UNIVERSIDADE FEDERAL FLUMINENSE

Margareth Apostolo dos Santos

Utilizando Técnicas de Confiança para Controle Adaptativo do Intervalo de *Polling* nos Sistemas de *Smart Metering*

Dissertação de Mestrado

Niterói

2014

UNIVERSIDADE FEDERAL FLUMINENSE

Margareth Apostolo dos Santos

Utilizando Técnicas de Confiança para Controle Adaptativo do Intervalo de *Polling* nos Sistemas de *Smart Metering*

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia de Telecomunicações da Universidade Federal Fluminense como parte dos requisitos necessários à do título de Mestre em Engenharia de Telecomunicações. Área de concentração: Comunicação de dados multimídia.

Orientadora: Natalia Castro Fernandes

Niterói

Janeiro 2014

UNIVERSIDADE FEDERAL FLUMINENSE

Margareth Apostolo dos Santos

Utilizando Técnicas de Confiança para Controle Adaptativo do Intervalo de *Polling* nos Sistemas de *Smart Metering*

Dissertação apresentada à Universidade Federal Fluminense, como parte das exigências do Programa de Pós-Graduação em Engenharia de Telecomunicações, área de concentração em Comunicação de Dados Multimídia, para a obtenção do título de Mestre.

Aprovada em ___ de _____ de _____

BANCA EXAMINADORA

_____

Profª. NATALIA CASTRO FERNANDES, D.Sc.
Universidade Federal Fluminense (UFF)
Orientadora

_____

Profº CARLOS ALBERTO MALCHER BASTOS
Universidade Federal Fluminense (UFF)

_____

Profº Marcel William Rocha da Silva
Universidade Federal Rural do Rio de Janeiro (UFRRJ)

Niterói

Janeiro 2014

“Conhecimento, filha, é o único bem que ninguém lhe tirará”.

Hugo Athanasio dos Santos e Edith Apostolo dos Santos

AGRADECIMENTOS

Meus primeiros agradecimentos são endereçados aos meus pais, Hugo e Edith, pela vida que me permitiram ter, pela minha educação, pela minha instrução, apesar de todas as dificuldades financeiras, pelo amor sincero que sempre recebi. Agradeço ao meu esposo José Antonio, ao meu filho Lucas e aos meus gatos Bidu e Leon, que diariamente suportaram meus momentos de nervosismo e me ajudaram com as tarefas de casa, a fim de me permitir um maior aproveitamento do tempo, com meus estudos. Agradeço às minhas irmãs Simone e Anália, meus cunhados Eduardo e Antonio, sobrinhos Ana Carolina, Allan e Andressa e aos demais membros da minha grande e maravilhosa família, pela paciência em função do meu afastamento em alguns momentos, por estar dedicada à conclusão desse projeto e ao oferecimento de computador e software quando meus recursos apresentavam problema ou não estavam suportando a complexidade do processamento requerido. Agradeço aos meus amigos José Carlos Dias, Jair e Milton Flores que não me deixaram desistir, me apoiaram em momentos de envolvimento com uma carga de trabalho muito alta, dificultando a minha disponibilidade para estudar, apesar de querer demais continuar. À Sebastiana, que ouvindo minhas reclamações a respeito do meu computador, rapidamente me entregou seu computador pessoal para que eu pudesse concluir as simulações, ainda por fazer. Por fim, agradeço ao professor Carlos Alberto Malcher Bastos que me concedeu essa oportunidade e começou orientando minha dissertação e à professora Natália Castro Fernandes que entrou em um segundo momento e me orientou na conclusão desse trabalho. Aos demais professores, pelo conhecimento! À Deus, pela saúde, pela presença constante em meu coração e pela oportunidade que me deu de viver esses grandes momentos e compartilhá-los com meus entes queridos.

.

Resumo da Dissertação apresentada à UFF como parte dos requisitos necessários para a obtenção do grau de Mestrado em Ciências (M.Sc.)

Utilizando Técnicas de Confiança para Controle Adaptativo do Intervalo de *Polling* nos Sistemas de *Smart Metering*

Margareth Apostolo dos Santos

Janeiro/2014

Orientadora: Natalia Castro Fernandes
Programa de Pós-Graduação em Engenharia de Telecomunicações

O *Smart Metering* é de grande importância para as *Smart Grids*, pois permite que os clientes interajam com o sistema, garantindo um melhor controle da rede elétrica. Contudo, o uso desses novos equipamentos de medição gera um grande volume de dados que precisa ser tratado pelas concessionárias de distribuição de energia. Além disso, por serem equipamentos eletrônicos capazes de processar dados e se comunicar, os *Smart Meters* também podem ser usados para realização de ataques contra o controle da rede elétrica. Esse trabalho propõe uma mudança na forma de coleta dos dados dos *Smart Meters*, para garantir uma maior velocidade na detecção de falhas e ataques e, ao mesmo tempo, controlar o volume de mensagens enviadas para a concessionária. O sistema proposto utiliza um modelo de confiança para avaliar os dados de diferentes áreas, observando aspectos como os tipos de mensagens enviadas, os relatórios de consumo, os relatórios de qualidade observada da energia e, ainda, as falhas no envio de mensagens. Com base nesses dados e em valores históricos, o sistema infere quais áreas possuem problemas, sejam eles falhas ou clientes fraudulentos, disparando rapidamente alarmes para a concessionária. Para tanto, os dados do sistema de confiança são usados para a determinação do intervalo de coleta de dados de uma determinada área, pois, caso alguma alteração seja detectada, uma coleta mais frequente pode ajudar a definir mais rapidamente se é necessário ou não o acionamento da concessionária. Da mesma forma, o sistema proposto aumenta o intervalo de *Polling* em áreas que não apresentam problemas, para reduzir o volume de dados coletados. Foi desenvolvido um simulador para analisar o sistema proposto e os resultados mostraram não apenas a capacidade de detectar áreas com problemas, mas também as vantagens com relação a tempo de detecção de falhas e volume de mensagens processados quando comparado aos sistemas de coleta padrão dos *Smart Meters*.

Palavras-Chave: Medidores inteligentes, *Polling*, sistema de confiança.

Abstract of Dissertation presented to UFF as partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

Using Trust Techniques to Adaptively Control the *Polling* Interval in *Smart Meter*ing Systems

Margareth Apostolo dos Santos.

January/2014

Advisor: Natalia Castro Fernandes
Department of Telecommunications Engineering

The Smart Metering is important for the Smart Grid because it allows customers to interact with the system, ensuring better control of the power Grid. The use of this new measurement equipment, however, generates a large volume of data that needs to be addressed by energy distribution concessionaries. Moreover, the Smart Meters are electronic equipment capable of processing data and communicating. Hence they can also be used to attack the control Grid. This paper proposes a change in the control of data gathering of Smart Meters to ensure greater speed in detecting failures and attacks while also controlling the volume of messages sent to the concessionary. The proposed system uses a trust model to evaluate data from different city areas based on aspects such as the types of messages sent by the consumers, consumption reports, quality of energy reports, and failures in sending messages. Based on this data and historical values, the proposed system infers which areas have problems, whether failures or fraudulent customers, quickly warning the concessionary. The trust system data is used to modify the data gathering interval of a particular area. Indeed, if any change is detected, more frequent data gathering can help to quickly decide whether to warn the concessionaire or not. Likewise, the proposed system increases the Polling interval in areas without problems to reduce the monitored data volume. A simulator was developed to analyze the proposed system. The results show the system ability to detect problem areas and also the advantages of the proposed system related to fault detection time and processed message volume when compared to the standard gathering systems of Smart Meters.

Keywords: *Smart Meters, Polling, trust system*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

ANEEL	Agência *Nacional de Energia Elétrica*
AMI	*Advanced Metering Infrastructure*
COR	Centro de Operação Remota
CSP	Energia Elétrica Concentrada
DEC	Duração Equivalente por Unidade Consumidora
DIC	Duração de Interrupção Individual por Unidade Consumidora
DMIC	Duração Máxima de Interrupção Contínua por Unidade Consumidora
DMZ	Zona Desmilitarizada
DNP	*Distributed Network Protocol*
DOE	*Department of Energy*
DoS	*Deny of service*
ENEL	*Ente Nazionale per l'energia ELettrica*
ENDESA	*Empresa Nacional de Electricidad Sociedad Anónima*
FEC	Frequência Equivalente de Interrupção por Unidade
FIC	Frequência de Interrupção Individual por Unidade Consumidora
GPRS	*General Packet Radio Services*
GSM	*Global System for Mobile*
HAN	*Home Area Network*
HTTP	*HyperText Transfer Protocol*
IEC	Comissão Eletrotécnica Internacional
IED	Dispositivo Eletrônico Inteligente
IETF	*Internet Engineering Task Force*
MME	Ministério de Minas e Energia
MTU	*Master Terminal Unit*
NIST	*National Institute of Standards and Technology*
ONS	Operador Nacional do Sistema Elétrico
OSI	*Open System Interconnection*
PDC	Phaser Data Concentrators
PLC	Programmable Logic Controller
PV	Energia Elétrica Fotovoltaica
RMS	*Root Mean Square*

SAML	*Security Assertion Markup Language*
SCADA	*Supervisory Control and Data Acquisition*
SIN	Sistema Interligado Nacional
SIP	*Session Initiation Protocol*
SLA	*Service Level Agreement*
SM	*Smart Meter*
TA	*Trust advertisement*
TREP	*Trust Reply*
TREQ	*Trust Request*
URI	*Uniform Resource Identifier*
URL	*Uniform Resource Locator*
UTR	Unidade Terminal Remota
WAMPAC	*Wide Area Monitoring Protection and Control*
WAN	*Wide Area Network*

SUMÁRIO

Capítulo 1

Introdução

Sabe-se que o sistema elétrico sofreu muito poucas inovações dentro dos últimos 100 anos (1). O Sistema Elétrico Brasileiro, predominantemente hídrico (88% da potência e 94% da energia gerada em 1999), gerou cerca de 5.000 TWh, quantidade de energia que, na geração exclusivamente térmica, corresponde a mais da metade da reserva brasileira de petróleo, avaliada em 20 bilhões de barris (1). Nesse século, o Sistema passou por períodos com diferentes taxas de crescimento, decorrentes ora do regime hidrológico, ora de dificuldades econômicas (1).A falta de incentivos, causada pela falta de competitividade, associada à necessidade de se oferecer um sistema estável, fez com a que rede elétrica chegasse, nos dias de hoje, muito próxima do seu limite de operação. Surge um novo conceito que vem colaborar na melhoria da prestação deste serviço, as redes elétricas inteligentes ou *Smart Grids*.

O avanço tecnológico nos sistemas de telecomunicações e na eletrônica de sensores também vem impulsionar essa nova arquitetura para redes elétricas. A população, cada vez mais exigente no controle de seus custos, facilitada pela Internet, também vem como uma forte incentivo para esse novo modelo.

A estrutura do sistema elétrico tradicional, na qual a arquitetura *Smart Grid* irá se encaixar, é composta pelos sistemas de geração, transmissão, distribuição, cada um com suas respectivas subestações. Muito interligado com questões geográficas, o sistema elétrico tradicional normalmente atinge grandes áreas territoriais. O Brasil e a China são exemplos de países cujas redes de transmissão têm extensões muito grandes. De fato, o sistema atual de energia elétrica é baseado em grandes usinas de geração que transmitem energia através de sistemas de transmissão de alta tensão, que é então distribuída em média e baixa tensão até os usuários finais. Nesse sistema, o fluxo de energia é unidirecional, vindo da geração até os clientes (2).

No sistema brasileiro, predominam as fontes hídricas e linhas de transmissão com grandes extensões, devido à geografia do país. A existência de muitas bacias hídricas permite o planejamento estratégico para a geração de energia ao longo do ano. Assim, é possível gerar a energia de diferentes pontos do Brasil de acordo com o nível dos reservatórios e as expectativas de chuva para os próximos meses. Mesmo tendo essa facilidade de armazenar água em reservatórios para prever futuras demandas, em 1999, o país sofreu o blecaute mais abrangente e prolongado de sua história. Dez Estados e o Distrito Federal ficaram sem luz por quatro horas entre 10 da noite e 2 da manhã. O trânsito parou nas maiores cidades, os bombeiros receberam centenas de chamados de pessoas presas em elevadores e houve acidentes (3). Tais eventos levaram à construção de novas usinas de geração, mas deixaram o questionamento sobre a eficiência de um modelo de geração centralizada, com ponto único de falha, tornando o sistema mais vulnerável.

Com o fim do monopólio da geração elétrica, em meados dos anos 80, o desenvolvimento da geração distribuída voltou a ser incentivado. Trata-se da geração elétrica junto ou bem perto do consumidor final, normalmente de pequeno porte, como por exemplo, painéis solares fotovoltaicos, pequenas turbinas eólicas e qualquer outro tipo de fonte geradora. Ela tem vantagem sobre a central, pois economiza investimentos em transmissão e ainda pode ajudar na estabilidade do serviço de energia elétrica centralizado. Ela já foi muito utilizada pelas indústrias, na década de 40, quando toda a energia era gerada localmente. Posteriormente, a energia pública ficou mais barata e passou a ser utilizada a fim de gerar uma economia nos custos (4). A geração distribuída de pequeno porte (classificada como micro ou minigeração distribuída) pode participar do Sistema de Compensação de Energia regulamentado pela Resolução Normativa ANEEL nº 482/2012. Esse sistema também é conhecido pelo termo em inglês *net meetering* (5). Com a preocupação pela preservação do meio ambiente, o crescimento exponencial da demanda e da população e ao mesmo tempo pouco investimento para a expansão do sistema elétrico com geração centralizada, a geração distribuída pode auxiliar às grandes concessionárias nos eventos dos apagões, na complementação de energia para cumprimento do *Service-Level Agreement* (SLA) desse serviço essencial.

Sabe-se também que os investimentos não devem ser apenas relacionados à construção de novas usinas, mas também com relação à qualidade e c do serviço oferecido aos clientes. Os equipamentos eletrônicos pessoais, mesmo com a utilização de baterias, necessitam cada vez mais de cargas frequentes, devido ao uso contínuo dos mesmos, pois estão se tornando indispensáveis na vida das pessoas. Assim, os investimentos da rede devem ser de tal magnitude e ágeis que sejam capazes de acompanhar o aumento da demanda e ainda modernizar a rede elétrica, a fim de satisfazer seus clientes cada vez mais exigentes quanto à qualidade, ao acompanhamento de suas faturas, controle dos seus gastos de maneira fácil e automatizada.

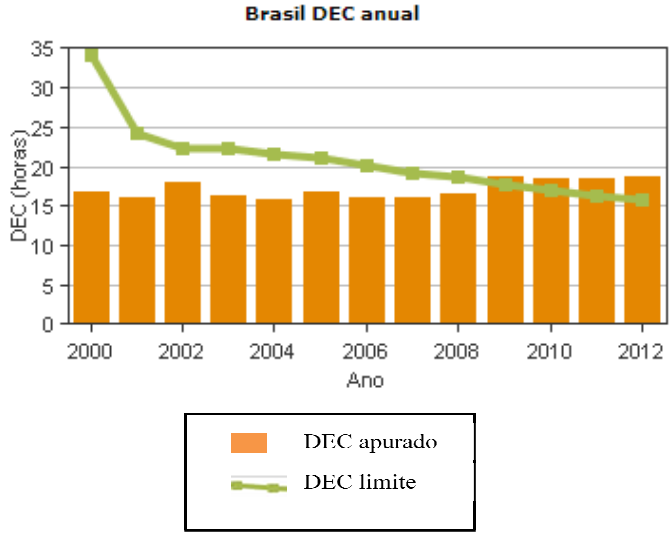
A ANEEL exige e acompanha alguns indicadores de qualidade das concessionárias do sistema elétrico, conforme mostra a Tabela 1. A DEC, a FEC, a DIC, a FIC e a DMIC são medidas que ANEEL se utiliza para manter o controle de qualidade do fornecimento de energia pelas concessionárias com a concessão para a prestação do serviço.

Tabela 1 Indicadores Aneel - (6)

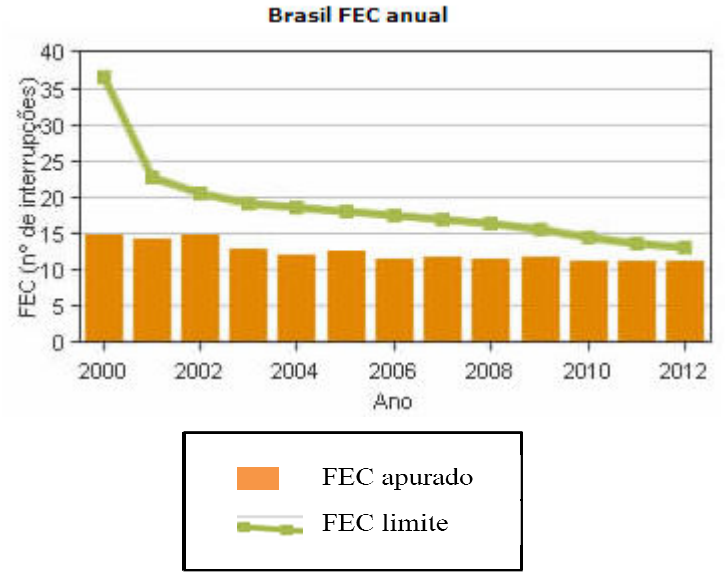
Indicador Aneel por área de concessão	
DEC	• Duração equivalente por Unidade Consumidora: indica o número de horas que, em média, as unidades consumidoras de determinado conjunto ficaram sem energia elétrica durante um determinado período: mensal, trimestral ou anual.
FEC	• Frequência Equivalente de Interrupção por Unidade Consumidora: indica quantas vezes, em média, as unidades consumidoras de determinado conjunto sofreram interrupção.
Indicador Aneel por unidade consumidora	
DIC	• Duração de Interrupção Individual por Unidade Consumidora: quantidade de horas que o consumidor ficou sem energia elétrica.
FIC	• Frequência de Interrupção Individual por Unidade Consumidora: quantidade de interrupções que o consumidor experimentou no período de apuração (mensal trimestral ou anual).

DMIC	• Duração Máxima de Interrupção Contínua por Unidade Consumidora: indica o número de horas da maior interrupção experimentada pelo consumidor no período de apuração.

A Figura 1 mostra o comportamento anual dos indicadores FEC e DEC no Brasil de 2004 a 2011, de acordo com a ANEEL. A FEC atendeu às expectativas da ANEEL, mas a DEC não, ou seja, a quantidade de interrupções no fornecimento de energia ficou dentro do tolerado, mas o tempo de interrupção não (6).



(a)



(b)

Figura 1 - Comportamento anual dos Indicadores FEC e DEC no Brasil verificado pela Aneel (6)

Esses indicadores mostram a necessidade de uma operação mais eficiente do sistema elétrico, com maior disponibilidade, ampliando os investimentos para expansão dos sistemas existentes, introduzindo fontes alternativas e inserindo o sistema em uma arquitetura inteligente que traga um melhor controle e supervisão, agilizando a manutenção e comutação para sistemas alternativos.

Os contratos de concessão assinados entre a Agência Nacional de Energia Elétrica- ANEEL e as empresas prestadoras dos serviços de transmissão e distribuição de energia estabelecem regras a respeito de tarifa, regularidade, continuidade, segurança, atualidade e qualidade dos serviços e do atendimento prestado aos consumidores. Da mesma forma, define penalidades para os casos em que a fiscalização da ANEEL constatar irregularidades. Os novos contratos de concessão de distribuição priorizam o atendimento abrangente do mercado, sem exclusão das populações de baixa renda e das áreas de menor densidade populacional. Prevê ainda o incentivo à implantação de medidas de combate ao desperdício de energia e de ações relacionadas às pesquisas voltadas para o setor elétrico (5).

Uma forma para garantir uma redução na quantidade e duração das falhas seria modificar o modelo de geração unidirecional de energia (2). Atualmente, já se conhece diversas formas de geração distribuída, como os painéis solares, as usinas eólicas, os geradores baseados no movimento das marés, entre outros, que poderiam ser utilizadas como forma de backup para as grandes usinas de geração. A aplicação de um modelo desse tipo, contudo, depende de uma grande reestruturação da infraestrutura da rede elétrica desde a geração até os clientes.

Outra questão que motiva a modernização da rede é a questão dos custos para instalação e manutenção. A rede elétrica é projetada para atender os horários de pico, garantindo que nenhuma área ficará sem energia nos momentos de maior demanda. Contudo, o que se observa dos gráficos de consumo é que a demanda máxima é concentrada em poucas horas do dia. Com isso, toda a infraestrutura fica ociosa durante a maior parte do dia. Observou-se que, se existisse uma maior interatividade com os clientes e algumas políticas de incentivo, os clientes poderiam distribuir parte de seu consumo ao longo do dia, diminuindo a demanda nos horários de pico (2). Contudo, devido às restrições tecnológicas das redes elétricas tradicionais em operação, isso não é possível.

Tudo isso reflete a baixa integração do sistema elétrico, em especial, das

redes de controle, com os consumidores. De fato, embora os consumidores sejam os grandes interessados no provimento da energia, eles não podem dar *feedbacks* em tempo real para as concessionárias sobre novas demandas ou a qualidade da energia observada. A principal prova dessa desconexão entre os clientes e as concessionárias é o fato da medição do consumo ainda existir em muitos clientes de forma manual, mesmo já existindo, há muitos anos, formas convenientes e baratas para comunicação dos clientes com as concessionárias. A medição manual, além de gerar um alto custo para as concessionárias, provê poucas informações que possam ajudar no controle de demanda ou de qualidade da rede.

Os medidores tradicionais podem ser analógicos ou digitais. Os analógicos são compostos por quatro relógios, começando a leitura pelo marcador da unidade à direita, os ponteiros geram no sentido horário e anti-horário e sempre no sentido crescente dos números, ou seja, do menor para o maior número. Os digitais ou ciclométricos apresentam os algarismos em formato digital, como se fosse um registrador de quilometragem de um veículo, nesse caso os valores apresentados já indicam o consumo (7). Os medidores de consumo digitais facilitam a leitura com relação aos analógicos e os *Smart Meters* vêm para fazer a leitura para faturamento junto à concessionária, e, com uma via bidirecional em que há uma troca de informações entre concessionária e consumidores, coleta dados e envia comandos remotos. A Ampla, por exemplo, está trabalhando e investindo em medidores eletrônicos e mais modernos. São automatizados, ficam nos postes e permitem sua leitura pelos consumidores. As medidas são enviadas automaticamente para a concessionária do sistema e também ficam visíveis ao consumidor. E por fim, permitem o disparo remoto de comandos (7).

O Sistema Elétrico tem uma história de protocolos proprietários, sistemas fechados e de difícil integração com outros sistemas. De fato, o sistema elétrico atual tem uma estrutura pouco baseada nas técnicas de comunicações mais modernas. As *Smart Grids* vêm se posicionando como uma arquitetura que proporcionará melhorias no sistema elétrico e com iniciativas espalhadas por todo o mundo. De modo a ilustrar esse conceito, seguem alguns projetos pelo mundo, ressaltando a iniciativas brasileiras:

- O *PowerMatching City* é um projeto liderado pela firma DNV KEMA *Energy and Sustainability,* que envolve vinte e cinco casas no distrito de *Hoogkerk* na Holanda, que estão interligadas e equipadas com

micro sistemas de potência e calor, bombas de calor híbridas, painéis fotovoltaicos, medidores inteligentes, estações de recarga de veículos e aplicações de casas inteligentes. (2)

- O GRID4EU é um projeto liderado por um grupo de operadores do sistema de distribuição de seis países que visa testar conceitos e tecnologias novas para diminuir as barreiras técnicas econômicas, sociais, ambientais e regulamentares no sistema de distribuição (2).
- OEU-DEEP é um projeto executado entre 2004 e 2009, integrando oito empresas de energia do sistema de distribuição de vários países da Europa, buscando remover a maioria dos obstáculos técnicos que impediam o gerenciamento das fontes distribuídas (2).
- O EPRI *Advanced Distribution Automation* (ADA) é a criação do sistema de distribuição do futuro. Visa melhorar a confiabilidade e a qualidade da energia, reduzir os custos operacionais, melhorar o tempo de restauração, aumentar as opções de serviços aos consumidores, integrar a geração distribuída e o armazenamento de energia e integrar os sistemas dos consumidores (2).
- A implementação das Smart Grids na China, de acordo com o *State Grid Corporation of China*, foi dividida em três etapas: planejamento e testes (2009- 10), construção e desenvolvimento (2010-15) e atualização (2016-20). Para tanto, uma série de projetos estão em andamento (2).
- No *Smart Grid Korea* 2030, foi escolhida, em 2009, a ilha Jeju como local para montar a testbed integral de *Smart Grid* inicialmente com 10 projetos. Consiste em testar e desenvolver novas tecnologias, assim como novos modelos de negócio. São três fases, subdivididas em cinco setores: *Smart power Grid, Smart consumer, Smart transportation, Smart renewable* e *Smart electricity service* (2).
- A empresa Light S.A., com seu Programa *Smart Grid Light*, tem um projeto piloto que abrange mil de seus clientes. Nesse projeto, medidores e tomadas inteligentes serão utilizados para permitir aos usuários conhecer seu consumo em tempo real, ao mesmo tempo em que detecta pontos de desperdício, horários de maior consumo e pontos

de possível redução de consumo para a tomada de medidas na gerência da rede (2).

- A Cemig, desde o ano 2010, está executando o projeto Cidades do Futuro, analisando os benefícios e as capacidades da arquitetura Smart Grid em implementação na cidade de Sete Lagoas (MG). A empresa distribuidora pretende aplicar as tendências da cadeia de valor das redes inteligentes de energia em suas instalações elétricas, telecomunicações, sistemas computacionais e interface com os consumidores e geradores distribuídos (2).
- O Projeto Cidade Inteligente de Búzios, em que o Grupo Enel através da Endesa está implantando em Búzios a primeira cidade inteligente do Brasil (8). O projeto inclui a colocação de medidores inteligentes nas residências, permitindo ao consumidor o controle do seu consumo e escolha do melhor momento de utilizar seus eletrodomésticos em função da redução de tarifa oferecida pela concessionária em horários fora do pico. A concessionária Ampla, por sua vez, controlará em tempo real a demanda de energia da cidade. A Ampla também controlará o acionamento da Iluminação Pública, de forma individualizada, por lâmpada. Cada lâmpada poderá remotamente ser ligada e desligada e ter sua luminosidade ajustada. Várias novas medidas serão coletadas, tais como temperatura e corrente, para ajustar os parâmetros da rede elétrica. Ainda está em estudo o tipo de acesso da rede Wide Area Network (WAN) a ser utilizada no projeto. Estuda-se a utilização de rede em malha de rádio na freqüência de 2,4GHz, **Ethernet Passive Optical Network** (EPON) a 1,25 Gbps, General Packet Radio Services (GPRS) na velocidade de 40kbps, Rádio Frequência a 400MHz e Programmable Logic Controller (PLC) em banda larga a 200Mbps.

As redes elétricas estão em um momento crítico da sua modernização e esforços para melhorar a comunicação dentro dessas redes são de importância primordial e por isso, se tornaram foco desse trabalho. Com a falta de crescimento sofrida pelo sistema elétrico nos últimos anos e o aumento da demanda, a modernização com uma supervisão mais inteligente, envolvendo inclusive o consumidor, principal alvo da concessão, incluindo novas fontes sustentáveis e

alternativas e controles mais objetivos, vem ajudar a reverter esse quadro, infelizmente perigoso em que o Brasil se encontra, pondo em risco os serviços ditos essenciais e o seu desenvolvimento tecnológico. Esse trabalho vem contribuir para essa nova iniciativa, promovendo ideias sobre a forma de coleta dos dados dos medidores inteligentes, que também se inserem nesse novo conceito de rede Smart Grid, e sobre o tratamento desses dados de modo a acelerar a identificação de falhas e fraudes.

1.1. Motivação

Os *Smart Grids* fazem uso, dentre outros recursos, de medidores inteligentes denominados *Smart Meters*, responsáveis pela coleta de dados da energia consumida em um imóvel e exportação para os sistemas de controle da concessionária, por meio de redes de telecomunicações.

Com isso, surge mais uma fonte de informação que efetivamente colabora na correção de problemas, e principalmente tornando o cliente um elemento ativo do sistema. Pode-se observar pela Figura 2, que mostra os investimentos em *Smart Grid* no mundo, que os sistemas de *Smart Metering* recebem investimentos nos países analisados. Com o uso dos *Smart Meters* é possível um conhecimento melhor da qualidade da energia oferecida e dos períodos de indisponibilidade do serviço, um controle mais eficiente das demandas e a inserção de incentivos para distribuição do consumo ao longo do dia pelos clientes, com políticas de redução de tarifa em horas de menor consumo de energia, por exemplo (2). Isso, sem mencionar a redução de custos devido ao fim da medição manual.

