

# 1 Introdução

Nos últimos anos assistimos a um crescimento explosivo dos mercados eletrônicos, dos quais os mais conhecidos são os sítios de leilão. Uma peculiaridade importante desses mercados é a possibilidade de adquirir produtos e serviços de pessoas e organizações das quais a única informação disponível é aquela obtida via Internet. Esse cenário facilita a execução de fraudes, já que nessas interações faltam uma série de elementos normalmente utilizados para julgar a qualidade do vendedor ou do prestador de serviços (Resnick, Zeckhauser, Friedman et al., 2000). Além disso, uma mesma pessoa ou organização pode atuar com diferentes identidades, o que dificulta a obtenção de uma visão global de um determinado agente.

Entre as soluções desenvolvidas para minorar esse problema, uma das mais populares é a dos *sistemas de reputação* (Resnick et al., 2000), que são mecanismos que possuem em comum a função de agregar opiniões sobre produtos vendidos e serviços prestados e disponibilizá-las para os futuros compradores, de modo a criar um incentivo para que os vendedores e prestadores de serviço se esforcem para cumprir o combinado. Normalmente os sistemas de reputação também publicam opiniões sobre o comportamento dos compradores; todavia, como normalmente o vendedor só fornece a mercadoria ou serviço depois de o comprador pagar, essas opiniões são menos relevantes.

A presença dos sistemas de reputação efetivamente possibilitou um grande desenvolvimento dos mercados eletrônicos, haja vista o crescimento no volume de negócios nos principais sítios que utilizam esse tipo de sistema (e.g. eBay, Amazon.com, MercadoLivre). No entanto, junto com o crescimento no volume de negócios veio o crescimento no volume de fraudes (Internet Crime Complaint Center, 2007), mostrando que os criminosos descobriram as vulnerabilidades do sistema e passaram a explorá-las sistematicamente.

As fraudes não só prejudicam a parte que foi enganada (comumente o comprador), mas também causam perdas diretas ao *operador* do mercado, isto é, à entidade que disponibiliza os mecanismos de interação entre as partes e que lucra

com os negócios realizados, e.g. cobrando comissões. Quando ocorre uma fraude, o operador normalmente deixa de receber comissões, tarifas, taxas etc. que seriam pagas caso as negociações não fossem fraudulentas. Também há perdas indiretas, causadas pelo aumento do risco percebido por parte dos demais participantes do mercado e a conseqüente redução no ritmo de crescimento dos negócios.

O operador vê-se então na necessidade de combater as fraudes, tendo em vista a preservação seu negócio. Esse combate se dá através do uso de procedimentos internos que identificam agentes suspeitos e aplicam medidas restritivas a esses agentes (e.g. suspensão de cadastro até que sejam apresentados determinados documentos). Todavia, essa solução levanta outro problema: o dos *falsos positivos*, vendedores honestos que acabam sendo considerados suspeitos. Esses vendedores podem abandonar o mercado ou pelo menos vender muito menos que o esperado durante a vigência das medidas restritivas, o que também prejudica o operador. O excesso de falsos positivos pode minar a confiança de potenciais vendedores no operador.

Resumindo: há perdas por conta dos falsos negativos (fraudadores que escapam dos controles do operador) e dos falsos positivos. O problema do operador passa a ser o de minimizar a perda total, já que a diminuição de uma delas normalmente implicará o aumento da outra. Como os fraudadores procuram ativamente fugir dos controles do operador, este precisa aperfeiçoar constantemente seus mecanismos de detecção.

