

# Desenvolvimento de um Sistema Especialista para Detecção de Pontos Potenciais de Perdas Comerciais

A. N. de Souza, P. S. Silva, A. M. Oltremari, M. G. Zago, F. L. do Amaral e P. da Costa Jr,  
Laboratório de Sistemas de Potência e Técnicas Inteligentes - LsisPoTi - UNESP - Bauru  
B. C. Costa Jr, L. C. Martins e T. D. Moreira, Manaus Energia

**Resumo** - As ligações clandestinas de energia elétrica são motivo de preocupações constantes, tanto para as concessionárias de distribuição de energia elétrica, quanto para as agências reguladoras. Dessa forma, este estudo tem por objetivo o desenvolvimento de um Sistema Especialista para detecção de pontos potenciais de perdas comerciais, tendo por base a análise dos registros de consumidores da Manaus Energia através da utilização de ferramentas inteligentes.

**Palavras-chave** – perdas comerciais, fraudes, ferramentas inteligentes, sistema especialista, Redes Neurais Artificiais.

## I. INTRODUÇÃO

As ligações clandestinas de energia elétrica são motivo de preocupações constantes, tanto para as concessionárias de distribuição de energia elétrica, quanto para as agências reguladoras. Especificamente, a fraude afeta o poder público que não recolhe os tributos, sobretudo, o ICMS (Imposto Sobre Circulação de Serviços e Mercadorias), o município que não recolhe a taxa de iluminação pública e o cliente que paga pelo prejuízo rateado entre os consumidores nas tarifas, e que não recebe os benefícios sociais de obras que seriam executadas pelo poder público com a receita em ICMS [1-2].

Um outro enfoque também muito importante é que a minimização das perdas provocadas por estas fraudes representa a garantia de investimentos na qualidade dos serviços, na manutenção do patrimônio da concessão e principalmente na possibilidade de expansão do atendimento com menor custo.

Chama-se de perda de energia elétrica a diferença existente entre a energia requerida por uma Unidade Consumidora (UC) e a energia medida nesta mesma (UC) em um intervalo de tempo [3-4].

As perdas de energia encontradas em um sistema de distribuição são basicamente de duas naturezas: técnica e comercial.

**Perdas Técnicas:** compreendem toda a energia dissipada por efeito joule no transporte da corrente elétrica nos condutores, equipamentos e conexões, acrescentadas a estas a energia associada às correntes de fuga à massa em um siste-

ma de potência.

**Perdas Comerciais:** são aquelas associadas à comercialização da energia fornecida ao usuário final. Existe uma parcela de energia que é produzida, transportada e fornecida, no entanto, não é faturada. Elas são classificadas em administrativas (quando não há responsabilidade do consumidor) e de intervenção ilícita (quando há responsabilidade do consumidor).

Dessa forma, como perda comercial de intervenção ilícita pode-se citar os seguintes tipos de fraudes:

- Desvio de energia elétrica em pontos localizados antes da medição;
- Adulteração dos mecanismos internos do medidor;
- Alteração dos registros de consumo;
- Interferência na chave de aferição ou na fiação dos circuitos dos sistemas de medição indireta;
- Ligação ou religação à revelia;
- Interferência ou avaria provocada nos transformadores para instrumentos; e
- Quaisquer outros atos provocados intencionalmente com o objetivo de diminuir o registro de energia elétrica efetivamente consumida.

As intervenções ilícitas correspondem ao montante de energia não faturado, e estão relacionadas às intervenções que não são autorizadas pela concessionária, sendo realizadas por usuários legalizados ou não, que intencionalmente provocam um registro de consumo inferior ao real, ou ainda executam o desvio da energia elétrica (popularmente conhecido como “gatos”).

Dessa forma, este estudo tem por objetivo a análise dos registros de consumo medido dos clientes da Manaus Energia, a implementação computacional de uma ferramenta inteligente para análise e classificação dos consumidores suspeitos de fraudes e desenvolvimento de um Sistema Especialista (*FraudInspector*) capaz de indicar pontos potenciais de perdas comerciais.

## II. HISTÓRICO

A análise de perdas não-técnicas no setor de distribuição de energia elétrica pode ser realizada com base em dois algoritmos de classificação populares: o classificador *Naïve*

---

Este trabalho de P&D intitulado “Desenvolvimento de Sistema Especialista para Detecção de Pontos Potenciais de Perdas Comerciais”, ciclo 2004/2005, recebeu apoio financeiro da Manaus Energia.

