DETECÇÃO DE FRAUDES EM MOVIMENTAÇÕES FINANCEIRAS USANDO A TÉCNICA DE SISTEMA IMUNOLÓGICO ARTIFICIAL

FRAUD DETECTION IN FINANCIAL TRANSACTIONS USING ARTIFICIAL IMMUNE SYSTEM TECHNIQUE

Cintia Yurie Yamada[1]; Danilo Medeiros Eler[2]; Ives Renê Venturini Pola[3]; Almir Olivette Artero[4]; Maurício Araújo Dias[5]

UNESP - Universidade Estadual Paulista – UNESP, Faculdade de Ciências e Tecnologia, Departamento da Matemática e Computação
E-mail: [1]cintiayys@gmail.com; [2]daniloeler@fct.unesp.br; [3]ivesrene@gmail.com; [4]almir@fct.unesp.br; [5]madias@fct.unesp.br

RESUMO – Técnicas de classificação como Rede Neural Artificial e Rede Bayesiana são muito utilizadas para a tarefa de reconhecimento de padrões. A maioria delas constrói um padrão e em seguida submete novas instâncias a uma comparação com o padrão construído. O mesmo ocorre para a detecção de fraude em movimentações financeiras. Entretanto, a maioria das técnicas precisa ser treinada novamente a cada alteração simples que o padrão possa sofrer. Com a técnica de Sistema Imunológico Artificial ocorre a evolução do padrão sem a necessidade de realizar um novo treinamento para a modificação do padrão. O objetivo principal deste trabalho foi aplicar a técnica de Sistema Imunológico Artificial no contexto de detecção de fraudes em movimentações financeiras e analisar o desempenho comparando-se com as técnicas clássicas. Além disso, os resultados foram comparados com outras duas técnicas muito utilizadas na detecção de fraude, a Rede Neural Artificial e a Rede Bayesiana. Os resultados e a análise das comparações dos resultados sugerem que a técnica de Sistema Imunológico Artificial foi aplicada com sucesso na detecção de fraudes em movimentações financeiras, e também existem aperfeiçoamentos para explorar melhor os mecanismos fornecidos pela técnica, permitindo que ela ultrapasse os resultados positivos das demais técnicas.

Palavras-chave: inteligência artificial; sistema imunológico artificial; detecção de fraudes.

ABSTRACT – Classification techniques such as Artificial Neural Network and Bayesian Network are heavily used for pattern recognition task. Most of them builds a pattern, and then submit new instances a comparison to the pattern built. The same is true for fraud detection in financial transactions. However, most of techniques need to be retrained every single change that pattern may suffer. Using the Artificial Immune System technique, the pattern evolution occurs without the need for new trainings. The objective of this work was to apply the Artificial Immune System technique in fraud detection context in financial transactions and to analyze its performance compared with

classical techniques such as Artificial Neural Network and Bayesian Network. Results of the detection performed by the system are provided, and also compared with the results of other two techniques widely used in the detection of fraud, Artificial Neural Network and Bayesian Network. The results and analysis of comparisons of results suggest that the Artificial Immune System technique can be implemented to detect fraud in financial transactions. However, there is room for improvements to further explore the mechanisms provided by technology, allowing it to exceed the results positive the other techniques.

Recebido em: 09/09/2016
Revisado em: 16/11/2016
Aprovado em: 0/11/2016

Keywords: artificial intelligence; artificial immune system; fraud detection.

1. INTRODUÇÃO

Em um evento promovido pela empresa multinacional Serasa Experian (empresa de serviço de informações de gerenciamento de risco de crédito, prevenção a fraudes, direcionamento de campanha de marketing e na automatização do processo de tomada de decisão), foi informado que o valor do prejuízo com as transações fraudulentas no Brasil chegou a 2,3 bilhões de reais no ano de 2013 e a Serasa Experian afirma ainda que 30% dos usuários já sofreram fraude (CHAER, 2014). Pela grandeza desse valor, as empresas investem cada dia mais na detecção de fraudes.

As tentativas de fraudes têm crescido nos últimos anos (EXPERIAN, 2015), além das técnicas usadas para praticar estas tentativas. Cada técnica busca explorar as vulnerabilidades do sistema de segurança e de pessoas. Em movimentações financeiras, é preciso estar cada dia mais atento a cada alteração que ocorre na conta de cada cliente.

Para evitar falsificação com cédulas, moedas e cheques, uma alternativa para compras mais seguras é o uso do cartão bancário. Além de ser um dispositivo pessoal que pode ser bloqueado em casos de roubo, ele evita troco nas compras, prevenindo que pessoas possam receber cédulas inválidas ou falsificadas. Entretanto, o uso de cartões bancários também apresenta desvantagens no aspecto de segurança, pois, com a popularização de seu uso, fraudadores encontraram formas de burlar o sistema de segurança e identificação destes cartões e passaram a clona-los usando as informações pessoais roubadas. Uma das formas é a utilização de uma máquina apelidada de “Chupa-Cabra” que, quando instalada no terminal bancário, captura informações como senha bancária dos clientes, além dos dados do cartão, como o código.

Com o avanço da tecnologia, o uso do cartão bancário foi ampliado com as máquinas portáteis que fazem a leitura de cartão bancário permitindo que lojistas e empresários tivessem mais uma forma de receber pagamentos. Mas, segundo o *blog* da Kaspersky Lab, *crackers* (*hackers* criminosos) brasileiros desenvolveram uma nova praga perigosa: o *malware* Chupa-Cabra. Esse *malware* possui a mesma função da máquina Chupa-Cabra implantada nos terminais bancários. Ele copia e rouba os dados de cartões bancários. Este vírus é instalado em um computador que receberá a conexão de uma máquina leitora de cartão bancário via USB (*Universal Serial Bus*). As leitoras possuem *hardware* e *software* de segurança, mas o problema é que o vírus é instalado no computador e consegue, através dele, capturar os dados bancários (ASSOLINI, 2012). Para dificultar a detecção, as movimentações financeiras realizadas com cartão de crédito não possuem um padrão, podem ocorrer com valores pequenos ou altos e ainda, a clonagem de cartões não se limita aos tipos de crédito, mas incluem os de débito (PARODI, 2014).

