MARCELO ZANETTI

SISTEMA DE IDENTIFICAÇÃO DE CONSUMIDORES FRAUDULENTOS EM REDES ELÉTRICAS INTELIGENTES

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Doutor em Informática.

CURITIBA

2017

MARCELO ZANETTI

SISTEMA DE IDENTIFICAÇÃO DE CONSUMIDORES FRAUDULENTOS EM REDES ELÉTRICAS INTELIGENTES

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Doutor em Informática.

Área de Concentração: Ciência da Computação
Orientador: Prof. Dr. Edgard Jamhour
Co-orientador: Prof. Dr. Marcelo Eduardo Pellenz

CURITIBA

2017

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central

Z28s
2017

Zanetti, Marcelo
Sistema de identificação de consumidores fraudulentos em redes elétricas inteligentes / Marcelo Zanetti; orientador: Edgard Jamhour; co-orientador: Marcelo Eduardo Pellenz. – 2017.
237 f. : il.; 30 cm

Tese (doutorado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2017
Bibliografia: 1125-132

1. Medidores elétricos. 2. Energia elétrica – Consumo. 3. Fraude. I. Jamhour, Edgard. II. Pellenz, Marcelo Eduardo. III. Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Informática. IV. Título.

CDD 20. ed. – 621.37

Pontifícia Universidade Católica do Paraná
Escola Politécnica
Programa de Pós-Graduação em Informática

PUCPR
GRUPO MARISTA

ATA DE SESSÃO PÙBLICA

DEFESA DE TESE DE DOUTORADO Nº 50/2017

PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA – PPGIa
PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ - PUCPR

Em sessão pública realizada às 09h30 de 14 de Dezembro de 2017, no Auditório Guglielmo Marconi – Bloco 8, ocorreu a defesa da tese de doutorado intitulada **"Sistema de Identificação de Consumidores Fraudulentos em Redes Elétricas Inteligentes"** elaborada pelo aluno **Marcelo Zanetti**, como requisito parcial para a obtenção do título de **Doutor em Informática**, na área de concentração **Ciência da Computação,** perante a banca examinadora composta pelos seguintes membros:

Prof. Dr. Edgard Jamhour (orientador) - PPGIa/PUCPR

Prof. Dr. Marcelo Eduardo Pellenz – PPGIa/PUCPR

Prof. Dr. Manoel Camillo de O. Penna Neto- PPGIa/PUCPR

Prof. Dr. Eduardo Parente Ribeiro–UFPR

Prof. Dr. Voldi Costa Zambenedetti - PUCPR

Após a apresentação da tese pelo aluno e correspondente arguição, a banca examinadora emitiu o seguinte parecer sobre a tese:

Membro	Parecer	
Prof. Dr. Edgard Jamhour	(X) Aprovada	( ) Reprovada
Prof. Dr. Marcelo Eduardo Pellenz	(X) Aprovada	( ) Reprovada
Prof. Dr. Manoel Camillo de O. Penna Neto	(X) Aprovada	( ) Reprovada
Prof. Dr. Eduardo Parente Ribeiro	(X) Aprovada	( ) Reprovada
Prof. Dr. Voldi Costa Zambenedetti	(X) Aprovada	( ) Reprovada

Portanto, conforme as normas regimentais do PPGIa e da PUCPR, a tese foi considerada:

(X) **APROVADO**
(aprovação condicionada ao atendimento integral das correções e melhorias recomendadas pela banca examinadora, conforme anexo, dentro do prazo regimental)

( ) **REPROVADO**

E, para constar, lavrou-se a presente ata que vai assinada por todos os membros da banca examinadora. Curitiba, 14 de Dezembro de 2017.

Prof. Dr. Edgard Jamhour

Prof. Dr. Marcelo Eduardo Pellenz

Prof. Dr. Manoel Camillo de O. Penna Neto

Prof. Dr. Eduardo Parente Ribeiro

Prof. Dr. Voldi Costa Zambenedetti

Dedicatória

Dedico este trabalho a todos aqueles que me apoiaram de forma direta ou indireta. Em especial a minha mãe e minha noiva.

Agradecimentos

Primeiramente agradeço a Deus, que me deu força para superar os obstáculos que surgiram durante a realização deste trabalho.

Agradeço a minha mãe pelo apoio e incentivo nos estudos. Obrigado por todo o aporte, sem você nada disso teria sido possível!

Ao meu pai (*in memorian*) que sei que de onde estiver sempre olhou por mim e fez com que esse momento se tornasse realidade.

A minha noiva, que esteve comigo nessa jornada sempre proferindo incentivos e não me deixando desanimar. Obrigado pelo companheirismo e por compreender os momentos que não conseguimos ficar juntos, ou ainda, ficamos juntos, mais cada um em seu computador estudando.

Ao meu orientador, Dr. Edgard Jamhour, pela amizade, dedicação, ensinamentos e paciência no desenvolvimento desta pesquisa. Agradeço imensamente! Nunca esquecerei de toda a ajuda e tempo dedicado pelo professor para que esse trabalho chegasse ao seu final.

Aos demais professores do Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná, em especial aos professores do grupo de Redes de Computadores e Telecomunicações, obrigado pelo auxílio durante esta caminhada.

À secretária do PPGIa, Cheila, pela amizade, atenção e auxílio durante o doutorado.

À Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES e a Fundação Araucária pelo auxílio financeiro por dois anos no desenvolvimento desta pesquisa.

À Universidade Federal da Fronteira Sul por permitir meu afastamento por dois anos das minhas atividades profissionais para que eu pudesse me dedicar exclusivamente ao doutorado.

E finalmente, agradeço a todas as pessoas as quais não citei aqui, mas que me apoiaram ao longo desta caminhada, obrigado por terem contribuído de alguma forma para que este momento se tornasse realidade.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Quadros

Lista de Abreviaturas

ABNT	Associação Brasileira de Normas Técnicas
ACM	*Association for Computing Machinery*
ANEEL	Agência Nacional de Energia Elétrica
AM	Aprendizado de Máquina
AMI	*Advanced metering infrastructure*
ARMA	*Auto regressive moving average models*
ANSI	*American National Standards Institute*
BMU	*Best Matching Unit*
CER	*Commission for Energy Regulation*
CODI	Comitê de Distribuição
CUSUM	Método de soma cumulativa
CVLR-ETDM	*Categorical Variable-Enhanced Linear Regression based scheme for Detection of Energy Theft and Defective Smart Meters*
DBSCAN	*Density-based spatial clustering of applications with noise*
DC	*Data Concentrator*
DTW	*Dynamic time warping*
ELM	*Extreme learning machine*
ERD	Energia roubada detectada
GMMD	*Gaussian-Mixture Model-based Detection*
IDS	Sistema de Detecção de Intrusão
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
IP	*Internet Protocol*
FCM	Fuzzy C-Means
FDI	*False* data *injection*
FDM	*Fraud detection model*
FP	Falso Positivo
FN	Falso Negativo
GLR	*Generalized likelihood ratio*
GPS	*Grid-Placed Sensor*
HAN	*Home Area Network*
LR-ETDM	*Linear Regression-based scheme for Detection of Energy Theft and Defective Smart Meters*
LSE	*Linear system of equations*
LU	*Lower upper*
MBT	Medidores de baixa tensão
M2M	Comunicação máquina a máquina
MOA	*Massive Online Analysis*
NAN	*Neighborhood Area Network*
NIST	*National Institute of Standards and Technology*
NTL	*Non-Technical Losses*
OPF	*Optimum-path Forest*
PCA	*Principal Component Analysis*
POMDP	*Partially observable Markov decision process*
PNT	Perdas não-técnicas
PT	Perdas Técnias
RBF	*Radial-Basis Function*

REIs	Redes Elétricas Inteligentes
RLS	*Recursive Least Square*
RMS	*Root Mean Square*
ROC	*Receiver operating characteristic*
SDP	*Semi-definite programming*
SG	*Smart Grid*
SM	*Smart Meter*
SOM	*Self-Organized Maps*
SVM	*Support Vector Machines*
TFP	Taxa de Falso Positivo
TL	Tensão de Leitura
TN	Tensão Nominal
TVP	Taxa de Verdadeiro Positivo
VC	Vida Curta
UC	Unidade Consumidora
VPN	Valor Preditivo Negativo
VPP	Valor Preditivo Positivo
VN	Verdadeiro Negativo
VP	Verdadeiro Positivo
WAN	*Wide-Area Network*

Resumo

Este trabalho contribui com o desenvolvimento de um sistema de identificação de consumidores de energia elétrica fraudulentos, com base nas medidas de consumo coletadas pela infraestrutura avançada de medição em redes elétricas inteligentes. A distribuição de energia elétrica envolve perdas técnicas e não-técnicas. Injeção de Dados Falsos de consumo de energia originada pelos consumidores são uma maneira de causar perdas não-técnicas de energia. Nesse trabalho são caracterizadas diferentes técnicas de Injeção de Dados Falsos, que podem ser utilizadas pelos consumidores em redes elétricas inteligentes para ocultar o seu real consumo de energia. A busca por consumidores fraudulentos é desencadeada quando ocorre uma inconsistência entre a energia fornecida pela rede de distribuição secundária e a relatada pelos medidores inteligentes. Uma abordagem inovadora é utilizada no sistema proposto, onde as medidas de consumo armazenadas pouco antes e depois da detecção de uma inconsistência são comparadas para detectar uma fraude. O sistema proposto mostra que é possível utilizar apenas um pequeno conjunto de medidas recentes para definir o perfil de consumo de um consumidor e detectar consumidores fraudulentos. Esta abordagem permite que o sistema proposto aponte mudanças naturais no comportamento de consumo dos consumidores e também ajuda a preservar a privacidade dos mesmos. O sistema proposto pode ainda ser ajustado, utilizando um procedimento de otimização que maximiza uma função objetivo sujeita a restrições nas taxas de verdadeiros positivos ou falsos positivos.

Palavras-chave: Infraestrutura avançada de medição, medidores inteligentes, perdas técnicas de energia, perdas não-técnicas de energia, injeção de dados falsos, roubo de energia, perfil de consumo de vida curta, detecção de fraude, clusterização.

Abstract

This work contributes to the development of an identification system of fraudulent electric power consumers, based on consumption measures collected by the advanced metering infrastructure in smart grids. The distribution of electric energy involves technical and non-technical losses. False Data Injection of energy consumption originated by consumers is a way to cause non-technical energy losses. In this work different techniques of false data Injection are characterized, which can be used by consumers in smart grid to hide their actual energy consumption. The search for fraudulent consumers is triggered when there is an inconsistency between the energy supplied by the low voltage distribution grid and the reported by the smart meters. An innovative approach is used in the proposed system, where the consumer measures stored shortly before and after detection of an inconsistency are compared to detect a fraud. The proposed system shows that is possible to use only a small set of recent measures to define the consumption profile of a consumer and detect fraudulent consumers. This approach allows the proposed system to point to natural changes in consumers' consumption behavior and also helps to preserve their privacy. The proposed system can still be adjusted using an optimization procedure that maximizes an objective function subject to restrictions on the rates of true positives or false positives.

Keywords: Advanced metering infrastructure, smart meters, technical losses, non-technical losses, false data injection, energy theft, consumption of short-lived, fraud detection, clustering.

Capítulo 1

Introdução

A eletricidade precisa ser produzida a partir de todos os outros tipos de energia e transportada aos consumidores no mundo inteiro por meio de sistemas elétricos complexos, compostos de três etapas: geração, transmissão e distribuição. Perdas de energia nesse sistema complexo podem ocorrer. Segundo Gandhi e Bansal [1] existem dois tipos de perdas: técnicas e não-técnicas. As perdas técnicas não podem ser evitadas, uma vez que estão associadas às leis físicas e podem ser causadas por fontes de naturezas diferentes, embora, em muitos casos, possam ser minimizadas durante as fases de geração, transmissão e distribuição. As perdas não-técnicas são caracterizadas pela utilização ilegal de energia elétrica. Essas perdas são causadas por conexões não autorizadas, consumo de energia não contabilizada e fraudes em instrumentos de medição. No Brasil estima-se que as perdas chegaram a 20,2% da energia gerada em 2015 [2]. Conforme Vermeulen [3] as perdas não-técnicas na África do Sul têm chegado a 32% da energia entregue pela empresa City Power Johannesburg. De acordo com Northeast Group [4] o mundo está perdendo cerca de $89,3 bilhões com o roubo de eletricidade anualmente.

Nas redes tradicionais de energia elétrica é difícil e oneroso identificar perdas não-técnicas, uma vez que é necessário inspecionar linhas de transmissão e unidades consumidoras [5]. Com o desenvolvimento das Redes Elétricas Inteligentes (*Smart Grid* - SG) e a introdução da Infraestrutura Avançada de Medição (*Advanced Metering Infrastructure* - AMI) [6] será possível realizar o monitoramento, a análise, controle e comunicação dentro da cadeia de suprimentos para ajudar a melhorar a eficiência, e maximizar a transparência e a confiabilidade da cadeia de fornecimento de energia e caracterizar padrões de consumo dos consumidores finais. Todavia, em comparação com as redes elétricas tradicionais, onde a adulteração só poderia ser realizada fisicamente, a AMI possibilita adulterações das medições através da conexão remota ao medidor e durante a transmissão das medições a central de monitoramento. Segundo Mo *et al.* [7] em AMI a integridade da informação (consumo de energia da Unidade Consumidora (UC)) é o ponto mais importante, e é preciso pensar urgentemente em sistemas de detecção de consumidores fraudulentos.

Este trabalho tem como principal contribuição identificar consumidores fraudulentos que causam perdas não-técnicas de energia utilizando técnicas de injeção de dados falsos (*False data injection* - FDIs) para ocultar o seu real consumo de energia. No sistema proposto um medidor coletivo é utilizado para mensurar o consumo total de energia das UCs conectadas a um transformador de distribuição. O valor mensurado pelo medidor coletivo é comparado com o total de energia relatado pelos medidores individuais dos consumidores ligados ao medidor coletivo. Se a comparação do somatório das leituras informadas for diferente da leitura do medidor coletivo, levando em consideração as perdas técnicas, os consumidores ligados ao medidor coletivo devem ser investigados. Para investigar os consumidores são propostas estratégias de identificação de perfis de consumo utilizando algoritmos de aprendizagem de máquina.

Além disso, o sistema proposto é inovador ao utilizar um pequeno conjunto de medições recentes para criar o perfil de consumo de um consumidor, o que faz com que o sistema se adapte a mudanças de perfil de um consumidor de forma célere. Os trabalhos encontrados na literatura ao utilizarem uma grande quantidade de dados históricos para realizar o treinamento dos sistemas propostos acabam por não identificarem vários tipos de fraudes recentes, uma vez que, estas podem ser ocultadas por um perfil antigo de consumo. O sistema proposto também busca manter a privacidade do consumidor ao utilizar um pequeno conjunto de medições, e não utilizando outras informações das unidades consumidoras como, quantidades de eletrodomésticos nas residências ou horários em que a unidade consumidora apresenta um maior ou menor consumo de energia.

1.1. Objetivo Geral

Desenvolver um sistema de identificação de consumidores de energia fraudulentos em Redes Elétricas Inteligentes com base no seu perfil de consumo.

1.1.1. Objetivos Específicos

Os objetivos específicos são descritos a seguir:

- Realizar o levantamento bibliográfico de métodos de detecção consumidores finais fraudulentos em Redes Elétricas Inteligentes;
- Caracterizar perdas técnicas e não-técnicas de energia elétrica;
- Desenvolver uma estratégia para estimar perdas técnicas e detectar anomalias em um subsistema secundário de distribuição;
- Caracterizar técnicas de Injeção de Dados Falsos que podem ser utilizadas por consumidores finais para causar perdas não-técnicas;
- Modelar o efeito das técnicas de Injeção de Dados Falsos;
- Caracterizar perfis de consumo das unidades consumidoras utilizando um conjunto de algoritmos supervisionados e não-supervisionados de aprendizagem de máquina;
- Extrair um conjunto de características dos perfis de consumo de energia dos consumidores finais que serão utilizadas para criar estratégias de detecção de FDIs;
- Desenvolver estratégias de detecção de FDIs específicas para cada um dos algoritmos de aprendizagem de máquina utilizados no presente trabalho;
- Criar um sistema robusto em relação as taxas de falsos positivos;
- Avaliar o desempenho das estratégias de detecção de FDIs propostas.

1.2. Contribuições

As principais contribuições deste trabalho são resumidas da seguinte forma:

- Propor um sistema para detectar unidades consumidoras que estão roubando energia. O sistema utiliza um medidor coletivo junto a um transformador para monitorar divergências entre a leitura do medidor coletivo e o somatório das leituras informadas pelos consumidores ligados ao medidor coletivo. Essa solução faz com que o sistema apenas busque por consumidores fraudulentos quando de fato estiverem ocorrendo furtos de energia. Dessa forma, o sistema diminui a taxa de falsos alarmes;
- Propor uma estratégia para estimar as perdas técnicas entre o medidor coletivo e os medidores individuais das unidades consumidoras;

- Determinar as condições de anomalia do subsistema secundário, isto é, quando a diferença entre os valores reportados pelos medidores individuais e coletivos excederem as perdas técnicas e os erros de precisão dos medidores;
- Definir um sistema que se adapta rapidamente a mudanças no perfil de consumo dos consumidores utilizando um pequeno conjunto de medidas recentemente coletadas pela AMI;
- Avaliar o sistema em termos de quantidade de energia furtada identificada e seu custo operacional, ao invés de apenas considerar as taxas de detecção de ataques e taxas de falso positivo, como a maioria dos trabalhos observados na literatura.

1.3. Publicações

Até o momento dois artigos foram publicados com os resultados deste trabalho de pesquisa. Sendo o mais recente publicado em uma revista e o anterior em uma conferência.

- Artigo publicado em revista:
  - Nome da revista: *IEEE Transactions on Smart Grid*;
  - Título do artigo: *A Tunable Fraud Detection System for Advanced Metering Infrastructure using Short-Lived Patterns;*
  - Qualis: A1.

- Artigo publicado em conferência:
  - Nome da conferência/local/data: *International Conference on Computer Safety, Reliability and Security*, 2016 (SAFECOMP), realizada em Trondheim, Noruega de 21 a 23 de setembro de 2016;
  - Título do artigo: *A New SVM-Based Fraud Detection Model for AMI;*
  - Qualis: B1.

1.4. Organização do Trabalho

Este trabalho está organizado em nove capítulos, conforme descrição a seguir:

O Capítulo 2 apresenta a fundamentação teórica relacionada às Redes Elétricas Inteligentes e a aprendizagem de máquina. Esse capítulo inicia conceituando as Redes Elétricas Inteligentes e a Infraestrutura Avançada de Medição. Na sequência perdas técnicas e não-técnicas de energia são definidas. Por fim, são apresentadas técnicas de aprendizagem de máquina que podem ser utilizadas para identificar consumidores fraudulentos. O Capítulo 3 apresenta o estado da arte sobre sistemas de detecção de consumidores fraudulentos. Este capítulo é dividido em duas sessões principais, sendo que a primeira apresenta os trabalhos baseados em estados da rede de energia. A segunda seção apresenta os principais trabalhos que utilizam perfil de consumo, e que estão relacionados com o sistema proposto. O Capítulo 4 apresenta a abordagem metodológica e define as estratégias utilizadas para a execução do trabalho. O Capítulo 5 apresenta o sistema de identificação de consumidores fraudulentos que está sendo proposto nesta pesquisa. Em um primeiro momento é apresentado o detector de anomalias proposto para identificar anomalias em um subsistema secundário. Em um segundo momento são apresentadas as estratégias propostas para identificar consumidores fraudulentos em um subsistema anômalo. O Capítulo 6 apresenta a preparação da base de dados utilizada nos testes e a estimação e validação dos parâmetros utilizados pelo detector de anomalias. No Capítulo 7 é realizada a afinação e validação dos parâmetros do detector de consumidores fraudulentos proposto e a comparação do mesmo com os mais recentes trabalhos encontrados na literatura. O Capítulo 8 apresenta os testes de integração do detector de anomalias de subsistemas com o detector de consumidores fraudulentos. Por fim, no Capítulo 9 são apresentadas as considerações finais, que concluem este trabalho, apresentando suas contribuições, limitações da pesquisa e trabalhos futuros.

1.5. Considerações

Este capítulo apresentou a introdução, os objetivos da pesquisa, as publicações e organização dos capítulos da tese.

Capítulo 2

Fundamentação Teórica

Nesse capítulo é apresentada uma visão geral sobre os principais conceitos utilizados no desenvolvimento desse trabalho e exposto os vários métodos que podem ser utilizados por consumidores fraudulentos para ocultar o real consumo de energia.

2.1. Redes Elétricas Inteligentes (Smart Grid)

As Redes Elétricas Inteligentes (REIs) (*Smart Grid* – SG) [8] devem ser entendidas mais como um conceito do que uma tecnologia ou equipamentos específicos. Existem várias definições para o conceito de redes elétricas inteligentes, mas a grande maioria converge para o uso de tecnologias de automação, computação e comunicação bidirecional de forma integrada em todo o sistema de energia elétrica, desde a geração até os pontos finais de consumo [9]. Segundo [10] e [11] uma REI inteiramente implementada possui as seguintes características:

- Permite a participação dos consumidores: os consumidores podem participar de uma forma mais ativa, ajudando a equilibrar a oferta e a demanda, alterando a forma como eles usam e compram energia;
- Acomoda todas as opções de geração e armazenamento: uma rede inteligente acomoda não apenas a geração centralizada, mas também microgeração distribuída. Várias formas de geração e armazenamento poderão ser alocadas na rede, o que possibilita aos consumidores a geração de sua energia, bem como a venda do excedente;
- Mercados e serviços: beneficia mercados competitivos de energia, criando oportunidades para que os consumidores escolham entre serviços concorrentes;
- Fornece energia com qualidade para diferentes necessidades: nem todas as empresas, e certamente nem todos os consumidores residenciais, precisam da

mesma qualidade de energia. Em uma rede elétrica inteligente é possível fornecer preços diferenciados dependendo da qualidade da energia desejada;

- Otimiza a utilização de ativos e a eficiência operacional: uma rede inteligente otimiza o uso de seus ativos, permitindo que toda a capacidade dos ativos seja utilizada, bem como avaliada continuamente. A eficiência pode ser otimizada com a manutenção baseada em alertas, que sinaliza a necessidade da manutenção de equipamentos de forma preventiva;
- Tolerância a ataques externos: capacidade de mitigar e resistir a ataques físicos e ciberataques;
- Menor impacto ambiental: reduzindo perdas e utilizando fontes renováveis e de baixo impacto ambiental;
- Auto-recuperação a perturbações, ataques e catástrofes naturais: a auto-recuperação refere-se à capacidade de um sistema reagir a eventos inesperados reparando-se automaticamente ou isolando os elementos problemáticos, enquanto o resto do sistema opera normalmente. Essas ações de auto-recuperação resultam na redução da interrupção do serviço aos consumidores e auxiliam as prestadoras de serviço a gerenciarem melhor suas infraestruturas e seus consumidores.

O Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology* - NIST) dos Estados Unidos propôs a divisão das REIs em sete domínios. Cada domínio é definido como sendo um grupo de atores com objetivos semelhantes, com requisitos de comunicação e características similares, podendo englobar outros domínios e subdomínios. Os atores são os dispositivos, equipamentos, sistemas computacionais ou aplicativos que tomam decisões e trocam informações necessárias para execução das aplicações. As aplicações são as tarefas executadas por um ou mais atores dentro de um domínio. A comunicação entre os domínios é estabelecida através de interfaces. As interfaces são as conexões elétricas e/ou conexões de comunicação. Cada uma destas interfaces pode ser uni ou bidirecional [12]. Os sete domínios são ilustrados na Figura 1 e explicados a seguir:

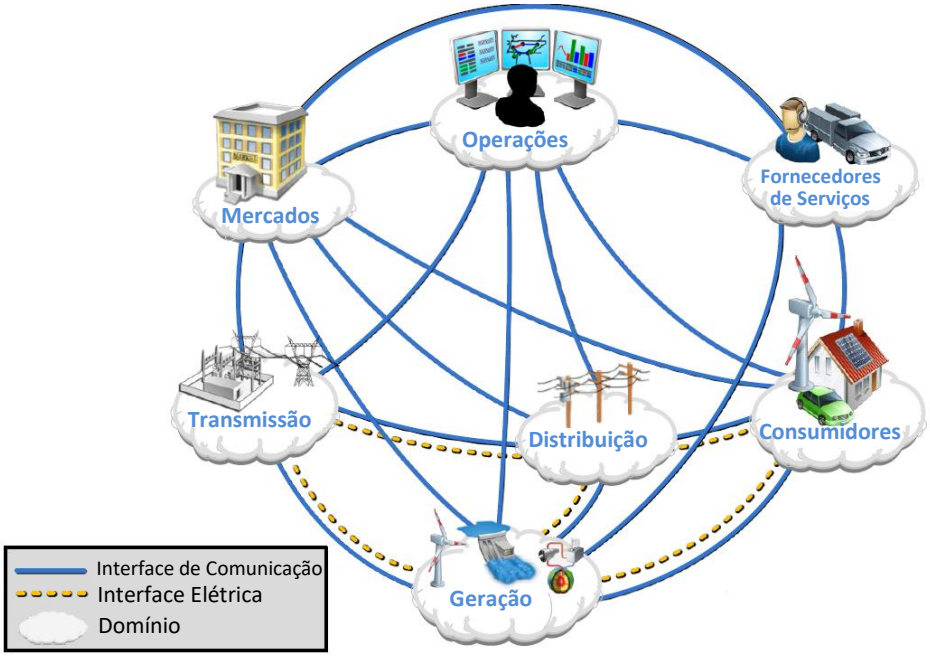

Figura 1: Modelo Conceitural da REI.
Adaptado de [12].

- Domínio de Geração: responsável pela produção em massa de eletricidade a partir de fontes renováveis e não renováveis. O domínio de geração também pode armazenar energia para posterior utilização;
- Domínio de Transmissão: responsável por transportar a energia através de grandes linhas de transmissão. Esse domínio transporta a energia por longas distâncias, desde a geração à distribuição;
- Domínio de Distribuição: é o domínio que contém as subestações, responsáveis por realizar a distribuição da energia para o consumidor final. Podem atuar também na geração e armazenamento de energia elétrica;
- Domínio de Consumo: os consumidores finais (unidades consumidoras) que utilizam a energia disponibilizada pelas subestações de energia. Também podem gerar, armazenar e gerenciar o uso da energia;
- Domínio de Mercado: possui uma interface com todos os outros domínios de forma a certificar-se que há um equilíbrio entre a oferta e a procura de energia e os valores cobrados. Também controla a troca de energia excedente produzida pelo consumidor final e o Domínio de Distribuição;
- Domínio de Operação: executa funções de gestão para o bom funcionamento do sistema de energia que incluem: monitoramento, controle e gerenciamento de falhas da rede, estatísticas operacionais e relatórios. Enquanto a maioria destas funções é

geralmente de responsabilidade de um agente regulamentador, muitas delas podem ser terceirizadas para provedores de serviços;

- Domínio de Fornecedores de Serviços: controla todas as operações de serviços terceirizados. Estes serviços vão desde processos tradicionais como: faturamento e gerenciamento da conta do consumidor para clientes de serviços avançados, bem como geração e gestão de energia em unidades consumidoras.

Nas REIs os medidores analógicos serão substituídos pelos medidores inteligentes (*Smart Meter* - SM) no domínio de Consumo. Com o medidor inteligente, grandezas elétricas, como tensão e frequência, também podem ser medidas e monitoradas em tempo real. Segundo os autores [13], [14] e [15] um medidor de energia inteligente deve apresentar as seguintes capacidades, além de atender as normas do Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO) [16]:

- Registrar em tempo real a energia consumida ou gerada;
- Armazenar informações de leituras;
- Possibilitar a leitura local e remota;
- Capturar eventos, como o estado do dispositivo e da qualidade da energia (queda da tensão);
- Suportar comunicação bidirecional com o fornecedor de energia;
- Tarifação dinâmica;
- Troca de fornecedor de energia;
- Possibilitar o controle remoto do medidor e até mesmo o corte de fornecimento de energia remotamente;
- Ser interoperável dentro de um ambiente de REI e com outros sistemas.

Para que a maioria das funcionalidades dos medidores inteligentes possam ser utilizadas pelas concessionárias de energia é necessária uma Infraestrutura Avançada de Medição (*Advanced Metering Infrastructure* - AMI). A Figura 2 ilustra a arquitetura AMI.

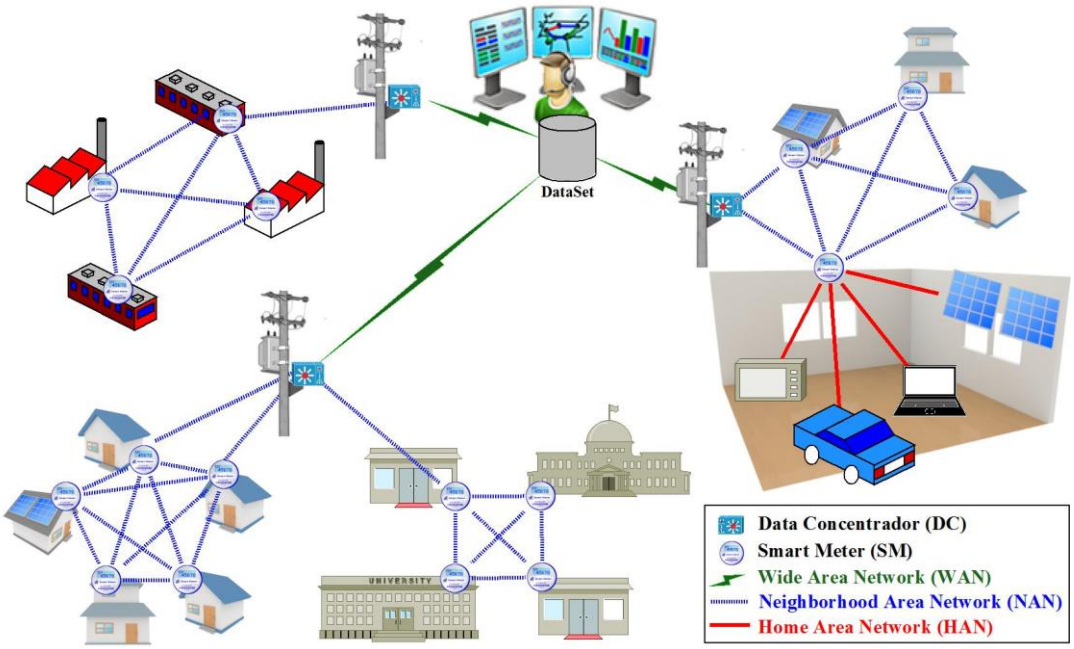

Figura 2: Arquitetura AMI.

A arquitetura de AMI tem como principal elemento o medidor inteligente, e é estruturada de forma hierárquica. Cada camada da hierarquia corresponde a um trecho no qual as informações deverão trafegar. A seguir são descritas as camadas da arquitetura de AMI [17]:

- Rede de área local (*Home Area Network* - HAN): abrange a unidade consumidora com um medidor inteligente instalado. Os aparelhos elétricos podem se conectar ao medidor inteligente permitindo ao consumidor monitorar e controlar o uso de energia;
- Redes de área vizinhança (*Neighborhood Area Network* - NAN): cobrem as informações concentradas nos diversos medidores que estão conectados a um Concentrador de Dados (*Data Concentrator* - DC). O DC assume a tarefa de agregar os dados de medição dos medidores inteligentes;
- Redes de área ampla (*Wide Area Network* - WAN): é a rede que conecta os diversos concentradores de dados ao centro de controle.

Conforme Zhang *et al.* [18] a AMI é essencial em uma REI. A AMI recolhe automaticamente dados dos medidores inteligentes em intervalos de tempo e os envia para o centro de controle [19]. Isso resultará em uma grande quantidade de dados disponíveis na central de controle que podem ser analisados com diferentes finalidades, como por exemplo, identificar fraudes de energia.

Além da coleta automática de dados, a AMI ainda fornece comunicação de duas vias, permitindo que informações e/ou comandos possam ser enviados para as unidades consumidoras com vários fins, como por exemplo, informações de preços cobrados em determinados horários do dia e desconexão de serviços de forma remota [20].

Esse trabalho tem seu foco nas medições coletadas das unidades consumidoras e informadas a central de controle, com o objetivo de identificar perdas não-técnicas de energia. A seguir são explicados os tipos de perdas de energia e onde as mesmas podem ocorrer em uma rede REI.

2.2. Perdas de Energia

Assim como outras cadeias produtivas, os sistemas elétricos de potência possuem perdas em cada uma de suas etapas. A energia medida pelas distribuidoras nas unidades consumidoras sempre será inferior à energia gerada. Segundo [21] de um ponto de vista operacional, as perdas de energia elétrica são um custo inevitável que precisam ser devidamente tratadas para se evitar uma demanda de carga adicional no sistema.

As perdas de energia em sistemas elétricos podem ser classificadas de diversas maneiras de acordo com as diferentes fontes que decorrem. De acordo com Alam *et al.* [22], as perdas são divididas em perdas técnicas (PT) e perdas não-técnicas (PNT). A primeira é o resultado da resistência inerente de condutores elétricos, o que faz com que a energia elétrica seja transformada em calor e ruído quando a corrente flui através dos condutores e dos equipamentos da rede. E as perdas não-técnicas têm a ver com a energia que é fornecida para consumo, mas que não é paga.

Além disso, é possível caracterizar as perdas em função do tipo de rede e nível de tensão que ocorrem. Segundo o Comitê de distribuição de energia elétrica (CODI) [23] as perdas podem ser divididas em perdas de geração, transmissão e distribuição. A soma dessas perdas dá-se o nome de perdas globais, ou seja, é a diferença entre a energia gerada e a energia consumida. Assim, as perdas globais podem ser definidas como, equação (1):

$$Perdas_{Globais} = Perdas_{Ger} + Perdas_{Transm} + Perdas_{Distr} \quad (1)$$

Ou

$$Perdas_{Globais} = Energia_{Gerada} - Energia_{Consumida} \quad (2)$$

Onde:

- $Perdas_{Ger}$: perdas causadas devido ao processo de transformação da energia primária em energia motriz, e em seguida, em energia elétrica;
- $Perdas_{Transm}$: são aquelas que ocorrem entre o local de geração da energia elétrica até o limite dos sistemas de distribuição;
- $Perdas_{Distr}$: aquelas que ocorrem dentro do próprio sistema de distribuição.

O presente trabalho tem seu foco nas perdas técnicas e não-técnicas no sistema de distribuição. Perdas técnicas são detalhadas na seção 2.2.1 e perdas não-técnicas na seção 2.2.2.

2.2.1. Perdas Técnicas

Perdas técnicas são inerentes ao transporte da energia elétrica na rede, relacionadas à transformação de energia elétrica em energia térmica nos condutores, perdas nos núcleos dos transformadores, perdas dielétricas, etc. Podem ser entendidas como o consumo dos equipamentos responsáveis pela distribuição de energia [24]. O nível das perdas técnicas depende diretamente do tipo de equipamento utilizado, tecnologia e topologia da rede, além da qualidade da manutenção do sistema elétrico. Além disso, as perdas podem ser categorizadas com base em cada segmento onde ocorrem.

De acordo com [21] as perdas de transmissão são medidas com precisão através de medição contínua. Por outro lado, as perdas de distribuição (redes secundárias) são estimadas, com um considerável grau de incerteza. De fato, em redes secundárias na maioria das vezes o operador do sistema de distribuição não tem informações sobre suas condições de operação. Isso pode ser justificado pelo grande número de redes secundárias que podem ser operadas no sistema de distribuição, o que exigiria um investimento maciço na implantação de sensores de medição e infraestrutura de comunicação. Em outros níveis da rede, como, média tensão e alta tensão, o monitoramento é necessário a fim de assegurar o fornecimento da energia e controlar impactos referentes a ações externas aos sistemas (por exemplo, falhas) nos ativos. Consequentemente, os operadores do sistema de distribuição redirecionam seus investimentos para as redes de média e alta tensão [25]. Nesse trabalho, o foco são as perdas nas redes secundárias, que podem estar relacionadas a:

- Condutores elétricos utilizados;
- Queda de tensão;

- Sistema trifásico desequilibrado;
- Baixo fator de potência;
- Imprecisão dos medidores.

A seguir uma breve descrição sobre cada um desses tópicos é apresentada.

2.2.1.1 Condutores Elétricos

Em qualquer sistema de energia elétrica, nota-se a presença de elementos condutores, que interligam os equipamentos elétricos às fontes e aos demais componentes do circuito. Os condutores transportam a corrente elétrica que transita da fonte para as cargas. Existem vários critérios para a classificação dos cabos e fios, como, material condutor, bitola, isolação e impedância. Quando se fala em impedância, todo condutor apresenta certa impedância elétrica, que depende da composição do material condutor, bem como de sua forma (bitola e comprimento). A resistência de um condutor é dada pela segunda lei de Ohm, equação (3): [26]

$$\mathrm{R} = \frac{p * l}{\mathrm{A}} \tag{3}$$

Onde:

- R: resistência, medida em ohm (Ω);
- p: resistividade do material condutor e, ohm * mm^2/m;
- l: comprimento do condutor (m);
- A: área de secção transversal (mm^2).

Sempre que uma corrente elétrica flui através de um material que apresenta alguma impedância, a energia elétrica é transformada em energia térmica, causando o aquecimento dos condutores. Esse fenômeno de conversão de energia elétrica em térmica é conhecido como efeito Joule e pode ser determinada através da seguinte equação (4): [27]

$$ED = R * I^2 * \Delta t \tag{4}$$

Onde:

- ED: é o calor gerado por uma corrente eficaz;

- R: resistência elétrica do condutor, medida em ohm (Ω);
- I: intensidade de corrente que percorre o condutor, medida em Ampères (A);
- Δt: intervalo de tempo da passagem da corrente.

Outro fator de influência é a temperatura do condutor metálico. À medida em que o condutor metálico é aquecido, sua resistência ao fluxo de corrente elétrica aumenta, acarretando em perdas técnicas de energia. As perdas que estão relacionadas com o aumento da temperatura dos condutores devido a corrente são mais significativas em momentos de pico, quando a carga do sistema é maior [28].

O aumento da temperatura nos condutores também pode ocorrer devido a condições climáticas.

2.2.1.2 Queda de tensão

O nível de tensão em cada local depende principalmente de dois fatores: a quantidade de energia reativa produzida ou consumida na vizinhança, e da quantidade da queda de tensão associada às perdas resistivas. Nos sistemas de distribuição radial, o efeito da queda de tensão domina [29]. A tensão diminui da fonte de alimentação para a extremidade do sistema de distribuição. A queda de tensão é descrita pela equação (5): [30]

$$V = R * I \tag{5}$$

Onde:

- V: diferença de potencial elétrico (ddp, ou tensão) entre suas extremidades, medida em Volt (V);
- R: resistência, medida em ohm (Ω);
- I: intensidade da corrente que flui através do condutor, medida em Ampères (A).

Na prática, a queda de tensão nos sistemas de distribuição é bastante significativa, especialmente para alimentadores longos. Reconhecendo que é fisicamente impossível manter um perfil perfeitamente plano, as diretrizes operacionais nos Estados Unidos prescrevem uma tolerância de ± 5% da tensão nominal [31]. Esta gama aplica-se a todos os sistemas de

transmissão e distribuição, até ao nível do consumidor. Por exemplo, uma unidade consumidora nominalmente recebendo 120V deve esperar medir entre 114 e 126V.

A Figura 3 ilustra o problema da queda de tensão ao longo de um alimentador (*freeder*). Se o alimentador é muito longo, a queda de tensão pode exceder a janela de tolerância, de modo que, se a primeira unidade consumidora está recebendo não mais do que 126V, a última receberia menos de 114V. A fim de manter um nível de tensão admissível ao longo de todo o comprimento de um alimentador, pode ser necessário intervir e aumentar a tensão em algum ponto o caminho. Além disso, a queda de tensão vária com a carga, com isso, o impulso pode ter de ser ajustado em diferentes momentos [29].

