja maior do que a soma das potências, pode-se concluir que houve perda, furto ou fraude de energia elétrica em dada localidade.

Palavras-chave: Telecomunicações, Redes, Wireless, Eletricidade, Fraude, Sensores, Monitoramento, IEEE 802.11.

Abstract

Eletric energy theft and fraud are facts that cause huge damages and hence deterioration of service. These practices could be easily detected through the implementation and use of sensors in the power grid in order to monitor the energy to be delivered by voltage transformers. This paper aims to develop a model to detect and monitor a theft, such as a fraud, whitout human intervention, through a mesh network. Using opensource platforms, it is possible to develop an infrastructure for acquisition and transmission of data on the amount of power delivered by the transformer. This value would be compared to the sum of the power delivered to all the establishments in which the transformer operates. If the value is bigger than the sum of powers, it is possible to conclude that there have been loss, theft or fraud of eletric energy in the studied place.

Keywords: Telecomunications, Networks, Wireless, Eletricity, Fraud, Sensors, Monitoring, IEEE 802.11.

Lista de ilustrações

Lista de abreviaturas e siglas

AMI	Advanced Metering Infrastructure
ANATEL	Agência nacional de telecomunicações
CF	Compact Flash
DAP	Data Aggregation Point
EIRP	Equivalent isotropically radiated power
EMT	Equipamento de medição e transmissão
GB	Gigabyte
IEEE	Institute of Electrical and Eletronics Engineers
IoT	Internet of Things
IP	Internet Protocol
ITU-T	Telecommunication Standardization Sector
ISM	Industrial, Scientifc and Medical
MAN	Metropolitan Area Network
ODP	Open Data Plattaform
OFDM	Orthogonal Frequency Division Multiplexing
OLSR	Optimezed Link State Routing
OSI	Open Systems Interconnection
PoE	Power Over Ethernet
MID	Multiple Interface Declaration
MPR	Multipoint Relay
PCI	Peripheral Componetn Interconnect
RAM	Random Access Memory
RF	Radiofrequência
SNMP	Simple Network Management Protocol

SNR	Signal Noise Ratio
SO	Sistema Operacional
TC	Topology Control
UFF	Universidade Federal Fluminense
UK-DALE	United Kingdom – Domestic Appliance Level Electricity
UTP	Unshielded twisted pair
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WISP	Wireless Internet Service Provider
WLAN	Wireless local area network
WMSN	Wireless Mesh Sensor Networks

Sumário

1 Introdução

A energia elétrica, desde sua descoberta, se tornou indispensável ao desenvolvimento humano. Cada vez mais a sua utilização se torna vital, tanto para atividades simples, como acender uma lâmpada, quanto para atividades complexas, em grandes indústrias, por exemplo.

O custo da energia elétrica é um fator muito importante na economia de um país. O aumento das tarifas pode impactar diretamente na inflação, o que afeta toda a cadeia produtiva, e a população consegue perceber isso prontamente.[1]

No caso da energia elétrica, o custo, desde a geração até chegar a residências e estabelecimentos comerciais, é dividido entre todos os consumidores[2].Desta forma, todos pagam pela energia que é gerada, transmitida e distribuída. Como consequência, todos arcam com os custos da energia furtada. Nessa perspectiva, a redução nos índices de furto implica numa possível diminuição de tarifas.[3]

As distribuidoras de energia elétrica sofrem altas perdas por motivos técnicos e comerciais. As perdas técnicas provêm principalmente de um fenômeno conhecido como efeito joule, que é a perda associada ao aquecimento de fios condutores. Já as perdas comercias são, geralmente, caracterizadas como furtos e fraudes na rede elétrica.

Os furtos fazem com que a energia consumida não seja contabilizada, o que ocorre, por exemplo, no caso das ligações clandestinas em postes. As fraudes, por sua vez, podem ser descritas como adulterações realizadas nos sistemas, a fim de burlar a correta tarifação. Ambas as práticas, são popularmente conhecidas como “gato”.[4]

Em virtude dos fatos apresentados, é possível, por meio das telecomunicações, monitorar todas essas questões, utilizando uma rede de sensores. Assim sendo, seria possível mapear áreas em que incidam tais práticas, a fim de adotar as medidas cabíveis para coibí-las, visto que haveria o material probatório necessário para a responsabilização dos infratores.

1.1 Problema - Motivação

Em diversos sistemas, sejam eles de energia elétrica ou de serviços bancários, por exemplo, existem cobranças adicionais das respectivas empresas, voltadas para minimizar o prejuízo das fraudes. Isso significa que as pessoas, ao contraterem estes serviços, já estão pagando por isso.

Tanto o furto quanto a fraude trazem diversos danos à sociedade, além dos prejuizos financeiros. Provavelmente, seria possível implementar melhorias na qualidade do fornecimento, revertendo o custo extra para tal finalidade. Há, ainda, a possibilidade de sobrecarga nos transformadores de média tensão, deixando sem energia elétrica todos os usuários de tal sistema.

Muitas dessas atividades ilícitas costumavam ser feitas apenas por pessoas que detinham um conhecimento técnico sobre redes elétricas. No entanto, atualmente, o conhecimento para pôr em práticas tais atividades pode ser facilmente encontrado na internet, em tutoriais também conhecidos como *howto*, onde pessoas publicam vídeos e documentos, contendo o passo a passo ou maneiras de concretizar essas ações.

Por conta da facilidade na execução de tais procedimentos, o índice de furtos cresce em todas as esferas da sociedade. Alguns números são bem expressivos, principalmente no que concerne ao furto. No Rio de Janeiro, por exemplo, estima-se que uma redução no número de ligações clandestinas permitiria uma queda em até 17% nas contas de luz.

De acordo com números divulgados pela concessionária Light, as perdas comerciais para a região metropolitana do Rio de Janeiro estariam próximas de R$ 2 bilhões por ano. Isso significa que todo o furto realizado nesta localidade seria equivalente ao consumo de todo o Estado do Espírito Santo.[5]

Já existe um vasto estudo, acerca de redes elétricas inteligentes ou também chamadas de *smart grids*. Este conceito, possui como principais motivações, o monitoramento e automação da rede elétrica, desde sua geração até a distribuição para o usuário final.

A implementação deste modelo poderia ajudar os consumidores e distribuidores, uma vez que as medições de consumo, por exemplo, seriam realizadas de maneira mais rápida e precisa, sem a necessidade de deslocamento de equipes. Há ainda, a possibilidade de combate das perdas comerciais, como fraude e furto.

Através do monitoramento constante, é possível gerar um grande volume de dados, extraindo informações vitais para a manutenção e melhorias da rede em tempo real, reduzindo, por exemplo, o tempo de ação para resolução de problemas.

Considerando a necessidade de minimizar perdas por furto e por fraude de energia elétrica, pode-ser ter como metas a inovação tecnológica e a conscientização social, além de operações de fiscalizações.

Uma vez que inovações tecnológicas são implementadas, em contrapartida, a sociedade recebe benefícios, pois os serviços poderão ser oferecidos com melhor qualidade e baixo custo, gerando desta forma até mesmo qualidade de vida para os cidadãos.

1.2 Objetivo

Este trabalho tem como objetivo encontrar uma forma eficiente e de fácil implementação para a detecção de áreas com incidência de furtos e fraudes, por meio de uma infraestrutura de telecomunicações.

O modelo de distribuição de energia elétrica utilizado pelas concessionárias, embora seja o mesmo utilizado há algumas décadas, facilita tal detecção, uma vez que as residências, pequenos comércios e indústrias são atendidos por áreas limitadas a alguns metros dos transformadores de média para baixa tensão. Em boa parte do território brasileiro, a tensão transformada é de 13,8 kV para 220 V ou 127 V.[6] Em alguns casos, por exemplo, a energia fornecida é feita em média tensão.

O monitoramento contínuo destas áreas, pela análise do padrão de consumo e dos comparativos com os medidores das unidades, pode levar à empresa distribuidora uma forma eficiente para coibir práticas criminosas em áreas específicas.

As concessionárias tem conhecimento quais unidades são atendidas por cada transformador, o que facilita a localização, uma vez que os técnicos precisariam visitar apenas algumas destas unidades (comerciais ou residenciais) para constatar a ilegalidade.

Paralelamente, esta infraestrutura poderá servir para localizar falhas de distribuição, uma vez que a interrupção da medida no secundário do transformador, pode indicar falha no transformador ou no fornecimento de média tensão, uma vez que o equipamento de transmissão poderá ser alimentado diretamente pela baixa tensão, entregue pelo transformador.

1.3 Metodologia

Para o desenvolvimento de um modelo de monitoramento do consumo de energia elétrica, este trabalho sugere a instalação de um equipamento de medição e transmissão (EMT) no secundário dos transformadores de média para baixa tensão.

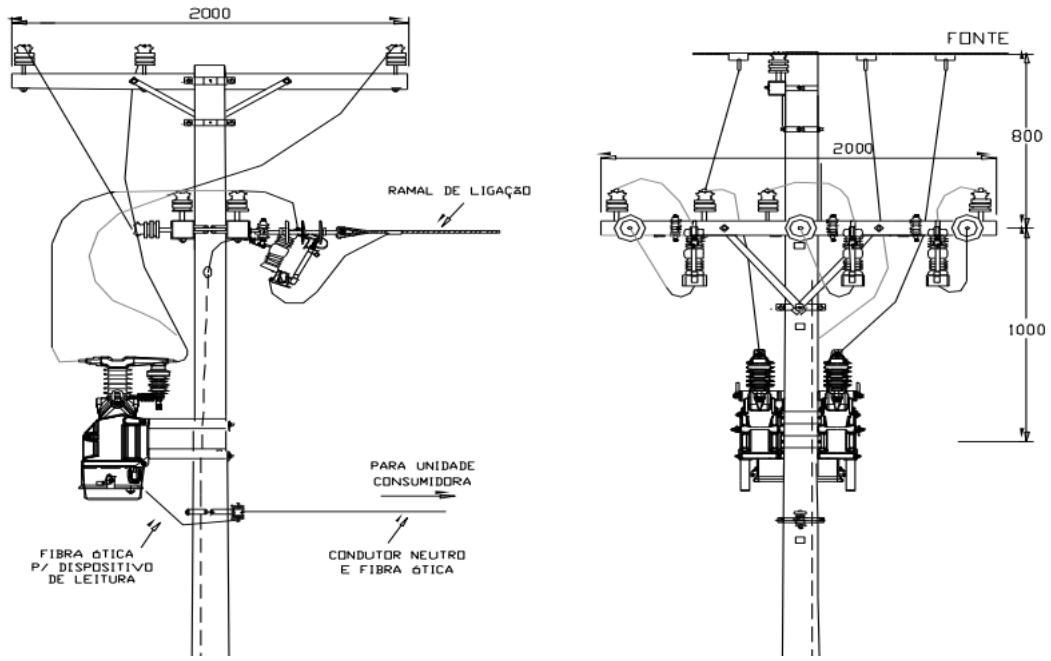
Esta infraestrutura permitirá a coleta de dados acerca da energia elétrica entregue pelo transformador e a comunicação entre os EMT's através do protocolo IEEE 802.11, popularmente conhecido como Wi-Fi, formando assim uma rede em malha. Desta forma, será possível transmitir as informações referentes aos transformadores monitorados, utilizando somente alguns destes EMT's como *gateways* para se comunicarem diretamente com a concessionária. Essa comunicação poderá ocorrer através do padrão IEEE 802.16 conhecido como WiMAX (MAN) ou através de tecnologias como 3G e 4G (WAN).