*Bayesian* e árvore de decisão (*decision tree*). Eles consistem na extração de padrões de consumo em kWh de dados históricos e arranjo dos dados de várias formas, calculando a média anual, mensal, semanal e diária. O objetivo consiste em assegurar resultados ótimos no desenvolvimento de perfis de carga para serem usados como referência na análise de perdas não-técnicas [6].

Pesquisadores portugueses também apresentam um sistema de caracterização de consumidores baseado em um procedimento de descoberta de conhecimento em bancos de dados (*knowledge discovery in databases* - KDD), auxiliado por técnicas de mineração de dados, aplicada em diferentes estágios do processo. O núcleo do sistema consiste em um modelo de mineração de dados através de uma combinação de técnicas de aprendizado supervisionado e não-supervisionado. O sistema é composto de dois módulos principais: o módulo de obtenção de perfil de carga e o módulo de classificação. O módulo de obtenção do perfil do carga cria um conjunto de classes de consumidores usando uma operação de agrupamento e perfis de consumo representativos para cada classe [7].

A obtenção de perfis de carga de consumidores de energia elétrica, conhecida como *knowledge discovery in databases* (KDD) tem como objetivo a construção de perfis de carga e técnicas de mineração de dados para classificar, detectar e prever perdas não-técnicas no setor de distribuição [8]. Além disso, esse conhecimento permite auxiliar na avaliação do comportamento e preferências dos consumidores com o objetivo de extrair vantagens no mercado, cada vez mais competitivo [9].

Pesquisadores gregos descrevem uma metodologia realizada em dois estágios para classificação de consumidores de eletricidade. Ela é baseada em métodos de reconhecimento de padrões, tais como algoritmo *k-means*, *mapa de Kohonen*, *k-means nebuloso* e *agrupamento hierárquico*. No primeiro estágio, curvas de carga horária típicas são estimadas usando métodos de reconhecimento de padrões, e seus resultados são comparados usando seis medidas de verificação de ajuste. No segundo estágio, a classificação dos consumidores é realizada pelos mesmos métodos e medidas, junto com os padrões de carga representativos de consumidores que foram obtidos no primeiro estágio. Os resultados do primeiro estágio podem ser usados para previsão de carga dos consumidores e determinação da forma de tarifação [10].

Pesquisadores coreanos analisaram dados de perfis de consumo, obtidos através de sistemas automáticos de medição, com o objetivo de extrair padrões de demanda de consumidores. Os dados do perfil de carga disponíveis consistem na demanda medida em intervalos de 15 minutos. A partir da análise dos dados das curvas de carga, aplica-se um algoritmo para agrupar padrões similares. Os resultados de classificação então podem ser usados para definir o contrato de demanda e a classificação industrial de cada grupo [11].

### III. AÇÕES DE COMBATE ÀS FRAUDES

O combate à fraude contra o consumo de energia elétrica tem como razão os crescentes casos de subtração de energia elétrica ocorridos em todo o país, e que são tratados pelas

Concessionárias das mais variadas formas, quer com relação à repressão, quer com relação à prevenção.

A sistematização de normas e procedimentos poderá dar às Concessionárias maiores e melhores condições de reduzir, minimizar ou eliminar esse problema, que vem se mostrando de difícil solução, dada a quantidade de maneiras e modos através dos quais vem sendo subtraída ilicitamente a energia.

Em consequência aos procedimentos de fraudes, há uma diminuição no consumo mensal medido pela unidade consumidora, provocando um faturamento inferior ao correto para o cliente. Este problema está presente em todos os tipos de consumidores. Entretanto, os clientes atendidos em alta tensão refletem maiores prejuízos financeiros às concessionárias devido ao seu alto consumo de energia e às tarifas diferenciadas para demanda e consumo [12-13].

Fraudes e suas formas de detecção têm sido objeto de estudos nas mais diversas áreas, englobando desde métodos matemáticos até a utilização de Softwares Inteligentes [14].

Como forma de possibilitar uma integração entre as equipes de desenvolvimento deste estudo, inicialmente foi realizada uma análise sobre as características de fraudes dos consumidores da Manaus Energia e as medidas tomadas pela empresa para impedir ou minimizar os eventos de fraudes no sistema de distribuição de energia.

Esta análise teve por objetivo mapear as características atuais do sistema de gestão da empresa e criar um paralelo com as diversas metodologias de identificação de fraudes existentes atualmente, possibilitando assim, o início do processo de análises experimentais e desenvolvimento da metodologia proposta.