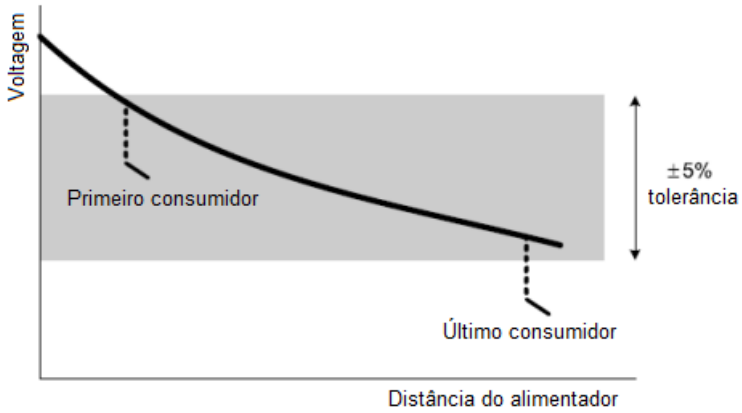

Figura 3: Queda de tensão ao longo de um alimentador.
Adaptado de [31].

No Brasil os Procedimentos de Distribuição de energia elétrica no sistema elétrico nacional - PRODIST [32] são elaboradas pela Agência Nacional de Energia Elétrica (ANEEL) [33] que normatiza e padroniza as atividades técnicas relacionadas ao funcionamento e desempenho dos sistemas de distribuição de energia elétrica. No módulo 8 [34] do PRODIST, são definidos níveis de tensão e valores de referência relativos à conformidade da tensão. Para cada nível de tensão são determinados limites para garantir a qualidade do fornecimento quanto à conformidade de tensão. Esses limites efetivamente medidos (Tensão de Leitura – TL) são baseados nos valores de Tensão Nominal (TN), conforme apresentado no Quadro 1. Assim, para cada valor de TN há uma faixa de tensão de leitura considerada adequada, com intervalos superiores e inferiores considerados precários e críticos. Por exemplo, para uma ligação trifásica com TN de 127V a faixa de tensão considerada adequada é de $116V \leq TL \leq 133V$.

Quadro 1: Tensões nominais (TN) padronizadas no Brasil.

Tensão Nominal (TN)		**Adequado**	**Precário**	**Crítico**
Ligação	**Volts (V)**			
Monofásica	**254/ 127**	(232≤TL≤264)/ (116≤TL≤132)	(220≤TL<232 ou 264<TL≤269)/ (109≤ TL<116 ou 132<TL≤140)	(TL<220 ou TL>269)/ (TL<109 ou TL>140)
	440/ 220	(402≤TL≤458)/ (201≤TL≤229)	(380≤TL<402 ou 458<TL≤466)/ (189≤ TL<201 ou 229<TL≤233)	(TL<380 ou TL>466)/ (TL<189 ou TL>233)
Trifásica	**220/ 127**	(201≤TL≤231)/ (116≤TL≤133)	(189≤TL<201 ou 231<TL≤233)/ (109≤TL<116 ou 133<TL≤140)	(TL<189 ou TL>233)/ (TL<109 ou TL>140)
	380/ 220	(348≤TL≤396)/ (201≤TL≤231)	(327≤TL<348 ou 396<TL≤403)/ (189≤TL<201 ou 231<TL≤233)	(TL<327 ou TL>403)/ (TL<189 ou TL>233)

Fonte: Adapatado de [34].

2.2.1.3 Desequilíbrio de fases

As linhas secundárias são normalmente alimentadas por um sistema trifásico constituído por três condutores de fase e um neutro. Este sistema incorpora o uso de três ondas senoidais balanceadas que operam na mesma frequência e amplitude, mas, defasadas $120^{\underline{0}}$ entre si. Para que um sistema trifásico esteja em um estado equilibrado são considerados os valores de corrente e tensão em cada fase como sendo a soma de três vetores ($\bar{V}$), tal que (6): [35]

$$\bar{V}_1 + \bar{V}_2 + \bar{V}_3 = 0 \qquad (6)$$

Um sistema será considerado equilibrado quando a soma dos três vetores for nula. No entanto, a carga elétrica destas redes é inerentemente desequilibrada devido à distribuição irregular de cargas por fase, que variam constantemente ocasionadas pela inserção e/ou retirada de cargas. Assim, as tensões e correntes das redes secundárias são também desequilibradas, ou seja, as amplitudes são diferentes, e o defasamento é diferente de $120^{\underline{0}}$. Isto leva ao aparecimento de uma corrente ($\bar{I}_0$) no condutor de neutro, expressa por (7): [30]

$$\bar{I}_0 = \bar{I}_1 + \bar{I}_2 + \bar{I}_3 \qquad (7)$$

Entre as causas do desequilíbrio de um sistema trifásico, a principal é a ligação desproporcional de cargas monofásicas, tais como, sistemas de iluminação e motores monofásicos, nas suas três fases de forma aleatória.

2.2.1.4 Fator de Potência

Define-se como Fator de Potência (FP) a razão entre a potência ativa (P) e a aparente (S), equação (8): [27]

$$FP = \frac{P}{S} \quad (8)$$

O fator de potência indica qual porcentagem da potência total fornecida é efetivamente utilizada como potência ativa. Assim, o fator de potência mostra o grau de eficiência do uso dos sistemas elétricos. Valores altos de fator de potência (próximos a 1,0) indicam uso eficiente da energia elétrica, enquanto valores baixos evidenciam seu mau aproveitamento, além de representar uma sobrecarga para todo o sistema elétrico.

Os baixos valores de fator de potência são decorrentes de quantidades elevadas de energia reativa. Essa condição resulta em aumento da corrente total que circula nas redes de distribuição de energia elétrica. Como essa corrente cresce com o excesso de energia reativa, estabelece-se uma relação direta entre o incremento das perdas técnicas e o baixo fator de potência, provocando pelo aquecimento de condutores e equipamentos [23].

O aumento da corrente devido ao excesso de energia reativa também leva a quedas de tensão acentuadas, podendo ocasionar a interrupção do fornecimento de energia elétrica e a sobrecarga em certos elementos da rede. Esse risco é, sobretudo acentuado durante os períodos nos quais a rede é fortemente solicitada. As quedas de tensão podem provocar a diminuição da intensidade luminosa nas lâmpadas e o aumento da corrente nos motores [23].

No Brasil a Agência Nacional de Energia Elétrica (ANEEL) [33] estabeleceu que o fator de potência nas unidades consumidoras deve ser superior a 0,92.

2.2.1.5 Medidor de energia

Nenhum medidor de energia é capaz de fornecer leituras de consumo com cem por cento de precisão. O Instituto Americano de Padrões Nacionais (*American National Standards Institute* (ANSI)) através das normas ANSI C12.1 [36], C12.10 [37] e C12.20 [38] estabelece os aspectos físicos e critérios de desempenho aceitáveis para medidores de energia. Sempre que

existirem diferenças, entre as normas, a C12.20 deve ser prevalecer. Na norma C12.20 são estabelecidas três classes de precisão para os medidores de energia. As três classes são:

- Classe .5 - com uma precisão de ± 0,5%;
- Classe .2 - com uma precisão de ± 0,2%;
- Classe .1 - com uma precisão de ± 0,1%.

É importante ressaltar que a classe .1 foi adicionada a norma C12.20 em 2015, antes de 2015 só eram previstas as classes .5 e .2.

No Brasil, o INMETRO visando à incorporação dos medidores e a sua padronização publicou a Portaria Inmetro nº 587, de 05 de novembro de 2012 [16]. Na portaria são estabelecidas quatro classes de limite de erro percentual admissível para os medidores de energia ativa:

- Classe A – com uma precisão de ± 2%;
- Classe B – com uma precisão de ± 1%;
- Classe C – com uma precisão de ± 0,5%;
- Classe D – com uma precisão de ± 0,2%.

A Companhia Paranaense de Energia (Copel) estabeleceu através da norma técnica ETC 4.04 [39] que os medidores fornecidos a companhia devem ter classe de precisão de 2% (classe A), ou melhor, para medidores eletromecânicos e classe de precisão de 1% (classe B), ou melhor, para medidores eletrônicos.

2.2.2. Perdas Não-técnicas

As perdas não-técnicas (PNT) são complementares às perdas técnicas. Todas as demais perdas associadas à distribuição de energia elétrica, tais como furtos de energia, erros de medição, erros no processo de faturamento, unidades consumidoras sem equipamento de medição são tratadas como perdas não-técnicas [40].

As PNT relacionadas ao furto de energia estão localizadas dominantemente na chamada “última milha” da rede de distribuição de energia elétrica. Tradicionalmente, os consumidores têm sido os principais causadores de perdas não-técnicas [41]. Os métodos mais comuns

utilizados para causar perdas não-técnicas de energia, indicados na literatura [42], [43], [44] são:

- Gerar leituras falsas de menor valor com ajuda dos funcionários corruptos;
- Colocar imã no medidor para que o disco rode em menor velocidade;
- Desviar energia através do *by-pass* dos equipamentos de medição ou de qualquer técnica de ligação clandestina;
- Adulterar equipamentos de medição, visando o registro de um menor consumo de energia elétrica.

Com a implantação dos medidores inteligentes e da AMI alguns métodos que originam perdas não-técnicas podem ser evitados [45]. Todavia, em comparação com as redes elétricas tradicionais, novos meios podem ser utilizados para causar perdas não-técnicas [46], [47]. De acordo com Skopik e Ma [48] há três níveis de vulnerabilidades em REIs:

- Nível 1: lida com ameaças a dispositivos elétricos, medidores inteligentes e sua conexão ao concentrador de dados. Esta parte é muitas vezes referida como a "última milha" e é considerada como a mais vulnerável a ataques de roubo de energia [49];
- Nível 2: trata as vulnerabilidades dos concentradores de dados até os data centers;
- Nível 3: lida com aplicações Web que utilizam os dados coletados pelos medidores inteligentes.

Um consumidor que tem por objetivo furtar energia e/ou ocultar o seu real consumo provavelmente vai aventurar-se a realizar ataques no Nível 1, pois o medidor inteligente pode ser a única fonte que o fornecedor de energia dispõe para verificar a quantidade de energia consumida. Não importa se a leitura do medidor é exata ou falsificada, o fornecedor de energia não tem meios para verificar a veracidade do relatório de leitura do medidor [50]. Salinas e Li [46] enfatizam que nesse nível há duas maneiras de roubar energia e causar perdas não-técnicas:

- Ataque Físico: medidores mecânicos convencionais e medidores inteligentes são ambos vulneráveis a esse tipo de ataque. Refere-se às situações em que usuários ilegais modificam fisicamente seus medidores para registrar valores falsos que diminuirão suas contas de energia elétrica. Uma maneira de detectar ataques

físicos é verificar visualmente o medidor a procura de selos quebrados ou outros sinais de danos;

- Ataques de Rede: Um usuário pode investir contra a conexão de rede de seu medidor para enviar falsas medições para o fornecedor de energia.

Neste trabalho, são consideradas as fraudes geradas no Nível 1. A Figura 4 combina os ataques mencionados em [41], [51], [52], [53], [54] e [55] e ilustra as principais vulnerabilidades do Nível 1 que podem ser utilizados para se ter acesso ao medidor inteligente e/ou a conexão de rede.

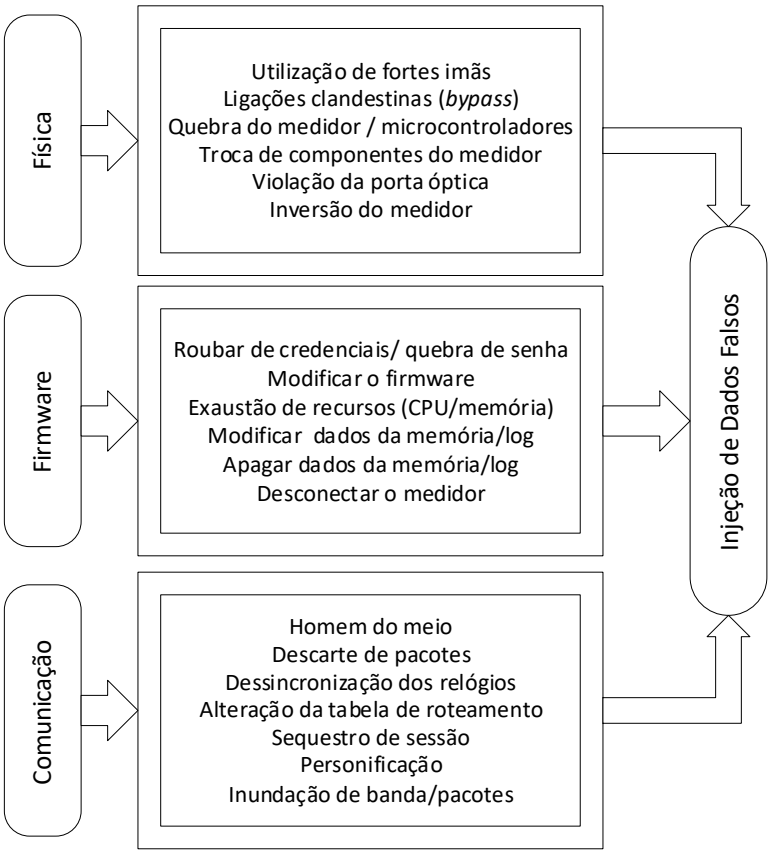

Figura 4: Vulnerabilidades no Nível 1.

Os ataques físicos podem ser minimizados com a instalação de medidores inteligentes com diversos tipos de sensores para detectar ataques físicos e de rede. Todavia, o preço dos medidores inteligentes com vários sensores aumenta e, geralmente, o tempo de vida útil dos sensores é menor do que do medidor, tornando sua utilização em larga escala inviável. Segundo Loeff [56] alguns sensores podem causar altas taxas de falsos positivos. Por exemplo, um sensor

que identifica que a caixa do medidor inteligente foi aberta pode ser disparado por um caminhão pesado passando perto do medidor inteligente.

Após ter acesso ao medidor ou a conexão de rede de seu medidor o consumidor (atacante) pode utilizar técnicas de injeção de dados falsos (*False Data Injection* – FDI) para ocultar o seu real consumo de energia [47], [57] e [58]. Em [52] é feito um primeiro levantamento sobre alguns tipos de FDIs que podem ser utilizados por consumidores maliciosos. O Quadro 2 apresenta uma compilação dos efeitos dos principais tipos de FDIs encontrados na literatura. Na tabela o x_t representa o consumo original relatado no intervalo de tempo monitorado e o $\tilde{x}_t$ representa o consumo após a sua adulteração. Deve-se observar que a tabela indica como as medidas de consumo são modificadas, e não como os ataques são feitos. A forma como os ataques são realizados não é importante na abordagem proposta, que se baseia apenas na análise das medidas de consumo. O objetivo da tabela é mostrar que existe uma diversidade de formas diferentes de modificar as medidas de consumo, e que o sistema proposto deve ser capaz de detectar fraudes independente da forma como os valores de consumo são reduzidos.

Quadro 2: Definição de FDIs.

Tipos de FDIs	**Modificação das Medidas**	**Descrição**
FDI1	$\tilde{x}_t \leftarrow y \cdot x_t \quad \text{onde} \quad 0 < y < 1$ y: é igual para todas as medições x_t: medida original no intervalo tempo	Todas as medidas de consumo (x_t) são multiplicadas por uma porcentagem de roubo (y)
FDI2	$\tilde{x}_t \leftarrow f(x_t)$ $f(x_t) = \begin{cases} x_t & se \quad x_t \leq c \\ \tilde{c} & se \quad x_t > c \end{cases}$ c: ponto de corte $c_{min} < \tilde{c} < c$: gerado aleatoriamente	Se a medida de consumo (x_t) for maior que o ponto de corte (c) a medida deve ser substituída por uma de menor valor
FDI3	$\tilde{x}_t \leftarrow \max(x_t - c, 0)$ c: valor constante de roubo fixado em KWh	Todas as medidas (x_t) são subtraídas por um valor constante de roubo (c)
FDI4	$\tilde{x}_t \leftarrow f(t) \cdot x_t$ $f(t) = \begin{cases} 0 & t_i < t < t_f \\ 1 & senão \end{cases}$ $t_f - t_i$: definido aleatoriamente para cada dia	Durante um intervalo de tempo aleatório todas as medidas devem ser substituídas por zero
FDI5	$\tilde{x}_t \leftarrow y_t \cdot x_t \quad \text{onde} \quad 0 < y_t < 1$ y_t: sorteado para cada relatório de consumo	Cada medida de consumo (x_t) é multiplicada por uma porcentagem de roubo sorteada aleatoriamente (y_t) para cada intervalo de medição
FDI6	$\tilde{x}_t \leftarrow y_t \cdot \overline{x}, \quad \text{onde} \quad 0 < y_t < 1$ y_t: sorteado para cada relatório de consumo $\bar{x}$: consumo médio do mês anterior	A média de consumo do mês anterior ($\overline{x}$) é multiplicada por uma porcentagem de roubo sorteada aleatoriamente (y_t) para cada intervalo de medição

Para o FDI1 todas as medidas são multiplicadas por uma porcentagem de roubo aleatória. Já para o FDI2 todas as medidas que forem maiores do que o ponto de corte estipulado pelo fraudador devem ser substituídas por um valor aleatório entre o mínimo de consumo estipulado e o ponto de corte. No FDI3 todas as medidas devem ser subtraídas por um valor constante de roubo. Para o FDI4 as medidas devem ser substituídas por zero durante um período de tempo aleatório. No FDI5 cada medida deve ser multiplicada por uma porcentagem aleatória diferente de roubo, para cada intervalo de medição. Por fim, para o FDI6, para cada intervalo de medição uma porcentagem aleatória de roubo é multiplicada pela média de consumo, do mês anterior, da unidade consumidora.

2.3. Padrão de Consumo de Energia

Todas as unidades consumidoras têm uma demanda de energia. Para Rathod e Garg [59] a demanda de cada unidade consumidora varia de forma diferente, dependendo do tipo de unidade consumidora, localidade, fatores ambientais, número de pessoas e nível de renda. Depuru [60] classifica as unidades consumidoras como:

- Comerciais (pequenos, médios e grandes);
- Residenciais (pequenos, médios e grandes);
- Agrícolas (pequenos, médios e grandes).

A implantação da AMI possibilita uma nova forma de identificar padrões de consumo entre os diferentes tipos de consumidores, que antes só podiam ser observados mensalmente ou anualmente. Mcloughlin *et al*. [61], ao avaliar um conjunto de dados coletados pela AMI percebeu que os perfis de consumo de energia são muito variáveis entre consumidores e em relação ao tempo. Em relação ao tempo uma única unidade consumidora pode mudar significativamente seu consumo de um dia para o outro bem como ao longo do dia. A Figura 5 representa uma unidade consumidora com variação diária no consumo de energia ao longo de uma semana. A unidade consumidora foi selecionada aleatoriamente no estudo de Mcloughlin *et al.*.

Há várias razões para o consumo diário mudar de um dia para o outro, em especial, o fato que o consumo residencial é determinado pelo conjunto de equipamentos eletrônicos utilizados pelos moradores e principalmente pelo fato que os seres humanos não apresentam

um comportamento uniforme. De acordo com Smith *et al.* [62] a maior parte da energia utilizada em uma residência é consumida coletivamente pelos ocupantes, como por exemplo, para a iluminação, aquecimento/resfriamento, e muitos aparelhos que servem ao grupo. Esse consumo coletivo pode ser caracterizado como a demanda mínima de energia para o agregado familiar. Todavia, muitos processos afetam o consumo de energia do agregado familiar, em especial fatores sociais. Por exemplo, a preparação do jantar exerce forte influência sobre o consumo de energia, o que pode causar picos de consumo ao longo do dia. Segundo Sanquist *et al.* [63] quando se fala em fatores sociais, o estilo de vida pode ser relacionado aos perfis de consumo, e são influenciados por decisões em vários pontos da vida, assim como a introdução de novos hábitos. Por exemplo, quando (ou se) casar, ter filhos, e escolhas mais próximas, sobre que equipamentos eletrônicos comprar e quando. Essa relação sugere que a análise do consumo de energia de uma unidade consumidora precisa levar em consideração o padrão de consumo recente de uma Unidade Consumidora (UC). Utilizar dados históricos para definir o padrão de consumo de uma unidade consumidora pode distorcer o padrão de consumo atual.

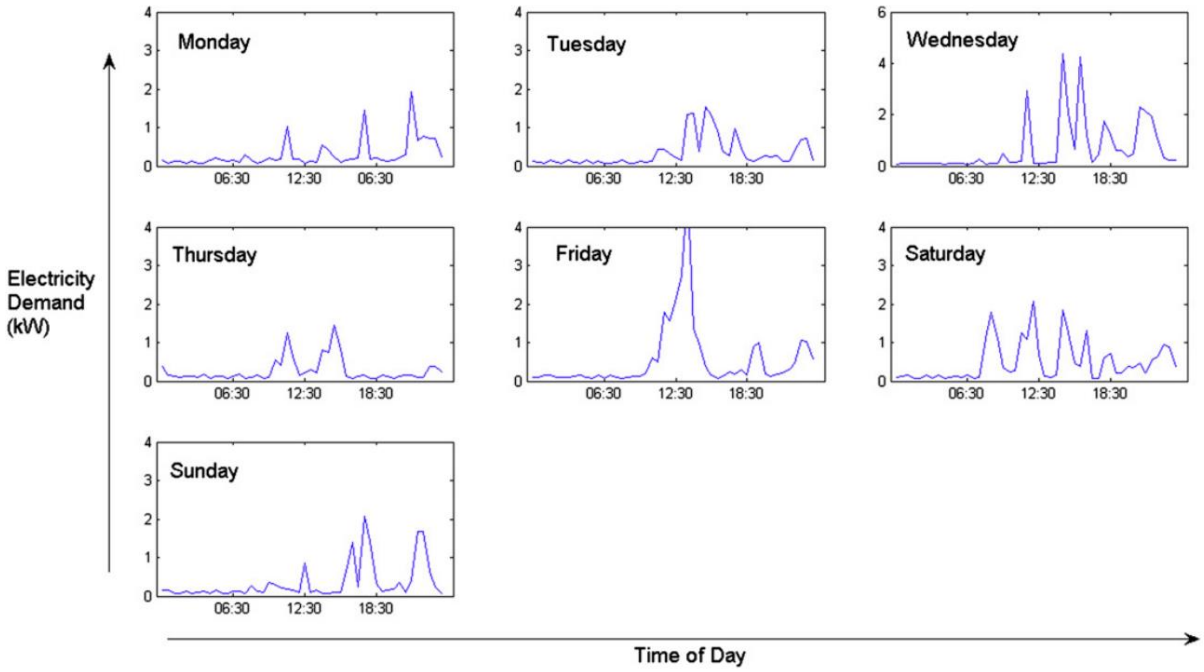

Figura 5: Variação diária ao longo de uma semana.
[61]

2.4. Aprendizagem de Máquina

Aprendizado de Máquina (AM) é um campo de pesquisa da Inteligência Computacional que estuda o desenvolvimento de métodos capazes de extrair conceitos (conhecimento) a partir de amostras de dados [64]. Essencialmente os mecanismos de aprendizagem podem ser separados em dois paradigmas: supervisionado e não-supervisionado. A escolha do paradigma de aprendizado determina a maneira como o algoritmo de AM se relaciona com seu meio ambiente, ou seja, o modo como ocorrerá o seu aprendizado por meio de um conjunto de dados [65]:

- Aprendizagem Supervisionada: Neste tipo de aprendizagem existe um supervisor que define a resposta desejada para o padrão de entrada. As observações no conjunto de treinamento são rotuladas pelo supervisor indicando a classe a que elas pertencem. O sistema tem que determinar as propriedades comuns na fase de treinamento através dos exemplos que lhe foram fornecidos. Estando as propriedades determinadas, é possível formular a regra de classificação que pode ser utilizada para classificar um novo conjunto;
- Aprendizagem Não-Supervisionada: Nesta forma de aprendizagem não existe um supervisor. O método de aprendizagem tem de determinar padrões sozinho, regularidades ou categorias que podem ser relacionadas de alguma maneira. Após a determinação das relações, em geral, é necessária uma análise para determinar o que as saídas significam no contexto do problema que está sendo analisado.

Dentro da aprendizagem não-supervisionada o agrupamento (*clustering*) é uma forma bem conhecida que visa separar objetos similares uns aos outros em classes/grupos (*clusters*). Ou seja, um conjunto de grupos é definido como um agrupamento. Os principais tipos de agrupamentos são: hierárquicos (aninhados) X particional (não aninhado), exclusivos X não exclusivos, completo X parcial e heterogêneos X homogêneos [66] e [67].

Particional (não aninhado) X hierárquicos (aninhados): Um agrupamento particional divide objetos de dados em grupos sem sobreposição tal que cada objeto de dados está exatamente em um grupo. Se os grupos puderem ter subgrupos, então se tem um agrupamento hierárquico. Um agrupamento hierárquico nada mais é do que um conjunto de grupos aninhados e organizados como uma árvore hierárquica, que mostra a relação grupo-subgrupo e a ordem em que foram divididos.

Exclusivos X Não Exclusivos: Agrupamentos exclusivos associam cada objeto a um único grupo, enquanto em agrupamentos não exclusivos, cada objeto pode pertencer a vários grupos. Nesse caso, um objeto pertence a um grupo com algum peso, entre 0 e 1, sendo que a soma dos pesos dos grupos ao qual o objeto pertence dever ser igual a 1.

Completo X Parcial: Em agrupamento completo, cada objeto está associado a pelo menos um grupo, enquanto em um agrupamento parcial alguns objetos podem não pertencer a pelo menos um grupo bem definido.

Heterogêneos X Homogêneos: Agrupamentos são considerados heterogêneos se possuírem tamanho, formato e densidade completamente diferentes; caso contrário são grupos homogêneos.

Os grupos criados pela técnica de agrupamento utilizada podem ser definidos como [66] e [67]:

- Grupos bem separados: é um conjunto de objetos em que qualquer objeto em um grupo está mais próximo (ou é mais similar) a todos os outros objetos no grupo do que a qualquer objeto que não pertence ao grupo;
- Grupos baseados em centro/protótipo: é um conjunto de objetos em que um objeto em um grupo está mais próximo (mais similar) ao centro de um grupo que ao centro de qualquer outro grupo. O centro de um grupo é um centroide, ou seja, a média de todos os pontos do grupo, ou um medóide (*medoid*), o ponto mais representativo de um grupo;
- Grupos baseados em grafo: os dados são representados como um grafo onde os nós são os objetos e a similaridade entre eles são as arestas;
- Grupos baseados em densidade: são regiões densas de objetos separadas por regiões de baixa densidade;
- Grupos conceituais: é um grupo de objetos que compartilham alguma propriedade. Esta definição engloba todas as definições anteriores de grupo.

Na literatura de detecção de intrusão e detecção de fraudes é possível encontrar diversos algoritmos que seguem tanto a abordagem supervisionada como a não-supervisionada. Nesse trabalho os algoritmos mais utilizados foram selecionados para serem avaliados na detecção de consumidores fraudulentos em REIs. Dentre os algoritmos de aprendizagem supervisionada o SVM foi selecionado. Já entre os algoritmos não supervisionados K-Means, Fuzzy C-Means (FCM) e Mapas Auto-Organizáveis (SOM) foram selecionados. A seguir os algoritmos são apresentados.

2.4.1. K-Means

K-Means é um algoritmo de clusterização que, dado um conjunto finito de *n* elementos $X = \{x_1, x_2, \ldots, x_n\}$, particiona *X* entre *k* grupos/clusters, onde cada observação x_i pertence a um dos *k* clusters fixados a priori. O objetivo principal é determinar *k* centroides (C_k), um para cada cluster [68]. O valor de cada centroide é calculado pela equação (9). O próximo passo é associar cada elemento x_i ao centroide mais próximo utilizando a função objetivo definida por (10). Quando todos os elementos forem associados a um determinado centroide, uma clusterização primária foi alcançada. Nesse momento é preciso voltar a calcular *k* novos centroides e obter uma nova associação entre os *n* elementos e os novos centroides. A cada ciclo os centroides C_k podem mudar o seu valor. Quando um centroide não mudar mais seu valor, e/ou o número máximo de interações for atingido o algoritmo K-Means resolveu o processo de clusterização. Os centroides são calculados através da equação (9):

$$C_k = \frac{1}{\mathrm{n_k}} \sum_{i=1}^{\mathrm{n_k}} x_i^{(k)} \qquad (9)$$

Onde: $\mathrm{n_k}$ é a quantidade de elementos pertencentes a um cluster *k* e $x_i^{(k)}$ representa os elementos x_i pertencentes ao cluster *k*.

Por fim K-Means resolve o processo utilizando a equação (10):

$$min \sum_{i=1}^{n} \sum_{j=1}^{k} \left(d_{ij}\right)^2 \qquad (10)$$

Onde $d_{ij} = \left\| x_i^{(j)} - C_j \right\|$ é a Distância Euclidiana entre um ponto de dado $x_i^{(j)}$ e o centroide C_j.

Os passos do algoritmo K-Means são [69]:

1. Inicializar randomicamente os C_k centroides;
2. Atribuir cada x_i ao centroide C_k mais próximo (equação (10));
3. Atualizar o valor de cada centroide C_k, calculando a média de todos os elementos x_i pertencentes ao cluster (equação (9));
4. Repita os passos 2 a 4 até que os elementos de cada cluster não mudem mais, e/ou o número máximo de iterações seja atingido.

2.4.2. Fuzzy C-Means

Diferente do método de clusterização K-Means, onde cada elemento pode pertencer somente a um único cluster, o Fuzzy C-Means (FCM) permite a atribuição de graus de pertinência aos clusters, onde os elementos podem pertencer a mais de um cluster [70]. Mais precisamente, dados *k* clusters e um conjunto $X = \{x_1, x_2, \ldots, x_n\}$ de *n* elementos, FCM retorna uma lista de centroides e uma matriz de pertinência que informa o grau de pertinência de cada elemento a cada cluster. A função objetivo de FCM é definida por (11):

$$min \sum_{i=1}^{n} \sum_{j=1}^{k} (u_{ij})^m (d_{ij})^2 \tag{11}$$

Onde $u_{ij} \in [0,1]$, $i = 1, \ldots, n$; $j = 1, \ldots, k$; e cada elemento u_{ij} diz o grau de pertinência do elemento x_i ao centroide C_j ; m é um fator denominado fuzzificador que determina o grau de incerteza.

O particionamento fuzzy é realizado através da função objetivo definida em (11), com a atualização do grau de pertinência u_{ij} e dos centroides C_j definidos por (12) e (13) respectivamente.

$$u_{ij} = \frac{1}{\sum_{l=1}^{k} \left(\frac{d_{ij}}{d_{il}}\right)^{\frac{2}{m-1}}} \tag{12}$$

$$C_j = \frac{\sum_{i=1}^{n} (u_{ij})^m x_i}{\sum_{i=1}^{n} (u_{ij})^m} \tag{13}$$

Os passos do algoritmo FCM são [71]:

1. Inicializar randomicamente os centroides;
2. Calcular os graus de pertinência nos clusters (equação (12));
3. Atualizar os novos centroides (equação (13));
4. Executar teste de parada, como por exemplo, $max \left| (u_{ij})^{(it)} - (u_{ij})^{(it-1)} \right| \leq \omega$, se o critério não for satisfeito, voltar ao passo 2.

2.4.3. Mapas Auto-Organizáveis

Os Mapas Auto-Organizáveis (*Self-Organized Maps* - SOM) são um tipo de rede neural artificial que tem como objetivo organizar dimensionalmente dados complexos em grupos (clusters), de acordo com suas relações, de tal forma que elementos similares sejam posicionados próximos uns dos outros [72].

SOM opera nos modos treinamento e mapeamento. Na etapa de treinamento a rede busca encontrar similaridades baseando-se apenas nos padrões de entrada. O conjunto de dados (*X*) é decomposto em um conjunto de amostras, $x = \{x_1, x_2, \dots, x_d\}$, onde d é a dimensão do vetor de entrada. Cada neurônio da grade é representado por um vetor de pesos sinápticos $w_j = \{w_{j1}, w_{j2}, \dots, w_{jd}\}$ e a distância entre um vetor de entrada *x* e o peso de cada neurônio *j*, será calculada para determinar o neurônio vencedor. O neurônio cujo vetor de pesos é mais próximo ao vetor de entrada é declarado vencedor utilizando o critério do melhor casamento (*Best Matching Unit* - BMU) [73]. A equação (14) identifica o neurônio vencedor.

$$v = \arg mim_j \left\| x - w_j \right\|, \qquad j = 1,2, \dots, k \tag{14}$$

Onde *k* é o número total de neurônios.

Em seguida, o vetor de pesos sinápticos w_j do neurônio *j* (neurônio vencedor) precisa ser atualizado em relação ao vetor de entrada *x*. Para isso o vetor $w_j(t)$ no tempo discreto *t* é ajustado pela equação (15):

$$w_j(t+1) = w_j(t) + \varrho(t) h_{vj}(t) \left[x - w_j(t) \right] \tag{15}$$

Onde:

- $w_j(t)$: é o vetor de pesos sinápticos no tempo discreto *t*;
- $w_j(t+1)$: é o vetor de pesos atualizado, no tempo *t* +1;
- $\varrho(t)$: é o parâmetro taxa de aprendizagem e dada pela equação (16);
- $h_{vj}(t)$: é a função vizinhança definida pela equação (17);
- x: é o vetor de entrada.

A equação (15) é aplicada a todos os neurônios da grade que se encontram dentro da região de vizinhança do neurônio vencedor. O parâmetro taxa de aprendizagem $\varrho(t)$ é variável e deve

diminuir gradualmente com o tempo. Para isso escolhe-se a taxa de aprendizagem como sendo exponencial decrescente como apresentado na equação (16) [74].

$$\varsigma(t) = \varsigma_0 exp\left(-\frac{t}{\tau_2}\right) t = 0,1,2,\ldots \quad (16)$$

Onde τ_2 é o número total de iterações.

A função vizinhança é tipicamente gaussiana dada pela equação (17).

$$h_{vj}(t) = exp\left(-\frac{\|r_v - r_j\|}{2\sigma^2(t)}\right) \quad (17)$$

Onde:

- $\|r_v - r_j\|$: é a distância entre o neurônio *v* (vencedor) e o neurônio *j* que está sendo atualizado;
- σ: define a largura da função e deve ser decrescente no tempo. Pode ser usada uma função linear, mas em geral é usada a exponencial [74].

Os passos na fase de treinamento do algoritmo SOM são:

1. Selecionar uma amostra de entrada *x*;
2. Calcular a distância euclidiana da amostra de entrada para cada um dos neurônios da grade e encontrar o neurônio vencedor *v* (equação (14));
3. Atualizar os valores dos neurônios na vizinhança do neurônio vencedor (equação (15));
4. Incrementar *t* enquanto houver amostras na base de entrada.

Na etapa de mapeamento SOM classifica um novo vetor de entrada entre os neurônios definidos na fase de treinamento. Para identificar os elementos que estão associados a cada neurônio um processo similar ao do algoritmo K-Means definido pela equação (10) é executado. Nesse trabalho neurônios serão chamados de centroides.

2.4.4. Máquinas de Vetores de Suporte (SVMs)

As Máquinas de Vetores de Suporte (*Support Vector Machines* - SVMs) são classificadores embasados na Teoria de Aprendizado Estatístico de aprendizagem supervisionada. Dado um conjunto de exemplos de treinamento, cada um rotulado com a categoria que pertence, SVM constrói um modelo que atribui novos dados a uma categoria ou outra [75].

Seja T um conjunto de treinamento com n dados x_i pertencendo a X e seus respectivos rótulos y_i pertencendo a Y, em que X constitui o espaço dos dados e $Y = \{-1, +1\}$. T é linearmente separável se é possível separar os dados das classes +1 e -1 por um hiperplano [76].

Classificadores que separam os dados por meio de um hiperplano são denominados lineares. A decisão entre as duas classes de um hiperplano é descrita pela equação (18):

$$g(x) = \langle w, x \rangle + b \tag{18}$$

Onde w e b são derivados de tal forma que os dados invisíveis são classificados corretamente. Isto é alcançado através da maximização da margem de separação entre as duas classes. De acordo com [64] para construir um hiperplano ideal com a maximização da margem e minimizando o erro sobre os dados de treinamento, o problema de otimização é resolvido por (19):

$$\min_{w,\varepsilon} \left(\frac{1}{2} \|w\|^2 + C \sum_{i=1}^{n} \varepsilon_i \right) \tag{19}$$

Ao minimizar o primeiro termo da equação (19) a complexidade de SVM é reduzida, e pela minimização do segundo termo o número de erros marginais de treinamento é reduzido. O parâmetro C na equação (19) é um termo de regularização que impõe um peso à minimização dos erros no conjunto de treinamento em relação à minimização da complexidade do modelo [77].

A equação (19) está sujeita à limitação de que todas as amostras de treino sejam corretamente classificadas, de acordo com a equação (20):

$$y_i(\langle w, x_i \rangle + b) \geq 1 - \varepsilon_i i = 1, 2, \ldots, n \tag{20}$$

Onde ε é uma variável de folga (*slack variable*).

A aplicação do procedimento da equação (20) suaviza as margens do classificador linear, permitindo que alguns dados permaneçam entre os hiperplanos formados pelos vetores de suporte e também a ocorrência de alguns erros de classificação. Por esse motivo, as SVMs obtidas neste caso também podem ser referenciadas como SVMs com margens suaves (*soft-margin*) [77].

O problema de otimização gerado na equação (19) com restrições lineares apresentadas na equação (20) é resolvido por meio da técnica dos multiplicadores de Lagrange (α). Essa abordagem pode ser expressa por (21):

$$\max_{\alpha}\left\{\sum_{i=1}^{n}\alpha_i - \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\alpha_j y_i y_j \langle x_i, x_j\rangle\right\} \tag{21}$$

Com as restrições (22):

$$\begin{cases} 0 \le \alpha_i \le C, \qquad i = 1, 2, \dots, n \\ \sum_{i=1}^{n}\alpha_i y_i = 0 \end{cases} \tag{22}$$

A partir da equação (18) verifica-se que o hiperplano ótimo no espaço de característica pode ser escrito como a combinação linear de amostras de treinamento com $\alpha_i \neq 0$. Estas amostras informativas, conhecidas como vetores de suporte, constroem a função de decisão do classificador com base nas funções kernel (23):

$$g(x) = \sum_{i=1}^{N_s}\alpha_i y_i K(x, x_i) + b \tag{23}$$

Onde $K(x, x_i) \rightarrow \langle x_i, x_j\rangle$ representa a função Kernel.

Funções kernel em SVMs são selecionadas com base na estrutura de dados e tipo das fronteiras entre as classes. Entre as funções Kernel mais utilizadas está a Gaussiana também conhecida como *Radial-Basis Function* (RBF) (24) [78]:

$$K(x_i x_j) = exp\left(-\gamma \left\| x_i - x_j \right\|^2\right) \quad (24)$$

Onde $\gamma > 0$ é o parâmetro do kernel RBF. O kernel RBF induz um espaço infinito-dimensional do kernel, em que todos os vetores de imagem têm a mesma norma, e o parâmetro de largura do kernel γ controla o escalonamento do mapeamento.

2.5. Métricas de Avaliação

Para avaliar os resultados obtidos é necessário definir algumas medidas de avaliação para as estratégias de detecção de consumidores fraudulentos. O resultado da classificação é um problema de duas classes, onde as classes são positivas ou negativas, sendo que poderá ocorrer uma predição correta ou incorreta. A matriz de confusão exibida no Quadro 3 ilustra o número de classificações corretas e incorretas de cada classe. As linhas da matriz representam as classes verdadeiras e as colunas, as classes preditas pela estratégia de classificação.

Quadro 3: Matriz de confusão.

Classes		**Classe Predita**	
		Positiva	**Negativa**
Classe Real	**Positivo**	Verdadeiro Positivo (VP)	Falso Positivo (FP)
	Negativo	Falso Negativo (FN)	Verdadeiro Negativo (VN)

Adaptado de [79].

Onde:

- Verdadeiros Positivos (VP): atividades ilegais que foram detectadas;
- Verdadeiro Negativo (VN): atividades legítimas que foram detectadas como atividades legítimas;
- Falsos Positivos (FP): atividades legítimas que foram detectadas como ilegais;
- Falsos Negativos (FN): atividades ilegais que ocorreram, mas não foram detectadas.