Todavia, os resultados obtidos com os mecanismos existentes nem sempre agradam os clientes. Concomitante ao crescimento do volume de fraudes, surgiram pessoas e organizações independentes que procuram combater esse problema, por exemplo criando fóruns de discussão, tutoriais que ajudam a identificar ofertas suspeitas, “listas negras” etc<sup>1</sup>. Outros foram além e se propuseram a ativamente tentar descobrir possíveis anúncios fraudulentos, denunciando-os aos operadores dos sistemas e procurando contatar os compradores interessados neles para que sejam cuidadosos<sup>2</sup>, chegando a violar as políticas de uso estabelecidas pelos operadores. Esses mecanismos informais mostram um conhecimento compartilhado

---

<sup>1</sup> Alguns exemplos desses sites: “eBayers that Suck” (sic) ([ebayersthatsuck.com](http://ebayersthatsuck.com)), “Monitor das fraudes” ([fraudes.org](http://fraudes.org)), “Lesados pelo MercadoLivre” ([www.veja.org](http://www.veja.org))

<sup>2</sup> Entrevista com um ebay “vigilante” ([www.auctionbytes.com/cab/abu/y205/m02/abu0136/s02](http://www.auctionbytes.com/cab/abu/y205/m02/abu0136/s02)).

de como as fraudes se dão e que alguns agentes conseguem aplicar de modo efetivo esse conhecimento (Chua, Wareham & Robey, 2007).

No entanto, há evidências conflitantes sobre a capacidade dos *consumidores* defenderem-se de fraudes, mesmo os experientes (Grazioli & Jarvenpaa, 2000). Além disso, com a popularização do comércio eletrônico, a quantidade de consumidores inexperientes tende a aumentar e tornar mais fácil a perpetração de fraudes. Ou seja, ainda que haja um conhecimento compartilhado sobre as estratégias dos fraudadores, os próprios agentes envolvidos nas negociações com frequência não conseguem fazer uso desse conhecimento.

A questão que surge é a de se o operador poderia empregar mais agentes humanos especificamente na tarefa de *detectar* fraudes, já que estes se mostram capazes de identificar fraudadores que nem o operador nem a contraparte de um fraudador localizaram. Já existem mecanismos para denunciar ofertas suspeitas, mas cabe examinar a possibilidade de empregar pessoas de modo mais sistemático na tarefa de identificação de fraudadores. A dificuldade óbvia que se apresenta é o volume de informações: no eBay, a cada dia são adicionados perto de sete milhões de novos anúncios (eBay, 2008). Ainda que não seja necessário analisar todos, claramente existe um problema de escala: quanto mais o mercado cresce, maior a quantidade de pessoas envolvidas na detecção de fraudes, o que vai na contramão da tendência de automatizar tarefas para reduzir custos.

No entanto, há uma solução intermediária que vem ganhando força em outros tipos de atividade: o *crowdsourcing* ou *computação humana* (Gentry, Ramzan & Stubblebine, 2005; Ahn & Dabbish, 2004), que consiste na delegação de tarefas relativamente simples para seres humanos (e.g. reconhecimento de imagens), mas complexas para o computador. Essas tarefas são distribuídas através da Internet via portais (públicos ou não) para as pessoas previamente cadastradas; essas pessoas fazem as tarefas e novamente através da Internet fornecem os resultados, recebendo algum tipo de retribuição (participar de um jogo, receber bônus para gastar em determinada loja virtual etc.). O problema de escala é reduzido por conta do alcance global da Internet e pela redução dos custos envolvidos.

Um interessante desafio que se apresenta é o de melhorar os processos de detecção de fraudadores atualmente existentes recorrendo à ajuda de agentes humanos, segundo o paradigma da computação humana.

## 1.1. Objetivo

O objetivo deste trabalho foi o de verificar a viabilidade de detectar fraudadores em mercados eletrônicos recorrendo ao auxílio da computação humana, ou seja, à colaboração de agentes humanos recrutados através de portais na Internet. Não advogamos a substituição dos procedimentos atuais de detecção de fraude, mas sua complementação com o uso de avaliações feitas por agentes humanos, de forma a melhorar a relação entre a recuperação (fração do total de fraudadores que foram localizados *antes* de cometerem fraude) e a precisão (quantidade de fraudadores localizados versus a quantidade de vendedores honestos incorretamente dados como fraudadores).

