Protótipo baseado em regras de produção e aprendizado de máquina para descoberta de fraudes em seguros de saúde

José Wander Nunes

jose_wander_nunes@hotmail.com

Resumo

Os algoritmos de aprendizado de máquina podem ser usados para detectar fraudes em conjuntos de dados de sinistros seguros de saúde. Esses algoritmos pressupõem que o padrão de fraude no futuro será o mesmo que no passado o que resulta em uma limitação devido a sua dependência de conhecimento prévio confiável. Na indústria de seguros, a maioria das operadoras não possui recursos suficientes para examinar todas as transações então essa presunção pode ser impraticável. Um dos caminhos para se proceder nesses casos é a composição de técnicas de inteligência artificial. Este trabalho teve por objetivo introduzir um sistema baseado em regras e aprendizado de máquina para descoberta de fraudes em seguros de saúde. O modelo proposto respondeu com relativa eficácia ao problema apresentado.

1. Introdução

A fraude é um problema que ocorre em muitos setores, causando prejuízos financeiros e morais às organizações. Nos seguros de saúde isso ocorre principalmente por apresentações falsas ou indevidas. Para o período de 2015 estima-se uma perda de mais de 12 bilhões de reais no caso das contas hospitalares e de mais de 10 bilhões de reais no caso dos exames laboratoriais (LARA, 2017).

Dentre as fraudes de mais difícil detecção nos seguros de saúde, há a do parcelamento de recibos de reembolso que ocorre quando mais de um recibo ou nota fiscal são emitidos pelo prestador, com valores menores e dentro do valor reembolsável e com datas diferentes.

Para Kirlidog e Asuk (2012), as técnicas de mineração de dados podem ser usadas para detectar fraudes em grandes conjuntos de dados de seguros, o que incluem por exemplo os algoritmos para aprendizado de máquina supervisionados. Kim e Vasarhelyi (2012) verificaram que a adoção de tais algoritmos pode ser impraticável no caso das seguradoras, já que os dados para treinamento podem estar incorretos porque a maioria das companhias não possui recursos suficientes para examinar todas as transações.

Entre as soluções apresentadas, há a de composição de técnicas de inteligência artificial, notadamente a combinação de conhecimento na forma de regras com algoritmos de aprendizado de máquina como investigada por Pandey, Saroliya e Kumar (2017) e também por Shin, Hyunjung et al. (2012).

Embora tal combinação possa ser considerada como o estado da arte na área, pouco ou nenhum estudo foi publicado para a realidade do mercado de seguros brasileiro.

Dado o cenário, criou-se a proposição de um sistema de detecção de fraudes baseado em duas etapas, cada qual empregando uma técnica de inteligência artificial. A

primeira utiliza um sistema especialista baseado em regras e a segunda emprega algoritmos de aprendizado de máquina. A hipótese é de que os índices de fraudes apontados pelo sistema especialista possam aumentar a acurácia dos resultados obtidos pelo algoritmo baseado em aprendizado de máquina

Somente o caso de parcelamento de recibos foi explorado por ter complexidade suficiente para provar o conceito e representatividade dentro do problema das fraudes. A base de regras foi construída com auxílio de especialistas brasileiros do setor.

2. Construção do protótipo

A linguagem de programação selecionada para a etapa do sistema especialista foi a Java, versão 7. A API para sistemas especialistas foi a do Drools, versão 6.2.0.

A ferramenta para execução de algoritmos de aprendizado de máquina escolhida foi o WEKA, versão 3.8.2. Os métodos selecionados para o trabalho foram o SVM, Árvores de Decisão, kNN e *Naïve* Bayes.

3. Execução do protótipo

O processamento se deu pelas seguintes etapas:

a) Enriquecimento de dados: para essa etapa foi utilizada uma massa de dados com sinistros - dentre os quais casos apontados como sendo de parcelamento de recibos - disponibilizada no formato CSV (arquivo 1). O sistema baseado em regras foi executado tendo como entrada o arquivo 1. Por meio das ativações das regras, o sistema gerou para cada sinistro os valores para os atributos faixaProbalidadeFraude, parcelamentoRecibo e *score*. Esses atributos adquiriram os seguintes valores:
   - faixaProbalidadeFraude: BAIXA (valor *default*), MÉDIA, ALTA;
   - parcelamentoRecibo: FALSO (valor *default*), VERDADEIRO;
   - *score*: valores entre 0 (default) e 10 (máximo alcançado).

   O sistema gravou um segundo arquivo (arquivo 2) no formato CSV com a massa de dados de treinamento e os três novos atributos.
b) Execução dos algoritmos de aprendizado de máquina com o arquivo com reforço;
c) Execução dos algoritmos de aprendizado de máquina com o arquivo sem reforço.

A tabela 1 mostra os resultados e as taxas de sensibilidade, especificidade e Curva ROC calculadas para cada uma das execuções:

Tabela 1 – Resultados e taxas de sensibilidade, especificidade e Curva ROC calculadas para cada uma das execuções

Método	Reforço	Sensibilidade	Especificidade	Curva ROC
Naïve Baiyes	Não	1,00000	0,4245	0,9970
	Sim	1,00000	0,6132	0,9980
SVM	Não	1,00000	1,0000	1,0000
	Sim	1,00000	0,9868	1,0000

Método	Reforço	Sensibilidade	Especificidade	Curva ROC
kNN	Não	1,00000	0,9933	1,0000
	Sim	1,00000	1,0000	1,0000
Árvore de Decisão	Não	0,99996	0,9737	0,9970
	Sim	1,00000	0,9868	1,0000

Fonte: Autor

Notas:

A coluna “Reforço” informa se a execução foi com o arquivo 1 (dados sem reforço do sistema especialista, leia-se ”Não”) ou com o arquivo 2 (dados com reforço do sistema especialista, leia-se ”Sim”).