Dessa forma, pode-se constatar que os mecanismos utilizados para verificar fraudes e desvios de energia utilizados pela Manaus Energia consistem em:

- Inspeções periódicas em Unidades Consumidoras (UC's) com medição em alta tensão, sendo que os critérios de seleção da UC a ser inspecionada são: ação massificada em clientes com o mesmo ramo de atividade, alimentadores com maior índice de perdas, clientes que dificultam a entrada de representantes da concessionária para realizar inspeções, inspeções em UC's com reincidência de fraude, inspeção com perícia;
- Inspeções periódicas para consumidores de baixa tensão, onde os critérios são: consumo mínimo, leitura atual menor que a anterior, denúncias, análise de consumo e reincidência; e
- Análise de dados de medições, tais como: consumo medido das UC's, fator de carga, carga instalada, constante de medição, entre outras informações.

Nas inspeções são verificados os lacres, medidas de corrente no primário e secundário, teste de sequência de fase, giro do medidor e teste do medidor com lâmpada de prova. Em seguida são realizadas inspeções em campo com o levantamento de correntes, entre outras informações.

Os tipos mais comuns de fraudes encontradas são: retroação de leitura, bobina de potencial seccionada, by-pass, lacres danificados, medidor quebrado, disco deformado, obje-

to impedindo o giro do disco e expansão dos contatos da chave de aferição.

#### IV. REDES NEURAIS ARTIFICIAIS

Redes Neurais Artificiais (RNA) são técnicas computacionais constituídas por sistemas paralelos distribuídos, compostos por unidades de processamento simples (neurônios) que tem a capacidade de aprender determinadas funções matemáticas. Essas unidades são dispostas em uma ou mais camadas e interligadas por um grande número de conexões, geralmente unidirecionais.

Na maioria dos modelos, essas conexões estão associadas a pesos, os quais armazenam o conhecimento representado no modelo e servem para ponderar a entrada recebida por cada neurônio da rede [15-19].

A possibilidade de aprender através de exemplos e de generalizar a informação aprendida é, sem dúvida, o atrativo principal da solução de problemas através de RNA.

A generalização, que está associada à capacidade de a rede aprender através de um conjunto reduzido de exemplos e posteriormente dar respostas coerentes para dados não conhecidos é uma demonstração de que a capacidade da RNA vai muito além do que simplesmente mapear relações de entrada e saída.

As Redes Neurais Artificiais são capazes de extrair informações não apresentadas de forma explícita através dos exemplos e de atuar como mapeadores universais de funções multivariáveis, com custo computacional que cresce apenas linearmente com o número de variáveis.

A capacidade de auto-organização e processamento temporal são outras características importantes, que, aliada àquelas citadas anteriormente faz das RNA uma ferramenta computacional extremamente poderosa e atrativa para a solução de problemas complexos.

Uma típica rede neural *Feedforward* está descrita na Figura 1, com  $N$  entradas e  $M$  saídas, e cada círculo representando um simples neurônio.

O nome *Feedforward* implica que o fluxo está seguindo um só caminho e não existe um caminho para realimentação entre os neurônios. As saídas de cada neurônio da primeira camada serão uma entrada para cada neurônio da próxima camada.

A camada inicial é denominada de camada de entrada, e a última camada é denominada de camada de saída. Todas as outras camadas entre elas são chamadas de camadas escondidas ou ocultas.

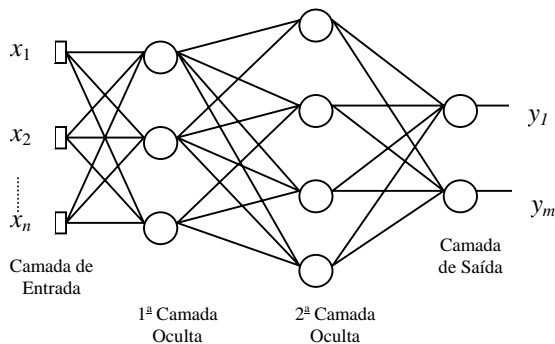


Figura 1 – Exemplo de RNA tipo Feedforward.

O modelo de neurônio proposto é uma simplificação do que se sabia então a respeito do neurônio biológico. Sua descrição matemática resultou em um modelo com  $n$  terminais de entrada  $x_1, x_2, \dots, x_n$  (representando os dendritos) e apenas um terminal de saída  $y$  (representando o axônio). Para emular o comportamento das sinapses, os terminais de entrada do neurônio têm pesos acoplados  $w_1, w_2, \dots, w_n$  cujos valores podem ser positivos ou negativos.