Figura 2 - Investimento previstos em vários países para a implantação de Smart Grids, referência de 2010.- Fonte: (9)

Contudo, a inserção dessa nova tecnologia cria uma nova preocupação para o controle da rede elétrica. Uma vez que os medidores são eletrônicos e capazes de se comunicar com a rede de controle do sistema elétrico, esses medidores podem ser usados maliciosamente para prejudicar o funcionamento da rede. De fato, os medidores funcionam como computadores, que podem ser usados tanto para o bem, ou seja, enviando as medidas observadas, quanto para o mal, para informar dados falsos. Em um cenário mais crítico, *hackers* podem disseminar vírus pelos medidores com a finalidade de realizar ataques de negação de serviço contra o sistema elétrico. A segurança passa, então, a ter uma complexidade maior, tendo que isolar dados adulterados dos dados reais de medição.

A segurança dos *Smart Grids* se fundamenta sobre três conceitos: disponibilidade, confidencialidade e integridade (Figura 4). Dependendo do tipo de ataque, um desses conceitos pode ser afetado.

A confidencialidade é a proteção do conteúdo dos dados coletados. Devido à quebra de privacidade das informações de consumo, ladrões poderiam usar estes dados sigilosos que foram obtidos para fazer um levantamento dos hábitos das residências. *Hackers* poderiam obter as informações confidenciais de usuários de uma determinada companhia elétrica e de posse desses dados, poderiam vendê-los para terceiros (10) motivando dentre outras, a oferta de

serviços de acordo com o perfil do cliente conforme Figura 3 - Perfis de consumo de energia fixados a partir dos eletrodomésticos utilizados no imóvel. Fonte:

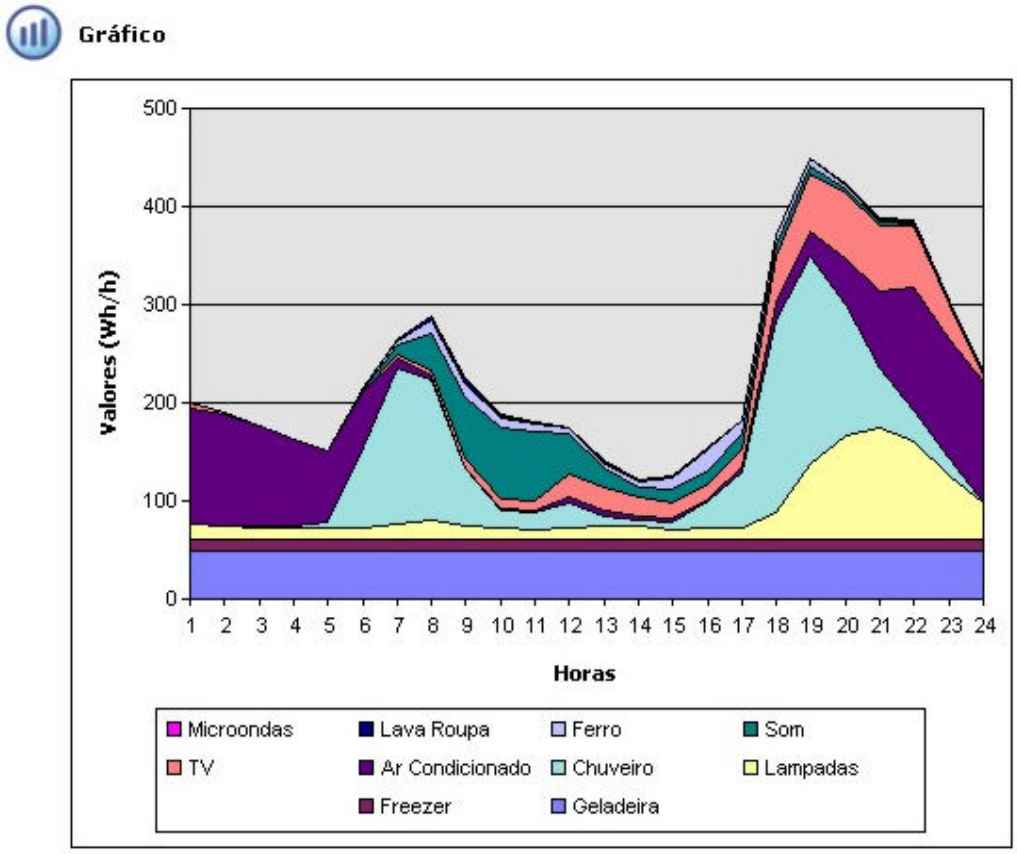


Figura 3 - Perfis de consumo de energia fixados a partir dos eletrodomésticos utilizados no imóvel. Fonte: (11)

A integridade é a não intervenção externa na informação, ou seja, a garantia de que os dados não foram adulterados. Dados incorretos podem afetar faturamento, percepção do sistema e estimular ações indevidas no sistema. Em um cenário em que os usuários tanto consumiriam quanto gerariam energia, uma simples mudança de dados pelo consumidor, fazendo com que a companhia acreditasse que ele estava produzindo energia, traria lucros indevidos ao usuário em questão. Outro exemplo, seria a fraude nas informações de preço vindas das companhias geradoras, visto que, se o consumidor recebe a informação adulterada para menos, ele incrementa o consumo, a companhia fica com prejuízo e se o consumidor recebe a informação de preço mais alto do que deveria ser, ele fica no prejuízo (10).

A disponibilidade é aferida pelo percentual de tempo que o sistema fica funcionando, que é a que afeta normalmente um maior número de consumidores,

sendo, portanto o item de maior gravidade. Mas também há a disponibilidade de fornecimento de relatórios para o consumidor, de preços atualizados. Quanto à coleta de dados de consumo, a disponibilidade não é tão grave porque pode ser coletada posteriormente (10).

Outro ataque importante é a negação de serviço (DoS) que consome recursos respondendo a uma avalanche de solicitações falsas. São utilizadas fontes de ataques distribuídos, como aparelhos e medidores inteligentes para essa geração de dados (10).

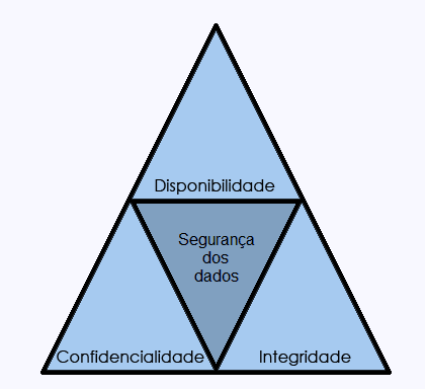


Figura 4 - Base da Segurança dos Dados Fonte: (10)

Outra ferramenta importante em um *Smart Grid* é utilizar *Data Mining* para tratar esse grande volume de dados a serem recebidos dos clientes em busca de padrões que são informações que ajudam na detecção de fraude. O desvio de um padrão pode representar uma mudança no perfil ou uma tentativa de fraude (10).

Outra questão é o aumento do volume de dados a ser tratado pelos sistemas de controle e supervisão. Uma vez que todas as unidades consumidoras tenham *Smart Meters* instalados, elas passam a enviar relatórios detalhados sobre o provimento e o consumo de energia. Embora individualmente esses dados tenham pequeno volume, ao se observar toda a massa de clientes, esses dados ganham status de *Big Data* (12). Assim, passam a existir não apenas problemas de coleta e armazenamento, mas também de processamento dentro de um tempo viável para a tomada de medidas de manutenção e de isolamento de fraudes (13).

Big Data significa grande volume de dados. Com a proliferação dos *Smart Meters* residenciais, com coletas de dados periódicas, a preocupação com armazenamento, processamento, filtragem de dados válidos passam a fazer parte

do cardápio das concessionárias do sistema elétrico. Para ilustrar esse conceito, o Operador Nacional do Sistema Elétrico (ONS) está conduzindo uma prova de conceito de *Big Data* em um projeto que vai coletar dados em tempo real de tensão, corrente e frequência por meio de sensores instalados em linhas de transmissão e sistemas de geração de energia. A coleta se dará na frequência de 60 vezes por segundo em um volume próximo a 200 terabytes. As medidas serão inicialmente coletadas por 30 PMU (*Phasor Measure Unit*)[1], processadas em tempo real para a verificação da saúde do sistema e armazenadas em uma nuvem contratada da *Amazon Web Services* (14).

A partir dos problemas apresentados anteriormente, as principais motivações para o desenvolvimento dessa dissertação são:

- Necessidade de um sistema que observe os dados coletados pelos *Smart Meters* e consiga extrair informações de problemas na rede, mesmo existindo usuários maliciosos, ou seja, usuários que tentam fraudar o sistema ou gerar interrupções no provimento de energia. Os problemas devem incluir tanto falhas na rede quanto a própria detecção do usuário malicioso.
- Detecção rápida dos problemas na rede, através do controle de requisições de medições aos *Smart Meters*, evitando que pequenos problemas levem a grandes falhas e/ou prejuízos no sistema.
- Controle do volume de dados gerados, diminuindo o processamento de dados dos *Smart Meters.*
- Aceleração da detecção de falhas e fraudes no sistema elétrico.

1.2. Sistema Proposto

O sistema proposto nesse trabalho visa controlar a periodicidade de coleta de dados dos medidores inteligentes, diminuindo o volume de dados a serem processados, criando regras de análise desses dados de modo a torná-los úteis à

[1] PMU é um equipamento que mede os fasores (representação gráfica semelhante a um vetor, se referindo às grandezas que variam no tempo, como as ondas senoidais) de corrente e de tensão, por meio de amostragens das formas de onda dessas informações, utilizando sinal de sincronismo de um GPS.

concessionária e aos consumidores de energia e acelerar a identificação de problemas no sistema referentes às falhas e fraudes.

A proposta desse trabalho inclui a variação da frequência de coleta dos dados, de modo a não processar os dados de todos os medidores inteligentes o tempo todo, criando o conceito de *Polling* adaptativo. Essa adaptação do intervalo de coleta de dados é feita com base em dados gerados por um sistema de confiança. Clientes com dados bem comportados, dentro de uma faixa de normalidade, permanecem com uma frequência menor de coleta. Quando existem clientes ou conjunto de clientes vizinhos que apresentem dados fora da normalidade, com suspeita de fraude ou de degradação do serviço, se efetiva o incremento do *Polling* de modo a conferir, o mais rápido possível, alguma condição anômala do sistema ou do cliente. A partir da confirmação desses problemas, a concessionária pode acionar a equipe técnica mais adequada ao problema, para inspeção em campo e outras medidas cabíveis.

Reduzir o tempo de detecção e correção de falhas também constitui um dos objetivos a ser alcançado.

Outro objetivo inclui um tratamento dos dados coletados, gerando alarmes para a concessionária, correlacionados a possíveis candidatos para fonte do problema. Para tanto, o sistema proposto faz:

- a correlação entre medidas de energia gerada com a consumida;
- a comparação de percepção de qualidade da energia fornecida emitida pelos vizinhos de um mesmo segmento do sistema, por exemplo, uma área composta por imóveis alimentados por um mesmo transformador;
- a distinção de mensagens de ataque à rede de telecomunicações de mensagens adequadas e aptas ao processamento.

A análise dos dados é feita baseada no grau de confiança que lhes são conferidos pela comparação com dados históricos, reincidência de eventos em curtos períodos de tempo e composição do próprio dado (conteúdo, formato, tamanho etc.).

Complementando o trabalho de estudo, foi elaborada uma simulação para a experimentação da proposta que incluiu: utilização do modelo de confiança, tratamento com comparação de dados e *polling* adaptativo.

O resultado da simulação foi satisfatório, confirmou a eficiência da proposta. Os testes mostraram que em condições normais da rede, houve uma

diminuição dos dados a coletar e consequentemente a processar e os alarmes de falhas e fraudes foram acelerados, dependo do problema, entre 10 e 57% do tempo.

1.3. Vantagens do Sistema Proposto

O sistema proposto trará vantagens tanto para os clientes quanto para as concessionárias do sistema elétrico.

Com a utilização dos *Smart Meters*, , o cliente poderá além de controlar o consumo dos seus eletrodomésticos e, consequentemente, seus gastos com energia elétrica, obter relatórios mais detalhados sobre a utilização da energia em seu imóvel ao longo do dia. Os relatórios mostrarão ao cliente os equipamentos com maior demanda energética e as horas do dia de maior consumo. De fato, o sistema proposto reduz os gastos das concessionárias de distribuição, pois permite a identificação remota de "gatos" e outras fraudes, uma rápida recuperação de falhas, coleta e processamento dos dados dos *Smart Meters* de forma mais inteligente. Essa economia poderá ser refletida na conta do cliente, que contará com uma rede mais bem gerenciada.

As concessionárias também terão vantagens como:

- perceber mensagens falsas;
- perceber consumos não registrados (vulgarmente chamado de *gato*);
- isolar pontos suspeitos de forma a dar um tratamento mais minucioso e detectar possíveis fraudes rapidamente.
- obter uma percepção de qualidade dividida por área, identificando reclamações impróprias de usuários dentro de áreas sem queixas, e, portanto com grande evidência de tratar-se de um problema de responsabilidade do cliente e não da concessionária;
- ter uma administração facilitada devido ao sistema automatizado de coleta de medições de consumo que reduz o número de mensagens coletadas;
- reduzir multas devido à manutenção mais rápida;
- aprimorar o planejamento da rede elétrica a partir de informações mais detalhadas ao longo do dia e não acumulada mensalmente.

1.4. Organização do Trabalho

A dissertação está organizada da seguinte forma: no Capítulo 2 descreve-se o Sistema Elétrico de Potência, tanto o tradicional quanto sua evolução para os *Smart Grids*. No Capítulo 3, o estado da arte dos modelos de confiança é descrito, apresentando alguns trabalhos relacionados. A ideia central que norteia o sistema proposto é o uso de um sistema de confiança tanto para identificar os problemas quanto para reduzir ou aumentar o intervalo de *polling*. No Capítulo 4, a proposta propriamente dita de *Polling* adaptativo com base no grau de confiança é descrita. No Capítulo 5, o ambiente de simulação da proposta com uso de Matlab é descrito, assim como os resultados obtidos. O Capítulo 6 conclui o trabalho e apresenta alguns trabalhos futuros.

Capítulo 2

O Sistema Elétrico de Potência

O Setor Elétrico tem participação vital no crescimento sustentável de um país. Ele interfere na economia, pois quase todos os setores econômicos de um país, que no somatório de sua produção definem a magnitude do PIB, consomem energia elétrica em alguns segmentos (15).

O setor elétrico sempre buscou a disponibilização de um sistema estável, com alta disponibilidade, mas a falta de investimentos em mais infraestrutura e a baixa utilização de novas tecnologias culminaram na crise de energia de 2001 no Brasil, quando apareceu a vulnerabilidade do setor (15).

Para entender o que causa problemas dessa natureza nas redes elétricas, e posterior proposta das *Smart Grids*, é preciso conhecer a estrutura interna do sistema e quais as suas principais desvantagens.

2.1. O Sistema Elétrico de Potência Tradicional

O sistema elétrico de potência envolve diversos elementos, como mostrado na Figura 5, que vão desde a geração até a distribuição de energia aos seus consumidores finais. Descrevendo melhor esses elementos temos:

- Usinas de geração: a geração de energia elétrica envolve a transformação de energia mecânica ou térmica em energia elétrica. No Brasil, a principal fonte de geração de energia são as usinas hidrelétricas. Nessas usinas, a água de rios é armazenada para posterior conversão em energia mecânica através de uma turbina hidráulica. O giro da turbina hidráulica permite o acionamento de um gerador elétrico e, então, a conversão para energia elétrica. O Brasil também dispõe de outras fontes, tais como termelétricas movidas a carvão vegetal, usinas nucleares que utilizam a energia

contida no núcleo dos átomos. Em menor escala, existe também a geração a partir da radiação solar, de energia de biomassa, produzida a partir de material orgânico, e do movimento do vento.

- Linhas de transmissão e distribuição: esses elementos são responsáveis pela condução da energia elétrica das usinas de geração até os consumidores. Durante a transmissão e a distribuição, o nível de potencial é variado algumas vezes de forma a reduzir perdas.
- Subestações: é um conjunto de equipamentos de manobra e ou transformação e eventual compensação de reativos utilizados para dirigir o fluxo de energia em rotas alternativas, possuindo sistemas de proteção capazes de detectar e isolar falhas. Ela pode ser do tipo transformadora, que converte a tensão para um nível diferente, ou seccionadora, de manobra ou de chaveamento, que interliga circuitos de suprimento sob o mesmo nível de tensão permitindo sua multiplicação. É também utilizada no seccionamento de circuitos, permitindo a energização em trechos sucessivos de menor comprimento (16).
- Barramentos: são linhas de transmissão internas das subestações. São utilizados para interconectar as diversas linhas que trazem a energia para a subestação com os diversos transformadores.
- Transformador: dispositivo elétrico utilizado para aumentar ou diminuir a tensão. A elevação normalmente é só na usina de geração e a diminuição é para alimentar as linhas de transmissão e distribuição.

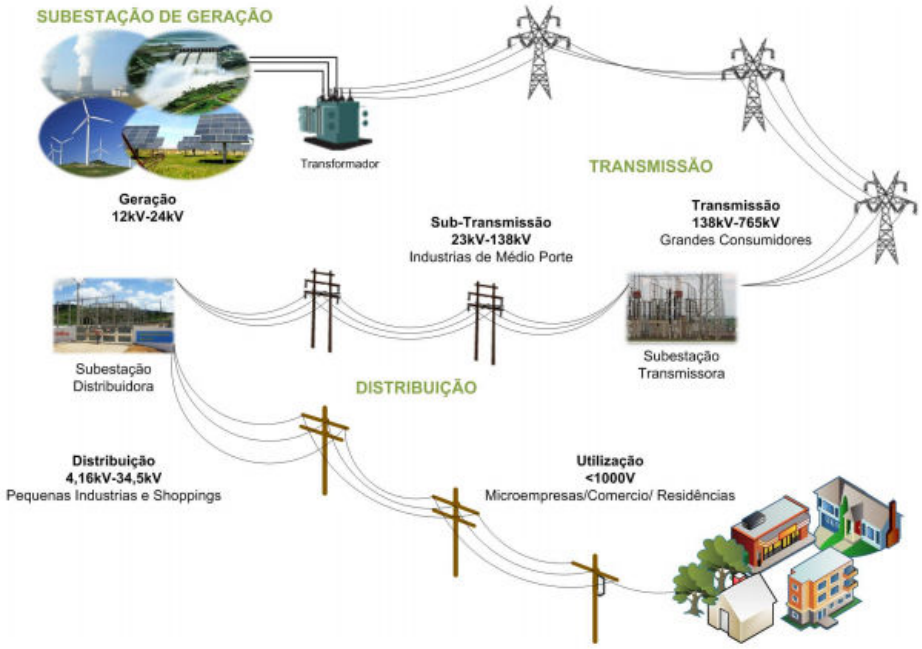


Figura 5 - Elementos do Sistema Elétrico de Potência (17)

Falhas no sistema elétrico têm um impacto muito grande na vida das pessoas e nos negócios, pois afetam o SLA acordado com cliente e a disponibilidade desse serviço essencial exigido pela regulamentação brasileira. Contudo, são muitos os problemas, alguns deles gerando falhas, como por exemplo: instabilidade, colapso de tensão, frequência e tensões indevidas, propagação de falhas, clientes mal intencionados que adulteram a medição do consumo do seu imóvel, clientes sem medidores, fazendo uso de ligações clandestinas, os famosos *gatos*, dentre outros. Algumas falhas comuns nesse sistema são a queda de "links" de transmissão devido a eventos da natureza e falha de equipamentos.

O Sistema Elétrico possui diversas proteções automáticas em caso de falha, que juntas formam o sistema de proteção. Sensores, disjuntores, chaves, relés e diversos outros elementos são utilizados para perceber o problema e acionar a comutação, automaticamente, para elementos redundantes e distribuição por outras vias, de forma a evitar a queda de energia. Mas a eficiência dessas ferramentas é muito limitada e não tem caráter preventivo. De fato, certos tipos de falhas dificilmente serão evitados, como é o caso das falhas geradas por eventos naturais como raios, ventos, terremotos, entre outros. O que é importante para o sistema elétrico é a contenção dos danos e a rápida identificação do problema, para que

medidas corretivas possam ser tomadas e a falta de energia não se propague, minimizando, ao máximo, as áreas afetadas.

2.1.1. Órgãos Reguladores e Normativos

O Brasil, devido a sua grande extensão territorial, distribuiu as atividades relacionadas à geração, à distribuição e ao controle do sistema em diversas entidades. Dentre elas, o Operador Nacional do Sistema Elétrico(ONS) e a Agência Nacional de Energia Elétrica (ANEEL) são as mais conhecidas. O Operador Nacional do Sistema Elétrico (ONS) é o órgão responsável pela coordenação e controle da operação das instalações de geração e transmissão de energia elétrica no Sistema Interligado Nacional (SIN), sob a fiscalização e regulação da Agência Nacional de Energia Elétrica (ANEEL).

O ONS desenvolve estudos e ações para administrar o estoque de energia e garantir que não haja interrupções na energia. É constituído por membros associados e membros participantes, constituídos por empresas de geração, transmissão, distribuição e consumidores livres de grande porte. Também participam importadores e exportadores de energia, além do Ministério de Minas e Energia (MME) (18).

O Ministério de Minas e Energia (MME) é encarregado de formulação, do planejamento e implementação de ações do Governo Federal no âmbito da política energética nacional, enquanto a Agência Nacional de Energia Elétrica (ANEEL) é uma autarquia sobre regime especial, vinculada ao MME, com finalidade de regular a fiscalização a produção, transmissão, distribuição e comercialização de energia elétrica, em conformidade com as políticas e diretrizes do Governo Federal (19). A Figura 6 mostra as instituições do atual modelo brasileiro.

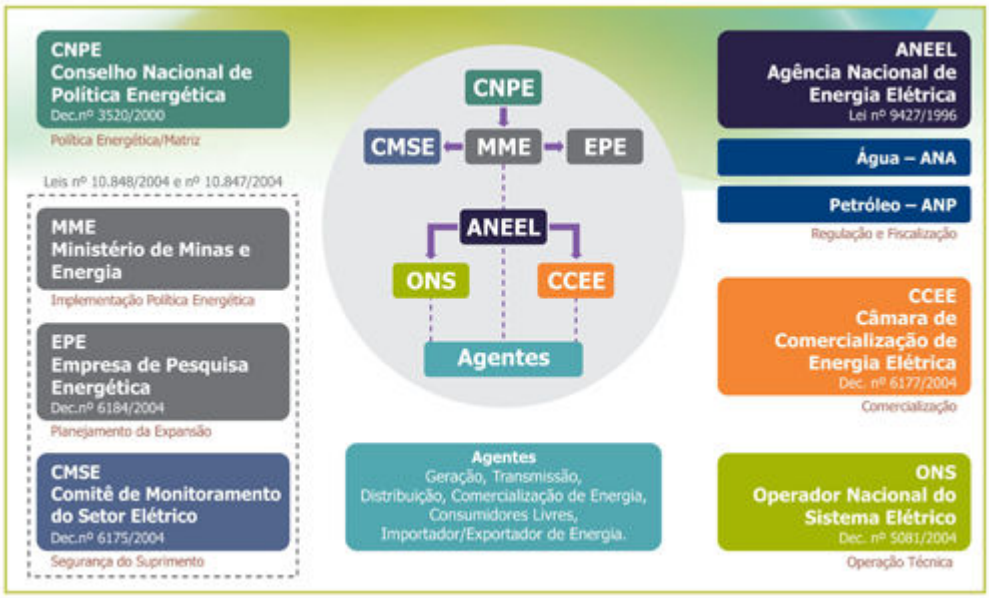


Figura 6 - Principais Instituições do Setor Elétrico no Brasil (18)

Dessa forma, são essas instituições que normatizam a forma como os serviços são providos, assim como os parâmetros de qualidade mínimos que devem ser atendidos pelas concessionárias. Assim, a implantação de novas tecnologias, como os *Smart Meters*, depende diretamente da regulamentação proposta por esses órgãos.

2.1.2. O Sistema de Distribuição

A transmissão e a distribuição do sistema de energia elétrico são responsáveis por levar a energia desde a usina de geração até o consumidor por meio de linhas de transmissão de alta potência, normalmente com corrente alternada. O sistema de transmissão transporta energia entre grandes centros de geração e centros de distribuição, estes já mais perto do consumidor final. A transmissão é feita em níveis altos de tensão para evitar perdas, e esse potencial é reduzido ao se conectar a transmissão com a distribuição.

Mas a tensão que chega aos centros de distribuição ainda é muito alta e é reduzida ao longo do processo de distribuição, até chegar a valores mais baixos como os utilizados nas residências, 110 e 220V. O sistema de distribuição de energia é aquele que se confunde com a própria topografia das cidades, ramificado ao longo de ruas e avenidas para conectar fisicamente o sistema de transmissão, ou

mesmo unidades geradoras de médio e pequeno porte, aos consumidores finais da energia elétrica. A energia distribuída, portanto, é a energia entregue aos consumidores conectados à rede elétrica de uma determinada empresa de distribuição, podendo ser rede de tipo aérea (suportada por postes) ou de tipo subterrânea (com cabos ou fios localizados sob o solo, dentro de dutos subterrâneos).

Assim como ocorre com o sistema de transmissão, a distribuição é também composta por fios condutores, transformadores e equipamentos diversos de medição, controle e proteção das redes elétricas. As redes de distribuição são compostas por linhas de alta, média e baixa tensão. As redes de baixa tensão, com tensão elétrica que pode variar entre 110 e 440 V, são aquelas que, também afixadas nos mesmos postes de concreto que sustentam as redes de média tensão, localizam-se a uma altura inferior. As redes de baixa tensão levam energia elétrica até as residências e pequenos comércios/indústrias por meio dos chamados ramais de ligação. Os supermercados, comércios e indústrias de médio porte adquirem energia elétrica diretamente das redes de média tensão, devendo transformá-la internamente para níveis de tensão menores, sob sua responsabilidade. O sistema de distribuição é muito mais extenso e ramificado, pois deve chegar a todos os consumidores (20). Os transformadores fazem a transformação para tensões mais baixas compatíveis com os imóveis da área alimentada por ele.

Os consumidores ainda tem uma percepção muito limitada da energia consumida. São obrigados a acreditar nos valores da fatura, por falta de medidas de aferição. A energia distribuída é contabilizada nos medidores dos imóveis, que em muitos casos está ficando no alto do poste de difícil visualização.

A falta de distribuição de energia, por apagões, por necessidade de manutenção e outras condições quaisquer, tem a reclamação acelerada pelo cliente por telefone ou via SMS para as concessionárias.

2.1.3. SCADA

Imaginando-se a quantidade de medidas que é coletada frequentemente de diversos equipamentos do sistema elétrico, mesmo sem considerar o novo cenário com medidores inteligentes, há necessidade de controle e processamento desse grande volume de dados para a verificação de falhas, fraudes, necessidades de

manutenção e de expansão. Para tanto, utiliza-se o Sistema de Controle, Supervisão e Aquisição de Dados (SCADA), responsável por coletar muitos dados de supervisão de todos os elementos gerenciados do sistema elétrico, indo desde a geração até os consumidores terminais, por processar as medidas recebidas, por dar comandos automáticos, em presença de situações já conhecidas e analisadas e também manuais, a fim de aumentar a eficiência e a disponibilidade do sistema.

O SCADA coleta dados de sensores, nos sistemas tradicionais, e também dos IED e dos *Smart Meters* nas *Smart Grids*. Para tanto, o SCADA possui grandes áreas de armazenamento de dados, painéis de controle, terminais para comunicação homem-máquina, grande capacidade de processamento, proteções contra acessos indesejáveis e rotinas disparadas por sistemas automatizados.

Os sistemas SCADA apresentam uma arquitetura hierárquica e consistem de dispositivos como a unidade terminal mestre (MTU), a interface homem máquina (HMI) e unidades terminais remotas (RTU). Normalmente a unidade terminal mestre é a raiz de todo o sistema, se comunicando com unidades terminais remotas. A RTU é formada por sensores para a aquisição de dados, um componente para realizar a comunicação e por outro responsável por executar os comandos vindos do MTU. A HMI é a interface homem-máquina que permite a interação do operador com o sistema (2).