4. Análise

Avaliando-se as Curvas ROC, verifica-se na Tabela 1 que para o *Naïve* Baiyes e a Árvore de Decisão houve um aumento de 0,9970 para 0,9980 e de 0,9970 para 1,0000 na segunda execução.

Para a taxa da sensibilidade, no caso da Árvore de Decisão pode ser feita observada uma evolução de 0,99996 para 1,00000.

Com relação a especificidade, é possível observar melhoras nos casos do *Naïve* Baiyes (de 0,4245 para 0,6132), kNN (de 0,9933 para 1,0000) e da Árvore de Decisão (de 0,9737 para 0,9868). A exceção ficou com o SVM onde houve uma piora de 1,0000 para 0,9868. Isso parece estar relacionado a casos de falsos positivos do sistema especialista e ao fato que a especificidade era de 1,0000 na primeira execução.

De acordo com as análises acima, montou-se a tabela 2 onde pode-se observar para cada critério de avaliação de desempenho se houve melhora ou manutenção da taxa a níveis ótimos para os quatro métodos analisados:

Tabela 2 – Evolução ou manutenção da capacidade de previsão dos métodos quando aplicado o reforço de dados do sistema especialista

Critério	Melhora	Manutenção de taxa
curva ROC	2	2
Sensibilidade	1	3
Especificidade	3	1

Fonte: Autor

5. Conclusão

De acordo com os critérios analisados, foi identificado que o acréscimo de conhecimento na forma de regras no processo de detecção de fraudes por algoritmos de aprendizado trouxe melhorias importantes nos resultados finais. Também foi verificado

que os sistemas especialistas podem ser utilizados com relativo sucesso para cumprir a tarefa de reforço de informações.

Do ponto de vista arquitetural, a solução se justifica por atender o desejo das seguradoras de contar com uma ferramenta precisa e barata que faça o trabalho de detecção de anomalias automaticamente. A arquitetura em etapas tira proveito de dois mundos nesse sentido: o conhecimento sobre fraudes é consolidado no formato de regras e a tarefa de detecção é delegada a etapa do sistema especialista que teria condições de substituir um especialista de forma muito precisa; a etapa do aprendizado de máquina participaria no processo para resolver o problema da incerteza ao confirmar ou rejeitar a hipótese de fraude.

Como sugestão de trabalhos futuros, é proposto o estudo com métodos de aprendizado de máquina não-supervisionados, particularmente o das redes neurais. Outro ponto a ser melhorado seria a utilização de dados de sinistros reais e mais abrangentes para amenizar o problema do *overfitting* e também para determinar se a hipótese se aplica a outros tipos de fraudes.

Referências

FRANK, Eibe; HALL, Mark A.; WITTEN, Ian H.. The WEKA Workbench: Online Appendix for "Data Mining: Practical Machine Learning Tools and Techniques", Morgan Kaufmann, Fourth Edition. 2016. Disponível em: <https://www.cs.waikato.ac.nz/ml/weka/Witten_et_al_2016_appendix.pdf>. Acesso em: 3 fev. 2019.

JBOSS DROOLS TEAM. Drools Documentation: Hybrid Reasoning. Disponível em: <https://docs.jboss.org/drools/release/7.7.0.Final/drools-docs/html_single/index.html>. Acesso em: 17 jun. 2018.

KIM, Yongbum; VASARHELYI, Miklos A.. A Model to Detect Potentially Fraudulent/Abnormal Wires of an Insurance Company: An Unsupervised Rule-Based Approach. Journal Of Emerging Technologies In Accounting, [s.l.], v. 9, n. 1, p.95-110, dez. 2012. American Accounting Association. DOI: http://dx.doi.org/10.2308/jeta-50411.

KIRLIDOG, Melih; ASUK, Cuneyt. A Fraud Detection Approach with Data Mining in Health Insurance. Procedia - Social And Behavioral Sciences, [s.l.], v. 62, p.989-994, out. 2012. Elsevier BV. DOI: http://dx.doi.org/10.1016/j.sbspro.2012.09.168.

LARA, Natalia Cairo. Evidências de práticas fraudulentas em sistemas de saúde internacionais e no Brasil. [s. L.]: Instituto de Estudos de Saúde Suplementar, 2017. Textos para Discussão nº 62-2017. Disponível em: <http://documents.scribd.com.s3.amazonaws.com/docs/6j0sz23kw05qrody.pdf>. Acesso em: 30 jun. 2018.

PANDEY, Pallavi; SAROLIYA, Anil; KUMAR, Raushan. Analyses and Detection of Health Insurance Fraud Using Data Mining and Predictive Modeling Techniques. Advances In Intelligent Systems And Computing, [s.l.], p.41-49, 25 nov. 2017. Springer Singapore. DOI: http://dx.doi.org/10.1007/978-981-10-5699-4_5.

SHIN, Hyunjung et al. A scoring model to detect abusive billing patterns in health insurance claims. Expert Systems With Applications, [s.l.], v. 39, n. 8, p.7441-7450, jun. 2012. Elsevier BV. DOI: http://dx.doi.org/10.1016/j.eswa.2012.01.105.