Cada EMT é composto por uma *sytem board*, sendo esta responsável pelo processamento e transmissão dos dados coletados. A *system board* utilizada, da marca PC Engine modelo Alix, possui uma capacidade satisfatória de processamento, com 500 Mhz de *clock* de processador e 256 MB de memória RAM. Como possui um poder de processamento maior

em comparação à outros modelos, este equipamento pode ser utilizado como *gateway* da rede, ou também como DAP.

A figura 1 ilustra o desenho técnico da concessionária Ampla, para um Conjunto de Medição em Subestação de 75 kVA a 300 kVA.

Figura 1 – Conjunto de Medição em Subestação de 75 kVA a 300 kVA

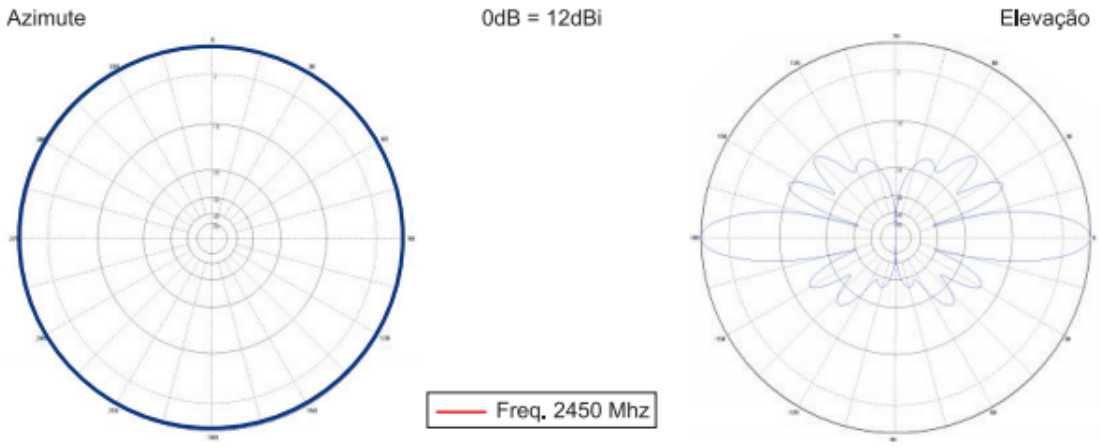


Fonte: https://www.ampla.com/a-ampla/normas-técnicas/normas-técnicas-de-distribuição.aspx

A *sytem board* permite a conexão de dois cartões de radiofrequência (RF) do tipo mini-PCI. Neste caso será utilizado apenas um para estabelecer a rede em malha. Tais cartões operam no padrão 802.11 a/b/g com modulação do tipo OFDM, e a vantagem destes, é a utilização de faixas de frequências que não necessitam de autorização para uso, pois são consideradas frequências não licenciadas pela Anatel, conhecidas também como ISM.

Para garantir qualidade tanto na transmissão quanto na recepção, e uma melhor cobertura do sinal, foi utilizada uma antena omnidirecional com ganho de 12dBi. Essa antena possuí como característica uma maior concetração do sinal na projeção vertical, e um alcance maior na projeção azimutal, podendo desta forma facilitar a comunicação entre os EMT's, pois em função da topologia, os mesmos poderão estar alocados no mesmo plano horizontal.

Figura 2 – Diagrama de radiação de antena omnidirecional com ganho de 12 dBi



Fonte: http://www.aquario.com.br/

Vale ressaltar que, de acordo com a resolução da Anatel número 506, de 1º de julho de 2008, seção IX, artigo 39, § 2º, a radiação máxima para esta faixa de frequência, mesmo sendo não licenciada, é de 400 mW e.i.r.p em localidades com população acima de 500.000 habitantes. Caso seja necessário uma potência de transmissão acima desta, as estações irão necessitar de uma licença específica concedida pela própria agência.[7]

Para atuar como sistema operacional foi utilizado o OpenWRT[8], que possui diversas vantagens. Por se tratar de um sistema *opensource*, baseado no *kernel* do Linux, não é necessário a comercialização de licenças para sua utilização, além da possibilidade de customização e criação de softwares para uma demanda específica na rede. O sistema operacional foi instalado em cartões do tipo CF (*Compact Flash*) com 4 GB de armazenamento.

Obviamente, cada localidade necessitará de estudos individuais, pois regiões urbanas, suburbanas e rurais de uma mesma cidade, possuem características diferentes, principalmente na questão da propagação de ondas eletromagnéticas. Com isso, poderá ocorrer a substituição por outros equipamentos com menor ou maior alcance.

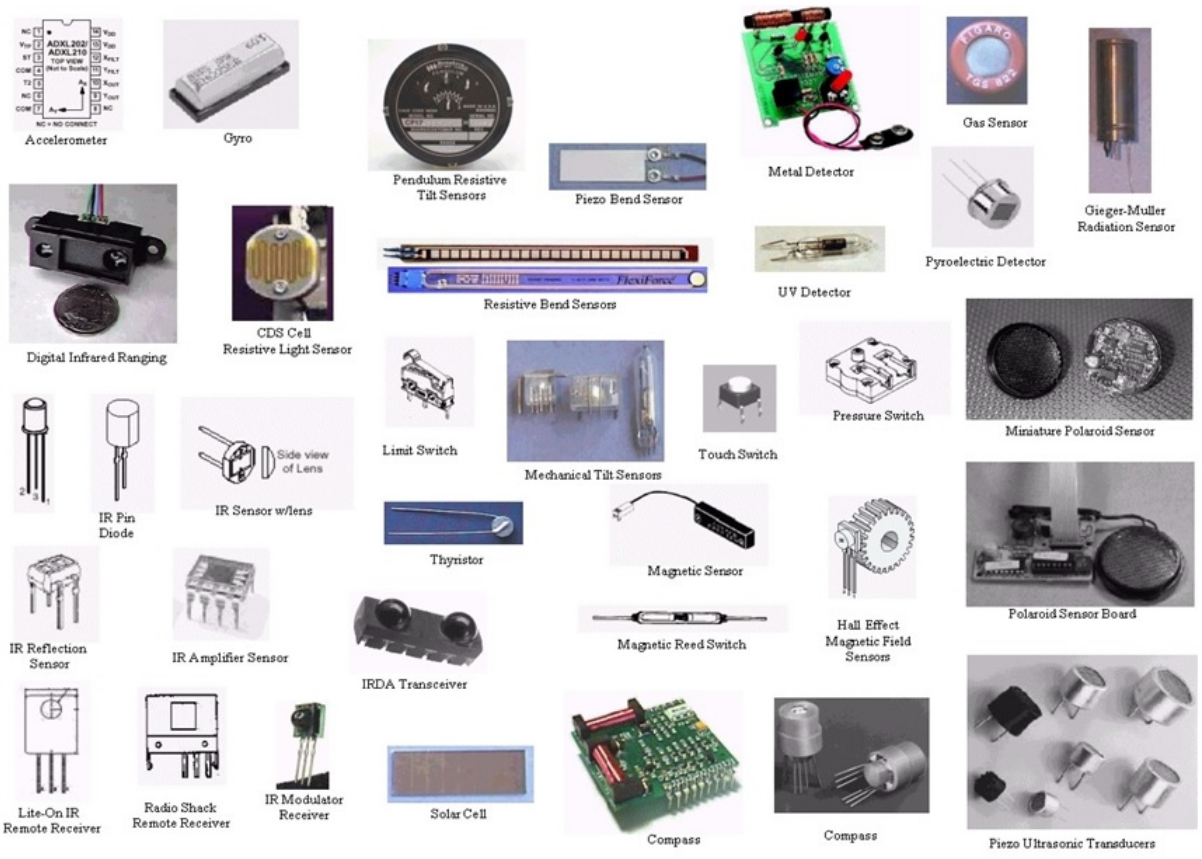
Porém, o conceito básico será sempre aplicado a todos os cenários, onde um roteamento eficiente e uma descentralização de funções, será primordial para criar uma rede robusta, tolerante a falhas e com maior alcance possível.

2 Redes de sensores sem fio

Sensores são utilizados para realizar a comunicação do mundo físico com o mundo digital, capturando os dados em formato analógico para serem posteriormente convertidos em bits. Atualmente, eles podem ser úteis em diversas áreas, tais como engenharias em geral, saúde, prevenção de catástrofes, dentre outras.

Cada sensor, em uma perspectiva simplista, é desenvolvido para obter um determinado dado, como temperatura, pressão ou corrente elétrica. Os sensores, por si só, não possuem a capacidade de armazenar, processar e transmitir informações, sendo necessário, portanto, que os mesmos estejam integrados a plataformas capazes de realizar tais procedimentos. Uma vez acoplados, pode-se definir este conjunto como nó sensor.

Figura 3 – Exemplo de sensores

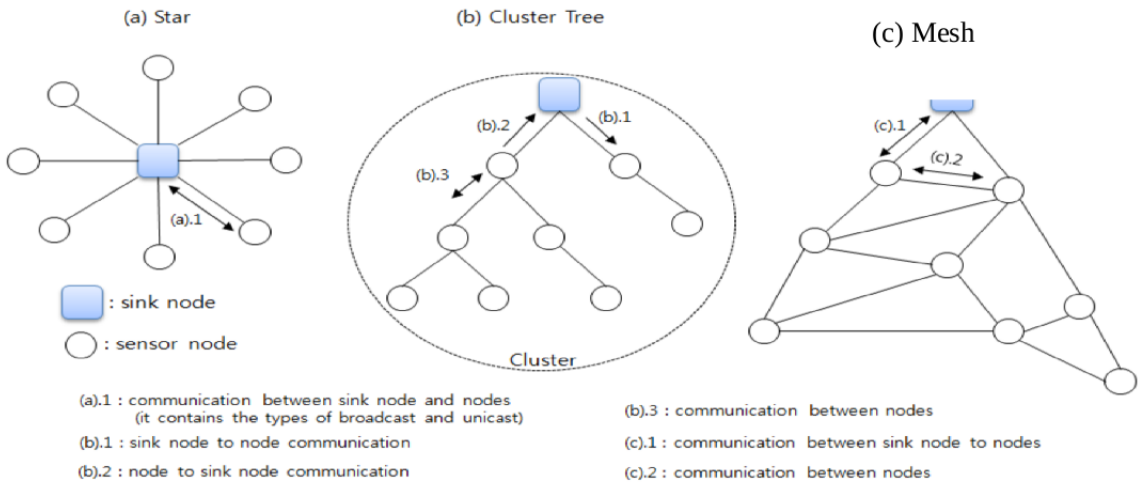


Fonte: Disponivel em http://cs.txstate.edu/ xc10/images/hetero-sensors.jpg

A partir dos nós sensores, é possível estabelecer uma rede que interconecta estes dispositivos, permitindo, assim, uma coleta distribúida e agregação dos dados. As RSSF são usualmente estruturadas utilizando uma das seguintes topologia: estrela, *cluster tree* ou *mesh*.