2.1.4. Principais Pontos Fracos do Sistema Elétrico Tradicional

O modelo tradicional do sistema elétrico se depara com uma demanda concentrada em determinados horários, ou seja, em momentos de pico, sem, contudo dispor de ferramentas que o auxiliem no espalhamento dessa demanda ao longo do dia, que minimizaria a ordem de grandeza dos investimentos. É muito mais custoso ter uma rede dimensionada para horários de pico, com alta demanda, do que com distribuição ao longo do dia. As medições de consumo dos clientes são feitas mensalmente, não permitindo um traçado de perfil horário ou até mesmo diário. As medidas são um acumulado mensal, portanto com muito pouca granularidade para permitir um projeto, por exemplo, de incentivo à utilização de eletrodomésticos em horários fora do pico e em dias de menor consumo. A iluminação pública urbana, com controle muito básico com células fotoelétricas,

não contempla sua regulagem em função de dados mais específicos como a temperatura, o horário do dia, a luminosidade ambiente, dentre outros.

Outra forma de incrementar a oferta de energia, sem promover tantas expansões do sistema centralizado, seria abrir o mercado para novas fontes alternativas autossustentáveis, mais próximas do consumidor final, como uma energia adicional, de emergência, de *backup*, que aumente a disponibilidade desse serviço.

Outro problema dos sistemas atuais é que o cliente, que poderia ser o maior termômetro do serviço que está sendo prestado, não participa da gerência da rede. Ele recebe a energia a ser consumida e uma fatura ao final do mês, nada mais do que isso. O cliente poderia participar mais efetivamente nesse sistema, fornecendo dados mais detalhados do consumo, informações sobre a qualidade observada no serviço prestado, ajudando no traçado do seu perfil de utilização e indicando possíveis problemas de queda parcial e total no provimento do serviço. Comandos remotos de acionamento de eletrodomésticos em horários mais adequados financeiramente poderiam ajudar no espalhamento da demanda e ao mesmo tempo na satisfação do cliente com a economia em sua fatura. A concessionária dispõe de um sistema unidirecional, onde ela sempre é provedora e o cliente sempre consumidor, não permitindo que este, com fontes adicionais em suas residências, participem como provedores e auxiliem no atendimento à demanda sem exigir maiores investimentos do sistema centralizado. O outro aspecto da bidirecionalidade seria a possibilidade da concessionária estar controlando remotamente elementos que hoje tem controles locais e automáticos de pouca eficiência, como a iluminação urbana. Com a colocação de sensores nesses elementos ela seria capaz de tomar providências em tempo real e mais eficientes.

Esses problemas no sistema atual, já detectados e conhecidos, são minimizados com a implantação dos *Smart Grids* que promovem a inserção de sensores e medidores inteligentes, participação dos clientes consumidores, inserção de fontes renováveis e distribuídas, mais próximas dos consumidores, comandos remotos baseados em um conjunto de dados mais detalhados e agora disponíveis com a introdução dos *Smart Meters*.

2.2. *Smart Grid*

A evolução do sistema elétrico traz o conceito de redes inteligentes (*Smart Grids*) como uma forma de integrar tecnologias tradicionais do sistema elétrico com soluções digitais, permitindo um gerenciamento mais eficiente com a introdução de medidores inteligentes (Smart Meters). A arquitetura da *Smart Grid* foi elaborada pelo *National Institute od Standards and Tecnology (NIST)* sob a solicitação do *Department of Energy (DOE)* do governo americano (21).

As *Smart Grids* integram ações de produtores e consumidores e combinam dispositivos inteligentes (Smart Meters) de monitoramento, controle e tecnologia de comunicação. Envolve os clientes no controle de seu consumo, melhora o funcionamento de todo o sistema, pode incorporar novas fontes alternativas através de uma geração distribuída, tendendo a aaumentar a confiabilidade da rede. O consumidor poderá inclusive tornar-se produtor, fornecendo o excedente da energia por ele produzida (22).

Cada edificação (domicílios, fábricas, estabelecimentos comerciais e de ensino, fazendas, clubes) pode não ser apenas um consumidor, mas também um fornecedor de energia para a rede. Isso é facilitado ao se utilizar medidores inteligentes capazes de medir a energia consumida e a energia gerada, e informar esses dados para a concessionária. Assim, a energia passa a fluir bidirecionalmente. Investimentos em redes inteligentes e linhas de transmissão para trazer energia de parques eólicos *offshore* e usinas de energia solar concentrada serão essenciais neste cenário. A formação de polos de microrredes (*microGrid*) de energias renováveis, especialmente em comunidades remotas (23), será uma peça-chave no fornecimento de energia alternativa.

As microrredes podem operar isoladamente como ilhas de distribuição de energia de média ou baixa tensão ou serem conectadas aos grandes sistemas elétricos das Concessionárias. Elas podem ajudar na complementação da energia gerada pela Concessionária, aumentando a disponibilidade do serviço. Por outro lado, elas inserem mais um ponto de segurança e de proteção ao sistema principal (2).

O conceito *microGrid* vai além da fonte autossustentável descentralizada e complementar à centralizada, gerenciada pelas grandes concessionárias. Ela

agrega essas fontes ao sistema central, fornecendo energia quando necessário, de maneira inteligente e não um sistema isolado com uma grande complexidade no seu acionamento.

2.2.1. *Arquitetura Smart Grid*

A arquitetura *Smart Grid* insere inúmeros conceitos, novos elementos e uma rede de telecomunicações, ilustrada na Figura 7. As *Smart Grids* inserem o consumidor além de fontes alternativas que auxiliam na disponibilidade do sistema, onde o elemento principal é o medidor inteligente, o *Smart Meter*.

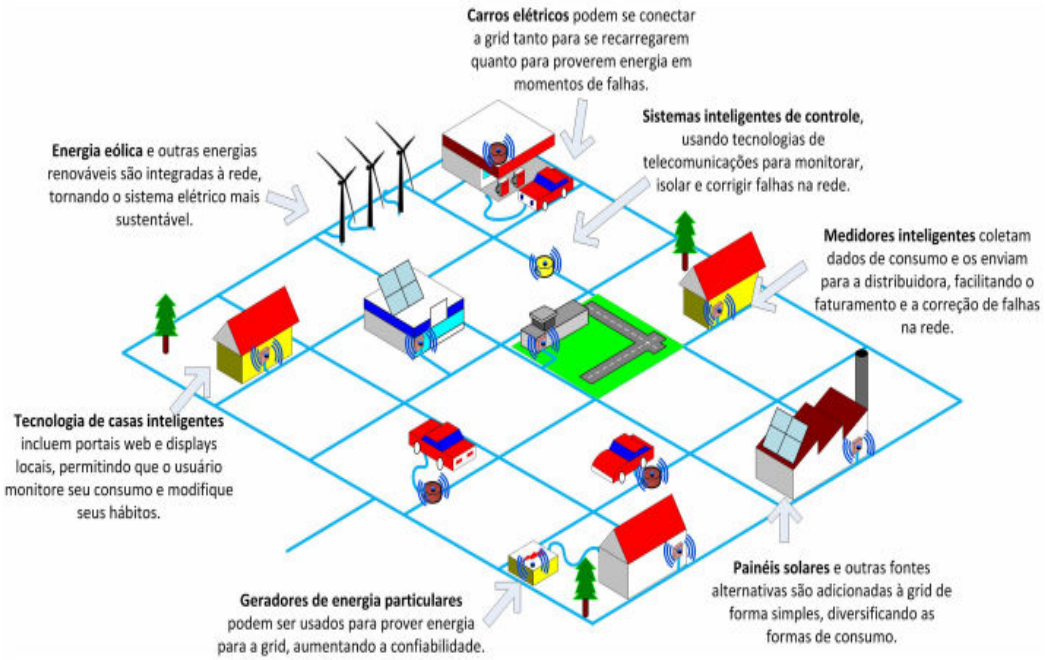


Figura 7 - Visão Geral dos componentes de um Smat *Grid*

Começando pela casa inteligente, ela passa a ter uma interface para gerência e controle dos eletrodomésticos em forma de um painel chamado *In-Home Display*. As casas inteligentes podem até ter uma interface IP para controle remoto de acionamento e desligamento pelo próprio consumidor. O display se interliga aos eletrodomésticos por meio de uma *Home Area Network* (HAN) (21).

Os veículos elétricos aparecem para eliminar uma grande fonte de poluição, inclusive a sonora. Mas também aparecem como mais uma fonte de energia. Suas baterias armazenam energia que pode virar fonte para as redes

inteligentes. Como o veículo é móvel, a distribuição itinerante torna-se uma possibilidade (2). A proliferação de veículos elétricos ajuda na preservação do meio ambiente e aparece como mais uma forma de armazenamento e provimento de energia, tornando-se mais um possível fator nos cálculos dos horários de pico de demanda.

2.2.2. Medidores Inteligentes (SMART METERS)

O sistema de *Smart Metering* é um dos pontos principais para a criação das *Smart Grids*. Os medidores inteligentes garantem transparência das medições para os clientes, que passam a controlar seus consumos de forma mais granular. Esse assunto será detalhado em capítulo específico mais adiante.

2.2.3. Rede WAN

As redes de telecomunicações dão suporte às *Smart Grids*, considerando a distância entre os elementos gerenciados, o grande volume de dados e a necessidade de baixos tempos de resposta para algumas aplicações. Para tanto, as redes precisam ser confiáveis, prover qualidade de serviço, prover altas taxas de transmissão e garantir tempos de resposta críticos. Ainda não se tem uma indicação do melhor modelo para as redes WAN das *Smart Grids*, mais alguns têm sido estudados, como o GSM (*Global System for Mobile*), o 3G, agora o 4G (2).

O padrão IEEE1815, também conhecido como *Distributed Network Protocol* (DNP3) (2) , define um conjunto de protocolos de comunicação e foi desenvolvido para a comunicação entre equipamentos de requisição de dados e controle, sendo muito utilizado em sistemas SCADA. O método é determinístico e com transferência confiável em meio físico com banda estreita. Vem sendo muito utilizado pelas companhias elétricas para a comunicação entre o centro de controle e os dispositivos elétricos inteligentes (IED) de uma subestação. A norma permite que o DNP3 se conecte a uma rede corporativa e usufrua de protocolos suportados na Internet e tenha uma comunicação confiável fim-a-fim com TCP.

2.2.4. Redes HAN e LAN

Home Area Network (HAN) é a rede no qual os eletrodomésticos e equipamentos do consumidor estão conectados.A LAN é a rede que interliga medidores, até mesmo de imóveis diferentes

As redes domiciliares HAN podem ser dos tipos Wi-Max, EPON (Ethernet Passive Optical Network), Bluetooth, ZigBee, IEEE 802.11/WiFi, Homeplug e as redes específicas de subestações de energia elétrica, tais como DNP3 e IEEE 61850 (2).

2.2.5. Vulnerabilidade dos Smart Grids

A ampla utilização das redes de comunicação e a interação direta do cliente com o sistema de controle traz uma vulnerabilidade que antes não existia no Sistema Elétrico. A abertura do acesso para consumidores, a utilização da Internet e de outras redes de dados interconectando elementos do "*core*" do sistema, os elementos periféricos e os centros de controle permitem que pessoas mal intencionadas tentem burlar o sistema. Com as *Smart Grids,* as fraudes podem ir muito além dos famosos "gatos".

Com essa nova tecnologia, os *hackers,* que são indivíduos mal intencionados e normalmente dotados de habilidade de invadir e burlar sistemas digitais, podem utilizar os *Smart Meters* como forma de acessar o controle da rede elétrica. Um tipo semelhante de usuário comum no sistema elétrico atual é o de pessoas que adulteram o relógio medidor residencial, de forma a diminuir seu consumo e consequentemente sua conta. Outras variáveis incluem o roubo de energia de outras residências ou do poste, sem geração de registro e conta para o cliente mal intencionado.

Com isso, sistemas de autenticação de usuário, zonas desmilitarizadas, firewalls controlando acessos, criptografia (2) e outros mecanismos, passam a fazer parte da implementação dessas redes, sem os quais o sistema fica muito desprotegido e sujeito a informações fraudulentas, ataques às redes, monitoração de dados por pessoas sem autorização etc.. Alguns cuidados se tornam, então, imprescindíveis. Assim, torna-se possível aferir a real identidade de alguém que queira acessar o sistema, garantir a integridade e a privacidade dos dados coletados, e realizar a auditoria dos dados, conferindo todas as ações históricas

para a verificação de má conduta na utilização do sistema (2).

Outro problema encontrado nos *smart grids* é a grande quantidade de dados que é gerada, nem sempre dados úteis, pois perturbações na rede de telecomunicações e nos medidores pode causar efeitos transitórios e temporários dando falsa impressão de problema e retornando rapidamente à normalidade. Ao mesmo tempo dados falsos podem ser inseridos por *hackers* e também mascararem problemas na rede. Todos esses dados falsos podem gerar alarmes indevidamente se não forem bem observados e filtrados sem se confundirem com dados úteis. Essa ideia foi um dos motivadores para esse trabalho e foi bem abordado. A quantidade de dados a serem transferidos não constitui problema, pois os meios de transmissão estão com as bandas cada vez de mais alta velocidade, mas a utilidade do dado é que deve ser verificada.

2.2.6. Clientes Produtores

Apesar de não fazer parte do escopo desse trabalho, é importante ressaltar que podem existir outros produtores de energia além da concessionária de energia oficial.

O Grupo de Trabalho de Redes Elétricas Inteligentes do Ministério de Minas e energia produziu um relatório (24) que, além de abordar os elementos de um *Smart Meter*, introduz a ideia de *Net Metering* que consiste na medição do fluxo de energia em uma unidade consumidora dotada de pequena geração, por meio de medidores bidirecionais de fluxo de energia. Dessa forma, registra-se o valor líquido da energia, ou seja, se a geração for maior que a carga, o consumidor recebe um crédito em energia ou em dinheiro na próxima fatura (tipicamente ao valor da tarifa do cativo). Outros tipos de acordos entre a Concessionária e o consumidor final podem ser realizados, como por exemplo, redimensionar as linhas de acordo com a demanda. Com base nas informações que são enviadas pelos medidores dos consumidores e da infraestrutura, esse trabalho propõe que é possível correlacionar medidas obtidas em diversos pontos da rede para detectar rapidamente problemas causados por falhas ou por ataques.

Seguem algumas leis importantes sobre o assunto:

Lei 9074 de 7 de julho de 1995 (25) faculta aos consumidores que pretendam utilizar, em suas unidades industriais, energia produzida por geração própria, em regime de autoprodução ou produção independente, a redução da

demanda e da energia contratada ou a substituição dos contratos de fornecimento por contratos de uso dos sistemas elétricos, mediante notificação à concessionária de distribuição ou geração, com antecedência mínima de 180 (cento e oitenta) dias. (Incluído pela Lei nº 10.848, de 2004)".

Lei nº 9.074, de 07 de julho de 1995 (25) "Art. 14. As linhas de transmissão de interesse restrito aos aproveitamentos de produção independente poderão ser concedidas ou autorizadas, simultânea ou complementarmente, aos respectivos contratos de uso do bem público."

Decreto nº 5.163, de 30 de julho de 2004 (25) "Art. 74. Os autoprodutores e produtores independentes não estão sujeitos ao pagamento das quotas da Conta de Desenvolvimento Energético - CDE, tanto na produção quanto no consumo, exclusivamente com relação à parcela de energia elétrica destinada a consumo próprio."

Atualmente, dos consumidores livres e autoprodutores conectados na Rede Básica são cobrados os encargos setoriais Conta de Consumo de Combustíveis (CCC) e Conta de Desenvolvimento Energético (CDE), cujos recursos são administrados e movimentados pela Eletrobrás.19

Vale ressaltar que a CCC dos sistemas isolados e a CDE são cobradas apenas sobre a energia consumida oriunda de comercialização, ou seja, a energia de autoprodução ou o consumo próprio de produtores independentes estão sujeitos apenas ao pagamento da CCC do sistema interligado onde suas cargas se conectam.

Lei nº 9.074, de 07 de julho de 1995 (25) "Art. 15. Respeitados os contratos de fornecimento vigentes, a prorrogação das atuais e as novas concessões serão feitas sem exclusividade de fornecimento de energia elétrica a consumidores com carga igual ou maior que 10.000 kW, atendidos em tensão igual ou superior a 69 kV, que podem optar por contratar seu fornecimento, no todo ou em parte, com produtor independente de energia elétrica.

Decreto nº 5.163, de 30 de julho de 2004 (25) "Art. 74. Os autoprodutores e produtores independentes não estão sujeitos ao pagamento das quotas da Conta de Desenvolvimento Energético - CDE, tanto na produção quanto no consumo, exclusivamente com relação à parcela de energia elétrica destinada a consumo próprio."

Um Produtor de Energia Independente pode vender parte ou a totalidade da

sua produção para clientes por sua própria conta e risco. O autogerador pode vender ou negociar qualquer energia excedente, a qual é incapaz de consumir, mediante autorização específica da ANEEL. Aos produtores de energia independentes e autogeradores não são concedidos os direitos de monopólio e não estão sujeitos a controles de preços, com exceção de casos específicos.

Capítulo 3

Smart Meter

Os medidores inteligentes (Smart Meters) são elementos imprescindíveis À evolução do sistema elétrico e a arquitetura de Smart Grid. Relacionado ao lado do consumidor, os medidores inteligentes permitiram a criação de *Smart Appliances,* que são aplicações inteligentes capazes de controlar o uso de certos equipamentos, também dotados de processador e placa de rede, no imóvel. Com isso, as *Smart appliances* conseguem informar à *Smart Grid* as demandas dos equipamentos e, ainda, controlar o uso dos mesmos de acordo com as variações tarifárias. Os *Smart Meters* também auxiliam às concessionárias, no sentido de obter dados de consumo acumulados, qualidade, temperatura e outros indicadores, remotamente e em frequência maior do que a atual.

Devido à grande quantidade de clientes que precisam enviar dados de consumo e monitoração da rede, gerados pelos *Smart Meters*, os sistemas de coleta utilizam nós concentradores intermediários. Esses nós coletam informações de uma área, agregam dados e os enviam ao sistema de processamento central. Com isso, se consegue uma maior escalabilidade para o sistema.

Transformadores e demais elementos do setor elétrico não tratam dados, somente medem e apresentam dados absolutos acumulados. Não fazem crítica e correlação entre as informações geradas por ele e os demais elementos. Os nós concentradores podem fazer uma primeira crítica e também aglutinações de dados antes de transferir as.medidas dos diversos elementos elétricos a ele associados, ao sistema SCADA,excluindo mais perto da fonte, dados ineficientes e agilizando o tratamento pelo sistema central. Nós concentradores também podem otimizar a rede de telecomunicações, de modo a se ter uma rede de dados de vários níveis, agregando os nós de última milha, depois alguns níveis de nós intermediários e nós o core onde se encontra o sistema central de processamento (SCADA). A fontes alternativas podem estar mais perto do consumidor final ou ligadas diretamente aos nós intermediários.

A comunicação dos *Smart Meters* com os concentradores pode ser feita utilizando diferentes tecnologias. De fato, não existe nenhuma normatização amplamente adotada que aponte uma única tecnologia ou um único protocolo de comunição. A 2 mostra uma comparação entre tecnologias para comunicação em *Smart Grids*. A escolha deve considerar o alcance necessário, as aplicações envolvidas, o custo e os pesos dados a cada um desses fatores.

Tabela 2 - Potenciais Tecnologias de Comunicação para *Smart Grids* (17)

Tecnologia	Espectro	Banda	Alcance	Aplicações	Limitações
GSM, GPRS	900-1800 MHz	Até 170 kbps	1-10 km	AMI, resposta a demanda (DR), HAN	Baixa largura de banda
4G	2.5 GHz	Até 200 Mbps	1-50 km	AMI, resposta a demanda (DR), HAN	Alto custo regulatório de espectro
Wi-Fi IEEE 802.11	2.4-5.8 GHz	Até 155 Mbps	1-300 m	AMI, HAN	Curto Alcance
WiMAX	2.5 GHz, 3.5 GHz, 5.8 GHz	Até 75 Mbps	1-5 km 1-5 km 10-50 km	AMI, resposta a demanda (DR)	Poucas implementações
PLC	3-500 kHz 1.8-30 MHz	1-3 Mbps Até 200 Mbps	1-3 km	AMI, Detecção de fraudes	Ruídos em redes
ZigBee	2.4 GHz 868-915 MHz	Até 250 kbps	30-90 m	AMI, HAN	Curto alcance e baixa largura de banda
Bluetooth	2.4-2.4835 MHz	Até 721 kbps	1-10 m	HAN	Curto alcance e alto consumo de energia

Não é viável economicamente que os meios de transmissão entre os *Smart Meters*, pulverizados pelo país, e o sistema centralizado de coleta e tratamento desses dados (SCADA) sejam diretos entre esses pontos. Faz-se necessária a introdução de elementos coletores que vão agregando esses links, diminuindo a complexidade da manutenção e podendo inclusive aplicar filtros e realizar algumas agregações também nos dados a serem transmitidos. A infraestrutura de medição avançada (Advanced Metering Infrastructure - AMI) implementa essa medição com mais recursos do que a tradicional. A AMI é bidirecional, coletando medidas, mas também podendo receber comandos de acionamento ou desligamento do fornecimento de energia. Assim, o meio de transmissão se torna um ponto de atenção. Essa atenção se deve a necessidade de se escolher a tecnologia mais adequada, em função de diversos fatores como volume de dados, distância entre os nós e condições geográficas e ambientais onde o sensor está instalado. O custo também é um fator preponderante.

Para a implementação da HAN não há necessidade nem de grande alcance, nem de muita banda, pois trafegam apenas as medidas de um cliente em áreas de

curto alcance. Seguindo a Tabela 2, os protocolos ZigBee,Wi-Fi e Bluetooth seriam adequados a esse segmento da rede. Por outro lado para perfazer longas distâncias, poderia se utilizar a própria rede elétrica (PLC) apesar de absorver ruído, ou optar em utilizar outra forma de acesso como 3G, 4G, pensando em rede móvel, ou uma rede metro-ethernet.

Esse trabalho não aborda o estudo mais detalhado de cada protocolo, mas realça a importância nessa escolha para a construção de uma rede de telecomunicações apropriada.

3.1. Smart Meters e Displays Residenciais de Mercado

Para entender com mais detalhes como funcionam os serviços oferecidos pelos *Smart Meters*, são descritos alguns exemplos de equipamentos de mercado, apresentando suas características básicas, como por exemplo, dados que são capazes de medir e protocolo de transmissão. Alguns deles medem decréscimo de tensão (Sag) e também o seu crescimento (Swell), intervalo de tempo sem energia (DIC) e quantidade de interrupções no período de observação (FIC). Para ilustrar seguem alguns equipamentos de mercado e algumas de suas características.

a) MD-3400: Medidor Trifásico da Ecil Energia (26)

O MD-3400 é um medidor de energia trifásico utilizado para medições residenciais e comerciais. Além de realizar medição de energia ativa (medida em kWh e que faz, por exemplo, os motores girarem) e reativa (medida em kVArh, utilizada para criar o fluxo magnético nas bobinas dos equipamentos, para que os eixos dos motores possam girar), esse medidor observa a corrente de neutro e possui relé de corte trifásico. A sua comunicação pode ser dar por meio de uma interface RS485 isolada, via *mesh*, utilizando uma frequência de 2,4GHz, ou por porta ótica de comunicação. Com uma antena RF interna, esse medidor pode funcionar também para a leitura de outros equipamentos via rede, tais como medidores de água e gás.

b) MD-3500: Medidor Trifásico e Indireto da Ecil Energia

O MD-3500 é um medidor de energia trifásico e indireto, utilizado para medições e monitoramento de tensão secundária de transformadores de distribuição (26). Esse equipamento faz medição de energia ativa e reativa, assim

como a medição de DIC e FIC e o monitoramento de temperatura através de sensor externo Pt100. A comunicação pode ser feita por porta óptica ou *mesh*, na frequência de 2,4GHZ.

c) DIMET-P da Discar *Telecom&Energy*

Esse equipamento mede o consumo e verifica a qualidade do serviço, armazenando a média das medidas a cada 15 minutos, com medidas de tensão, corrente, frequência e energia ativa reativa e aparente. Esse medidor pode receber comandos com controle de limites de consumo de energia e tensões mínimas e máximas, se comunicando via *Power Line Communications* (PLC). Ele também registra a abertura do medidor e a desconexão do medidor, armazena tabelas de tarifas e suporta energia pré-paga e pós-paga. Pode ser colocado um elemento concentrador que se comunicará com o elemento de processamento final via GSM/GPRS ou via ADSL usando uma porta ethernet. O *Smart Meter* utiliza criptografia com seu concentrador e este último com o sistema SCADA, fazendo uso de processo de autenticação.

3.2. Troca de Mensagens entre *Smart Meters* e SCADA

Como esse trabalho visa analisar dados obtidos dos medidores dos imóveis de uma determinada área e a sua recepção em um concentrador, segue um exemplo para ilustrar os tipos de mensagens passíveis de troca.

As mensagens geradas pelos medidores inteligentes dos imóveis têm características diferentes das geradas pelo sistema SCADA para os medidores inteligentes. A Figura 8 mostra os tipos de informações que são trocadas entre os elementos do *Smat Grid* . A Tabela 3 apresenta mais alguns detalhes de cada tipo de informação.

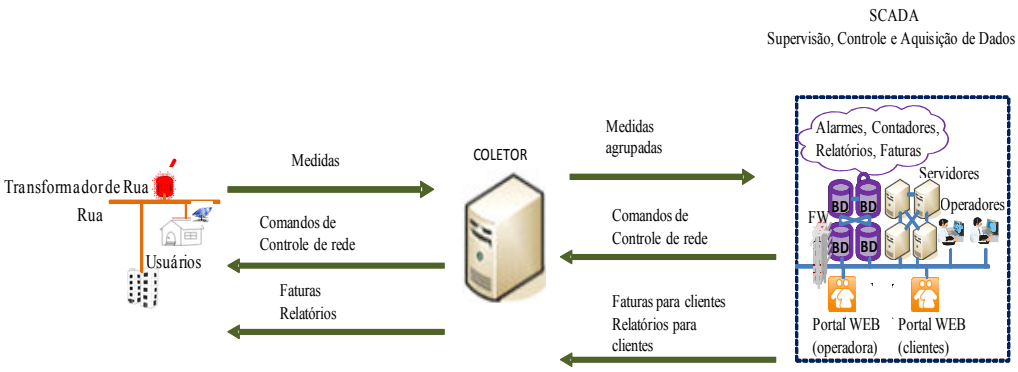


Figura 8 - Fluxo de Informações entre elementos do *Smart Grid*

Pode-se verificar que as mensagens podem ser curtas ou longas, com ou sem criticidade, dependendo da ação vinculada àquele dado/comando. Dados que podem ser coletados novamente mais tarde e dados que se perdidos podem deixar de apontar problemas graves ou deixar de acionar ações de contingência, trazendo graves consequências para o sistema.

Tabela 3 - Características das mensagens trocadas entre os elementos do *Smart Grid*

Tipo de Mensagem	Direção do Fluxo	Características
Medidas	SM-->Coletor	Poucas mensagens e curtas Alta frequência de atualização Perda de informação não crítica, passível de reenvio em tempo real Dados mais vulneráveis aos ataques
Medidas agrupadas	Coletor --> SCADA	Muitas mensagens curtas Alta frequência de atualização Perda de informação não crítica, passível de reenvio em tempo real Dados mais vulneráveis aos ataques
Comandos de controle de Rede	SCADA-->Coletor-->SM	Mensagens curtas Baixa frequência Perda de informação crítica, com criticidade na necessidade de reenvio
Faturas Relatórios	SCADA--> SM	Mensagens longas Baixa frequência Perda de informação não crítica, passível de reenvio.

Os consumidores de energia elétrica pagam por meio da conta recebida da

sua empresa distribuidora de energia elétrica, um valor correspondente a quantidade de energia elétrica consumida, no mês anterior, estabelecida em kWh (quilowatt-hora) multiplicada por um valor unitário, denominado tarifa, medida em R$/kWh (reais por quilowatt-hora), que corresponde ao preço de um quilowatt consumido em uma hora. As empresas de energia elétrica prestam este serviço na sua área de concessão, ou seja, na área em que lhe foi dado autorização para prestar o serviço público de distribuição de energia elétrica. A Agência Nacional de Energia Elétrica – ANEEL é responsável por estabelecer as tarifas. (6)

3.3. Identificação das Mensagens

Os medidores inteligentes devem conter, no mínimo, as informações a seguir, para a identificação das suas mensagens:

- Número de identificação único do medidor inteligente e/ou número de do imóvel
- Tipo de mensagem: contador ou alarme.
- Data e hora
- Conteúdo da Mensagem

O conteúdo da Mensagem, dentre outros, pode ser:

- contador de consumo, qualidade e outras medições;
- alarme de má qualidade do serviço prestado ou falta de energia;
- alarme de violação ou tentativa de violação do *Smart Meter*.
- Gráficos.