Além destas máquinas leitoras, o *e-commerce* acabou sendo outra facilidade da tecnologia, permitindo que pessoas comprem sem a necessidade de estar fisicamente na loja, mas é também outra forma que os atacantes exploram com o *malware*, pois no pagamento é preciso digitar dados pessoais e relacionados com o cartão bancário.

Para realizar a detecção de fraudes em movimentações financeiras, é necessário que um sistema faça a análise de registros antigos para que sejam comparados com o registro inserido. O padrão das movimentações financeiras depende dos registros relacionados a cada conta bancária e cada cliente possui um padrão de movimentações financeiras: podendo ser um empresário que costuma comprar mercadorias de alto valor, ou então, um empregado cujo padrão de movimentação financeira é gastar em necessidades como abastecimento do carro e compras em supermercados. Logo, aplicar uma única técnica de detecção de fraude para ambas as contas bancárias não seria a forma mais eficiente para proteger os clientes. O mais adequado é que, como cada pessoa possui um determinado padrão, a detecção seja feita individualmente, assim, qualquer movimentação feita fora do padrão pode caracterizar uma fraude.

Certos tipos de fraude seguem um padrão que, com o tempo, são detectados por gerentes e empresas de segurança. Um exemplo antigo de padrão de fraude é o uso do cartão de crédito roubado ou clonado em que os fraudadores realizam uma pequena compra para validar a utilidade do cartão, e,

uma vez que a movimentação é aprovada, é realizada uma compra num valor mais alto para estourar o limite do cartão. A descoberta de padrões de fraudes acaba gerando novas técnicas de fraude, por este motivo é necessário a utilização de uma técnica que possa acompanhar a evolução dos tipos de fraudes, detectando novas fraudes e adaptando o sistema de detecção de forma rápida e simples.

O que a maioria das técnicas de detecção faz é usar um conjunto de dados para o treinamento do sistema e construir um padrão (definição de valores numéricos que identificam uma estrutura comum à maioria dos registros de treinamento considerados verdadeiros) e, caso o padrão do cliente mude, é preciso realizar o treinamento novamente para que o sistema esteja apto para o novo padrão acompanhando a evolução do padrão do cliente. O novo treinamento é um passo muito custoso, uma vez que a cada movimentação diferente, é preciso que o sistema reveja todos os registros de treinamento para se adaptar ao modo de utilização do cliente. Para evitar que este treinamento seja refeito a cada nova movimentação, que não seja fraude e, que não siga o padrão previamente estabelecido, a técnica de Sistema Imunológico Artificial permite que o treinamento seja realizado no início da implementação do sistema e, em seguida, ele consiga evoluir de forma automática, sem a necessidade de um novo treinamento.

Recentemente, alguns trabalhos utilizam a técnica de Sistema Imunológico Artificial (SIA) para detecção de intrusão, como nos trabalhos de Carneiro et al. (2015), Aickelin, Dasgupta e Gu (2014) e Leão (2015). Além da preocupação da detecção de fraudes em transações eletrônicas com o avanço da tecnologia e do *e-commerce* como apresentada nos trabalhos de Carneiro et. al. (2015) e Assis et. al. (2014). Embora pouco explorada, a técnica de SIA possui características relevantes que foram motivações para auxiliar na detecção de fraudes.

O objetivo deste trabalho foi aplicar a técnica de Sistema Imunológico Artificial no contexto de detecção de fraude em movimentações financeiras e analisar o seu desempenho comparando-se com técnicas clássicas como Rede Neural Artificial e Rede Bayesiana.

Este artigo está organizado da seguinte maneira. Na Seção 2 são descritos os principais trabalhos relacionados da literatura. Na Seção 3 é feita uma breve descrição

de conceitos relacionados ao sistema imunológico biológico, além dos mecanismos e detalhes da implementação do ambiente computacional de análise de movimentações

financeiras. Na Seção 4 são apresentados os resultados obtidos pelo ambiente computacional e discussões sobre os resultados. Por fim, na Seção 5 são relatadas as conclusões obtidas por meio da análise dos resultados e são apresentadas propostas para trabalhos futuros.

2. TRABALHOS RELACIONADOS

Alguns trabalhos são relacionados à aplicação da técnica de Sistema Imunológico Artificial (SIA) em outros contextos, como no trabalho realizado por Brabazon et. al. (2010), no qual, os autores aplicaram a técnica de SIA para identificar fraudes no uso de cartão de crédito para compras online. Ao final do trabalho, eles concluíram que a técnica pode ser aplicada nesse domínio, mas é preciso tomar alguns cuidados quanto à decisão dos algoritmos a serem usados. Ainda, os autores verificaram que a utilização de rotinas ou regras para definir fraudes podem ser aplicadas para detectar fraudes mais óbvias, para que a detecção utilizando a técnica de SIA seja feita apenas em casos mais sutis de fraude, ou seja, aqueles casos em que é preciso uma análise mais detalhada.

Já Dasgupta e Forrest (1999) aplicaram o mecanismo de seleção negativa do SIA para detectar quebra em ferramentas em indústrias. Nesse estudo, foi verificado que o mecanismo detectou todas as quebras de ferramentas em todos os testes realizados, mostrando a potencialidade do mecanismo.

Outros trabalhos focam no estudo aprofundado e as possibilidades que as características da técnica SIA proporcionam ou podem proporcionar, como no trabalho realizado por Bachmayer (2008), que introduziu as características e abstrações da técnica. Dasgupta, Yu e Nino (2011) alertam que há sobreposições das características (clonagem, mutação e seleção) dos mecanismos de Rede
Imunológica Artificial e Seleção Clonal com o Algoritmo Genético.