Neste trabalho nos restringiremos aos sítios de leilão, que são os mercados eletrônicos mais populares e que por isso atraem muitos fraudadores. Apesar do nome, esses sítios costumam trabalhar também com compra e venda de produtos a preço fixo. Também vamos nos restringir às fraudes de não-entrega, que são aquelas nas quais o fraudador anuncia produtos apenas para receber os pagamentos, sem intenção de entregar. Essas fraudes são as mais frequentes (Internet Crime Complaint Center, 2007) e as que geram mais reclamações no eBay (Gregg & Scott, 2008).

## 1.2. Solução proposta

Para atingir nosso objetivo, propomos um jogo chamado “pega ladrão”, no qual a meta dos participantes é analisar vendedores e prever quais cometerão fraude de não-entrega dentro de um prazo estipulado pelo operador. Chamamos esse prazo de *janela de fraude*, que é o tempo no qual se espera que a maior parte dos fraudadores tenha perpetrado seu golpe. A premiação de cada jogador depende da quantidade de *verdadeiros positivos*, que são vendedores que previu que cometeriam fraudes e de fato agiram de forma suspeita; depende também da quantidade de *falsos positivos*: vendedores dados como suspeitos que não apresentaram indícios de fraude decorrido o prazo em questão.

A lógica do jogo é alinhar o interesse individual dos jogadores – conseguir prêmios – com o interesse do operador do mercado eletrônico – descobrir, com boa precisão, quais os fraudadores atuando no mercado. É um tipo de “jogo com propósito” (Ahn & Dabbish, 2004), onde os participantes ajudam o sistema a re-

resolver um problema computacional complexo (descobrir intenção de cometer fraude com base nos dados disponíveis) pelo fato de procurarem maximizar seu desempenho no jogo.

Chamaremos de *perfil público* ou simplesmente *perfil* o conjunto de informações associadas a um vendedor e que são disponibilizadas publicamente no mercado eletrônico. Essas informações incluem os anúncios de produtos e serviços, as negociações anteriormente feitas, incluindo o retorno dado pela contraparte, dados de localização (em que cidade o vendedor está), desde quando está cadastrado no mercado etc. Há também um perfil que podemos chamar de *privado*, composto por informações como nome real, endereço, número de identidade, número de cartão de crédito etc. Vamos assumir que os jogadores só têm acesso ao perfil público dos vendedores para fazer a sua previsão.

O jogo “pega ladrão” interage com o operador do mercado e com os jogadores. O operador deseja classificar os vendedores entre suspeitos e não suspeitos; os jogadores desejam receber premiações ao acertarem quem vai cometer fraudes. O jogo faz a intermediação entre ambos, transformando o problema do primeiro em desafio para o segundo.