Na topologia estrela, a comunicação dos nós sensores ocorre po meio de um nó central. A topologia *cluster tree* pode ser comparada com a estrela, mas conectado a cada nó sensor podem estar conectados outros dois e assim sussesivamente. Na topologia *mesh*, existe a comunicação de pelo menos dois nós com duas ou mais rotas nas ligações entre os nós. [9]

Figura 4 – Três tipos de topologia para RSSF



Fonte: [ITU-T X.1311] Security requirements for wireless sensor network routing

As redes de sensores sem fio, denominadas RSSF, são implementadas visando a atender uma função específica, o que pode ocasionar peculiaridades em cada nó sensor, por exemplo. No entanto, existem outros parâmetros que devem ser implementados em qualquer RSSF, independente dos dados a serem coletados.

Pode-se citar como características a serem abordadas em projetos de RSSF: escalabilidade, autonomia e eficiência energética. A escalabilidade está associada ao fato da rede poder possuir diversos nós, aumentando, assim, sua área de cobertura. A autonomia visa a permitir que a RSSF se adapte a mudanças sem a necessidade de intervenção humana.[10] E a eficiência energética permite aos nós da rede uma maior flexibilidade, podendo, desta forma, construir redes onde a energia elétrica é limitada.

2.1 Aplicações

Com o avanço da tecnologia e com a redução nos custos de aparelhos eletrônicos, os sensores estão se popularizando, inclusive entre as pessoas mais leigas no meio tecnológico, uma vez que até mesmo um *smartphone* possui caracterísitcas de sensor e possibilita a criação ou conexão com uma rede de sensores.

Pode-se categorizar as áreas de atuação dessas redes em algumas grandes áreas, dentre as quais podem ser citadas: militar, médica, ambiental, comercial e residencial. Cada área

apresenta suas particularidades, com sensores específicos, ou até mesmo integração entre eles.[11]

Uma das grandes vantagens das redes de sensores é a possibilidade de implementação em ambientes com risco de vida como, por exemplo, locais com alto índice de radiação, materiais tóxicos, altas temperaturas etc.

No caso de ambientes dómesticos, podem ser utilizados para monitorar a qualidade da água, o consumo médio de energia com lâmpadas, eletrodomésticos dentre outras. A partir dos dados coletados, é possível traçar estratégias com o intuito de otimizar algum processo, por exemplo, a troca de lâmpadas por outras com menor potência, a fim de reduzir o gasto com energia.

No segmento militar, uma rede de sensores pode ser utilizada para coletar dados sobre a saúde do combatente, o estado das armas e blindados. Os dados serão transmitidos ao centro de operações para que sejam definidas estratégias.

2.2 Redes Mesh

As redes *wireless* do tipo *mesh* são constituídas por nós e podem ser divididas em basicamente dois grupos, denominados de *mesh routers* e *mesh clients*. Cada *mesh router* possui como função principal realizar o roteamento entre os outros nós da rede, sejam eles outros *mesh routers* ou *clients*. Os nós do tipo *client* podem ser sensores, *notebooks*, *smartphones* ou qualquer outro dispositivo que consiga, de alguma forma, se comunicar com os *routers*.[11]

Em termos de topologia para este tipo de rede, os *mesh routers* podem ser divididos em mais três grupos, denominados como:

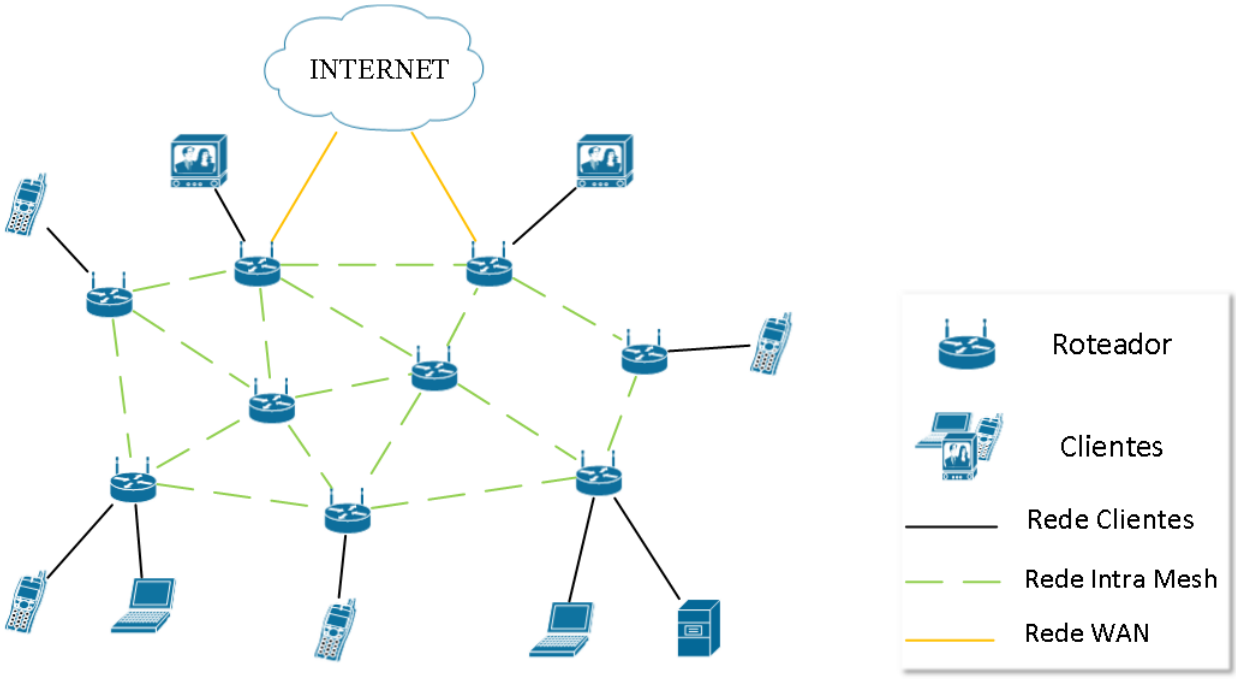
- Acesso
- *Backbone*
- *Gateway*.

Os roteadores do tipo acesso, estão focados em prover a conectividade para os clientes, como *notebooks*, *smartphones*, sensores, etc. Os roteadores do *backbone*, são os responsáveis pela interconexão entre os roteadores de acesso e os *gateways*. Vale ressaltar que os roteadores de acesso também podem se conectar diretamente aos *gateways*, levando em consideração o *design* da rede. Por fim, os roteadores do tipo *gateway* tem como função principal realizar a conectividade entre o *backbone* e a internet, por exemplo.

É importante destacar que os *mesh routers* podem realizar as três funcionalidades, concomitantemente, conforme ilustrado na figura 5.

As redes *mesh* possuem grande vantagem quando comparadas com outras topologias. É possível implementar uma rede utilizando como nós os mesmos roteadores/*switches*

Figura 5 – Topologia de uma possível arquitetura para rede mesh



Fonte: XXXXXXXXXXXXXXXXXXXX

utilizados em um ambiente dómestico. Esses equipamentos possuem baixo custo, baixo consumo de energia e podem ser customizados utilizandos sistemas operacionais *opensource*, otimizando, assim, a performace do *hardware*.

Figura 6 – Exemplo de equipamento para uso doméstico, que possibilita comunicação em malha

Fonte: Autor

Outra vantagem, além do baixo custo, é o alcance que esta rede pode ter em áreas

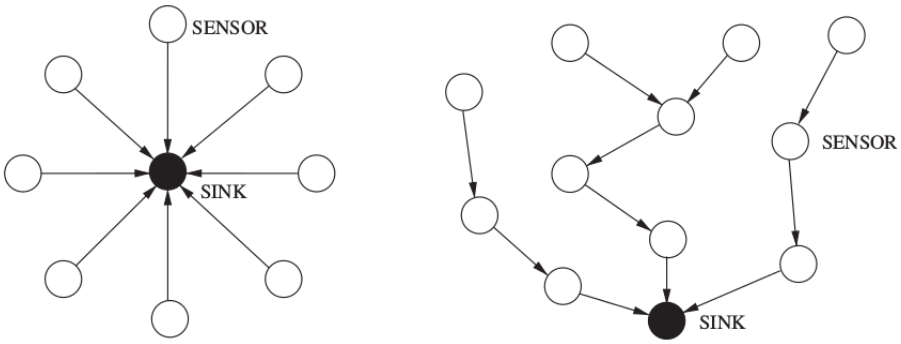
urbanas. A partir deste modelo de comunicação, é possivel estabelecer uma rede entre sensores para enviar os dados para um servidor local, por exemplo, sem que as informações precisem trafegar pela internet.

2.3 Protocolos de roteamento

Para uma transmissão eficiente da informação através de uma RSSF, a camada de rede precisa estar bem estruturada. Esta camada está relacionada com a operação do tráfego de pacotes entre a origem e o destino da informação.Desta forma, para se ter um desempenho satisfatório, é necessário que esta camada conheça toda a topologia da rede, a fim de escolher a melhor rota para a comunicação entre os dispositivos a ela conectados.

Em uma arquitetura *multi-hop*, um dos principais desafios para os nós de uma RSSF é identificar a melhor rota para se comunicar com outros nós da rede, tendo em vista que todos esses nós poderão atuar também como *relays*. As RSSF possuem peculiaridades que tornam a arquitetura *multi-hop* mais complexa, visto que os nós possuem limitações, tais como processamento, armazenamento, banda, além de estarem submetidas a constantes mudanças, o que faz com que a rede seja modificada de forma dinamica.