O efeito de uma sinapse particular  $i$  no neurônio pós-sináptico é dado por  $x_i w_i$ . Os pesos determinam em que grau o neurônio deve considerar sinais de disparo que ocorrem naquela conexão.

Um neurônio biológico dispara quando a soma dos impulsos que ele recebe ultrapassa o seu limiar de excitação (threshold). O corpo do neurônio, por sua vez, é emulado por um mecanismo simples que faz a soma dos valores  $x_i w_i$  recebidos pelo neurônio (soma ponderada), chamado de combinador linear e decide se o neurônio deve ou não disparar comparando a soma obtida ao limiar ou *threshold* do neurônio.

Nesse modelo a ativação do neurônio é obtida através da aplicação de uma função de ativação, que ativa ou não a saída, dependendo do valor da soma ponderada das suas entradas. Na descrição do modelo, a função de ativação é dada pela função de limiar descrita em (1).

$$\sum_{i=1}^n x_i w_i \geq \theta \quad (1)$$

onde:

$x_1, x_2, \dots, x_n$  são os sinais de entrada;

$w_1, w_2, \dots, w_n$  são os pesos associado a cada entrada;

$\theta$  é o limiar (threshold) do neurônio;

$\varphi(\cdot)$  é a função de ativa;

$y$  é o sinal de saída do neurônio.

A Figura 2 mostra um esquema de um neurônio artificial.

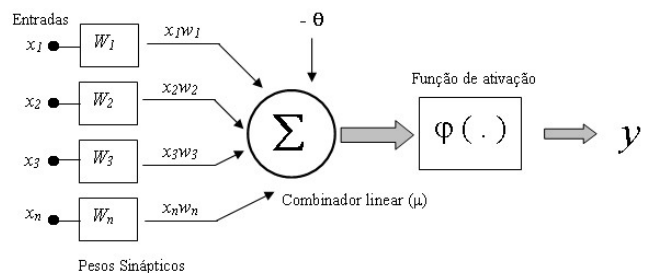


Figura 2 – Esquema de um neurônio artificial.

O neurônio descrito através da Figura 2 pode ser matematicamente interpretado da seguinte maneira:

$$y = \varphi \left( \sum_{i=0}^n w_i x_i \right) \quad (2)$$

ou vetorialmente da seguinte maneira:



Uma descrição dos dados obtidos pela simulação é exibida na Tabela II.

TABELA II – DESCRIÇÃO DOS PRINCIPAIS VALORES OBTIDOS COM A SIMULAÇÃO DA RNA-1

Descrição	Valor
Dados simulados	6
Erros cometidos	1
Acertos	5
Potenciais fraudadores encontrados	0
Potenciais fraudadores reais	1

De acordo com os dados exibidos na Tabela II, pode-se verificar que a RNA-1 obteve uma porcentagem de acerto na ordem de 83,33%. Porém, apesar de apresentar uma baixa taxa de erro a RNA-1 não foi capaz de detectar um fraudador confirmado entre as amostras usadas. Dessa forma, essa topologia não poderá ser utilizada para a indicação de pontos potenciais de perdas comerciais.

Essa incapacidade de indicação de fraudadores pode ter sido ocasionada pelo baixo número de amostras devido ao cálculo da média.

### C. Segunda Rede Neural Utilizada – RNA-2

#### 1) Arquitetura da Segunda Rede Neural Artificial

De acordo com a definição das entradas da RNA-2, foram efetuados diferentes treinamentos e análises para determinar qual a melhor arquitetura para obtenção dos pontos potenciais de perdas comerciais.

Dessa forma, a RNA-2 utilizada para o problema consistiu em quatro variáveis de entrada, uma camada oculta contendo quinze neurônios e uma camada de saída com um neurônio, sendo que em todos os neurônios foram utilizadas as funções de ativação ‘logarítmica sigmoidal’.

Para a saída da RNA-2 foi implementada uma função de quantização de dois níveis, possibilitando-se a obtenção do valor ‘1’ para possível fraudador e do valor ‘0’ para não fraudador. A Figura 4 exibe a topologia utilizada para a RNA-2.