A partir da matriz de confusão, uma série de medidas quantitativas de desempenho pode ser derivada, dentre elas [80]:

- Acurácia: é a proporção de predições corretas, sem levar em consideração o que é positivo e o que é negativo, (equação (25));

$$\text{Acurácia} = \frac{\text{VP} + \text{VN}}{\text{VP} + \text{VN} + \text{FP} + \text{FN}} \qquad (25)$$

- Taxa de erro: é o número de predições incorretas, (equação (26));

$$Taxa\ de\ erro = \frac{FP + FN}{VP + VN + FP + FN} \qquad (26)$$

- Taxa de verdadeiros positivos (TVP) / Sensibilidade / Cobertura (*Recall*): é a capacidade do sistema de classificação em predizer corretamente a condição para casos onde ela realmente ocorre, (equação (27));

$$\text{TVP} = \frac{\text{VP}}{\text{VP} + \text{FN}} \qquad (27)$$

- Especificidade: é a capacidade do sistema em predizer corretamente a ausência da condição para casos onde ela realmente não ocorre (equação (28));

$$\text{Especificidade} = \frac{\text{VN}}{\text{VN} + \text{FP}} \qquad (28)$$

- Taxa de falsos Positivos (TFP): também chamada de taxa de falsos alarmes é equivalente a (1-Especificidade), (equação (29));

$$\text{TFP} = \frac{\text{FP}}{\text{FP} + \text{VN}} \qquad (29)$$

- Valor Preditivo Positivo (VPP) / Precisão (*Precision*): é a proporção de verdadeiros positivos em relação a todas as predições positivas, (equação (30));

$$VPP = \frac{VP}{VP + FP} \tag{30}$$

- Valor Preditivo Negativo (VPN): é a proporção de verdadeiros negativos em relação a todas as predições negativas, (equação (31));

$$VPN = \frac{VN}{VN + FN} \tag{31}$$

- Medida F: é a média harmônica das medidas de Precisão (Valor Preditivo Positivo (VPP)) e de Cobertura (Taxa de verdadeiros positivos (TVP)), (equação (32));

$$F = 2.\frac{VPP.TVP}{VPP + TVP} \tag{32}$$

Uma forma de visualizar graficamente as combinações de TVP e TFP é através da representação da curva *receiver operating characteristic* (ROC). As taxas de VP e FP juntas determinam um único ponto no espaço ROC, e a posição de um ponto no espaço ROC mostra o equilíbrio entre a sensibilidade e especificidade, isto é, o aumento na sensibilidade é acompanhado por uma diminuição na especificidade. Assim, a localização do ponto no espaço ROC descreve se a classificação do sistema é boa ou não [80]. Em uma situação ideal, um ponto determinado por TVP e TFP produz uma coordenada (0, 1), localizada no canto superior esquerdo do espaço ROC. Este ponto indica que o sistema de classificação é perfeito. Um ponto que está acima da diagonal representa uma boa classificação, abaixo, uma má classificação. Uma apresentação gráfica do que foi descrito acima é mostrada na Figura 6.

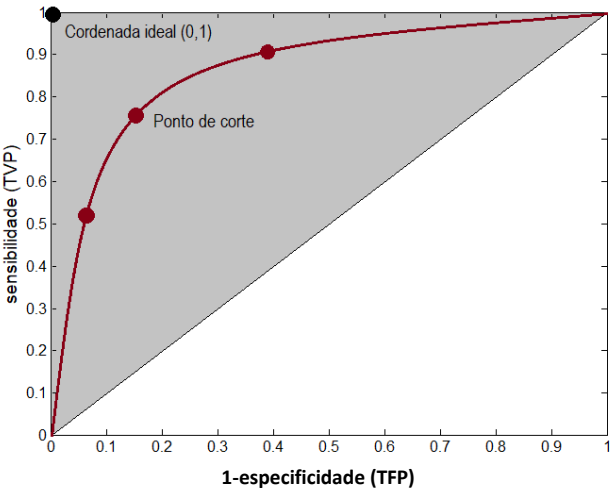

Figura 6: Curva ROC.
Adapatado de [79].

Entre as métricas apresentadas nessa seção algumas são altamente suscetíveis ao desbalanceamento do conjunto de dados e podem facilmente induzir a uma conclusão errada sobre o desempenho de um sistema de classificação. Nesses casos as métricas de acurácia, taxa de erro, valor preditivo positivo e valor preditivo negativo devem ser evitadas.

Outro critério importante é determinar o impacto do uso de sistemas de detecção de fraudes sobre o lucro da concessionária. O lucro de um uma concessionária sem a utilização de um sistema de detecção de fraudes durante um período de observação predefinido pode ser modelado utilizando a expressão (33) [81].

$$P = \sum_{i \in \Theta} T\left(q^i - q_u^i\right) - C\left(\sum_{i \in \Theta} q^i\right) \tag{33}$$

Onde:

- Θ: é o conjunto de consumidores da concessionária;
- q^i: é o consumo do consumidor i;
- q_u^i: é a energia não contabilizada do consumidor i. Para consumidores honestos $q_u^i = 0$;
- T: é o preço da eletricidade;
- $C\ (.)$: é o custo de produção da eletricidade.

O lucro da concessionária que utiliza um sistema de detecção de fraudes pode ser modelado utilizando a equação (34), que é uma versão simplificada da expressão proposta por [81].

$$P^* = P + \sum_{i \in \Theta} p\left(q_u^i\right).F\left(q_u^i\right) - (vp + fp).\psi \tag{34}$$

Na expressão,

- Θ: é o conjunto de consumidores da concessionária;
- $p(.)$: é a probabilidade de detectar um roubo de energia;
- $F(.)$: representa as multas sobre o roubo de energia detectado;
- $(vp + fp)$: número de alarmes, verdadeiro ou falso, gerado durante o período de observação;
- ψ: é o custo médio de inspeção no local.

2.6. Considerações

Este capítulo apresentou os principais conceitos aplicados ao longo deste trabalho como: infraestrutura de medição avançada, perdas não-técnicas, injeção de dados falsos, perfis de consumo, agrupamento, cluster e métricas de avaliação. Oferecendo os subsídios teóricos necessários para o desenvolvimento deste trabalho.

Capítulo 3

Trabalhos Relacionados

Neste capítulo, são descritos os principais sistemas de detecção de furto de energia encontrados na literatura. Atualmente os sistemas existentes podem ser classificados em baseados em estados e em perfis de consumo. Os sistemas baseados em estados na maioria dos casos utilizam dispositivos específicos como sensores para verificar os estados da rede de distribuição, e assim identificarem consumidores fraudulentos. Os sistemas baseados em perfis de consumo podem ser ainda divididos em três categorias: 1) estatísticos; 2) aprendizagem de máquina supervisionada; e 3) aprendizagem de máquina não-supervisionada. As próximas seções descrevem os principais sistemas encontrados na literatura.

3.1. Baseados em Estados

Xiao *et al.* [82] propõem um regime de controle mútuo com instalação de um medidor redundante no provedor de energia para inspecionar cada consumidor. Isso significa que para cada unidade consumidora há dois medidores inteligentes instalados: um que representa a leitura do provedor e outro que representa a leitura do consumidor. A diferença entre os dois valores de leitura deve estar dentro de certo intervalo. Caso contrário, o medidor pode estar sob ataque. Uma limitação do regime de controle mútuo é o seu custo. Adicionar um medidor redundante para cada unidade consumidora implica em um aumento no orçamento de hardware necessário. Em um novo trabalho [5] Xiao *et al.* busca identificar medidores maliciosos através de inspeções. No trabalho os autores assumem que existe um dispositivo chamado caixa de inspeção localizado na entrada de um prédio. A caixa de inspeção contém uma série de inspetores. Sendo que existe um inspetor principal, chamado de cabeça, que é responsável pelo monitoramento dos demais inspetores. O inspetor cabeça deve identificar se existem anomalias de consumo na leitura do prédio, através da comparação da sua leitura com o somatório de do consumo de energia relatada pelos medidores do prédio. Caso exista uma divergência o inspetor

cabeça monta uma árvore binária de inspetores com o objetivo de encontrar o medidor que está cometendo uma anomalia. Cada inspetor da árvore pode monitorar um único consumidor, ou vários consumidores que estão em sua subárvore. Os consumidores são considerados os nós folhas da árvore. A busca deve continuar nas subárvores anômalas até que o medidor malicioso seja identificado.

No trabalho de Lo e Ansari [58] é formulado um modelo de ataque (consumidor) que tem por objetivo adulterar medidores inteligentes, de forma que um consumidor pode ocultar o seu real consumo de energia, diminuindo a leitura do seu consumo e aumentando o consumo de outros consumidores da vizinhança, a fim de evitar que os centros de controle identifiquem atividades anômalas. A estrutura do sistema de detecção de intrusão trabalha com a colocação de sensores para coletar informações de potência e corrente, e assim aumentar a observabilidade da rede para verificar se atividades maliciosas estão ocorrendo. Os sensores são alocados em toda a rede de distribuição de energia utilizando um algoritmo de observabilidade, chamado *Grid-Placed Sensor* (GPS). O algoritmo proposto é baseado em teoria dos grafos.

Mclaughlin *et al.* [52] propõem um Sistema de Detecção de Intrusão AMI (Amids) que utiliza fusão de informações de sensores dedicados para verificar se os dispositivos estão funcionando em um estado seguro e suas operações respeitam as especificações elaboradas. A técnica de fusão proposta consiste em combinar as informações de três categorias: A primeira categoria considera os ataques físicos, a segunda categoria considera os ciberataques e, por fim, na terceira categoria são considerados os ataques contra o consumo de energia. Na primeira categoria são utilizados sensores de detecção de violação dos medidores e na segunda categoria sistemas de detecção de intrusos. Caso um alarme seja gerado nas categorias físicas e/ou ciber o sistema faz uso de um gráfico de ataque que combina os possíveis ataques de primeira e segunda categoria e verifica se esses geram um ataque de terceira categoria. As fraudes de terceira categoria são identificadas utilizando o algoritmo supervisionado Naive Bayes.

3.2. Baseados em perfis de consumo

A seguir os sistemas baseados em perfis de consumo são descritos.

3.2.1. Baseados em perfil estatístico

Mashima *et al.* [83] propõem a utilização de distribuição de probabilidades para modelar o consumo de energia de consumidores normais e fraudulentos e a utilização de teste de razão de verossimilhança (*generalized likelihood ratio* - GLR) para detectar furtos de energia. Os autores assumem que consumidores fraudulentos irão utilizar a média de seu consumo real para fraudar as suas medições, então o modelo auto-regressivo de médias móveis (*auto regressive moving average models* - ARMA) é utilizado para modelar o consumo de energia. O sistema ARMA-GLR só é eficaz se o comportamento normal e fraudulento puder ser modelado pelo ARMA.

Wu *et al.* [84] utiliza os métodos de soma cumulativa (CUSUM) e gráficos de controle para verificar alterações significativas na média e na variância das unidades consumidoras. Além de buscar por possíveis fraudes, os autores estão interessados em identificar medidores com defeitos que não estão realizando a leitura de forma adequada. Para fundir as informações dos dois métodos um algoritmo é desenvolvido com o objetivo de fornecer uma decisão final sobre a unidade consumidora avaliada. Os autores informam que seu método só eficiente para grandes alterações no perfil de consumo.

Salinas *et al.* [46] e [85] propõem um modelo de detecção de fraudes que preserva a privacidade dos consumidores. Um sistema equações de equações lineares (*linear system of equations* - LSE) é definido impondo que a soma das medidas de consumo de um grupo de consumidores deve corresponder à eletricidade fornecida pela grade. O consumo de cada consumidor é multiplicado por um coeficiente de honestidade igual a um para consumidores honestos e maior que um para consumidores suspeitos. Os coeficientes de honestidade são calculados pela resolução do LSE com um algoritmo distribuído baseado na decomposição *lower upper* (LU). Para preservar a privacidade, cada medidor inteligente calcula seu próprio coeficiente de honestidade sem conhecer as medidas de consumo de outros medidores inteligentes.

Liu e Hu [86] também utilizam um medidor coletivo para verificar se uma anomalia está ocorrendo na área monitorada. Caso esteja ocorrendo uma anomalia, os autores buscam identificar a(s) unidade(s) consumidora(s) fraudulenta(s) utilizando banda de Bollinger e processo de decisão de Markov parcialmente observável (*partially observable Markov decision process* - POMDP). Bandas de Bollinger utilizam a média e o desvio padrão para criar margens superiores em inferiores da variação do perfil de consumo de uma unidade consumidora. Se o consumo monitorado estiver fora dessas margens, POMDP utiliza probabilidades de estados

para identificar se a anomalia acusada por Bollinger corresponde a um estado de furto de energia.

Leite e Mantovani [87] desenvolveram um algoritmo de identificação de consumidores fraudulentos que utiliza gráficos de controle combinado com o algoritmo de busca A* (A-estrela). Quando a análise do gráfico de controle multivariado revelar a existência de perdas não-técnicas o algoritmo executa uma rotina para identificar os dispositivos de campo que revelaram essas perdas. A rotina de identificação é fundamentada no diagrama de dispersão das diferenças de corrente e tensão. Cada ponto no diagrama de dispersão representa um consumidor. Pontos que estiverem fora da região confiável do diagrama de dispersão devem ser armazenados e utilizados como entrada para o algoritmo de busca A*, que localiza a unidade consumidora que pode estar cometendo uma fraude.

Han e Xiao 2016 [88] propõem um esquema rápido de detecção de fraudes (*Fast NTL Fraud Detection scheme* (FNFD)) baseado em mínimos quadrados recursivos (*Recursive Least Square* (RLS)) para modelar o comportamento dos consumidores de energia. Para cada consumidor existe um grupo de pares de medidas, sendo que, cada par representa a energia consumida pelo medidor no intervalo de tempo t_j, e a energia relatada ao medidor coletivo no período de tempo t_j. Como não é possível gerar uma função para representar os pontos das coordenadas, os autores propõem encontrar uma linha próxima a esses pontos utilizando mínimos quadrados para estimar o padrão de consumo de um consumidor. Para atualizar a estimativa com novas medições a RLS é utilizada. No período de avaliação, a linha que estiver acima da linha estimada representa um consumidor fraudulento, enquanto que a linha abaixo da estimada representa um consumidor normal. Em um novo trabalho Han e Xiao [89] utiliza seu esquema FNFD para detectar perdas não-técnicas coniventes (*Colluded Non-Technical Loss* (CNTL)), que consistem em vários fraudadores colaborarem para cometer uma fraude. Em [90] Han e Xiao propõem um novo sistema para detectar perdas não-técnicas chamado *NTL Fraud Detection* (NFD). O sistema NFD baseia no polinômio de Lagrange para modelar e detectar medidores adulterados. Para cada medidor é gerado um polinômio de Lagrange que modela o comportamento de um consumidor. Para gerar o polinômio os autores utilizam as mesmas informações utilizadas em [88] e também utilizam a mesma estratégia de verificação de consumidores fraudulentos e normais. Consumidores que tiverem a linha de consumo acima do polinômio gerado serão considerados consumidores fraudulentos.

Os autores Su, Lee e Wen [91] utilizam estimativa de estados da rede de distribuição de energia para detectar roubo de eletricidade. Para calcular as estimativas de estado do sistema técnicas de otimização baseadas em programação semi-definida (*semi-definite programming*

(SDP)) são utilizadas para obter o vetor de estados de tensão do sistema de distribuição com base nos valores coletados nos medidores. Após a estimativa dos estados, as incertezas de potenciais erros nas medições dos medidores são consideradas e combinadas com modelos de probabilidades (distribuição normal, distribuição F e distribuição qui-quadrado) para determinar anormalidades. Quando um suspeito é encontrado, os dados históricos de consumo de energia são usados pela ANOVA para verificar se a curva de consumo de energia é anormal ou normal.

Villar-Rodruguez *et al.* [92] utilizaram séries temporais para identificar consumidores fraudulentos. A métrica *Dynamic time warping* (DTW) foi utilizada como medida de similaridade entre os perfis de consumo dos consumidores. Ao comparar as séries temporais passadas (perfis de consumo) com as atuais e medir a similaridade das séries temporais, consumidores que apresentavam maior dissimilaridade entre seus perfis de consumo eram considerados consumidores fraudulentos.

Os autores Yip *et al.* [93] [94] desenvolveram dois algoritmos para identificar consumidores fraudulentos, bem como para identificar medidores inteligentes defeituosos. Os dois algoritmos são baseados em regressão linear e são utilizados para estimar coeficientes de variação para cada um dos consumidores. Um coeficiente diferente de zero representa um consumidor fraudulento e/ou um medidor defeituoso. No modelo proposto pelos autores um medidor coletivo é utilizado para verificar energia consumida pelas unidades consumidoras ligadas ao mesmo. Se o consumo monitorado em um intervalo de tempo pelo medidor coletivo for diferente do somatório relatado pelas unidades consumidoras os algoritmos desenvolvidos utilizam os dados informados para criar o modelo de regressão linear e estimar o coeficiente de variação de cada um dos consumidores. O primeiro algoritmo chamado de LR-ETDM (*Linear Regression-based scheme for Detection of Energy Theft and Defective Smart Meters*) consegue identificar fraudes somente quando os consumidores adulteram todas as leituras de energia em um medidor inteligente. Para identificar consumidores que roubam energia em determinados períodos do dia o algoritmo CVLR-ETDM (*Categorical Variable-Enhanced Linear Regression based scheme for Detection of Energy Theft and Defective Smart Meters*) foi proposto pelos autores. Nesse algoritmo, variáveis categóricas são utilizadas para buscar identificar consumidores fraudulentos. As variáveis categóricas representam períodos de tempo em que um consumidor pode estar furtando energia. Por exemplo, uma variável categórica pode representar um furto das 8 horas da manhã às 8 horas da noite.

3.2.2. Baseados em aprendizagem de máquina supervisionada

Na sequência são apresentados os trabalhos que utilizam aprendizagem de máquina supervisionada para identificar consumidores fraudulentos. Vários trabalhos têm utilizado o classificador *Support Vector Machine* (SVM) combinado ou não com outras estratégias para identificar consumidores fraudulentos. Nagi *et al.* [49] realiza o treinamento de SVM utilizando somente medições de consumo, enquanto Depuru *et al.* [95] treina SVM com informações de localização geográfica, estação do ano, tipos de consumidores (comerciais, residências e agrícolas) e porte, além das medições de consumo. Na sequência, Depuru *et al.* [96] utilizou Redes Neurais para estimar a função Kernel adequada para SVM, a fim de diminuir o tempo de formação do classificador. Por fim, Depuru *et al.* [42] e [97] propõem o pré-tratamento das medidas de consumo para tornar a análise mais rápida. Nesse mesmo trabalho, SVM e regras que levam em consideração padrões das medidas são utilizadas em paralelo para determinar se um consumidor é fraudulento. Se o resultado da classificação por SVM e pelas regras for igual o processo é finalizado, caso seja diferente os dados devem ser reavaliados por ambos os algoritmos.

Em [98] Nagi *et al.* estende seu trabalho anterior [49] utilizando SVM em conjunto com operações Fuzzy. O conhecimento do especialista humano é utilizado para a criação das regras Fuzzy. Assim, após o processamento das medições através de SVM, Fuzzy é utilizado para selecionar os consumidores que apresentam maior probabilidade de estarem cometendo uma fraude.

Jindal *et al.* [99] utilizam um medidor coletivo para identificar divergências entre o somatório das leituras relatadas pelos consumidores ligados ao medidor coletivo e a sua própria leitura. Os algoritmos SVM e árvore de decisão (C4.5) são utilizados para identificar as unidades consumidoras fraudulentas. Várias características (temperatura, hora, estação do ano, N° de pessoas e aparelhos na unidade consumidora) são utilizadas para criar a árvore de decisão. O valor de consumo estimado pela árvore de decisão é informado a SVM juntamente com a medida coletada e as características utilizadas para criar a árvore de decisão.

Em Guo *et al.* [100] um medidor coletivo também é utilizado, mas agora, em conjunto com SVM e o algoritmo de agrupamento Fuzzy C-Means (FCM), que foi utilizado para realizar o agrupamento das medidas coletadas. Os centroides dos clusters foram utilizados para treinar SVM.

Jokar *et al.* [101] também utiliza um medidor coletivo. Em seu trabalho SVM *multiclass* é utilizado em conjunto com o algoritmo de clusterização K-Means. K-Means é utilizado para

agrupar medidas semelhantes, cada grupo de medidas semelhantes corresponde a uma classe no SVM *multiclass*. Para cada amostra de dados normais são criadas amostras anormais através da simulação de diferentes tipos de ataques, gerando os dados necessários para treinar o classificador SVM.

Nizar *et al.* [102], [103] utilizam diferentes perfis para cada unidade consumidora. São criados perfis de consumo de dias úteis, sábados, domingos e feriados. A média de consumo de cada intervalo de medição é calculada, em seguida o desvio padrão é utilizado para identificar consumidores que tem seu consumo acima ou abaixo do limite estabelecido pelo desvio padrão. Os padrões de consumo são utilizados para realizar o treinamento do algoritmo de aprendizagem de máquina estrema (*extreme learning machine* - ELM) e a avaliação de consumidores fraudulentos.

Ramos *et al.* [104] utilizou o algoritmo supervisionando Floresta de Caminhos ótimos (*optimum-path forest* - OPF), em dois conjuntos de dados já rotulados. A base era formada por consumidores industriais e comerciais. Para realizar o treinamento de OPF os autores utilizaram as informações de demanda contratada, demanda máxima ou média e potência instalada. Em um novo trabalho, Ramos *et al.* [105] estende seu trabalho anterior utilizando técnicas evolutivas para seleção de características e posterior treinamento de OPF.

Kosut *et al.* [106] elencou trinta características que podem ser observadas e avaliadas em uma unidade consumidora. Entre essas trinta características os autores selecionam algumas, como por exemplo: dias que se passou desde a última leitura, número de irregularidades já encontradas na unidade consumidora, tipo de cliente e localização. De posse dessas informações o algoritmo de árvore de decisão C4.5 é treinado e utilizado para realizar a classificação das novas amostras de dados dos consumidores.

3.2.3. Aprendizagem de máquina não-supervisionada

Por fim, os trabalhos que utilizam aprendizagem de máquina não-supervisionada são descritos. Ford *et al.* [107] utiliza Redes Neurais para identificar consumidores fraudulentos. Uma base de dados com aproximadamente dois anos de consumo é utilizada para validar seu modelo. São testados três tipos de perfis (perfil sazonal, mensal e semanal). Para os perfis mensais e sazonais, o mesmo mês/estação do ano seguinte é utilizado para fazer a avaliação se houve uma fraude. Estes dois testes têm como principal problema a necessidade de aguardar um ano para fazer o teste de avaliação. Para o perfil semanal, o modelo é treinando com as três

primeiras semanas da base de dados, e avaliado com as próximas semanas. Os autores informam que obtiveram uma elevada taxa de falsos positivos (25%) nos testes devido a variações de perfis causados por feriados, novos eletrodomésticos, variações metrológicas e/ou férias em família que não se enquadram nos perfis mapeados pela rede neural. Em um trabalho posterior [108] a mesma estratégia de testes com perfis sazonais, mensais e semanais são realizados, mais agora, utilizando o algoritmo de árvore de decisão M5P.

Em [109] [110] Ângelos *et al.* utilizam o algoritmo Fuzzy C-Means para identificar grupos de consumidores com perfis de consumo semelhantes. Para compor o perfil de cada consumidor cinco atributos dos últimos seis meses de consumo foram utilizados. O valor total, máximo, médio, desvio padrão do consumo do consumidor e a média de consumo do setor que o consumidor pertencia. Após a clusterização, as distâncias entre os grupos de consumidores eram normalizadas e um índice gerado. Ao efetuar a clusterização dos atributos atuais e verificar o índice gerado, consumidores que estivessem mais distantes de seus índices, eram considerados os possíveis fraudadores.

Krishna *et al.* [111] utiliza Análise de Componentes Principais (*Principal Component Analysis* - PCA) e o algoritmo de agrupamento espacial baseado em densidade com ruído (*Density based spatial clustering of applications with noise* - DBSCAN). A base de dados utilizada no trabalho é caracterizada por uma matriz de alta dimensionalidade, onde cada dimensão representa um intervalo de medição para as sessenta semanas monitoradas. A estratégia baseada em PCA ajuda a diminuir a dimensionalidade dos dados coletados mantendo suas características. Após transformar a matriz de medição em uma matriz de baixa dimensão o algoritmo DBSCAN é utilizado para descrever o padrão de consumo semanal de cada unidade consumidora. Quando o padrão de consumo semanal se distanciar do padrão estabelecido pelo algoritmo DBSCAN, o mesmo será caracterizado como uma anomalia. Hartmann *et al.* [112] utiliza aprendizagem de máquina contínua para criar múltiplos perfis globais. São criados perfis diários, semanais e mensais levando em consideração aspectos como estações do ano, feriados e dia da semana, além do tipo de consumidor (individual, familiar, industrial, comercial). Para cada nova amostra de medições que será avaliada, o contexto é analisado (dia da semana, feriado, condições de tempo, etc.), para que o sistema possa escolher o perfil adequado. Caso as medições da unidade consumidora avaliada forem muito diferentes do perfil selecionado para a avaliação, o sistema deve emitir um alerta de consumo suspeito.

Yang ET al. [113] [114] propõem um Modelo de detecção baseado em Mistura Gaussiana (*Gaussian-Mixture Model-based Detection* (GMMD)) para detectar ataques de integridade dos dados de medição. Para cada consumidor foram utilizadas as seguintes

informações: intervalo de tempo das medições, valor das medições e dia da medição, sendo que, para cada consumidor foram selecionados *m* dias (geralmente um mês) como conjunto de dados de treinamento para aprender as características de consumo do consumidor. Com as características definidas, o modelo de Mistura Gaussiana foi utilizado para dividir os dados de treinamento em *k* clusters. Após a criação dos clusters o sistema aprende os valores mínimos e máximos de cada cluster, que são utilizados para determinar se o valor de medição no intervalo de tempo *t,* no dia *n* é benigno ou malicioso. Os dados medidos que estiverem fora do intervalo dos valores mínimos e máximos aprendidos na fase de treinamento serão classificados como maliciosos, caso contrário, serão classificados como normais.

Em [115] Viegas e Vieira buscam identificar consumidores fraudulentos utilizando clusterização em indicadores de características dos dados de consumo de energia. Os indicadores representam a relação entre o consumo atual e passado, mudanças de padrão de consumo por horário, diferença de consumo entre consumidores com características semelhantes e diferenças no padrão de consumo dos consumidores com características semelhantes em diferentes horários. Os indicadores são então clusterizados com o objetivo de descobrir consumidores fraudulentos. A detecção de consumidores fraudulentos consiste em medir a distância dos indicadores clusterizados em relação aos centroides dos clusters. Quanto maior a distância dos indicadores em relação aos centroides, maior a chance de um consumidor ser acusado com fraudulento. Os algoritmos K-Means, Fuzzy C-Means e Gustafson-Kessel fuzzy foram utilizados nos testes. Segundo os autores o algoritmo Gustafson-Kessel fuzzy captura melhor o comportamento dos consumidores, conseguindo um bom desempenho com um baixo número de clusters, enquanto os algoritmos K-Means e Fuzzy C-Means só conseguem capturar o comportamento dos consumidores fraudulentos com um elevando número de clusters.

3.3. Considerações

Neste capítulo foram apresentados os trabalhos encontrados na literatura que se relacionam a esta pesquisa. Os trabalhos baseados em estados utilizam dispositivos específicos como sensores para detectar ações indevidas sobre qualquer elemento da rede de distribuição e assim gerar alarmes que permitam identificar uma fraude em andamento. Todavia, esses

sistemas têm um alto custo de implantação e manutenção, e o grande volume de alarmes falsos gerados pelos sensores dificultam o uso prático dessa abordagem.

O Quadro 4 apresenta um resumo das principais características dos trabalhos baseados perfil de consumo. Na tabela é possível observar a estratégia adotada por cada trabalho e as informações utilizadas para caracterizar o perfil de consumo de uma unidade consumidora. Os trabalhos baseados em perfil estatístico levam geralmente em consideração a média e o desvio padrão. Conforme Mcloughlin *et al.* [116] caracterizar perfis de consumo utilizando técnicas tradicionais de análise de dados tais como a estatística descritiva, em especial quando a média ou processos de agregação são aplicados, está tornando-se cada vem mais difícil. É preciso utilizar outros métodos para analisar grande quantidade de dados. Outra técnica bastante utilizada nesses trabalhos é a aprendizagem de máquina supervisionada. Os trabalhos que utilizam essa abordagem têm em comum as seguintes características: necessitam ser treinados com dados normais e anormais para que possam fazer a classificação dos consumidores e necessitam de uma grande quantidade de dados de treinamento, geralmente mais de cinquenta por cento das entradas da base de dados são utilizadas para realizar o treinamento do modelo. Por fim, estratégias baseadas em aprendizagem de máquina não-supervisionada procuram estabelecer um perfil de consumo normal e medir a distância do consumo suspeito em relação ao normal. Essa abordagem dispensa o uso de uma base rotulada com consumos normais e falsos. Contudo, como a distância máxima aceitável entre o consumo suspeito e o normal é frequentemente imposta de forma heurística, os trabalhos avaliados geraram uma alta taxa de falsos positivos, o que é indesejável.

Ainda no Quadro 4 é possível observar que a maioria dos sistemas existentes compromete a privacidade do consumidor ao utilizar dados históricos de consumo e outras informações como número de pessoas residindo em uma unidade consumidora ou ainda, o número de aparelhos que utilizam energia elétrica. Por fim, também foi possível observar que poucos trabalhos têm utilizado a abordagem de um medidor coletivo para encontrar consumidores fraudulentos. Entre os trabalhos que utilizam aprendizagem de máquina não-supervisionada, nenhum utiliza a abordagem de um medidor coletivo, além de não estarem preocupados com a privacidade dos consumidores.

Quadro 4: Principais características dos trabalhos encontrados na literatura.

Autor	Tipo de Perfil	Estratégia	Técnica	Medidor coletivo	Privacidade
[83]	1*	E	ARMA-GLR		
[84]	1*	E	CUSUM - Shewhart		
[46], [85]	1*	E	Decomposição LU	X	X
[86]	1*	E	Bandas de Bollinger e POMDP	X	
[87]	2*	E	gráfico de controle multivariado		
[88], [89]	1*	E	Mínimos quadrados recursivos	X	
[90]	1*	E	Polinômio de Lagrange	X	
[92]	1*	E	Séries temporais		
[93], [94]	2*	E	Regressão Linear	X	
[91]	2*	E	ANOVA		
[49]	1*	S	SVM		
[95]	2*	S	SVM		
[96]	3*	S	Redes Neurais e SVM		
[97], [42]	3*	S	Regras empíricas e SVM		
[98]	1*	S	SVM e Fuzzy		
[99]	2*	S	C4.5 e SVM	X	
[100]	1*	S	FCM e SVM	X	
[101]	1*	S	K-Means e SVM	X	X
[102], [103]	2*	S	ELM		
[104]	3*	S	OPF		
[105]	3*	S	OPF-HS		
[106]	2*	S	C4.5		
[107]	2*	NS	Redes Neurais		
[108]	1*	NS	Árvore de decisão / M5P		
[109] [110]	3*	NS	Fuzzy C-Means		
[111]	1*	NS	PCA - DBSCAN		
[112]	4*	NS	Aprendizagem de máquina contínua		
[113], [114]	3*	NS	Modelo de Mistura Gaussiana		
[115]	2*	NS	Gustafson-Kessel fuzzy		

1* - perfil individual - informações de consumo (medidas)
2* - perfil individual - informações de consumo e outras características
3* - diversos perfis individuais - informações de consumo
4* - diversos perfis coletivos - informações de consumo
E - Estatístico / S - Supervisionado / NS - Não-Supervisionado

No capítulo seguinte, é descrita a abordagem metodológica com as etapas do método utilizado.

Capítulo 4

Abordagem Metodológica

Este capítulo visa apresentar o método e as técnicas que compõem a metodologia de pesquisa utilizada para o desenvolvimento do presente trabalho. Segundo Lakatos e Marconi [117] “O Método Científico é o conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo – conhecimentos válidos e verdadeiros, traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista”. Assim o método do presente trabalho segue as orientações da Pesquisa de Desenvolvimento, proposta por Maren [118]. Segundo o Maren, esta pode assumir três formas: desenvolvimento de conceito, o desenvolvimento do objeto e o desenvolvimento de habilidades pessoais.

Como o presente trabalho tem como objetivo propor um sistema de detecção de consumidores fraudulentos esta pesquisa enquadra-se como desenvolvimento do objeto. Tal método envolve quatro etapas principais: Análise do Mercado, Análise do Objeto, Preparação e Desenvolvimento. As próximas seções apresentam as atividades desenvolvidas em cada uma das etapas.

4.1. Etapa 1 – Análise do Mercado

O objetivo foi pesquisar na literatura trabalhos que estavam preocupados com perdas não-técnicas causadas por consumidores finais em redes elétricas inteligentes, para avaliar a importância e a viabilidade dessa proposta. Durante a pesquisa observou-se que a grande maioria dos trabalhos estavam preocupados com perdas não-técnicas na transmissão e distribuição e poucos com a identificação de consumidores finais fraudulentos. Os trabalhos que focavam os consumidores estavam na sua grande maioria preocupados em descobrir acessos não autorizados, todavia, não faziam uma avaliação dos dados de medição, para avaliar se durante os acessos não autorizados foram causadas perdas não-técnicas. Os trabalhos que estavam preocupados com perdas não-técnicas causadas por consumidores finais utilizavam

bases antigas. Essas bases de dados eram compostas por apenas uma medição mensal para cada unidade consumidora, o que não correspondia ao padrão de medição da AMI em REIs. Criado o aporte motivacional, deu-se da análise do objeto.

4.2. Etapa 2 – Análise do Objeto

Nessa etapa, houve a preocupação de identificar trabalhos que estavam preocupados com perdas não-técnicas no domínio de consumo. Assim, foi realizada a revisão da literatura onde se pesquisou artigos publicados em periódicos científicos, conferências, simpósios e *workshops*, durante o período de 2008 a 2017. Escolheu-se esse período por ser uma área ainda relativamente nova, em relação a outras áreas. As bases de pesquisa foram: IEEEXplore; *Association for ComputingMachinery* (ACM); *Science Direct*, SCOPUS, Springerlink e portal de periódicos da CAPES.

Foram realizadas três revisões da literatura, a primeira no primeiro bimestre de 2015, a segunda, no primeiro bimestre de 2016 e terceira no início do segundo semestre de 2017.

4.3. Etapa 3 – Preparação

Com base na Análise do Mercado e na Análise do Objeto foi possível planejar os procedimentos para elaboração do sistema.

4.3.1. Procedimentos para o Desenvolvimento do Sistema

Para a concepção do sistema proposto algumas atividades foram realizadas:

- Identificou-se fontes de perdas técnicas nas redes secundárias;
- Identificou-se estratégias para estimar perdas técnicas em redes secundárias;
- Analisou-se os sistemas mais conhecidos apontados durante a fase de revisão da literatura. Alguns sistemas foram implementados;
- Observou-se as principais características das bases disponíveis e utilizadas nos trabalhos encontrados;

- Identificou-se a anatomia dos principais tipos de FDIs utilizados para ocultar o real consumo de energia de uma unidade consumidora;
- Buscou-se estratégias de identificação de anomalias que estavam sendo utilizadas em sistemas de detecção de intrusão que poderiam ser aplicadas na identificação de anomalias no perfil de consumo de uma unidade consumidora.

4.3.2. Materiais utilizados

Para o desenvolvimento das estratégias propostas foram utilizados os softwares Matlab 2014 [119] e Mathematica [120].

4.3.3. Conjunto de dados utilizado

A base de dados utilizada no presente trabalho foi desenvolvida pela *Commission for Energy Regulation* (CER) [121] da Irlanda e disponibilizada em [122]. A base é composta por cinco mil unidades consumidoras. O período de monitoramento de referência é de julho de 2009 a dezembro de 2010. O consumo de eletricidade (KWh) é medido em intervalos de trinta minutos, o que gera quarenta e oito medições diárias para cada unidade consumidora. Na base de dados, cada medida representa o consumo no intervalo de tempo de trinta minutos. A base não informa a medida acumulada. Mais informações e testes realizados sobre a base podem ser encontradas em [123].

A Figura 7 ilustra o consumo de uma unidade consumidora selecionada aleatoriamente da base de dados. O retângulo indica um período de consumo muito baixo, possivelmente devido à ausência de moradores, que será uma fonte importante de falsos positivos. Esse fato ocorre em várias unidades consumidoras e pode ser caracterizado como um período de férias.

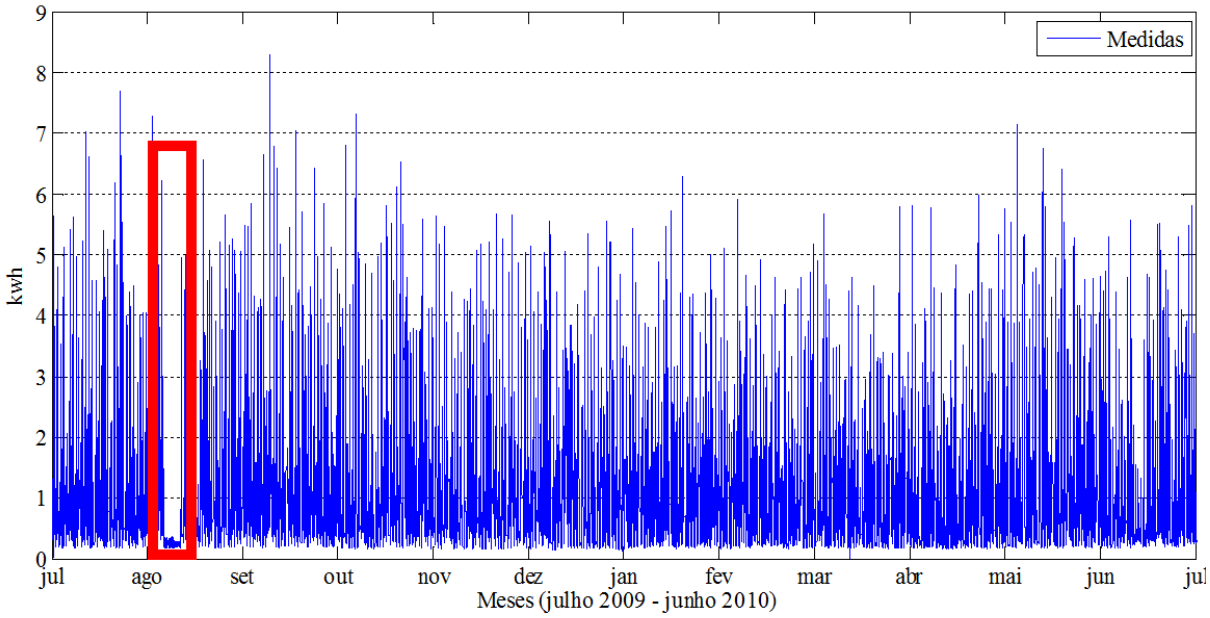

Figura 7: Consumo de energia de uma unidade consumidora.

4.4. Etapa 4 - Desenvolvimento

Na última etapa foram realizados testes e a avaliação do sistema. Os testes realizados tinham os seguintes objetivos:

a) Determinar as melhores condições de ajuste de vários parâmetros que influenciam o desempenho dos algoritmos do sistema proposto;
b) Obter o desempenho do sistema proposto;
c) Identificar qual das estratégias de clusterização propostas para o sistema apresentam melhor desempenho;
d) Determinar o desempenho da estratégia de detecção proposta sob diferentes condições de ataque, ou seja, sob os diversos tipos de FDIs que podem ser utilizados para se cometer uma fraude.

Para avaliação das estratégias propostas deve-se levar em consideração a proporção de unidades consumidoras anômalas em relação às normais. Como descrito na seção 2.5 algumas métricas podem induzir a uma conclusão errada sobre o desempenho de um sistema de classificação quando o conjunto de dados é desequilibrado. Para evitar conclusões equivocadas o sistema proposto foi avaliado utilizando as métricas de taxa de falso positivo (TFP), taxa de verdadeiros positivos (TVP) e medida F. Outro critério importante para determinar o impacto

do uso do sistema proposto é o lucro da concessionária de energia. Para fazer essa avaliação a equação (34), apresentada na seção 2.5, foi utilizada.

4.5. Considerações

Nesse capítulo foi explicado o método científico utilizado para desenvolver um sistema para identificação de consumidores fraudulentos em REIs. Também foram apresentadas as ferramentas e a base de dados utilizada, bem como os procedimentos de testes e avaliação de desempenho das estratégias propostas. No capítulo 5 o sistema de identificação de consumidores fraudulentos proposto é apresentado.