A maioria dos trabalhos relacionados à detecção de fraudes em cartões de crédito utiliza as técnicas de Rede Neural Artificial (RNA) e Rede Bayesiana (RB), como no trabalho apresentado por Patidar et. al. (2011), onde a técnica de RNA é a mais usada na detecção de fraudes em cartões de crédito. No trabalho, foi utilizada a RNA treinada com o algoritmo de *Backpropagation*, o algoritmo mais popular para o treinamento da RNA. Os autores ainda utilizaram a combinação de RNA com Algoritmo Genético para melhorar o desempenho do sistema na detecção de fraudes. Ainda segundo eles, a ideia de combinar as duas técnicas vem da análise da junção de uma pessoa talentosa e que treina,

combinação que aumenta as chances da pessoa ser bem-sucedida.

Um outro trabalho, desenvolvido por Lima e Pereira (2012), comparou o desempenho das técnicas de Regressão Lógica e Rede Bayesiana na detecção de fraudes em transações eletrônicas usando cartão de crédito. O estudo permitiu concluir que o modelo Bayesiano foi o mais eficaz na maioria dos experimentos realizados.

No trabalho realizado por Kirkos, Soathis e Manolopoulos (2007) foi comparado o desempenho de três técnicas de Mineração de Dados: Árvore de decisão, Rede Neural Artificial e Rede Bayesiana, sendo a Rede Bayesiana a que apresentou melhor desempenho com 90% de acerto na classificação.

Dasgupta (1997) comparou as características das técnicas de RNA e SIA, destacando o poder de aprendizagem, memorização, treinamento e ainda a influência dos parâmetros de controle para o desempenho das técnicas. Concluiu que o sistema imunológico é mais complexo que o sistema neural e ainda funciona como um "segundo cérebro", pois armazena memórias de experiências passadas e pode responder a novos padrões.

Ji e Dasgupta (2006) alertam que o mecanismo de Seleção Negativa não pode ser usado em qualquer tipo de problema, pois é preciso analisar a representação dos dados e a variável de controle. Seguindo estas recomendações, no caso de variáveis não numéricas, para o presente trabalho, foram utilizadas funções específicas para a seleção e ainda foram feitos testes para definir os valores das variáveis de controle para que o sistema tivesse o melhor desempenho.

De acordo com os trabalhos relacionados nessa seção, foi possível verificar que a detecção de fraude é uma tarefa muito utilizada e provavelmente será utilizada por muito mais tempo dadas as crescentes tecnologias e a ousadia dos fraudadores. Além disso, o uso da técnica de Sistema Imunológico Artificial vem ganhando foco e estudo da comunidade de Inteligência Artificial.

3. DESENVOLVIMENTO

Para o desenvolvimento deste trabalho, alguns obstáculos foram enfrentados. O principal foi a privacidade dos dados bancários armazenados em qualquer tipo de movimentação financeira. Algumas instituições bancárias foram contatadas para verificar a possibilidade de fornecer apenas os principais dados que são armazenados em cada movimentação, mas nenhuma forneceu qualquer tipo de informação, o que é aceitável visando a proteção dos dados bancários que é defendido por lei (Art. 5º da Constituição Federal de 1988) e, para evitar a evolução e criação de novas técnicas de

fraude. Mas, para pesquisas, esta proteção torna-se um obstáculo. Para superá-lo, foram supostos alguns atributos. Como as instituições bancárias não fornecem nem ao menos os atributos armazenados, é óbvio que não forneçam um banco de dados que possa ser utilizado para pesquisas e experimentos. Logo, tanto os atributos armazenados no registro de uma movimentação financeira como os bancos de dados utilizados para treinamento e testes são fictícios. O que não reduz o valor dos resultados apresentados neste trabalho pois o objetivo principal é verificar o desempenho da técnica aplicada ao contexto além de compará-lo com o das outras duas técnicas (Rede Neural Artificial e Rede Bayesiana).

Para entender a técnica de Sistema Imunológico Artificial (SIA), é preciso conhecer alguns conceitos básicos do Sistema Imunológico Biológico (SIB). Segundo Gonzalez (2003), Dasgupta e Attoh-Okine (1997), Dasgupta e Forrest (1999), Dasgupta et al. (2003), Aickelin, Dasgupta e Gu (2014), Nasaroui, Gonzalez e Dasgupta (2002) e Forrest e Hofmeyr (1999), o SIB é um sistema complexo, robusto, distribuído, paralelo e adaptativo composto por tecidos especializados, órgãos, células e produtos químicos que tem como função principal diferenciar as células (ou moléculas) que estão dentro do corpo, em próprias e não-próprias. Em seguida, classificar as não-próprias para induzir um mecanismo apropriado de modo a eliminá-las ou neutralizá-las.

O SIB aprende, através da evolução, a distinguir entre antígenos estrangeiros perigosos e as próprias células do corpo. Além de usar a aprendizagem, utiliza também a memória para resolver problemas de reconhecimento de padrão. O SIA abstrai conceitos básicos do SIB, como a diferenciação entre próprio e não-próprio realizada pelas células de defesa, no contexto deste trabalho, movimentação financeira legal ou ilegal (fraude).

Dos vários tipos de célula que compõe o sistema, os principais são os anticorpos e as células de memória. O primeiro tipo é responsável por agir quando uma substância invade o sistema, ele é quem faz o reconhecimento da substância estranha e, dependendo das reações químicas que ocorrem entre a célula e a substância estranha, a célula começa o processo de eliminação ou neutralização da substância (AICKELIN; DASGUPTA; GU, 2014). No processo de eliminação, ocorre a produção de outro tipo de célula, a de memória, que é produzida a partir de um processo de clonagem, processo este que é acionado quando ocorre o reconhecimento de uma substância estranha. O anticorpo é sacrificado durante a eliminação da substância, por este motivo, antes da

eliminação completa, o anticorpo é clonado, assim, o sistema continua protegido contra substâncias iguais a que iniciou o processo de eliminação ((AICKELIN; DASGUPTA; GU, 2014).