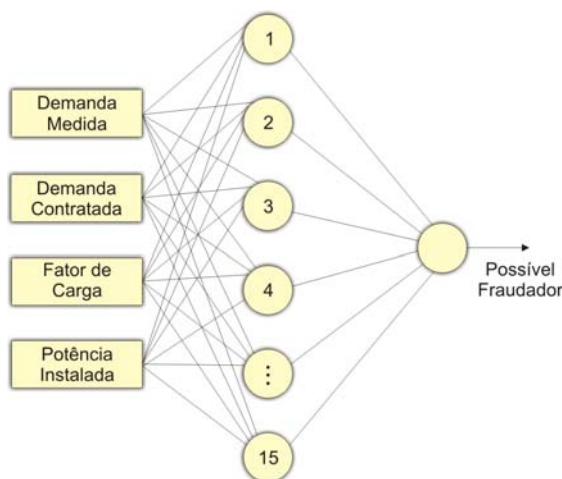


Figura 4 – Arquitetura da RNA2

#### 2) Treinamento e Validação da RNA-2

Para efetuar o treinamento da segunda Rede Neural com a arquitetura proposta na seção anterior, foram utilizados 715 dados (de consumidores fraudadores ou não), contendo como variáveis de entrada a Demanda Medida, Demanda Contratada, Fator de Carga e a Potência Instalada, sendo a variável de saída o valor ‘1’ ou ‘0’ indicando se o consumidor é um potencial fraudador ou não, respectivamente.

Para efetuar-se a validação da RNA-2, utilizou-se um total de 126 dados. Dessa forma foi possível obter, através da simulação em MATLAB®, o percentual de acertos relativos aos dados de validação.

Uma descrição dos dados obtidos pela simulação é exibida na Tabela III.

TABELA III – DESCRIÇÃO DOS PRINCIPAIS VALORES OBTIDOS COM A SIMULAÇÃO DA RNA-2

Descrição	Valor
Dados simulados	126
Erros cometidos	18
Acertos	108
Potenciais fraudadores encontrados	9
Potenciais fraudadores reais	27

De acordo com os dados exibidos na Tabela III, pode-se verificar que a RNA-2 obteve uma porcentagem de acerto na ordem de 85,71%. Isso corresponde a uma média de acertos superior aos outros estudos encontrados na área até o presente momento [20].

Vale ressaltar que a taxa de indicação de potenciais fraudadores apresenta-se em torno de 33,33%. Esse valor é a média de acertos encontrada em outros estudos na área [21].

É importante comentar que não houve nenhuma indicação de consumidores considerados como sendo fraudadores de maneira indevida, ou seja, todos os consumidores que foram indicados eram realmente fraudadores, diferentemente de outros estudos abordados por esta pesquisa, cujas taxas de indicação indevida giraram em torno de 18,5% [22].

## VI. DESENVOLVIMENTO DO SISTEMA ESPECIALISTA: FRAUDINSPECTOR

Um modelo arquitetônico descreve a arquitetura lógica de um sistema, isto é, sua decomposição em múltiplos subsistemas, bem como a comunicação e o acoplamento entre eles.

Atualmente, as mais utilizadas são as arquiteturas multicamadas, nas quais os diversos subsistemas são distribuídos em camadas verticais de acordo com suas responsabilidades.

Dentre as arquiteturas multicamadas, a mais difundida é arquitetura de três camadas, composta pelas camadas de apresentação, lógica da aplicação e de armazenamento de dados.

A qualidade singular dessa arquitetura é a separação da lógica da aplicação em uma camada intermediária de software, subdividida em duas subcamadas, a subcamada de domínio do problema e a subcamada de serviços.

A Figura 5 ilustra essa arquitetura.

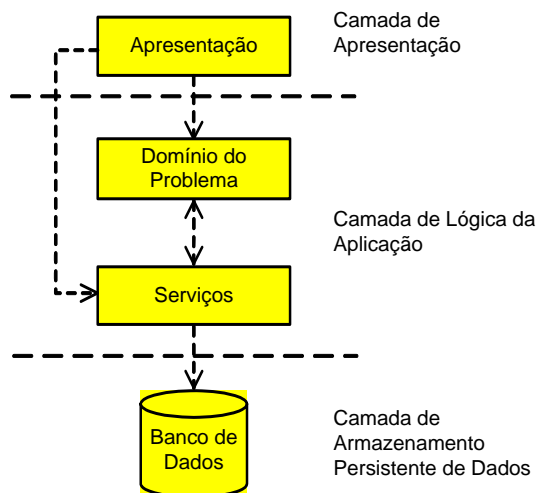


Figura 5 – Arquitetura de três camadas

A camada de *apresentação* é responsável pela interface com o usuário. Portanto, os componentes dessa camada são as janelas que compõem a interface gráfica de usuário. A camada de apresentação é relativamente livre de processamento ligado à aplicação, e as janelas repassam as solicitações de tarefas para a camada intermediária (lógica da aplicação).