Capítulo 5

Proposta

Este capítulo apresenta o sistema proposto para detecção de consumidores fraudulentos com suporte a infraestrutura avançadas de medição (AMI) em redes secundárias de energia elétrica.

Uma entidade chamada “detector de anomalias” é responsável pela detecção de inconsistências através da comparação do somatório das medidas de consumo dos medidores residenciais com o consumo monitorado por medidores conectados à saída dos transformadores de distribuição. Quando o número de unidades consumidoras alimentada pelo mesmo transformador for muito grande, múltiplos medidores conectados à rede secundária podem ser utilizados para criar subsistemas com poucas dezenas de casas.

A detecção de inconsistências pelo detector de anomalias é feita em dois estágios. No primeiro estágio o detector observa se os subsistemas monitorados estão em estado coerente, isto é, a energia medida pelos medidores conectados à rede secundária é compatível com aquela indicada pelos medidores das unidades consumidoras. Caso algum subsistema seja considerado em estado inconsistente, o segundo estágio é disparado para identificar o consumidor ou o conjunto de consumidores responsáveis pelo erro de energia no subsistema.

A detecção de inconsistência do subsistema é feita no primeiro estágio resolvendo-se um conjunto de equações analíticas que modelam as perdas técnicas da rede que conecta o transformador aos consumidores finais. A identificação de consumidores fraudulentos no segundo estágio é realizada utilizando técnicas de aprendizagem de máquina que detectam anomalias nos perfis de consumo dos consumidores conectados a um subsistema inconsistente.

5.1. Detector de Anomalias

A Figura 8 ilustra um sistema de distribuição secundário e os elementos necessários para implementar o sistema de detecção de consumidores fraudulentos proposto. A abordagem proposta requer o uso de medidores conectados à rede secundária (medidor de baixa tensão -

MBT) para medir a energia fornecida por um transformador de distribuição. Quando o número de unidades consumidoras conectadas ao mesmo transformador for muito grande, MBT(s) adicionais podem ser utilizados para dividir a rede elétrica em subsistemas conforme indicado pelas letras “A” e “B” na Figura 8.

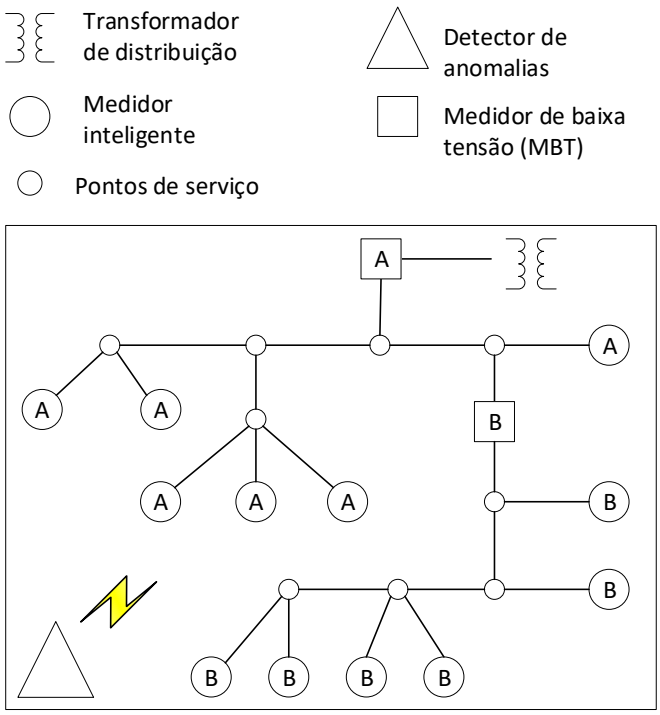

Figura 8: Sistema de distribuição secundário de um bairro.

Uma entidade denominada “detector de anomalias” é responsável por detectar inconsistências comparando o consumo reportado pelos medidores residenciais e os MBT(s). Conceitualmente, o detector de anomalias pode ser implantado em qualquer lugar, incluindo, remotamente, no centro de controle da concessionária de energia. Todavia, para reduzir o risco de comprometer a privacidade dos consumidores, é proposto que o detector de anomalias seja colocado nas proximidades da região que está monitorando. O detector de anomalias e os medidores inteligentes devem preferencialmente formar uma rede hermética, utilizar endereçamento privado e toda a comunicação deve ser máquina a máquina (M2M). Nessa abordagem, o centro de controle da concessionária tem acesso limitado ao detector e recebe apenas alarmes e relatórios baixa frequência. Por sua vez, o detector de anomalias recebe regularmente através da AMI as medidas de consumo das unidades consumidoras e do(s) MBT(s), em intervalos de uma hora ou menos. Todavia, apenas as medidas de consumo mais recentes são armazenadas, reduzindo assim a exposição dos consumidores, caso a segurança do detector for comprometida.

Para detectar inconsistências, o detector deve considerar as perdas técnicas na rede secundária e a imprecisão dos medidores inteligentes. Se o subsistema monitorado pelo MBT for muito grande, pequenos furtos de energia podem ser ocultados devido às incertezas quanto às perdas técnicas e imprecisões das medições. Para reduzir a incerteza, múltiplos MBT(s) podem ser utilizados para dividir um subsistema em subsistemas menores. Nesse caso a energia fornecida para um subsistema é calculada pela diferença entre as energias reportadas pelos MBT(s) que isolam o subsistema. Em cada intervalo de tempo (*t*), o detector consultará todos os medidores em um subsistema *S* para estimar a diferença entre a energia fornecida pela rede e a energia relatada pelos medidores inteligentes do subsistema como segue:

$$e_{MS}(t) = e_{TL}(t) + \xi \sum_{s \in S} e_s(t) \tag{35}$$

$$\Delta e(t) = \frac{e_{MS}(t) - e_G(t)}{e_G(t)} \tag{36}$$

Na equação (35), tem-se:

- $e_{TL}(t)$: São as perdas técnicas estimadas no subsistema *S*;
- ξ: São os erros de medição dos medidores;
- $e_s(t)$: É a medida de consumo do medidor inteligente $s \in S$;
- $e_{MS}(t)$: É a estimativa da energia fornecida para o subsistema S.

Na equação (36), tem-se:

- $e_G(t)$: É a energia relatada pelo MBT;
- $\Delta e(t)$: É a razão entre a energia relatada pelo MBT e a estimada no subsistema *S*.

O fator $\xi \geq 1$ é utilizado para evitar o desencadeamento incorreto do sistema causado por erros de medição relacionados a imprecisão dos medidores inteligentes. As equações (35) e (36) só são válidas se todos os medidores estiverem perfeitamente sincronizados e o detector de anomalias for capaz de receber todas as medidas de consumo dentro do intervalo de tempo (*t*). Por isso, utilizar uma única estimativa de $\Delta e(t)$ para detectar uma anomalia em um sistema de energia seria uma estratégia pouco realista. É preciso avaliar um conjunto maior de observações para gerar um alerta de anomalia no subsistema. No presente trabalho, a lógica do

detector de anomalias é modelada através de máquinas de estados, conforme será apresentado nas próximas subseções.

5.1.1. Máquina de Estados do Detector de Anomalias de Subsistemas

O detector de anomalias de subsistemas mantém uma máquina de estados para cada subsistema e uma máquina de estados independente para cada consumidor no subsistema. De acordo com a Figura 9, um subsistema pode estar em três estados: normal (G^1), suspeito (G^2) ou anormal (G^3).

Um subsistema é considerado em um estado normal se o consumo relatado pelos medidores inteligentes mais as perdas técnicas estimadas ($e_{MS}(t)$) é consistente com o consumo relatado pelo MBT ($e_G(t)$). O subsistema estará em um estado suspeito, quando o valor calculado para $\Delta e(t)$ exceder a um limiar, porém, são necessárias mais observações para afirmar que está ocorrendo um roubo de energia. O estado suspeito é uma prevenção para evitar que o subsistema entre em um estado anormal devido ao atraso ou perda de medidas de consumo vindas dos medidores. O detector avalia o estado do subsistema em intervalos regulares. A transição entre os estados é controlada pelos limiares ε_1 e ε_2. Estes limiares são limites impostos em relação à razão da energia relatada pelo MBT e a estimada $e_{MS}(t)$, definida na equação (36) por $\Delta e(t)$. O limiar ε_1 é o limite imposto a $\Delta e(t)$ em uma única observação, ε_2 é um limite para a média dos valores de $\Delta e(t)$ em sucessivos intervalos observados. Estes limiares estão relacionados com o conhecimento sobre o número de consumidores ligados ao transformador de distribuição, enlaces de comunicação, precisão dos medidores e perdas técnicas. O subsistema começa em G^1, e a cada intervalo de tempo $\Delta e(t)$ é calculado. Quando $\Delta e(t) < \varepsilon_1$, significa que o somatório das energias relatadas pelas UCs pertencentes ao subsistema mais a estimação das perdas técnicas está abaixo do limite imposto em relação à energia medida pelo MBT. A máquina de estados do subsistema move-se então para G^2, e $\Delta e(t)$ é adicionado ao conjunto E. O conjunto E é utilizado para acumular $\Delta e(t)s$ observados sucessivamente.

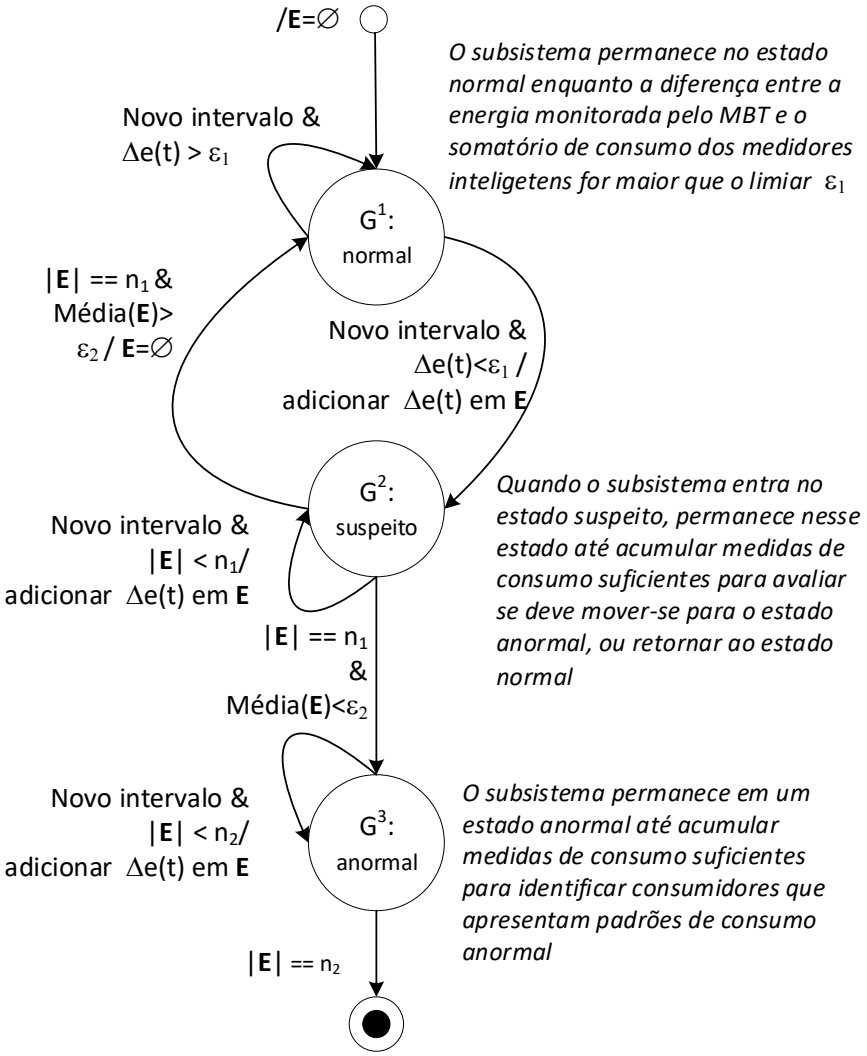

Figura 9: Possíveis estados de um subsistema.

O sistema permanece em G^2 até acumular n_1 observações de $\Delta e(t)$, por exemplo, $|E| == n_1$. Então, se a média do conjunto $E < \varepsilon_2$, o sistema move-se para G^3, caso contrário, volta para G^1. O sistema permanece no estado G^3 até acumular medidas de consumo suficientes (n_2) para permitir identificar consumidores com padrões anormais, enquanto o subsistema também está em estado anormal. Uma vez que o sistema se move para G^3, ele não voltará para G^1 sem uma inspeção local do subsistema ou uma reinicialização manual do detector de anomalias, mesmo se o consumo relatado pelo MBT e os medidores inteligentes se tornam consistentes novamente. A seguir a máquina de estados dos consumidores é apresentada.

5.1.2. Máquina de Estado do Detector de Consumidores Fraudulentos

A máquina de estados utilizada para representar o detector de consumidores fraudulentos é exibida na Figura 10. Um consumidor pode estar em um dos seguintes estados durante o monitoramento: normal (C^1), transitório (C^2) ou suspeito (C^3). A máquina de estado do consumidor é atualizada quando uma nova medida de consumo é recebida do medidor inteligente correspondente. O estado de um consumidor é dependente do estado do subsistema à qual ele está conectado. Se o subsistema está no estado normal (G^1) não há roubo, e todos os consumidores conectados a este subsistema estão em um estado normal (C^1). Quando um subsistema está em um estado normal, medidas de consumo são utilizadas para atualizar o conjunto de dados normais dos consumidores. Se o subsistema está em estado anormal (G^3), todos os consumidores conectados ao subsistema são considerados suspeitos (C^3). Quando um consumidor está em um estado suspeito, medidas de consumo não são mais utilizadas para atualizar o conjunto de dados normais. Em vez disso, elas são utilizadas para criar um conjunto de dados suspeitos para que seja confrontado com o conjunto de dados normais. Os consumidores estão em um estado transitório (C^2), quando o subsistema está em um estado suspeito (G^2), e o detector está aguardando por mais medidas de consumo para determinar se o subsistema tem de ser colocado em um estado anormal ou não. Quando os consumidores estão em um estado transitório, medidas de consumo são armazenadas em um conjunto de dados transitório (T). Estas medidas são movidas para o conjunto de dados normais ou suspeitos do consumidor, uma vez tomada a decisão sobre o estado do subsistema.

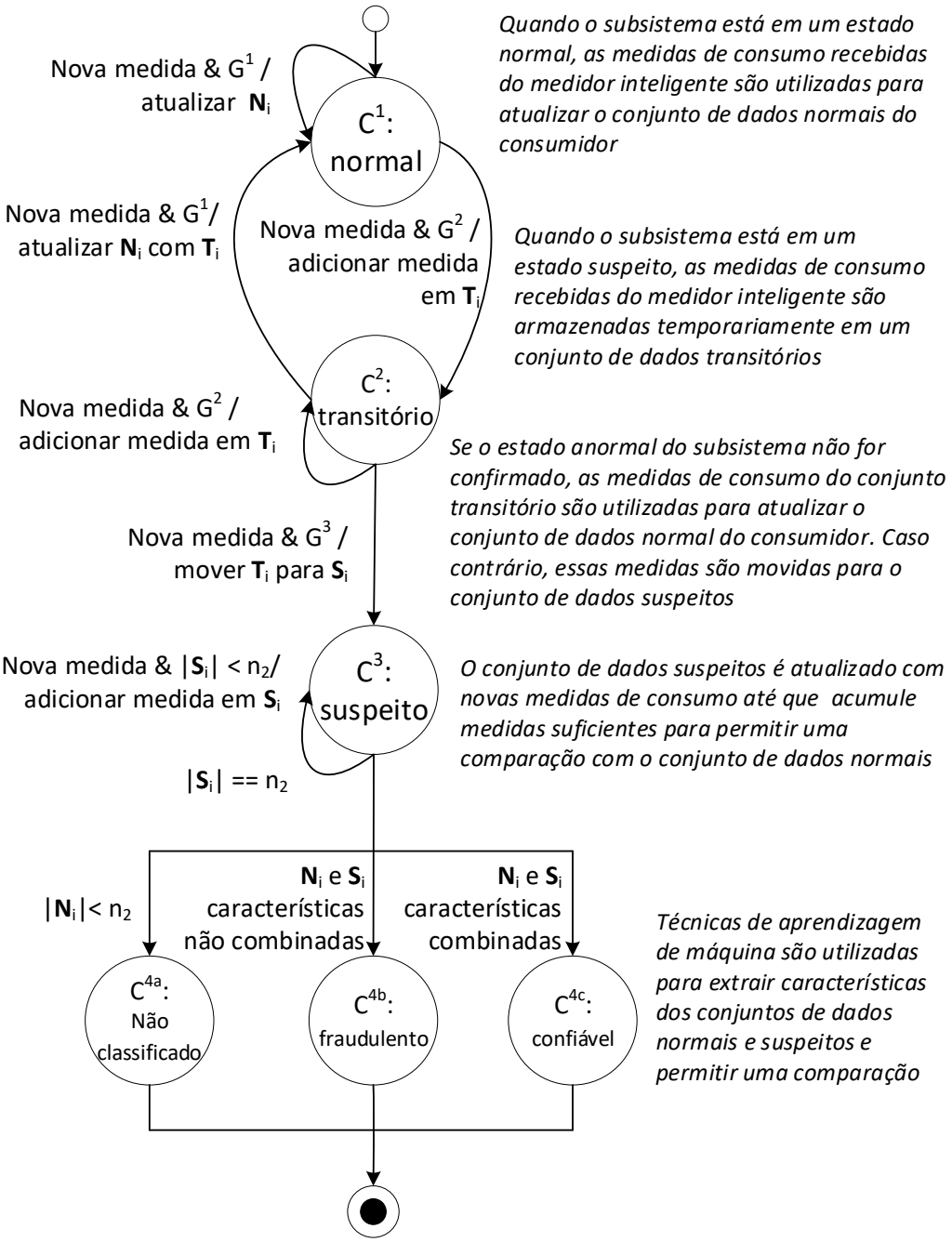

Figura 10: Possíveis estados de um consumidor em um subsistema.

No estado C^1, medidas de consumo são armazenadas em N_i (conjunto de dados normais do consumidor i^{th}). No estado de C^3, as medidas são armazenadas em S_i (conjunto de dados suspeitos do consumidor i^{th}). Ambos N_i e S_i têm tamanho máximo igual à n_2. N_i é uma janela deslizante que é atualizada continuamente enquanto o subsistema permanece em um estado normal. Quando o subsistema está em um estado anormal, o conjunto S_i deve receber as medidas de consumo. No estado C^2, as medidas são armazenadas temporariamente em T_i (conjunto de dados transitório do consumidor i^{th}). Se o subsistema se mover de G^2 para G^1, as

medidas armazenadas em T_i devem substituir as medidas mais antigas armazenadas em N_i, caso contrário, elas serão utilizadas para construir o conjunto S_i. Quando o detector obtém uma quantidade suficiente de medidas de consumo, com o subsistema em um estado anormal, a máquina de estados que representa o consumidor termina, e a decisão se o consumidor deve ser inspecionado é tomada. A decisão final pode colocar um consumidor em um dos seguintes estados finais: não-classificado (C^{4a}), fraudulento (C^{4b}) ou confiável (C^{4c}). O estado não-classificado significa que o detector não foi capaz de tomar uma decisão sobre um consumidor. Essa condição pode ocorrer para novos consumidores, quando o subsistema se move para o estado anormal antes de ocorrer a coleta de medidas de consumo suficientes para construir um conjunto de dados normais do consumidor. Um caso particular pode surgir quando um alarme de anomalia é acionado para o subsistema, mas o detector não pode identificar qualquer consumidor como fraudulento ou confiável. As possíveis causas deste estado podem estar relacionadas com falhas na rede de distribuição, ou a consumidores que fazem conexão ilegal diretamente nas linhas secundárias. Neste caso, as linhas e o transformador do subsistema devem ser inspecionados para detectar a causa da anomalia no subsistema da rede. Os consumidores que forem classificados como fraudulentos (C^{4b}) devem ser inspecionados. Consumidores que forem classificados pelo sistema como confiáveis (C^{4c}), são considerados consumidores honestos e não precisam ser inspecionados.

5.2. Perfis de Consumo de Vida Curta

A abordagem proposta é baseada no conceito de perfis de consumo de Vida Curta (VC). Um perfil de VC captura o comportamento de um consumidor por um curto período, que pode ser de poucos dias a algumas semanas, apenas o suficiente para detectar uma fraude em andamento. Um conceito chave de perfis de VC é que nenhuma informação sazonal é utilizada. Os perfis de VC são sensíveis a grupos de aparelhos utilizados simultaneamente durante um intervalo de medição e a frequência com que são utilizados. Perfis de longa duração, por outro lado, não podem ignorar informações sazonais, porque o comportamento dos consumidores pode ser significativamente influenciado por estações do ano, dias da semana ou feriados. No entanto, a correlação sazonal é muito difícil de ser capturada e é uma das principais fontes de falsos alarmes. Reduzindo o período de observação, encontra-se uma solução que é ao mesmo tempo mais simples e robusta contra mudanças no comportamento do consumidor. Essa

estratégia é inovadora em relação aos trabalhos citados no Quadro 4, página 63, e faz com que o sistema se adapte rapidamente a mudanças no padrão de consumo da unidade consumidora, sem a necessidade de utilizar outras informações como por exemplo, o número de pessoas e/ou quantidade de aparelhos eletrônicos pertencentes a uma unidade consumidora.

Na abordagem proposta perfis de VC são comparados através dos conjuntos N_i e S_i como exibido na Figura 10. Para realizar essa comparação são extraídas características de N_i para determinar limites de consumo que devem ser respeitados em um futuro próximo, representado por S_i. O número de medidas de consumo em N_i e S_i é o mesmo, n_2. O valor ótimo para n_2 é discutido na seção 6.3. Para criar os perfis de consumo de N_i e S_i são utilizados algoritmos de agrupamento, para agrupar as medidas de consumo semelhantes e extrair as características, utilizando métricas sobre centroides de agrupamento ou de frequência de itens em cada agrupamento. A estratégia de agrupamento permite criar perfis de consumo, mesmo quando algumas medidas de consumo destoam dos valores frequentes do conjunto de dados. Serão avaliados três algoritmos de agrupamento, FCM (Fuzzy C-Means), K-Means e SOM (*self-organized map*) para determinar qual é o mais adequado para a abordagem proposta.

Para todos os algoritmos, o conjunto de dados de entrada $X = \{x_1, \dots, x_n\}$ são as medidas de consumo a partir de N_i ou S_i. A estratégia proposta não leva em conta correlações sazonais, os elementos do conjunto de dados de entrada são escalares. Por exemplo, nas Figuras 11, 12 e 13 são mostrados os resultados dos três algoritmos de agrupamento aplicados nas medidas de consumo de um único consumidor. Nas três figuras, a coluna "Normal" foi gerada através da aplicação do algoritmo de agrupamento para o conjunto de dados normais (N_i). A coluna "nãoFDI" foi gerada a partir do conjunto de dados suspeitos (S_i), mas assumindo que o consumidor não tenha cometido nenhuma fraude. As colunas restantes foram geradas a partir da aplicação dos seis tipos de FDIs definidos no Quadro 2, página 37, para o conjunto de dados suspeitos (S_i). A quantidade de energia removida no exemplo foi a mesma para todos os tipos de FDIs, e corresponde a 20% do consumo real. Para os métodos K-Means e FCM, Figuras 11 e 12 respectivamente, os pontos exibidos nas figuras correspondem aos centroides dos agrupamentos. Para o método SOM, os círculos representam os nós (neurônios) e as fatias escuras representam o número de elementos do conjunto de dados de entrada que foram mapeados para o nó. O algoritmo SOM foi treinado utilizando dados normais N_i, e cada elemento dos conjuntos N_i e S_i foi mapeado para o nó que representa melhor o elemento. Nas três figuras, nós e centroides estão ordenados em relação ao consumo de energia que representam, a partir do mais baixo (inferior) consumo até o mais alto (superior).

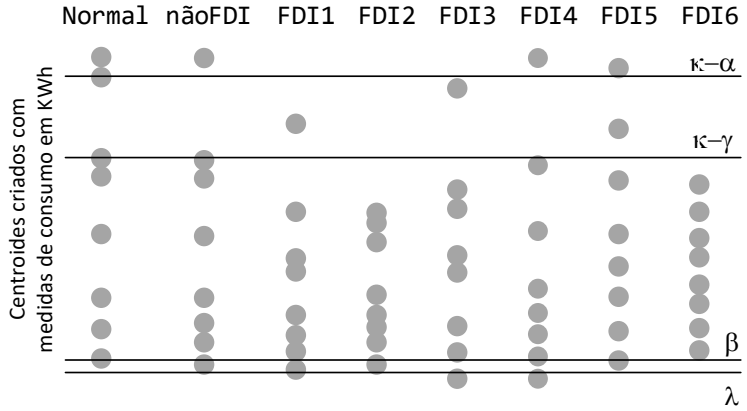

Figura 11: Como os FDIs afetam a clusterização no algoritmo K-Means.

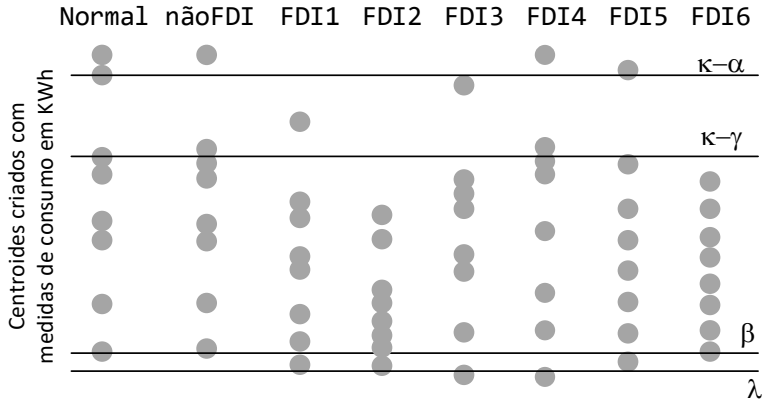

Figura 12: Como os FDIs afetam a clusterização no algoritmo FCM.

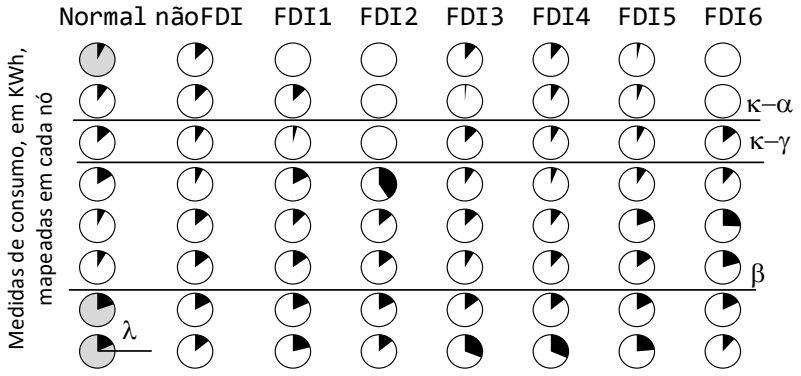

Figura 13: Como os FDIs afetam a clusterização no algoritmo SOM.

Utilizando a representação do algoritmo SOM como referência, é possível observar como os FDIs afetam as medidas de consumo de forma diferente. O FDI1 diminui todas as medidas de consumo em um percentual fixo, deixando o nó que representa as medidas mais altas vazio. O FDI2, afeta principalmente as medidas de consumo mais altas. O FDI3, reduz todas as medidas de consumo através de um valor constante, de modo que, o efeito é mais

significativo para as medidas mais baixas. O FDI4, afeta um intervalo específico de medidas de consumo, aumentando a taxa de medidas de baixo consumo. O efeito de FDI5 é semelhante ao do FDI1. O FDI6 cria um novo perfil de consumo sintético, por isso, não há nenhuma correspondência com o perfil de consumo normal. As representações de K-Means e FCM mostram que a maioria dos FDIs afetam significativamente o valor de cada um dos centroides, representados nas figuras através de sua localização (posição). Assim, é possível medir os deslocamentos dos centroides para detectar anormalidades no conjunto de dados avaliados.

As linhas horizontais nas Figuras 11, 12 e 13 identificadas como *k*-α (*k* menos α), *k*-γ (*k* menos γ), β, e λ ilustram como as informações obtidas a partir dos agrupamentos podem ser utilizadas para fazer comparações entre os conjuntos de dados normais e suspeitos. O parâmetro *k* representa o número de agrupamentos criados. Para o método SOM é possível criar regras com base no número de medidas de consumo classificadas em cada um dos nós. Por exemplo, uma regra pode indicar que o número total de medidas de consumo de todos os nós acima de *k*-γ-linha de um perfil suspeito, não pode ser menor que, o número de medidas de consumo que fazem parte do nó mais alto de um perfil normal. Esta regra permitiria detectar o FDI de tipo 2. Uma segunda regra poderia indicar que, o número de medidas de consumo pertencentes ao menor nó do perfil suspeito, não pode ser maior do que, o número de medidas de consumo pertencentes ao menor nó do perfil normal dividido por um fator λ. Esta segunda regra permitiria detectar FDIs dos tipos 3 e 4. Regras mais complexas podem ser definidas através da imposição de condições simultâneas, tal como, comparar o número de medidas de consumo acima de *k*-α-linha e abaixo de β-linha, com o número de medidas de consumo no nó mais alto e nó mais baixo do perfil normal, respectivamente. As regras devem ser cuidadosamente planejadas para não classificar incidentalmente um conjunto de dados sem FDIs (normal) como anormal e gerar falsos alarmes.

A mesma ideia pode ser aplicada aos métodos baseados em centroides, tais como K-Means e FCM. Uma regra poderia ser definida utilizando o conceito que o maior centroide (mais alto) do conjunto de dados suspeitos não pode ser menor que o centroide-*k*-γ do conjunto de dados normais. Esta regra isolada permite a detecção dos FDIs dos tipos 2 e 6 em ambos os métodos de agrupamento. Outra regra poderia assegurar que o menor centroide do conjunto de dados suspeitos não pode ser inferior ao menor centroide do perfil de consumo normal multiplicado por um fator λ. Esta regra seria capaz de detectar os FDIs dos tipos 3 e 4 em ambos os métodos de agrupamento. Regras mais complexas podem impor condições simultâneas, tais como, o maior e o menor centroide do conjunto de dados suspeitos não pode ser inferior ao centroide *k*-α e ao menor centroide do conjunto de dados normais, respectivamente. Esta

regra permitiria detectar os FDI dos tipos 1, 2 e 3, em ambos os métodos de agrupamento, sem disparar um falso alarme.

Para fins de ilustração, o número de centroides utilizados nas figuras foi pequeno. No entanto, resultados mais precisos podem ser obtidos utilizando um maior número de agrupamentos. Neste caso, o processo de criação de regras com base na saída dos algoritmos de agrupamento pode tornar-se complexo. Na próxima seção é explicado o processo de extração de características semi-automatizado que é válido para qualquer número de agrupamentos.

5.3. Processo de Extração de Características Semi-automatizado

As características são extraídas a partir dos dados agrupados, medindo a distância entre os centroides (FCM e K-Means), ou contando o número de medidas de consumo mapeadas em cada agrupamento (SOM). É proposto um método semi-automatizado para extrair as características das saídas dos algoritmos de agrupamento. As características são definidas de forma paramétrica. Os parâmetros são determinados utilizando um procedimento de otimização que maximiza uma função objetivo sujeita a restrições nas taxas de verdadeiros positivos ou falsos positivos. A abordagem de extração de características para os métodos K-Means e FCM é ilustrada na Figura 14.

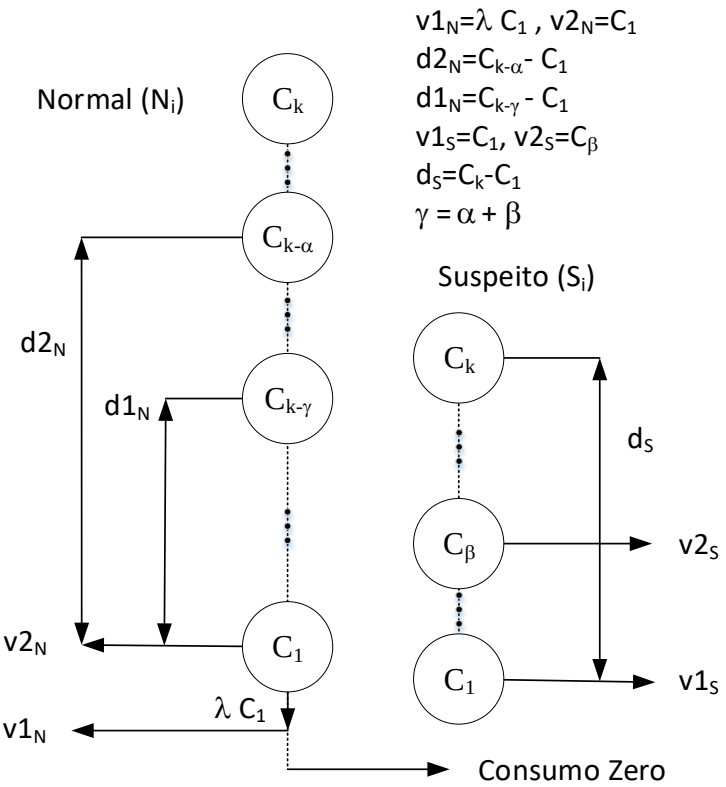

Figura 14: Extração de características para os métodos K-Means e FCM.

Os centroides são classificados a partir de C^1 (o mais baixo) para C^k (o mais alto), onde k é o número de agrupamentos usados. As características são parametrizadas por α, β ∈ $\mathbb{N}^*$, tal como $0 \leq \alpha + \beta \leq k$ e $0 < \lambda < 1$. Os parâmetros α, β e λ controlam o quão semelhante às medidas normais e suspeitas devem ser para que um consumidor possa ser considerado confiável. Eles também controlam qual parte do perfil de consumo é observado (medidas de consumo, alto, médio ou baixo). Um consumidor é considerado fraudulento (estado C^{4b}) se a expressão lógica (37) for verdadeira.

$$v1_S < v1_N \vee d_S < d1_N \vee (v2_S < v2_N \wedge d_S < d2_N) \qquad (37)$$

A expressão define que um consumidor é considerado fraudulento se as medidas de baixo consumo caírem excessivamente, ou a variabilidade das medidas de consumo diminuírem excessivamente, ou ainda se, as medidas de baixo consumo e a variabilidade caírem moderadamente, mas simultaneamente.

A abordagem de extração de características para o algoritmo SOM é ilustrada na Figura 15.

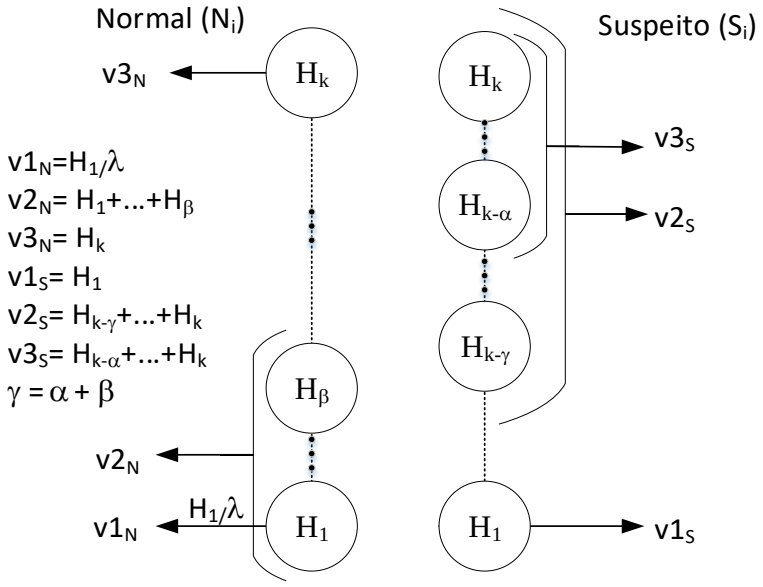

Figura 15: Extração de características para o método SOM.

Os nós são classificados de H_1 (neurônio que representa as menores medidas) para H_k (neurônio que representa as maiores medidas), onde k é o número de nós (neurônios). As características são extraídas com base no número de medidas de consumo em cada neurônio, ou seja, o número de entradas do conjunto de dados fornecido que foram mapeadas para cada um dos neurônios. O símbolo H_i representa o número de medidas de consumo do neurônio i^{th}. Como antes, os recursos são parametrizados por $0 \leq \alpha + \beta \leq k$ e $0 < \lambda < 1$. Um consumidor será considerado fraudulento (estado C^{4b}) se a expressão lógica (38) for verdadeira.

$$v1_S > v1_N \vee v2_S < v3_N \vee (v3_S < v3_N \wedge v1_S > v2_N) \qquad (38)$$

A expressão define que um consumidor é considerado fraudulento se o número de medidas de baixo consumo aumentar excessivamente, ou o número de medidas de alto consumo diminuir excessivamente, ou ainda se, as medidas de baixo consumo aumentar e as de alto consumo diminuem moderadamente, mas simultaneamente.

A próxima seção apresenta a estratégia adotada para afinar os diversos parâmetros do sistema proposto.

5.4. Afinação do Sistema de detecção de consumidores fraudulentos

No sistema proposto um conjunto de parâmetros (n_1, ε_1, ε_2) controla a detecção de anomalias nos subsistemas secundários e outro conjunto de parâmetros (n_2, k, α, β, λ) controla a detecção de consumidores fraudulentos. Os parâmetros (n_1, ε_1, ε_2) estão relacionados ao conhecimento sobre topologia da rede, links de comunicação, precisão dos medidores e perdas técnicas. O parâmetro ε_2 também pode ser utilizado para controlar a porcentagem de roubo de energia que justifica uma inspeção de campo. Esses parâmetros devem ser ajustados com base no conhecimento sobre uma implantação específica real. Os parâmetros (n_2, k, α, β, λ), por outro lado, podem ser afinados para maximizar o desempenho do sistema de detecção de consumidores fraudulentos. A afinação do sistema afeta o lucro da concessionária de energia, porque o aumento da TVP aumenta probabilidade de detectar um roubo de energia e um aumento na TFP aumenta o custo com inspeções desnecessárias. Para realizar o cálculo do lucro da concessionária a equação (34), apresentada na seção 2.5 é utilizada. A afinação do sistema de detecção de consumidores fraudulentos requer um conjunto de dados com medidas de consumo rotuladas como normais ou fraudulentas. O conjunto de dados deve conter uma quantidade suficiente de UCs e diferentes perfis de consumo para que o resultado da afinação possa ser aplicado a qualquer outro conjunto de consumidores.

O parâmetro n_2 representa a quantidade de medidas de consumo necessárias nos conjuntos normais (N_i) e suspeitos (S_i). O parâmetro k é o número de clusters (K-Means e FCM) ou neurônios (SOM) utilizado pelos algoritmos de agrupamento. A escolha de α, β, λ depende do objetivo do sistema. Valores mais baixos de β e α tornam o sistema mais rigoroso, forçando os consumidores a apresentar limites de consumo máximos e mínimos similares em N_i e S_i. Tanto a TVP como a TFP diminuem com esses parâmetros. Valores baixos de λ tornam o sistema mais tolerante a um maior número de medidas de baixo consumo ou inatividade, diminuindo o TVP e o TFP. Dado n_2, os parâmetros (k, β, α e λ) podem ser determinados solucionando o seguinte problema de otimização:

$$\arg\max_{\alpha,\beta,\lambda} \boldsymbol{\mathcal{O}}(k,\alpha,\beta,\lambda) \quad sujeito\ a: \begin{cases} \alpha,\beta \in \mathbb{N} \wedge 1 \leq \beta+\alpha \leq k \\ \lambda \in \mathbb{R} \wedge \lambda \in [0,1] \end{cases} \tag{39}$$

Em (39), $\mathcal{O}$ é a função objetivo que está sendo maximizada, por exemplo, o lucro da concessionária P^* (equação (34)), a medida F (equação (32)). Além disso, limites de TVP ou TFP podem ser utilizados como restrições adicionais. Observe que n_2 é uma entrada para o problema de otimização. Idealmente, n_2 representa o menor número de medidas de consumo que permitem ao sistema identificar a origem das fraudes com precisão.