A célula de memória circula pelo sangue, vasos linfáticos e tecidos, quando são reexpostas à substância estranha que a originou, ela se diferencia em plasmócitos que são capazes de produzir anticorpos (SILVA, 2001). No caso do SIA, o conceito de anticorpo engloba a capacidade de reagir ao estímulo do componente estranho, ou seja, movimentações financeiras fraudulentas e memorizar as características destas movimentações.

3.1. Sistema imunológico inato e adquirido

O corpo humano é protegido por um sistema complexo, sendo a pele a primeira barreira protetora do corpo que impede que substâncias de tamanho consideravelmente grande, como poeira, não invada o sistema. Caso a substância não seja barrada pela pele e consiga invadir o sistema biológico humano, é submetida à uma nova barreira, a fisiológica, que mantém o pH (potencial Hidrogeniônico) e a temperatura impróprios para a sobrevivência de algumas substâncias estranhas (AMARAL, 2006), mas caso a substância seja forte o bastante para sobreviver e apresente resistência a estas barreiras, ainda precisam enfrentar os anticorpos, que são os guardiões do SIB.

O sistema imunológico inato é um subconjunto do SIB e é composto por células destinadas à defesa do sistema imunológico biológico no início da vida. O leite materno influencia muito na construção deste sistema, mas a medida que o ser humano se desenvolve, é exposto a outros tipos de substâncias estranhas cujo sistema imunológico inato não está apto a agir para eliminá-las. Nestes casos, entra em ação as células que compõe o sistema imunológico adquirido, que, como o nome sugere, é construído e adquirido conforme o sistema é exposto a substâncias estranhas diferentes das que já conhece.

No SIA, o sistema imunológico inato pode ser composto por um conjunto de movimentações registrado no histórico da conta de cada cliente. Assim, no início, o sistema é capaz de se proteger apenas contra as movimentações fraudulentas registradas no histórico do cliente. Quando um novo tipo de fraude é detectado, é preciso que ele se adapte ao novo tipo de invasor, ou seja, o sistema imunológico adquirido é acrescido. O processo de composição do sistema imunológico inato equivale ao processo de treinamento de técnicas de classificação como a Rede Neural Artificial. Portanto, quando o sistema de detecção é iniciado, possui uma limitada população inicial de anticorpos. Esta população é ampliada conforme novas invasões são detectadas. A

nomenclatura dos sistemas é apenas para diferenciar a origem dos anticorpos, mas eles ficam espalhados por todo o corpo humano, formando um único conjunto de anticorpos. O mesmo ocorre com o SIA, após a geração do conjunto de anticorpos iniciais, ele é reforçado com novos anticorpos.

O fluxograma mostrado na Figura 1 ilustra uma iteração na construção do sistema imunológico inato (treinamento).

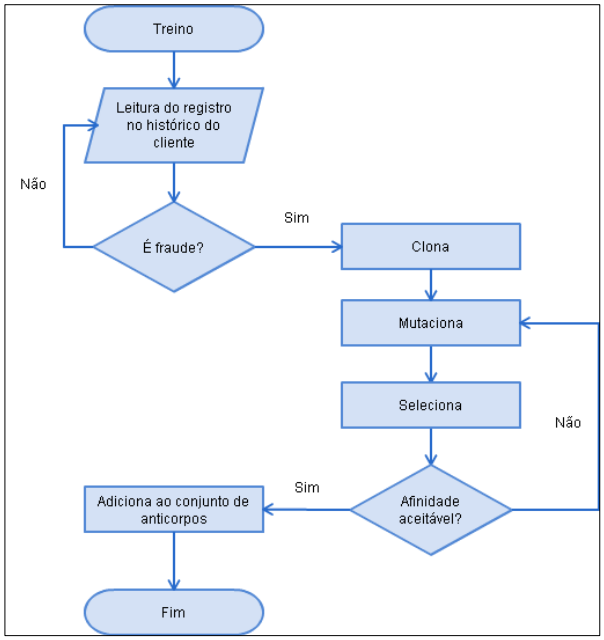

Figura 1. Iteração no Sistema Imunológico inato

3.2. Algoritmos inspirados no SIB

Alguns mecanismos do SIB inspiraram a criação de algoritmos que são usados em sistemas que implementam a técnica de SIA. Na implementação feita neste trabalho, foram utilizados três algoritmos: Seleção Clonal, Seleção Negativa e Seleção Positiva. Esses mecanismos são acionados quando ocorre uma detecção no SIB. Logo, no SIA, esses algoritmos são acionados quando ocorre a detecção de uma movimentação fraudulenta.

A Seleção Clonal ocorre, no SIB, para que anticorpos que reconheçam um tipo de intruso não sejam eliminados e o sistema fique desprotegido, assim, o anticorpo é clonado. Estes clones sofrem mutações para que o sistema consiga evoluir. É preciso que estes clones mutacionados passem por uma seleção para que apenas anticorpos que façam a proteção do sistema sejam mantidos (AMARAL, 2006). No SIA, deve ocorrer um procedimento semelhante, mas a única diferença é que o anticorpo que realiza a detecção do intruso não precisa ser eliminado para proteger o sistema, basta apenas que ele seja clonado e modificado aleatoriamente.

A Seleção Negativa tem como objetivo proteger o sistema de si mesmo, impedindo que um anticorpo gere uma doença autoimune (AMARAL, 2006). No SIA, a Seleção Negativa busca garantir que o sistema não detecte uma movimentação normal, indicando ser uma fraude, evitando a ocorrência de detecções falso-positivas (detectar uma movimentação legal como ilegal).

A Seleção Positiva seleciona os anticorpos que detectam positivamente os intrusos do sistema (BOEHMER, 1994) (SILVA, 2001), garantindo assim a proteção do

sistema contra substâncias não-próprias. No SIA, a Seleção Positiva é o processo em que os anticorpos são testados para verificar a capacidade de detectar movimentações fraudulentas.

