Detecção de Fraude e Prevenção Utilizando Inteligência Artificial

André Sandri

Ciência da Computação – Centro Universitário La Salle (UNILASALLE)
Av. Victor Barreto, 2288– 92.010-000 – Canoas – RS – Brazil

andresandri@hotmail.com

Abstract. *This article presents a research about fraud detection and prevention using artificial intelligence.*

Resumo. *Este artigo apresenta uma pesquisa sobre detecção de fraude e prevenção utilizando inteligência artificial.*

1.

2. 1. Introdução

3. **Este artigo apresenta um estudo sobre a utilização de inteligência artificial para detectar e prevenir tentativas de fraudes. Para isso, foram pesquisadas as principais áreas de negócio das qual a inteligência artificial é utilizada para a detecção e prevenção de fraudes.**
4. **Neste documento são citadas também as técnicas de inteligência artificial utilizadas nestas áreas de negócio, incluindo uma breve introdução para exemplificar a técnica utilizada.**

No capítulo 3 são citadas as principais empresas que atuam nesta área, com citações dos seus principais produtos voltados a detecção de fraudes, e no último capítulo é apresentada uma breve conclusão a respeito das principais técnicas empregadas pelas áreas de negócios pesquisadas.

5. 2. Detecção e Prevenção de Fraudes

Se, logo após de você utilizar seu cartão bancário, o banco telefonar para você confirmando a transação, isso é por que cada vez mais estas instituições estão utilizando a inteligência artificial para detectar fraudes.

Conforme PRESSLER, fraudes em cartões de crédito custam para a indústria cerca de um bilhão de dólares por ano, ou sete centavos de cada 100 dólares gastos no cartão de plástico. Mas isto está diminuindo significativamente desde a década passada devido à tecnologia que consegue identificar padrões incomuns de gastos. (PRESSLER, 2002)

As transações com cartão de crédito através da Internet são consideradas pelos bancos e administradoras como CNP - Cartão Não Presente (COELHO, RAITTZ, TREZUB, 2006). Como não há a assinatura do comprador para validar a compra neste tipo de transação, a responsabilidade pela transação é do lojista e não do banco emissor ou da administradora do cartão. As fraudes com cartão de crédito podem ocasionar prejuízos para o comerciante bem como podem levar ao cancelamento do convênio do estabelecimento com as administradoras de cartão.

Estes prejuízos, por ocasião de fraudes, não são limitados apenas a bancos e administradoras de cartões de crédito. Conforme GRAHAM-ROWE, mais de 15.000 telefones portáteis são roubados a cada mês na Inglaterra. De acordo com a empresa sueca *Ericsson*, fabricante de telefones celulares, o uso fraudulento de celulares roubados significa uma perda entre dois a cinco por cento das receitas das operadoras. (GRAHAM-ROWE, 2001)

Os custos com fraudes para um estabelecimento incluem (COELHO, RAITTZ, TREZUB, 2006):

- Perda de mercadorias;
- Perda com taxas bancárias, frete e embalagem;
- Risco de cancelamento do contrato com as administradoras dos cartões;
- Taxa de desconto maior no contrato com as administradoras;
- Perda de faturamento pela rejeição de pedidos;
- Custo elevado de uma equipe de análise de risco;
- Perda de confiança do cliente;
- Perda do cliente por insatisfação (demora e incômodo).

Fraudes em cartões de crédito diminuíram na Inglaterra pela primeira vez após uma década, isso no ano de 2004, de acordo com uma pesquisa da APACS - *Association of Payment Clearing Services* (YOUNG, 2004). A queda deve-se ao crescente uso de redes neurais que têm a habilidade de detectar comportamentos fraudulentos através da análise das transações seguidas de um alerta da atividade suspeita para uma equipe em prontidão.

As técnicas mais utilizadas para a detecção de fraude que utilizam técnicas de inteligência artificial em grandes volumes de dados são:

- *Data Warehouse* e *Data Mining*: são técnicas avançadas de análise de dados através de técnicas e métodos estatísticos, onde algumas destas técnicas podem utilizar algoritmos de inteligência artificial, utilizando refinamentos sucessivos a partir de dados de alto nível descendo a níveis de detalhes cada vez maiores para uma análise interativa. Através destas técnicas podem-se descobrir novos padrões de fraude e tipos e fraudes existentes ainda desconhecidas.
- Pontuação através de Redes Neurais: para cada novo caso de fraude, o sistema calcula um valor de pontuação conforme sua similaridade com um padrão conhecido. Atualmente é a técnica mais utilizada, pois oferece melhores resultados.