5.5. Considerações

Este capítulo apresentou o sistema de detecção de consumidores fraudulentos proposto no presente trabalho. O sistema foi modelado utilizando máquinas de estados que trabalham em conjunto para identificar consumidores fraudulentos. A máquina de estados dos consumidores proposta pode utilizar diferentes estratégias de aprendizagem de máquina para criar perfis de consumo individuais de vida curta. O perfil de consumo de vida curta proposto no presente trabalho captura o comportamento de um consumidor por um curto período de tempo sem levar em consideração outras informações das unidades consumidoras. Para extrair características dos perfis de consumo de vida curta foi proposto um procedimento de extração de características semi-automatizado que maximiza uma função objetivo sujeita a restrições. Esse procedimento faz com que o sistema possa ser configurado de acordo com os interesses da concessionária de energia, aumentando a taxa de detecção de fraudes ou diminuindo a taxa de falsos alarmes. Nos próximos capítulos são realizados testes e avaliações do sistema proposto. Em um primeiro momento as máquinas de estados serão avaliadas de forma isolada e na sequência o sistema será testado e avaliado no todo.

Capítulo 6

Avaliação do Detector de Anomalias em Subsistemas

Este capítulo apresenta os principais testes que foram realizados com o detector de anomalias em subsistemas. O capítulo está dividido em quatro seções principais. Na seção 6.1 é apresentada a preparação da base de dados utilizada para os testes. Foi necessário adotar uma estratégia para criar as medidas dos medidores de baixa tensão (MBTs), uma vez que, as bases de dados encontradas na revisão da literatura não apresentam leituras de MBTs. Na subseção 6.1.3 é apresenta a estratégia de poluição da base de dados, visto que nenhuma das bases encontradas apresentava informações sobre UCs poluídas. Na seção 6.2 é apresentado como seu deu a estimação das perdas técnicas no detector de anomalias do subsistema através das informações recebidas do MBT e das UCs do subsistema monitorado. Na seção 6.3 são apresentadas as estratégias de estimação e validação dos parâmetros ε_1 e ε_2 do detector de anomalias de subsistemas. Na seção 6.4 são apresentados os testes utilizados diferentes números de unidades consumidoras por MBT. Esses testes têm como objetivo avaliar o desempenho do detector de anomalias para diferentes tamanhos de subsistemas. Por fim, na seção 6.5 são apresentadas as considerações finais do capítulo.

6.1. Preparação da base de dados

A base de dados de dados utilizada no presente trabalho foi disponibilizada pela *Commission for Energy Regulation* (CER) [121] da Irlanda e é composta somente por informações de consumo das UCs (quantidade de energia consumida em certo intervalo de tempo). Como o sistema proposto faz uso de um MBT, que mede a quantidade de energia fornecida a um subsistema em certo intervalo de tempo, foi necessário gerar as medidas do mesmo. Na abordagem proposta também é necessário que os medidores inteligentes reportem a tensão RMS (*Root Mean Square*) média observada durante um intervalo de medição de consumo juntamente com a medida de consumo. Essas informações são utilizadas no detector de anomalias do sistema proposto para estimar as perdas técnicas. Na seção 6.1.1 é explicado o

sistema de equações proposto para gerar a tensão RMS na entrada das UCs e as medidas do MBT, já que a base de dados utilizada não continha essas informações.

Na descrição da base de dados original também não havia nenhuma informação sobre a precisão dos medidores utilizados para fazer a leitura de consumo das UCs. Assumiu-se que, as medidas disponíveis correspondiam exatamente a energia consumida em cada uma das UCs. Para efeito dos testes, também foi necessário simular a imprecisão dos medidores inteligentes. Na seção 6.1.2 é explicado como se deu o processo de geração de erros de imprecisão nas medidas de consumo das UCs e do MBT.

Para avaliar o sistema de detecção de consumidores fraudulentos proposto, foi necessário simular o furto de energia em algumas UCs da base. Na seção 6.1.3 é apresentada a estratégia utilizada para poluir a base de dados original.

6.1.1. Estratégia de estimação das medidas de consumo dos MBTs e tensões na entrada das UCs

Para avaliar o detector de anomalias proposto são necessárias medidas de consumo de um MBT, que mede a quantidade de energia fornecida a um subsistema em certo intervalo de tempo (t), bem como, medidas de consumo das UCs e o valor da tensão na entrada das mesmas. Idealmente, o consumo de energia do lado secundário de um transformador é igual à soma dos consumos de todas as cargas conectadas. Na prática, de acordo com Ni *et al* [124], esse princípio não pode ser utilizado para gerar a leitura de um MBT por uma série de incertezas, entre elas:

- A fase que cada medidor está conectado;
- A queda do nível de tensão;
- A perda nos condutores;
- O grau de desequilíbrio de sistemas trifásicos;
- A imprecisão da leitura dos medidores inteligentes.

Devido a esses fatores foi preciso simular uma rede secundária para que algumas incertezas estivessem presentes na leitura do MBT. Para a geração das incertezas é preciso conhecer alguns detalhes da rede secundária, como: topologia e parâmetros físicos das linhas/cabos. Segundo [125] as concessionárias de energia, geralmente, não possuem todos os dados que caracterizam as redes secundárias. Devido à ausência dessas informações algumas

premissas foram adotadas, como, a topologia da rede e cabeamento. Para gerar a topologia da rede de distribuição secundária o Módulo 7 da Agência Nacional de Energia Elétrica (ANEEL) [33] que trata da apuração das perdas foi utilizado. Nesse módulo a ANEEL determina que na ausência de informação sobre topologia, cada circuito do sistema secundário deve ser classificado de acordo com uma das cinco tipologias da Figura 16, ou seja, conforme o comprimento total do circuito, em metros. As características de cada configuração estão resumidas na Tabela 1. A variável L_{circ} refere-se ao comprimento do circuito em metros.

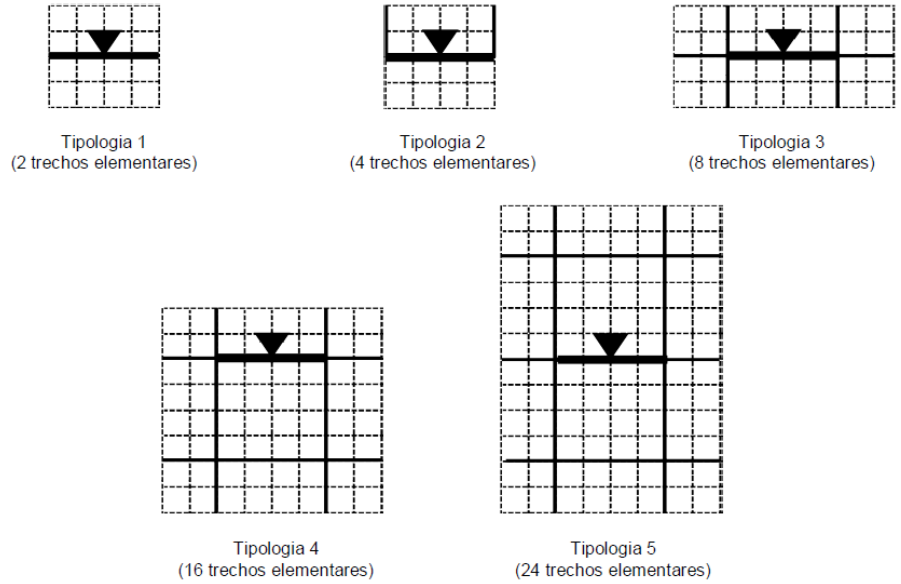

Figura 16: Tipologia das redes secundárias, [33].

Tabela 1: Características típicas das tipologias de redes secundárias, [33].

Tipologia	Comprimento
1	$L_{circ} \leq 100$
2	$L_{circ} \leq 200$
3	$L_{circ} \leq 350$
4	$L_{circ} \leq 500$
5	$L_{circ} \geq 500$

No presente trabalho a tipologia 3 foi escolhida por ser uma tipologia intermediaria e representar a maioria das redes secundárias em bairros residenciais. Como a base de dados [121] utilizada no presente trabalho é composta por cinco mil UCs, foram simulados diversos subsistemas para a tipologia. A Tabela 2 apresenta o número de UCs por agrupamento e o número de subsistemas criados. O número de cinquenta unidades consumidoras por subsistema foi adotado, pois, segundo [126] a maioria dos transformadores de distribuição atende a essa média de unidades consumidoras em bairros residenciais.

Tabela 2: Número de UCs por subsistema e número de subsistema para a tipologia de testes.

Tipologia	Subsistemas	Número de UCs
3	100	50

Para a criação dos subsistemas foi adotado que o sistema de distribuição secundário utiliza uma série padronizada de cabos com resistência constante e com distribuição de carga uniforme e balanceada. Sendo que cada subsistema está ligado a um transformador de distribuição secundário. As UCs pertencentes a cada um dos subsistemas foram sorteadas aleatoriamente da base de dados original, e para cada UC, um comprimento de cabo, em metros, foi sorteado de acordo com a tipologia 3.

A Figura 17 apresenta o circuito da rede secundária utilizado para cada um dos subsistemas simulados. Assumiu-se que, o MBT está junto ao transformador de distribuição.

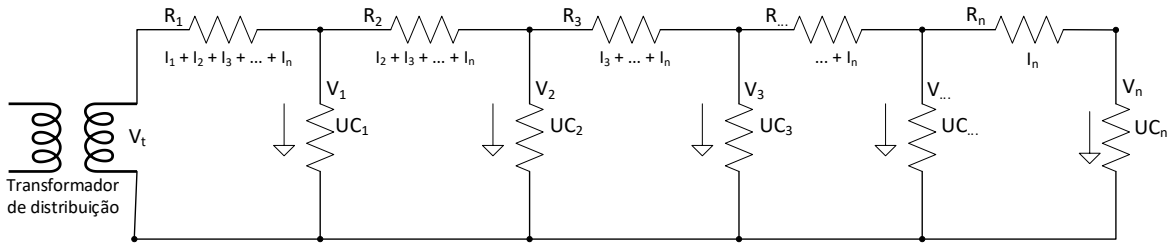

Figura 17: Circuito de uma rede secundária.

Através do circuito apresentado na Figura 17 um sistema de equações lineares foi desenvolvido para estimar a energia mensurada em um MBT e a voltagem (V) na entrada de cada UC. O sistema de equações lineares apresentado em (40) tem como entrada a tensão da rede da secundária (V_t), quantidade de energia consumida em certo intervalo de tempo (KWh) por cada unidade consumidora (UC) e a resistência dos cabos (R). Sendo que, a resistência dos cabos é obtida através da multiplicação do seu comprimento pelo fator de resistência do mesmo. Como a base de dados utilizada para gerar as leituras dos MBTs e as voltagens (V) na entrada de cada UC, foi disponibilizada pela *Commission for Energy Regulation* (CER) [121] da Irlanda, utilizou-se V_t=230, uma vez que, essa é a tensão padrão nas redes secundárias da Irlanda [127]. Assumiu-se ainda que, as medidas de consumo das UCs da base de dados estão livres de erros de imprecisão dos medidores, e que a energia mensurada no MBT não contém erros de imprecisão do MBT.

Na linha 1, do sistema de equação (40), é calculada a potência média consumida pela UC durante o intervalo de tempo entre duas medições sucessivas. Como as informações sobre consumo das UCs disponíveis na base de dados foram coletadas em intervalos de trinta minutos,

foi necessário dividir o consumo por dois, já que, o KWh se refere ao consumo durante uma hora. Na linha 2 são estimadas as correntes ($\mathrm{I}_{1\ldots n}$) e nas linhas 3 a 7 é estimada a tensão perdida em cada trecho do circuito. Nas linhas 8 a 12 são formuladas as equações para determinar a tensão (V) na entrada de cada UC. Resolvendo-se o sistema de equações lineares formado pelas equações de eq_1 a eq_n determina-se o valor de V_1 até V_n. Uma vez resolvido o sistema de equações, a corrente total ($\mathrm{I_t}$) é calculada, e por fim, é estimada a energia medida pelo MBT para o intervalo de tempo de trinta minutos.

$$
\begin{array}{ll}
1 & P_{1\ldots n} = UC_{1\ldots n} * 1000/2 \\
2 & \mathrm{I}_{1\ldots n} = P_{1\ldots n} / V_{1\ldots n} \\
 & \\
3 & v_1 = R_1 * (I_1 + I_2 + I_3 + \cdots + I_n) \\
4 & v_2 = R_2 * (I_2 + I_3 + \cdots + I_n) \\
5 & v_3 = R_3 * (I_3 + \cdots + I_n) \\
6 & \vdots \\
7 & v_n = R_n * I_n \\
 & \\
8 & eq_1 = V_\mathrm{t} - v_1 == V_1 \\
9 & eq_2 = V_\mathrm{t} - v_1 - v_2 == V_2 \\
10 & eq_3 = V_\mathrm{t} - v_1 - v_2 - v_3 == V_3 \\
11 & \vdots \\
12 & eq_n = V_\mathrm{t} - v_1 - v_2 - v_3 - \cdots - v_n == V_n \\
 & \\
13 & \mathrm{I_t} = \sum_{1}^{n} \mathrm{I} \\
 & \\
14 & P_t = V_t * \mathrm{I_t} \\
15 & KWh_{MBT} = P_t * 2/1000
\end{array}
\tag{40}
$$

Onde:

- $UC_{1\ldots n}$: Energia consumida em cada UC em KWh;
- $P_{1\ldots n}$: Potência em cada UC;
- $V_{1\ldots n}$: Tensão que se deseja estimar em cada UC;
- $I_{1\ldots n}$: Corrente estimada para cada trecho do circuito;
- $R_{1\ldots n}$: Resistência do cabo, levando-se em consideração o comprimento, multiplicado pelo fator de resistência do mesmo;
- $v_{1\ldots n}$: Tensão perdida em cada trecho do circuito;
- $eq_{1..n}$: Equações que devem ser resolvidas pelo sistema de equações lineares;
- $\mathrm{I_t}$: Corrente total do circuito;
- V_t: Tensão de entrada no sistema secundário;

- P_t: Potência total do circuito;
- KWh_{MBT}: Energia mensurada no MBT.

6.1.2. Imprecisão dos medidores inteligentes

Como já apresentado no referencial teórico, existem diversas classes de precisão em que os medidores podem ser enquadrados, ficando a critério de cada distribuidora a escolha dos medidores. A Companhia Paranaense de Energia (Copel) através norma técnica ETC 4.04 [39] determinou que medidores eletromecânicos residenciais utilizados pela companhia devem ter classe de precisão de 1% (classe B) [16] ou melhor. Segundo a fabricante ELO [128] os medidores de classe B são recomentados para realizar medições em instalações de consumidores de baixa tensão. De acordo com a fabricante Landis+Gyr [129] medidores de classe C (precisão 0,5%) [16] devem ser utilizados para consumidores de médio e grande porte. No presente trabalho os MBTs foram considerados como medidores de médio porte. Para cada medida disponível na base de dados foi gerado um erro aleatório de ± 1% nas medidas dos medidores residenciais e de ± 0,5% nas dos MBTs. Para gerar o erro aleatório a distribuição uniforme [130] foi utilizada.

6.1.3. Poluição da Base de Dados

A identificação de consumidores fraudulentos utilizando as medições coletadas pela AMI é um assunto recente e ainda não foram disponibilizadas bases com dados de consumidores normais e fraudulentos. Para realizar a avaliação das estratégias de detecção propostas foi necessário poluir a base de dados com os tipos de FDIs exibidos no Quadro 2. Foram criadas seis bases, cada base contendo um dos tipos de FDIs descritos. Sendo que, em cada base 10% das unidades consumidoras (500 UCs) foram selecionadas aleatoriamente e poluídas em diferentes momentos. Para os FDIs dos tipos 1, 5 e 6, o parâmetro y foi definido como $0{,}1 < y < 0{,}8$. Para o FDI4, definiu-se t randomicamente entre 4 e 48. Para os FDIs 2 e 3 c foi configurado de forma a causar um roubo entre [0,1, 0,8]. As Figuras 18 e 19 exibem o perfil de consumo durante um dia de uma unidade consumidora. A linha pontilhada indica o

consumo normal enquanto as outras linhas exibem a alteração do perfil de consumo quando utilizado alguns dos tipos de FDIs exibidos na Quadro 2.

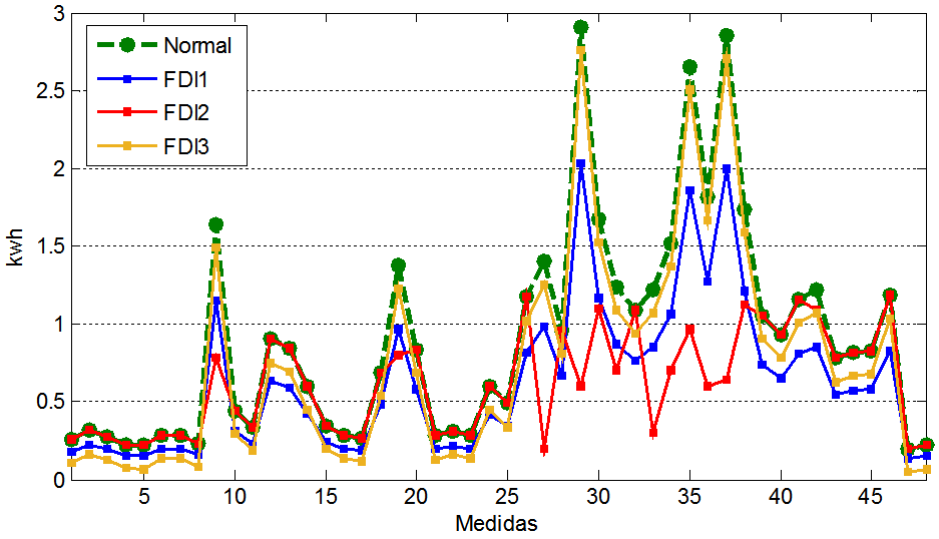

Figura 18: Exemplos dos FDIs 1, 2 e 3.

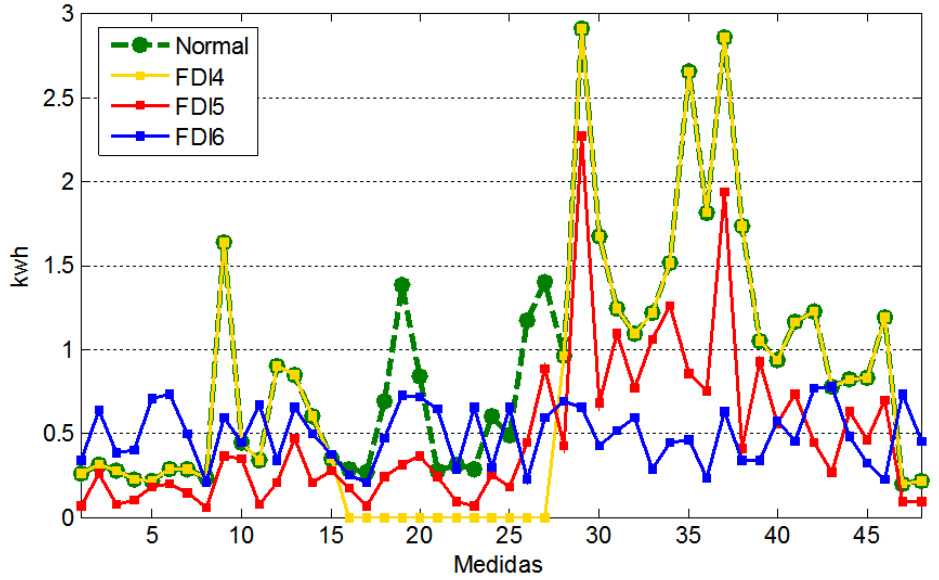

Figura 19: Exemplos dos FDIs 4, 5 e 6.

6.2. Estimativas das perdas técnicas no Detector de Anomalias de Subsistemas

Nesse trabalho adotou-se uma abordagem que permite estimar as perdas técnicas sem conhecer os detalhes das redes de distribuição de energia elétrica secundárias. Para que essa

abordagem possa ser utilizada o detector de anomalias de subsistemas, deve receber a cada intervalo de tempo, a leitura do MBT, as medidas de consumo e tensões das UCs ligadas ao MBT. De posse dessas informações o mesmo utiliza um sistema de equações lineares, proposto logo a seguir, para estimar as perdas técnicas no subsistema avaliado. As perdas técnicas estimadas mais o somatório do consumo de energia relatada pelos consumidores ligados a um MBT deve ser consistente com a energia monitorada pelo MBT. Caso ocorram inconsistências no subsistema avaliado uma fraude pode estar em andamento. Todavia, algumas incertezas da rede secundária podem prejudicar a identificação de inconsistências. Para verificar o funcionamento do detector de anomalias de subsistemas, as premissas a seguir foram adotadas, com o objetivo de minimizar a ocorrência de inconsistências, sem que uma fraude esteja ocorrendo no subsistema avaliado.

- Todas as UCs ligadas ao transformador são equipadas com medidores inteligentes;
- A energia consumida com iluminação pública é medida por um medidor inteligente;
- Os medidores são capazes de reportar a tensão RMS média observada durante um intervalo de medição de consumo;
- Não existe perda de dados na comunicação entre os medidores e detector de anomalias;
- O sistema elétrico é trifásico e está equilibrado;
- Cada medidor residencial está conectado a apenas uma fase, sendo que cada fase é avaliada de forma independente.

Isoladas as principais fontes de inconsistências, um sistema de equações lineares foi proposto para estimar as perdas técnicas no subsistema avaliado. O sistema de equações lineares é apresentado na equação (41) e tem como entrada as informações de consumo de energia e voltagens disponibilizadas ao detector de anomalias pelo MBT e pelas UCs monitoradas pelo MBT. Nas linhas 1 a 4 do sistema de equações (41) é ilustrado o cálculo das medidas de consumo recebidas das unidades consumidoras ($UC_{1\dots n}$) e do MBT (KWh_{MBT}) para potência, bem como, o calculo da corrente total do circuito (I_t), e da corrente consumida em cada unidade consumidora ($I_{1\dots n}$). Nas linhas 5 a 9 é verificada a queda da tensão em cada trecho do circuito e nas linhas 10 a 14 a corrente consumida. Por fim, na linha 15 é estimada a perda técnica em KWh no circuito secundário avaliado. A estimativa da perda técnica é utilizada para determinar o valor de $\Delta e(t)$ na equação (36), apresentada na seção 5.1, que utiliza as perdas técnicas e

informações de consumo para verificar a existência de divergências entre o somatório de consumo das UCs e a medida do MBT.

$$
\begin{array}{ll}
1 & P_t = KWh_{MBT} * 1000/2 \\
2 & I_t = P_t/V_t \\
3 & P_{1\ldots n} = UC_{1\ldots n} * 1000/2 \\
4 & I_{1\ldots n} = P_{1\ldots n}/V_{1\ldots n} \\
5 & \Delta V_1 = V_{\mathrm{t}} - V_1 \\
6 & \Delta V_2 = V_1 - V_2 \\
7 & \Delta V_3 = V_2 - V_{\ldots} \\
8 & \vdots \\
9 & \Delta V_n = V_{\ldots} - V_n \\
10 & \Delta I_1 = I_{\mathrm{t}} \\
11 & \Delta I_2 = I_{\mathrm{t}} - \mathrm{I}_1 \\
12 & \Delta I_3 = I_{\mathrm{t}} - \sum_1^2 \mathrm{I} \\
13 & \vdots \\
14 & \Delta I_n = I_{\mathrm{t}} - \sum_1^{\ldots} \mathrm{I} \\
15 & e_{TL}(t) = \left(\sum_1^n \Delta V * \Delta I \right) * 2/1000
\end{array}
\tag{41}
$$

Onde:

- KWh_{MBT}: Energia mensurada no MBT;
- P_t: Potência total do circuito;
- V_{t}: Tensão do sistema secundário;
- $\mathrm{I_t}$: Corrente total do circuito;
- $UC_{1\ldots n}$: Energia consumida em cada unidade consumidora em KWh;
- $P_{1\ldots n}$: Potência em cada UC;
- $V_{1\ldots n}$: Tensão medida em cada UC;
- $I_{1\ldots n}$: Corrente em cada UC;
- $\Delta V_{1\ldots n}$: Representa a tensão perdida em cada trecho do circuito;
- $\Delta I_{1\ldots n}$: Representa a corrente consumida em cada trecho do circuito;
- $e_{TL}(t)$: Representa a perda técnica total em KWh estimada para o circuito no intervalo de tempo monitorado.

6.3. Estimação e Avaliação dos parâmetros do detector de anomalias em subsistemas

O detector de anomalias em subsistemas pode estar em três estados: normal (G^1), suspeito (G^2) ou anormal (G^3) e utiliza os parâmetros ε_1 e ε_2 para tomar a decisão de mover-se de um estado para o outro. O primeiro parâmetro ε_1 é um limite que faz com que o sistema mova-se do estado normal (G^1) para o estado suspeito (G^2), observado um único $\Delta e(t)$. Já ε_2 é um limite que faz com que o sistema tome a decisão de voltar para o estado normal (G^1), ou mover-se para o estado anormal (G^3), observando a média de sucessivos $\Delta e(t)s$.

Na sequência de estados do detector de anomalias de subsistemas, o primeiro parâmetro a ser ponderado é o limiar ε_1, sendo que o limiar ε_2 só será avaliado se ε_1 for rompido. Devido a essa característica do detector de anomalias de subsistemas a estimação e validação do parâmetro ε_1 foi realizada em um primeiro momento. Obtido o melhor valor para ε_1, deu-se a estimação e validação do parâmetro ε_2. Para realizar-se a estimação de ambos os parâmetros foi utilizada a base de dados sem furtos de energia, configurada de acordo com a tipologia criada na seção na 6.1.1, sendo que a imprecisão dos medidores também foi considerada. Na fase de avaliação dos parâmetros as bases de dados poluídas foram utilizadas levando-se em consideração a imprecisão dos medidores e a tipologia criada na seção na 6.1.1. Sendo que no cenário de fraudes, em todos os subsistemas, em algum instante, uma ou mais UCs estavam cometendo uma fraude. As seções, 6.3.1 e 6.3.2 apresentam respectivamente a estimação e validação dos parâmetros ε_1 e ε_2.

6.3.1. Estimação e validação do parâmetro ε_1

Para realizar a estimação do valor do parâmetro ε_1 os subsistemas criados na seção na 6.1.1 foram utilizados. Em cada subsistema, a cada intervalo de tempo, calculou-se o valor de $\Delta e(t)$ através da equação (36) apresentada na página 71. O valor de $\Delta e(t)$ é obtido através da comparação entre a medida fornecida pelo MBT e o somatório de consumo das UCs, levando-se em conta as perdas técnicas estimadas pelo sistema de equações descrito previamente e a imprecisão dos medidores. Através dos valores de $\Delta e(t)$ coletados estimou-se o valor de ε_1, posto que, o valor de $\Delta e(t)$ será comparado com ε_1, como apresentado na Figura 9, página 73. O valor estimado para ε_1 deve ser grande o suficiente para que, assim que um furto for iniciado

em um subsistema, o detector de anomalias de subsistemas mude do estado normal para suspeito. Valores muito conservadores podem fazer com que o detector de anomalias de subsistemas não mude de estado, ou ainda que, atrase a mudança de estado, o que prejudicaria a identificação dos consumidores fraudulentos pelo detector de consumidores fraudulentos.

A Figura 20 apresenta o histograma da frequência dos valores de $\Delta e(t)$. Na figura são exibidos os $\Delta e(t)$s obtidos a cada interalo de tempo, em um cenário sem furtos de energia, para todos os subsistemas. Como não há roubo de energia, a variação de $\Delta e(t)$ é provocada exclusivamente pela imprecisão dos medidores. Os menores valores de $\Delta e(t)$ representam as maiores diferenças entre a energia relatada pelo MBT e o somatório da energia consumida pelas UCs mais as perdas técnicas estimadas devido à imprecisão dos medidores. Nos casos em que $\Delta e(t)$ apresentou um valor maior que zero, significa que, o somatório da energia consumida mais a perda técnica estimada foi maior que a medida do MBT devido a imprecisão dos medidores.

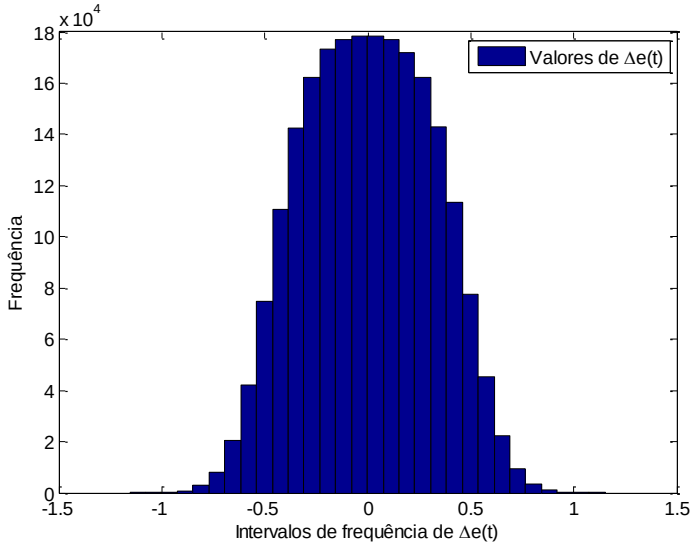

Figura 20: Histograma de frequência dos valores de $\Delta e(t)$.

Os valores de $\Delta e(t)$ expostos na Figura 20 apresentam similaridade com a distribuição normal. Todavia, ao se fazer o teste de aderência dos dados a distribuição normal, os mesmos foram rejeitados pelo teste de hipótese. Para o teste a função *lillietest* [131] do Matlab foi utilizada. A Figura 21 ilustra a relação dos dados com a distribuição normal, onde a linha pontilhada em vermelho é uma referência para julgar se os dados seguem uma distribuição normal. Como pode ser visualizado na figura, os maiores e menores valores de $\Delta e(t)$ afastam-se da linha da distribuição normal.

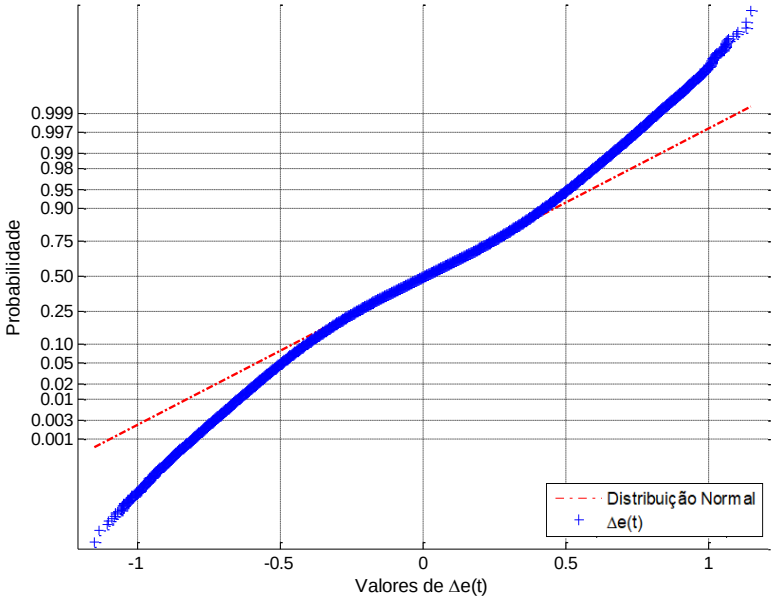

Figura 21: Teste com os $\Delta e(t)$s para uma distribuição normal.

Uma vez que os valores de $\Delta e(t)$ não puderam ser caracterizados como uma distribuição normal, a função de distribuição cumulativa empírica [132] foi utilizada. A Figura 22 apresentada o gráfico da distribuição com os valores de $\Delta e(t)$, onde é possível perceber a porcentagem de $\Delta e(t)$s que estão acima ou abaixo do valor que se pretende atribuir ao parâmetro ε_1. É possível observar que, todos os valores de $\Delta e(t)$ são maiores que -1,16%, ou ainda que, cinquenta por cento dos valos de $\Delta e(t)$ são menores que zero. Se ε_1 for configurado com zero, em cinquenta por cento das vezes o detector de anomalias de subsistemas deverá entrar em um estado suspeito (G^2), mesmo não havendo furtos de energia. Já para ε_1=-1,16% o sistema não deverá entrar em um estado suspeito em nenhuma das vezes. Todavia, em um cenário com furto de energia, a utilização de ε_1=-1,16% pode fazer com que o sistema não mude para o estado suspeito, ou atrase a mudança de estado. Para avaliar qual valor de ε_1 faz com que o detector mude para um estado suspeito, assim que uma fraude for iniciada, ε_1 foi testado com zero e -1,16%.

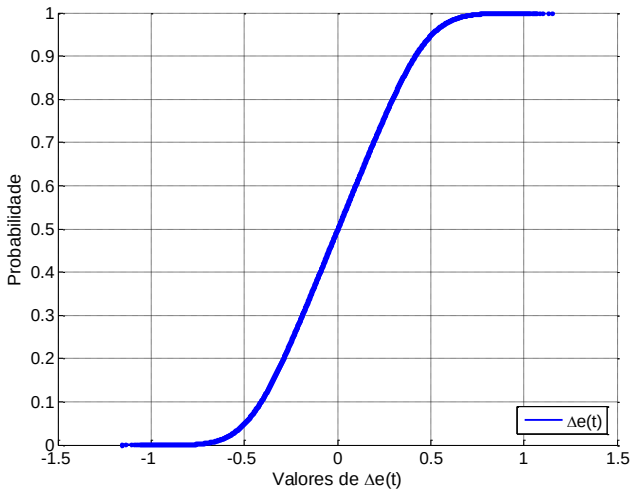

Figura 22: Valores de $\Delta e(t)$ representados através da distribuição cumulativa empírica.

Para os testes com o parâmetro ε_1 todos os subsistemas criados a partir das seis bases de dados poluídas foram utilizados. Para ambos os valores de ε_1 o detector de anomalias de subsistemas mudou de um estado normal (G^1) para um estado suspeito (G^2) de forma correta em todas as ocorrências de roubo. Todavia, em vários casos de fraude, o detector de anomalias de subsistemas deixou passar vários intervalos de tempo, sendo que cada intervalo de tempo representa a energia consumida por todas as UCs de um subsistema durante trinta minutos, antes de mudar do estado normal para suspeito. Na Tabela 3, é apresentado através dos percentis a quantidade de intervalos de tempo que se passaram a partir do início de uma fraude até a mudança do estado normal para suspeito para os dois valores de ε_1 testados. Cada linha da tabela corresponde a um percentil do conjunto de intervalos de tempo contabilizados após o início de uma fraude, mas que não romperam o limiar ε_1 e consecutivamente não fizeram com que o sistema mudasse do estado normal para suspeito. Por exemplo, para o percentil 95 (P95), em 5% dos casos de fraude, o detector de anomalias de subsistemas atrasou trezentos e cinquenta ou mais intervalos de tempo antes de mudar do estado normal para suspeito. Quando ε_1 foi avaliado com zero para o mesmo percentil, o detector atrasou poucos intervalos de tempo antes de mudar para o estado suspeito. Mesmo para o percentil 80 (P80), quando ε_1=-1,16%, em 20% dos casos de fraude o detector de anomalias de subsistemas atrasou 34 ou mais intervalos de tempo antes de mudar para o estado suspeito. Como ε_1 é o primeiro limiar do detector de anomalias de subsistemas, assumiu-se que, utilizar um valor baixo, como ε_1=-1,16%, poderia prejudicar a identificação de consumidores fraudulentos, nas próximas fases do sistema, uma vez que, para 20% (P80) dos casos de furto, muitos intervalos de tempo se passaram desde o início de uma fraude até que o sistema mudasse de estado. Dessa forma, zero foi definido para o limiar ε_1.

Tabela 3: Número de intervalos de tempo que se passaram a partir do início de uma fraude até a mudança do estado normal para suspeito para cada ε_1 testado.

Percentil	ε_1=0	ε_1=-1,16%
P100	8	2045
P95	2	350
P90	2	103
P85	1	56
P80	1	34
P50	1	7

6.3.2. Estimação e validação do parâmetro ε_2

Após a quebra do limiar ε_1, o sistema irá armazenar sucessivos $\Delta e(t)s$ em um conjunto E de tamanho n_1, como apresentado na Figura 9, página 73. O parâmetro ε_2 é um limite para a média do conjunto E. Ao avaliar o limiar ε_2 o detector de anomalias do subsistema retornará ao estado normal ou irá mover-se para o estado anormal (G^3). O valor de ε_2 deve ser suficientemente baixo de forma a não empurrar o sistema para o estado G^3 sem que uma fraude esteja ocorrendo. A mudança para o estado G^3 sem a ocorrência de furtos não é desejada nessa fase do sistema, o que ocasionaria a busca por consumidores fraudulentos de forma equivocada.

Para estimar o valor de ε_2 é preciso levar em consideração o tamanho (n_1) do conjunto E. Para os testes definiu-se que o tamanho do conjunto E poderia representar doze horas de observação, um dia, dois dias, quatro dias ou ainda uma semana, que equivalem respectivamente a: 24, 48, 96, 192 e 336 observações na base de dados utilizada para os testes.

Durante a fase de estimação do valor de ε_2, o detector de anomalias de subsistemas foi configurado com ε_1=0 e assim como na estimação de ε_1, todos os subsistemas criados a partir da base de dados normal foram utilizados. Toda vez que o limiar ε_1 era rompido, um conjunto E de tamanho n_1 era formado e a média do mesmo calculada e armazenada. Na Figura 23 a distribuição cumulativa empírica foi utilizada para exibir a média dos valores armazenados no conjunto E para os diferentes $n_1 s$. Através da figura é possível observar a porcentagem das médias dos conjuntos Es que estão acima ou abaixo do valor que se pretende atribuir ao parâmetro ε_2. Por exemplo, para n_1=48, cem por cento das médias dos conjuntos Es são maiores que -0,21%, ou ainda, cinquenta por cento das médias são menores que zero. Como já definido anteriormente o limiar ε_2 deve ser suficientemente baixo de forma a empurrar o sistema para o estado anormal somente quando uma fraude estiver em andamento. Para evitar que pequenas variações possam colocar o sistema no estado anormal, mesmo sem furtos de

energia, o limiar ε_2 será configurado como a menor média dos conjuntos Es mais um desvio padrão das médias dos conjuntos Es para cada n_1. A Tabela 4 apresenta o desvio padrão das médias dos conjuntos Es e a menor média dos conjuntos Es para cada n_1.

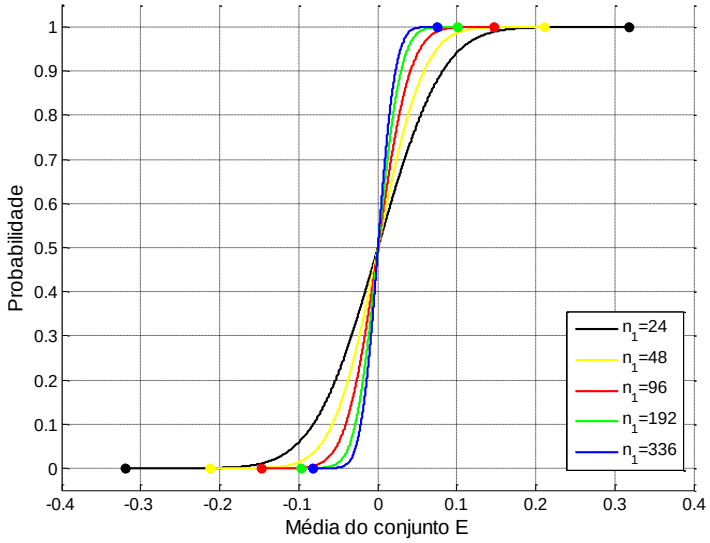

Figura 23: Variação da média dos conjuntos Es para os diferentes tamanhos de conjuntos avaliados.