Figura 7 – Modelo *single-hop* (esquerda) e modelo *multi-hop* (direita)

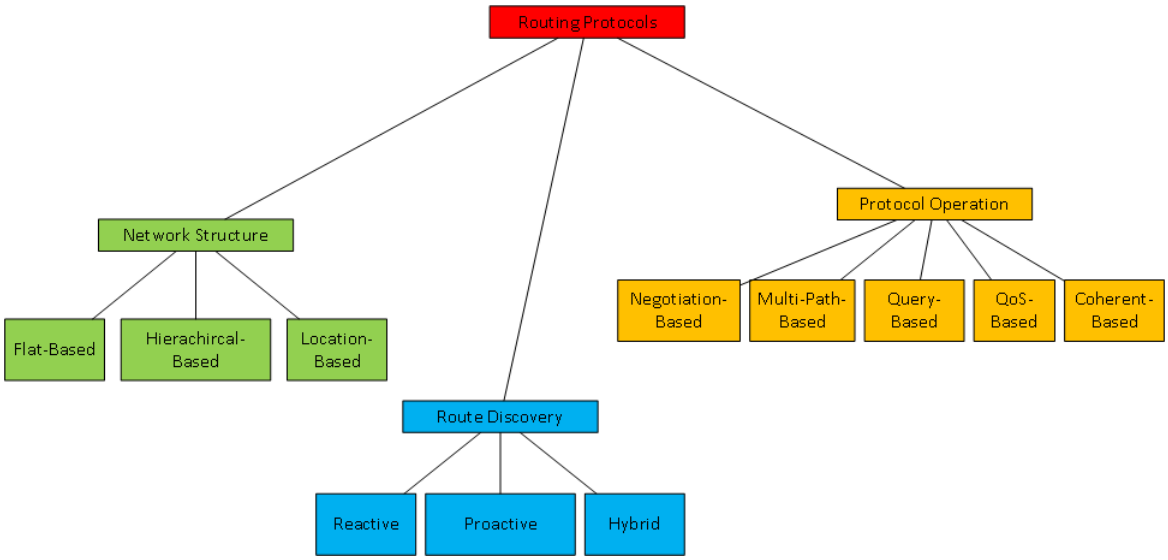


Fonte: Fundamentals of wireless sensor networks: theory and practice

Diante disso, é necessário estabelecer soluções de roteamento que sejam adaptáveis e flexivéis para as RSSF, uma vez que determinados protocolos para este tipo de rede podem não ser capazes de se comunicarem através de um endereçamento global como, por exemplo, endereçamento IP.

É possível classificar os protocolos de roteamento em três grandes áreas, baseadas na estrutura da rede (*network structure*), descoberta de rotas (*route discovery*), e operação do protocolo (*protocol operations*). A figura abaixo apresenta um diagrama para classificação dos tipos de protocolo de roteamento.

Figura 8 – Organograma contedo tipos de protocolos de roteamento



2.3.1 Protocolo OLSR

Ao longo do trabalho, o protocolo *Optimized Link State Routing Protocol* (OLSR) receberá maior destaque. Tal protocolo é utilizado para o roteamento dos pacotes em redes Ad Hoc e o mesmo é caracterizado como sendo *Proactive*, em referência à estrutura anteriormente apresentada.

Protocolos desta natureza têm como objetivo estabelecer rotas, antes mesmo de serem estas necessárias, o que é uma vantagem em comparação a outros protocolos, pois é possível diminuir o tempo ao procurar rotas a serem utilizadas, no instante em que a informação necessita ser transmitida. Por outro lado, como desvantagem, há um maior *overhead* envolvendo a descoberta e a manutenção de uma grande tabela de roteamento, onde alguma informação desatualizada pode acarretar em erros na transmissão. Um possível aumento no consumo da CPU poderá também ocasionar problemas nos nós sensores.

O protocolo OLSR é baseado em um algorítimo denominado *link-state*,[12] que consiste no envio periódico, via *broadcast*, de atualizações da topologia da rede por parte dos nós. Desta forma, cada nó utiliza as informações de seus vizinhos para identificar a rede e criar consequentemente a tabela de roteamento, mantendo assim uma comunicação com todos os outros nós.

Nas redes de sensores sem fio, o tráfego de pacotes deve ser otimizado por diversos aspectos. Um deles é a necessidade de um baixo consumo de energia por parte dos nós, pois, em alguns casos, a mesma pode ser escassa. Outro fator está associado à banda que, em redes *wireless*, pode ser muito inferior em comparação a redes cabeadas.

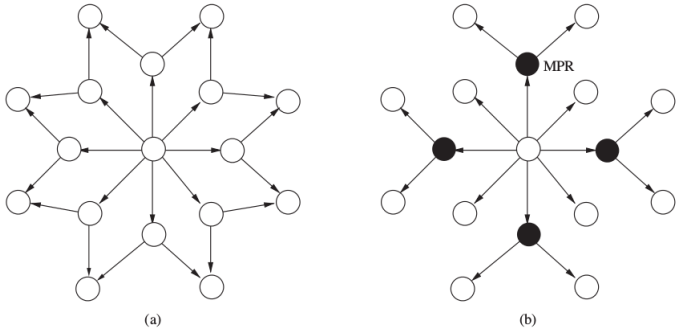
Para otimizar este tráfego, existe um mecanismo com o objetivo de evitar inundações que possam afetar o desempenho da rede, por propagarem as informações em todos os nós. Esta técnica é conhecida como MPR *(multipoint relay)*.

Deste modo, cada nó, a partir das atualizações recebidas, pode selecionar qual outro nó

será utilizado como seu MPR, a fim de otimizar a utilização dos recursos da rede. Assim, somente os MPR são capazes de retransmitir essas informações.

A Figura abaixo exibe uma comparação entre a utilização ou não da técnica de MPR

Figura 9 – *Flooding* (a) e MPR (b)

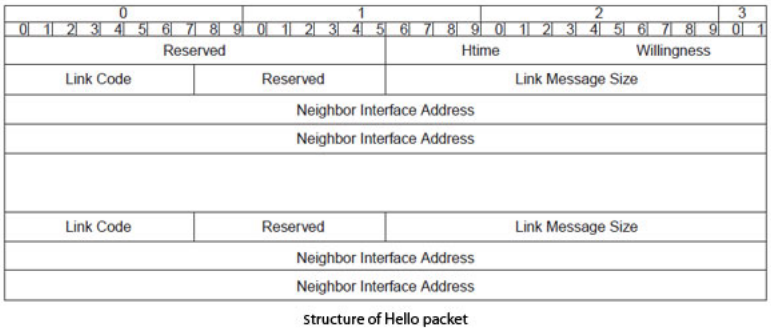


Fonte: Fundamentals of wireless sensor networks: theory and practice

O protocolo trabalha essencialmente com três tipos de mensagens para mapear e manter a rede funcional, sendo elas conhecidas como HELLO,TC e MID.

A mensagen do tipo HELLO é utilizada basicamente para conceber a topologia da rede, com a identificação dos MPR's e de toda vizinhança. A mensagem TC *(Topology Control)* possui como finalidade o envio de informaçoes que permitam a estruturação da tabela de roteamento. A mensagens MID (Multiple Interface Declaration) é gerada para declaração de múltiplas interfaces, como o nome sugere. Esta mensagem consiste a associação de outras interfaces de um mesmo nó, para cáculo de rotas. Esta mensagem só será útil, no caso de existirem outras interfaces.

Figura 10 – Estrutura do pacote *Hello*



Fonte:

2.4 Segurança

Com o avanço da tecnologia, equipamentos de todos os tipos estão cada vez mais interconectados. Atrelado a isso encontra-se a questão da segurança da informação que necessita ser constantemente aprimorada.

Em um passado recente, havia um medo muito grande com relação a dados bancários, já que o furto de credenciais poderia gerar sérios problemas. Atualmente, com a facilidade de acesso à internet através de dispositivos móveis, as pessoas se preocupam também com o sigilo de suas informações, principalmente no que tange à privacidade, como, por exemplo, com suas fotos.

A segurança da informação ganha cada vez mais notoriedade em face das diversas ameaças cibernéticas que surgem a cada dia e são divulgadas através da mídia. Ao se projetar sistemas de telecomunicações, é indispensável abordar este tópico, a fim de proteger tais sistemas das vulnerabilidades já existentes e mitigar as falhas ainda não exploradas.

Neste contexto, os principais pilares da segurança da informação, de acordo com a ISO/IEC 27002 podem ser descritos como:

- Disponibilidade
- Integridade
- Confidencialidade.

A disponibilidade faz referência ao fato da informação estar ou não acessível. Por exemplo, se um equipamento é desligado, proposital ou acidentalmente, as informações não estariam disponíveis para serem transmitidas, gerando assim algum impacto no serviço.

A integridade é a garantia da veracidade das informações, para que estas não sofram alterações por códigos maliciosos ou intervenção humana, assegurando que sejam transmitidas entre a origem e destino corretos.

A confidencialidade deve garantir que somente quem possua determinado nível de autorização possa acessar a informação. Isso consiste também na não divulgação das informações, como, por exemplo, origem, destino e conteúdo.

Todos esses pilares devem ser adotados desde a camada física até a camada de aplicação em referência ao modelo OSI. Caso um equipamento de radiocomunicação, por exemplo, fique exposto diretamente a precipitações e isso venha a danificá-lo, isso pode ser caracterizado como falta de segurança, uma vez que gerará indisponibilidade. Se um código malicioso for injetado em uma dada aplicação e atuar como um MITM (*Man in the middle*), a integridade e a confidencialidade pode ser comprometidas.

A ITU-T X.1051 estabelece orientações para implementação, manutenção e aperfeiçoamento para gerência de segurança da informação em sistemas de telecomunicações, baseado na ISO/IEC 27002.

Para RSSF, a questão de segurança deve ser abordada de forma diferenciada, visando a atender peculiaridades de cada fenômeno monitorado. Caso os sensores estejam monitorando a temperatura de uma cidade, por exemplo, e os dados sejam furtados, possivelmente este fato não irá gerar grandes transtornos, pois não possuem grande confidencialidade, tendo em vista que qualquer pessoa pode realizar esta medição. O que se deseja como prioridade é a integridade e disponibilidade dos dados.

As redes *wireless* em geral, possuem uma fragilidade a mais em comparação a redes cabeadas. A informação está mais vulnerável pelo fato de não trafegar em um meio confinado, estando, assim, sujeita a ataques do tipo *signal jamming*, por exemplo, que ocorre quando um transmissor com cárater malicioso gera sinais na mesma frequência, impedindo que os nós se comuniquem de forma eficiente. [13]

Outro fator crítico de segurança envolvendo a primeira camada do modelo OSI é o fato dos nós sensores estarem alocados em ambientes sem segurança física ou monitoramento constante. Isto possibilita o dano tanto por ações naturais, depredação ou com a finalidade de furtar os dados.

São conhecidos diversos tipos de ataques voltados para redes sem fios, e os mesmos podem ser classificados em ativos e passivos. Os ataques passivos, estão voltados para captura de informações sem o intuito de adulterá-las. Esse fato é conhecido também como espionagem. Em síntese, os ataques ativos, são caracterizados por modificar a integridade dos dados transmitidos, e podem atuar nas diversas camadas do modelo OSI.[14]

Existem algumas formas para minimizar o ataque, que podem ser descritas como utilização de redundância, verificação de bidirecionalidade do enlance, autorização e invetigação.[14] A utilização de criptografia também é fundamental, uma vez que ela possuí um alto grau de confiabilidade. Dependendo do tipo de criptografia utilizada, a sua quebra poderá necessitar um alto poder computacional, o que diminui a quantidade de atacantes aptos para tal empreitada.