Para cada movimentação financeira registrada no histórico da conta bancária, é verificada se é uma fraude, e caso seja, o sistema deve se proteger contra este tipo de fraude e, para isto, a movimentação fraudulenta é clonada e cada clone é mutacionado aleatoriamente. Após a mutação, os clones passam por uma seleção na qual é verificada a semelhança do clone mutacionado e da fraude que o gerou. Se a similaridade for maior que um limiar definido, então o clone é adicionado ao conjunto de anticorpos do sistema imunológico inato. Caso a similaridade seja inferior ao limiar, o clone é mutacionado até que atinja o grau de similaridade definido.

No SIB, os anticorpos que são selecionados negativamente devem ser eliminados, mas no SIA a eliminação custaria a criação de uma outra instância de um anticorpo para passar pela seleção novamente. Em termos computacionais, não é uma ação necessária e além disto, a geração requer mais tempo que uma modificação aleatória em alguns atributos do anticorpo, portanto no SIA, os anticorpos selecionados negativamente sofrem uma mutação para melhorar a afinidade na detecção da substância estranha.

3.3. Afinidade e Mutação

A afinidade, citada anteriormente no SIB, refere-se à força estabelecida pela ligação entre o anticorpo e a substância estranha. Esta ligação pode ser química ou física, sendo que a primeira ocorre com reações químicas entre os receptores do anticorpo e a substância estranha, e a segunda ocorre quando a forma física do receptor encaixa com a substância. Nem sempre o encaixe é perfeito, mas pode ser aperfeiçoado com a mutação (TIMMIS, 2000) (MACHADO, 2005). No SIA, não são representadas formas geométricas e nem reações químicas, a afinidade é baseada no cálculo da proximidade dos atributos da nova movimentação e da fraude. A equação utilizada no cálculo da afinidade depende do domínio de cada atributo da movimentação. Neste trabalho, foi utilizada a Equação (1) a qual representa a Distância Euclidiana para atributos numéricos (CASTRO; ZUBEN, 1999).

$$D = \sqrt{\sum_{i=1}^{L}(ab_i - ag_i)^2} \qquad (1)$$

Na Equação (1), ab_i é o anticorpo que detectará a fraude, ag_i é a fraude registrada no histórico e L é a dimensão do conjunto de atributos dos anticorpos e das fraudes.

O anticorpo é uma representação da movimentação, assim, o anticorpo e a fraude possuem os mesmos atributos. Foram definidos três tipos de movimentações:

- Tipo 1: Movimentação caracterizada simplesmente pelo valor, com $valor \in R$, data da realização da movimentação e a localização da ocorrência da movimentação.
- Tipo 2: Movimentação caracterizada pelo valor, com $valor \in R$, data da realização da movimentação, a localização da ocorrência da movimentação e o tipo do estabelecimento.
- Tipo 3: Movimentação caracterizada pelo valor, com $valor \in R$, data da realização da movimentação, nome do favorecido (quem receberá o valor da movimentação), nome do banco cuja conta bancária do favorecido pertence e a localização da agência bancária do favorecido.

Para os atributos não numéricos como a *localização* foi utilizada a seguinte regra: se os atributos são idênticos, *0,01* é adicionado ao valor da afinidade entre as movimentações. Caso contrário, o valor da afinidade não é alterado.

3.4. Ambiente computacional de análise de movimentações financeiras

Esta seção descreve o funcionamento do ambiente computacional desenvolvido para a análise do desempenho do SIA para detecção de fraudes em movimentações financeiras.

Constantes como a quantidade de clones gerada em cada Seleção Clonal, a taxa de mutação que o anticorpo sofre e o limiar que define o quão próximo o anticorpo e a fraude devem estar para que seja mantido (afinidade) são definidas em uma classe separada para que durante os experimentos as alterações delas possam ser feitas de forma rápida e apenas em um local. Duas variáveis simples foram adicionadas para que os valores mínimo e máximo pudessem ser registrados e comparados a cada nova movimentação, permitindo verificar se a nova movimentação ultrapassa o valor máximo registrado pelo cliente ou se está abaixo do menor valor já gasto por ele.

Para cada tipo de movimentação, foi criada uma classe específica com atributos e métodos. Os atributos comuns a todos os tipos de movimentações são *valor, data e localização*, e os métodos são para o cálculo da afinidade e para clonar o anticorpo. Após o primeiro passo, o treinamento que segue o fluxograma apresentado na Figura 1, todas as movimentações contidas na base de dados são exibidas para que seja analisado o desempenho do sistema e a avaliação do comportamento esperado do sistema para

uma nova movimentação, Figura 2. Com a população inicial definida com o treinamento, o sistema está protegido contra as fraudes registradas no histórico.

Figura 2. Movimentações separadas por tipos e separadas em fraude ou legal

Antes da inserção de uma nova movimentação no histórico, ela passa por uma detecção que compara a afinidade dela com todos os anticorpos do sistema, visto na Figura 3.

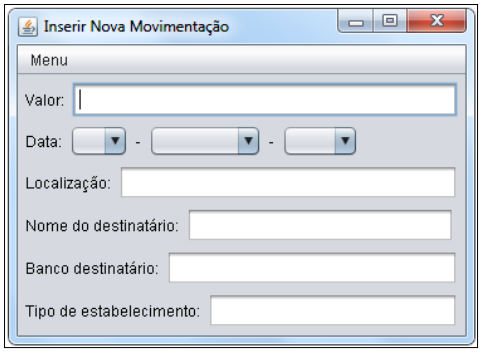

Figura 3. Interface usada para fazer nova movimentação.

Quando uma fraude é detectada, o anticorpo é clonado e mutacionado, mas antes que ele seja mantido pelo sistema ocorre a Seleção Clonal. Após ser selecionado, o clone que possui uma afinidade suficiente com o anticorpo que detectou a movimentação é inserido em uma hierarquia que tem como pai o anticorpo que o originou.

Quando é utilizada uma base de dados para realizar os experimentos, é gerada, ao final de todas as classificações, uma matriz de confusão com as movimentações classificadas e com as porcentagens de acerto e erro do sistema, um exemplo é mostrado na Figura 4.