Tabela 4: Menor média dos conjuntos Es para cada n_1 avaliado.

n_1	Menor média dos conjuntos Es	Desvio Padrão
24	-0,32	±0,08
48	-0,21	±0,05
96	-0,16	±0,03
192	-0,10	±0,03
336	-0,08	±0,02

Na fase de avaliação as seis bases de dados poluídas foram utilizadas e divididas de acordo com a tipologia apresentada na seção 6.1.1. Nessa fase, além de avaliar se o detector de anomalias do subsistema mudou do estado suspeito para anormal, quando uma fraude estava ocorrendo, também se buscou averiguar a quantidade de intervalos de tempo em que o montante de energia furtada não chegava a romper os limiares ε_1 e ε_2. Essa averiguação é necessária pelo fato que, o detector de consumidores fraudulentos, explicado na seção 5.1.2, página 74, precisa de dois conjuntos de medidas, um normal e um suspeito. O conjunto suspeito é formado pelas medidas a partir do intervalo de tempo em que o $\Delta e(t)$ calculado rompeu os limiares ε_1 e ε_2. As medidas anteriores ao intervalo de tempo que iniciou o conjunto suspeito são consideradas medidas normais. A utilização de medidas anormais no conjunto de dados normais poderá fazer

com que o sistema crie perfis de consumo falsos, o que dificultaria a identificação de consumidores fraudulentos pelo detector de consumidores fraudulentos.

Nos testes realizados com os valores estimados para ε_2, o detector de anomalias do subsistema não entrou nenhuma vez no estado anormal, sem que uma fraude estivesse em andamento. Em 99% das ocorrências de fraude, o sistema mudou de forma correta para o estado anormal, independentemente o tamanho do conjunto E. Na Figura 24, a média de intervalos de tempo para os seis tipos de FDIs, em que medidas fraudulentas eram reportadas, mas o valor calculado para $\Delta e(t)$ não rompia os limiares ε_1 e ε_2 é apresentada. Os percentis são utilizados na figura para visualizar, para cada porcentagem dos casos de fraudes identificadas, o número de intervalos de tempo em que fraudes estavam ocorrendo, mas que o valor calculado para $\Delta e(t)$ não chegou a romper os limiares ε_1 e ε_2. É possível observar que para n_1=336, percentil P90, em apenas 10% dos casos de fraudes identificadas, se passaram 79 ou mais intervalos de tempo desde o intervalo de tempo que de fato a fraude foi iniciada, até o início do armazenamento do valor de $\Delta e(t)$ no conjunto E que quebrou o limiar ε_2. Essa característica de intervalos de tempo em que fraudes estavam ocorrendo, mas não foram identificados pelo sistema como intervalos de tempo anormais ocorreu para todos os n_1 avaliados. Ou seja, os $\Delta e(t)s$ calculados com medidas fraudulentas não romperam os limiares ε_1 e ε_2.

Uma característica visualizada durante os testes chamou a atenção. O detector de anomalias também classificou intervalos de tempo em que não estavam ocorrendo roubo, como intervalos de tempo anormais. Essa classificação de forma equivocada pode prejudicar a criação dos perfis suspeitos no detector de consumidores fraudulentos. Na Figura 24, os valores negativos representam os intervalos de tempo em que medidas normais foram classificadas como anormais. Para n_1=336, percentil P70, em 70% dos casos de fraudes identificadas, foram contabilizados 140 ou mais intervalos de tempo em que o valor calculado para $\Delta e(t)$ foi armazenado no conjunto E que rompeu o limiar ε_2, mesmo que uma fraude não estivesse ocorrendo no intervalo de tempo avaliado. Já para n_1=24, percentil P10, em apenas 10% dos casos de fraudes o sistema classificou de forma equivocada 18 ou mais intervalos de tempo normais como anormais. Esse fato ocorreu uma vez que, ε_1 foi configurado de forma frouxa, o que fez com que o sistema se movesse para o estado suspeito (G^2) mesmo quando uma anomalia não estava ocorrendo. Ao mover-se para o estado G^2, $\Delta e(t)$s começavam a ser armazenados no conjunto E. Em muitos casos o detector de anomalias estava armazenando $\Delta e(t)$s e uma fraude foi iniciada. Ao calcular a média do conjunto E, o limiar ε_2 era excedido e uma anomalia era acusada pelo detector de anomalias. Essa característica ocorreu principalmente nos casos onde

o fraudador ao iniciar um roubo, roubava uma alta porcentagem de energia do subsistema monitorado. Assim, como não se deseja que o detector de consumidores fraudulentos utilize medidas fraudulentas na criação dos perfis normais, também não se quer que medidas normais sejam utilizadas na criação de perfis suspeitos. A utilização de várias medidas normais na criação dos perfis suspeitos pode fazer com que, uma UC fraudulenta que está originando um grande roubo de energia não seja detectada quando n_1s grandes forem utilizados. Por outro lado, para todos os valores de n_1 avaliados, em 10% dos casos (percentil P90), várias medidas fraudulentas foram utilizadas de forma equivocada para criar perfis normais de consumo. O que prejudicaria principalmente a detecção de UCs que estão roubando uma baixa porcentagem de energia. Como o detector de consumidores fraudulentos, mesmo em condições perfeitas, onde, assim que uma fraude tem início, faz uso das medidas anteriores ao período de fraude para criar os perfis normais, e utiliza as medidas após o aviso para criar os perfis suspeitos, não atinge cem por cento de sucesso, como será apresentado na secção 7.1.2, considera-se que para o sistema completo, a utilização de n_1 =24 fará com que o sistema apresente um melhor desempenho. Uma vez que as fraudes que demoram a ser identificadas pelo detector de anomalias de subsistemas, são provavelmente as UCs que não são identificadas pelo detector de consumidores fraudulentos. Na seção 8.1 são apresentados testes do sistema completo com três diferentes valores de n_1 para que se possa visualizar o efeito do valor de n_1 na detecção de consumidores fraudulentos.

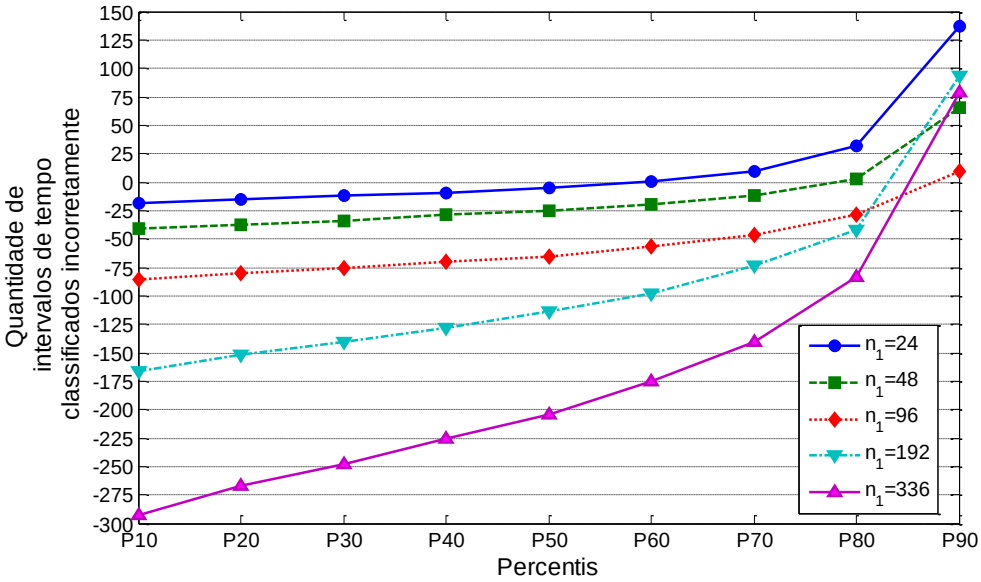

Figura 24: Quantidade de intervalos de tempo classificados de forma incorreta para os diferentes tamanhos de conjuntos avaliados.

A Figura 25, exibe através dos Percentis, a quantidade de intervalos de tempo que se passaram desde o início de uma fraude, até que uma anomalia fosse identificada pelo sistema para cada tipo de FDI, com n_1=24. Também é apresentada a quantidade de intervalos de tempo antes do início da fraude que estavam sendo classificados de forma equivocada. É possível visualizar que os FDIs dos tipos 1, 2 e 3 são os mais difíceis de serem identificados pelo detector de anomalias do subsistema, uma vez que o sistema deixou passar várias ocorrências de furto (intervalos de tempo) sem conseguir identificar.

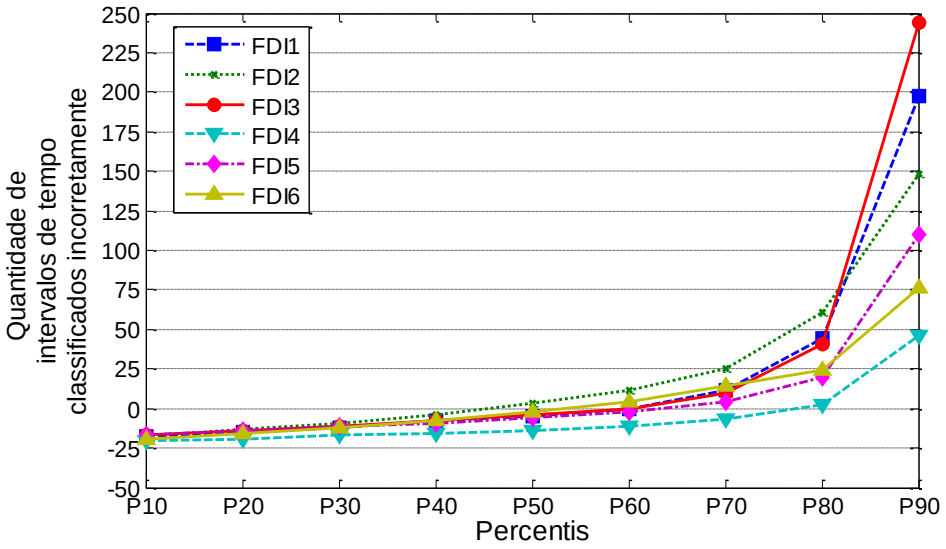

Figura 25: Quantidade de intervalos de tempo classificados de forma incorreta para cada tipo de FDI, utilizando n_1=24.

6.4. Avaliação do detector de anomalias com diferentes tamanhos de subsistemas

Nos testes realizados até o momento a tipologia criada na seção 6.1.1 foi utilizada. Todavia, como apresentado na proposta do detector de anomalias o subsistema monitorado pode ser dividido em novos subsistemas. A divisão de um subsistema em subsistemas menores pode aprimorar a identificação de pequenos furtos de energia que poderiam ficar ocultos em subsistemas grandes devido às incertezas quanto às perdas técnicas e imprecisão dos medidores. Para os testes foram criados dois novos cenários. No primeiro cenário cada subsistema foi configurado com 25 UCs e no segundo cenário cada subsistema foi configurado com 10 UCs. Consequentemente, em cada cenário de testes, a distância máxima entre o MBT e as UCs foi menor, o que ocasionou um menor valor de perdas técnicas no subsistema avaliado. Para criar

as medidas dos novos MBTs, o sistema de equações (40) apresentado na seção 6.1.1 foi utilizado.

Para realizar a comparação entre os três cenários avaliou-se a quantidade de intervalos de tempo que foram classificados de forma incorreta antes do rompimento dos limiares ε_1 e ε_2. Para os três cenários, os parâmetros ε_1, ε_2 e n_1 foram configurados respectivamente com, zero, -0,40% e 24. Para os testes as seis bases de dados poluídas foram utilizadas e configuradas de acordo com os cenários descritos anteriormente. Em 99% das ocorrências de fraudes, o sistema mudou de forma correta para o estado anormal, independentemente do cenário de testes. Na Figura 26 a média de intervalos de tempo que foram classificados de forma incorreta é apresentada, levando-se em consideração os seis tipos de FDIs. Na figura, os Percentis são utilizados para entender melhor os resultados para os diferentes cenários. Por exemplo, para o cenário onde 25 UCs são monitoradas por um MBT, P90, em 10% das ocorrências de fraudes identificadas, o detector de anomalias classificou de forma incorreta 18 ou mais intervalos de tempo até que os $\Delta e(t)$s calculados começassem a ser armazenados no conjunto E e o limiar ε_2 fosse rompido. Já para o cenário com 50 UCs em um subsistema foram classificados 137 ou mais intervalos de tempo de forma incorreta em 10% das ocorrências de fraude identificadas. Como já se esperava, quanto menor o subsistema, mais facilmente o detector de anomalias de subsistemas acusará que uma fraude pode estar em andamento. Na seção 8.2 são apresentados testes utilizando o sistema de detecção de consumidores fraudulentos completo nos três cenários.

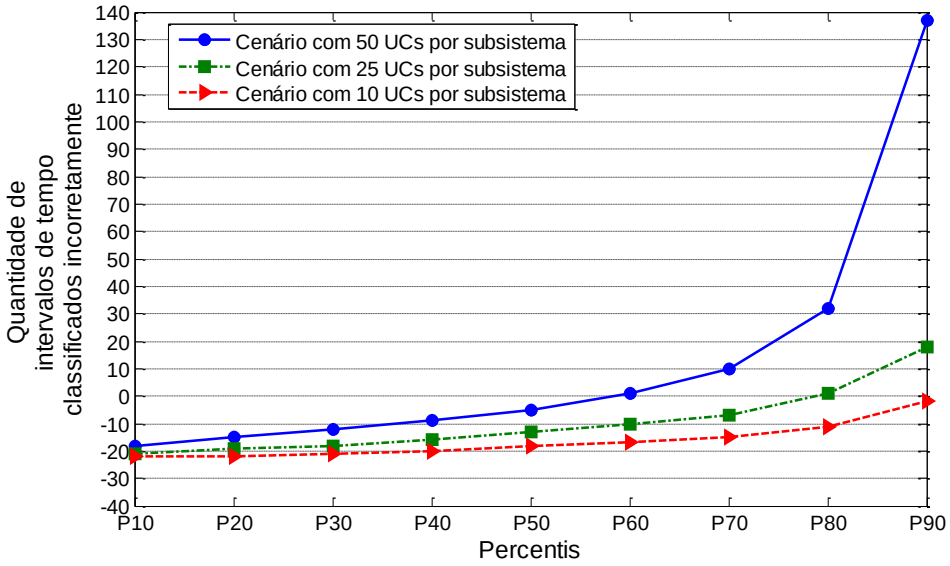

Figura 26: Quantidade de intervalos de tempo classificados incorretamente para diferentes tamanhos de subsistema, utilizando n_1=24.

6.5. Considerações

Nesse capítulo foram apresentadas as estratégias utilizadas para preparar a base de dados utilizada nos testes, bem como, os testes com o detector de anomalias de subsistemas proposto. Durante os testes foi possível visualizar que o detector de anomalias de subsistemas pode deixar passar várias medidas fraudulentas antes de identificar que uma fraude está ocorrendo no subsistema monitorado. Essa característica pode fazer com que, perfis criados pelo detector de consumidores fraudulentos não sejam totalmente confiáveis. Como pode ser visto na seção 6.4 a divisão de subsistemas maiores em subsistemas menores pode ser uma solução adequada para resolver o problema. O próximo capítulo apresenta os testes com o detector de consumidores fraudulentos em um cenário perfeito. Onde, assim que uma fraude é iniciada, as medidas recebidas pelo detector de consumidores fraudulentos são utilizadas para criar os perfis suspeitos e as anteriores ao período de furto são utilizadas para criar perfis normais. No capítulo 8 será apresentada a integração dos dois detectores.

Capítulo 7

Avaliação do Detector de Consumidores Fraudulentos

Nesse capítulo é realizada a avaliação do detector de consumidores fraudulentos apresentado na seção 5.1.2. Na seção 7.1 são apresentadas as estratégias de afinação e validação dos parâmetros do detector de consumidores fraudulentos. Nessa etapa de testes os algoritmos de agrupamento, FCM, K-Means e SOM foram testados juntamente com o detector de consumidores fraudulentos com o objetivo de identificar qual deles apresenta melhor ajuste ao sistema proposto. Na seção 7.2 o detector de consumidores fraudulentos proposto é comparado com o mais recente trabalho encontrado na literatura e na seção 7.3 são apresentadas as considerações finais do capítulo.

7.1. Afinação e Validação dos parâmetros do Detector de Consumidores Fraudulentos

Nessa fase de testes assumiu-se que o detector de consumidores fraudulentos apresentado na Figura 10, página 75, trabalha em um cenário idealizado. Onde, assim que uma fraude é iniciada, o detector de consumidores fraudulentos proposto, se move para o estado suspeito. O foco dessa fase de testes foi avaliar o desempenho do detector de consumidores fraudulentos sem incertezas sobre perdas técnicas ou imprecisão dos medidores.

A avaliação do sistema foi dividida em duas fases: a afinação e a validação. Na fase de afinação, os valores ótimos dos parâmetros n_2, k, β, α e λ são definidos. A afinação foi realizada utilizando apenas 1/3 das UCs selecionadas aleatoriamente. A fase de validação utilizou os 2/3 restantes das UCs. Utilizou-se para os testes a tipologia criada na seção 6.1.1. Todavia, considerou-se que a energia medida pelo MBT é igual à soma do consumo das UCs conectadas, enquanto não existir um furto de energia no subsistema monitorado. Na seção 7.1.1 é

apresentada a afinação dos parâmetros do detector de consumidores fraudulentos e na 7.1.2 a validação dos mesmos.

7.1.1. Afinação dos parâmetros detector de consumidores fraudulentos

Para realizar a afinação do detector de consumidores fraudulentos a função objetivo $\mathcal{O}$, apresentada na seção 5.4 foi utilizada. Com o objetivo de testar a hipótese que o detector de consumidores fraudulentos proposto não requer um conhecimento prévio de todos os tipos de fraudes para operar, o mesmo foi afinado utilizando apenas os conjuntos de dados modificados com os FDIs dos tipos 1, 2 e 3. A função objetivo utilizada foi a medida F. O sistema foi ajustado para maximizar F considerando o tipo de FDI mais difícil. No algoritmo, exibido na Figura 27, para cada valor de *k*, F foi calculado de forma independente para cada conjunto de dados e o valor máximo de F foi utilizando como função objetivo $\mathcal{O}$.

O número de medidas de consumo utilizadas (n_2) para a construção dos perfis normais (N_i) e suspeitos (S_i) é uma entrada para o algoritmo, exibido na Figura 27. O desempenho do detector de consumidores fraudulentos foi testado considerando n_2 =48 medições (equivalente a um dia de consumo), n_2 =144 medições (equivalente a três dias de consumo), n_2 =336 medições (equivalente a uma semana de consumo), n_2 =672 medições (equivalente a duas semanas de consumo) e n_2 =1008 medições (equivalente a três semanas de consumo). O número de clusters utilizados depende do tamanho de n_2, conforme indicado na Tabela 5, e foi definido segundo uma escala de quadrados perfeitos dos números dois a doze. Assim, foi possível avaliar um intervalo amplo de *k* sem a necessidade de um número excessivo de testes.

Tabela 5: Parâmetros dos algoritmos de Agrupamento.

Estratégia	n_2	Número de Clusters (*k*)
FCM K-Means SOM	48	4, 9, 16, 25
	144	4, 9, 16, 25, 36, 49, 64
	336	4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144
	672	
	1008	

Entre com n_2 ▷ $|\mathbf{N}_i| = |\mathbf{S}_i| = n_2$
$\mathcal{O} \leftarrow 0$ ▷ valor objetivo
$\mathbf{K} \leftarrow \{k \mid j \in \mathbb{N} \wedge k = j^2 \wedge 2 < k < n_2\}$
for para cada $k \in \mathbf{K}$ **do**
    determine α_k, β_k e λ_k que maximize $\mathcal{O}_k$
    if $\mathcal{O}_k > \mathcal{O}$ **then**
        $\mathcal{O} \leftarrow \mathcal{O}_k$
        $\mathcal{R} \leftarrow (k, \alpha_k, \beta_k, \lambda_k)$
    end if
end for
return $(\mathcal{O}, \mathcal{R})$

Figura 27: Algoritmo de afinação.

A Figura 28 exibe os resultados levando em consideração a medida F para cada valor de k, com o melhor ajuste de (β, α, λ) para cada um dos valores de n_2 avaliados. Como exibido na Figura 28, o desempenho do sistema é maximizado com um número relativamente alto de clusters, e quase não é afetado por $k > 2^4$. Isso ocorre porque (β, α, λ) são ajustados em relação à *k*, e várias combinações de (*k*, β, α, λ) dão resultados semelhantes. Ainda é possível observar que para quase todos os valores de k e n_2 o detector de consumidores fraudulentos apresenta melhores resultados utilizando a estratégia FCM. Apenas para n_2=1008 o a estratégia K-Means foi superior a FCM quando $k > 2^4$.

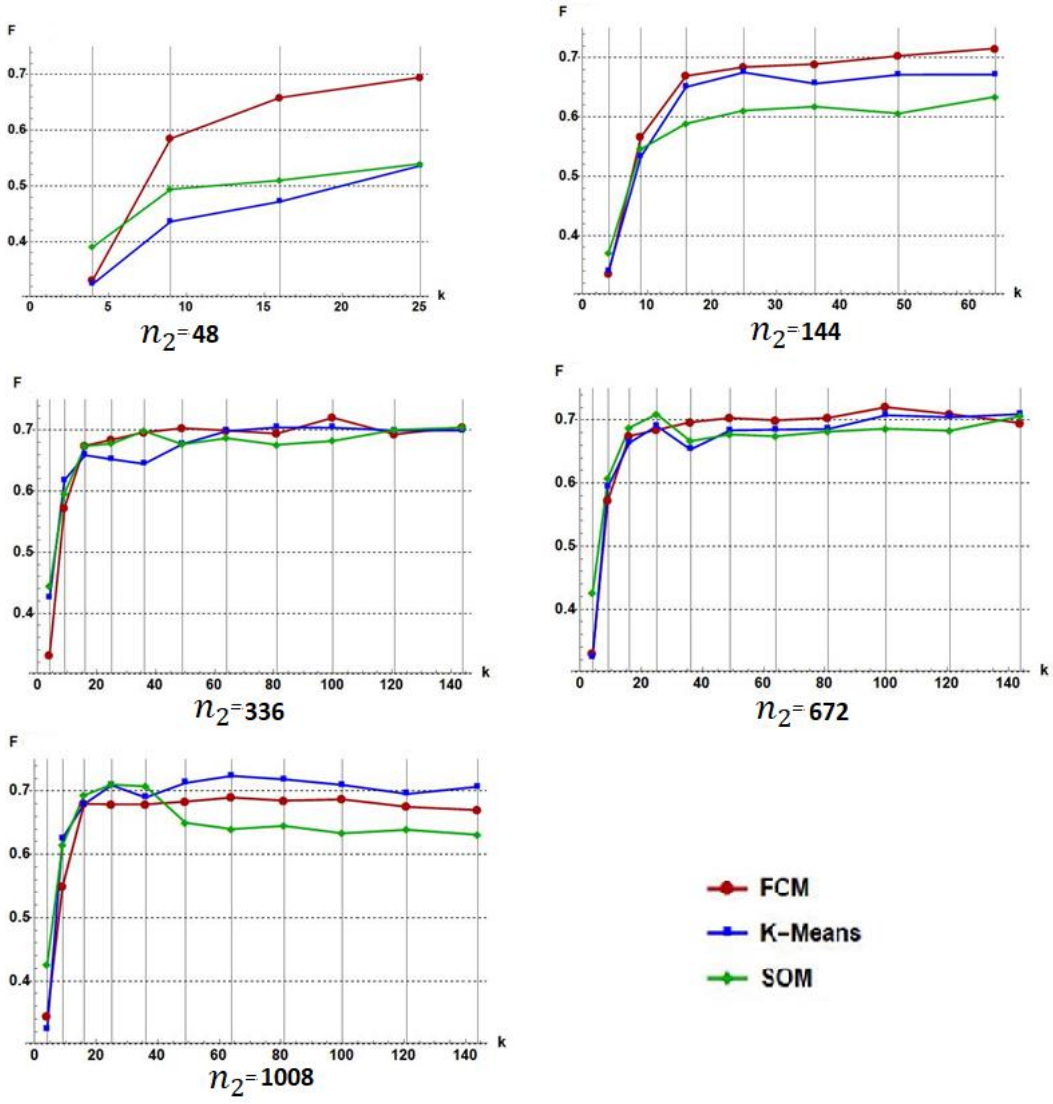

Figura 28: Número de agrupamentos (*k*) x Medida F para diferentes períodos de observação (n_2).

As Tabelas 6, 7 e 8 mostram as combinações ótimas de (*k*, β, α e λ) para os diferentes valores de n_2, expressos em dias, para as estratégias FCM, K-Means e SOM respectivamente.

Tabela 6: Afinação dos parâmetros do sistema para a estratégia FCM.

Dias	*k*	α	β	λ	F
1	25	4	1	0,3	0,69
3	64	10	1	0,2	0,72
7	100	12	1	0,2	0,72
14	100	12	1	0,2	0,72
21	64	7	1	0,2	0,69

Tabela 7: Afinação dos parâmetros do sistema para a estratégia K-Means.

Dias	*k*	α	β	λ	F
1	25	5	2	0,2	0,54
3	25	5	1	0,3	0,68
7	81	9	2	0,2	0,70
14	144	14	3	0,1	0,71
21	64	11	2	0,2	0,72

Tabela 8: Afinação dos parâmetros do sistema para a estratégia SOM.

Dias	*k*	α	β	λ	F
1	25	9	2	0,4	0,54
3	64	11	2	0,2	0,63
7	144	15	2	0,1	0,70
14	25	4	1	0,4	0,71
21	25	4	1	0,4	0,71

A Figura 29 exibe uma compilação dos resultados exibidos nas Tabelas 6, 7 e 8. A estratégia FCM obteve o melhor desempenho com menos medidas de consumo do que K-Means e SOM. Também é perceptível que períodos de observação excessivamente longos não melhorem o desempenho do sistema. Como se busca obter o melhor resultado no menor tempo possível, a utilização de n_2=672 torna a resposta do sistema mais rápida e com um menor nível de comprometimento da privacidade do consumidor, que quando comparado com n_2=1008. Dessa forma, n_2=672 (duas semanas / quatorze dias) medições foi definido como o período de observação ótimo para realizar a comparação dos três métodos de agrupamento.

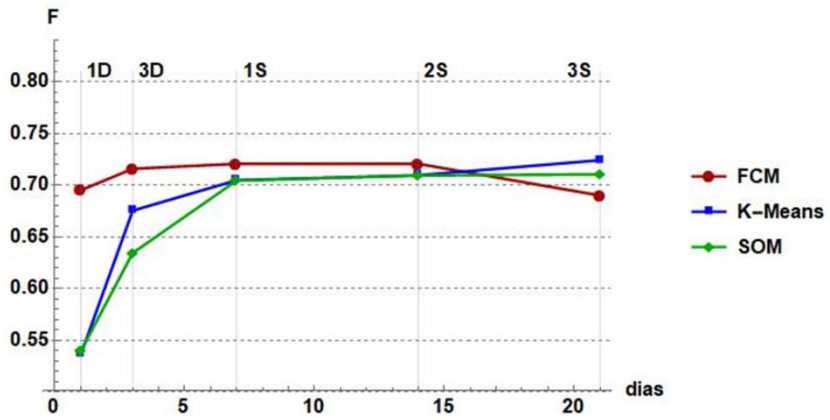

Figura 29: Afinação: Medida F x período de observação

Obtidos os melhores valores de β, α e λ para cada combinação de n_2 e *k* deu-se início validação do sistema.

7.1.2. Validação do detector de consumidores fraudulentos

Para validar o desempenho do detector de consumidores fraudulentos, aplicou-se o mesmo aos conjuntos de dados modificados com FDIs dos tipos 1 a 6 para os diferentes valores de n_2. Para cada valor de n_2 foi utilizada a configuração de *k*, β, α, λ ótima obtida na fase de afinação. Os valores utilizados são exibidos nas Tabelas 6, 7 e 8.

Na Figura 30 é possível observar qual estratégia apresentou melhor medida F para cada um dos valores de n_2 avaliadas. Para n_2=48 as estratégias baseadas em K-Means e FCM apresentaram resultados idênticos. Já para os outros valores de n_2, FCM apresentou um desempenho superior, sendo que para n_2=1008 o resultado da medida F foi praticamente idêntico a n_2=672.

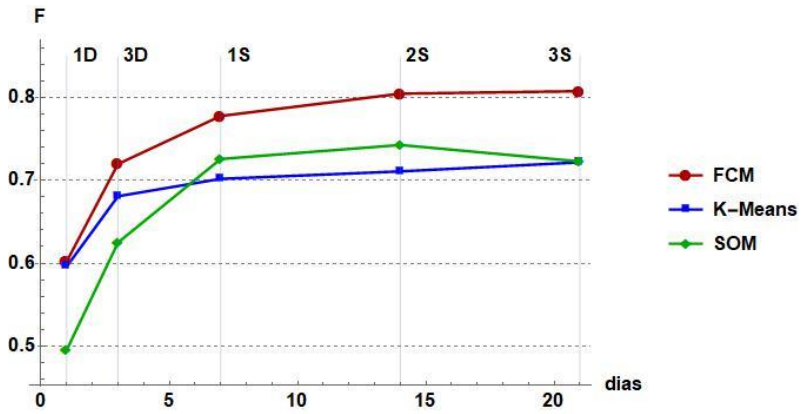

Figura 30: Validação: Medida F x período de observação.

O desempenho comparativo dos três algoritmos de agrupamento para cada tipo de FDI quando o sistema é configurado com n_2=672, como o período ótimo de observação é exibido nas Figuras 31, 32 e 33. São apresentadas as Taxas de Falsos Positivos (TFP), Taxas de Verdadeiro Positivo (TVP) e a medida F alcançada pelas estratégias de agrupamento.

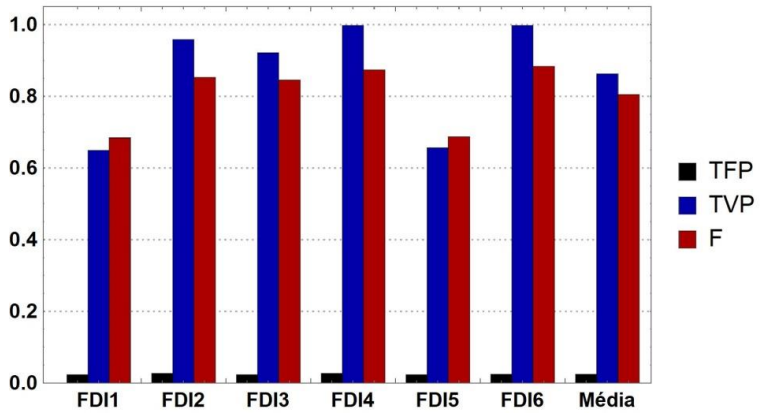

Figura 31: Resultados dos testes de detecção dos diferentes tipos de FDIs utilizando FCM.

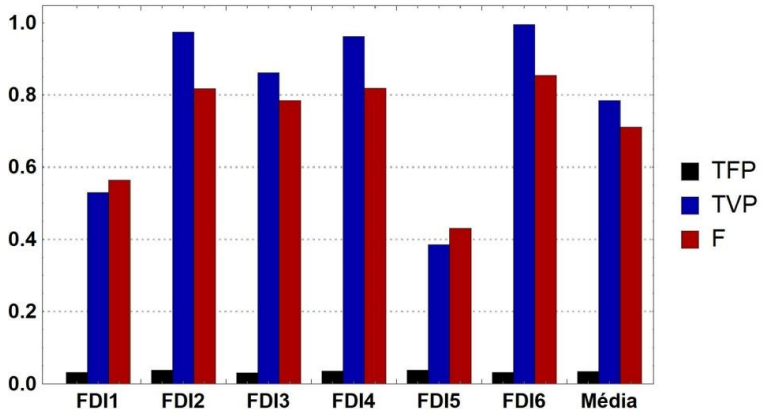

Figura 32: Resultados dos testes de detecção dos diferentes tipos de FDIs utilizando K-Means.

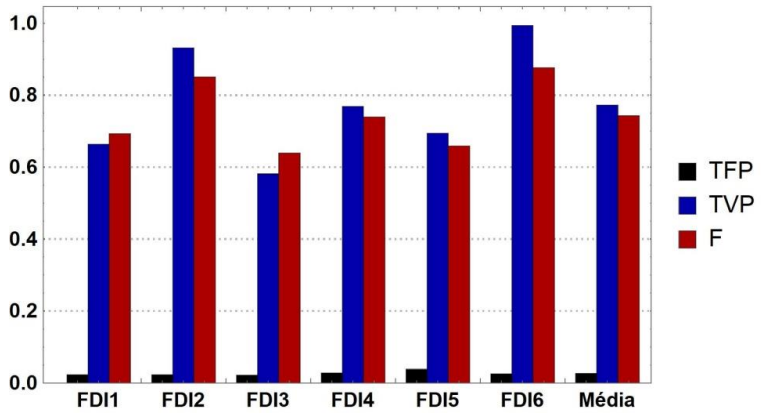

Figura 33: Resultados dos testes de detecção dos diferentes tipos de FDIs utilizando SOM.

No geral, o FCM foi o melhor método, mas o SOM foi superior para os FDIs dos tipos 1 e 5 quando comparada a TVP. Estes FDIs reduzem os as medidas de consumo em uma porcentagem e o que torna difícil a detecção por métodos baseados na medição da distância entre centroides (FCM e K-Means). A abordagem baseada no mapeamento e na contagem de medidas de consumo utilizados pelo método SOM é melhor para detectar esses tipos de

fraudes. No entanto, o SOM funciona mal para fraudes que diminuem os as medidas de consumo baseado em deslocamento (FDI do tipo 3). O resultado obtido indica que o detector de consumidores fraudulentos proposto é robusto contra diferentes tipos de fraudes, uma vez que, os FDIs do tipo 4 a 6, não considerados na fase de afinamento, foram detectados com precisão igual ou maior que os utilizados na fase de afinação.

A quantidade de roubo de energia tem um enorme impacto na capacidade de qualquer sistema na detecção de fraudes. A Figura 34 mostra a taxa média de UCs fraudulentas detectadas corretamente (TVP) pelo método FCM em relação à porcentagem de roubo utilizada pelo fraudador. Na Figura 34 é apresentada a média dos seis tipos de FDIs avaliados no presente trabalho. Pode-se concluir que o sistema começa a apresentar uma TVP satisfatória a partir de trinta por cento de roubo. Roubos abaixo dessa porcentagem podem não ser detectados pelo sistema para evitar uma elevada TFP. Vários trabalhos recentes encontrados na literatura utilizam porcentagens de roubo acima de trinta por cento, ou ainda consumo negativo [85], [100], [107], [108], [111] e [112].

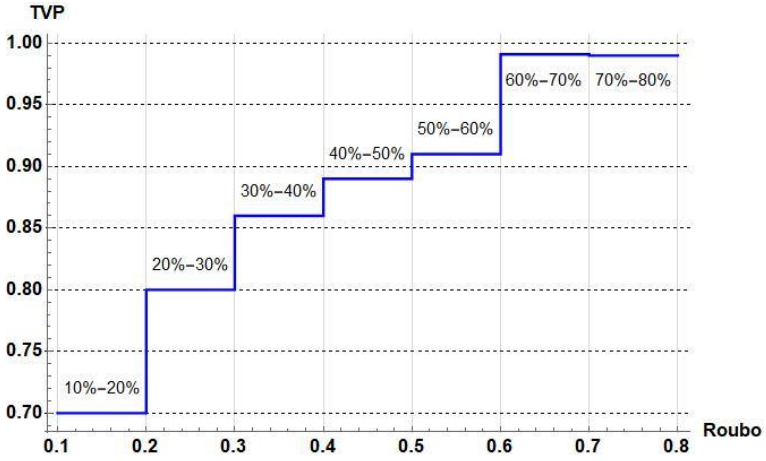

Figura 34: FCM: TVP x porcentagem de energia roubada identifiada.

Outra análise pode ser feita é em relação à quantidade de energia furtada e a quantidade energia detectada pelo sistema. Na Figura 35 é possível observar que as técnicas de roubo FDI1 e FDI5, são mais difíceis de serem identificadas. Isso se deve ao fato que as alterações de perfil de consumo causadas por esses ataques são mais difíceis de serem modeladas. Na média dos seis tipos de FDIs avaliados o sistema proposto baseado na estratégia FCM foi capaz de detectar 90,6% da energia furtada.

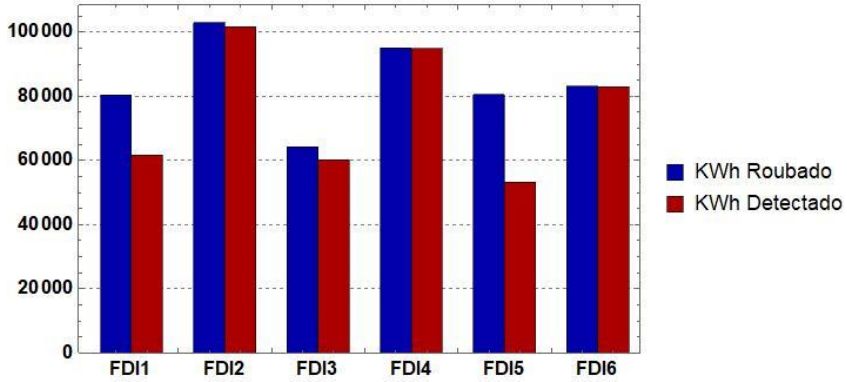

Figura 35: KWh roubado X KWh detectado.

Todos os resultados mostrados anteriormente referem-se a um sistema treinado para maximizar a medida F. No entanto, o sistema pode ser treinado para atingir diferentes objetivos, ajustando os parâmetros β, α e λ. A Tabela 9 define cinco configurações diferentes como problemas de otimização. Além das métricas típicas, a coluna energia roubada detectada (ERD) mostra a fração de roubo de energia detectada para cada configuração. Maximizar a TVP aumenta ERD ao custo de uma taxa mais alta de falsos alarmes (TFP). O aumento do lucro da concessionária de energia é provavelmente a melhor métrica para avaliar a utilidade de um sistema de detecção de fraudes. A variação de lucro ΔP pode ser definida como $(P^* - P)/P$, em que P e P^* pode ser calculado usando (33) e (34) respectivamente. Supondo que as UCs fraudulentas paguem apenas os valores monetários correspondentes à quantidade de energia roubada detectada, sendo utilizados os seguintes valores pelas concessionárias:

- Valor cobrado pelo KWh consumido, T = 0,12$/KWh;
- Custo de produção de energia, C = 0,1 $/KWh;
- Custo médio das inspeções no local, ψ = 30$.

A variação de lucro para cada configuração na Tabela 9 é mostrada na Figura 36. Observe que $\Delta P = 0$ é utilizado para uma concessionária sem um sistema para detectar consumidores fraudulentos. O aumento máximo de lucro com o uso do sistema de detecção de consumidores fraudulentos é 9,2% para a configuração 4, o que corresponde à maximização da medida F. Este resultado é válido somente para o cenário descrito nesta avaliação, em que 10% dos consumidores roubam entre 10% e 80% da eletricidade. O aumento do lucro é maior quando a quantidade de roubo de energia é maior e a margem entre o preço pago pelos consumidores e o custo para produzir eletricidade é menor.

Tabela 9: Resultados obtidos com diferentes configurações.

	Configuração	TFP	TVP	F	ERD
1.	Maximizar TVP com TFP < 0,2	0,20	0,97	0,47	0,98
2.	Maximizar TVP com TFP < 0,1	0,10	0,96	0,62	0,98
3.	Maximizar TVP com TFP < 0,07	0,07	0,94	0,71	0,96
4.	Maximizar F	0,02	0,86	0,81	0,91
5.	Minimizar TFP com TVP > 0,7	0,01	0,74	0,75	0,80

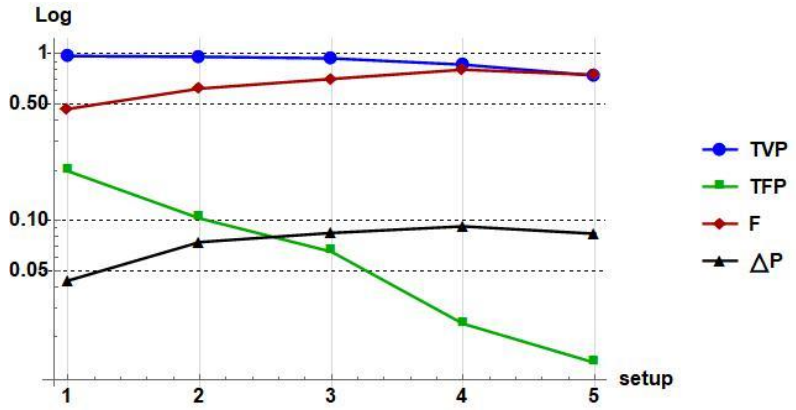

Figura 36: Variação do desempenho para diferentes configurações de treinamento.