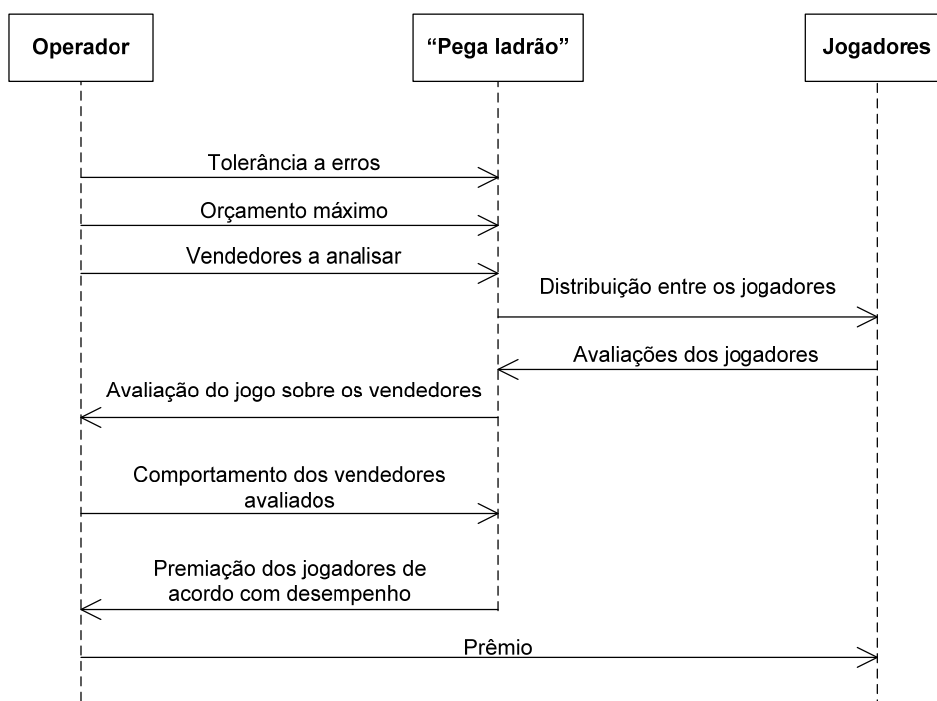


Figura 1: interações entre operador, jogo e jogadores

Na Figura 1 vemos de forma esquemática a seqüência de interações que se dão ao longo de um ciclo de execução do jogo, no qual é avaliado um conjunto de vendedores. A seguir vamos descrever cada uma dessas interações:

1. O operador informa ao jogo qual a sua *tolerância a erros*, isto é, qual é a maior fração de vendedores honestos que ele aceita que sejam dados como suspeitos.
2. O operador informa qual o orçamento disponível para remunerar os jogadores. Essa remuneração pode ser em dinheiro, descontos, prêmios, pontos etc.
3. O operador informa ao jogo um conjunto de vendedores que ele deseja analisar. Esses vendedores podem ser oriundos de um processo automático de classificação, que já fornece uma lista de suspeitos, só que com uma precisão muito baixa (excesso de falsos positivos).
4. O jogo atribui a tarefa de analisar os vendedores em questão a um ou mais jogadores.
5. Cada um dos jogadores comunica suas respostas ao jogo, isto é, para cada vendedor analisado por ele diz se considera que ele vai cometer uma fraude.
6. O jogo decide, em função das respostas dos jogadores, da tolerância informada pelo operador e das demais informações que ele dispõe (e.g. histórico do desempenho de cada jogador), se cada um dos vendedores em questão deve ser considerado suspeito ou não. Essa informação é repassada ao operador, que então pode tomar medidas preventivas com relação aos vendedores considerados suspeitos, de forma a reduzir os prejuízos caso alguns deles efetivamente cometam fraudes.
7. Decorrido o tempo da janela de fraude, o operador informa ao jogo quais dentre os vendedores analisados comportaram-se de forma fraudulenta.
8. O jogo compara as respostas dos jogadores com o desfecho real e informa ao operador qual a premiação devida a cada um dos jogadores, por conta dos seus acertos e erros.
9. O operador remunera os jogadores de acordo com as informações fornecidas pelo jogo.

Repetindo esse ciclo diversas vezes, o operador terá condições de avaliar todos os vendedores que ele desejar.

O objetivo da tese nos termos da solução proposta é o de mostrar que é possível especificar as diversas operações que o jogo faz de tal forma que, dado um orçamento, dada uma determinada tolerância e dada uma população de jogadores, o valor esperado da quantidade de fraudadores que são considerados suspeitos é significativo.

### **1.3. Metodologia**

Para especificar a solução proposta e validar os resultados obtidos, utilizamos a seguinte metodologia:

- Revisamos a literatura sobre os temas relacionados com a ocorrência de fraudes em mercados eletrônicos e sobre temas relacionados com computação humana.
- Executamos uma pesquisa exploratória para avaliar as dimensões da atuação fraudulenta nesses mercados.
- Fizemos um teste piloto para verificar a viabilidade de utilizar agentes humanos não-especializados na detecção de fraudadores.
- Construimos um mecanismo de identificação de fraudadores baseado em modelos probabilísticos da atuação dos jogadores e em princípios tirados da teoria de projeto de mecanismos.