Para o caso do OLSR, existe um mecanismo de proteção, que é adotado como extensão, chamado de SOLSR (*Secure Optimized Link State Routing Protocol*), que consiste na utilização de chaves siméticas para assinar cada mensagem de controle, gerando assim uma autenticação das mensagens.

Esta extensão, em síntense, garante que ao colocar um novo nó na rede, sem conhecimento da chave pré-compartilhada, o mesmo não não poderá encaminhar mensagens e consequentemente obter as tabelas de roteamento. Por outro lado, caso um nó autentico seja violado, é possível dizer que a chave foi comprometida, pois a mesma fica armazenada localmente. Sendo assim, este é um método parcialmente seguro, pois garante uma segurança salto-a-salto e não fim-a-fim.

3 Medições e implementação da rede

3.1 Planejamento das medições

A fim de emular um ambiente com equipamentos de medição e transmissão através de uma *Wireless Mesh Sensor Network*, denominada WMSN, foi implementada uma pequena infraestrutura com quatro nós dispostos no terraço do prédio da engenharia no campus da Praia Vermelha da UFF.

Cada nó foi alocado em pontos equidistantes do nó vizinho, de maneira que pudessem ter visada direta para pelo menos outro nó. Este procedimento foi adotado por se tratar de apenas quatro dispositivos em uma distância de aproximadamente 100 metros e não possuir muitos obstáculos.

A figura 12 mostra o posicionamento de cada nó.

Figura 11 – Disposição geográfica dos nós

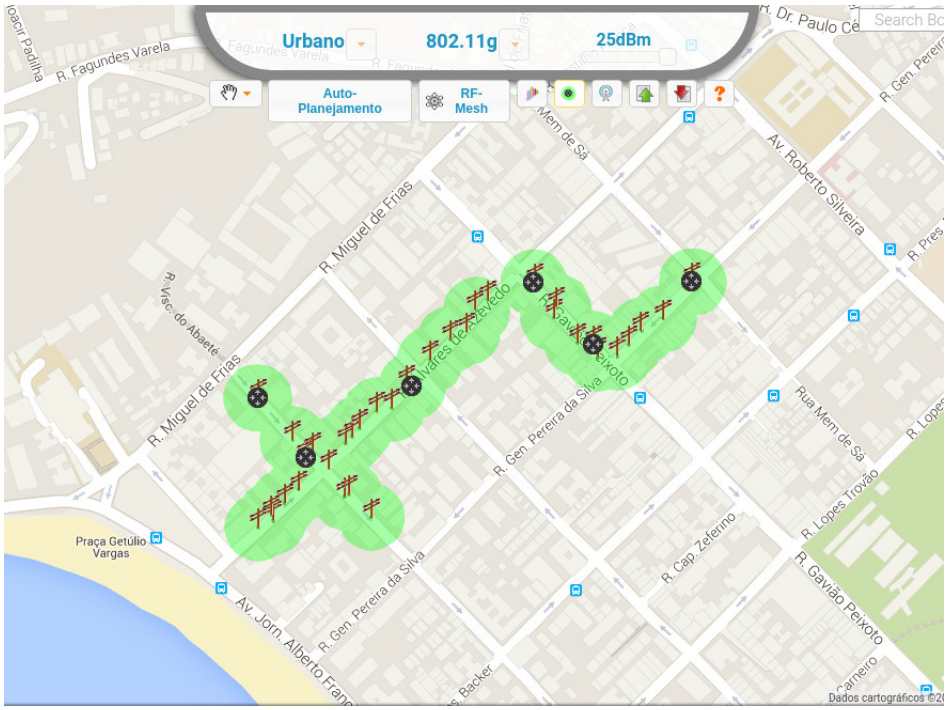
Fonte: Google Maps

Para uma situação real, o posicionamento destes equipamentos pode ser realizado com auxílio da ferramenta *Smart Planner*. Este sistema possui como objetivo o planejamento de uma rede de comunicação de curta distância para *smart grids*[15], visando a atender uma AMI (*Advanced Metering Infrastructure*). Esta AMI é composta por medidores inteligentes (*smart meters*) e agregadores, denominados DAP (*Data Aggregation Point*).

Como exemplo da utilização do *Smart Planner* no auxílio da implementação da rede, as figuras abaixo ilustram dois cenários. O primeiro é referente à localização aproximada

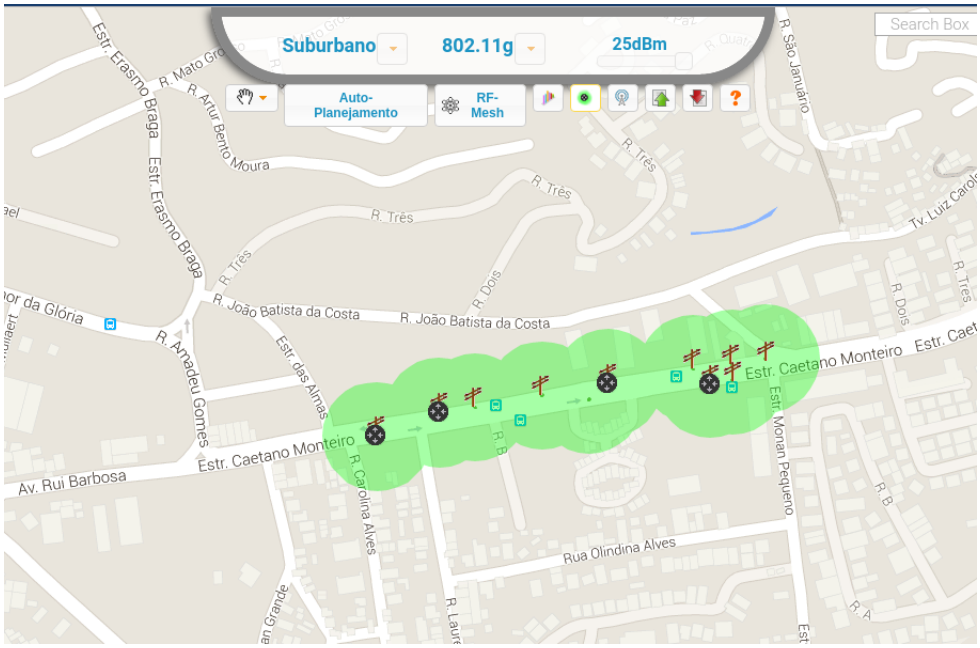
de transformadores nas ruas do bairro de Icaraí (cenário urbano) e o segundo refere-se à região de Pendotiba (cenário suburbano), ambas na cidade de Niterói.

Figura 12 – Mapeamento de transformadoes e DAP's no bairro de Icaraí



Fonte: http://www.midiacom.uff.br/smartplanner

Figura 13 – Mapeamento de transformadoes e DAP's na região de Pendotiba



Fonte: http://www.midiacom.uff.br/smartplanner

3.1.1 Materiais utilizados

Para concepção de cada nó, foram utililzados os seguintes equipamentos e acessórios:

- Abraçadeiras de nylon
- Antena omnidirecional de 12 dBi (conector N fêmea)
- Cabo coaxial RG-58 com 1 metro de comprimento (conectores N macho)
- Cabo UTP
- Caixa hermértica de PVC
- Cartão *wireless* mini-PCI
- Conector 5,5 mm (Macho e Fêmea)
- Conector N fêmea x U.FL Fêmea
- Compact Flash
- Fitas de autofusão e isolante
- Fitilho de polietileno
- Fontes de 12V
- Prensa cabos
- Tubo de PVC de 3/4"e 1 metro de comprimento
- *System board*

3.1.2 Instalação e configuração

O SO (sistema operacional) utilizado foi o OpenWRT, com a versão CHAOS CALMER (15.05.1). Para gravar o SO no *compact flash*, foi utilizado o seguinte comando, a partir de um computador linux:

dd if=openwrt-15.05.1-x86-geode-combined-ext4 of=/dev/sdb

A partir deste ponto, com o SO já instalado, foi realizada a instalação e a configuração de outros pacotes. Vale ressaltar que a imagem utilizada foi adquirida diretamente do site, de acordo com a arquitetura da *system board*. Poderia ser feita uma compilação manual, instalando somente pacotes que de fato seriam utilizados, otimizando, assim, o uso de CPU, memória RAM e armazenamento.

Com as placas conectadas à internet, foram utilizados os seguintes comandos para instalação dos pacotes:

opkg update
opkg install pciutils luci-app-olsr luci-app-olsr-services luci-app-olsr-viz olsrd olsrd-mod-arprefresh olsrd-mod-bmf olsrd-mod-dot-draw olsrd-mod-dyn-gw olsrd-mod-dyn-gw-plain olsrd-mod-httpinfo olsrd-mod-mdns olsrd-mod-nameservice olsrd-mod-p2pd olsrd-mod-pgraph olsrd-mod-secure olsrd-mod-txtinfo olsrd-mod-watchdog olsrd-mod-quagga wireless-tools luci-lib-json

Após esta etapa, foram realizadas as mesmas configurações em todas as placas. As únicas diferenças foram o endereço IP da interface *wireless* SensorMesh e o *hostname* de cada nó.

As configurações foram separadas em quatro grupos, conforme descrito abaixo e estão em anexo ao final deste trabalho.

- Firewall (Anexo A)
- Interfaces (Anexo B)
- OLSRD (Anexo C)
- Wireless (Anexo D)

3.1.3 Montagem

As *system boards* foram fixadas em caixas herméticas para proteção contra possíveis intempéries. Em seguida foram conectadas à elas o *compact flash*, contendo o sistema operacional e o cartão mini-PCI *wireless*.

Utilizou-se em seguida o conector N x U.FL, onde uma extremidade foi conectada ao cartão *wireless* e a outra fixada junto à caixa hermética conforme a figura 15.

Figura 14 – Conector N X U.FL

Fonte: Autor

As caixas e antenas foram fixadas utilizando abraçadeiras de nylon em tubos de PVC. Os tubos, por sua vez, foram fixados em bases de concreto e amarrados com fitilho de polietileno para garantir uma sustentação maior, em razão dos ventos. A figura 16 ilustra a disposição final.

Figura 15 – Caixa hermética e antena fixadas em tubo de PVC

Fonte: Autor

Cabe destacar que o ideal para esta sustentação seria a utilização de cabos de aço e esticadores. No entanto, como o fitilho possui uma resistência considerável e o tempo de exposição dos equipamentos foi pequeno, optou-se por este, pelo seu fácil manuseio e implementação.