7.2. Comparação da estratégia baseada em FCM com os mais recentes trabalhos

Recentemente cinco trabalhos que estão preocupados com a identificação de consumidores fraudulentos em REIs foram publicados. Entre estes trabalhos dois utilizam máquina supervisionada (Jindal *et al.* [99] e Jokar *et al.* [101]) e três aprendizagem de máquina não-supervisionada (Ford *et al.* [108], Krishna *et al.* [111] e Hartmann *et al.* [112]). Os trabalhos que utilizam aprendizagem não-supervisionada não utilizam um medidor coletivo para ajudar na identificação de consumidores fraudulentos, o que torna a comparação com o trabalho proposto injusta devido à alta taxa de falsos alarmes. Entre os trabalhos que utilizam aprendizagem supervisionada Jindal *et al*. utiliza diversas informações dos consumidores como: temperatura, hora, estação do ano, N° de pessoas e aparelhos na unidade consumidora. A utilização dessas informações torna a implementação do sistema complexa, uma vez que é necessário manter essas informações sempre atualizadas, além de comprometer a privacidade do consumidor.

O trabalho de Jokar *et al*. utiliza um medidor coletivo, além de estar preocupado com a privacidade dos consumidores como apontado no Quadro 4, e ter apresentar o melhor

desempenho entre os trabalhos encontrados na literatura. Em Jokar *et al*. a abordagem SVM multiclass foi comparada com a abordagem ARMA-GLR [83] e apresentou um desempenho significativamente melhor. Os tipos de FDIs considerados em [101] são semelhantes aos listados no Quadro 2, mas não incluem os tipos 2 e 3. Para comparar ambos os métodos, foram formuladas as seguintes condições de treinamento e testes:

- Todos os tipos de FDIs são conhecidos no momento do treinamento e todos os tipos de FDIs foram incluídos na fase de teste;
- Todos os tipos de FDIs foram incluídos na fase de testes, mas um tipo de FDI estava faltando na fase de treinamento. Isso resulta em seis condições de treinamento diferentes.

As Figuras 37 e 38 mostram os resultados obtidos para cada tipo de FDI quando ambos os sistemas foram treinados com todos os tipos de FDIs. Nesta avaliação, a abordagem proposta no presente trabalho foi ajustada para maximizar a medida F. A observação mais notável é que o sistema proposto gera um menor número de falsos alarmes. A fração média de falsos alarmes considerando todos os tipos de FDIs foi de 2,7% para o FCM e 14,4% para o SVM. A taxa média de detecção do método SVM foi superior (93,1% contra 87,1%). No entanto, a superioridade do método SVM na taxa média de detecção ocorreu pelo fato que a estratégia proposta no presente trabalho foi ajustada para maximizar a medida F, o que penaliza a taxa média de detecção do método FCM. O método FCM obteve uma medida F de 83% contra 52% do método SVM. O método SVM apresentou como vantagem um desempenho semelhante para todos os tipos de FDIs, enquanto o método FCM teve mais dificuldades para detectar os FDIs de tipo 1 e 5.

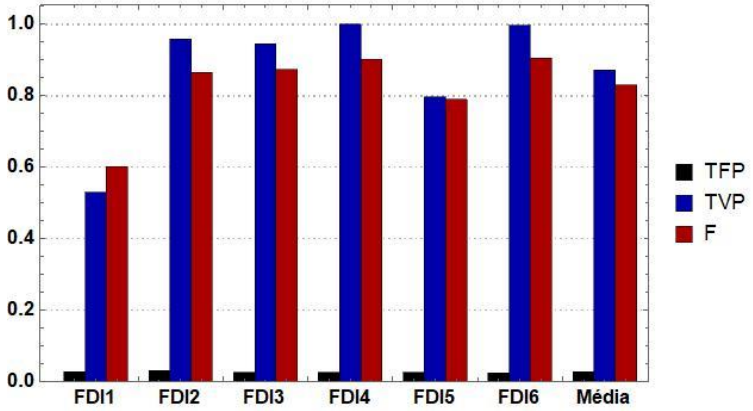

Figura 37: Desempenho médio do método FCM quando todos os FDIs são utilizados no treinamento.

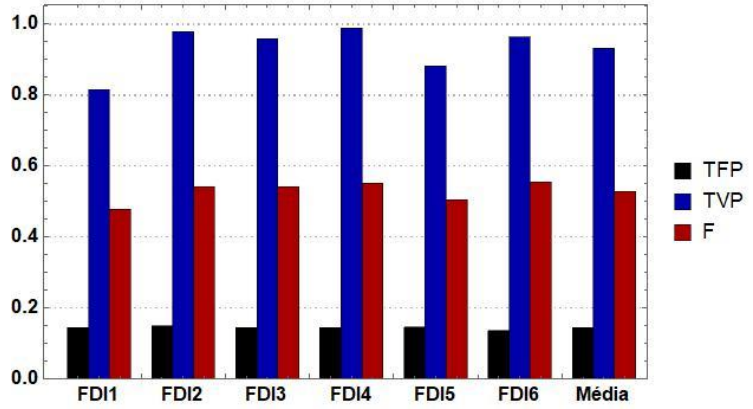

Figura 38: Desempenho médio do método SVM quando todos os FDIs são utilizados no treinamento.

As Figuras 39 e 40 mostram os resultados obtidos quando um tipo específico de FDI não foi incluído no treinamento. Por exemplo, o resultado do FDI1 foi obtido treinando o sistema com todos os tipos de FDIs, exceto o FDI1; obteve-se o resultado do FDI2 treinando o sistema com todos os tipos de FDIs, exceto o FDI2, e assim por diante. Portanto, as Figuras 39 e 40 mostram o desempenho do pior caso para ambos os métodos. Nessa formulação de treinamento e testes o sistema baseado em FCM não apresentou aumentou no número de falsos alarmes, no entanto, os FDIs dos tipos 1 e 5 tiveram uma queda maior na taxa de detecção de fraudes do que os outros tipos de FDIs. A média da medida F foi de 77% para FCM e 46% para SVM.

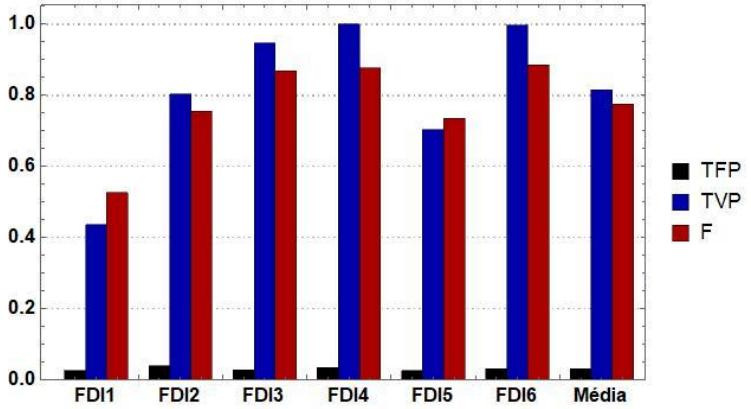

Figura 39: Desempenho médio do método FCM quando falta um tipo FDI no treinamento.

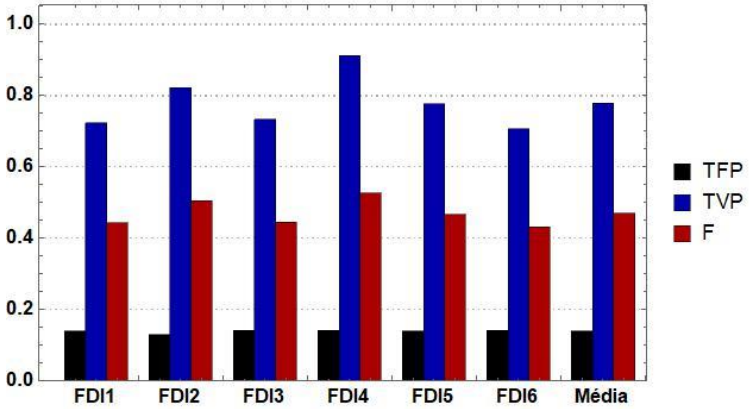

Figura 40: Desempenho médio do método SVM quando falta um tipo FDI no treinamento.

A Figura 41 ainda se refere à configuração em que ambos os sistemas foram avaliados com seis condições diferentes de treinamento, mas mostra o desempenho médio obtido para todos os seis tipos de FDIs incluídos nos testes, em vez de apenas um FDI faltando como nas Figuras 39 e 40. Na Figura 41 o desempenho relativo do sistema baseado em FCM em relação à abordagem SVM é considerando utilizando as métricas TFP, TVP e F. Por exemplo, o desempenho relativo para a medida F foi calculado por (42):

$$\frac{(F^f - F^s)}{F^s} \tag{42}$$

Onde F^f e F^s são os valores de F obtidos utilizando os métodos FCM e SVM, respectivamente. SVM obteve uma taxa de detecção ligeiramente superior (4%), mas o sistema baseado em FCM gera 80% menos falsos alarmes e tem uma medida F 65% maior.

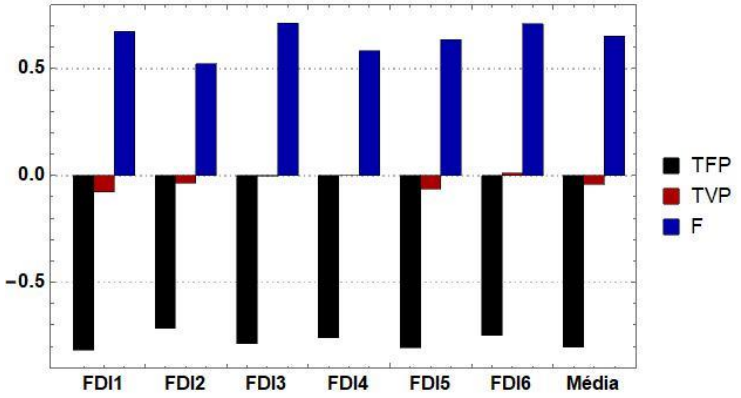

Figura 41: Desempenho relativo do método FCM em relação ao método SVM multiclass proposto em [101].

No presente trabalho também foi desenvolvida uma implementação baseada em SVM semelhante àquela proposta por Jokar *et al*. Os procedimentos adotados e os resultados obtidos são descritos no apêndice A.

7.3. Considerações

Este capítulo apresentou os testes com o detector de consumidores fraudulentos proposto que utiliza algoritmos de clusterização para criar perfis de consumo dos consumidores com as medidas de consumo observadas antes e depois da detecção de uma anomalia no subsistema monitorado. Durante os testes o algoritmo de clusterização FCM apresentou melhor desempenho que os algoritmos K-Means e SOM para esse uso particular. A estratégia de comparar perfis de consumo recentes se mostrou eficiente na detecção de consumidores fraudulentos, pois ela apresentou menor taxa de falsos alarmes em relação a outros trabalhos encontrados na literatura.

Capítulo 8

Testes de integração dos detectores de anomalia de subsistemas e de consumidores fraudulentos

Nesse capítulo é apresentada a avaliação dos detectores de anomalias de subsistemas e de consumidores fraudulentos de forma integrada. Nos testes realizados na seção 6.3.2 percebeu-se que o detector de anomalias de subsistemas classificava de maneira equivocada várias medidas normais como fraudulentas quando valores maiores eram utilizados para n_1. A classificação das medidas normais como fraudulentas pode prejudicar principalmente a identificação de consumidores fraudulentos que estão roubando uma grande porcentagem de energia. Na seção 8.1 são apresentados os testes de integração dos dois detectores utilizando diferentes valores de n_1. Através dos testes será possível avaliar o impacto do valor de n_1 na detecção de consumidores fraudulentos.

Nessa fase de integração dos dois detectores também será avaliado o sucesso na detecção de consumidores fraudulentos quando subsistemas grandes são divididos em subsistemas menores. A divisão de subsistemas grandes em subsistemas menores aprimora a identificação de pequenos furtos de energia, que poderiam ficar ocultados devido às incertezas quanto às perdas técnicas e imprecisões dos medidores. Na seção 8.2 são apresentados os testes dividindo a tipologia criada não seção 6.1.1 em subsistemas menores, sendo que em cada novo subsistema um novo MBT foi alocado.

8.1. Avaliação do impacto do valor de n_1 na detecção de consumidores fraudulentos

Para avaliar o impacto do valor de n_1 quando da integração do detector de anomalias de subsistemas com o detector de consumidores fraudulentos, foram realizados testes utilizando n_1=24, 96 e 336. Para cada valor de n_1, o valor estimado para ε_2, de acordo com a Tabela 4 foi utilizado. O detector de consumidores fraudulentos foi configurado com os valores ótimos

(n_2=672, k=100 β=1, α=12 e λ=0,2) obtidos nos testes apresentados na seção 7.1.1. Durante os testes, as seis bases de dados poluídas foram utilizadas. Todas as bases foram configuradas de acordo com a tipologia apresentada na seção 6.1.1, e levando-se em considerando as perdas técnicas e a imprecisão dos medidores inteligentes. A Figura 42 exibe as taxas de VP obtidas na identificação de consumidores fraudulentos para cada valor de n_1. Com exceção do FDI 3, que apresentou melhor TVP para n_1=96, para todos os outros tipos FDIs o sistema apresentou melhor TVP para n_1=24. Na média, a TVP final do sistema integrado foi de 80,1% para n_1=24, 68,5% para n_1 =96 e 49,4% para n_1 =336, com taxas de FP de 2,6%, 2,7% e 2,6% respectivamente. A Figura 43 ilustra outra forma de avaliar o impacto do tamanho do conjunto E quando da integração dos detectores do sistema. A figura mostra a taxa média de UCs fraudulentas detectadas corretamente (TVP) em relação à porcentagem de roubo utilizada pelo fraudador. Na Figura 43 é apresentada a média dos seis tipos de FDIs avaliados no presente trabalho. É possível observar que quanto maior o valor de n_1 menor é a TVP por faixa de roubo, sendo que para roubos acima de cinquenta por cento, ocorreu uma diferença na TVP de 40% entre n_1=24 e n_1=336.

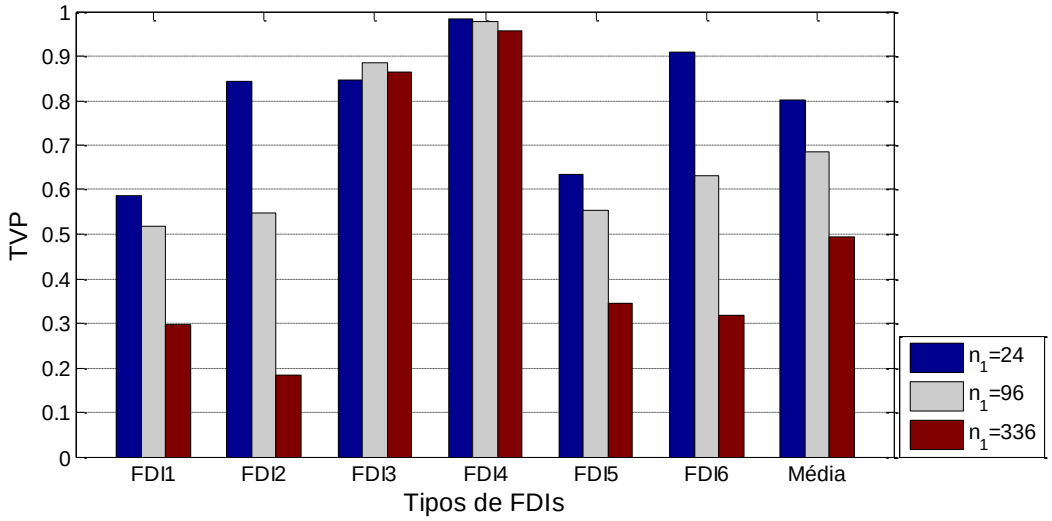

Figura 42: Testes de integração com diferentes valores de n_1.

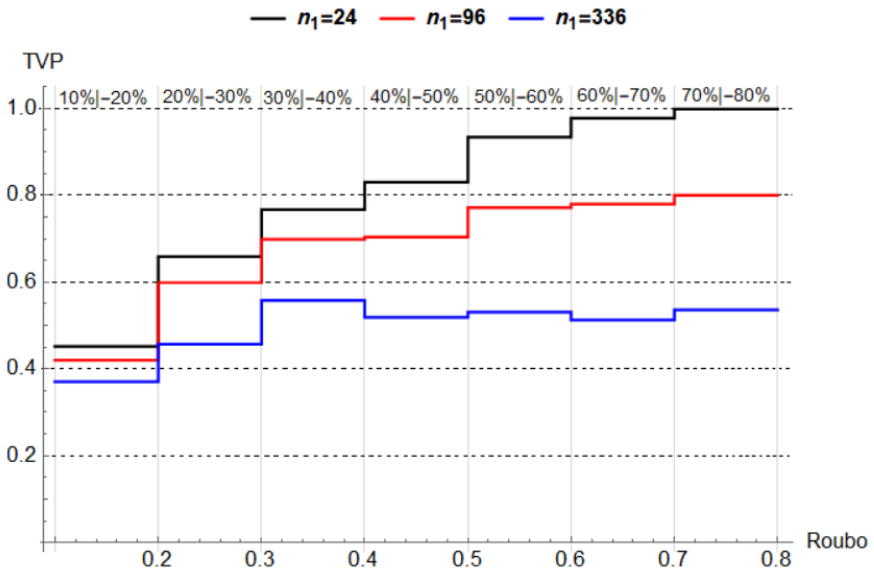

Figura 43: FCM - TVP por faixa de roubo para diferentes valores de n_1.

8.2. Avaliação do sistema de detecção de consumidores fraudulentos com diferentes números de UCs por subsistema

Na seção 6.4 foram criados dois novos cenários além da tipologia criada na seção 6.1.1. No primeiro cenário 25 UCs foram alocadas em cada subsistema e no segundo cenário 10 UCs foram alocadas em cada subsistema. Através dos resultados apresentados na seção 6.4 percebeu-se que quanto menos UCs em um subsistema, mais rapidamente o detector de anomalias de subsistemas detectava uma fraude após o seu início. O que faz com que os perfis criados pelo detector de consumidores fraudulentos sejam mais próximos à veracidade. Nessa seção busca-se avaliar as taxas de VP e FP levando-se em consideração o tamanho do subsistema quando da integração dos dois detectores. Na Tabela 10 são apresentados os resultados dos testes. Para todos os testes o detector de anomalias de subsistemas foi configurado com ε_1 =0, n_1 =24 e ε_2 =-0,4% e o detector de consumidores fraudulentos configurado com os valores ótimos descritos anteriormente. É possível visualizar na Tabela 10 que o sistema de detecção de consumidores fraudulentos apresentou resultados semelhantes para os três tamanhos de subsistemas avaliados. Sendo que para subsistemas com 10 e 25 UCs os resultados foram idênticos e muito próximos a TVP de 86,3% alcançada nos testes realizados com o detector de consumidores fraudulentos trabalhando em um cenário perfeito. Os resultados mostram que o sistema proposto pode ser utilizado em um ambiente real para diferentes tamanhos de subsistemas.

Tabela 10: Resultados dos testes com diferentes números de UCs alocadas em um MBT.

FDIs	Cenário com 50 UCs por MBT		Cenário com 25 UCs por MBT		Cenário com 10 UCs por MBT	
	TFP	TVP	TFP	TVP	TFP	TVP
FDI1	0,025	0,588	0,026	0,616	0,025	0,616
FDI2	0,025	0,842	0,027	0,844	0,026	0,844
FDI3	0,027	0,846	0,029	0,916	0,031	0,920
FDI4	0,026	0,984	0,029	0,990	0,032	0,998
FDI5	0,025	0,634	0,025	0,648	0,028	0,656
FDI6	0,025	0,910	0,026	0,910	0,027	0,916
Média	**0,026**	**0,801**	**0,027**	**0,821**	**0,028**	**0,825**

8.3. Considerações

Através dos testes apresentados nesse capítulo percebeu-se que o sistema de detecção de consumidores fraudulentos apresenta resultados satisfatórios mesmo quando várias UCs são monitoradas por um único MBT. No próximo capítulo são apresentadas as considerações finais do trabalho e sugestões de trabalhos futuros.

Capítulo 9

Considerações

No presente trabalho desenvolveu-se um sistema de identificação de consumidores fraudulentos para redes secundárias de energia elétrica. O sistema proposto é representado por duas máquinas de estados, a primeira é utilizada para representar o detector de anomalias de subsistemas e a segunda para representar o detector de consumidores fraudulentos pertencentes ao subsistema monitorado. O detector de anomalias de subsistemas utiliza várias medições consecutivas para avaliar se uma fraude está ocorrendo no subsistema monitorado. Essa abordagem é inovadora em relação aos trabalhos encontrados na literatura. Os trabalhos que utilizam um medidor coletivo adotam a hipótese irreal que é possível detectar o momento exato do início do furto de energia com uma única medida. Nesse trabalho, uma abordagem mais realista que leva em conta os erros de medição e as perdas técnicas é adotada. É proposta uma estratégia original na qual a tensão fornecida pelos medidores é usada para estimar as perdas técnicas sem o conhecimento prévio da topologia da rede. Adicionalmente várias medidas são usadas para tomar uma decisão sobre a existência de uma anomalia, o que reduz a taxa de falsos alarmes e também ajuda na identificação de fraudes que roubam uma baixa porcentagem de energia. Durante a avaliação do detector de anomalias de subsistemas de forma isolada, 99% das fraudes foram identificadas sem a geração de falsos alarmes.

O detector de consumidores fraudulentos proposto apresenta como inovação a criação de perfis de consumo de vida curta. Os perfis de consumo são criados utilizando medidas de consumo observadas um pouco antes e depois de uma anomalia ser identificada pelo detector de anomalias de subsistemas. Os perfis de consumo de vida curta são sensíveis a mudanças recentes no consumo de energia, o que contribui para a identificação de anomalias que poderiam ficar ocultas em perfis de consumo de longa duração. Outra vantagem dos perfis de consumo de vida curta é a preservação da privacidade dos consumidores. Como são utilizadas poucas medidas para criar os perfis de consumo, a privacidade dos consumidores será mantida caso o detector de anomalias sofra algum ataque.

Para criar os perfis de consumo de vida curta foram avaliados três algoritmos de clusterização. O algoritmo FCM apresentou melhor desempenho que os algoritmos K-Means e

SOM para esse uso particular. O algoritmo FCM apresentou como vantagem a rápida adaptação a mudanças de perfil de consumo, sem necessitar conhecer todos os tipos de fraudes que podem ser utilizados por consumidores fraudulentos para ocultar o seu real consumo de energia.

Outra vantagem do detector de consumidores fraudulentos é que as concessionárias de energia podem alterar a sensibilidade do sistema utilizando um procedimento semi-automatizado para extrair características dos perfis de consumo. O procedimento otimiza vários parâmetros do detector de consumidores fraudulentos com objetivo de selecionar os valores mais relevantes para ajustar o sistema a métrica especificada. A concessionária pode optar pelas métricas de FP, VP e medida F de acordo com os objetivos para os quais o sistema está sendo aplicado. Os testes de ajustes e avaliação foram realizados utilizando diferentes unidades consumidoras e diferentes tipos de FDIs. Mostrando que o procedimento semi-automatizado de extração de características é robusto, e resultados semelhantes podem ser obtidos sem a necessidade de ajustes adicionais para diferentes conjuntos de dados.

Quando o detector de consumidores fraudulentos proposto foi comparado com o mais recente trabalho encontrado na literatura as taxas de VP foram bem próximas. Todavia, quando comparada às taxas de FP o detector de consumidores fraudulentos proposto se mostrou bastante superior. Em um ambiente real isso significa uma diminuição de custos com inspeções desnecessárias. A avaliação do detector de consumidores fraudulentos proposto em termos de energia furtada identificada e esforços investidos para investigar falsos alarmes mostrou que, se o sistema for configurado de forma a obter uma alta taxa de detecção, o retorno financeiro será penalizado com o custo adicional de vários falsos alarmes. Por outro lado, se o sistema for configurado de forma a apontar uma baixa taxa de falsos alarmes também haverá uma diminuição na identificação da energia que está sendo furtada. É necessário equilibrar a taxa de identificação de energia furtada com uma taxa de falsos alarmes aceitável, considerado os valores da energia e os custos de inspeção. Na avaliação realizada foi possível observar que maximizar a medida F contribuiu para um maior ressarcimento de valores financeiros perdidos com furtos de energia.

Durante a avaliação do detector de anomalias de subsistemas de forma isolada percebeu-se que, em 20% dos casos de fraudes identificadas, o detector de anomalias de subsistemas demorava a perceber que uma fraude estava ocorrendo no subsistema monitorado. O que poderia prejudicar a identificação de consumidores fraudulentos pelo detector de consumidores fraudulentos. Nos testes de integração dos dois detectores foi possível avaliar o real impacto do atraso na identificação de uma anomalia pelo detector de anomalias do subsistema. Nos testes de integração a TVP foi de 80,1%, enquanto nos testes com o detector de consumidores

fraudulentos em um cenário perfeito foi de 86,3%. A TVP de 80,1%, foi obtida no cenário com cinquenta UCs monitoradas por um único MBT. No cenário onde um MBT monitora 25 UCs a TVP foi de 82,1%, com 2,7% de TFP. Os resultados obtidos foram muito próximos às taxas de VP e FP obtidas com o detector de consumidores fraudulentos trabalhando em um cenário perfeito. Os testes realizados com diferentes cenários evidenciaram que o sistema proposto pode ser utilizado em um ambiente real, e que as concessionárias de energia podem adequar o mesmo de acordo com as suas necessidades. Podendo alocar várias UCs para cada MBT, ou ainda, quando houver a necessidade de um maior grau de precisão do sistema, diminuir o número de UCs monitoradas por um MBT.

Entre as principais limitações encontradas, pode-se citar a carência de bases de dados contendo informações de medições de consumo coletas pela AMI. Foram encontradas duas bases de dados de domínio público, uma contendo dados de cinco mil unidades consumidoras [121] e outra de trinta e uma unidades consumidoras [133]. Todavia, as duas bases de dados continham apenas informações da energia consumida pelas UCs, o que exigiu com que fossem criadas as medidas do MBT estimadas as potências em cada uma das UCs. Também foi necessário simular fraudes para avaliar o sistema proposto.

Como trabalhos futuros ainda é preciso avaliar o detector de anomalias de subsistemas em cenários mais realistas, onde o sistema trifásico está desequilibrado. É preciso também avaliar o sistema em cenários onde há unidades consumidoras que produzem sua própria energia e enviam a energia excedente para a rede. Nesse cenário podem surgir novos tipos de ataques, onde, unidades consumidoras produtoras de energia podem reportar que enviaram mais energia para a rede do que a realmente foi enviada.

Outro trabalho futuro é utilizar o sistema de detecção proposto para identificar consumidores cujo aumento significativo de consumo acarrete em redução excessiva nos níveis de tensão na entrada dos medidores devido às perdas técnicas. Este novo recurso ajudará os serviços públicos a antecipar possíveis problemas, notificar consumidores e reconfigurar a rede de distribuição secundária em certas áreas para evitar apagões ou quedas de energia devido ao excesso de consumo.

Referências Bibliográficas

[1] K. Gandhi e H. Bansal, "Smart Metering in electric power distribution system," em *Control, Automation, Robotics and Embedded Systems (CARE), 2013 International Conference on*, 2013.

[2] BRASIL - Ministério de Minas e Energia; Empresa de Pesquisa Energética, "Anuário Estatístico de Energia Elétrica 2016 - ano base 2015," BRASIL - Ministério de Minas e Energia, 2016.

[3] J. Vermeulen, 01 2015. [Online]. Available: http://businesstech.co.za/news/general/77495/electricity-theft-in-sa-this-is-what-it-looks-like/. [Acesso em 07 07 2015].

[4] Northeast Group, LLC, 09 2014. [Online]. Available: http://www.prnewswire.com/news-releases/world-loses-893-billion-to-electricity-theft-annually-587-billion-in-emerging-markets-300006515.html. [Acesso em 08 07 2015].

[5] Z. Xiao, Y. Xiao e D. Du, "Exploring Malicious Meter Inspection in Neighborhood Area Smart Grids," *Smart Grid, IEEE Transactions on,* vol. 4, nº 1, pp. 214-226, March 2013.

[6] NIST, "NIST Framework and Roadmap for Smart Grid Interoperatibility Satandards, Release 3," 2014.

[7] Y. Mo, T.-H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig e B. Sinopoli, "Cyber-Physical Security of a Smart Grid Infrastructure," *Proceedings of the IEEE,* vol. 100, nº 1, pp. 195-209, Jan 2012.

[8] S. M. Amin e B. F. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *IEEE Power and Energy Magazine,* pp. 34-41, 2005.

[9] H. Gharavi e R. Ghafurian, "Smart grid: The electric energy system of the future," *IEEE,* vol. 99, p. 5, 2011.

[10] M. R. Hossain, A. M. T. Oo e A. B. M. S. Ali, "Smart Grid," em *Smart Grids - Opportunities, Developments, and Trends*, London, ringer-Verlag, 2013.

[11] International Energy Agency, "Technology Roadmap Smart Grids," OECD/IEA, Paris, 2011.

[12] National Institute of Standards and Technology, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0," 2014.

[13] S. J. R. W. Rob van Gerwen, "Smart Metering," *leonardo-energy.org,* vol. 9, pp. 1-9, 2006.

[14] D. W. G. L. L. Jixuan Zheng, "Smart Meters in Smart Grid: An Overview," em *IEEE Green Technologies Conference,* 2013.

[15] X. Y. Damminda Alahakoon, "Smart electricity meter data intelligence for future energy systems: A survey," *IEEE Transactions on Industrial Informatics,* vol. 12, nº IEEE, pp. 425-436, 2016.

[16] Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO), "Portaria Inmetro nº 587, de 05 de novembro de 2012," BRASIL - Ministério do Desenvolvimento, Indústria e Comércio Exterior Ministério, Duque de Caxias - RJ, 2012.

[17] E. Hossain, Z. Han e H. V. Poor, Smart Grid Communications and Networking, C. U. Press, Ed., New York: Cambridge, 2012.

[18] J. Zhang, Z. Chen, X. Yang, K. Chen e K. Li, "Ponder over Advanced Metering Infrastructure and Future Power Grid," em *Power and Energy Engineering Conference (APPEEC), 2010 Asia-Pacific*, 2010.

[19] W. Luan, J. Peng, M. Maras, J. Lo e B. Harapnuk, "Smart Meter Data Analytics for Distribution Network Connectivity Verification," *Smart Grid, IEEE Transactions on,* vol. 6, nº 4, pp. 1964-1971, July 2015.

[20] P. Prakash, "Data concentrators: The core of energy and data management," Dalas, 2013.

[21] European Regulators' Group for Electricity and Ga (ERGEG), "Treatment of Losses by Network Operators," Bruxelas, 2008.

[22] M. Alam, E. Kabir, M. Rahman e M. Chowdhury, "Power sector reform in Bangladesh: Electricity distribution system," *Energy* , vol. 29, nº 11, pp. 1773-1783, 2004.

[23] CODI - Comitê de Distriuição de Energia Elétrica, *Energia Reativa Excedente*, 2004.

[24] Agência Nacional de Energia Elétrica, 2015. [Online]. Available: http://www.aneel.gov.br/area.cfm?idArea=801. [Acesso em 08 07 2015].

[25] L. A. M. Marques, *Detection and Location of Non-Technical Losses in Low Voltage Distribution Networks,* Porto: U.Porto, 2016.

[26] H. Creder, Instalações Elétricas, 15 ed. ed., Rio de Janeiro: LTC, 2015.

[27] R. L. Boylestad, Introdução À Análise de Circuitos, 12 ed. ed., São Paulo: Pearson, 2012.

[28] Sohn Associates Limited , "Electricity Distribution Systems Losses: Non-Technical Overview," Sohn associates, 2009.

[29] R. Comfort, M. Gonzalez, A. Mansoor, P. Barker, T. Short e A. Sundaram, "Power quality impact of distributed generation: effect on steady state voltage regulation," em *PQA 2001 North America Conference,*, Pittsburgh, Pennsylvania, 2001.

[30] D. E. Johnson, J. L. Hilburn e J. R. Johnson, Fundamentos de Análise de Circuitos Eétricos, 4 ed ed., Rio de Janiero: Prentice-Hall do Brasil, 1994.

[31] A. V. Meier, Electric Power Systems: A Conceptual Introduction, Ney Jersey: John Wiley & Sons, 2006.

[32] Agência Nacional de Energia Elétrica – ANEEL, "Procedimentos de Distribuição de Energia Elétrica no Sistema Elétrico Nacional – PRODIST," [Online]. Available: http://www.aneel.gov.br/prodist. [Acesso em 16 12 2017].

[33] Agência Nacional de Energia Elétrica - ANEEL, "Módulo 7– Cálculo de Perdas na Distribuição," 2013.

[34] Agência Nacional de Energia Elétrica – ANEEL, "Módulo 8 – Qualidade da Energia Elétrica," 2017.

[35] C. M. M. Fernandes, *Desequilíbrio entre fases e perdas na rede de baixa tensão: Parte II - Estratégias óptimas de redução do desequilíbrio,* Lisboa, 2010.

[36] American National Standard, "ANSI C12.1 American National Standard for Electric Meters-Code for Electricity Metering," National Electrical Manufacturers Association, Rosslyn, Virginia, 2016.

[37] American National Standards Institute, "ANSI C12.10 Physical Aspects of Watthour Meters-Safety Standard," National Electrical Manufacturers Association, Rosslyn, VA, 2011.

[38] American National Standards Institute, *ANSI C12.20 Electricity Meters - 0.1, 0.2, and 0.5 Accuracy Classes*, Rosslyn: National Electrical Manufacturers Association, 2015.

[39] Copel, "ETC 4.04 - Especificaçõa Técnica para medidores de energia," 2008.

[40] W. Bank, "Reducing technical and non-technical losses in the power sector.," *Washington, DC: World Bank Group.*, 2009.

[41] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen e X. S. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Science and Technology*, vol. 19, nº 2, pp. 105-120, April 2014.

[42] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni e R. C. Green, "High performance computing for detection of electricity theft," *International Journal of Electrical Power \& Energy Systems* , vol. 47, nº 0, pp. 21-30, 2013.

[43] M. Anas, N. Javaid, A. Mahmood, S. Raza, U. Qasim e Z. Khan, "Minimizing Electricity Theft Using Smart Meters in AMI," em *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2012 Seventh International Conference on*, 2012.

[44] J. Nagi, "An Intelligent System for Detection of non-technical losses in Tenaga Nasional Berhad (TNB) Malaysia Low Voltage Distribution Network," Selangor, 2009.

[45] R. R. Mohassel, A. Fung, F. Mohammadi e K. Raahemifar, "A survey on Advanced Metering Infrastructure," *International Journal of Electrical Power \& Energy Systems* , vol. 63, pp. 473-484, 2014.

[46] S. Salinas, M. Li e P. Li, "Privacy-preserving energy theft detection in smart grids," em *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012 9th Annual IEEE Communications Society Conference on*, 2012.

[47] P.-Y. Chen, S. Yang, J. McCann, J. Lin e X. Yang, "Detection of false data injection attacks in smart-grid systems," *Communications Magazine, IEEE*, vol. 53, nº 2, pp. 206-213, Feb 2015.

[48] F. Skopik e Z. Ma, "Attack Vectors to Metering Data in Smart Grids under Security Constraints," em *Computer Software and Applications Conference Workshops (COMPSACW), 2012 IEEE 36th Annual*, 2012.

[49] J. Nagi, K. Yap, S. K. Tiong, S. Ahmed e M. Mohamad, "Nontechnical Loss Detection for Metered Customers in Power Utility Using Support Vector Machines," *Power Delivery, IEEE Transactions on*, vol. 25, nº 2, pp. 1162-1171, April 2010.

[50] Z. Xiao, Y. Xiao e D.-C. Du, "Non-repudiation in neighborhood area networks for smart grid," *Communications Magazine, IEEE*, vol. 51, nº 1, pp. 18-26, January 2013.

[51] D. Grochocki, J. Huh, R. Berthier, R. Bobba, W. Sanders, A. Cardenas e J. Jetcheva, "AMI threats, intrusion detection requirements and deployment recommendations," em *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, 2012.

[52] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier e S. Zonouz, "A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructures," *Selected Areas in Communications, IEEE Journal on*, vol. 31, nº 7, pp. 1319-1330, July 2013.

[53] X. Liu, P. Zhu, Y. Zhang e K. Chen, "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure," *Smart Grid, IEEE Transactions on*, vol. PP, nº 99, pp. 1-1, 2015.

[54] H. Suleiman, I. Alqassem, A. Diabat, E. Arnautovic e D. Svetinovic, "Integrated Smart Grid Systems Security Threat Model," *Inf. Syst.*, vol. 53, nº C, pp. 147-160, #oct# 2015.

[55] T. Sharma, K. Pandey, D. Punia e J. Rao, “Of pilferers and poachers: Combating electricity theft in India,” *Energy Research \& Social Science* , vol. 11, pp. 40-52, 2016.

[56] B. Loeff, “Deputizing data: using AMI for revenue protection,” vol. 13, nº Utility automation & engineering, p. 44, June 2008.

[57] X. Liu, P. Zhu, Y. Zhang e K. Chen, “A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure,” *Smart Grid, IEEE Transactions on,* vol. PP, nº 99, pp. 1-1, 2015.

[58] C.-H. Lo e N. Ansari, “CONSUMER: A Novel Hybrid Intrusion Detection System for Distribution Networks in Smart Grid,” *Emerging Topics in Computing, IEEE Transactions on,* vol. 1, nº 1, pp. 33-44, June 2013.

[59] R. R. Rathod e R. D. Garg, “Regional electricity consumption analysis for consumers using data mining techniques and consumer meter reading data,” *International Journal of Electrical Power \& Energy Systems* , vol. 78, pp. 368-374, 2016.

[60] S. S. Depuru, “Modeling, detection, and prevention of electricity theft for enhanced performance and security of power grid,” Toledo, 2012.

[61] F. McLoughlin, A. Duffy e M. Conlon, “Evaluation of time series techniques to characterise domestic electricity demand,” *Energy* , vol. 50, nº 0, pp. 120-130, 2013.

[62] B. A. Smith, J. Wong e R. Rajagopal, “A simple way to use interval data to segment residential customers for energy efficiency and demand response program targeting,” em *ACEEE Summer Study on Energy Efficiency in Buildings*, 2012.

[63] T. F. Sanquist, H. Orr, B. Shui e A. C. Bittner, “Lifestyle factors in US residential electricity consumption,” *Energy Policy,* vol. 42, pp. 354-364, 2012.

[64] T. M. Mitchell, Machine Learning, 1 ed., New York, NY, USA: McGraw-Hill, Inc., 1997.

[65] S. Haykin, Neural Networks: A Comprehensive Foundation, 2nd ed., Upper Saddle River, NJ, USA: Prentice Hall PTR, 1998.

[66] V. Kumar, An Introduction to Cluster Analysis for Data Mining, 2000.

[67] P.-N. T. M. S. V. Kumar, “Introduction to Data Mining,” A. C. B. Site, Ed., http://www-users.cs.umn.edu/~kumar/dmbook/index.php, 2006, p. 487–586.

[68] G. Tzortzis e A. Likas, “The global kernel k-means clustering algorithm,” em *Neural Networks, 2008. IJCNN 2008. (IEEE World Congress on Computational Intelligence). IEEE International Joint Conference on*, 2008.

[69] J. A. Hartigan, Clustering Algorithms, 99th ed., New York, NY, USA: John Wiley \& Sons, Inc., 1975.

[70] J. C. Bezdek, R. Ehrlich e W. Full, “FCM: The fuzzy c-means clustering algorithm,” *Computers \& Geosciences,* vol. 10, nº 2, pp. 191-203, 1984.

[71] J. C. Bezdek, Pattern Recognition with Fuzzy Objective Function Algorithms, Norwell, MA, USA: Kluwer Academic Publishers, 1981.

[72] T. Kohonen, “The self-organizing map,” *Proceedings of the IEEE,* vol. 78, nº 9, pp. 1464-1480, Sep 1990.

[73] J. Vesanto e E. Alhoniemi, “Clustering of the self-organizing map,” *Neural Networks, IEEE Transactions on,* vol. 11, nº 3, pp. 586-600, May 2000.