A matriz de confusão é uma forma de representar a quantidade de registros classificados correta e incorretamente, ela é uma matriz quadrada cuja dimensão é a quantidade de classes, e neste trabalho, a dimensão da matriz de confusão é 2x2 pois a movimentação pode ser classifica em legal ou fraude. As colunas indicam as classes desejadas e as linhas as classes obtidas por meio da classificação. Desta forma, cada elemento m_{ij} representa a quantidade de registros que pertencem à classe j e foram classificados como pertencentes à classe i, ou seja, o valor do elemento m_{00} é a quantidade de movimentações que são legais e foram classificadas como legais. Logo, o comportamento ideal dos registros na matriz

de confusão é pertencer à diagonal principal, como na Figura 4.

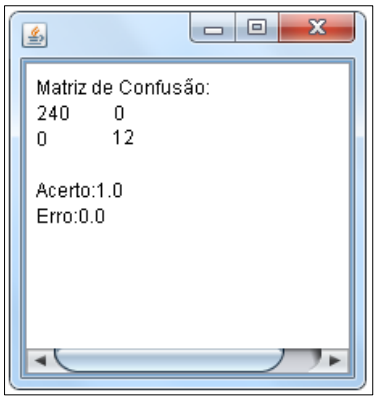

Figura 4. Matriz de confusão.

4. RESULTADOS E DISCUSSÕES

Como não foram encontradas bases de dados reais para a realização dos experimentos, a avaliação da proposta apresentada neste trabalho incluiu a criação de duas bases de dados com o mesmo padrão, mas com diferentes movimentações. Uma base é destinada para o treinamento e outra para a realização dos experimentos.

A base de dados utilizada na primeira parte dos experimentos tem a composição da seguinte maneira: o de treinamento que é composto por 66 movimentações (60 legais e 6 fraudes), e mantendo a proporção de $10 \setminus 1$ e o de teste a proporção é de $20 \setminus 1$.

Para gerar bases de dados com o mesmo padrão de movimentações foram definidas algumas variáveis para determinar intervalos dos valores de movimentações legais e ilegais. Valores aleatórios pertencentes ao padrão definido foram utilizados para gerar movimentações para as duas bases de dados.

Para definir o limiar de afinidade, foram realizados experimentos mantendo as demais constantes sem alteração para que a influência da alteração do limiar fosse o principal fator variante. Foram realizados três experimentos e cada um foi composto por dez execuções consecutivas de treinamento e teste. A cada execução, foram coletados o tempo gasto para realizar o treinamento e a matriz de confusão gerada após a classificação da base de dados de teste. Com os resultados, foi gerado o gráfico apresentado na Figura 5. Analisando o gráfico gerado, o limiar de 92% foi escolhido uma vez que ele é o menor valor que atingiu a maior porcentagem de acerto.

Além do acerto, foi verificada a influência do limiar no tempo gasto no treinamento. Quando o limiar for 0%, qualquer valor gerado para o anticorpo será aceito, pois não precisa ter afinidade com a fraude, logo, com 0% de afinidade, o tempo gasto é o menor, além da consequência da utilização deste limiar configurar um sistema fraco em que nenhum caso é realizada a detecção de fraude. Enquanto com o 100% de afinidade o tempo é muito maior, pois os valores gerados são aleatórios e apenas anticorpos idênticos seriam aceitos. Por estas análises e estes motivos, estes dois valores não foram utilizados nos experimentos.

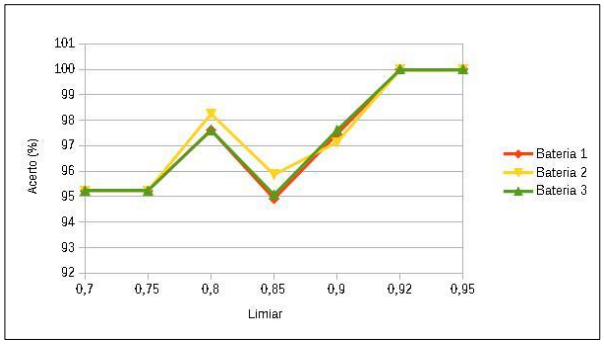

Figura 5. Influência do limiar de afinidade no acerto da detecção do sistema.

A Figura 6 apresenta um gráfico gerado com os três experimentos, sendo possível verificar que não há uma similaridade entre os resultados, o que é compreensível dada a forma como os dados são modificados. Portanto, como os valores são modificados aleatoriamente, não há um padrão de gasto de tempo com a variação do limiar de afinidade e como treinamento inicial ocorre uma vez, o tempo gasto no treinamento não tem relevância no tempo de detecção.

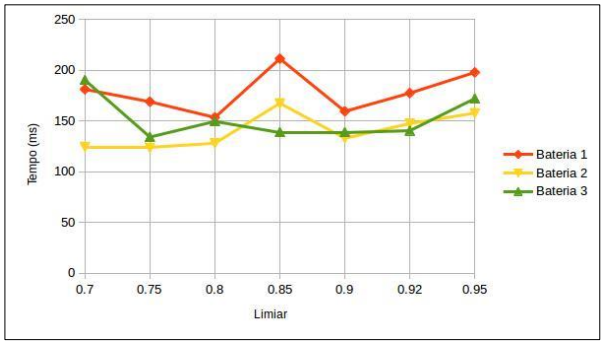

Figura 6. Influência do limiar de afinidade no tempo de treinamento.

Com as constantes selecionadas e definidas, foram utilizadas as movimentações da base de dados de teste. Os resultados são exibidos na forma de uma matriz de confusão apresentada pela Figura 4. Esta forma foi utilizada pois as outras técnicas de classificação (Rede Neural Artificial e Rede Bayesiana) foram testadas usando a ferramenta Weka, que exibe os resultados em forma de matriz de confusão, facilitando assim a comparação dos resultados apresentados. Este software é uma coleção de algoritmos de aprendizagem de máquina para tarefas de mineração de dados (HALL, 2009).