Capítulo 4

Estado da Arte no Uso de Modelos de Confiança

As redes elétricas estão sujeitas a diversos tipos de falha que precisam ser identificadas e tratadas, a fim de reduzir tempos de indisponibilidade de serviço e de reduzir o tamanho das áreas atingidas pelos problemas. Essas falhas incluem eventos naturais, erros de configuração, falhas em equipamentos, entre outros. Existem ainda problemas de outra natureza, como usuários que fraudam a medição do consumo para reduzir seus custos. De fato, as fraudes na medição do consumo têm consequências que vão além do prejuízo direto causado a concessionária, ou seja, não receber pela energia provida. Essas fraudes causam a dificuldade de se prever a demanda e a detecção de outros problemas na rede.

A inserção de uma nova tecnologia, onde uma rede de telecomunicações passa a interligar elementos de rede, Backoffice da empresa concessionária e principalmente clientes, traz a preocupação com segurança, tanto do próprio sistema quanto da informação que nela trafega. A inserção pulverizada e em grande quantidade de medidores nos imóveis, faz aparecer um volume de dados a serem entendidos, tratados, guardados e protegidos contra o mau uso, pois neles se encontra o mapeamento das rotinas das pessoas. Esses dados podem ser adulterados na fonte, onde o usuário viola o medidor para registrar um consumo menor do que o efetivo ou ainda por hackers, que podem realizar ataques contra qualquer elemento da rede de comunicação e controle a partir de um *Smart Meter*. Mesmo com esse grande número de informações, é preciso identificar o que é dado bom e o que deve ser descartado. O uso de técnicas de confiança vem para permitir essa identificação, não permitindo que um dado espúrio venha a comprometer a análise de todo um sistema.

Devido ao grande volume de informações, fica mais difícil ainda diferenciar problemas na rede, fraudes e falso-positivos na detecção remota dos problemas. Enfim, encontrar a causa raiz.

Por essas razões, esse trabalho propõe a utilização de metodologias de confiança para o auxílio na detecção de problemas na rede, tanto para a

interpretação dos problemas quanto para o ajuste dos intervalos de coleta de dados.

A proposta é analisar tendências, reincidência de dados suspeitos para finalmente apontar áreas e clientes a serem verificados pela equipe de campo da concessionária. E não disparar medidas mais complexas de averiguação na primeira percepção de dados com comportamento não esperado.

4.1. Modelos de Confiança

Confiança e reputação têm sido reconhecidos como uma questão-chave nas áreas de computação *peer-to-peer*, serviços Web, *e-business*, *e-commerce* e ambientes de computação pervasiva (presente em todos os momentos da vida das pessoas) etc. A computação móvel consiste em sistemas computacionais distribuídos em diferentes dispositivos que se comunicam entre si por meio de uma rede de comunicação sem fio. Por outro lado, a computação pervasiva implica que o computador está embarcado no ambiente de forma invisível para o usuário, tendo a capacidade de obter informações sobre o ambiente e utilizá-la para controlar, configurar, ajustar as aplicações para melhor se adequar às características do ambiente. Para isso os ambientes ficam repletos de sensores e serviços computacionais (27).

Como a computação baseada em agentes tem sido defendida como o modelo de computação natural para tais sistemas, pesquisas sobre confiança e reputação em ciência da computação são geralmente desenvolvidas em termos de sistemas multiagentes (28). E como não há consenso sobre a definição de confiança e modelos a serem utilizados, muita literatura tem sido gerada querendo fixar conceitos e metodologias de determinação de níveis de confiança.

Quando se estuda técnicas de confiança, várias perguntas se fazem presentes, como quando um agente deve confiar no outro e por quais motivações; quando os agentes devem avaliar a confiabilidade dos outros e que técnicas utilizar; qual deve ser a atitude de um agente depois de obter a confiabilidade dos outros; entre outras. Respostas diferentes para essas perguntas trazem diferentes interpretações, noções, técnicas e modelos de confiança e reputação. Principalmente, as respostas para a primeira pergunta dão origem aos significados concretos de confiança. As respostas para as demais perguntas ajudam a definir os modelos de confiança e reputação. Assim, essas respostas formam uma estrutura para investigar as noções,

técnicas e modelos de confiança e reputação (29).

A confiança é determinada pelo posicionamento de algo dentro de um comportamento esperado. No caso dos dados referentes ao sistema elétrico, espera-se um consumo dentro de um perfil, espera-se uma avaliação de qualidade semelhante entre os consumidores, mensagens que cheguem em padrões pré-definidos. Para isso, dados históricos, comparações com elementos vizinhos, comparações com perfil, entre outros, podem se tornar as referências para determinação da confiança nesse dado.

Um sistema de confiança irá coletar e combinar opiniões dos usuários sobre a confiabilidade de uma entidade e calcular os valores de reputação de acordo com seu modelo de confiança. O modelo de confiança é composto por três blocos: representação que define a métrica a ser utilizada, sua normalização, que coloca as medidas geradas pela aplicação das métricas em uma mesma base para comparações entre elas e agregação, em que se agrupam as diferentes medidas normalizadas em visões globais ou personalizadas de reputação (30) (31).

São muitos os trabalhos relacionados ao conceito de confiança e reputação, englobando média móvel, análise dos dados históricos, análise por perfil e análise da vizinhança, que serviram como base desse mecanismo proposto.

Sabater e Sierra (32) avaliaram modelos de confiança e reputação caracterizados pela confiança a partir de crenças, do que se espera do outro e de informações obtidas anteriormente. Observaram também os tipos de dados: observação direta e pessoal, o famoso “boca a boca”, ou seja, informações de terceiros, chamadas testemunhas, as informações sociológicas, ou seja, da base de conhecimento a partir das relações sociais entre os agentes e o papel que eles estão desempenhando no momento na sociedade. Eles afirmam que o modelo mais subjetivo só deve ser aplicado a grupos pequenos e com relativo grau de intimidade e que são admitidas interpretações diferentes da mesma situação. Para grupos grandes o modelo objetivo é o mais aplicável. Acreditam que está na hora de explorar combinações desses métodos mais subjetivos com os mais teóricos, envolvendo sociólogos e psicólogos com a visão mais humana do que a imposta nos atuais modelos que são elaborados por economistas e cientistas da computação.

Sloman et.al (28) abordam que os sistemas de confiança atuais se preocupam com a determinação da confiança para a implementação de acesso ou

autenticação, mas não se preocupam com a necessidade das entidades estarem constantemente aprendendo com sua experiência e determinando ajustes nesses níveis de confiança. No caso, por exemplo, da Internet, a autorização pode ser vista como o resultado do refinamento de uma relação de confiança. Uma pessoa é autorizada, por exemplo, a realizar a instalação de um software, porque ela foi bem sucedida em outras oportunidades fazendo essa mesma função. Com a autorização para essa atividade vem o processo de autenticação que é a verificação da identidade de uma entidade, que pode ser por atribuição de uma senha particular. Nesse caso o processo de autorização é que deve ser sempre revisto e a autenticação é somente uma consequência. A autorização não tem nada a ver com a identidade, mas sim com o nível de confiança naquela entidade. Eles classificam a relação de confiança em cinco categorias conforme a seguir:

- O acesso aos recursos do outorgante, onde ele confia um administrador para usar os recursos que ele possui ou controla, o que poderia ser um ambiente de execução de software ou um serviço de aplicação.
- A prestação de serviço onde o outorgante confia no administrador para prestar um serviço que não envolve o acesso aos recursos do outorgante, o que às vezes é impossível, como serviços web que fazem download de *applets* e *cookies*, e por isso precisam de acesso a recursos de propriedade do outorgante.
- Certificação de confiança baseada na certificação por um terceiro, de modo que a confiança seria baseada em critérios estabelecidos.
- Delegação, onde o outorgante confia um administrador para tomar decisões em seu nome, no que diz respeito a um recurso ou serviço que o outorgante possui ou controla.
- Infraestrutura, que se refere à infraestrutura de base que o outorgante deve confiar como, por exemplo, estação de trabalho, rede local e servidores locais.

Nesse modelo, o gerenciamento de confiança é a coleta das informações necessárias para tomar uma decisão de relação de confiança bem como monitorar e reavaliar sempre essa relação (28).

Mui et al. (33) definiram tipos de reputação baseados em contextualização, ou seja, inerente a um contexto. Por exemplo, não é aconselhável

atribuir um nível de reputação a um especialista em biologia quanto a forma dele realizar contas matemáticas complexas e vice-versa. Outro tipo seria por personalização, ou seja, a reputação de uma entidade é válida para o grupo afim, de modo que a reputação de uma cozinheira é importante no meio de pessoas que trabalham em restaurantes e bares, mas não em laboratórios químicos, por exemplo. Os autores colocam também que a reputação pode ser individual de uma entidade ou de um grupo. Por exemplo, o grupo *Amazon* tem uma boa reputação e com isso seus membros podem pertencer a vários grupos, carregando ou não o nível de reputação do todo. A reputação pode ser medida por observações feitas diretamente ou depender de inferências a partir de informações de terceiros ou da reputação do grupo ao qual pertence.

Mui (34) aborda a importância da informação social na escolha para uma possível parceria. Ela coloca que os membros de uma rede social podem refinar seu comportamento com base na interação com outras pessoas, nas informações adquiridas desse relacionamento, como por exemplo, confiança e reputação, objetos de seu estudo, a partir de interesses e estratégias pessoais.

Marti e Molina (35) comentam em seus trabalho o grande uso de sistemas de reputação nos últimos anos. O objetivo do trabalho deles foi organizar ideias e trabalhar no intuito de facilitar esse tipo de projeto. Abordaram os componentes de um sistema de reputação. O primeiro componente é responsável pela coleta de dados do comportamento histórico dos nós. O segundo pontua, atribui pesos e o terceiro constrói uma classificação para aqueles nós, que podem ser aceitos ou punidos. Artz e Gil (36) descrevem sobre a confiança baseada na reputação, ou seja, nas interações passadas e de desempenho. Por exemplo, ter a credencial de um diploma universitário significa que seu titular tenha sido reconhecido pela universidade emissora como tendo certo nível de educação. A reputação é uma avaliação com base no histórico de interações com esse indivíduo ou observações de uma entidade sobre ele, seja diretamente com o avaliador (experiência pessoal) ou como relatado por outros.

Chong et.al (37) dizem que pessoas dão feedback sobre o elemento em avaliação, que pode ser uma pessoa individualmente, um grupo, uma marca, um serviço, um software, um hardware ou qualquer outro que se deseja investigar e enquadrar em algum nível de confiança. O e-Bay e o "site" http://www.reclameaqui.com.br, são exemplos de aplicações que coletam o

feedback de usuários sobre transações passadas com uma entidade e a classifica em níveis de confiança pré-determinados. O perigo da coleta de feedback de pessoas é que algumas, de forma fraudulenta, podem promover avaliações boas ou ruins que não expressam a realidade, a fim de prejudicar uma entidade idônea ou avaliam muito bem querendo alavancar seus serviços em proveito próprio. O meio eletrônico e a Internet beneficiam as informações mal intencionadas, possibilitando a manipulação dos resultados de confiança atribuídos às entidades.

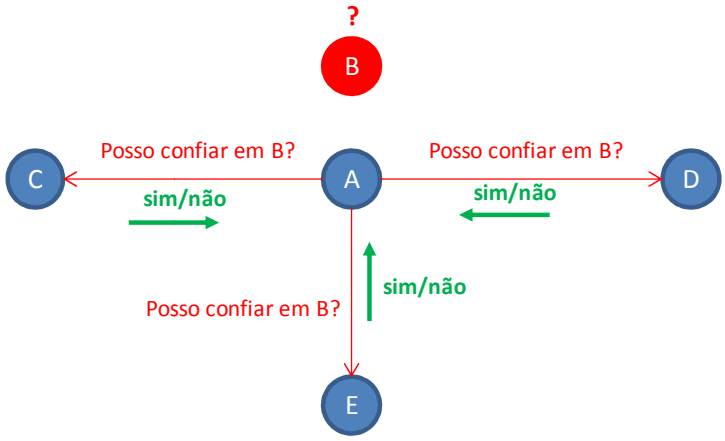
Velloso et al. (38) propõe um trabalho de análise de modelos de confiança para redes *ad-hoc*, a partir da coleta de informações locais e dos nós vizinhos diretos, introduzindo a maturidade da relação entre nós como um grande peso a considerar. Relacionamentos de mais longa duração recebem um grau maior de confiabilidade. O modelo de Fernandes et.al (39) propõe um mecanismo de exclusão de nós não cooperativos inspirado em um tribunal de júri, em que os nós possuem vários papéis: testemunhas e jurados. As testemunhas avaliam e informam ao júri que julga a partir das evidências e decide sobre a exclusão do nó na condição de réu.

4.2. Aplicações de Modelos de Confiança

Seguem algumas aplicações fazendo uso de modelos de confiança em diversos cenários relacionados às redes de computadores.

Sun et al. (40) propõem uma metodologia para a determinação da confiança de um nó, onde ele verifica as suas próprias experiências e também a percepção dos vizinhos sobre esse novo elemento, porém mantendo as reavaliações constantes. A partir dessa ideia, os autores propõem uma metodologia de avaliação de confiança em redes *ad hoc*. Quando um nó quer estabelecer uma rota para um destino, são buscadas todas as possíveis rotas e aquela que for avaliada como a de maior confiança é escolhida para realizar o encaminhamento. Após utilização da rota escolhida, a origem realimenta a tabela de confiança com a própria observação de qualidade na última transmissão. A primeira etapa é obter recomendações de confiança. Quando um nó A quer se comunicar com um nó B desconhecido, ele escolhe alguns nós da sua tabela de avaliação de confiança, para os quais ele vai questionar sobre a idoneidade de B com um comando TRR (*Trust Recommendation Request Message*). O nó A envia esse pedido tanto para nós

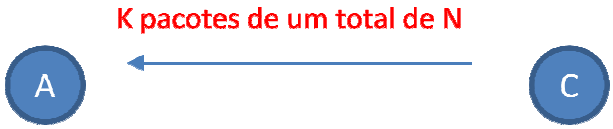
confiáveis quanto também para alguns não confiáveis a fim de não tornar pública sua lista de bons relacionamentos. Essa lista pode também contemplar os próprios nós em avaliação, nesse caso o nó B. Essa mensagem tem um tempo de vida, pois A precisa se decidir rapidamente sobre o estabelecimento ou não da relação com B. Os nós questionados respondem a A, se quiserem, pois não são obrigados a revelar suas relações de confiança. Os nós respondem a solicitação com suas próprias informações ou após consulta aos seus vizinhos. Essas mensagens trazem um grande overhead ao sistema.



A segunda etapa é gerenciar e atualizar as relações de confiança. Nesse estudo, a relação de confiança entre nós já conhecidos, como por exemplo, A com C, é estabelecida baseada na informação de C ter ou não enviado os pacotes para A, ou seja, {A:C, envio de pacotes}.Supondo que C enviou k pacotes para A de : , = + + (1 calcula o relacionamento de confiança (P) de A com C,:

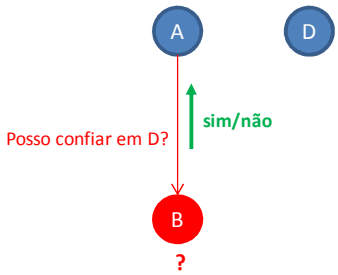
— **(1)**

A determinação de valores de k e N é



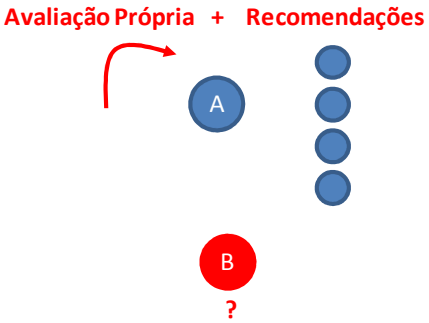
Voltando ao nó B, cuja confiança ainda é desconhecida por A, além de ser

analisado, B também informa relação de confiança com um outro nó D, a pedido de A e este registra como D sendo confiável por uma informação de propagação realizada por terceiros, $T^{r}_{A\text{-}D}$. Quando, então, A realiza uma transmissão de pacotes para D, A verifica, efetivamente, quantos pacotes foram transmitidos e calcula sua própria avaliação de D, $T^{a}_{A\text{-}D}$. A partir daí, o nó A compara a $TACa - TACr| \leq \alpha$ (**2**. Se a diferença estiver maior que um determinado limite α a ser estipulado pelo administrador da rede como erro tolerável, A vai entender que B fez uma má recomendação e sua relação de confiança vai ser deteriorada, caso fique dentro do erro tolerável, A vai julgar ter sido bem informado por B e o verá como uma indicação de boa fonte e ajudará na indicação de B com uma boa escola de encaminhamento de novos pacote . As recomendações de nós terceiros também irão nortear a análise de A sobre o nó B.



$$|T^{a}_{AC} - T^{r}_{AC}| \leq \alpha \qquad (2)$$

Portanto, o nó A tem duas memórias: sua própria avaliação baseada na eficiência de transmissões anteriores e as avaliações recebidas de terceiros. Os possíveis nós que podem conduzir ao destino desejado são então analisados pelo nó A baseado em suas duas memórias.



Velloso et al. (38) propuseram uma análise de modelos de confiança para redes *ad-hoc* a partir da coleta de informações locais e dos nós vizinhos diretos, privilegiando as redes móveis. Como os nós de uma rede *ad-hoc* acumulam as funções de roteador, servidor e cliente, a honestidade de comportamento desses

nós é imprescindível ao bom funcionamento das aplicações e dos protocolos aplicáveis a essas redes. O objetivo do modelo proposto é estimar um grau de confiança entre um nó e cada um dos seus vizinhos diretos a partir de informações locais, observadas pelo próprio nó e recebidas dos seus vizinhos dentro do raio de alcance do raio. A primeira etapa do modelo é coletar dados de confiança e a segunda etapa é conferir o comportamento dos vizinhos a partir das informações coletadas. Só após o julgamento dos dados coletados é que a indicação do nível de confiança é estabelecida. Uma terceira avaliação é considerada nesse trabalho: a maturidade da relação entre nós. Relacionamentos de mais longa duração recebem um grau maior de confiabilidade. Uma das diferenças desse trabalho para o do Yan et.al é incorporação da maturidade da relação como um peso importante na definição da confiança. Sempre que um nó encontra um nó vizinho, ele atribui um grau de confiança que é dado pelas condições da rede e do próprio nó avaliador. Logo em seguida começa o pedido de recomendações aos nós vizinhos, chegando ao cálculo de confiabilidade a partir da soma da sua própria avaliação com as avaliações recebidas dos seus vizinhos, conforme Equação $\boldsymbol{T_a(b) = (1 - \alpha)Q_a(b) + \alpha C_a(b)}$ (3:

$$\boldsymbol{T_a(b) = (1 - \alpha)Q_a(b) + \alpha C_a(b)} \quad \textbf{(3)}$$

onde:

- $T_a(b)$ é o grau de confiança de um nó a em relação a um b baseado na soma da sua própria avaliação com as avaliações dos seus nós vizinhos diretos.
- $Q_a(b)$ é a capacidade de um nó avaliar o grau de confiança baseado nas suas próprias informações;
- $C_a(b)$ é a contribuição dos vizinhos; e
- α é o peso atribuído a cada informação que compõe o grau de confiança do dado.

O cálculo de $Q_a(b)$, descrito na Equação**Erro! Auto-referência de indicador não válida.**, é realizado somando o grau de confiança obtido através do seu próprio julgamento a respeito do comportamento do nó vizinho em análise e o grau atribuído anteriormente, dando os respectivos pesos em função de β, na forma de:

$$\boldsymbol{Q_a(b) = \beta E_T + (1 - \beta)T_a^*(b)} \quad \textbf{(4)}$$

onde:

- E_T é o grau de confiança obtido pelo julgamento do próprio nó com relação ao vizinho;

- $T_a^*(b)$é o grau de confiança obtido anteriormente;
- β é o valor para o cálculo do peso de cada medida que pode ser atribuído de acordo com a relevância atribuída a cada informação.

A contribuição de vizinhos, $C_a(b)$, descrita na Equação $\boldsymbol{C_a(b)} = \frac{\sum_{i \in K_a} \boldsymbol{T_a(i) M_i(b) X_i(b)}}{\sum_{j \in K_a} \boldsymbol{T_a(j)} \sum_{j \in K_a} \boldsymbol{M_j(b)}}$ (5 considera as avaliações de vários outros nós para definição de umq confiança de um determinado nó, ou seja:

$$\boldsymbol{C_a(b)} = \frac{\sum_{i \in K_a} \boldsymbol{T_a(i) M_i(b) X_i(b)}}{\sum_{j \in K_a} \boldsymbol{T_a(j)} \sum_{j \in K_a} \boldsymbol{M_j(b)}} \qquad \textbf{(5)}$$

onde:

- i é cada nó vizinho;
- K_a é o conjunto de nós vizinhos comuns aos nós (a) e (b);
- M é a maturidade de relacionamento; e
- X é uma variável que representa a maturidade do relacionamento.

O pedido de contribuição aos vizinhos pode ser realizado através de envio de *Trust Request* (TREQ) com respostas *Trust Reply* (TREP) ou o recebimento de mensagens espontâneas (*Trust Advertisement* - TA) quando a tabela do nó vizinho sofrer atualização de confiança com relação a algum outro nó que modificou de forma expressiva seu comportamento, alterando seu nível de confiança.

Para o correto funcionamento do sistema, o limiar de maturidade deve ser baseado na média dos valores de maturidade de relacionamento de todos os vizinhos.

O trabalho de Velloso et al. serviu como base para a realização de outros trabalhos, como o de Lyno et al. (41) e Fernandes et.al (39) .O modelo de Fernandes et.al. propõe um mecanismo de exclusão de nós não cooperativos inspirado em um tribunal de júri, em que os nós possuem vários papéis: testemunhas e jurados. As testemunhas verificam o nível de confiança dos nós vizinhos e avisam ao júri. Nesse caso, um nó pode ser considerado mau por falhas ou por ter natureza maliciosa. O júri se baseia nas mensagens de evidência para a possível exclusão do nó.

O mecanismo realiza controle de acesso, identificando e retirando nós maliciosos da rede. Baseado em um tribunal de júri, cada nó assume papel de testemunha, jurado e réu. A testemunha monitora e avalia o nível de confiança de seus vizinhos, enviando mensagens periodicamente de evidência de mau

comportamento de nós para o júri. O jurado julga se um certo nó deve ser excluído ou não, e vota de acordo com sua avaliação. O júri é composto por um grupo dinâmico de nós escolhidos aleatoriamente e reconfigurado com a entrada e a saída de nós da rede. Cada nó assume papel de réu para ser avaliado pelo júri. Aplica-se a função *hash* ao identificador de um réu para se achar um nó jurado da rede e novamente a função *hash* para a identificação de outro jurado até a formação do júri. Por fim, um jurado atribui um valor de reputação para seu réu que é decrementado a partir de novas evidências de mau comportamento que ao atingir um limite pré-determinado pela administração da rede, faz com que o nó seja excluído (39).

4.3. Modelos de confiança e outros mecanismos de segurança aplicados em sistemas elétricos

Sistemas de confiança também vem sendo utilizados no contexto de redes elétricas inteligentes, embora não tenha sido encontrado nenhum trabalho de aplicação semelhante ao proposto, ou seja, na avaliação das mensagens dos *smart meters*.

Coates et al. (42) propõe um trabalho que investiga políticas e mecanismos de rede para aumentar a segurança da rede que interliga os elementos do sistema SCADA com a aplicação de sistemas de confiança em pontos estratégicos dessa rede. A ideia é utilizar esses mecanismos durante a transição da plataforma legada para a tecnologia IP, através da introdução de equipamentos com padrões modernos como o IEC61850. O sistema de confiança vem suprir a necessidade de se ter comandos e um maior controle de eventos de ataques de rede ou qualquer outro ato suspeito. Ele também pode ajudar no controle de acesso, alertas, bloqueio de elementos com mau comportamento, registro dos eventos e outras ações suspeitas (43) .

Outras formas de segurança complementares a de confiança são aplicadas, como por exemplo a proposta Sherman et.al (44), que visa utilizar a própria linha do sistema elétrico como um segundo canal para autenticação dos dados da origem.O sistema proposto conecta um computador do usuário a um medidor elétrico seguro via um detector de Autorização Humana (HAD). O medidor tem um identificador

secreto único e uma chave criptografada se comunicando com segurança com o *Power Grid Server* (PG). A partir de uma requisição de um servidor de aplicação (AS) da Internet, o usuário envia um certificado de localização ao AS, obtido via PLC assinado pelo PG. O usuário, por sua vez, pode autorizar ou negar requisições e entregas lendo o display do HAD e apertando o botão do HAD quando da autorização do acesso ao seu medidor. Trata-se, portanto de uma proposta de uso do PLC como um canal *out-of-band* para a autenticação de localização. Cabe ressaltar que sem um bom sistema de autenticação, os sistemas de confiança não podem ser aplicados com tanta eficiência. Trata-se de uma alternativa à recepção de GPS para a determinação da localização, apesar das aplicações sobre PLC terem que lidar com vários desafios, como largura de banda estreita, atenuação do sinal, interferência nas linhas de baixa tensão, transformadores que obstruem sinais e uma estrutura hierárquica constituída de baixa, média e alta tensões.

A segurança também pode ser tratada no nível de roteamento, através da inserção de firewalls e escolha de rotas seguras. Gonzalez et.al (45) propõem um método matemático para a escolha dos pontos de instalação de nós confiáveis que conterão uma combinação de firewalls e detectores de intrusão para dar algum nível de segurança ao sistema de controle central (SCADA). A ideia é que esses nós façam a segurança do acesso ao sistema de controle, tendo em vista que os sistemas de energia nunca necessitaram de segurança contra invasão da Internet e pessoas mal intencionadas.. O sistema intercepta mensagens para o sistema SCADA e para outros nós da rede, avaliando seu conteúdo. Com base no conteúdo, o sistema identifica riscos de segurança, dando alertas para o nó de controle. O sistema também determina se o nó tem permissão para enviar ou não a mensagem sob análise, corrigindo partes da mensagem antes do seu reencaminhamento e até mesmo excluindo a mensagem como um todo.

Seguindo a linha de prover a segurança das *Smart Grids* durante o encaminhamento de pacotes, *Zhang* et al. (46) propõem um algoritmo para a inserção de uma quantidade mínima de nós de confiança que maximize a detecção de intrusões dentro de uma rede *Smart Grid*. Os nós de confiança, colocados em pontos estratégicos, realizam uma análise em tudo que passa por eles. Quando o fluxo de dados passa , eles ativam funções de detecção de intrusão, validam dados e geram alarme quando identificam ataques. O trabalho apresentado visa inserir o menor numero possível desses nós de confiança e maximixar a detecção de

intrusos. A inoperância ou a perda de acesso a nó de confiança deve fazer com que outro nó da rede seja eleito para exercer a nova função de nó de confiança. O protocolo Dijkstra, por exemplo, decide o encaminhamento baseado na distância entre os nós ou custos das arestas. O objetivo desses autores é encontrar o caminho de roteamento de menor custo que tenha pelo menos um nó de confiança, inserindo também a contabilização do custo de processamento do próprio nó. A criptografia e alteração dos dados transmitidos geram atrasos que também são contabilizados no algoritmo.

Comentando um pouco sobre as características dos dados trocados entre *Smart Meters* e sistemas SCADA, Kim et al. (47) consideram que não há protocolo de transporte adequado à transmissão de mensagens curtas, com grande frequência e em tempo real de forma segura e escalável, Dados estes gerados por sensores inteligentes, medidores avançados, estações de carga a partir de veículos elétricos. Os dados dos medidores são menos críticos pois logo em seguida novos dados dos sensores são sobrepostos aos anteriores e portanto podem ser corrigidos em coletas subsequentes. Já no outro sentido, um comando de contingencia, se perdido, pode comprometer todo o sistema, tornando-se, portanto mais crítico. Com isso os requisitos de segurança não são simétricos.

4.4. Correlação entre a literatura e a proposta da dissertação

A inserção de sistemas de confiança no setor elétrico está principalmente relacionada à proteção do sistema SCADA. Na proposta desse trabalho, a confiança é aplicada para validação das informações enviadas pelos *Smart Meters*. Os conceitos introduzidos pelos modelos de confiança citados contribuíram para a construção desse novo modelo de coleta, onde a sua forma de acionamento é disparada a partir do grau de confiança nos dados recebidos anteriormente. Essa nova proposta faz uso de perfis de consumidores, de dados históricos, de comparação com os dados dos vizinhos (38) (39) e do princípio que a maioria é mais confiável do que a minoria (32). Diferentemente dos outros sistemas apresentados, o modelo proposto observa a evolução e a degradação do grau de confiança, até limiares pré-determinados, a partir dos quais deve-se intensificar a frequência de coleta para a detecção de fraudes e falhas no sistema ou diminuir de

modo a diminuir a quantidade de dados a serem processados.