[74] E. M. Viana, “Agrupamento de Conjuntos Consumidores de Energia Elétrica Utilizando Mapas Auto-Organizáveis,” Viçosa -MG, 2006.

[75] N. Cristianini e J. Shawe-Taylor, An Introduction to Support Vector Machines: And Other Kernel-based Learning Methods, New York, NY, USA: Cambridge University Press, 2000.

[76] B. Scholkopf e A. J. Smola, Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond, Cambridge, MA, USA: MIT Press, 2001.

[77] A. C. Lorena e A. C. P. L. F. d. Carvallho, "Uma Introdução às Support Vector Machines," *RITA*, vol. Volume XIV, nº 2, p. 67, 2007.

[78] D. Wang, D. Yeung e E. Tsang, "Weighted Mahalanobis Distance Kernels for Support Vector Machines," *Neural Networks, IEEE Transactions on*, vol. 18, nº 5, pp. 1453-1462, Sept 2007.

[79] W. Zhu, N. Zeng, N. Wang e others, "Sensitivity, specificity, accuracy, associated confidence interval and ROC analysis with practical SAS{\textregistered} implementations," *NESUG proceedings: health care and life sciences, Baltimore, Maryland*, pp. 1-9, 2010.

[80] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognition Letters* , vol. 27, nº 8, pp. 861-874, 2006.

[81] A. A. Cárdenas, S. Amin, G. Schwartz, R. Dong e S. Sastry, "A game theory model for electricity theft detection and privacy-aware control in AMI systems," em *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*, 2012.

[82] Z. Xiao, Y. Xiao e D.-C. Du, "Building Accountable Smart Grids in Neighborhood Area Networks," em *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, 2011.

[83] D. Mashima e A. A. Cárdenas, "Research in Attacks, Intrusions, and Defenses: 15th International Symposium, RAID 2012, Amsterdam, The Netherlands, September 12-14, 2012. Proceedings," D. a. S. S. J. a. C. M. Balzarotti, Ed., Berlin, Heidelberg, Springer Berlin Heidelberg, 2012, pp. 210-229.

[84] Z. Wu, T. Zhao, L. He e X. Shen, "Smart grid meter analytics for revenue protection," em *Power System Technology (POWERCON), 2014 International Conference on*, 2014.

[85] S. Salinas, M. Li e P. Li, "Privacy-Preserving Energy Theft Detection in Smart Grids: A P2P Computing Approach," *Selected Areas in Communications, IEEE Journal on*, vol. 31, nº 9, pp. 257-267, September 2013.

[86] Y. Liu e S. Hu, "Cyberthreat Analysis and Detection for Energy Theft in Social Networking of Smart Homes," *IEEE Transactions on Computational Social Systems*, vol. 2, nº 4, pp. 148-158, Dec 2015.

[87] J. B. Leite e J. R. S. Mantovani, "Detecting and Locating Non-technical Losses in Modern Distribution Networks," *IEEE Transactions on Smart Grid*, vol. PP, pp. 1-1, 2016.

[88] W. Han e Y. Xiao, "FNFD: A Fast Scheme to Detect and Verify Non-Technical Loss Fraud in Smart Grid," em *Proceedings of the 2016 ACM International on Workshop on Traffic Measurements for Cybersecurity*, New York, NY, USA, 2016.

[89] W. Han e Y. Xiao, "A novel detector to detect colluded non-technical loss frauds in smart grid," *Computer Networks*, pp. -, 2016.

[90] W. Han e Y. Xiao, "NFD: Non-technical loss fraud detection in Smart Grid," *Computers \& Security*, vol. 65, pp. 187-201, 2017.

[91] C. L. Su, W. H. Lee e C. K. Wen, "Electricity theft detection in low voltage networks with smart meters using state estimation," em *2016 IEEE International Conference on Industrial Technology (ICIT)*, 2016.

[92] E. Villar-Rodriguez, J. D. Ser, I. Oregi, M. N. Bilbao e S. Gil-Lopez, "Detection of non-technical losses in smart meter data based on load curve profiling and time series analysis," *Energy*, vol. 137, pp. 118-128, 2017.

[93] S.-C. Yip, K. Wong, W.-P. Hew, M.-T. Gan, R. C. W. Phan e S.-W. Tan, "Detection of energy theft and defective smart meters in smart grids using linear regression," *International Journal of Electrical Power & Energy Systems*, pp. 230-240, 2017.

[94] S.-C. Yip, C.-K. Tan, W.-N. Tan, M.-T. Gan e A.-H. A. Bakar, "Energy theft and defective meters detection in AMI using linear regression," em *IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)*, Milan, 2017.

[95] S. Depuru, L. Wang e V. Devabhaktuni, "Support vector machine based data classification for detection of electricity theft," em *Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES*, 2011.

[96] S. Depuru, L. Wang, V. Devabhaktuni e P. Nelapati, "A hybrid neural network model and encoding technique for enhanced classification of energy consumption data," em *Power and Energy Society General Meeting, 2011 IEEE*, 2011.

[97] S. Depuru, L. Wang e V. Devabhaktuni, "Enhanced encoding technique for identifying abnormal energy usage pattern," em *North American Power Symposium (NAPS), 2012*, 2012.

[98] J. Nagi, K. S. Yap, S. K. Tiong, S. Ahmed e F. Nagi, "Improving SVM-Based Nontechnical Loss Detection in Power Utility Using the Fuzzy Inference System," *IEEE Transactions on Power Delivery*, vol. 26, nº 2, pp. 1284-1285, April 2011.

[99] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar e S. Mishra, "Decision Tree and SVM-based Data Analytics for Theft Detection in Smart Grid," *IEEE Transactions on Industrial Informatics*, vol. PP, nº 99, pp. 1-1, 2016.

[100] Y. Guo, C. W. Ten e P. Jirutitijaroen, "Online Data Validation for Distribution Operations Against Cybertampering," *IEEE Transactions on Power Systems*, vol. 29, nº 2, pp. 550-560, March 2014.

[101] P. Jokar, N. Arianpoo e V. C. M. Leung, "Electricity Theft Detection in AMI Using," *IEEE Transactions on Smart Grid*, nº 1, pp. 216-226, Jan 2016.

[102] A. H. Nizar, Z. Y. Dong e Y. Wang, "Power Utility Nontechnical Loss Analysis With Extreme Learning Machine Method," *IEEE Transactions on Power Systems*, vol. 23, nº 3, pp. 946-955, Aug 2008.

[103] A. H. Nizar e Z. Y. Dong, "Identification and detection of electricity customer behaviour irregularities," em *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, 2009.

[104] C. C. O. Ramos, A. N. de Sousa, J. P. Papa e A. X. Falcao, "A New Approach for Nontechnical Losses Detection Based on Optimum-Path Forest," *IEEE Transactions on Power Systems*, vol. 26, nº 1, pp. 181-189, Feb 2011.

[105] C. C. O. Ramos, A. N. de Souza, A. X. Falcao e J. P. Papa, "New Insights on Nontechnical Losses Characterization Through Evolutionary-Based Feature Selection," *IEEE Transactions on Power Delivery*, vol. 27, nº 1, pp. 140-146, Jan 2012.

[106] J. P. Kosut, F. Santomauro, A. Jorysz, A. Fernández, F. Lecumberry e F. Rodríguez, "Abnormal consumption analysis for fraud detection: UTE-UDELAR joint efforts," em *Innovative Smart Grid Technologies Latin America (ISGT LATAM), 2015 IEEE PES*, 2015.

[107] V. Ford, A. Siraj e W. Eberle, "Smart grid energy fraud detection using artificial neural networks," em *Computational Intelligence Applications in Smart Grid (CIASG), 2014 IEEE Symposium on*, 2014.

[108] C. Cody, V. Ford e A. Siraj, "Decision Tree Learning for Fraud Detection in Consumer Energy Consumption," em *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*, 2015.

[109] E. W. S. Ângelos, "Sistema para classificação de anormalidades no consumo de energia elétrica," São Luis, 2009.

[110] E. W. S. Ângelos, O. R. Saavedra, O. A. C. Cortes e A. N. d. Souza, "Detection and Identification of Abnormalities in Customer Consumptions in Power Distribution Systems," *IEEE Transactions on Power Delivery*, vol. 26, pp. 2436-2442, 2011.

[111] V. Badrinath Krishna e G. A. a. S. W. H. Weaver, "Quantitative Evaluation of Systems: 12th International Conference, QEST 2015, Madrid, Spain, September 1-3, 2015, Proceedings," J. a. H. R. B. Campos, Ed., Cham, Springer International Publishing, 2015, pp. 70-85.

[112] T. Hartmann, A. Moawad, F. Fouquet, Y. Reckinger, T. Mouelhi, J. Klein e Y. L. Traon, "Suspicious electric consumption detection based on multi-profiling using live machine learning," em *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2015.

[113] X. Yang, P. Zhao, X. Zhang, J. Lin e W. Yu, "Toward a Gaussian-Mixture Model-Based Detection Scheme Against Data Integrity Attacks in the Smart Grid," *IEEE Internet of Things Journal*, vol. 4, pp. 147-161, Feb 2017.

[114] X. Yang, X. Zhang, J. Lin, W. Yu e P. Zhao, "A Gaussian-Mixture Model Based Detection Scheme against Data Integrity Attacks in the Smart Grid," em *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, 2016.

[115] J. L. Viegas e S. M. Vieira, "Clustering-based novelty detection to uncover electricity theft," em *IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, Naples, 2017.

[116] F. McLoughlin, A. Duffy e M. Conlon, "A clustering approach to domestic electricity load profile characterisation using smart metering data," *Applied Energy* , vol. 141, pp. 190-199, 2015.

[117] E. M. Lakatos e M. d. A. Marconi, Metodologia Científica, 2 Edição ed., São Paulo: Atlas, 2006.

[118] V. D. Maren, Méthodes de recherche pour I´Éducation, Montréal: De Boeck, 1999.

[119] MathWorks, "Matlab," [Online]. Available: http://www.mathworks.com/products/matlab/. [Acesso em 15 06 2016].

[120] Wolfram Computation Meets Knowledge, "Mathematica," Wolfram , [Online]. Available: https://www.wolfram.com/mathematica/. [Acesso em 12 09 2017].

[121] CER, "Commission for Energy Regulation," 2016. [Online]. Available: http://www.cer.ie/. [Acesso em 03 06 2016].

[122] UCD, "Irish Social Science Data Archive," 05 2016. [Online]. Available: http://www.ucd.ie/issda/data/commissionforenergyregulationcer/. [Acesso em 03 06 2016].

[123] F. McLoughlin, A. Duffy e M. Conlon, “Evaluation of time series techniques to characterise domestic electricity demand,” *Energy* , vol. 50, nº 0, pp. 120-130, 2013.

[124] F. Ni, P. H. Nguyen, J. F. G. Cobben, v. d. Brom, H. E. e D. Zhao, “Uncertainty Analysis of Aggregated Smart Meter Data for State Estimation,” em *In Applied Measurements for Power Systems (AMPS), 2016 IEEE International Workshop on IEEE*, 2016.

[125] M. I. d. M. P. M. Vaz, *Controlo de Tensão em Redes de Baixa Tensão por Atuação em Recursos Distribuídos,* F. d. E. -. U. d. Porto, Ed., Porto: U.PORTO, 2015, p. 95.

[126] P. R. Pimentel, “Smart Trafo – inovação brasileira para acelerar a implantação do conceito smart grid,” 2013.

[127] Electric Ireland, “https://www.electricireland.ie,” [Online]. Available: https://www.electricireland.ie/residential/help/safety/what-is-the-standard-voltage-in-ireland. [Acesso em 29 08 2017].

[128] ELO, “ELO Sistemas Eletrônicos,” [Online]. Available: http://www.elonet.com.br/produto.php?id=31. [Acesso em 08 07 2017].

[129] Landis + Gyr, “E650 Medidor Eletrônico, Multifunção Multitarifa,” 2016.

[130] M. N. Magalhães e A. C. P. d. Lima, “Noções de Probabilidade e Estatística,” 7 edição ed., EDUSP, 2010.

[131] MathWorks, “https://www.mathworks.com/,” MathWorks, [Online]. Available: https://www.mathworks.com/help/stats/lillietest.html. [Acesso em 18 08 2017].

[132] Mathworks, “https://www.mathworks.com/,” Mathworks, [Online]. Available: https://www.mathworks.com/help/stats/ecdf.html. [Acesso em 17 08 2017].

[133] Department of Industry and Science, 2014. [Online]. Available: https://data.gov.au/dataset/sample-household-electricity-time-of-use-data. [Acesso em 10 08 2014].

Apêndice A

A New SVM-Based Fraud Detection Model for AMI

A New SVM-Based Fraud Detection Model for AMI

Marcelo Zanetti, Edgard Jamhour(✉), Marcelo Pellenz, and Manoel Penna

Pontifical Catholic University of Parana, Curitiba, Brazil
marcelo.zanetti11@gmail.com, ejamhour@gmail.com,
marcelopellenz@gmail.com, camillo.penna@gmail.com

Abstract. This paper presents a new strategy for fraud detection in Advanced Metering Infrastructure (AMI) based on the analysis of disturbances in the pattern consumption of end-customers. The proposed strategy is based on the use of SVM (Supported Vector Machine). SVM requires labeled training data in order to define a classification function. The need of labeled data is a serious limitation for practical implementation of fraud detection systems in AMI. To work around this problem, we propose a new strategy for training SVM classifiers that requires only normal consumption patterns in the training phase. The anomalous consumption is generated by simulating attacks on the normal consumption patterns.

Keywords: AMI · Fraud detection · Energy theft · Smart grid · SVM

1 Introduction

In power systems, losses refer to the amounts of electricity injected into the transmission and distribution grids that are not paid by the end users. There are two types of losses: technical and non-technical [13]. Technical losses are inherent to the transmission of energy and consist mainly of power dissipation. Non-technical losses (NTL) consist primarily of electricity theft, non-payment by customers, and errors in accounting and record-keeping. Non-technical losses (NTL) are small in developed countries [13]. In contrast, the situation tends to be significantly different in developing countries, and can commonly exceed 10 %. NTL may be very difficult and costly to identify in grids based on monthly manual measures of consumption [14]. However, with the introduction of Advanced Metering Infrastructure (AMI) in Smart Grids new automated approaches are possible. A promising approach consists to generate consumption patterns for the end users and monitor significantly divergences from these patterns. According to [7], with the large amount of data obtained with AMI, to determine user profiles using statistical techniques may be very difficult. However, machine learning techniques are a very promising and suitable approach.

In this paper, we presented a new method for detecting energy theft in grids monitored by AMI. The method uses a SVM (Supported Vector Machine) learning approach to generate a fraud detection model (FDM) capable of detecting

A. Skavhaug et al. (Eds.): SAFECOMP 2016, LNCS 9922, pp. 226–237, 2016.
DOI: 10.1007/978-3-319-45477-1_18

disturbances in the pattern of consumption of end-users. SVM is a supervised learning model that requires labeled training data in order to define a classification function. The need of labeled data is a serious limitation for practical implementation of fraud detection systems in AMI. To work around this problem, we propose a new strategy for training SVM classifiers that requires only normal consumption patterns in the training phase. The anomalous consumption is generated by simulating attacks on the normal consumption patterns.

The main contribution of this paper is not the use of a specific machine learning technique. Instead, the innovation of our approach is to build individual consumer profiles, while most proposals in the literature builds profiles to classes or groups of users (see Sect. 2). Also, we have defined and formalized a strategy to simulate several types of false data injection into consumer patterns (defined in Sect. 3), which permits a robust training of the proposed machine learning detection model (presented in Sect. 4) and also works as an accurate test-bed to evaluate the performance of any other fraud detection model for AMI (presented in Sect. 5). Our evaluation (Sect. 6) shows that this approach is very promising, as it permits to detect the most common types of frauds.

2 Related Works

In this section we review some works that also address the problem of detecting energy theft by customers. The authors in [2] uses a fuzzy-based clustering algorithm to identify subgroups of users with similar profiles. Suspect profiles are identified by measuring the distance between the client consumption and the regular (normal) profile. The fraud detection model proposed by the authors is unsupervised and independent of rules. A SVM based approach that uses customer load profile information and additional attributes to expose abnormal behavior that is known to be highly correlated with NTL activities is proposed by [8]. The authors dispose of profile information of two types of users: normal and anomalous. That permits to generate a labeled training dataset, and use SVM to generate a decision function that can classify new users into the classes normal or anomalous.

An intrusion detection system (IDS) that combines meter audit logs of physical and cyber events with consumption data to more accurately model and detect theft-related behavior is proposed by [7]. The authors evaluate that smart meters are more vulnerable than mechanical meters. The IDS uses an attack graph based information fusion technique to combine evidences of three types: network and host-based IDS, on-meter anti-tampering sensors and anomalous consumption detectors.

A non-repudiation technique to detect frauds that employs two meters for each individual wire connecting the subscriber and the provider is proposed by [15]. The readings of the two meters are continuously compared and if a certain threshold is exceeded a fraud alarm is generated. The same approach is used in [14], but in this case, instead of using a redundant meter for each subscriber, a single meter is used for a group of subscribers. The authors proposes a set of

techniques to detect frauds by comparing the reading from the collective meter with the summation for the reading from the subscriber meters. A framework for training and testing customer energy consumption datasets in order to separate and group illegal consumers is proposed by [5]. The authors use a SVM algorithm to classify consumption patterns with respect to geographical location, type of customer (residential, commercial, etc.) and season of the year. A set of rules is used to classify customers into different classes that represents how suspect the user profile is. The authors in [11] also conclude that the introduction of AMI may increase the risk of frauds because smart meters are subject to more types of attacks than mechanical meters. The authors are concerned about proposing a fraud detection model that preserve the privacy of consumption information from the end users. To address this problem the authors proposed a distributed technique that identifies the honesty of users by solving a linear system of equations that takes into account the consumption of users in a neighborhood and the total energy consumption of this neighborhood measured at a local data collector.

The method proposed in this paper have some similarities with [2,5,8]. However, these works generate profiles based on group of users. On the other hand, our approach consists to generate a different profile for each user. In the evaluation section we show the superiority of our approach by comparing with the method proposed by [8]. Another important difference is that our approach uses a dataset with measures obtained from a real AMI deployment. Therefore, the method developed in this paper uses unique information about the consumption patterns that have been ignored by most of the other studies.

3 Non-Technical Losses

Non-technical losses (NTL) in power systems refers mainly to energy theft, but also may include losses due to poor equipment maintenance, calculation errors and accounting mistakes. Usually, NTL related to energy theft are located in the "last mile" of the power distribution system. Traditionally, consumers are the primary source of NTL [6]. Some common methods used by consumers to generate NTL in non-AMI grids are discussed in [1,4]. With the use of smart meters and deployment of AMI, some NTL threads may be avoided. However, the introduction of networking elements and digital communication offers new possibilities for malicious users. Figure 1 illustrates a typical AMI topology [9]. In AMI, malicious users may generate false measures of consumption by modifying the meter, the communication from the meter to the utility billing system or by tapping energy illegally from the grid in order to bypass meters. According to [12], three levels of vulnerability can be considered in Smart Grids: from smart meters to concentrator nodes (HAN), from concentrator nodes to data centers (NAN) and on application level and community networks that use gathered meter data (WAN). In this paper we consider the frauds generated by modifying the meter or its communication in the HAN, which are usually referred as false data injection (FDI). The authors in [7] enumerate the following types of FDI

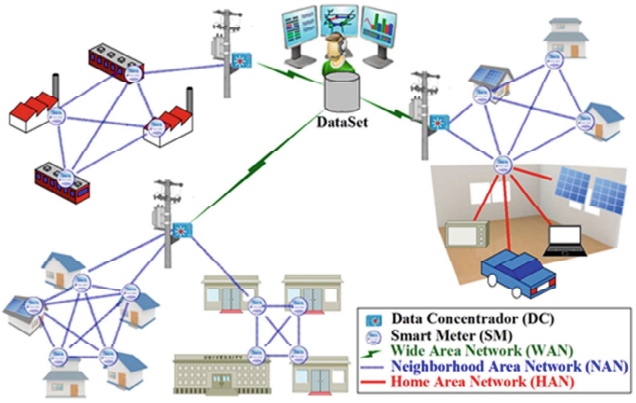

Fig. 1. Advanced Meter Infrastructure (AMI)

generated by malicious users: (i) Zero consumption: report zero consumption; (ii) Act as generator: report negative consumption; (iii) Percentage: cut the report by a given percentage; (iv) Cut-off point: alter the load profile to hide large loads. In this paper we consider two additional types of FDI: (v) Offset: cut report by a constant value and (vi) Low profile: report a low profile to simulate vacancy;

4 SVM-Based Fraud Detection System

Supported Vector Machine is a supervised learning method that generates classification functions [3]. A classification function defines a mapping $V \mapsto Y$ where $v \in V$ is some object and $y \in Y$ is a class label. Let's assume a binary SVM, and objects corresponding to a vector of real numbers. So: $v \in R^n$, $y \in \{-1, 1\}$. If the elements in V are linearly separable, SVM produces a decision function $g(v)$ as a hyperplane in R^n that permits to classify each element v into -1 or $+1$.

In this paper, we employ a linear (binary) SVM algorithm to construct a fraud detection model (FDM) for individual consumption profiles. To generate a decision function, SVM requires a training dataset with labeled data that includes both normal and anomalous measures. In this section, we explain how to generate the training dataset using only normal measures.

Figure 2 shows the main steps used to generate the SVM-based FDM. Usually, data is acquired regularly by the AMI system in intervals of an hour or less. We assume that a dataset without frauds is available for SVM training (a). Normal profiles can be obtained by assuring that the sum of the consumption reported by a group of users match collective meters placed in the low power distribution grid. This approach is not trivial, as it requires taking into account technical losses, but it is feasible [11,16]. In order to generate a successful classification model, the training dataset must include enough number of normal and anomalous samples. In our method, anomalous samples are generated by injecting false measures in the normal profile dataset (b). Assuming that $x \in X$ are the normal

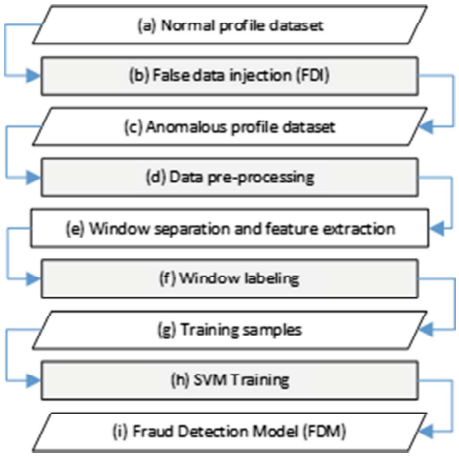

Fig. 2. Fraud Detection Model (FDM) generation

measures, the anomalous dataset X' is generated by replacing x by x' according to Table 1. In this paper we have not considered frauds in energy production because there is still not enough public data with this type of profile available. In the table, P represents a parameter that controls the amount of energy stolen and $\bar{x}$ is the average value of $x \in X$. The cut-off point FDI replaces all measures above the threshold A by a random value $\in (A_{min}, A)$. For the purpose of the tests presented in this paper, A and A_{min} are adjusted to match the amount of energy stolen defined by P. The zero consumption and the low profile FDIs are not controlled by P. In the low profile FDI, X_{low} represents a subset of the lower measures in X. In our tests, X_{low} is lower third part of the measures in X.

Table 1. FDI definitions

FDI	Measure modification
Offset	$x' \leftarrow x - P \cdot \bar{x}$
Percentage	$x' \leftarrow (1 - P) \cdot x$
Cut-off point	$x' \leftarrow \begin{cases} x & \text{if } x \leq A \\ \text{rand}\,(A_{min}, A) & \text{if } x > A \end{cases}$
Zero consumption	$x' \leftarrow 0$
Low profile	$x' \leftarrow \text{rand}\,(a \in X_{low})$

During the training, the offset, cut-off point and percentage FDIs are applied to the normal dataset in order to generate an anomalous dataset as illustrated in Fig. 3 (c). The other types of FDI are not used because they are easier to detect. They can be considered extreme cases of the other FDIs. The sensitivity

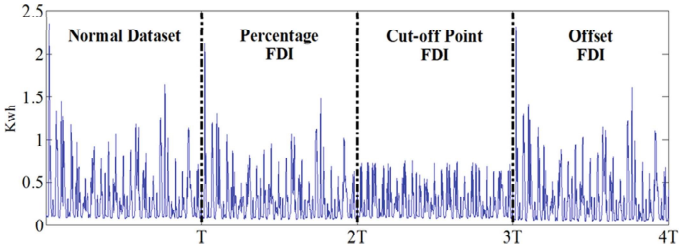

Fig. 3. Training dataset example

of the training procedure is controlled by the parameter P. An excessive small P can cause the system to generate many false alarms. Conversely, a large P may cause the system to neglect small frauds.

When the measurement interval is small, the incremental consumption may variate significantly. The incremental variations of consumption are not very useful to typify the behavior of a consumer. Indeed, our tests indicate that SVM generate poor classifiers when raw data is used for training. We have observed that it is more useful to smooth the consumption data by using a simple or exponential moving average, which is performed in step (d). In our tests we have employed a simple moving average where each measure is the mean of the measures within the last two-hours.

The samples used to train the SVM classifier must correspond to vectors $v = (x_1 \cdots x_w)$ of same dimension. In step (e), the training dataset is divided in windows with w measures. We have also observed that using all measures in a window as training samples results in bad classifiers. Therefore, we propose to use only a fraction of the data in a window, extracted in accordance to a heuristic that depends on the type of fraud we want to detect. The measures from a windows of size w are ordered and divide into three subsets of equal size $(v_{min}, v_{avc}, v_{max})$. The subset v_{max} is used to generate FDM for detecting frauds of type "cut-off point" and "low profile". The subset v_{min} is used for all other types of frauds. The same feature extraction strategy is used during the training and evaluation phases.

In step (f), each window v is labeled as normal (1) or anomalous (-1) by tracking the measures to determine if they came from a normal or anomalous dataset. The labeled features extracted from the windows correspond to the samples used by the SVM (g). Finally, the SVM algorithm (h) is used to generate the fraud detection model (i).

5 Dataset Preparation and Metric Definition

The dataset used in this paper was obtained from the Project Smart City from the City of Newcastle, Australia [10]. The dataset contains the consumption information of 31 houses, monitored for about one year. The energy consumption (kwh) is measured in intervals of 30 min, generating 48 daily records per house.

In our experiments, only 28 houses were considered. Three houses were excluded because they are energy producers. To evaluate our system, we have divided the dataset into two parts: training data and evaluation data. Because the original dataset contains only normal data, we have injected frauds in the dataset using the algorithm 1. The variables used by the algorithm are explained in Table 2. Basically, the algorithm uses two exponentially distributed variables to control the fraction of measures from the original dataset that are replaced by frauds. In average, the fraction of measures replaced is given by: $\frac{A}{A+N}$, where A and N are the means of the random variables a and n, respectively. Figure 4 shows how the measures of a consumer are affected by the fraud injections. We can also observe that periods with very low consumption are common in the dataset, as residents may be in vacancy (narrowest rectangle in Fig. 4). Except when the size of the evaluation window is very large, these periods tend to generate false alarms.

Table 2. Symbols in the algorithm used to contaminate the dataset

Symbol	Meaning
T	Number of measures used for training
D	Number of measures in the dataset
n	Random variable that controls a normal period (mean N)
a	Random variable that controls a FDI (mean A)
f	FDI function

Algorithm 1. Contaminate the dataset with FDI

1: $i \leftarrow T$ ▷ i measure index
2: **repeat**
3: $n \leftarrow Floor\,(Random\,(N))$
4: $i \leftarrow i + n$ ▷ jumps normal period
5: $a \leftarrow Floor\,(Random\,(A))$
6: $f \leftarrow$ Randomly selected FDI function
7: **while** $i < Min\,(i + a, D)$ **do** ▷ applies FDI
8: $x_i \leftarrow f\,(x_i)$
9: $i \leftarrow i + 1$
10: **end while**
11: **until** $i < D$

In the evaluation section we have used the following metrics to measure the performance of the fraud detection system: tpr (true positive rate), fpr (false positive rate) and F-measure (F). The F-measure definition requires the definition of an intermediate metric called precision (p). These metrics are defined as follows: $tpr = \frac{tp}{tp+fn}$; $fpr = \frac{fp}{fp+tn}$; $p = \frac{tp}{tp+fp}$ e $F = 2 \cdot \frac{p.tpr}{p+ptr}$, where: tp (true positive): a corrupted window was detected; fp (false positive): a normal window was pointed as fraud; fn (false negative): a corrupted window was not detected and tn (true negative): a normal window was pointed as legitimate.

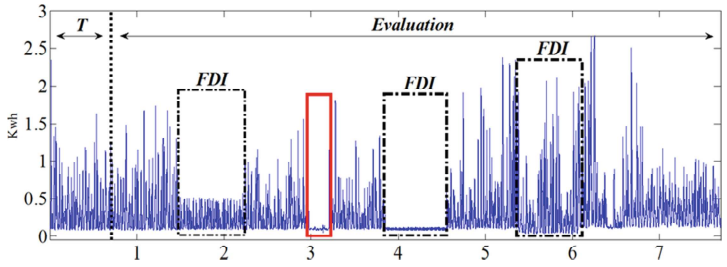

Fig. 4. Dataset preparation

6 Fraud Detection System (FDS) Evaluation

The evaluation presented in this section has the following purposes: (i) Determine the best configuration of the parameters: T (training period), w (window size) and the training distribution approach used to account for the effect of seasons; (ii) Determine the performance under different attack conditions expressed in terms of the amount of energy stolen: P and (iii) Compare our strategy with the group-based profile generation approach defined in [8].

According to our method, a window is the minimum set of measures that can be reported as a fraud. Figure 5 shows the influence of the windows size (w) on the FDS performance. This evaluation was performed considering only FDIs of type cut-off point, percentage and offset, randomly applied to 30 % of the dataset. The average FDI duration was $A = 1008$ measures (21 days). The other types of FDI were not used in this test because they are easier to detect and may masquerade the results. The test was repeated with three different amounts of energy theft: $P = 10\,\%$, $20\,\%$ and $30\,\%$. The SVM classifier was trained with a dataset injected with the same frauds, but only $P = 10\,\%$ of energy theft. All tests in this section have used $P = 10\,\%$ for training. It is important to note that neither the type of FDI nor the amount of energy theft need to be known beforehand.

The figure shows the average result obtained considering all houses and all amounts of energy theft. The best metric to evaluate the performance of the FDS is the F-Measure, because it can balance the ability of the system to detect frauds without generating excessive false positives. Using this metric as reference, the best overall result was obtained with $w = 144$ measures per window (or 3 days).

The effect of the training period on the performance of the FDS is shows in Fig. 6. This test was executed with $w = 144$ (3 days). The performance increases up to $T = 3024$ (63 days). After this point increasing the training period does not increase the performance of the system.

In the previous tests the training period was placed in the beginning of the database. However, the consumption profile of a customer is heavily influence by the season. Therefore, we have evaluated if distributing the training period among different seasons can improve the FDS performance. We have considered four different techniques with respect to how the training period was distributed: Technique 1: one training period $T = 3024$ (63 days) in the beginning of

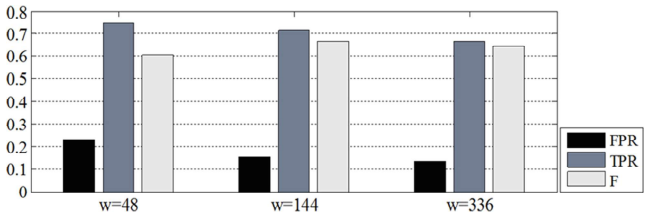

Fig. 5. Effect of the window size on the FDS performance

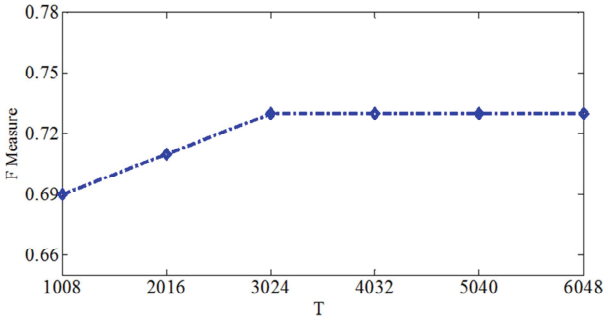

Fig. 6. Effect of the training period on the FDS performance.

the dataset; Technique 2: one training period in the beginning of each season ($T = 756$ for each period); Technique 3: one training period in the beginning of each month ($T = 252$ for each period) and Technique 4: one different model for each season ($T = 756$). Techniques 1 to 3 generate a single model that is applied to the remaining of the dataset. Technique 4 generates a distinct model for each season, and the model is shifted accordingly when the season changes. Figure 7 shows the performance of these techniques with respect to the FDIs of type offset, cut-off point, percentage and the average result considering all three types of FDI.

In Fig. 7, techniques 1 and 4 presented similar results. Figures 8 and 9 present a more detailed comparison between these techniques. Both techniques were evaluated with the same dataset, where 30 % of the measures were randomly contaminated with all types of FDI. One can observe that both techniques have similar detection rates, but technique 4 generates far less false positives. Normal seasonal variations of consumption are misinterpreted as attacks by technique 1, but not by technique 4 that employs a shifting model.

We have used the same dataset [10] to evaluate the SVM-based FDS presented by [8]. The FDS proposed in [8] follows a different approach, as a fraud detection model is generated by using data gathered from group of users. Because the number of houses is small, we have selected 10 houses to generate the anomalous profile and the remaining 18 houses to generate the normal profile. We have modified 30 % of the measures available for the anomalous houses with the

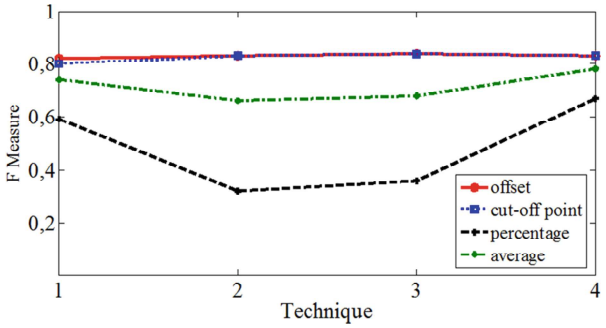

Fig. 7. Effect of the training distribution on the FDS performance.

five types of FDI defined in Table 1. To approximate the conditions suggested by the authors, we have used a window size of 1440 measures (1 month) and used 50 % of the dataset for training and 50 % for evaluation of the resulting SVM classifier. Figure 10 shows the average result obtained for all houses with respect to different amounts of energy stolen. Given the diversity of profiles used for training, the resulting classifier is very conservative, and generates a very low rate of false positives. However, it is also inaccurate to detect true attacks. For $P = 30\,\%$, our approach achieves $F = 0.66$ with $TPR = 0.95$ (technique 1) and $F = 0.76$ with $TPR = 0.95$ (technique 4), while [8] achieves only $F = 0.5$ with $TPR = 0.45$. As pointed by the authors, their method is expected to perform well only for large amounts of energy stolen.

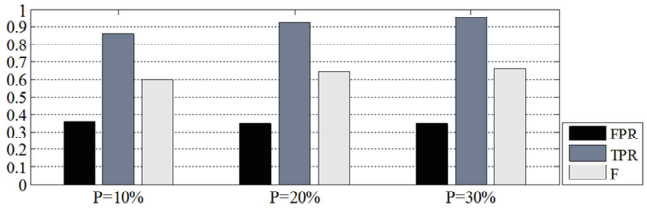

Fig. 8. Evaluation of technique 1 with respect to the amount of energy stolen

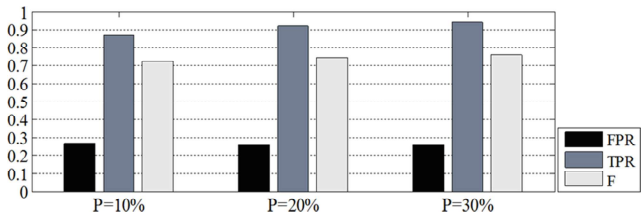

Fig. 9. Evaluation of technique 4 with respect to the amount of energy stolen

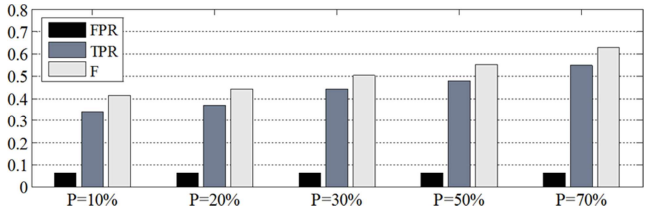

Fig. 10. Performance of the group based profile proposed in [8].

7 Conclusion

We have presented a fraud detected system (FDS) for detecting energy theft in grids monitored by AMI. In the literature, the most common approach consists to generate a fraud detection model (FDM) using information gathered from a group of users. Our evaluation with a dataset based on measures obtained from an actual AMI deployment indicates that a neighborhood with similar economical conditions presents significant differences on their consumption profiles. Therefore, a FDM based on information of a group of users tends to be very inaccurate to hold significant consumption discrepancies. We have addressed this issue by generating a different FDM for each consumer, greatly improving the accuracy of the FDS. As a future research, we intend to integrate the information from meters that measure the total consumption of a neighborhood. That approach will permit to update the consumption profile of the users whenever the comparison between the neighborhood meter and the individual meters indicate no fraud.

References

1. Anas, M., Javaid, N., Mahmood, A., Raza, S.M., Qasim, U., Khan, Z.A.: Minimizing electricity theft using smart meters in AMI. In: 2012 Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), pp. 176–182, November 2012
2. Angelos, E.W.S., Saavedra, O.R., Cortés, O.A.C., de Souza, A.N.: Detection and identification of abnormalities in customer consumptions in power distribution systems. IEEE Trans. Power Deliv. **26**(4), 2436–2442 (2011)
3. Cortes, C., Vapnik, V.: Support-vector networks. Mach. Learn. **20**(3), 273–297 (1995)
4. Depuru, S.S.S.R., Wang, L., Devabhaktuni, V., Green, R.C.: High performance computing for detection of electricity theft. Int. J. Electr. Power Energy Syst. **47**, 21–30 (2013)
5. Depuru, S.S.S.R., Wang, L., Devabhaktuni, V.: Support vector machine based data classification for detection of electricity theft. In: 2011 IEEE/PES Power Systems Conference and Exposition (PSCE), pp. 1–8, March 2011
6. Jiang, R., Lu, R., Wang, Y., Luo, J., Shen, C., Shen, X.S.: Energy-theft detection issues for advanced metering infrastructure in smart grid. Tsinghua Sci. Technol. **19**(2), 105–120 (2014)

7. McLaughlin, S., Holbert, B., Fawaz, A., Berthier, R., Zonouz, S.: A multi-sensor energy theft detection framework for advanced metering infrastructures. IEEE J. Sel. Areas Commun. **31**(7), 1319–1330 (2013)
8. Nagi, J., Yap, K.S., Tiong, S.K., Ahmed, S.K., Mohamad, M.: Nontechnical loss detection for metered customers in power utility using support vector machines. IEEE Trans. Power Deliv. **25**(2), 1162–1171 (2010)
9. NIST. Nist framework and roadmap for smart grid interoperatibility satandards, release 3. Technical report, U.S. Department of Commerce (2014)
10. Department of Industry and Science. Sample household electricity time of use data, July 2014
11. Salinas, S., Li, M., Li, P.: Privacy-preserving energy theft detection in smart grids. In: 2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), pp. 605–613, June 2012
12. Skopik, F., Ma, Z.: Attack vectors to metering data in smart grids under security constraints. In: 2012 IEEE 36th Annual Computer Software and Applications Conference Workshops (COMPSACW), pp. 134–139, July 2012
13. World Bank. Reducing technical and non-technical losses in the power sector. World Bank Group, Washington, DC (2009)
14. Xiao, Z., Xiao, Y., Du, D.H.: Exploring malicious meter inspection in neighborhood area smart grids. IEEE Trans. Smart Grid **4**(1), 214–226 (2013)
15. Xiao, Z., Xiao, Y., Du, D.H.-C.: Building accountable smart grids in neighborhood area networks. In: 2011 IEEE Global Telecommunications Conference (GLOBECOM 2011), pp. 1–5, December 2011
16. Xiao, Z., Xiao, Y., Du, D.H.-C.: Non-repudiation in neighborhood area networks for smart grid. IEEE Commun. Mag. **51**(1), 18–26 (2013)