A camada de *lógica da aplicação* é responsável pelas regras e tarefas que governam o processo (subcamada de domínio do problema) e pela interface com o banco de dados utilizado e geração de relatórios (subcamada de serviços).

A camada *armazenamento de dados* é responsável pelos mecanismos de armazenamento persistente de dados. Esse armazenamento persistente de dados será realizado por meio de tabelas de dados relacionais armazenadas em um DBMS Oracle, uma vez que a Manaus Energia utiliza esse sistema de gerenciamento de banco de dados, nas versões 9i para o Servidor e 8i para os Clientes.

Como forma de possibilitar a integração das ferramentas inteligentes ao sistema de banco de dados da Manaus Energia, um Sistema Especialista (denominado *FraudInspector*) foi desenvolvido utilizando a plataforma JAVA. A Figura 6 exibe a Janela principal do software.



Figura 6 – Janela principal do FraudInspector

Dessa forma, depois de efetuado o treinamento e validação da Rede Neural Artificial, foram utilizados os pesos e limiares da Rede no Sistema Especialista. Sendo assim, a-

través da análise dos registros do banco de dados fornecido pela Manaus Energia, foi possível verificar o desempenho do software desenvolvido.

#### A. Filtragem dos Registros

As ferramentas inteligentes de análise dos dados para obtenção de pontos potenciais de perdas comerciais foram implementadas com a funcionalidade de possibilitar uma filtragem dos dados. Os campos referentes ao filtro são: Classe, Subclasse, Bairro e Atividade de cada consumidor.

Deve-se mencionar que além do filtro configurável pelo usuário, o *FraudInspector* também restringe suas análises a consumidores cujas atividades estejam relacionadas com o setor de atividade escolhido para o treinamento. A Figura 7 exibe a Janela para filtragem dos registros.

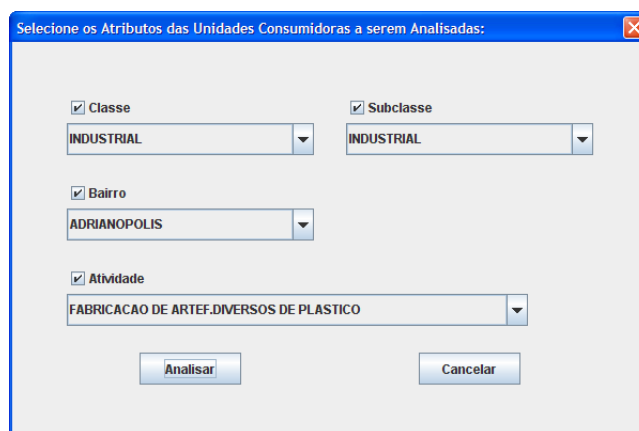


Figura 7 – Janela para filtragem dos registros a serem analisados

#### B. Visualização dos Pontos Potenciais de Perdas

Após a aplicação do filtro definido pelo usuário, o *FraudInspector* inicia sua análise para verificar cada registro do banco de dados, indicando a potencialidade dos registros em serem fraudadores ou não. Como saída, o software exibe uma janela contendo a lista com todos os possíveis fraudadores.

A Figura 8 exibe a Janela com a lista de potenciais fraudadores.

Unidade	Cliente	Endereço	Bairro	Classe	Subclasse	Situação	Tipo Ligação	Atividade
1				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
2				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
3				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE EM
4				INDUSTRIAL	INDUSTRIAL	DESL	ALTA TENSÃO	FABRICACAO DE AR
5				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
6				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
7				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	INDUSTRIA DE PRO
8				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	INDUSTRIA DE PRO
9				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE EM
10				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
11				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
12				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
13				INDUSTRIAL	INDUSTRIAL	CORT	ALTA TENSÃO	FABRICACAO DE PLA
14				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
15				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
16				INDUSTRIAL	INDUSTRIAL	DESL	ALTA TENSÃO	FABRICACAO DE AR
17				INDUSTRIAL	INDUSTRIAL	DESL	ALTA TENSÃO	FABRICACAO DE AR
18				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
19				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
20				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
21				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE EM
22				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE EM
23				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
24				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE EM
25				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
26				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE RE
27				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	FABRICACAO DE AR
28				INDUSTRIAL	INDUSTRIAL	NORM	ALTA TENSÃO	INDUSTRIA DE PRO

Figura 8 – Janela com a lista de possíveis fraudadores fornecido pelo *FraudInspector*

## VII. CONCLUSÕES

Este estudo teve por objetivo, o desenvolvimento de uma nova ferramenta para a identificação dos problemas relacionados às fraudes no sistema de distribuição de energia elétrica. Dessa forma, pode-se através do estudo das características dos eventos de fraudes, identificar onde o problema de fraude se acentuava, definindo-se uma diretriz para o desenvolvimento das ferramentas inteligentes.