Esse trabalho considerou a experiência obtida com a leitura das referências mostradas nesse documento e tomou como base três trabalhos considerados mais adequados. Velloso et al. (38) propõe um modelo que estima um grau de confiança entre um nó e cada um dos seus vizinhos diretos a partir de informações locais, observadas pelo próprio nó e recebidas dos seus vizinhos dentro do raio de alcance do raio. A primeira etapa do modelo é coletar dados de confiança e a segunda etapa é conferir o comportamento dos vizinhos a partir das informações coletadas. Só após o julgamento dos dados coletados é que a indicação do nível de confiança é estabelecida. Também fez uso do cálculo estatístico chamado média móvel exponencial ponderada para o cálculo da confiança, utilizado para a identificação de tendências de um conjunto de dados ao longo do tempo. Esses conceitos foram utilizados na análise dos dados. Outro conceito utilizado nesse trabalho foi a maturidade da relação entre nós presente no trabalho de Yan et.al (40). Sabater e Sierra (32) também exibem a importância da crença, dos dados históricos para comparação e análise com os dados atuais, sendo mais um conceito também muito utilizado nesse trabalho.

Capítulo 5

A Proposta de *Polling* Adaptativo com Base no Grau de Confiança

A proposta deste trabalho é analisar de forma eficiente os dados coletados dos smart meters. Ao invés de tratar todos os dados em coletas sucessivas e permanentes, administra-se essa frequência em função do comportamento dos dados recebidos. Se a área em análise estiver enviando dados dentro do comportamento esperado, pode-se espaçar as novas coletas, ou seja, diminuir a frequência de processamento de informações. Caso algum dado venha apresentar comportamento suspeito ou de indicação de falha grave no fornecimento do serviço, a coleta é intensificada, ou seja, aumenta-se a frequência de novas análises. Essa variação na frequência com que se coleta e processa dados foi batizado de Polling Adaptativo.

Um dado isolado não traz informação alguma. Ele precisa de outros dados para se correlacionar e aí sim gerar uma informação eficiente. Essas correlações, comparações, a fim de gerar informações úteis, também fazem parte do escopo dessa proposta. Comparações entre valores produzidos e consumidos, dados atuais com dados históricos e percepção individual com percepção coletiva sobre um mesmo dado.

Embora, não muito profunda, essa proposta inclui o uso do protocolo SIP para autenticação dos smart meters, de modo a garantir que eles sejam quem realmente dizem ser.

Todos os componentes do sistema elétrico são passíveis de controle, conforme mostrado na Figura 9, pois, dentro do modelo das *Smart Grids,* esses elementos possuem medidores e atuadores interconectados em tempo real com o sistema SCADA. Os medidores estão nos imóveis consumidores, nos transformadores das ruas, na rede de distribuição, nas subestações, enfim, nas diversas camadas do sistema elétrico desde a geração até o consumidor final.

Detalhando melhor as comparações, os dados dos medidores dos consumidores podem ser comparados entre si e com o concentrador que é o

transformador que os alimenta. Em um nível acima, a comparação pode ser feita entre os transformadores finais e os transformadores intermediários da rede de distribuição e assim sucessivamente. É possível que haja adulteração nos dados dos consumidores finais e nos dados do transformador direto, podendo o primeiro nível não ser eficiente a detecção de problemas. Isso poderia ocorrer se um hacker, além de modificar medidores inteligentes em casas para roubar energia, também modificasse o medidor do transformador para evitar que seu crime fosse notificado. Esse trabalho assume que, quanto maior o nível dentro do sistema elétrico, maiores são as medidas de segurança para evitar ataques e, assim, garantir a segurança do sistema. Com isso, se não for possível detectar um roubo no primeiro nível, existe uma alta probabilidade de detectá-lo nas camadas superiores subsequentes, apontando problemas na camada inferior.

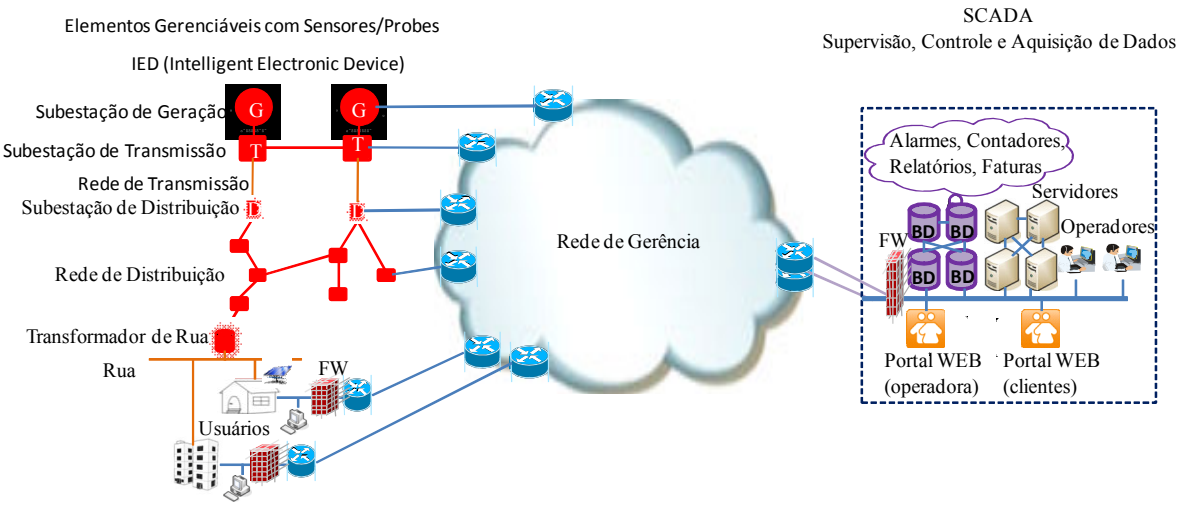


Figura 9 - Elementos do Sistema Elétrico que pode podem fornecer dados para o controle do sistema

5.1. Autenticação da Fonte dos Dados

Embora não seja parte do escopo desse trabalho, devido a sua importância vale ressaltar, considerando tratar-se de redes *Smart Grids* e, portanto com um alto grau de promiscuidade em seus acessos, a necessidade de se verificar a procedência dos dados a serem coletados. A coleta de dados, que é realizada a partir de medidores instalados nos diversos componentes do sistema elétrico, como gerador, subestação e medidores inteligentes dos imóveis dos consumidores,

precisa ter sua fonte verificada pelo sistema coletor da concessionária. Existem diversos protocolos utilizados para a identificação e autenticação dos usuários. O principal ponto na escolha desses esquemas é que eles devem ser escaláveis e seguros, considerando a grande quantidade de usuários do sistema que precisam ser autenticados.

A proposta desse trabalho é fazer uso do processo de registro de um protocolo de controle da camada de aplicação do modelo de referência OSI (*Open System Interconnection*), que é usado para estabelecer sessões ou chamadas multimídias. É um protocolo cliente-servidor, baseado no HTTP (*HyperText Transfer Protocol)*, envolvendo métodos de requisições e respostas, denominado *Session Initiation Protocol* (SIP), muito utilizado em aplicações de voz. Guimarães et al. propuseram a combinação do protocolo SIP com o protocolo IEC 61850-7-420 para controle de recarga das baterias dos veículos elétricos a partir dos dados coletados referentes à carga atual do veículo e a distância a percorrer (2). Esse trabalho tenta ressaltar o processo de registro e autenticação para a determinação da confiabilidade da origem da sessão conforme Figura 10 (48).

No protocolo SIP, há uma primeira solicitação de registro por parte do medidor inteligente (que funcionará como um terminal SIP) para o sistema que autenticará essa fonte, que pode ser o próprio coletor de dados, exercendo a função de SIP *Proxy,* como mostrado Figura 10. O SIP *Proxy*, por sua vez, responde propositadamente com uma mensagem de não autorizado (401) ou de autenticação do Proxy requerida (407) e com ela são encaminhados os dados necessários para o registro, utilizando o método *Digest* e *nonces* no cabeçalho da mensagem. O *nonce* é um número aleatório definido pelo SIP Proxy, e que é utilizado uma única vez, para garantir que mensagens de autenticação antigas de clientes legítimos não sejam reutilizadas por atacantes. O terminal SIP, então, constrói uma resposta criptografada a partir do *nonce*, *username*, senha e URI da mensagem 401 e envia uma nova mensagem de registro (REGISTER) contendo um cabeçalho de autorização. O SIP Proxy responde com uma mensagem 200 OK com um valor de expiração do registro. Antes de expirar o tempo de registro, o terminal SIP envia uma nova requisição de registro para que fique sempre apto a responder à novas requisições de registro. No modelo proposto, o SIP Proxy pode ser um elemento coletor de dados intermediário que irá agregar os dados de uma área antes do envio para o sistema SCADA.

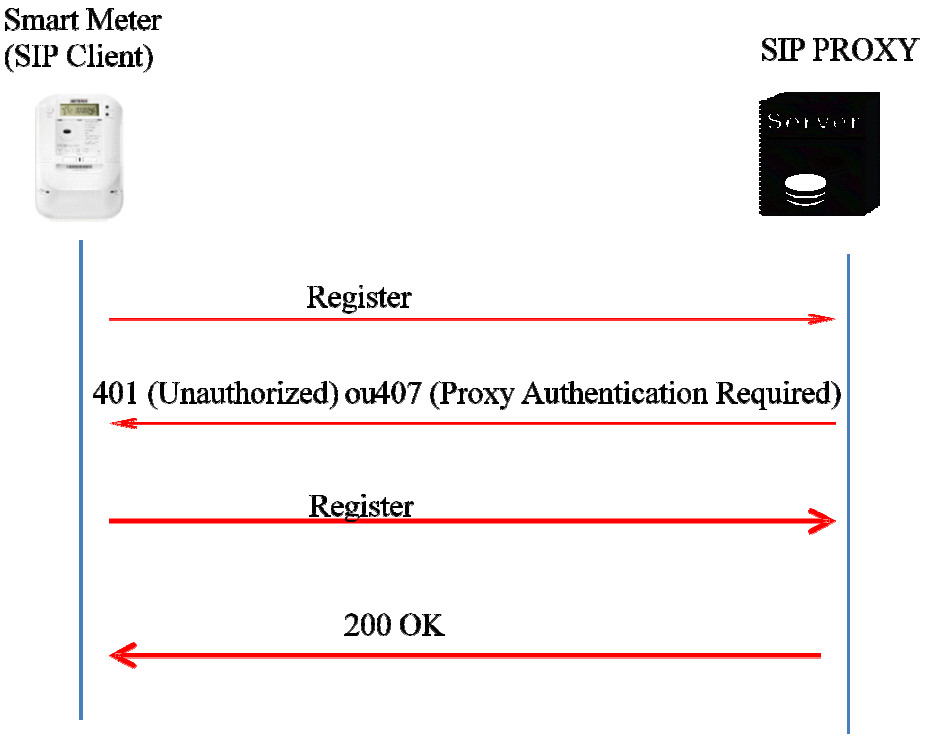


Figura 10 – Mensagens trocadas para o registro do protocolo SIP, assumindo que os medidores atuam como clientes e os coletores como SIP *Proxies*.

O SIP é um ótimo protocolo considerando a quantidade de elementos a serem gerenciados, a mobilidade e a confiabilidade necessária nesse tipo de sistema.

5.2. Polling Adaptativo

A questão chave tratada por essa proposta é controlar o intervalo de coleta de dados dos *Smart Meters* de acordo com os eventos observados na rede. Para tanto, foi proposto um sistema de confiança que, além de servir como base para a identificação de problemas, também é usado para aumentar ou diminuir o intervalo de coleta e consequentemente o volume de dados a serem processados, minimizando a necessidade de processamento do sistema SCADA para essa função quando a rede estiver em condições normais de funcionamento.

De modo a permitir o controle da coleta pelo sistema de processamento e não pelo medidor, a ideia é fazer uso de *Polling* e não de mensagens espontâneas de envio de medidas pelos *Smart Meters*. O *Polling* é um protocolo de acesso a

qualquer meio que normalmente é utilizado quando o acesso para coleta de dados se dá em direção a diversos elementos. Ao invés de cada medidor inteligente decidir o momento do envio do dado, cada coletor , que poderá ser um nó coletor ou o próprio SCADA, orquestrará a coleta (o *Polling*) até a entrega dos dados para o sistema SCADA. A orquestração da coleta pode decidir por reduzir a coleta para reduzir o volume de dados ou aumentar, para averiguar possíveis problemas como queda de link elétrico ou de comunicação.

Outra motivação para a escolha do *Polling* é evitar ataques de negação de serviço (*Deny of Service* - DoS*)* (49), nos quais atacantes enviam mensagens não solicitadas com o único fim de interromper o serviço. Assim, se mensagens são recebidas sem que tenha havido um *Polling*, já se sabe previamente que pode ser descartada. Um relaxamento para essa premissa pode ser feito para possibilitar o envio de mensagens de alarme. Contudo, para evitar os ataques, essas mensagens só poderiam ser enviadas para os concentradores em taxas muito baixas.

As medidas que indicam fraude ou medidor com defeito podem ser feitas através da comparação das medidas de consumo do cliente com as medições dos elementos agregadores do Sistema Elétrico como, por exemplo, o transformador associado. Enfim, sem que haja um exagero de coletas e uma inundação de dados a processar em condições de normalidade de rede, é possível determinar momentos de real necessidade de coleta de dados.

Antes de mostrar a forma de variação do *Polling* sugerida, é importante mostrar que esse processo utilizará o conceito de área. Na modelagem proposta, uma área será a composição de elementos de uma das camadas do sistema elétrico. Um exemplo de área é a composição de medidores inteligentes dos vários imóveis alimentados por um transformador, ou seja, pode ser um segmento de rua. O conceito se estende a um conjunto de transformadores alimentados por uma subestação de distribuição e assim sucessivamente. Dessa forma, os dados podem ser comparados localmente, como por exemplo, em uma rua, mas também abrangendo grandes áreas, observando dados de vários concentradores e os dados de medição de uma subestação de distribuição.

A proposta é começar um *Polling* com uma frequência *default* e modificá-la de acordo com as condições da rede e do cliente. Com a presença de indicativos de fraude nos dados de uma área, diminuindo o grau de confiança daquela fonte, duas medidas são tomadas: os clientes recebem *Polling* com frequências mais

altas, ou seja, a área é avaliada em períodos de coleta mais curtos e após reincidência de problemas na área, é disparada a equipe técnica da Concessionária para as devidas ações de manutenção ou verificação de possível fraude no cliente

Outros indicativos que podem sugerir fraude ou problema no medidor podem ser dados pela observação da variação das medidas coletadas com relação ao histórico daquele imóvel. Assim, se a área apresenta disparidade entre o que se declarou como consumido e a energia que foi oferecida, os primeiros clientes a serem investigados pela equipe de manutenção da concessionária são aqueles que apresentam grande variação com relação ao seu histórico de consumo. A ausência de consumo e a recepção de informações sobre a qualidade da rede divergente daquela vinda de vizinhos de uma mesma área também são indicativos para determinar que um medidor esteja adulterado ou com defeito, necessitando de intervenção da concessionária. Enfim, em função dos dados disponibilizados pelo medidor, diversas são as comparações que são possíveis para a verificação da veracidade do dado e da indicação de problemas de real falta de energia.

As medidas coletadas, quanto mais detalhadas, permitem uma melhor percepção do que está acontecendo no sistema. Essa é a razão para a redução do intervalo de *Polling* quando há uma desconfiança de problema em uma área. Por exemplo, se um medidor não envia o seu consumo em um pedido de *Polling*, há um indício de problema. Contudo, o problema pode ser apenas uma perda de mensagem ou alguma interrupção temporária no funcionamento do medidor, que não precisa de intervenção da concessionária, ou uma falha de hardware, que requisita a intervenção de uma equipe. Com a realização rapidamente de novos *Pollings*, esse problema pode ser identificado como temporário ou definitivo. Da mesma forma, uma divergência entre o que foi medido no transformador de uma área e o que foi declarado como consumido é um indicador de que existe fraude. Contudo, novas medidas subsequentes que apontam um consumo igual ou muito próximo a oferta podem mostrar que naquele intervalo onde ocorreu a disparidade pode ter ocorrido algum tipo de curto circuito, como um galho encostando-se à fiação elétrica. Ou ainda, um atraso na entrega do pedido de *Polling* para alguns medidores pode ter gerado a disparidade, mas um novo conjunto de medidas mostra que não existe fraude. Assim, queda parcial ou total do consumo medido, percepção da qualidade da rede pelos consumidores e comparação de consumo com a energia produzida são exemplos de dados que

podem levar a uma avaliação de problemas específicos no sistema, se tratados adequadamente.

Um detalhe importante é que a falta de indícios negativos por certo tempo é uma indicação de que o medidor voltou à normalidade e que é possível voltar a diminuir a frequência do *Polling,* pois o grau de confiança no cliente ou na área aumentou. Portanto, aumenta-se a frequência de *Polling* em presença de reincidência de indicativo de fraude ou falha e diminui-se a partir da volta à normalidade.

5.3. Distribuição dos elementos coletores de medidas de energia

A distribuição dos elementos coletores de dados deve ser devidamente definida de modo a facilitar a agregação dos dados. Alguns parâmetros devem servir como base para essa definição, como por exemplo, a capacidade de processamento do nó coletor, a disposição geográfica dos elementos cujos dados serão coletados, a existência de infraestrutura adequada (energia, ar-condicionado, área física etc.), a segurança no acesso para fins de manutenção e reparos, entre outros.

Além de considerar todas essas questões, no modelo proposto, os elementos coletores também devem ser hierarquizados, como mostrado na Figura 11 de modo a permitir a coleta de medições dos diversos elementos, conforme a seguir:

- Nos clientes do sistema Elétrico;
- Nos transformadores mais próximos do cliente (T1, T2, T3,...);
- Nos transformadores intermediários (TI1, TI2, TI3,...);
- Nas subestações de Distribuição (SD1, SD2, SD3,...);
- Nas subestações de Transmissão (ST1, ST2, ST3,...)
- No sistema gerador.

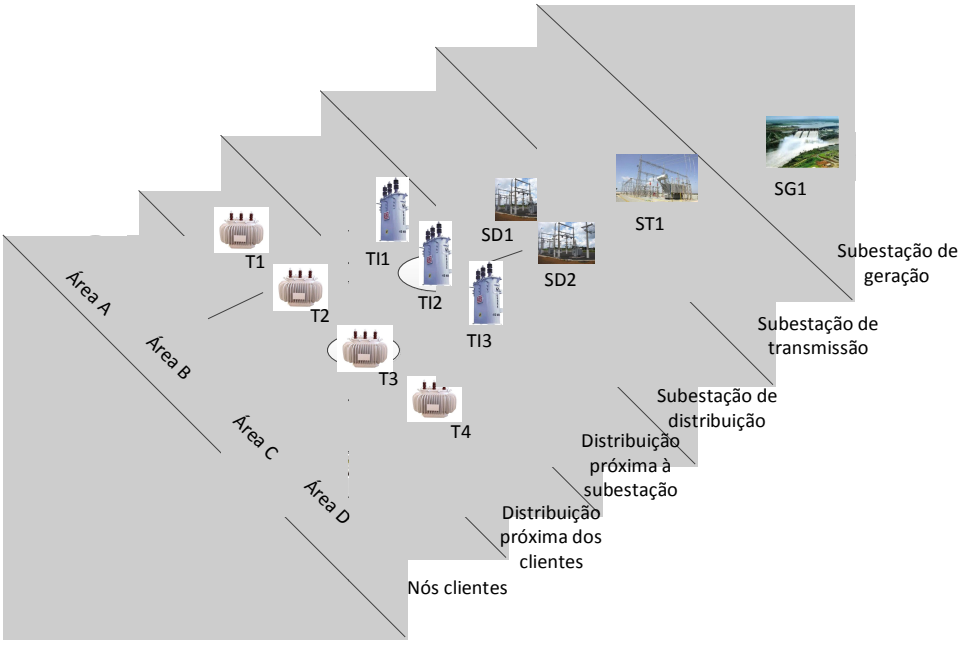


Figura 11 - Esquema hierarquizado de medidores utilizado na proposta, onde em cada nível é feita a agregação dos dados e verificação com o uso do modelo de confiança proposto.

Como um resumo, a partir de um suposto conjunto de dados coletados, a Figura 12 mostra alguns dos fatores que podem alterar o grau de confiança em um cliente ou em uma área e influenciar na reprogramação da periodicidade de *Polling*. É claro que existem inúmeras outras informações geradas pelos *Smart Meters* que podem apontar outros tipos de problemas.

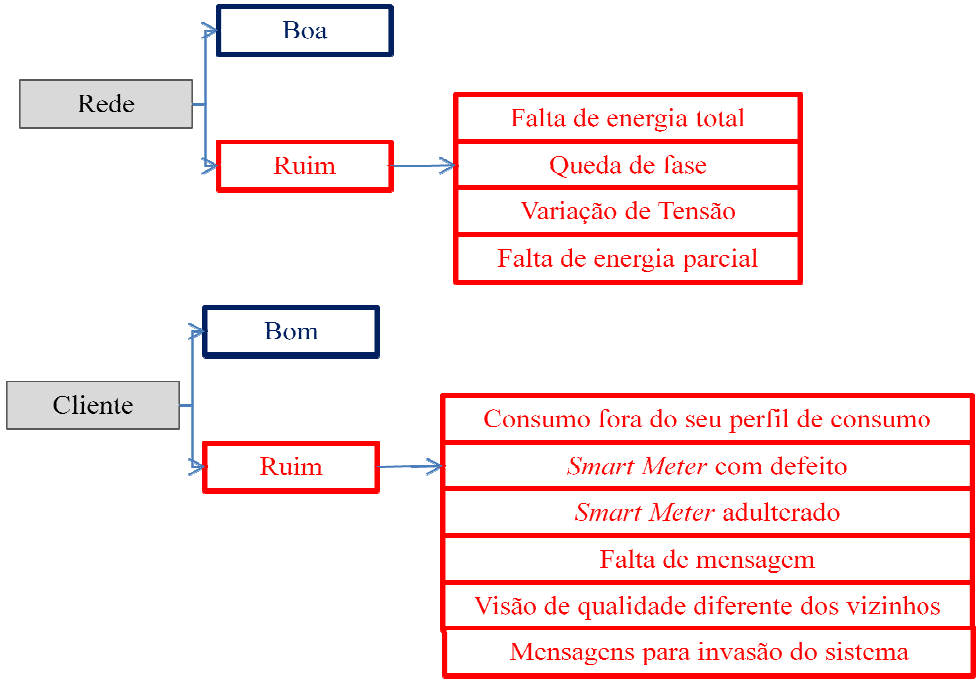


Figura 12 - Fatores bons e ruins para a variação da frequência de *Polling*

5.4. Medidas Observadas

O funcionamento do sistema proposto começa pela coleta dos dados dos medidores dos imóveis e dos elementos do sistema elétrico, tais como transformadores, subestações e assim sucessivamente, através da promoção de um *Polling* em intervalos Δt.

No nível do cliente, foram escolhidos três tipos de dados para avaliação: consumo medido (kWh) do imóvel, características das mensagens que carregam esses dados e a qualidade do serviço prestado pela concessionária percebido por cada cliente. Esses dados são tratados nos níveis superiores de forma agregada, onde cada um dos elementos vai representar toda a área coberta.

O consumo, normalmente medido em kWh, é o valor que o *Smart Meter* envia para a concessionária para ser utilizado para tarifação. As informações de consumo detalhadas também podem ser utilizadas pelo cliente para a administração dos seus próprios gastos e por órgãos que controlam o sistema para o planejamento da rede.

A qualidade é a medida que informa a visão do cliente sobre a qualidade da energia oferecida pela concessionária. Essa medida pode ser enviada para a concessionária com o intuito de notificar se o fornecimento está sendo feito de forma adequada ou se existem variações muito grandes no nível de tensão ou na frequência de alguma das fases que chegam até o cliente. No modelo proposto, essa medida é representada com notas, por simplicidade.

Outro item verificado pelo sistema proposto é o formato das mensagens enviadas. Por exemplo, uma mensagem pode vir maior ou menor do que o padrão definido ou ainda ter tamanho zero, o que significa que o *Smart Meter* não respondeu à solicitação do *Polling*. Mensagens com tamanhos fora do padrão podem significar dados maliciosos como vírus e *worms* (*Deny of Service* - DoS), que podem afetar o funcionamento do sistema.

Um conceito importante utilizado nesse trabalho é a figura do vizinho, que são medidores de uma mesma área, alimentados por um mesmo dispositivo central. Por exemplo, na Figura 11, as casas da área A são consideradas como vizinhas umas das outras. Em algumas situações, que serão explicadas a seguir, as comparações de medidas de vizinhos são aplicáveis.

O perfil histórico de uso é outro conceito que determina a faixa de consumo esperado para um imóvel. Inicialmente, para medidores recém-instalados, o perfil é montado a partir da expectativa a respeito dos eletrodomésticos comuns a um tipo de imóvel em uma determinada área. Em imóveis residenciais de classe média baixa, por exemplo, espera-se encontrar o uso de uma máquina de lavar, um ou dois aparelhos de ar, um ou dois aparelhos de TV, geladeira, micro-ondas, ferro de passar roupas e um computador, cujos tipo de consumo podem compor um perfil de consumo baixo residencial. Após a coleta de dados, durante algum tempo, daquele cliente, o perfil utilizado será composto pelas medidas passadas e não mais uma estimativa.

5.4.1. Análise da medida consumo

O medidor (*Smart Meter*) de um cliente do sistema elétrico mostra o consumo de energia do seu imóvel. Essa medida pode ser avaliada de diversas formas, criando indicadores de variações, que podem indicar mudança de comportamento, conforme mostrado a seguir.
O modelo proposto analisa dois parâmetros relativos ao consumo.

- a comparação da medida atual com dados históricos, resultando em uma variação da reputação do cliente;
- a comparação do somatório das medições de uma área com o que foi medido em um nível acima na hierarquia, por exemplo, a comparação do somatório do consumo de um conjunto de casas vizinhas com o que foi fornecido pelo transformador daquela área. Essa comparação resulta em uma variação da reputação da área.

5.4.1.1. Análise do consumo medido comparado com dados históricos

No modelo proposto, a concessionária mantém um banco de dados com consumo médio de cada cliente, por hora e por dia do ano. Esse valor pode ser comparado com o dado atual nas mesmas condições de data e hora. A Equação

$x_1 = \frac{(C_{sm\ histórico} - C_{sm\ atual})}{C_{sm\ histórico}}$, (6 calcula o percentual da diferença entre o valor real e o valor histórico com relação ao valor histórico, designada como x_1. Assim,

$$x_1 = \frac{(C_{sm\ histórico} - C_{sm\ atual})}{C_{sm\ histórico}}, \quad \textbf{(6)}$$

onde C_{sm} é o consumo fornecido pelo *Smart Meter,* atual ou histórico, com base na mesma hora do mesmo dia do ano anterior.

Uma vez que o modelo proposto é baseado em diversos indicadores e para permitir uma correlação simples entre eles, normaliza-se o conteúdo de forma que fique entre [0,1]. Assim, normaliza-se x_1 em C_i (consumo de análise individual do **$Ct=0$, se $x1 < 0$ $x1$, se $x1 \geq 0$** (7. Quando a medida atual do *Smart Meter* é maior do que a medida histórica, ou seja, $x_1 < 0$, também há um indício de alteração de comportamento, porém de caráter positivo para a concessionária, pois houve um incremento no consumo, fixando o valor em zero. Quanto mais próximo do valor um está C_i, maior é a diferença entre o consumo atual e o consumo histórico, ou seja, maior é a indicação de alteração de comportamento.

$$C_i = \begin{cases} 0, \text{se } x_1 < 0 \\ x_1, \text{se } x_1 \geq 0 \end{cases} \quad \textbf{(7)}$$

Cabe observar que C_i é um indício, mas não um indicador direto, pois o imóvel pode ter recebido novos eletrodomésticos, pode ter ficado vazio por motivo de doença, viagem ou mesmo por venda. Mas, de qualquer forma, como essas condições não são frequentes, na maioria das vezes, a variação C_ié um dado que pode ser considerado para detecção de fraudes ou medidores defeituosos.

5.4.1.2. Análise da energia consumida pelos Smart Meters comparada com a energia distribuída

Esse parâmetro do modelo proposto compara a soma do cosumo de todos os vizinhos de uma área com o valor medido pelo transformador que atende àquela **$x2 = (CT - áreaCsm)CT$** (8. Essa medida pode ser aplicada a todos os

níveis adjacentes da hierarquia de equipamentos descrita na Figura 11.