Muitas aplicações comerciais consideradas críticas estão começando a avaliar a utilização de inteligência artificial para imitar as habilidades humanas, visando presumir qual atividade é normal e qual não é.

Para a detecção de fraude em âmbito financeiro é utilizada freqüentemente a técnica de inteligência artificial chamada de pontuação através de redes neurais, que é uma tecnologia que imita o funcionamento de um cérebro humano de forma que computadores possam aprender e tomar decisões de forma semelhante á dos humanos. Redes neurais utilizam um conjunto de elementos de processamento, ou nodos, que são modelados conforme neurônios do cérebro. Estas redes podem então aprender a partir da experiência, forma semelhante utilizada pelos seres humanos.

Conforme BIGELOW, as técnicas de redes neurais começam a partir da análise em um banco de dados, utilizando métodos sistemáticos para identificar características, tendências e padrões dos dados (BIGELOW, 2002). Estas características podem ser utilizadas para analisar dados atuais e adivinhar se a transação é legítima ou não.

Conforme exemplificado por BIGELOW, nos casos de fraude em cartões de créditos, por exemplo, um cartão de crédito roubado é normalmente utilizado em uma compra de valor pequeno em um posto de combustível logo após seu roubo ou furto para determinar se o cartão está ainda ativo. Em seguida, é utilizado na tentativa de compra de joalheria ou outro produto com valor maior. Estes padrões de transações ilícitas são automaticamente detectados nestes sistemas caso a rede neural for treinada para reconhecer estes tipos de situações.

Conforme (ANDREATTO, 1999), a função básica de cada neurônio é:

1. Avaliar todos os valores de entrada;
2. Calcular o total combinado dos valores de entrada;
3. Comparar o valor total com um valor limiar;
4. Determinar qual será a saída do neurônio.

Cada neurônio participa de uma rede formada para o cálculo progressivo do valor final da pontuação referente à probabilidade de fraude conforme os valores (pesos) de cada neurônio. Os valores de pesos de cada neurônio são determinados a partir de treinamentos iterativos da rede neural. Na ilustração abaixo é apresentado um exemplo da hierarquia de uma rede neural.