Nas próximas seções descreveremos com mais detalhes cada um desses passos. No final, apresentaremos as limitações da metodologia adotada.

#### **1.3.1. Revisão da literatura**

Fizemos em primeiro lugar uma revisão da literatura relacionada com o problema das fraudes em sítios de leilão e com temas relacionados com computação humana. Nos próximos parágrafos vamos apresentar os diversos tópicos pesquisados e sua relação com o problema que estamos abordando.

**Fraudes em sítios de leilão:** para justificar o trabalho desenvolvido e conhecer melhor o fenômeno da fraude, procuramos os trabalhos existentes que analisam atividade fraudulenta nesses sítios.

**Sistemas de reputação:** são os mecanismos mais utilizados para melhorar a confiabilidade dos mercados eletrônicos e por isso são alvos de tentativas de manipulação por parte dos fraudadores.

**Mecanismos de detecção de fraudes:** procuramos o estado da arte no campo de detecção de fraudadores, de forma a verificar a novidade e as contribuições da nossa proposta.

**Computação humana:** pesquisamos os trabalhos nessa área de forma a encontrar modelos para sistemas que utilizam esse paradigma e também descrições de sistemas desse tipo já existentes.

**Mecanismos de revelação de informação:** a solução que estamos propondo envolve o fornecimento de informações por agentes humanos, o que levanta o problema da atuação estratégica, isto é, de decidir que informações fornecer levando em conta os benefícios que podem advir com isso, ao invés de revelar sempre informações verdadeiras. Por conta disso, procuramos trabalhos relacionados com *mecanismos de incentivo*, que visam garantir revelação verdadeira de informações mesmo em situações onde os agentes podem agir estrategicamente e conseguem calcular qual o benefício que pode ser auferido em função da informação fornecida.

### 1.3.2. Pesquisa exploratória sobre atividade fraudulenta

Dado que o objetivo do trabalho é identificar fraudadores, procuramos averiguar as dimensões do problema. Como encontramos poucos números acerca da atuação fraudulenta e todos eles referentes ao eBay, empreendemos uma pesquisa exploratória sobre a ocorrência de fraudes no MercadoLivre, o maior mercado eletrônico do Brasil. A escolha desse sítio se deveu a dois motivos principais:

- A ausência de trabalhos na literatura acerca da atuação fraudulenta nesse sítio, apesar de ser um fenômeno divulgado na Internet<sup>3</sup>.
- Dado nosso objetivo de utilizar agentes humanos para avaliar vendedores, seria muito mais fácil validar nossa proposta utilizando um sítio que estivesse na língua portuguesa e fosse popular no Brasil.

A pesquisa exploratória teve como objetivo caracterizar a atividade fraudulenta em diversas dimensões (frequência, tipo de produto, duração etc.). Como na vasta maioria dos casos não existe confirmação oficial de que houve de fato uma

---

<sup>3</sup> Cfr. sítio ReclameAqui ([www.reclameaqui.com.br](http://www.reclameaqui.com.br)).



fraude, essa pesquisa utilizou alguns critérios de análise de evidências para concluir se houve ou não fraude e também para estimar qual a dimensão da perda sofrida pelo operador.

Foi feita uma coleta de dados longitudinal durante um mês, acompanhando a evolução temporal dos produtos e vendedores encontrados. Restringimo-nos a determinadas informações e a determinadas categorias de produtos.

### **1.3.3.**

#### **Teste do uso de pessoas na identificação de fraudadores**

Para confirmar a viabilidade de utilizar agentes humanos não especializados na detecção de fraudadores, fizemos um teste piloto com uma amostra de conveniência de 26 pessoas. Cada participante do experimento avaliou cópias de perfis de 20 vendedores, prevendo para cada um se iria ou não cometer fraude no futuro. Comparamos as respostas com o desfecho real para avaliar o quanto os agentes humanos acertaram.