A Equação$\mathbf{x_2} = \frac{(C_T - \sum_{área} C_{sm})}{C_T}$ (8 calcula o percentual da diferença entre o valor do consumo total dos *Smarts Meters* da área e a energia distribuída pelo transformador, designada como x_2:

$$\mathbf{x_2} = \frac{(C_T - \sum_{área} C_{sm})}{C_T} \quad \textbf{(8)}$$

onde C_{sm} é o consumo fornecido por cada *Smart Meter* da área e C_T é a medição da energia distribuída pelo transformador que alimenta todos os *Smart Meters* da área.

Para permitir uma correlação simples entre os indicadores, normaliza-se seu conteúdo, de x_2 para C_a (Consumo analisado na área), conforme a Equação $\boldsymbol{C_a} = \begin{cases} \mathbf{1}, \mathbf{se}\ \boldsymbol{x_2} < 0 \\ \boldsymbol{x_2}, \boldsymbol{se}\ \boldsymbol{x_2} \geq \mathbf{0} \end{cases}$ (9. Quando a medida de consumo total de todos os *Smart Meter* é maior do que a medida de energia distribuída pelo transformador da área, também há um indício de problema, pois a energia consumida não pode ser maior do que a distribuída, então C_a é fixado no valor um (1), caso contrário, C_a recebe o valor da diferença calculada. Assim,

$$\boldsymbol{C_a} = \begin{cases} \mathbf{1}, \mathbf{se}\ \boldsymbol{x_2} < 0 \\ \boldsymbol{x_2}, \boldsymbol{se}\ \boldsymbol{x_2} \geq \mathbf{0} \end{cases} \quad \textbf{(9)}$$

Quanto mais próximo de um, maior é a

Este modelo prevê uma margem de erro no

Apesar de não fazer parte do escopo desse

5.4.2. Análise da medida de qualidade na área

A qualidade observada pelos clientes é

5.4.2.1. Análise da média da qualidade observada

A qualidade percebida pelos clientes de uma área pode dar a indicação do

$$\boldsymbol{Q\acute{a}rea = \acute{a}reaQsmquantidade\ total\ de\ SM}$$ (10. Se uma grande parte dos clientes acusar má qualidade na rede, provavelmente há problemas no fornecimento na área. Assim,

$$\boldsymbol{Q}_{\acute{a}rea} = \frac{\sum_{\acute{a}rea} \boldsymbol{Q}_{sm}}{\boldsymbol{quantidade\ total\ de\ SM}} \qquad \textbf{(10)}$$

onde $Q_{área}$ é qualidade média observada pelos *Smart Meters* da área, a qual é uma nota derivada das observações feitas da rede e Q_{SM} é a qualidade informada por cada *Smart Meter* (SM).

A qualidade medida na área pode mostrar um desempenho de ótimo à ruim. Se a $Q_{área}$ for menor que um determinado limite L_1, configurável pela concessionária, há uma condição de suspeita de problemas na instalação da área. Para uso no sistema, é feita uma transformação de $Q_{área}$ para Q_a, o qual vale zero ou um, conforme a equação $\boldsymbol{Q_a} = \begin{cases} \boldsymbol{1}, & \boldsymbol{se\ Q_{\acute{a}rea} < L_1} \\ \boldsymbol{0}, & \boldsymbol{se\ Q_{\acute{a}rea} \geq L_1} \end{cases}$ (11. Se determina o valor um em caso de a nota da área estar acima da tolerância admitida pela concessionária e zero em caso de uma média acima do limiar tolerado, ou seja:

$$\boldsymbol{Q_a} = \begin{cases} \boldsymbol{1}, & \boldsymbol{se\ Q_{\acute{a}rea} < L_1} \\ \boldsymbol{0}, & \boldsymbol{se\ Q_{\acute{a}rea} \geq L_1} \end{cases} \qquad \textbf{(11)}$$

5.4.2.2. Análise da variação da qualidade observada entre vizinhos

Um *Smart Meter* pode acusar má qualidade da rede, sem que os demais vizinhos percebam, devido a problemas internos no imóvel ou no medidor. Outra possibilidade é a ação de um *hacker* contra a rede de controle. Contudo, em condições normais, as medidas de uma mesma área deve apresentar baixa variação em torno da média da qualidade da área, $Q_{área}$. Calcula-se, portanto a diferença entre a qualidade informada pelo *Smart Meter* e a média da qualidade informada pelos vizinhos de forma a identificar a validade da informação prestada, conforme equação $\boldsymbol{x4 = Q_{área} - Q_{sm}}$ (12, onde Q_{sm} é a medida de qualidade de cada cliente.

$$\boldsymbol{x_4 = Q_{\acute{a}rea} - Q_{sm}} \qquad \textbf{(12)}$$

Quando o valor absoluto da diferença entre a qualidade informada por um *Smart Meter* e a qualidade informada pelos vizinhos é maior do que um limite L_2, tolerância essa determinada pela concessionária, há indicação de problema, caso contrário é uma diferença aceitável. Normalizando x_4 em Q, para facilitar a correlação entre as medidas, tem-se que:

$$\boldsymbol{Q = \begin{cases} 0, se\ x_4 < L_2 \\ 1, se\ x_4 \geq L_2 \end{cases}} \qquad \textbf{(13)}$$

Nessa equação, o valor um é aplicado no caso de diferença entre medidas fora do valor tolerável pela concessionária e zero no caso de medidas bem próximas.

5.4.3. Análise das mensagens

A mensagem recebida com o tamanho, o protocolo ou a formatação dos dados da mensagem diferentes do padrão podem indicar suspeita de fraude ou de equipamentos com defeito. Por outro lado, são diversas as condições que podem afetar o bom comportamento de um dado sem ser falha ou fraude. O parâmetro *M* recebe valor zero se a mensagem estiver fora do padrão esperado e um se estiver como esperado, conforme

$$\boldsymbol{M = \begin{cases} 0, se\ mensagem\ dentro\ do\ padrão \\ 1, se\ mensagem\ fora\ do\ padrão \end{cases}} \qquad \textbf{(14)}$$

5.5. Grau de confiança de um indicador

Um indicador por si só não deve expressar um problema que justifique o acionamento da equipe técnica de manutenção da concessionária do sistema elétrico. A repetição sucessiva de certos indícios, sim, deveria ser o momento certo. Portanto, no modelo proposto, para se evitar falsos positivos na detecção de problemas, é feita uma observação das mensagens dos *Smart Meters* por um período maior de tempo, antes de gerar o alarme para a concessionária. Isso é feito

através cálculo do grau de confiança.

Assim como no modelo de Velloso et al. (38), esse trabalho faz uso de um cálculo estatístico chamado média móvel exponencial ponderada para o cálculo da confiança. Em estatística, média móvel é um recurso utilizado para a identificação de tendências de um conjunto de dados ao longo do tempo. É possível a utilização desse conceito para se identificar a variação de certo dado em função do seu passado, ou seja, dos valores históricos assumidos por ele. A média móvel retira oscilações, ruídos dos dados amostrados e suaviza a curva de variação do dado tornando mais simples a análise das tendências. Essa média pode ser calculada de diversas formas, desde a mais simples até a mais complexa com ponderações entre os valores comparados, conforme detalhado a seguir (50).

A média móvel exponencial ponderada trata-se de uma variação da média móvel exponencial que permite que se atribua pesos que definem a importância tanto dos dados históricos quanto do dado atual. Uma média móvel exponencial ponderada ($EWMA$) é calculada como:

$$\boldsymbol{EWMA_t = \alpha\, Valor_{atual} + (1-\alpha)\, EWMA_{t-1}}, \qquad \textbf{(15)}$$

onde α, $0 < \alpha \leq 1$, é a constante que determina o peso do valor atual.

O uso de $\alpha=1$ indica que apenas a medição mais recente influencia na média móvel. Um pequeno valor de α dá mais peso aos valores antigos. O peso das medidas anteriores é reduzido exponencialmente com o aumento de t, de acordo com α, pela aplicação da equação.

A escolha do valor de α permite que a concessionária dê um peso maior ao que considerar como mais interessante para a sua detecção de problema. Dentro do modelo proposto, o α assume um valor diferente para cada um dos parâmetros.

5.6. Cálculo do Grau de Confiança (GC)

Todo o processo de análise começa em um instante t_0, no qual todos os medidores analisados começam com um alto grau de confiança, ou seja, todos são considerados confiáveis até que eventos com indicação de alguma anormalidade possam modificar essa confiança a eles depositada. Como a concessionária é

responsável pelo projeto e instalação dos medidores, ela os considera inicialmente confiáveis.

O sistema proposto tem por objetivo que, se alguma instabilidade momentânea for detectada, isso não gere grande alteração no grau de confiança, evitando o envio de um alarme desnecessário. Contudo, caso se observe a reincidência da instabilidade em um determinado período de tempo, o grau de confiança deve diminuir a ponto de disparar um alarme.

A cada medida recebida por *Polling*, o grau de confiança é recalculado, através de uma média móvel exponencial ponderada.

Toda vez que o grau de confiança de um dado é decrementado, maior é o interesse da concessionária em obter mais dados a fim de ratificar a suspeita. De modo a resolver essa necessidade, a cada diminuição do grau de confiança, a frequência de *Polling* para solicitação de dados é aumentada, permitindo a análise de mais dados da medida suspeita. Esse procedimento foi chamado de *Polling* adaptativo. Com algumas medidas com comportamento inadequado, sem atingir a tolerância determinada pela concessionária, seguidas de novas medidas dentro da faixa esperada, o grau de confiança torna a subir. Essa variação do *Polling* e, principalmente, do grau de confiança, faz com que perturbações passageiras no sistema não sejam consideradas.

O cálculo do grau de confiança é determinado por:

$$\boldsymbol{GC_{x_i}(t_{atual}) = (\alpha * medida_{nova}) + \left((1-\alpha) * GC_{x_i}(t_{anterior})\right)} \quad \textbf{(16),}$$

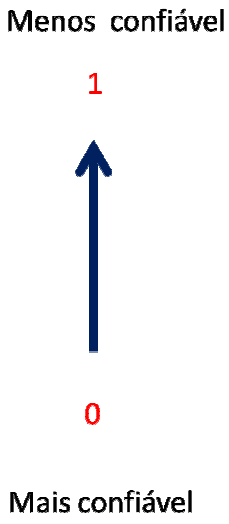
onde, α é o peso que será atribuído à medida mais nova, t_{atual} é o momento da medida atual e $t_{anterior,}$ o momento do último GC_{x_i} calculado. Essa fórmula é aplicada a todos os indicadores.

Os indicadores que geram um grau de confiança, e a indicação de aplicação na área ou por cliente são listados na Tabela 4.

Tabela 4 - - Indicadores Normalizados com suas medidas já compreendidas entre [0,1], onde 0 representa dado confiável e 1, não confiável.

Indicador	Função	Tipo	$\boldsymbol{x}$
C_i	Variação entre consumo atual e perfil histórico.	Cliente	$\boldsymbol{x_1}$
C_a	Comparação do consumo da área entre clientes e transformador	Área	$\boldsymbol{x_2}$
Q_a	Qualidade média da energia na área	Área	$\boldsymbol{x_3}$

Q	Diferença de qualidade entre vizinhos.	Cliente	
	Validação das mensagens	Cliente	



5.7. Avaliação da Área

Uma área é avaliada pelos indicadores e , que representam, respectivamente a variação do valor medido pelos *Smart Meters* e o transformador, e o valor da qualidade média da área. Cada indicador terá seu grau de confiança analisado, onde é o grau de confiança relativo à e é o grau de confiança relativo à .

Os cálculos dos graus de confiança são realizados conforme equações abaixo:

(17)

(18)

É importante observar que os pesos α variam de acordo com o indicador. O mesmo se aplica aos indicadores de cliente.

Quando os dados se apresentam dentro do comportamento esperado, o *Polling* para coleta de novos dados tem sua frequência diminuída do padrão inicial mais γ_s até um intervalo_máximo admitido pela concessionária para a verificação da rede.

Quando os dados não se apresentam dentro do comportamento esperado, o *Polling* para coleta de novos dados tem sua frequência aumentada de γ_d até um

intervalo_mínimo admitido pela concessionária para a verificação da rede.

Uma particularidade do modelo de *Polling* adaptativo proposto é que quando o indicador GC_{x3} aciona o *Polling* adaptativo, por ser uma condição, que se confirmada, é de alto grau de severidade, o *Polling* adaptativo é colocado na maior frequência possível de coleta, de forma acelerar a confirmação ou não do problema.

5.8. Geração de Alarme da Área

No modelo proposto, a concessionária deve determinar o limite inferior (β_{1i}) do grau de confiança, a partir do qual se coloca a área sob suspeita, incrementa-se a frequência de *Polling* e dispara a verificação dos indicadores de clientes em busca do cliente causa raiz da áreas. A concessionária deve determinar também o limite superior (β_{2i}), a partir do qual se considera a emissão de alarme para a área e que esta deve receber a presença de técnicos para a realização de manutenção para a correção dos problemas apresentados, mesmo que cliente algum tenha ainda alarmado, mas a área merece verificação da equipe de campo.

Os índices β_{1i} e β_{1i} são variáveis de acordo com o indicador que está sendo analisado. Cada indicador tem sua ordem de grandeza e com isso os limiares para sua análise tornam-se específicos para ele.

5.9. Avaliação do Cliente

Quando uma área é colocada sob suspeita, seus clientes passam a ter seus dados avaliados para uma possível detecção da origem do problema. Um cliente é avaliado pelos indicadores C_i, Q e M que representam respectivamente Variação entre consumo atual e perfil histórico, diferença de qualidade entre vizinhos e validação da mensagem . Cada indicador terá seu grau de confiança analisado, onde GC_{x1} é o grau de confiança de C_i, GC_{x4} é o grau de confiança relativo à Q e GC_{x5} o grau de confiança de M.

Os cálculos dos graus de confiança são realizados conforme equações

abaixo:

$$\boldsymbol{GC_{x1}\,(t_{atual}) = (\alpha_1 * \, medida_{nova}) + \big((1-\alpha_1) * \, GC_{x1}\,(t_{anterior})\big)} \quad \textbf{(19)}$$

$$\boldsymbol{GC_{x4}\,(t_{atual}) = (\alpha_4 * \, medida_{nova}) + \big((1-\alpha_4) * \, GC_{x4}(t_{anterior})\big)} \quad \textbf{(20)}$$

$$\boldsymbol{GC_{x5}(t_{atual}) = (\alpha_5 * \, medida_{nova}) + \big((1-\alpha_5) * \, GC_{x5}(t_{anterior})\big)} \quad \textbf{(21)}$$

O indicador C_i, mostra que o consumo atual está fora do perfil histórico do referido imóvel, o que pode ser devido a diversas razões, como ausência dos seus ocupantes por motivo de viagem, eletrodomésticos com defeito reduzindo o consumo, aquisição de novos eletrodomésticos aumentando o consumo, medidor com perda de precisão ou até mesmo adulteração do medidor por pessoas mal intencionadas.

O indicador Q mostra a diferença de

O indicador M mostra que a mensagem de

A adaptação do intervalo de *Polling*

5.10. Geração de Alarme de Cliente

Quando os indicadores de clientes são

A concessionária deve determinar

Toda essa dinâmica de avaliação da área e do

Algoritmo 1: Pseudocódigo que avalia graus de confiança e emite alarmes para concessionária.

Input: $x_1, x_2, x_3, x_4, x_5, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \beta1_1, \beta1_2, \beta1_3, \beta1_4, \beta1_5, \beta2_1, \beta2_2, \beta2_3, \beta2_4, \beta2_5$, intervalo_max, intervalo_min, γ_s, γ_d

```
1  if momento_polling ( ) then
2  GCx1, GCx2, GCx3, GCx4, GCx5 = calcula_confiança(x1, x2, x3, x4, x5, α1,
                                                    α2, α3, α4, α5)
3   if GCx3 > β23
4                emite_alarme (GCx3)
5                analisa_clientes (GCx1, GCx4, GCx5 )
6      else if GCx2 ≤ β12 and GCx3 ≤ β13 then
7                                  intervalo=intervalo + γs
8                if intervalo > intervalo_max then
9                    Intervalo = intervalo_max
10              end
11     end
12     elseif  β12 < GCx2 ≤ β22 or β13 < GCx3 ≤ β23 then
13               Intervalo = intervalo - γd
14               if intervalo < intervalo_min
15                 Intervalo = intervalo_min
16               end
17               analisa_clientes (GCx1, GCx4, GCx5 )
18     end
19     elseif  GCx2 > β22  then
20               analisa_clientes (GCx1, GCx4, GCx5 )
21     end
22     return intervalo
23 end
```

Segue explicação do pseudocódigo.

Dados de entrada do pseudocódigo,

No momento do polling [1], são

I. Se o grau de confiança GC_{x3} , que indica a qualidade do serviço na área, estiver acima do limite $\beta2_3$ [3], é emitido o alarme para acionamento da manutenção local[4] e a análise dos graus de confiança específicas de cada cliente GC_{x1} , GC_{x4} e GC_{x5} [5].

II. Se GC_{x3} e GC_{x2}, relacionados à qualidade do serviço e a diferença entre a energia distribuída e consumida na área, estiverem até o limite de

tolerância aceitável $\beta 1_3$ e $\beta 1_2$ respectivamente [6], incrementa-se o intervalo de tempo para um novo polling de γ_s [7] devido a ausência de problemas. Esse intervalo não pode ultrapassar o intervalo_max fixado pela operadora, para que mesmo em condições normais sejam feitas sempre verificações periódicas. [9,10,11].

III. Se GC_{x3} e GC_{x2} estiverem entre os limites de tolerância $\beta 1_3$ e $\beta 1_2$ e o de confirmação de problema $\beta 2_3$ e $\beta 2_2$ [12], intervalo entre novos pollings é reduzido de γ_d [13] para que mais coletas sejam feitas para verificação até o intervalo mínimo passível de tratamento dos dados, determinado pela operadora [14,15,16]. Adicionalmente, é feita a análise dos graus de confiança específicas de cada cliente GC_{x1} , GC_{x4} e GC_{x5} [17].

IV. Se GC_{x2} alcançar o limite de confirmação de problema $\beta 2_2$ [19] é feita a análise dos graus de confiança específicas de cada cliente GC_{x1} , GC_{x4} e GC_{x5} [5], em busca do(s) cliente(s) ofensor(es) [20].

O segundo algoritmo mostra a forma de

Conforme mostrado no gráfico 1, os limites

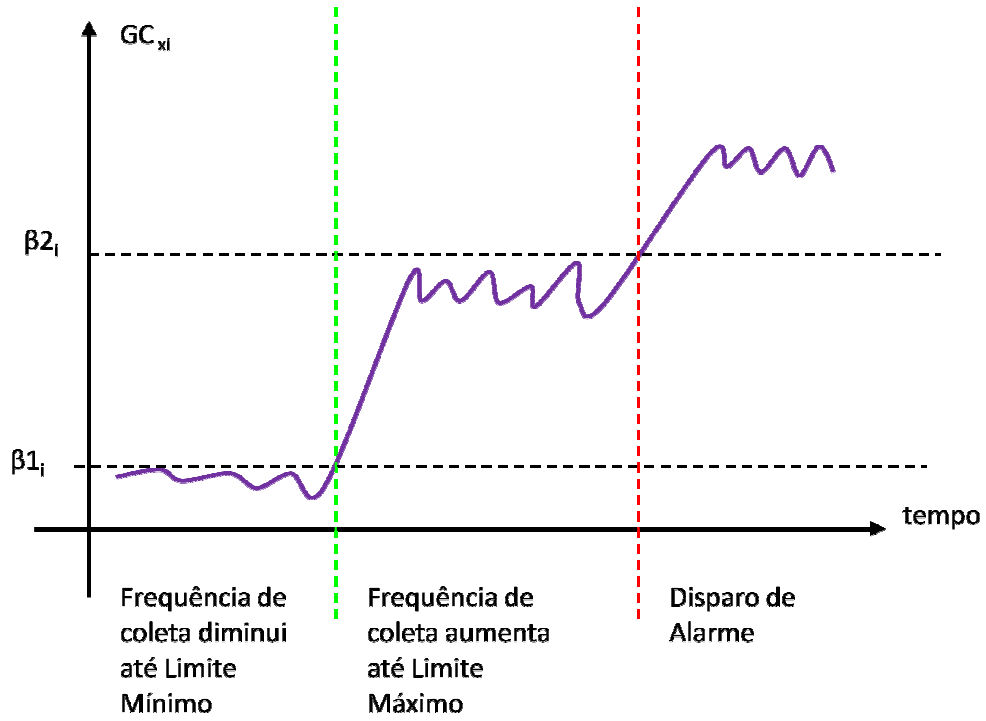
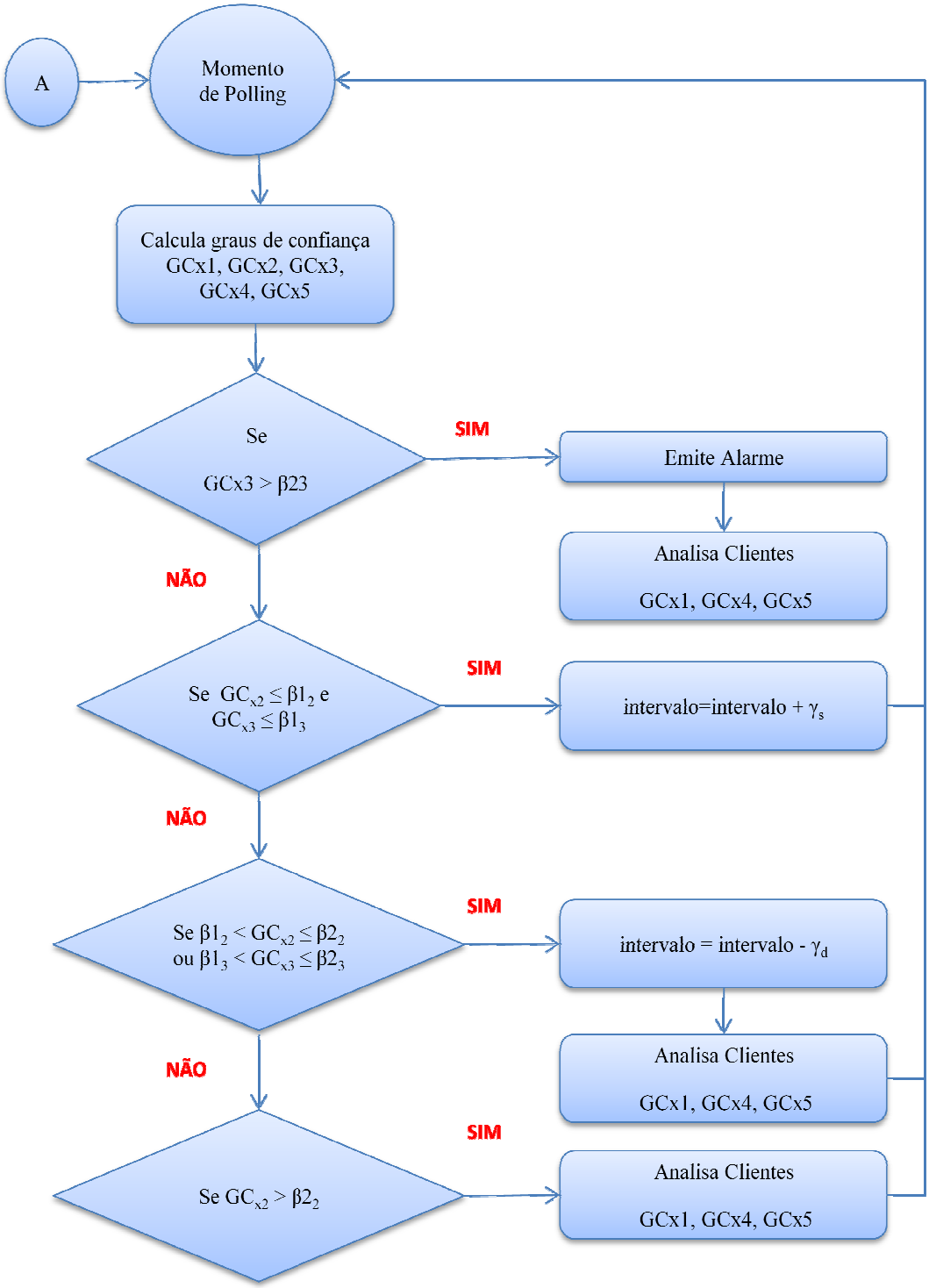
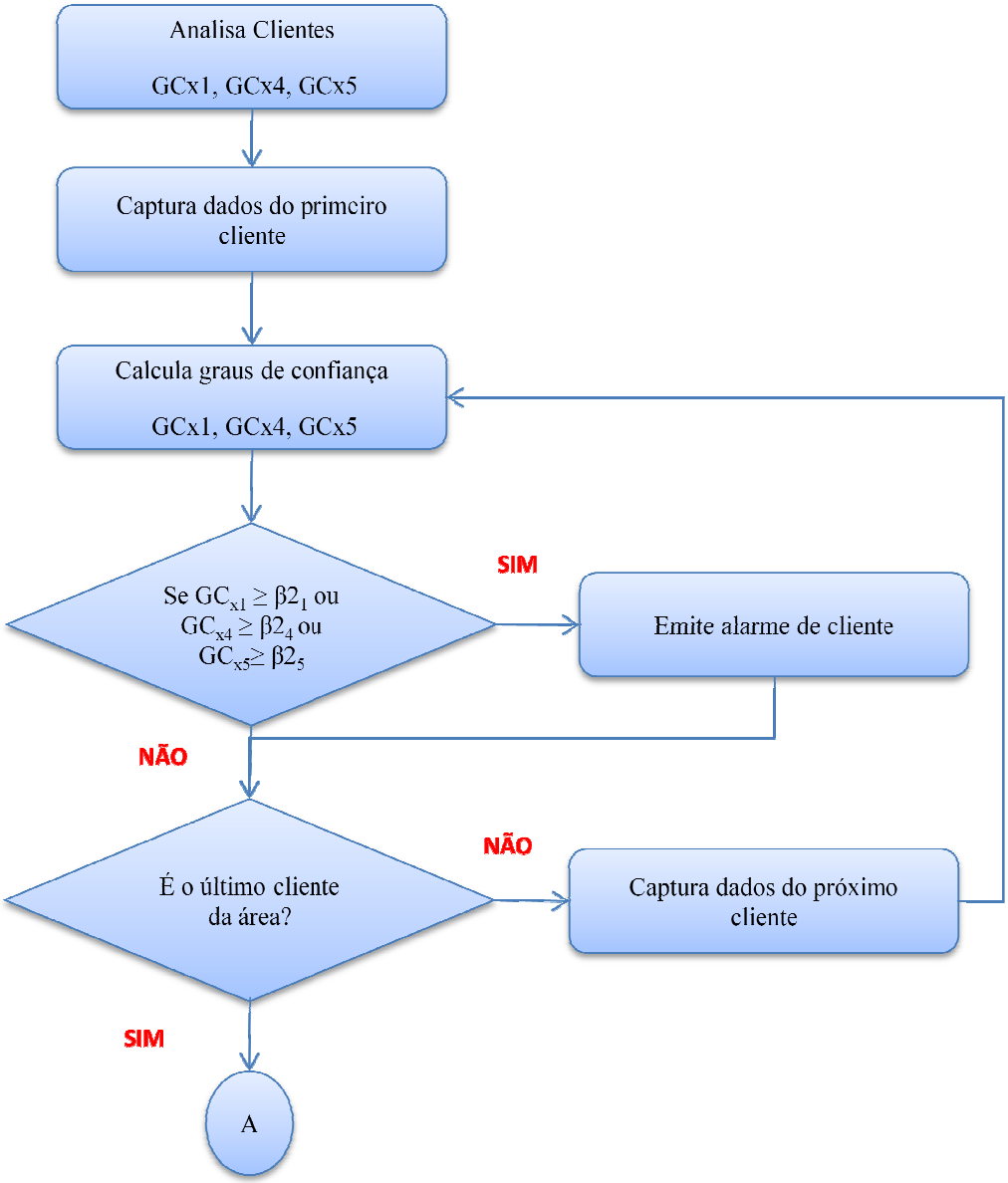


Gráfico 1 - thresholds" dos Graus de Confiança

Seguem Fluxograma 1 e Fluxograma 2 para melhor visualização dos algoritmos.



Fluxograma 1 algoritmo 1



Fluxograma 2 - algoritmo 2

5.11. Parametrização

A parametrização do sistema proposto possui alguns valores definidos de forma empírica, obtida das simulações realizadas para teste das ideias apresentadas. A periodicidade de coleta é uma definição da concessionária e foi

simulada de forma empírica. A Tabela 5 mostra esses parâmetros e os valores atribuídos a cada um.