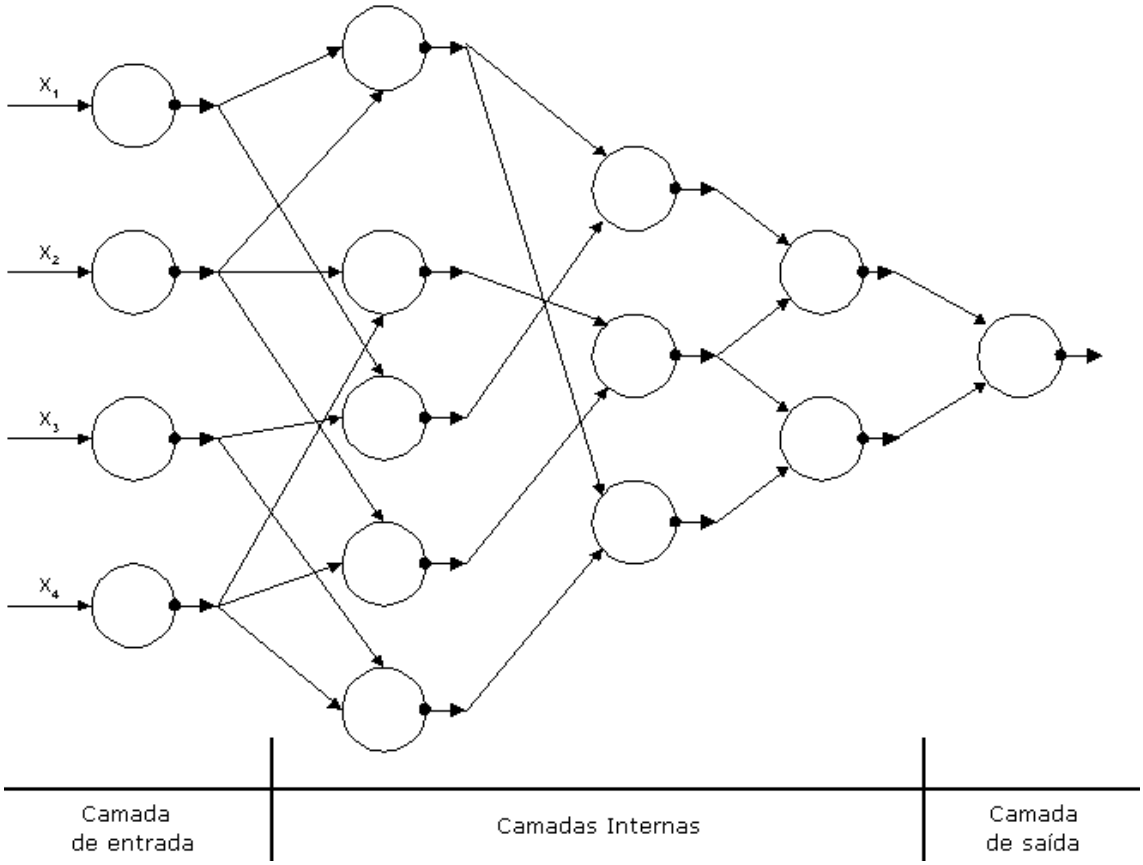

Ilustração – Estrutura de exemplo da hierarquia de uma rede neural
Fonte: Criação própria.

Softwares que utilizam redes neurais são integrados com os sistemas bancários de gerência de cartão e sistemas de autorização. Estes tipos de softwares consistem em uma gama de programas que reconhecem padrões a partir do comportamento do portador do cartão, o qual é fruto de uma longa história em trabalhos de reconhecimento de padrões utilizando computadores. O sistema monitora o comportamento do portador do cartão procurando por volumes transacionais, quantias e localidades incomuns, conforme os hábitos do titular. Monitora também os tipos de comerciantes que são utilizados e padrões que não combinam com o histórico de utilização do cartão.

O sistema contabiliza pontos para cada transação, dando valores maiores para aqueles em que ele suspeita que sejam fraudulentos. O sistema pode monitorar os resultados em tempo real ou analisar os históricos periodicamente para reforçar as próximas detecções da rede neural.

Normalmente, não é o sistema que impede que uma transação suspeita seja bloqueada. Quem efetua a confirmação ou o bloqueio de uma transação é a equipe de prevenção de fraudes que fica em prontidão para a tomada da decisão final. Este time recebe o alerta do sistema e na mesma hora, com o apoio de um sistema de decisão, aplica as regras e políticas da instituição para reagir ou não à atividade fraudulenta suspeita. Se a preocupação com a atividade do cliente é considerada importante pela empresa, neste momento eles podem tentar ligar ao portador do cartão para verificar a

legitimidade da transação. Se esta suspeita for muito grave, podem até interromper a transação sem o consentimento do cliente.

Instituições financeiras compram ou alugam estes tipos de softwares de empresas especializadas que operam globalmente, oferecendo a habilidade de compararem dados e analisar padrões de fraudes em diversos países.

O custo de utilizar um software destes para reduzir o nível de fraudes é sempre uma combinação entre o custo de instalação e de execução do sistema e a quantidade de fraudes que estiverem acontecendo, além das perdas contabilizadas.

Os programadores de redes neurais estão atualmente competindo para criar sistemas mais rápidos, que aprendam mais rápidos, que sejam mais fáceis de entender e de utilizar, e sejam mais integráveis em outros sistemas de decisão. A comunidade de inteligência artificial está constantemente trazendo novas soluções, incluindo sistemas híbridos que organizam e analisam diversos padrões de transações.

Os sistemas de inteligência artificial estão sendo previstos para também avaliar transações on-line (de sites da Internet) e via telefone. Atualmente existe um esforço em substituir os cartões plásticos por cartões com chip, chamados de *smarts cards*. Estes cartões têm como principal característica sua impossibilidade de realizar clones dos cartões, além de possibilitar, dentro do chip, um mecanismo utilizado para validar a senha digitada pelo usuário sem comprometer a leitura desta senha por algum dispositivo de leitura, pois a senha não é armazenada no chip - ela é validada através de criptografia moderna, com a utilização de certificados. A utilização *de smarts cards* não evitará fraudes, mas diminuirá sua utilização fraudulenta por pessoas que não sejam os reais portadores do cartão.

Sistemas de detecção de fraudes podem ser aplicados em outras áreas, como, por exemplo, em redes de telecomunicações, sistemas de redes elétricas, sistemas de alarmes e sistemas de aviação.