Os dados da base de teste e de treinamento foram exportados para o formato *arff* (*Attribute-Relation File Format*), o qual é utilizado para como padrão pelo Weka. Nesse tipo de formato de arquivo são especificados os tipos e as nomenclaturas dos atributos e em seguida os atributos em si. O exemplo apresentado pelo código na Figura 7 é um trecho do arquivo utilizado para treinar a RNA e a Rede Bayesiana (RB) com o software Weka que utiliza este formato de arquivo para a entrada de dados.

```
%1. Title: Banco de dados movimentação financeiras
%
%2. Source: (a) Creator: C.Y.Yamada
%           (b) Date: March,2015
%
@RELATION transacoes
@attribute VALOR real
@attribute CONTESTADA {true, false}
@data
5561.69,true
1879.55,false
```

Figura 7. Estrutura do arquivo gerado.

Os atributos representados por símbolos, como a *data* e a *localização*, não foram exportados para arquivo no formato *arff*, pois não podem ser usados para a classificação nas técnicas utilizadas (RNA e RB).

Para comparar o comportamento das técnicas, a quantidade de registros na base de dados variou. A cada experimento, as bases de dados de treino e de teste foram dobrados. Para cada uma das três variações foram realizadas dez execuções para avaliar a média do desempenho do sistema e os resultados apresentados no gráfico da Figura 8 são a média dos valores obtidos em cada experimento. Lembrando que a quantidade de registros mostrada na Figura 8 é a junção dos registros de teste e treino. Logo, dos 129 registros, 63 são de testes e 66 de treino. Dos 258, 132 são destinados para treinamento e 126 para teste. E dos 516 registros, 252 são para os testes e 264 para o treinamento.

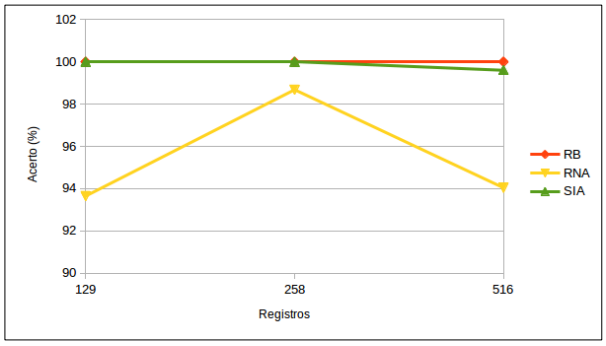

Figura 8. Desempenho das técnicas variando a quantidade de registros.

A RNA utilizada nos experimentos possui uma camada oculta com dois neurônios, seguindo o cálculo da média geométrica dos atributos e das classes possíveis: $\sqrt{atributos * classes} = \sqrt{2 * 2} = \sqrt{4}$.

5. CONCLUSÃO

O objetivo principal deste trabalho foi implementar a técnica de Sistema Imunológico Artificial no contexto de detecção de fraude em movimentações financeiras e analisar o desempenho desta técnica comparando o com o desempenho de técnicas clássicas como Rede Neural Artificial e Rede Bayesiana, como mostra a Figura 8.

Com a comparação realizada, foi possível verificar que a técnica apresenta um bom desempenho, porcentagem de acerto próximo dos 100%, ficando à frente de técnicas clássicas como a Rede Neural Artificial. Dada essa anotação, é importante explorar os demais mecanismos e abstrações da técnica para aperfeiçoar o desempenho do sistema de detecção.

A técnica difere quanto à evolução do padrão do usuário, permitindo que o sistema de detecção se adapte a mudanças sem a necessidade de processos custosos de treinamento e/ou inicialização, além de trabalhar com atributos representados por símbolos, como nome e localização, e que

não pertencem necessariamente a um conjunto pré-definido.

Como trabalhos futuros no contexto da detecção de fraudes em movimentações financeiras são sugeridos a utilização do atributo de localização baseada em coordenadas geográficas e uma possível aplicação de um *score* de acordo com o tipo de movimentação que ocorreu de forma legal.

A utilização do atributo de localização pode ser feita definindo um raio, em *km*, que será calculado a partir das coordenadas da cidade onde ocorreram as movimentações legais, pois no caso de um cliente realizar movimentações financeiras em uma cidade, *C*, localizada em um país, *P*, e no histórico da conta bancária aparece uma movimentação efetuada em um outro país, P_i que fica em um continente diferente de *P*, esta movimentação deve ser considerada suspeita.

A aplicação de um *score* é para aumentar a confiança do sistema. As movimentações podem ser agrupadas de acordo com um atributo, por exemplo, *valor*. Em seguida, é feita a separação deste grupo e o *score* é dado de acordo com a quantidade de movimentações que o grupo possui; todas as movimentações do mesmo grupo possuem a mesma pontuação. Assim, uma movimentação que ocorreu por ocasião, por exemplo comprar uma casa, não afetará tanto o sistema pois a pontuação deste tipo de movimentação é baixa e outra semelhante gera uma suspeita. Ressalta-se que o sistema de *score* pode ser otimizado com a determinação de um intervalo de movimentações que são consideradas na pontuação.

REFERÊNCIAS

AICKELIN, U.; DASGUPTA, D.; GU, F. Artificial immune systems. In: **Search Methodologies**. [S.l.]: Springer, 2014. p. 187–211. https://doi.org/10.1007/978-1-4614-6940-7_7

AMARAL, J. L. M. do. **Sistemas imunológicos artificiais aplicados à detecção de falhas**. 2006. Tese (Doutorado) - Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2006.

ASSIS, C. A. et al. Técnicas de programação genética para descoberta de fraudes em transações de comércio eletrônico. In: SYMPOSIUM ON KNOWLEDGE DISCOVERY, MINING AND LEARNING (KDMiLe), 2. **Anais...** 2014.

ASSOLINI, F. **The 'Chupa Cabra' malware:** attacks on payment devices. 2012. Disponível em: <https://securelist.com/blog/incidents/32248/the-chupa-cabra-malware-attacks-on-payment-devices-27/i>.

BACHMAYER, S. **Artificial immune systems**. 2008. Disponível em: <http://www.cs.helsinki.fi/u/niklande/opetus/SemK07/paper/bachmayer.pdfi>.