Após todas as fixações serem realizadas, utilizou-se o cabo coaxial para ligação entre a placa e a antena. Nas conexões externas, foram utilizadas fitas de autofusão e isolante, para proteção contra umidade, sendo este um fator prejudicial em transmissões de RF.

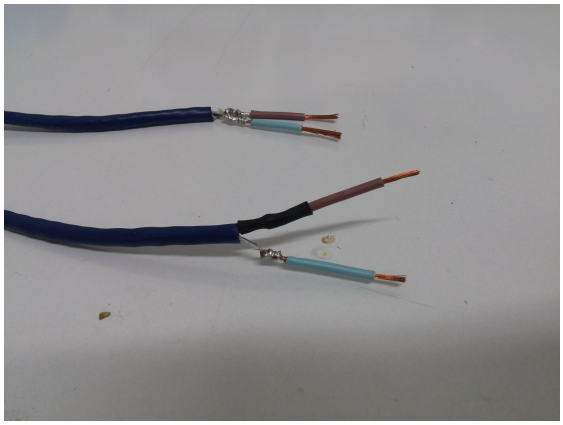
Para a obtenção de um cenário mais preciso, a medição ideal seria realizada junto a postes de energia elétrica distribuídos pelas ruas, levando em consideração ruídos,interferências geradas por outros dispositivos eletromagnéticos, múltiplos percursos causados pelas reflexões das ondas em edificações, desvanecismento, dentre outros.

3.1.4 Alimentação elétrica

As *system boards* foram energizadas através de cabos UTP e, para esta emulação, os cabos foram utilizados somente com a finalidade de alimentação elétrica. No entanto, é possível trasmitir dados e eletricidade pelo mesmo condutor (dois pares transmitem dados e dois energia), sendo esta associação conhecida como 802.3af ou PoE (Power over ethernet).

As figuras abaixos ilustram a confecção dos cabos para esta emulação. Este procedimento foi necessário, para que os EMT's pudessem ficar dispostos em determinados pontos, pois no terraço do prédio havia escassez de recursos elétricos.

Figura 16 – Preparação dos cabos



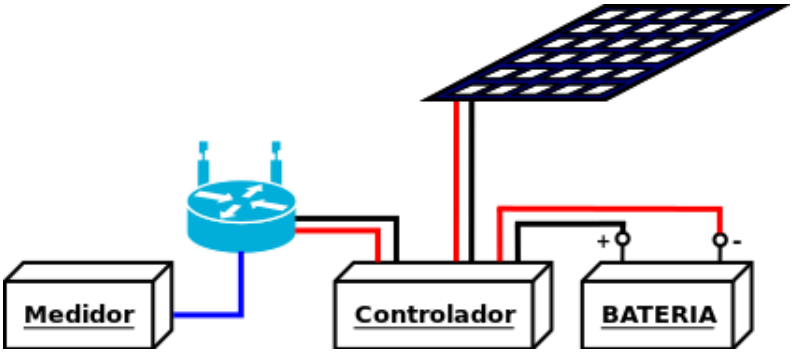
Fonte: Autor

Figura 17 – Cabo e conector

Fonte: Autor

Para o caso real, as *sytem boards* poderiam ser alimentadas diretamente pelo transformador de potência, sem a necessidade da confecção destes cabos, que serviram apenas como extensões. É possível ainda, a utilização de energia solar, para esta finalidade, onde seriam utilizadas células fotovoltáicas, contrololador de carga e uma bateria, conforme ilustra figura abaixo.

Figura 18 – Esquema para utilização de bateria e fotocélula



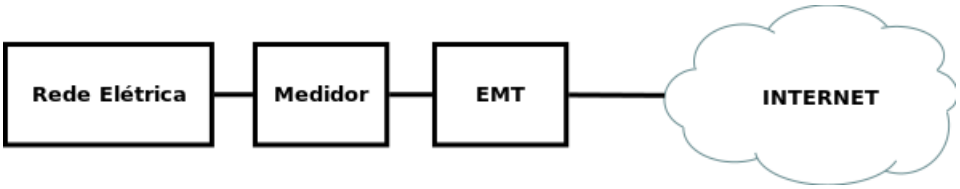
Fonte: Autor

3.2 Aquisição dos dados

Inicialmente, este trabalho foi planejado para criar condições reais de coleta de dados, utilizando medidores eletrônicos polifásicos. Contudo, houve dificuldades em estabelecer comunicação na porta ethernet do medidor.

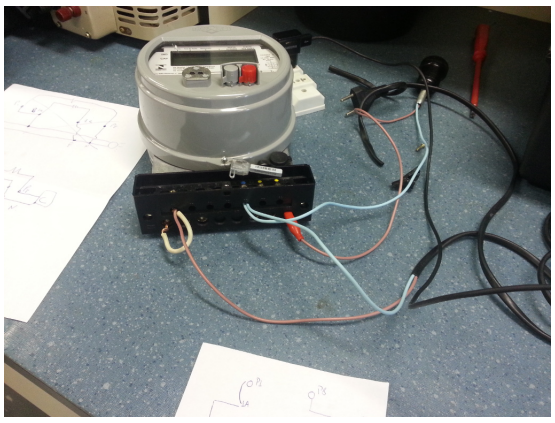
O diagrama em blocos abaixo ilustra como seria realizada esta medição e transmissão.

Figura 19 – Diagrama em blocos da amostragem



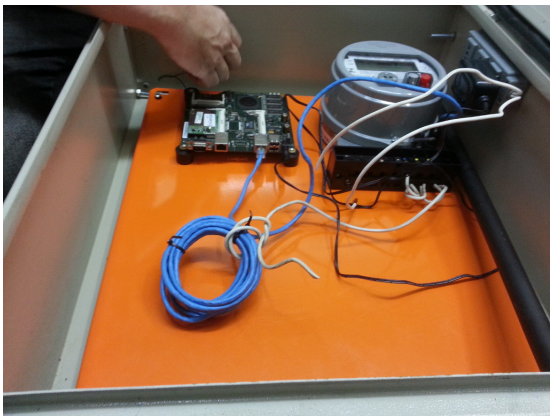
Fonte: Autor

Figura 20 – Preparação do medidor



Fonte: Autor

Figura 21 – Equipamento de medição e transmissão



Fonte: Autor

Desta forma, esse processo foi substituido por valores de consumo de energia elétrica obtidos pelo projeto Uk-dale. Este projeto[16] é descrito como um *open-access*, e teve como

objetivo estudar o comportamento de consumo de energia elétrica a partir de cinco casas do Reino Unido, através de dispositivos conectados à rede elétrica como eletrodomésticos, computadores, lâmpadas e vários outros.

Foram utilizados sensores de corrente passivos denominados CT, para obtenção dos dados e, conectado a eles, utilizou-se como transmissor um Nanode[17], que é um micro-controlador *opensource* que possibilita a conexão com a internet. Na prática, o Nanode se assemelha ao Arduino, porém com outras particularidades.

A amostragem foi realizada a cada seis segundos, em cada um dos dispositivos, e os valores coletados foram armazenados em arquivos. Após, um outro arquivo foi gerado, com o consumo agregado de todos os dispositivos em cada casa. O consumo é obtido a partir dos valores de corrente e tensão, caracterizado pela potência.

Em substituição ao uso do medidor eletrônico, foram utilizadas as medidas referentes aos valores agregados, representando, assim, a potência total entregue pelo transformador. Foram separados em quatro arquivos e cada um ficou armazenado em um nó da rede.

Foi criado, então, um código, escrito em *shell script*, responsável por ler tais arquivos e em seguida transmiti-los para o site ThingSpeak. O ThingSpeak, é uma ODP que recebe dados de diversos entusiastas dessa nova era de internet das coisas, ou IoT. Abaixo segue o código criado.

```
#!/bin/bash

#Recupera as informacoes do ultimo dado transmitido no formato json
until $(curl -k https://api.thingspeak.com/channels/127852/fields/1/last.
    json?api_key=YYY > json);do
  sleep 5
done

#Realiza um parse para a quantidade de registros enviados
ultimo=`grep -Eo ':\w+,' json | tr -d \":,`
tail -n +$ultimo medidas.txt > recuperado.txt

#Verifica a conectividade e envia os dados
while read line
do
  until $(curl -k --output /dev/null --silent --head --fail https://api.
     thingspeak.com); do
    sleep 1
  done
  curl -k "https://api.thingspeak.com/update?api_key=XXX&field1=$line"
  echo -e "$line"
  sleep 30
done < recuperado.txt
```

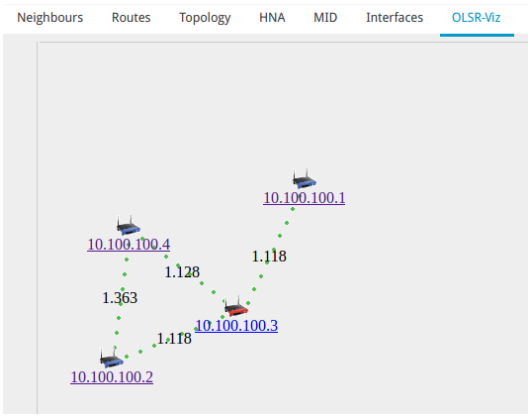
Foi realizada uma configuração para garantir que o código fosse reinicializado em caso de queda de energia, pois estes sistemas, uma vez ligados, devem garantir uma alta disponibilidade. Esta configuração foi realizada no arquivo /etc/rc.local. Desta forma, todos os *scripts* esseciais ao funcionamento do sistema devem estar programados para este tipo de evento.

Outro fator importante é garantir, em determinados horários, uma verificação do funcionamento do *script*. Isto tem como objetivo a disponibilidade, pois um dado código, em algum momento, pode ser encerrado de forma inesperada. Esta verificação pode ser feita através de uma cron, onde é possível, por exemplo, todo dia a meia noite executar tal verificação.

3.3 Transmissão

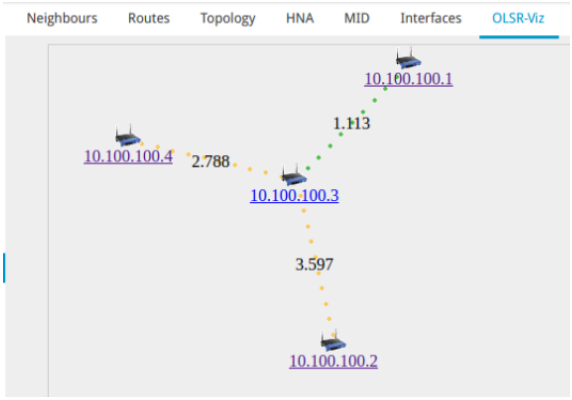
Após realizadas todas as configurações, os nós se conectaram e formaram a rede. As imagens abaixo ilustram desenhos das topologias estabelecidas, que foram criados a partir de dados obtidos pelo protocolo OLSR. Essas imagens mostram, ainda, como o protocolo atua em decorrência das mudanças realizadas na rede.