### **1.3.4.**

#### **Mecanismo de identificação de fraudadores**

O mecanismo de identificação de fraudadores é o cerne do jogo “pega ladrão”; consiste na composição de dois submecanismos: o de classificação de vendedores e o de incentivo aos agentes humanos.

O primeiro consiste em um algoritmo de classificação, cujo funcionamento depende de um modelo probabilístico da atuação fraudulenta e de outro modelo da atuação dos agentes humanos na tarefa de encontrar fraudadores. O primeiro modelo foi derivado dos resultados da pesquisa exploratória. O modelo de atuação dos agentes humanos foi construído com base no modelo probabilístico utilizado em mecanismos de incentivo para revelação verdadeira de informação, dentro do contexto de sistemas de reputação e de recomendação (Miller, Resnick & Zekhauser, 2005; Jurca & Faltings, 2004). Como o nosso contexto é o de previsão de conduta fraudulenta, dependemos da hipótese de que essa diferença de tarefas não afeta o modelo.

O mecanismo de incentivo foi construído com base na teoria de projeto de mecanismos, de forma a oferecer pagamentos<sup>4</sup> tais que a melhor ação para os agentes humanos seja sempre a de fornecer informações verdadeiras. No entanto,

---

<sup>4</sup> Podem ser brindes, descontos ou mesmo algum tipo de pontuação.

não chegamos a especificar completamente o mecanismo nem a derivar as estratégias que os agentes adotam em situações de equilíbrio.

A avaliação do mecanismo de identificação de fraudadores foi feita utilizando simulações, tomando como população de agentes humanos aqueles que participaram do teste piloto. Os conjuntos de parâmetros utilizados nessas simulações foram construídos com base nos dados empíricos obtidos a partir da pesquisa exploratória, do teste piloto e também no sítio Mechanical Turk, que disponibiliza tarefas para pessoas fazerem mediante uma remuneração pequena. Construímos oito conjuntos de parâmetros e calculamos qual seria o desempenho esperado do mecanismo de identificação de fraudadores para cada um desses conjuntos.

### **1.3.5. Limitações da metodologia adotada**

A pesquisa exploratória sobre ocorrência de fraudes no MercadoLivre oferece informações limitadas, devido ao período curto de tempo no qual foi feita a coleta de dados (um mês), além da pequena abrangência da mesma (cerca 0,1% do total de vendedores ativos e pouco menos de 10% do total de produtos anunciados). Com isso, o modelo de fraude proposto precisa ser confirmado com ulteriores estudos.

As conclusões do teste piloto feito com agentes humanos têm um alcance limitado, por conta do uso de uma amostra de conveniência e da quantidade pequena de avaliações feitas por cada agente. Ainda assim, oferece bons indícios de que o modelo testado se aplica ao menos para algumas classes de pessoas.

Os mecanismos de classificação e incentivo foram avaliados apenas por simulações com conjuntos de parâmetros cuja justificativa é frágil. Seria necessário obter mais dados empíricos.

Resumindo, a metodologia adotada permite obter indícios bem fundamentados sobre a viabilidade da solução proposta. São necessários, no entanto, estudos mais aprofundados para confirmar esses indícios e verificar a real eficácia dessa solução.

### **1.4. Estrutura do trabalho**

No Capítulo 2 revisamos a literatura de acordo com a metodologia adotada. No Capítulo 3 examinamos o problema da atividade fraudulenta no MercadoLivre, apresentando os dados coletados em uma pesquisa exploratória. No Capítulo

4 apresentamos o teste piloto feito com agentes humanos, descrevendo a metodologia utilizada, como foi feita a execução do teste e os resultados obtidos.

No Capítulo 5 apresentamos o mecanismo de identificação de fraudadores com seus dois submecanismos (o de classificação e o de incentivo). Também avaliamos sua eficácia, apresentando resultados de diversas simulações.

No Capítulo 6 concluímos o trabalho, descrevendo as contribuições feitas e os trabalhos futuros. No Anexo 1 encontra-se o material impresso utilizado no teste piloto realizado com agentes humanos.