Uma abordagem neural foi utilizada para a identificação, classificação e indicação de potenciais fraudadores, através da utilização dos registros de consumo do banco de dados da Manaus Energia.

Para avaliar a sensibilidade da abordagem escolhida, foram implementadas duas arquiteturas distintas (RNA-1 e RNA-2), sendo que na primeira utilizaram-se os dados referentes às médias anuais e na segunda os dados referentes aos registros mensais. Além disso, optou-se por utilizar um conjunto de variáveis diferentes para cada arquitetura.

Durante o processo de validação, verificou-se que RNA-1 obteve uma ótima porcentagem de acertos, porém ela foi incapaz de indicar os possíveis fraudadores, inviabilizando sua implementação. Para a RNA-2, a taxa de acerto também estava em um patamar alto, com a indicação de possíveis fraudadores. Convém salientar que essa segunda Rede não indicou potenciais fraudadores indevidamente.

Dessa forma, após a validação da segunda Rede, foi possível o desenvolvimento de um Sistema Especialista que utiliza os pesos e limiares da RNA-2 para através de uma varredura no sistema de banco de dados da Manaus Energia efetuar a indicação de potenciais fraudadores.

A partir dos resultados apresentados até o momento ficou evidenciado que esta nova tecnologia poderá ser aplicada diretamente nos processos internos da Manaus Energia com os seguintes impactos esperados:

- a) Aperfeiçoamento e emprego de ferramentas eficientes e técnicas alternativas para identificar com precisão clientes fraudadores de energia elétrica da Manaus Energia.
- b) Identificação precisa do relacionamento existente entre variáveis que possam indicar tipos de fraudes no sistema.
- c) Utilização de metodologias e abordagens eficientes que auxiliem na determinação exata do local da fraude.
- d) Disponibilidade de subsídios que permitam a adoção de práticas seguras e rápidas para restaurar o circuito fraudado (adulterado).
- e) Adoção de técnicas e estudos diferenciados que sejam direcionados para resolver os problemas associados com a identificação de fraudes, atentando, sobretudo, para as particularidades operacionais da Manaus Energia.
- f) Estabelecimento de diretrizes bem consolidadas no sentido de diminuir os prejuízos financeiros da empresa em relação às fraudes.
- g) Fixação de procedimentos para corrigir eventuais deficiências no rastreamento de sistemas fraudados da Manaus Energia.
- h) Desenvolvimento e delineamento de estratégias financeiras para novos investimentos advindos dos ganhos efetivos quantizados nesta pesquisa em relação às perdas de receita nos erros de faturamento e custos operacionais provocados pelas fraudes de energia.

Através deste estudo intitulado “Desenvolvimento de Sistema Especialista para Detecção de Pontos Potenciais de

Perdas Comerciais” várias técnicas e metodologias para identificação de consumidores fraudulentos puderam ser estudadas para a elaboração da diretriz metodológica do projeto, conforme apresentado na Seção II, sendo que para o produto final foram utilizadas as Redes Neurais Artificiais.

Contudo, este estudo de novas metodologias trouxe para a equipe de desenvolvimento do LsisPoTi – UNESP e da Manaus Energia um novo conhecimento que possibilitará a implementação computacional e o desenvolvimento de técnicas derivadas da junção entre as metodologias utilizadas atualmente.

Sendo assim, a finalização deste projeto instiga para que as atividades de combate a fraudes continuem, o que possibilitará o aprimoramento das técnicas desenvolvidas, bem como no refinamento dos dados para outras atividades de consumo. Isto demonstra a abrangência e a aderência deste projeto de pesquisa, ponto fundamental para o seu sucesso.

Deve-se salientar que a Rede Neural concebida nesta pesquisa foi treinada para um tipo de segmento específico da classe industrial. Para outros ramos de atividades se faz necessário novos treinamentos.