Espera-se que, em um futuro próximo, as redes neurais possam ser substituídas ou complementadas por sistemas que imitam outros padrões biológicos. Novas pesquisas sobre imunidade computacional utilizam o conceito de fraude de forma semelhante ao um ataque em um organismo saudável. AIS - *Artificial Immune Systems* são algoritmos inspirados nos princípios e processos do sistema de imunidade dos vertebrados. Estes algoritmos tipicamente simulam as características de aprendizagem e memorização dos sistemas de imunidade para resolver um dado problema. AIS são muito parecidos com algoritmos genéticos.

Na Inglaterra estão lançando um novo sistema de detecção de fraudes em cartão, chamado de *iHex* (FINEXTRA, 2004), baseado em novas tecnologias de inteligência artificial desenvolvidas na Universidade de Computação de Oxford, nos laboratórios de biometria. O produto está sendo desenvolvido para ser utilizado em empresas prestadoras de serviços financeiros, agências governamentais e corporações. Este sistema detecta fraudes utilizando técnicas ILP - *Inductive Logic Programming*, que é uma nova técnica da inteligência artificial utilizada para a identificação de padrões de fraudes e anomalias. O fornecedor desta tecnologia diz que a principal diferença desta técnica, comparado com outras técnicas, é que esta técnica automaticamente gera e aperfeiçoa suas próprias regras de detecção.

Entre os maiores desafios existentes em um sistema com o objetivo de detectar fraude podemos citar:

- Deve-se tentar detectar uma fraude que pode acontecer entre cerca de 50.000 transações, por exemplo;
- Os fraudadores rapidamente modificam seus comportamentos assim que um padrão de atividade é descoberto. Nestes casos, ou utilizam outras técnicas, ou até acabam migrando seus ataques para outras instituições;
- Uma rede neural precisa de dados históricos recentes de pelo menos seis meses de atividades transacionais para permitir sua aprendizagem de padrões de fraudes;
- O grande problema com a detecção de fraudes em cartões de créditos é que se deve tomar uma decisão em milisegundos, ou realizar a análise logo após o evento da utilização do cartão.

No próximo capítulo serão apresentadas algumas das principais empresas que atuam nesta área, com seus principais produtos voltados para a área de detecção de fraudes.

6. 3. Principais Empresas e Produtos

Nesta seção estão relacionadas as principais empresas e seus principais produtos voltados à detecção de fraudes utilizando inteligência artificial.

3.1. *Fair Isaac Corporation*

Fair Isaac Corporation (FAIRISAAC, 2006) é uma empresa americana líder em gerência de decisão dirigida por análise estatística avançada. Esta empresa utiliza diversas tecnologias, entre elas inteligência artificial, para calcular níveis de confiabilidade de crédito para pessoas físicas e jurídicas, para avaliar transações de crédito, entre outras. É comum encontrar neste país muitas empresas que trabalham com concessão de crédito utilizando a pontuação FICO - *Fair Isaac Credit Score*, para avaliar a capacidade financeira de um cliente.

Esta empresa oferece dez soluções para a gerência de fraudes, das quais podemos destacar:

- *Fraud Predictor with Merchant Profiles*: é um produto que utiliza uma tecnologia de detecção de fraudes em pagamentos com o uso de cartão, a qual calcula uma pontuação para avaliar a possibilidade de fraude baseada tanto no histórico do portador do cartão quanto no histórico da empresa que realiza a operação.

- *Falcon Fraud Manager*: é um produto utilizado para proteger mais de 450 milhões de cartões de crédito e de débito. O diferencial deste produto é que esta tecnologia recebe avanços tecnológicos regularmente, permitindo assim detectar

novos tipos de fraudes. Processa em torno de 65% das transações de cartão do mundo utilizando uma rede neural, entre outras tecnologias proprietárias.

- *Falcon One*: é um produto direcionado para utilização centralizada dentro de uma empresa, permitindo assim interligá-lo com sistemas empresariais para a detecção de fraudes. É um sistema configurável de detecção e gerência, com capacidades analíticas para prepará-lo para situações específicas de fraudes, compartilhando dados e serviços para prover máxima proteção em cada canal ou linha de negócio.

Os softwares desta empresa estão sendo também utilizados para combater fraudes ao solicitar indenizações médicas, ao solicitar medicamentos prescritos, ou durante a compra de um automóvel, por exemplo.

3.2. *NeuroTech*

A empresa paulista *NeuroTech* (NEUROTECH, 2006) utiliza tecnologias de inteligência artificial e de mineração de dados para sistematizar a identificação de fraudes, entre outros objetivos, visando a minimização de riscos. Entre os dez principais produtos oferecidos por esta empresa, podemos destacar:

- FRAUDDETECTOR: produto que alerta seus usuários sobre a possibilidade de ocorrência de fraude, seja caracterizada por uma situação de fraude cadastral ou fraude transacional (comportamental). A solução gera a pontuação de risco, a estimativa de ganho ou perda com a operação e escalona prioridades na investigação das possíveis fraudes em função do custo da investigação e da perda causada pelo evento fraudulento. Os resultados são a redução de prejuízos causados por fraudes e o maior controle sobre as operações.