Figura 22 – Topologia rede



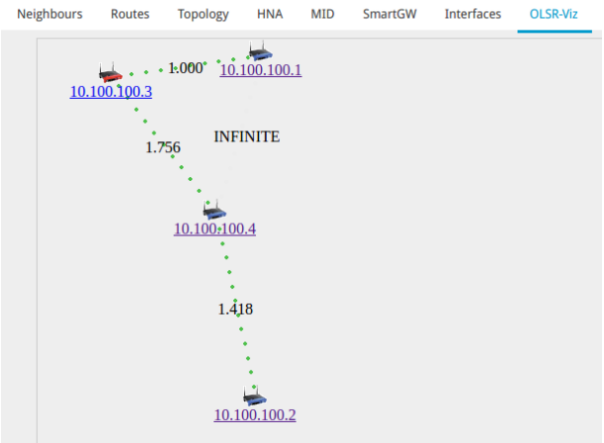
Fonte: Autor

Figura 23 – Topologia rede



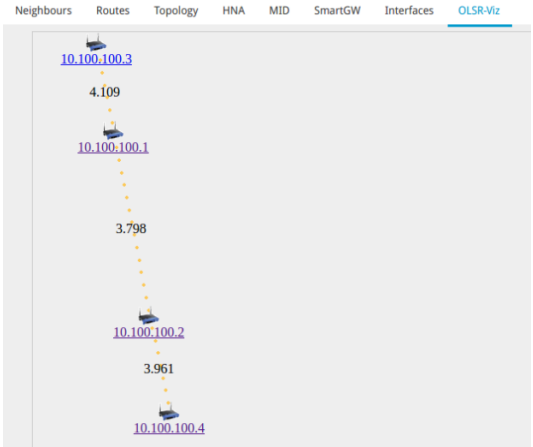
Fonte: Autor

Figura 24 – Topologia rede



Fonte: Autor

Figura 25 – Topologia rede



Fonte: Autor

A seguir, são apresentadas as tabelas de roteamento e de nós conhecidos, vistos a partir do nó com endereço IP 10.100.100.1. A topologia referente a estas tabelas é mostrada na figura 24.

Figura 26 – Tabela de roteamento para o nó 1

Overview of currently known routes to other OLSR nodes

Announced network	OLSR gateway	Interface	Metric	ETX
10.100.100.3/32	10.100.100.3	wlan0	1	1.000
10.100.100.4/32	10.100.100.3	wlan0	2	2.756
10.100.100.2/32	10.100.100.3	wlan0	3	4.174

Fonte: Autor

Figura 27 – Tabela de nós conhecidos

Overview of currently known OLSR nodes

OLSR node	Last hop	LQ	NLQ	ETX
10.100.100.3	10.100.100.1	1.000	1.000	1.000
10.100.100.1	10.100.100.3	1.000	1.000	1.000
10.100.100.2	10.100.100.4	0.894	0.788	1.418
10.100.100.4	10.100.100.3	0.839	0.831	1.433
10.100.100.4	10.100.100.2	0.788	0.839	1.511
10.100.100.3	10.100.100.4	0.732	0.776	1.756

Fonte: Autor

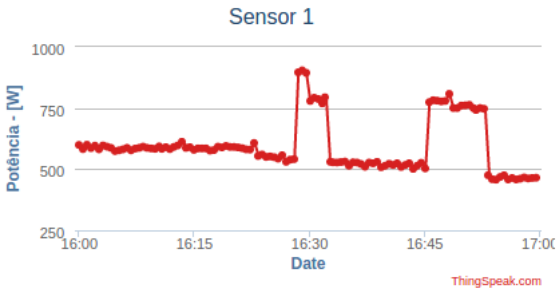
Nestas tabelas, é possivel verificar três parâmetros importantes para manutenção da rede, que são LQ, NLQ e ETX[18].

O LQ (*Link Quality*) representa a probalidade de ocorrer uma transmissão bem sucedida dos pacotes de um determinado nó para outro. O NLQ (*Neighbor Link Quality*) informa a qualidade do *link* entre um dado nó e seus vizinhos. O ETX (Expected Transmission Count) é obtido através da relação 1 / (NLQ x LQ) para cada *link*. Esses parâmetros estão em constante mudança na rede.

Após a rede ter sido organizada, utilizou-se um nó como *gateway* para acesso à internet através da tecnologia 4G. A partir deste ponto, os dados de cada nó foram enviados ao site ThingSpeak. Neste caso as informações foram transmitidas para a internet. Entretanto, de acordo com a topologia implementada, é possível enviar as informações para um servidor na rede local, sem a necessidade de trafegar pela internet, reduzindo, assim, possíveis custos.

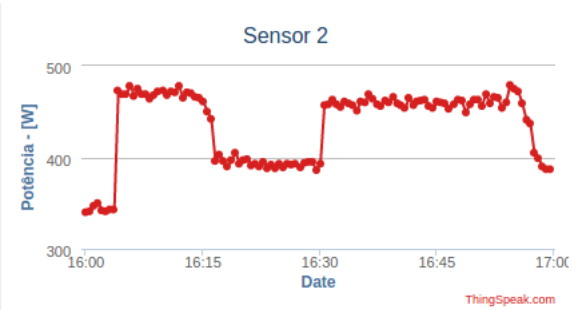
Abaixo estão os gráficos referentes a cada nó, enviados em campo em um dia com ensolarado.

Figura 28 – Dados enviados pelo nó 1



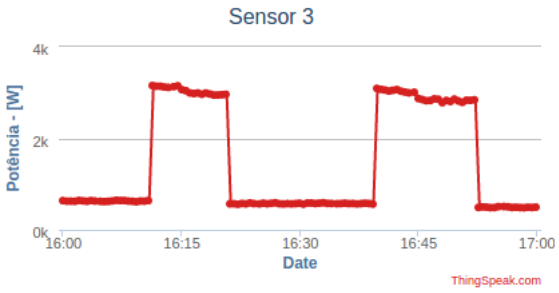
Fonte: Autor

Figura 29 – Dados enviados pelo nó 2



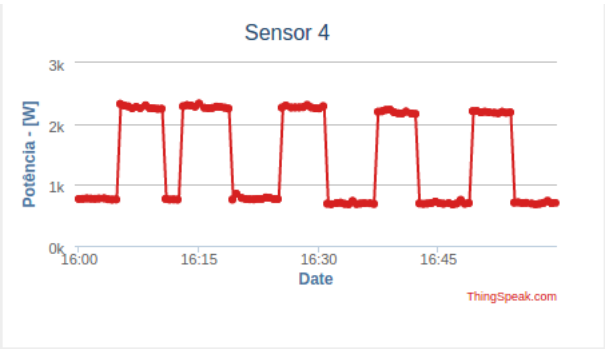
Fonte: Autor

Figura 30 – Dados enviados pelo nó 3



Fonte: Autor

Figura 31 – Dados enviados pelo nó 4



Fonte: Autor

Caso fosse uma situação real de coleta de dados, a potência total entregue pelo transformador, representada nas figuras acima, deveria estar próxima (considerando uma margem de erros) da soma das potências individuais das unidades em dada localidade.

3.4 Resultados obtidos

Os dados enviados em campo foram comparados com dados enviados em laboratório. Pode-se, ainda, verificar a existência de dois fatores que influenciaram na transmissão.

Quando realizado em laboratório, 100% dos valores foram transmitidos com sucesso, onde cada transmissão ocorreu a cada 15 segundos. Ao diminuir este valor, ocorreram erros em maior frequência. A conexão com a internet, neste caso, foi cabeada.

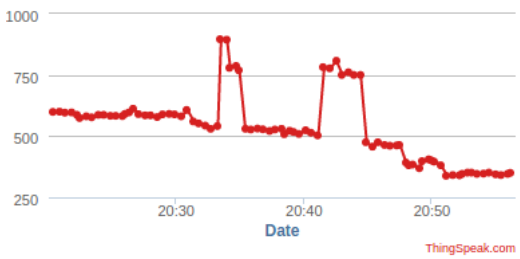
No trabalho de campo, os dados foram transmitidos utilizando a tecnologia 3G/4G e inicialmente também com intervalo de envio a cada 15 segundos.

No entanto, durante o período que os equipamentos ficaram expostos, as transmissões ocorreram em dias chuvosos e ensolarados. Independente de fatores climáticos, sempre ocorreram erros, em menor ou maior escala.

Pôde-se verificar que quanto maior o número de saltos e menor o intevalo de tempo, os erros ocorreram em maior frequência tanto no dia chuvoso e ensolarado. No dia chuvos entretato, a qualidade do sinal ficou mais instável devido aos efeitos que a chuva causa em comunicações *wireless*.

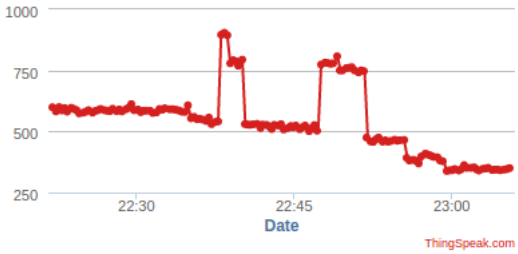
Porém, mesmo com os erros na transmissão que não superaram 20%, foi possível ainda uma boa aproximação em comparação com uma transmissão livre de erros. Uma prova disto, foi a realização da transmissão em laboratório de 150 valores. Com intervalo de transmissão de 10 segundos, foram transmitidos com sucesso 85 dos 150 valores, aproximadamente 56% do total. No intervalo de 15 segundos todos os valores transmitidos com sucesso. Abaixo seguem os gráficos comparativos.

Figura 32 – Intervalo de envio de 10 segundos



Fonte: Autor

Figura 33 – Intervalo de envio de 15 segundos



Fonte: Autor

Com isso, é possível realizar uma amostragem com intervalo maior garantindo assim uma maior confiabilidade na transmissão, não alterando desta forma o valor esperado.

Possivelmente o código responsável pela mineração e envio dos dados, poderá sofrer modificações com intuito de garantir um tempo menor na execução dos comandos, podendo inclusive diminuir o aparecimento de erros.

4 Conclusões

Como dito no início deste trabalho, a demanda pela energia elétrica, seja para uso comercial, industrial ou residencial é um fator importante na economia de um país. Com isto, o monitoramento deste serviço é fundamental para garantir uma qualidade e possível redução de custos.

O modelo de distribuição de energia elétrica não é totalmente padronizado, onde cada região possui suas peculiaridades. Para isto, foi abordada a instalação de medidores e equipamentos de transmissão, em postes com rede elétrica áerea. No entanto, existem situações onde a distribuição é subterrânea, trazendo assim novos desafios para o monitoramento.

Outro fator relevante, foi a observância do número de transformadores em certas regiões. Em locais suburbanos, onde predominantemente é formado por casas, como exemplo, o bairro de São Francisco em Niterói, o número de transformadores é inferior em comparação com uma área urbana, o que torna a distância entre eles maior.