## VIII. REFERÊNCIAS BIBLIOGRÁFICAS

- [1] N. A. Eller. “Arquitetura de Informação para o Gerenciamento de Perdas Comerciais de Energia Elétrica”. Dissertação de Doutorado, Universidade Federal de Santa Catarina, Florianópolis SC, Jan, 2003.
- [2] A. A. F. Rocha, et al. “Recuperação de Perdas Comerciais de Energia Elétrica Ativa”. Seminário Nacional de Distribuição de Energia Elétrica, São Paulo, 1997, CD.
- [3] E. S. Ferreira. “Padronização de Padrões de Entrada Econômicos”. SENDI - XVII Seminário Nacional de Distribuição de Energia Elétrica, Vol. CD-ROM, 2006.
- [4] J. L. Neto, et al. “Projeto e Desenvolvimento de Conjunto de Medição Fiscal para Mapeamento e Redução de Perdas”. XVII Seminário Nacional de Distribuição de Energia Elétrica, Belo Horizonte, MG, 2006.
- [5] M. E. de Oliveira, A. P. Feltrin, F. J. Candian. “Investigation of the Relationship between Load and Loss Factors for a Brazilian Electric Utility”. TDC '06. IEEE/PES Transmission & Distribution Conference and Exposition: Latin America, 2006, 1-6, Aug., 2006.
- [6] A. H. Nizar, Z. Y. Dong, J. H. Zhao, P. Zhang. “A Data Mining Based NTL Analysis Method”. Power Engineering Society General Meeting, 2007. IEEE, 1-8, June, 2007.
- [7] V. Figueiredo, F. Rodrigues, Z. Vale, J. B. Gouveia “An Electric Energy Consumer Characterization Framework Based on Data Mining Techniques”. IEEE TRANSACTIONS ON POWER SYSTEMS, vol. 20, no. 2, 596-602, May, 2005.
- [8] A.H. Nizar, Z.Y. Dong, J.H. Zhao. “Load Profiling and Data Mining Techniques in Electricity Deregulated Market”. IEEE Power Engineering Society General Meeting., June, 2006.
- [9] A.H.Nizar, Z. Y. Dong, M. Jalaluddin, M.J. Raffles. “Load Profiling Method in Detecting non-Technical Loss Activities in a Power Utility”. Power and Energy Conference, 2006. PECon '06. IEEE International, 82 - 87, Nov., 2006.
- [10] G. J. Tsekouras, N. D. Hatziaargyriou, E. N. Dialynas. “Two-Stage Pattern Recognition of Load Curves for Classification of Electricity Customers”. Power Systems, IEEE Transactions on, vol. 22, no. 3, 1120 - 1128, Aug., 2007.
- [11] I. H. Yu, J. K. Lee, J. M. Ko, S. I. Kim. “A method for classification of electricity demands using load profile data”. Fourth Annual ACIS International Conference on Computer and Information Science, 2005., 164-168, 2005.
- [12] B. Regueira, N. P. F. Souza, F. C. Ferreira. “Experiências e Ações no Combate a Perdas Comerciais com Resultados na Otimização de Perdas Técnicas. XVII Seminário Nacional de Distribuição de Energia Elétrica, Belo Horizonte, MG, 2006.
- [13] J. Reis Filho, et al. “Fraud Identification in Electricity Company Customers Using Decision Tree”. IEEE International Conference on Systems, Man and Cybernetics, v.4, p.3730 – 3734, 1994.

- [14] N. Shan., W. Ziarko, H. J. Hamilton and N. Cercone. "Using Rough Sets as Tool for Knowledge Discovery". International Conference on Knowledge Discovery and Data Mining, p. 263-268, 1995.
- [15] S. Haykin. "Neural Networks – A Comprehensive Foundation", New York: MacMillan, 1994.
- [16] C. Bishop. "Neural Networks for Pattern Recognition", Oxford University Press, 1995.
- [17] Z. L. Kovács Z. L. "Redes Neurais Artificiais – Fundamentos e Aplicações", 2ª Ed., São Paulo, 1996.
- [18] D. S. Levine. "Introduction to Neural & Cognitive Modeling". New Jersey: Lawrence Erlbaum Associates, Inc., 1990.
- [19] F. Luo. "Applied Neural Networks for Signal Processing Cambridge": Cambridge University Press, 1998.
- [20] C. M. M. M. Patrício. "Detecção de Fraude e Erro de Medição em Grandes Consumidores de Energia Elétrica Utilizando Rough Sets Baseados em Dados Históricos e Dados em Tempo Real". Dissertação de Mestrado, 2005.
- [21] J. E. Cabral, E. M. Gontijo, J. O. P. Pinto, J. Reis Filho. "Fraud Detection in Electrical Energy Consumers Using Rough Sets". IEEE International Conference on Systems, Man and Cybernetics, v.4, p 3625 – 3629, 2004.
- [22] C. Larman. "Applying UML and Patterns – An Introduction to Object-Oriented Analysis and Design". 2 ed. Upper Saddle River: Prentice Hall, 2001.