Tabela 5 - Parametrização da Proposta

Parâmetro	Descrição	Valor
Notas	Avaliação da qualidade da	4 e 5
Notas	Avaliação da qualidade da	0,1,2,3
L_1	Nota a partir da qual a	4
L_2	Diferença máxima admitida	1
α_1	Peso dado ao valor atual	0,4
α_2	Peso dado ao valor atual	0,4
α_3	Peso dado ao valor atual.	0,6
α_4	Peso dado ao valor atual	0,4
α_5	Peso dado ao valor atual	0,4
$1- \alpha_i$	Peso dado ao valor	1-α
γ_s	Incremento no intervalo	Não
γ_d	Decremento no intervalo	3 horas
$\beta 1_2$	Valor a partir do qual o	0,002
$\beta 1_3$	Valor a partir do qual o	0,1

$\beta 2_1$	Valor a partir do qual o	0,2
$\beta 2_2$	Valor a partir do qual o	0,06
$\beta 2_3$	Valor a partir do qual o	0,7
$\beta 2_4$	Valor a partir do qual o	0,7
$\beta 2_5$	Valor a partir do qual o	0,7

5.12. Intensidade da adulteração de um Usuário Malicioso

Um usuário malicioso que adultera de forma

Um usuário malicioso que adultera de

Capítulo 6

Simulação

A dinâmica utilizada foi simular dados dos

O modelo proposto de avaliação de

Essa proposta é extensível às demais

6.1 Dados Simulados

A primeira ação foi criar uma massa de medidas simulando os dados coletados dos *Smart Meters* de todos os imóveis. Foram considerados dois perfis de clientes, residencial e industrial. Os dados de consumo foram gerados a partir de curvas padrão que descrevem o consumo de residências e industrias O perfil 1 é ilustrado na Figura 13 e o perfil 2 na Figura 14.

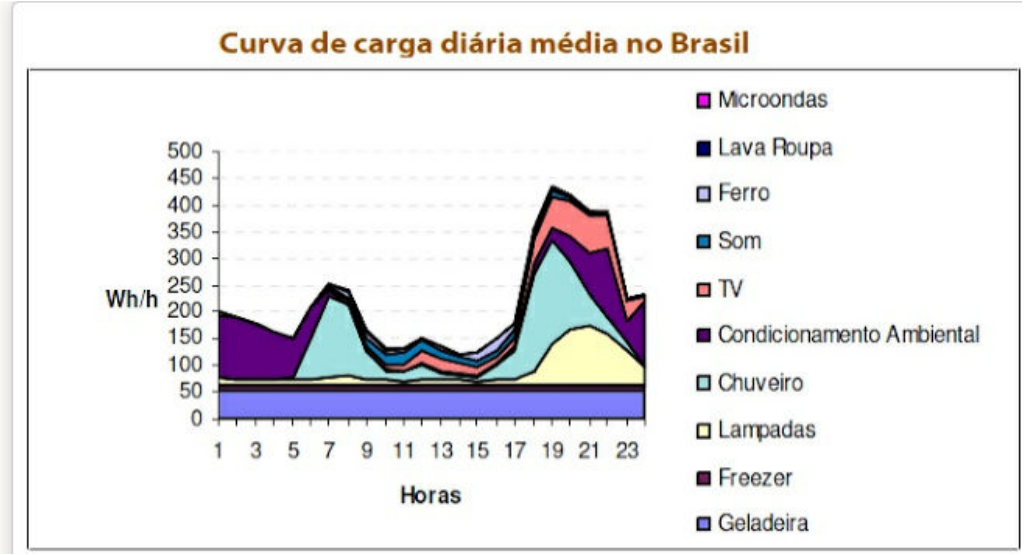


Figura 13 - Médias de Consumo Residencial- (51)

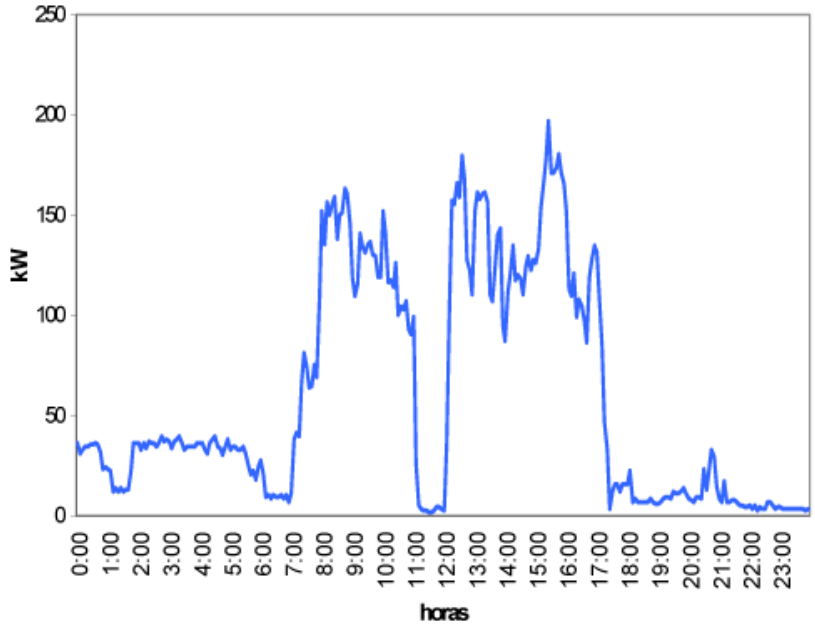


Figura 14 - Médias Reais de uma Indústria (52)

Esses valores padrão foram utilizados

A distribuição normal é uma distribuição estatística. Esse tipo de distribuição tem formato de um sino, conforme Figura 15, , sendo simétrica dos dois lados do dado médio. Se consideramos a probabilidade de um dado acontecer, a área sob a curva contabiliza 100% e com isso a probabilidade de uma observação assumir um valor entre dois pontos é igual a área entre eles. Esse conceito foi utilizado para a geração dos dados da simulação de forma a mostrar que um dado normalmente fica em torno de um comportamento médio

e que qualquer valor fora dessa variação gera uma indicação de mudança de comportamento.

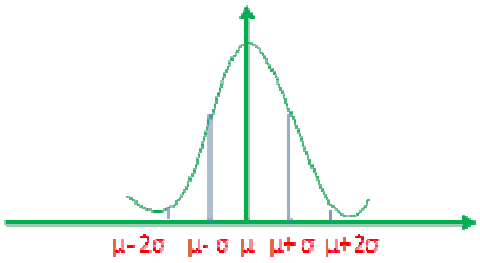


Figura 15 - Curva Normal

A equação da curva Normal é calculada utilizando-se dois parâmetros: a média (μ) e o desvio padrão (σ), onde a média é o centro da distribuição e o desvio-padrão padrão, o espalhamento da curva. Os gráficos das Figuras Figura 16 Figura 17 mostram exemplos de dados gerados, assumindo σ=15 e μ como o valor da curva de consumo padrão (Figura 13 e Figura 14).

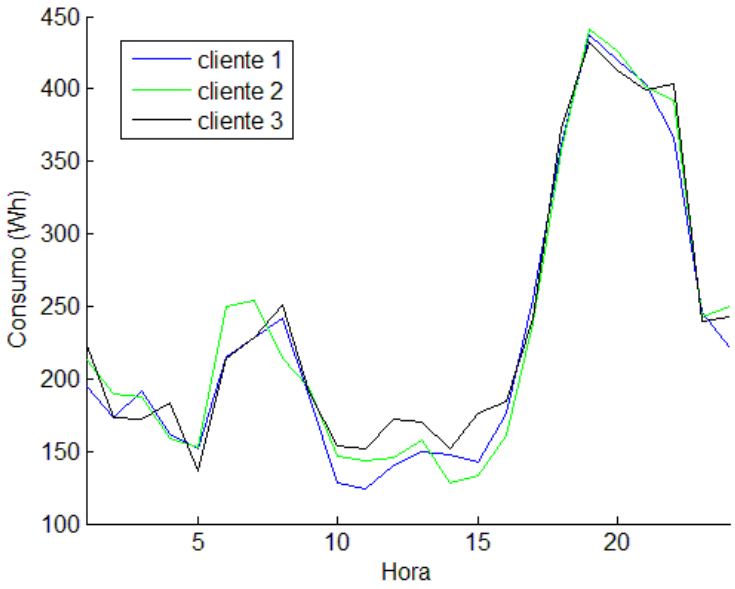


Figura 16 - Dados Simulados para o Perfil Residencial

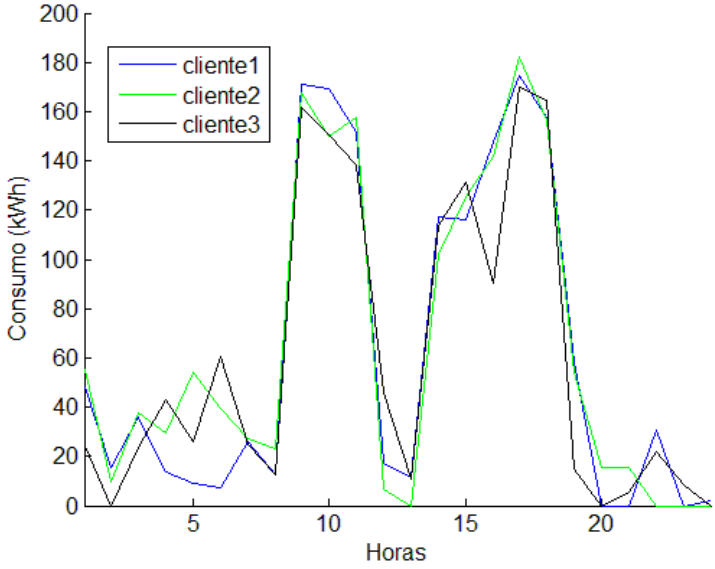


Figura 17 - Dados Simulados para o Perfil Industrial

O objetivo desse trabalho e, portanto,

Os dados de qualidade foram simulados

Desempenho	Nota
f≤56,5Hz ou f≥63,5Hz	0
57,5≤f<56,5 ou	1
58≤f<57,5 ou	2
58,5≤f <58 ou	3
59,5<f<58,6 ou	4
59,5≤f≤60,5	5

Os dados referentes ao comportamento

Os pesos α foram variados durantes os

Os limites β_1 e β_2 também precisaram

Os limiares de tolerância para o cálculo do grau de confiança, ***Qa=1, se Qárea < L1 0, se Qárea ≥ L1*** (11 e Quando o valor absoluto

da diferença entre a qualidade informada por um *Smart Meter* e a qualidade informada pelos vizinhos é maior do que um limite L2, tolerância essa determinada pela concessionária, há indicação de problema, caso contrário é uma diferença aceitável. Normalizando x_4 em Q, para facilitar a correlação entre as medidas, tem-se que:

$$\boldsymbol{Q = \begin{cases} 0, se\ x_4 < L_2 \\ 1, se\ x_4 \geq L_2 \end{cases}} \quad (13,$$

foram escolhidos como L_1=4 e L_2 =1. L_1=4 indica que 0,1,2 e 3 são notas que apontam má qualidade de rede e notas 4 e 5, uma rede de boa qualidade. L_2 =1 porque como as notas variam somente entre 0 e 5, diferenças até de uma unidade podem ser consideradas percepções semelhantes sobre a energia fornecida, mas acima disso já há indicação de divergência de opiniões. Foi atribuído o valor 3 ao parâmetro γ_d ,que determina a velocidade de decrescimento do intervalo de polling, utilizado nas simulações a seguir. Esse número foi estimado, em função do *Polling* ter começado em 15 horas.

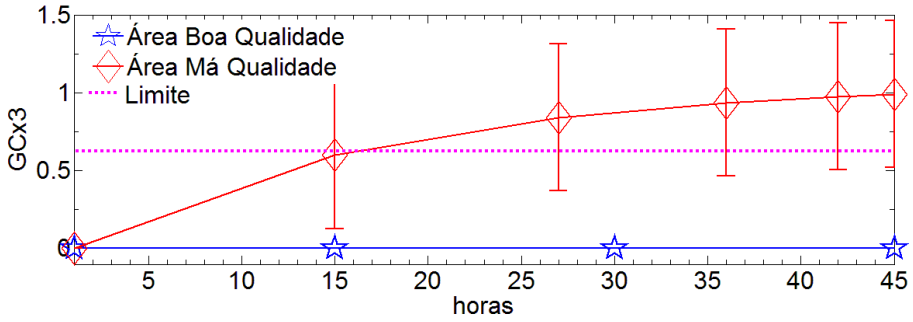
O incremento em caso de normalidade da rede, representado pelo parâmetro γ_s, não foi necessário em nenhum dos cenários simulados, mas sugere-se um valor fixo correspondente a metade do valor de γ_d , cujo impacto foi avaliado nas simulações.

6.2 Resultados

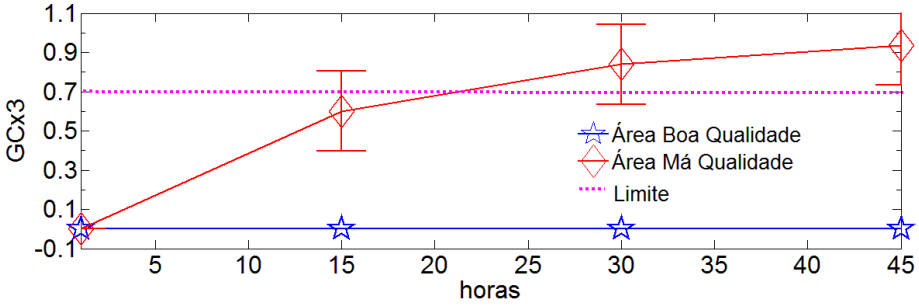
De modo a simular a eficiência do *Polling* adaptativo, foram geradas algumas simulações considerando uma área com 50 imóveis recebendo energia distribuída por um transformador, representando uma rua ou um quarteirão. 50 casas foi um número escolhido de forma aleatória, não tendo nenhuma relação formal com algum tipo de regra da Operadora de Energia. A quantidade de imóveis alimentados por um transformador depende dos cálculos de carga produzida e consumida, tipo de consumidor e outros fatores, cálculo esse que não faz parte do escopo desse trabalho.

Na maioria das simulações, considerou-se α=0,4 de modo a não se confirmar, logo nos primeiros indícios, que a área está sob suspeita, mas sim somente após algumas reincidências do problema.

Simulação 1: Na análise de uma área, o indicador GC_{x3}, conforme Figura 18 , mostra a qualidade média da percepção de qualidade dos imóveis de uma determinada área. Como se a média estiver baixa, há forte indício de problemas na área, ao contrário de indicadores de problemas em imóveis de forma individual, o α_i foi colocado em 0,6 de modo a valorizar o dado mais recente e alarmar o quanto antes, por tratar-se de um indício grave e abrangente de falha, e os limites em β_1 em 0,1 e β_2 em 0,7 cujos valores foram ajustados de forma empírica. Foram simuladas duas áreas. A primeira área com 50 clientes, considerando uma rua do Rio de Janeiro com 25 casas de cada lado e um transformador alimentando-as, com notas de média entre 4 e 5 indicando boa qualidade na área e a segunda também com 50 clientes, com média abaixo de 3 indicando problemas de queda parcial ou total no fornecimento de energia na área.



(a) *Polling* Adaptativo



(b)*Polling* Fixo

Figura 18 - Maioria dos clientes indicando problemas de qualidade na área

Agora é possível resumir o comportamento da aceleração do alarme de uma área apontando má qualidade da energia que está sendo distribuída, com a ultrapassagem do limite fixado para β_2, igual a 0,7. A partir desse limite é confirmada a existência de problema na respectiva área. O *Polling* adaptativo fez a área receber um alarme muito mais rápido do que no *Polling* fixo. O alarme foi acelerado em torno de 10%, conforme mostrado na Figura 19 - Momentos de ativação do alarme de área no uso do *Polling* adaptativo e do *Polling* fixo.

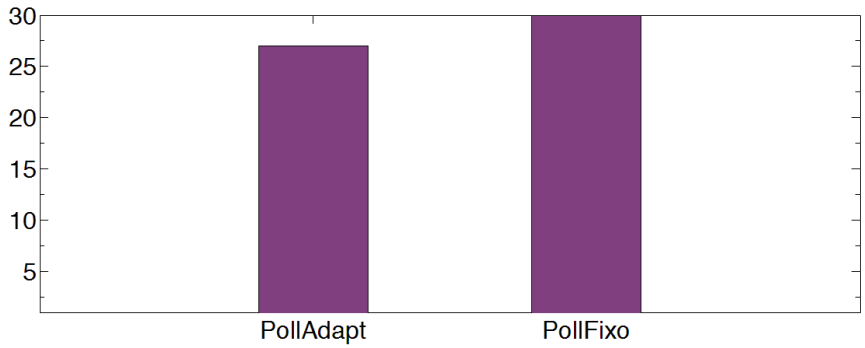
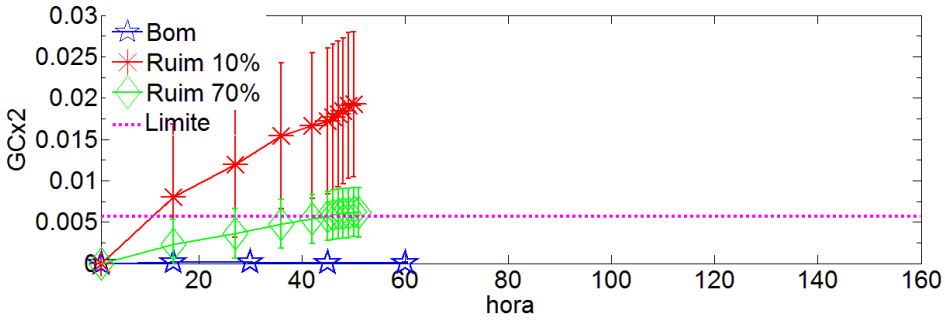


Figura 19 - Momentos de ativação do alarme de área no uso do *Polling* adaptativo e do *Polling* fixo

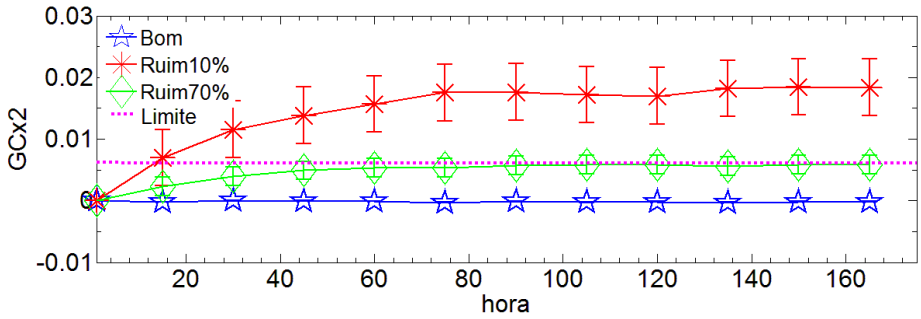
Simulação 2: O próximo parâmetro analisado foi o GC_{x2}, que representa a

diferença entre a energia provida e a energia medida na área. Para análise do indicador GC_{x2} foram analisados os dados gerados durante 7 dias. Foram comparados os dados de três áreas com diferentes tipos de clientes, mas mantendo a quantidade de 50 clientes por área, conforme simulação anterior. Área 1 com 50 clientes bons, área 2 com 49 clientes bons e um cliente com medição de consumo indicando em torno de 10% do valor consumido e área 3 com 49 clientes bons e um cliente com medição de consumo indicando em torno de 70% do valor consumido. Se fosse possível adivinhar os tipos de problemas que apareceriam, poderiam ser fixados limiares para análise diferenciada para cada tipo de problema, acelerando ainda mais a ratificação do mau comportamento de um cliente ou de uma área. Mas como essa previsão é impossível, foram utilizados os menores limiares que podem sensibilizar qualquer tipo de problema, mesmo que sem a mesma eficiência. dessa Foram utilizados os parâmetros β_1=0,002 e β_2=0,006.

A Figura 20 mostra o comportamento do grau de confiança relativo à comparação do consumo informado pelos *Smart Meters* dos clientes com o distribuído pelo transformador (indicador GC_{x2}), com aplicação de *Polling* adaptativo e depois com *Polling* fixo.



(a) *Polling* adaptativo.



(b) *Polling* fixo.

Figura 20 - Comportamento do GC_{x2} ao longo do tempo, ao se utilizar ou não o *Polling* adaptativo.

Com base nesses dados, é possível observar o impacto do comportamento da aceleração do alarme. A Figura 21 resume a emissão de alarmes com a ultrapassagem do limite fixado para β_2, 0,006. A partir desse limite é confirmada a existência de problema na área. O *Polling* adaptativo fez a área receber um alarme muito mais rápido do que o fixo. Os consumos ruins de aproximadamente 10% do esperado tiveram o alarme da área acelerado em 40% e os de 70% do consumo esperado tiveram o alarme acelerado em 57% do tempo.

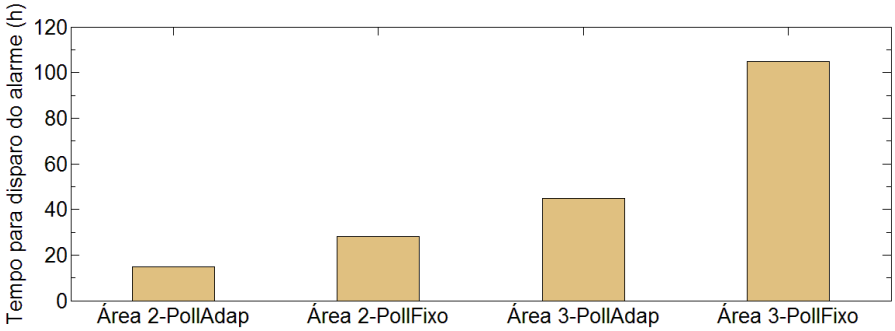
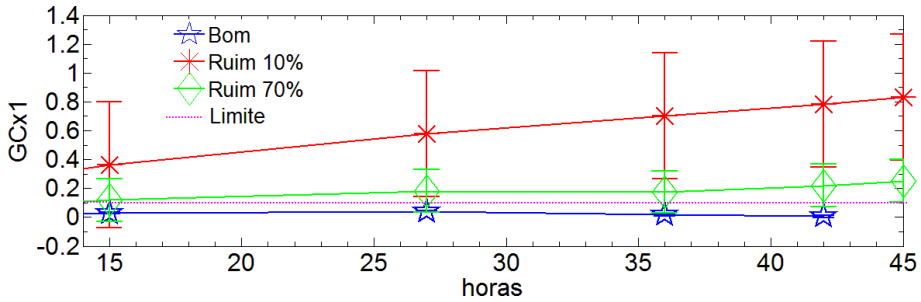


Figura 21 - Momentos de ativação do alarme da área no uso do *Polling* adaptativo e do *Polling* fixo.

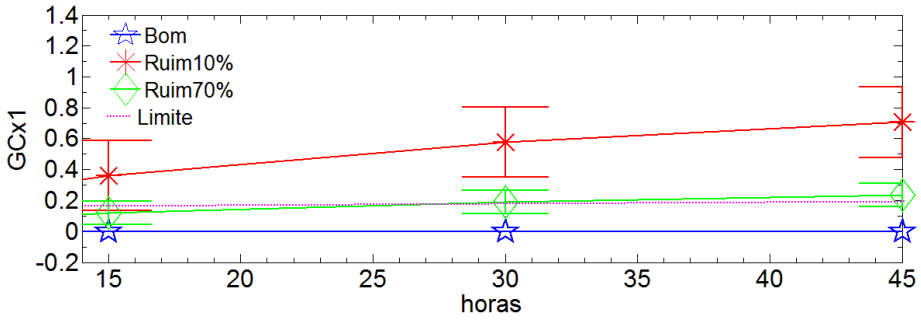
No primeiro *Polling*, ou seja, na 15a hora, o grau de confiança atingiu o limite β_1, indicando suspeita de problema na área e consequentemente o *Polling* adaptativo foi ativado e a análise por cliente começou a ser realizada em busca da possível fonte de problemas na área.

A partir da suspeita de problemas na área disparados a partir da análise dos indicadores GC_{x3} e $GC_{x2,}$ passaram a ser analisados os indicadores individuais de cliente GC_{x1}, GC_{x4} e GC_{x5}.

Simulação 3: O primeiro indicador de cliente avaliado na simulação foi o GC_{x1}. A Figura 22 mostra a evolução do grau de confiança dos três tipos de clientes com relação à medida de consumo recebida: bom, ruim 10% do consumo esperado e ruim 70% do consumo esperado. O *Polling* adaptativo começou na 15a hora, a partir da qual o indicador GC_{x1} começou a ser avaliado.



(a)*Polling* Adaptativo



(b)*Polling* Fixo

Figura 22 - Comparação do consumo medido com o consumo histórico - Indicador GC_{x1}

Agora é possível resumir o comportamento da aceleração do alarme de um cliente com mau comportamento da informação de consumo, na Figura 23 com a ultrapassagem do limite fixado para β_2=0,2. A partir desse limite é confirmada a existência de problema no respectivo cliente. O *Polling* adaptativo acelerou a identificação do cliente ofensor da área, quando o consumo esperado foi de até 70% do esperado. Em condições em que o consumo informado foi extremamente mais baixo do que o esperado, no caso da simulação 10% do esperado, os *Polling*s fixo e adaptativo se mostraram com desempenhos equivalentes. Os consumos Ruins de aproximadamente 10% do esperado tiveram o alarme da área no mesmo instante e os de 70% do consumo esperado tiveram o alarme acelerado em 7% do tempo.

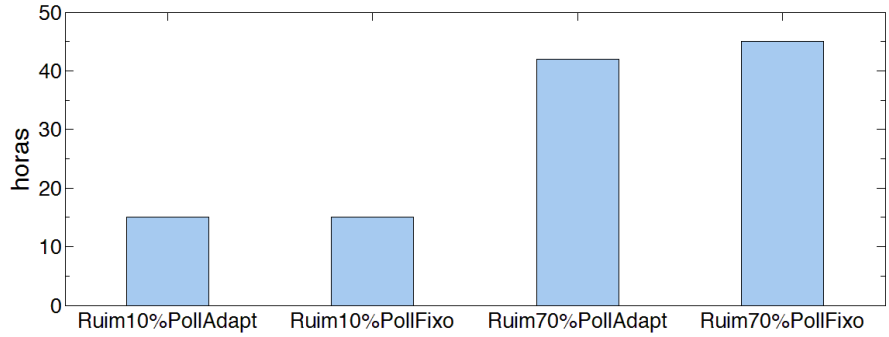
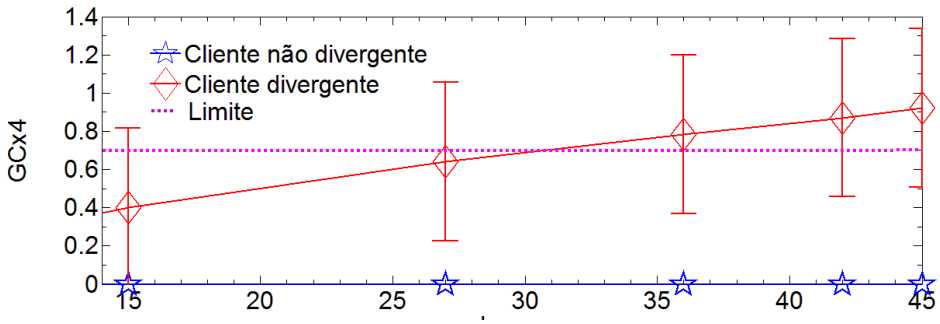
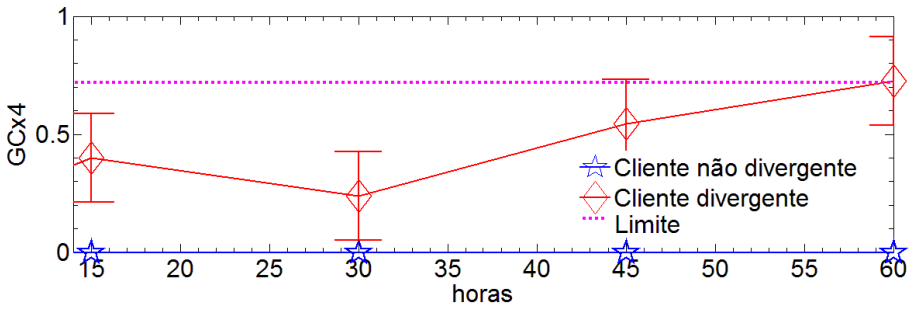


Figura 23 - Momentos de ativação do alarme de cliente no uso do *Polling* adaptativo e do *Polling* fixo.

Simulação 4: Outro indicador de cliente ativado a partir da suspeita da área é o GC_{x4}. Assim, um novo cenário foi criado para avaliação da percepção da qualidade da energia provida. A Figura 24 mostra a evolução do grau de confiança de clientes que apresentaram percepção da qualidade da energia recebida diferente dos demais da área, indicador GC_{x4}, no *Polling* adaptativo e no *Polling* fixo. Foram simuladas dois tipos clientes: um que informa qualidade compatível com a média da área (2 clientes) e outro (1 cliente) que mostra divergência de opinião da média dos demais clientes da área. Para a emissão de alarme para o cliente suspeito de falha ou fraude, foi utilizado o limite β_2=0,7.