BOEHMER, H.V. Positive selection of lymphocytes. **Cell**, v. 76, n. 2, p.219–228, 1994. https://doi.org/10.1016/0092-8674(94)90330-1

BRABAZON, A. et al. Identifying online credit card fraud using artificial immune systems. In: IEEE. EVOLUTIONARY COMPUTATION (CEC). **Proceedings...** 2010. p. 1–7. https://doi.org/10.1109/CEC.2010.5586154

CARNEIRO, S. M. et al. Sistemas imunológicos artificiais no teste de agentes inteligentes. Revista **Brasileira de Computacão Aplicada**, v. 7, n. 2, p. 62–76, 2015. https://doi.org/10.5335/rbca.2015.4540

CASTRO, L. N. D.; ZUBEN, F. J. V. Artificial immune systems: Part i – basic theory and application. **Tech. Rep**, v. 210, 1999.

CHAER, M. **Brasil teve prejuízo de R$ 2,3 bilhões com fraudes em 2013**. 2014. Disponível em: <http://www.conjur.com.br/2014-abr-02/brasil-teve-prejuizo-23-bilhoes-fraudes-internet-2013i>.

DASGUPTA, D. Artificial neural networks and artificial immune systems: similarities and differences. In: IEEE. SYSTEMS, MAN, AND CYBERNETICS, 1997. COMPUTATIONAL CYBERNETICS AND SIMULATION., 1997 IEEE INTERNATIONAL CONFERENCE ON. **Proceedings...** 1997. v. 1,p. 873–878.

DASGUPTA, D.; ATTOH-OKINE, N. Immunity-based systems: A survey. In: IEEE. SYSTEMS, MAN, AND CYBERNETICS, 1997. COMPUTATIONAL CYBERNETICS AND SIMULATION., 1997 IEEE INTERNATIONAL CONFERENCE ON. **Proceedings...** 1997. v. 1, p. 369–374.

DASGUPTA, D.; FORREST, S. Artificial immune systems in industrial applications. In: IEEE. INTELLIGENT PROCESSING AND MANUFACTURING OF MATERIALS, 1999. IPMM'99. **Proceedings...** 1999. v. 1, p. 257–267. https://doi.org/10.1109/IPMM.1999.792486

DASGUPTA, D. et al. Artificial immune system (ais) research in the last five years. In: IEEE CONGRESS ON EVOLUTIONARY COMPUTATION, 1. **Proceedings...** 2003. p. 123–130. https://doi.org/10.1109/CEC.2003.1299565

DASGUPTA, D.; YU, S.; NINO, F. Recent advances in artificial immune systems: models and applications. **Applied Soft Computing**, v. 11, n. 2, p. 1574–1587, 2011. https://doi.org/10.1016/j.asoc.2010.08.024

EXPERIAN, S. **Abril registra alta nas tentativas de fraude contra o consumidor, revela Indicador Serasa Experian**. 2015. Disponível em: <http://www.serasaconsumidor.com.br/abril-registra-alta-nas-tentativas-de-fraude-contra-o-consumidor-revela-indicador-serasa-experian/i>.

FORREST, S.; HOFMEYR, S. A. John holland's invisible hand: An artificial immune system. In: FESTSCHRIFT CONFERENCE IN HONOR OF JOHN HOLLAND. **Proceedings...** 1999.

GONZALEZ, F. **A study of artificial immune systems applied to anomaly detection**. 2003. Tese (Doutorado) - University of Memphis, Memphis, 2003.

HALL, M. et al. The weka data mining software: An update. **SIGKDD Explor. Newsl.,** v. 11, n. 1, p. 10–18, nov. 2009. Disponível em: <http://doi.acm.org/10.1145/1656274.1656278i>.

JI, Z.; DASGUPTA, D. Applicability issues of the real-valued negative selection algorithms. In: ACM. THE ANNUAL CONFERENCE ON GENETIC AND EVOLUTIONARY COMPUTATION, 8. **Proceedings…** 2006. p. 111–118. https://doi.org/10.1145/1143997.1144017

KIRKOS, E.; SPATHIS, C.; MANOLOPOULOS, Y. Data mining techniques for the detection of fraudulent financial statements. **Expert Systems with Applications**, v. 32, n. 4, p.

995–1003, 2007. https://doi.org/10.1016/j.eswa.2006.02.016

LEÃO, A. A. C. F. **Clusterização de dados usando algoritmos imunoinspirados**. 2015. Trabalho (Conclusão de Curso) - Universidade Federal de Lavras, Minas Gerais, 2015.

LIMA, R. F.; PEREIRA, A. C. **Aplicação de técnicas de inteligência computacional para detecção de fraude em comércio eletrônico**. Revista de Iniciação Científica, v. 12, n. 3, 2012.

MACHADO, R. B. **Uma abordagem de detecção de intrusão baseada em sistemas imunológicos artificiais e agentes móveis**. Tese (Doutorado) — Universidade Federal de Santa Catarina, 2005.

NASAROUI, O.; GONZALEZ, F.; DASGUPTA, D. The fuzzy artificial immune system: Motivations, basic concepts, and application to clustering and web profiling. In: IEEE. FUZZY SYSTEMS, 2002. FUZZ-IEEE'02. OF THE 2002 IEEE INTERNATIONAL CONFERENCE ON. **Proceedings...** 2002. v. 1, p. 711–716.

PARODI, L. **Cartões de crédito falsos, roubados ou clonados**. 2014. Disponível em: <http://www.fraudes.org/showpage1.asp?pg=99i>

PATIDAR, R. et al. Credit card fraud detection using neural network. **International Journal of Soft Computing and Engineering (IJSCE),** v. 1, n. 32-38, 2011.

SILVA, L.N.C. **Engenharia imunológica:** desenvolvimento e aplicação de ferramentas computacionais inspiradas em sistemas imunológicos artificiais. 2001. Tese (Doutorado) – Universidade Estadual de Campinas, 2001.

TIMMIS, J. **Artificial immune systems:** a novel data analysis technique inspired by the immune network theory. Tese (Doutorado) - Department of Computer Science, 2000.