Consequentemente, o número de dispositivos do tipo *gateway* ou DAP tende também a ser maior, sendo necessário inclusive alguns equipamentos somente com a função de *relay*, não aferindo dados.

Além do objetivo principal, como mapear áreas com fraudes e monitorar a saúde da rede elétrica, tal implementação, permitirá ainda a agregação e exploração, de diversos serviços de telecomunicações, onde é possível citar: acesso às redes de comunicação públicas, transportes urbanos, segurança pública, aplicações para telemetria e telecontrole, entre outras.

O setor de energia elétrica está começando, com auxílio das telecomunicações, a adotar medidas para tornar a distribuição de energia mais eficiente. Em um futuro próximo, será possível ter cidades totalmente interconectadas com esses serviços, o que possibilitará extrair uma quantidade de informações valiosas.

4.1 Trabalhos Futuros

A implementação desta rede teve como objetivo apenas um evento, que seria o monitoramento de potência entregue por cada transformador. No entanto, ao se tratar de redes elétricas inteligentes e redes de sensores, é possível ainda desenvolver diversos trabalhos correlatos.

Uma outra abordagem, é a comunicação de *smart meteers* dos consumidores finais à estes dispositivos. A partir disto, seria possível estabelecer uma forma rápida de realizar o cálculo do consumo de cada unidade, sem necessidade de intervenção humana.

A figura 1 traz uma concepção artística para o modelo em questão, como possível implementação.

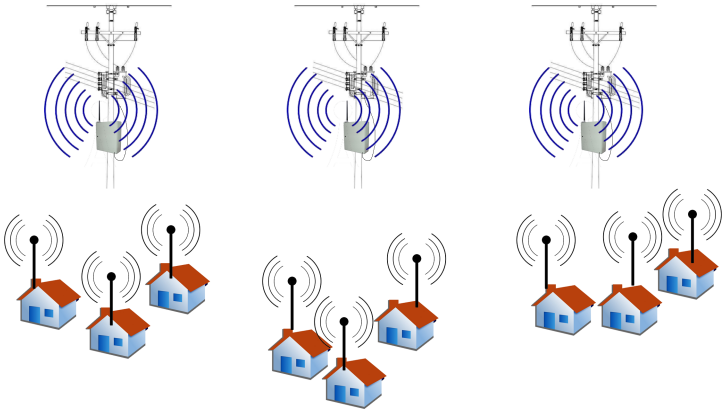


Figura 34 – Ilustração para modelo de comunicação entre *smart metering* e rede mesh

A elaboração de um sistema de gerenciamento também é algo importante, pois o número de dispositivos tende a ser elevado, o que torna a gerência local inviável. Este sistema possibilitaria então, o acesso remoto a uma dada localidade e o controle de todos os dispositivos, podendo futuramente implementar automação, onde seria possível desligar um transformador para manutenção por exemplo.

Já exitem sistemas capazes de realizar este tipo de gerência de pontos de acesso, como por exemplo o SciFi do laboratório Midiacom da UFF[19] e o OpenWISP[20] que inclusive possui outras funções, como *Captive Portal* por exemplo.

Existem também ferramentas *opensource* já conceituadas, que auxiliam na gestão da rede, como o Cacti[21] e o MRTG[22] por exemplo. Estes sistemsa se baseam no envio de informações através do protoloco SNMP (*Simple Network Management Protocol*).

Outor fator que pode garantir a qualidade do fornecimento de energia, é o monitoramento da saúde dos trasnformadores, aferindo por exemplo o nível de óleo isolante,temperatura[23], dentre outros. Isto garantiria ações preventivas, evitando assim explosões ou acidentes mais graves, uma vez que poderia se estabeler valores limítrofes para funcionamento dos mesmos, e caso fossem atingidos seria executada uma ação.

Referências

1 CâMBIO e energia pressionam inflação, diz IBGE. Disponível em: <http://www.valor.com.br/brasil/4169740/cambio-e-energia-pressionam-inflacao-diz-ibge>. 10

2 FURTO de energia faz conta ser 17Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2015/05/furto-de-energia-faz-conta-ser-17-mais-cara-no-rio-aponta-pesquisa.html>. 10

3 CARTILHA uso indevido energia. Disponível em: <http://www.aneel.gov.br/documents/656835/14876406/Cartilha-uso-indevido-energia.pdf>. 10

4 FURTO e fraude de Energia. Disponível em: <http://www.abradee.com.br/setor-de-distribuicao/perdas/furto-e-fraude-de-energia>. 10

5 LIGHT: Volume de energia roubado equivale a consumo do Espírito Santo. Disponível em: <http://www.valor.com.br/empresas/4065082/light-volume-de-energia-roubado-equivale-consumo-do-espirito-santo>. 11

6 REDES de Energia Elétrica. Disponível em: <http://www.abradee.com.br/setor-eletrico/redes-de-energia-eletrica>. 12

7 RESOLUçãO nº 506, de 1º de julho de 2008. Disponível em: <http://www.anatel.gov.br/legislacao/resolucoes/2008/104-resolucao-506#art2>. 14

8 OPENWRT. Disponível em: <https://openwrt.org/>. 14

9 [ITU-T X.1311] Security requirements for wireless sensor network routing. 16

10 RUIZ, L. B.; NOGUEIRA, J. M.; LOUREIRO, A. A. F. Manna: a management architecture for wireless sensor networks. *IEEE Communications Magazine*, v. 41, n. 2, p. 116–125, Feb 2003. ISSN 0163-6804. 16

11 ÇAYıRCı, E.; RONG, C. *Security in wireless ad hoc and sensor networks*. [S.l.: s.n.], 2009. 17

12 DARGIE, W.; POELLABAUER, C. *Fundamentals of wireless sensor networks : theory and practice*. [S.l.: s.n.], 2010. 20

13 SEGURANçA em Redes de Sensores Sem Fio. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2009/042.pdf>. 23

14 FERNANDES, N. C. *Análise de Ataques e Mecanismos de Segurança em Redes Ad Hoc*. [S.l.: s.n.], 2006. 23

15 SISTEMA DE POSICIONAMENTO DE AGREGADORES DE DADOS EM REDES ELÉTRICAS INTELIGENTES. Disponível em: <http://www.midiacom.uff.br/midiacom/images/documentos/artigos-siris/Eriac2015.pdf>. 24

16 UK-DALE. Disponível em: <https://www.doc.ic.ac.uk/~dk3810/data/>. 30

17 NANODE. Disponível em: <http://www.nanode.eu/>. 31

18 OLSR. Disponível em: <http://www.olsr.org/docs/README-Link-Quality.html>. 34

19 MIDIACOM. Disponível em: <http://www.midiacom.uff.br/midiacom/index.php/pt-BR/projetos/redes-sem-fio/scifi>. 38

20 OPENWISP. Disponível em: <http://openwisp.org/whatis.html>. 38

21 CACTI. Disponível em: <http://www.cacti.net/>. 38

22 MRTG. Disponível em: <http://oss.oetiker.ch/mrtg/>. 38

23 REVISTA Crea. Disponível em: <http://revistacrea.crea-pr.org.br/artigo-2/>. 38

ANEXO A – Configuração de firewall

```
config defaults
        option syn_flood '1'
        option input 'ACCEPT'
        option output 'ACCEPT'
        option forward 'REJECT'

config zone
        option name 'lan'
        option input 'ACCEPT'
        option output 'ACCEPT'
        option forward 'ACCEPT'
        option network 'lan'

config zone
        option name 'mesh'
        option input 'ACCEPT'
        option output 'ACCEPT'
        option forward 'ACCEPT'
        option network 'SensorMesh'

config zone
        option name 'wan'
        option input 'REJECT'
        option output 'ACCEPT'
        option forward 'REJECT'
        option masq '1'
        option mtu_fix '1'
        option network 'wan'

config forwarding
        option src 'mesh'
        option dest 'wan'
```

ANEXO B – Configuração das interfaces

```
config interface 'loopback'
        option ifname 'lo'
        option proto 'static'
        option ipaddr '127.0.0.1'
        option netmask '255.0.0.0'

config interface 'lan'
        option ifname 'eth0'
        option type 'bridge'
        option proto 'static'
        option netmask '255.255.255.254'
        option ipaddr '10.100.200.1'
        option ipv6 '0'

config interface 'wan'
        option ifname 'eth1'
        option proto 'dhcp'

config interface 'SensorMesh'
        option _orig_ifname 'radio0.network1'
        option _orig_bridge 'false'
        option proto 'static'
        option netmask '255.255.255.248'
        option ipaddr '10.100.100.X'
        option dns '8.8.8.8 8.8.4.4'
```

ANEXO C – Configuração OLSRD

```
config olsrd
        option IpVersion '4'
        option FIBMetric 'flat'
        option LinkQualityLevel '2'
        option LinkQualityAlgorithm 'etx_ff'
        option OlsrPort '698'
        option Willingness '3'
        option NatThreshold '1.0'

config Interface
        list interface 'wlan'
        option ignore '0'

config InterfaceDefaults
        option Mode 'mesh'

config Interface
        option ignore '0'
        option interface 'SensorMesh'
        option Mode 'mesh'

config LoadPlugin
        option library 'olsrd_nameservice.so.0.3'
        option ignore '0'
        option sighup_pid_file '/var/run/dnsmasq.pid'
        option interval '30'
        option timeout '300'
        option name_change_script 'touch /tmp/namechange'
        list name 'Node-00X'

config LoadPlugin
        option library 'olsrd_arprefresh.so.0.1'
        option ignore '0'




config LoadPlugin
        option library 'olsrd_dyn_gw.so.0.5'
        option ignore '0'

config LoadPlugin
        option library 'olsrd_httpinfo.so.0.1'
```

```
        option port '1978'
        list Net '0.0.0.0 0.0.0.0'
        option ignore '0'

config LoadPlugin
        option library 'olsrd_txtinfo.so.0.1'
        option accept '0.0.0.0'
        option ignore '0'

config LoadPlugin
        option library 'olsrd_jsoninfo.so.0.0'
        option ignore '0'

config LoadPlugin
        option library 'olsrd_dot_draw.so.0.3'
        option ignore '0'

config LoadPlugin
        option library 'olsrd_watchdog.so.0.1'
        option ignore '0'

config LoadPlugin
        option library 'olsrd_secure.so.0.6'
        option ignore '0'
```

ANEXO D – Configuração wireless

```
config wifi-device 'radio0'
        option type 'mac80211'
        option channel '11'
        option hwmode '11g'
        option path 'pci0000:00/0000:00:0e.0'
        option country 'US'
        option txpower '15'

config wifi-iface
        option device 'radio0'
        option ssid 'SensorMesh'
        option network 'SensorMesh'
        option mode 'adhoc'
        option encryption 'wep-shared'
        option key '1'
        option key1 'foo'
```