- NEURALINSPECTOR: produto que busca por ocorrências que fogem ao padrão comum do perfil da operação, possibilitando a prevenção ou correção de situações indesejadas na instituição, redução de prejuízos decorrentes do mau uso da legislação corrente, de inconsistências nas informações, ou mesmo de condutas fraudulentas. Alguns exemplos de aplicação são: auditoria em lavagem de dinheiro, em folhas de pagamento, no pagamento a fornecedores, compras e orçamentos e na aderência a normas e políticas.

- NEURALBEHAVIOR: produto voltado para a avaliação de risco de crédito de antigos e novos clientes, com sugestão de limites e acompanhamento do comportamento do cliente. A solução oferece um sistema para análise do perfil da operação quanto ao seu risco e capacidade de pagamento, sendo capaz de analisar um grande número de informações complexas do cliente, entre variáveis cadastrais e comportamentais (transacionais).

Só nesse primeiro semestre, esta empresa fechou dois novos contratos no segmento bancário: Banco Semear, pertencente ao grupo minério *Secculus*; e com o Tribanco, do Grupo Martins. (BAGUETE, 2006)

4. Conclusão

Neste documento foram apresentadas as principais áreas de negócio das quais a inteligência artificial é utilizada para a detecção e prevenção de fraudes, as quais são freqüentemente áreas financeiras, onde os principais clientes são as operadoras de cartões de crédito e as instituições bancárias.

As principais técnicas de inteligência artificial utilizadas nestas áreas de negócio são as redes neurais, e, para um futuro próximo, espera-se que seja também utilizadas as técnicas chamadas de ILP - *Inductive Logic Programming* e AIS - *Artificial Immune Systems*.

Referências

American Association for Artificial Intelligence. **Fraud Detection & Prevention**. Disponível em <http://www.aaai.org/aitopics/html/>. Acesso em 26 jun 2006.

PRESSLER, M. **Credit Card Companies Turn To Artificial Intelligence**. The Washington Post. Tampa Tribune, 29 set. 2002.

GRAHAM-ROWE, D. **Phone Friend**. New Scientist Magazine, 31 jan. 2001. Disponível em <http://www.newscientist.com/article.ns?id=dn370>. Acesso em 26 jun 2006.

YOUNG, K. **Mimicking fraudsters**. The Guardian, 9 set. 2004. Disponível em <http://technology.guardian.co.uk/online/story/0,3605,1299691,00.html>. Acesso em 26 jun 2006.

O Baguete. **Ciab 2006: Neurotech traz soluções para gestão de risco**. 12 jun. 2006. Disponível em <http://www.baguete.com.br/noticia.php?id=10832>. Acesso em 26 jun 2006.

Fair Isaac Corporation. **Fraud Management Solutions**. 2006. Disponível em <http://www.fairisaac.com/Fairisaac/Solutions/Solutions+by+Function/Fraud+Management/>. Acesso em 26 jun 2006.

NeuroTech. **Soluções NeuroTech para o Mercado Financeiro**. 2006. Disponível em <http://www.neurotech.com.br/solucoes-mf.html>. Acesso em 26 jun 2006.

Finextra Research. **Future Route releases AI-based fraud detection product**. 19 ago. 2004. Disponível em <http://www.finextra.com/fullstory.asp?id=12365>. Acesso em 26 jun 2006.

BIGELOW, B. **Computers try to outthink terrorists**. The San Diego Union-Tribune, 13 jan. 2002. Disponível em <http://www.signonsandiego.com/news/>. Acesso em 26 jun 2006.

COELHO, L., RAITTZ. R., TREZUB, M. **FControl: sistema inteligente inovador para detecção de fraudes em operações de comércio eletrônico**. Universidade Federal de São Carlos, Abril 2006.

ANDREATTO, R. **Construindo Um Data Warehouse e Analisando Suas Informações Com Data Mining e OLAP**. Monografia de Conclusão de Curso de

Ciências da Computação, Faculdade de Ciências Administrativas Valinhos. 1999. Disponível em <http://www.datawarehouses.hpg.ig.com.br/>. Acesso em 26 jun 2006.