(a) *Polling* adaptativo



(b) *Polling* Fixo

Figura 24- Comparação da percepção de qualidade de um cliente com os demais da área, quando ele tem divergência de opinião - Indicador GC_{x4}.

Agora é possível resumir o comportamento da aceleração do alarme de um cliente com mau comportamento da informação de qualidade na Figura 25 com a ultrapassagem do limite fixado para β_2, igual a 0,7. A partir desse limite é confirmada a existência de problema no respectivo cliente. O *Polling* adaptativo fez o cliente ofensor da área receber um alarme muito mais rápido do que no *Polling* fixo. A aceleração foi em torno 40%.

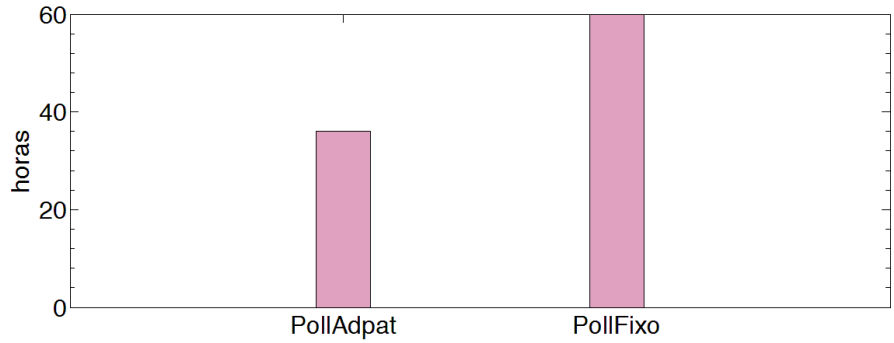
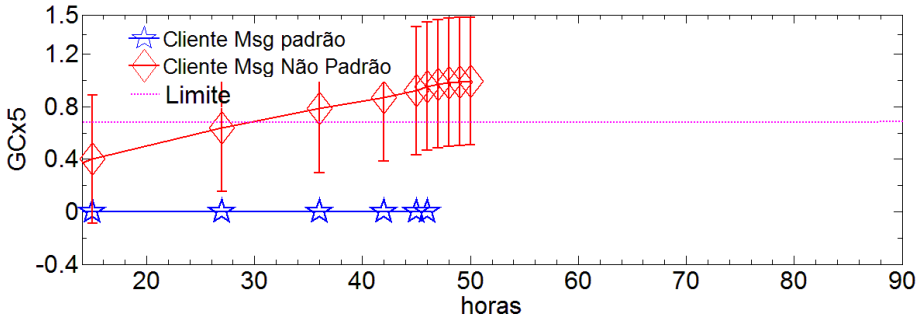
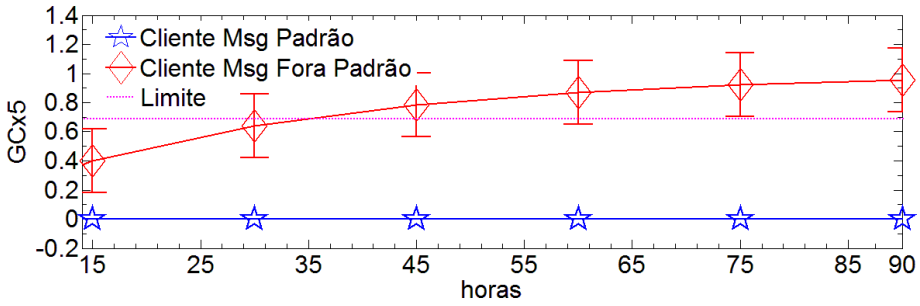


Figura 25- - Momentos de ativação do alarme de cliente no uso do *Polling* adaptativo e do *Polling* fixo

Simulação 5: A Figura 26 mostra a evolução do grau de confiança de clientes que apresentaram mensagem fora do padrão, indicador GC_{x5}, no *Polling* adaptativo e no *Polling* fixo, próximo indicador de cliente disparado em presença de problema na área. Para tanto, foi criado um novo cenário, no qual foram simulados dois clientes: um com mensagem dentro do padrão e outro com mensagem fora do padrão. Foi utilizado para disparo do alarme do respectivo cliente o limite β_2=0,7.



(a) *Polling* Adaptativo



(b)*Polling* Fixo

Figura 26- Cliente com mensagem fora do padrão - Indicador GC_{x5}

Agora é possível resumir o comportamento da aceleração do alarme de um cliente com mensagem fora do padrão na Figura 27 com a ultrapassagem do limite fixado para β_2, igual a 0,7. A partir desse limite é confirmada a existência de problema no respectivo cliente. O *Polling* adaptativo fez o cliente ofensor da área receber um alarme muito mais rápido do que no *Polling* fixo. O alarme foi acelerado em torno de 20%.

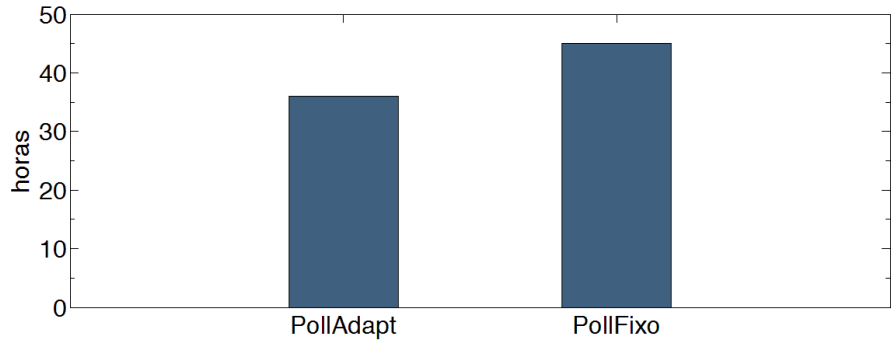


Figura 27- Momentos de ativação do alarme de cliente no uso do *Polling* adaptativo e do *Polling* fixo

Simulação 6: Uma outra análise foi feita com um cliente que apresentou consumo 70% do esperado, em um cenário com 50 clientes, sendo os demais com comportamento padrão. Foram simulados decréscimos variados no *Polling*, acelerando a frequência de coleta. A Figura 28 mostra uma coleta com *Polling* fixo e depois com aceleração da frequência de *Polling*. É possível perceber que a quanto mais se incrementa a frequência da coleta, mais rápido é o acionamento do alarme.

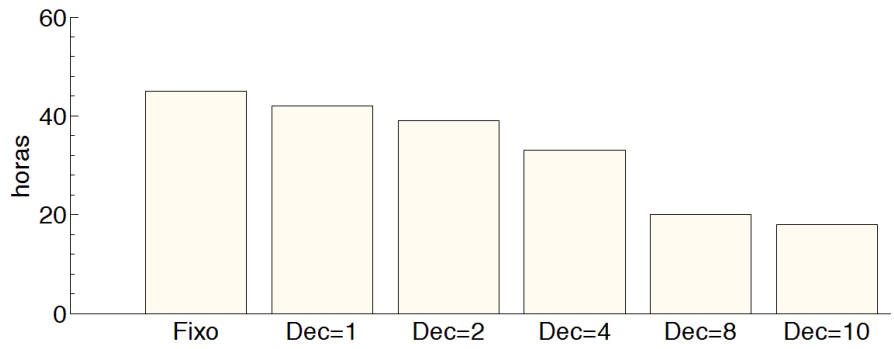


Figura 28 Impacto na variação do *Polling* para um cliente com consumo 70% do esperado

Analisando melhor a Figura 28 Impacto na variação do *Polling* para um cliente com consumo 70% do esperado. A aceleração eficiente do *Polling* adaptativo pode ser observada na Tabela 6 - aceleração em função do aumento da frequência de *Polling*.

Tabela 6 - aceleração em função do aumento da frequência de *Polling*

	fixo	dec=1	dec=2	dec=4	dec=8	dec=10
hora do alarme	45h	43h	38h	37h	22h	20h
aceleração		4,4%	15%	18%	51%	56%

Pelos resultados , observou-se que não ocorreram falso-positivos ou falso-negativos no método proposto. Em todas as simulações o incremento da frequência de *Polling* acelerou a detecção de problemas.

Trabalhos Futuros

Esse trabalho abordou a detecção de fraudes de proporções moderadas a altas, baseado em modelos de confiança que se deterioram em condições anormais de comportamento dos dados coletados dos medidores inteligentes.

Clientes que provocam fraudes sutis, de pequena variação no consumo informado pelos medidores, precisam de outras métricas de análise. Esse seria um trabalho complementar ao que foi abordado nesse documento.

Outra questão que poderia tornar-se um trabalho interessante seria a composição de novas regras e modelos estatísticos a serem aplicados a análise de outros dados gerados pelos medidores inteligentes (*Smart Meters*), em busca de variações de comportamento para a emissão de alarmes de outra natureza.

A gama de dados que os novos medidores são capazes de gerar, vem crescendo, dando margem a novas comparações e composição de novas informações úteis à operação, manutenção e administração do sistema elétrico.

Considerações Finais

Esse trabalho apresenta e analisa um modelo de confiança para detecção de fraudes, de diversas naturezas, no sistema elétrico, já se inserindo na arquitetura *Smart Grid*, a partir de pessoas mal intencionadas, que adulteram os medidores inteligentes (*smart meters*) de seus imóveis e invadem a rede de telecomunicações que suporta esse novo conceito, bem como os sistemas de pós-processamento (SCADA).

O modelo proposto analisa os dados gerados pelos medidores inteligentes, por meio de diversos tipos de comparações. Comparação com perfis, retirados dos dados históricos dos clientes e armazenados em bancos de dados da concessionária de energia. comparação entre a energia produzida , pela concessionária e por produtores independentes e energia consumida. Comparação da percepção dos clientes de uma área quanto à qualidade da energia fornecida. Enfim, comparações estas que extraem informações úteis de dados coletados individualmente dos diversos *smart meters*. Após comparações dos dados coletados, o nível de confiança precisa ser estabelecido. Para isso faz-se uso do cálculo estatístico, chamado média móvel exponencial ponderada para o cálculo da confiança, utilizado para a identificação de tendências de um conjunto de dados ao longo do tempo. O grau de confiança deteriora em presença de comportamentos não esperados e incrementa em presença de uma rede bem comportada. A partir da deterioração do grau de confiança acima de limiares pré-definidos,é provocada a emissão de alarmes e o acionamento da equipe de manutenção em busca de fraudes e falhas, em campo.

O modelo se limita à análise de fraudes de moderada à alta intensidade, ficando de fora, para um estudo posterior, fraudes sutis, de pequena variação nos dados enviados para processamento.

Também foi proposto um modelo de coleta de dados dos smart meters, controlado pelo coletor, em forma de *polling* e não de envio de forma espontânea, com controle de periodicidade em função da necessidade de coletas mais frequentes. Na presença de suspeita de fraude ou falha no sistema, a periodicidade de coleta é intensificada em busca do elemento

ofensor. Quando o sistema em condições de normalidade, a periodicidade de coleta é desacelerada, diminuindo a quantidade de dados a serem processados.

Várias simulações foram realizadas e estão mostradas em forma de gráficos autoexplicativos, nos quais é possível verificar a eficiência do modelo proposto.

Ficou evidente que, na maioria dos casos, não é eficaz que a suspeita se concretize logo na primeira coleta, pois problemas temporários na rede de comunicações ou instabilidade momentânea nos elementos eletrônicos, incluindo sensores e medidores, podem gerar dados falsos que logo nas próximas coletas são corrigidos, desviando as equipes técnicas de campo para serem utilizados em áreas de real necessidade. O sistema de confiança promove a investigação da real mudança de comportamento de uma informação, comparando com dados coletados anteriormente. Permite também que se opte em dar mais atenção ao um dado novo ou a um comportamento histórico e bem conhecido. O sistema de confiança proposto reduz o número de falso positivos na detecção de problemas e de fraudes no sistema.

Os indicadores gerados pelo sistema de confiança dão a oportunidade da concessionária identificar previamente o tipo de problema no cliente antes da sua atuação em campo para manutenção, pois mostram a possível causa raiz do alarme.

A introdução do *polling* adaptativo, que intensifica a frequência da coleta de dados, em momentos de suspeita de problemas, acelera o acionamento de alarme para a concessionária. Por outro lado, quando não ativado devido às condições normais do sistema, diminui o volume de dados a serem processados. Há, portanto, um controle dos dados que realmente precisam ser tratados e em que momento eles precisam ser investigados com maior frequência.

Na maioria dos cenários das simulações, o *polling* adaptativo é satisfatório, acelera a emissão de alarmes entre 7 e 57% do tempo, dependendo do caso, que se alcançaria com o *polling* fixo. Porém, quanto maior é a diferença entre o dado lido e o valor esperado, mais rapidamente o grau de confiança se deteriora e o alarme é gerado, até mesmo na primeira coleta, ou seja, podendo chegar ao ponto de não haver diferença entre o *polling* fixo e o adaptativo. Mas, até mesmo esse comportamento é

satisfatório, como por exemplo, quando a média das notas auferidas pelos *smart meters* dos imóveis aponta para uma queda de energia ou péssima qualidade da energia fornecida. Nesse caso, o grau de confiança é rapidamente denegrido, de modo a gerar o alarme à concessionária. Esse evento é apontado pela maioria dos consumidores e requer providências urgentes. Diferenças grandes entre consumos dos clientes de uma área com o auferido pelo medidor do transformador, também mostram problemas graves em uma grande região, não se mostrando como distúrbios momentâneos que podem ocorrer com um determinado *smart meter* e de logo retorno à normalidade.

As propostas desse trabalho em muito se assemelham à vida, em que se observa o comportamento de uma pessoa suspeita de alguma má conduta, procura-se obter mais informações sobre ela comparando com ações anteriores e em caso de ratificação da suspeita, ela é excluída da sociedade ou é levada para tratamento.

A simulação mostrou que os objetivos propostos foram alcançados, o sistema de confiança e o *polling* adaptativo se mostraram muito eficientes pois reduzem as abordagens desnecessárias em campo para manutenção, permitem a identificação dos clientes causadores do problema da área, aceleram a identificação de problemas e minimizam o processamento de dados dos sistemas SCADA.

Bibliografia

1. **Ferreira, Omar Campos.** *O Sistema Elétrico Brasileiro.* 2011.
2. **Pedro Henrique V. Guimarães, Andrés Murillo, Martin Andreoni,Diogo M.F.Mattos, Lyno Henrique G.Ferraz, Fabio Antonio V.Pinto, Luís Henrique M.K.Costa e Otto Carlos M.B.Duarte.** *Comunicação em Redes Elétricas Inteligentes: Eficiência, Confiabilidade, Segurança e Escalabilidade.* Universidade Federal do Rio de Janeiro e Centro Federal de Educação Tecnológica Celso Suckov da Fonseca RJ. Rio de Janeiro : s.n., 2013.
3. **Secco, Alexandre.** *Blecaute.* s.l. : Abril - Veja on-line, 2001.
4. **INEE.** Geração Distribuída e Cogeração. *Instituto Nacional de Eficiência Energética.* [Online] 2013. [Citado em: 02 de Dezembro de 2013.] http://www.inee.org.br/forum_ger_distrib.asp.
5. **Aneel.** Agência Nacional de Energia Elétrica. [Online] 2013. [Citado em: 10 de novembro de 2013.] http://www.aneel.gov.br.
6. **ANEEL.** *Agência Nacional de Energia Elétrica - Indicadores.* 2013.
7. **COPEL.** Pura Energia. [Online] 2012. [Citado em: 03 de Dezembro de 2013.] http://www.copel.com.
8. **André Trigueiro.** g1.globo.com. *Búzios aplica projeto para se tornar uma cidade inteligente.* [Online] Globo, 13 de Dezembro de 2012. [Citado em: 11 de Janeiro de 2014.] http://g1.globo.com/jornal-da-globo/noticia/2012/12/buzios-aplica-projeto-para-se-tornar-uma-cidade-inteligente.html.
9. **GE Reports.** Countries for Smart Grid Investment. [Online] 2010. [Citado em: 02 de Dezembro de 2013.] http://www.gereports.com/top-10-countries-for-smart-grid-investment/.
10. **Duarte, Otto Carlos Muniz Bandeira.** *Segurança em Smart Grids.* Universidade Federal do Rio de Janeiro. Rio de Janeiro : s.n., 2012.
11. **Rede Inteligente.** Consumo Inteligente. [Online] 19 de Agosto de 2009. [Citado em: 12 de Janeiro de 2014.] http://www.redeinteligente.com/2009/08/19/consumo-inteligente/.
12. **Lisa Arthur.** What is Big Data. *Forbes.* [Online] Forbes, 2014. [Citado em: 11 de Janeiro de 2014.] http://www.forbes.com/sites/lisaarthur/2013/08/15/what-is-big-data/.
13. **SAS.** O que é Big Data? *Soluçõe Big Data.* [Online] 2011. [Citado em: 11 de Janeiro de 2014.] http://www.sas.com/offices/latinamerica/brazil/solucoes/bigdata/.
14. **Nery, Carmen.** *rio info 2013.* [Online] 2013. [Citado em: 4 de Dezembro de 2013.] http://www.rioinfo.com.br/ons-usa-big-data-para-controlar-sistema-eletrico-nacional/.
15. **Pereira, Roberto Martins e Spritzer, Ilda Maria de Paiva Almeida.** *AUTOMAÇÃO E DIGITALIZAÇÃO EM SUBESTAÇÕES DE ENERGIA.*

Campus Ponta Grossa - Paraná : s.n., 2007. pp. 147-160. ISSN 1808-0448 / v. 03, n. 04: p. 147-160, 2007.

16. **Duailibe, Paulo.** *Subestações: Tipo, Equipamentos e Proteção.* Centro federal de Educação Tecnológica Celso Suckow da Fonseca. 1999.
17. **Yona Lopes, Ricardo Henrique Frazao Franco, David Acosta Molano, Margareth Apostolo dos Santos, Flavio Galvao Calhau, Carlos Alberto Malcher Basto, Joberto S. B. Martins, Natalia Castro Fernandes.** *Smart Grid e IEC 61850: Novos Desaos.* XXX SIMPOSIO ´ BRASILEIRO DE TELECOMUNICAC¸OES - SBrT'12, 13-16 DE SETEMBRO DE 2012, BRAS´ILIA, DF. Brasília : s.n., 2012.
18. **ONS.** O Setor Elétrico. *Operador Nacional do Sistema Elétrico.* [Online] 2013. [Citado em: 06 de 11 de 2013.] http://www.ons.org.br/institucional_linguas/modelo_setorial.aspx.
19. **Leão, Professora Ruth.** *Geração, transmissão e Distribuição de Energia Elétrica.* Ceará : Universidade Federal do Ceará, 2009.
20. **ABRADEE.** A Distribuição de Energia. [Online] Associação Brasileira de Distribuidores de Eneria Elétrica, 2013. [Citado em: 03 de Dezembro de 2013.] http://www.abradee.com.br/setor-de-distribuicao/a-distribuicao-de-energia.
21. **Carmo, Ubiratan.** *Smart Grid: Conceitos, arquitetura e impacto na automação de subestações.* XI Seminário Técnico de Proteção e Controle. Santa Catarina : s.n., 2012.
22. **ENEL.** Smart Grids - Intelligent networks driving the future. [Online] 2012. [Citado em: 21 de Outubro de 2013.] http://www.enel.com/it-IT/doc/innovation.
23. **Kevin Bullis .** Microgrid Mantém a Energia Local, Barata e Confiável. *Technology Review.* [Online] Opinno, 24 de Julho de 2012. [Citado em: 12 de Janeiro de 2014.] http://www.technologyreview.com.br/read_article.aspx?id=40882.
24. **Grupo de Trabalho criado pela Portaria No 440, de 15 de abril de 2010 envolvendo várias empresas.** *Smart Grid.* Brasília : Ministério de Minas e Energia, 2010.
25. **ANEEL, Agência Nacional de Energia Elétrica -.** *Acesso e Uso dos Sistemas de Transmissão e de Distribuição.* Brasília : s.n., 2005.
26. **Ecil Informática Indústria e Comércio LTDA.** Medição Inteligente - Smart Grid. *http://www.ecilenergia.com.br/download/Medidores.pdf.* [Online] 2013. [Citado em: 23 de Novembro de 2013.] http://www.ecilenergia.com.br/download/Medidores.pdf.
27. **Cirilo, Carlos Eduardo.** *Computação Ubíqua: definição, princípios e tecnologias.* São Carlos, São Paulo : Departamento de Computação – Universidade Federal de São Carlos.
28. **Sloman, Tyrone Grandison e Morris.** *A Survey of Trust in Internet.* 2000. pp.

2-16.

29. **Hongbing Huang, Guiming Zhu, Shiyao Jin.** *Revisiting Trust and Reputation in Muiti-agent Systems.* 2008. pp. 424-429. 978-0-7695-3290-5.
30. **Wei Liu, Yang-Bin Tang, Huai-Min Wang,Gang Lu.** *"An Ordering-Based Approach to the Evaluation of Trust Systems".* 27-29 Maio2011. pp. 520-524.
31. **Gutsher, A.** *"Possibilities and Limitations of modeling Trust and Reputation".* Kaiserlautern : s.n., 2008.
32. **Jordi Sabater, Carles Sierra.** *"Review on computational trus".* 2005. pp. 33-60.
33. **Ari Halbertstadt, Mojdeh Mohtashemi, Lik Mui.** *Notions of Reputation in Multi-agents Systems: a Review.* Bologna : s.n., 2002. pp. 280-287.
34. **Mui, Lik.** *Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks.* Massachusetts Institute of Technology. Massachusetts : s.n., 2002.
35. **Sergio Marti, Hector Garcia-Molina.** *Taxonomy of Trust:Categorizing P2P Reputation Systems.* 2006. pp. 472-484.
36. **Donovan Artz, Yolanda Gil.** *A Survey of Trust in Computer-Science and the Semantic Web.* 2007. pp. 58-71.
37. **Chong, Soon-Keow, Deakin Univ., Geelong e Abawajy, J.H.** *"Feedback Credibility Issues In Trust Management Systems.* 2007. pp. 387-394.
38. **Pedro B. Velloso1, Rafael P. Laufer2 , Otto Carlos M. B. Duarte3 , Guy Pujolle1.** *Analise de um modelo de confiança para redes móveis ad hoc.* França EUA e Brasil : UFRJ,UCLA, UPMC, 2008.
39. **Natalia Castro Fernandes, Marcelo Duffles Donato Moreira, Otto Carlos Muniz Bandeira Duarte.** *Safeguarding ad hoc networks with a self-organized membership control system.* Rio de Janeiro : s.n., 2013. pp. 2656–2674.
40. **Yan Lindsay Sun¤, Zhu Hany, Wei Yuy and K. J. Ray Liuy.** *A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks.* USA : Universities of Rhode Island Kinsgston and of Maryland, College Park, 2006.
41. **Lyno Henrique G. Ferraz, Natalia C. Fernandes, Pedro B. Velloso.** *Um Mecanismo de Exclusão acurado baseado em Confiança para Controle de Acesso em Redes Ad Hoc.* 2011. pp. 395-408.
42. **Coates, G.M., Hopkinson, K.M., Graham, S.R. e Kurkowski, S.H.** Collaborative, Trust-Based Security Mechanisms for a Regional Utility Intranet. *Power Systems, IEEE Transactions on (Volume:23 , Issue: 3).* Agosto de 2008, pp. 831-844.
43. **Coates, G.M., Hopkinson, K.M.; Graham, S.R.; Kurkowski, S.H.** *A Trust System Architecture for SCADA Network Security.* 2010. pp. 158 - 169. 0885-8977.
44. **Alan T. Sherman, Dhananjay Phatak, Bhushan Sonawane, Vivek G. Relan.**

"Location Authentication throuugh Power Line Communiction Design, Protocol and Analysis of a New Out-Of-Band Strategy. *Power Line Communications and Its Application (ISPLC).* 28-31 de Março de 2010, pp. 279-284.

45. **Juan M. Carlos Gonzalez, Kenneth M.Hopkinson, Gabriel H.Greve, Matthew D. Compton, Joseph Wilhelm, Ryan W.Thomas.** *Optimization of Trust System Placement for Power Grid Security and Compartmentalization.* USA : IEEE Transactions on Power Systems, 2011.
46. **Yichi Zhang, Lingfeng Wang, Weiqing Sun.** Trust System design Optimization in Smart grid Network Infrastructure. *IEEE Transactions on Smart Grid.* 1 de março de 2013, pp. 184-195.
47. **Young-Jin Kim, Vladimir Kolesnikov, Hongseok Kim, Marina Thottan,Murray Hill.** SSTP a Scalable and Secure Transport Protocol for Smart Grid Data Collection. *Communication Networks for Smart Grid IEEE Smart Grid Comm.* 2011, pp. 162-166.
48. **J.Rosenberg, H.Schulzrinne.G.CAmarillo, A.Johnston, J.Peterson, R.Sparks,M.Handley, E.Schooler.** SIP: Session Initiation Protocol. June de 2002.
49. **Seth, S. e Gankotiya, A.** *Denial of Service Attacks and Detection Methods in Wireless Mesh Networks.* Chandigarh, India : IEEE Xplore, 2010. 978-1-4244-5956-8.
50. **Vieira, Dalton.** Médias Móveis – Aprenda como utilizá-las para auxiliar suas operações. *daltonvieira.com.* [Online] 2013. [Citado em: 17 de novembro de 2013.] http://daltonvieira.com/medias-moveis-aprenda-como-utilizar-as-medias-moveis-para-auxiliar-suas-operacoes.
51. **Lenz, André Luis.** Conversores Bidirecionais Integrados CA/CC e CC/CC para EVs e PHEVs. *Veículos Elétricos - Os carros verdes - Emissão "Zero" de carbono Tecnologias e Empreendimentos.* [Online] 2012. [Citado em: 10 de outubro de 2013.] http://automoveiseletricos.blogspot.com.br/2012/07/conversores-bidirecionais-integrados.html.
52. **José Ângelo Cagnon, Ivaldo de Domenico Valarelli, Ricardo Martini Rodrigues.** Gestão Energética em Indústrias Madeireiras. *Scielo Proceedings.* [Online] 2006. [Citado em: 24 de Novembro de 2013.] http://www.proceedings.scielo.br/.
53. **Mohammad Esmalifalak, Huy Nguyen, Rong Zheng, and Zhu Han.** Stealth False Data Injection using Independent Component Analysis in Smart Grid. *Cyber and Phisical Security and Privacy IEEE Smart Grid Comm.* 2011, pp. 244-248.
54. **JWG34/35.11, Members of.** *Protection using Telecommunications.* Cigré. 2000.
55. **Sven Teske, Greenpeace Internacional.** *Revolução Energética - A caminho do*

Desenvolvimento Limpo. Rio de Janeiro : s.n., 2013.

56. **Netto, Ezequiel de O. P., Barbosa, Thiago A. e Carvalho, Fabrício B. S. de.** *Rede de Comunicação de Medidores Inteligentes sem Fio.* Universidade Estadual de Feira de Santana e Universidade Federal da Paraíba. Feira de Santana e Paraíba : s.n., 2013.
57. **Chiganer, Luis, et al.** *A reforma do setor elétrico brasileiro - aspectos institucionais.* Scielo Proceedings. Rio de Janeiro : s.n., 2002.
58. **Line & Ground.** PowerPrimer. [Online] 2013. [Citado em: 05 de Dezembro de 2013.] http://powerprimer.wordpress.com/2013/03/29/han-wan-fan-nan-pan-lan/.
59. **Célio Bermann, Paula Franco Moreira,Roberto Kishinami,Oriana Rey,Philip M. Fearnside,Brent Millikan,Wilson Cabral de Sousa,Ricardo Baitelo,Ligia Pitta Ribeiro,Cássio Franco Moreira,Pedro Bara Neto,Heather Rosmarin.** *O Setor elétrico brasileiro e a sustentabilidade no século 21 - Oportunidades e Desafios.* Brasília : s.n., 2012.
60. **ORACLE.** Oracle e Big Data - Grandes Dados pa a Empresa. [Online] 2013. [Citado em: 03 de Dezembro de 2013.] http://www.oracle.com/br/technologies/big-data/index.html.
61. **Sarvapali D. Ramvhurn, Dong Huynh, Nicholas R.Jennings.** *"Trust in multi-agent systems".* 2004. pp. 1-25.
62. **Audun Josang, Roslan Ismail e Colin Boyd.** *"A Survey of trust and reputation systems for online service provision".* 2007. pp. 618-644.