Detecção de anomalias: uma pesquisa

Artigo em ACM Computing Surveys · Julho de 2009

DOI: 10.1145/1541880.1541882 · Fonte: DBLP

3 autores:

Varun Chandola

Universidade de Buffalo, Universidade Estadual de Nova York

119 PUBLICAÇÕES 13.878 CITAÇÕES

VER PERFIL

Arindam Banerjee

Escola SP Jain de Gestão Global

136 PUBLICAÇÕES 22.736 CITAÇÕES

VER PERFIL

Vipin Kumar

Universidade de Minnesota Twin Cities

746 PUBLICAÇÕES 86.128 CITAÇÕES

VER PERFIL

Relatório Técnico

Departamento de Ciência da
Computação e Engenharia
Universidade de Minnesota
Edifício EECS 4-192
200 Union Street SE
Minneapolis, MN 55455-0159 EUA

TR 07-017

Detecção de anomalias: uma pesquisa

Varun Chandola, Arindam Banerjee e Vipin Kumar

15 de agosto de 2007

Uma versão modificada deste relatório técnico aparecerá na ACM Computing Surveys, setembro de 2009.

Detecção de anomalias: uma pesquisa

VARUN CHANDOLA

Universidade de Minnesota
ARINDAM BANERJEE

Universidade de Minnesota
e

VIPIN KUMAR

Universidade de Minnesota

A detecção de anomalias é um problema importante que tem sido pesquisado em diversas áreas de pesquisa e domínios de aplicação. Muitas técnicas de detecção de anomalias foram desenvolvidas especificamente para certos domínios de aplicação, enquanto outras são mais genéricas. Esta pesquisa tenta fornecer uma visão geral estruturada e abrangente da pesquisa sobre detecção de anomalias. Agrupamos as técnicas existentes em diferentes categorias com base na abordagem subjacente adotada por cada técnica. Para cada categoria, identificamos as principais suposições, que são usadas pelas técnicas para diferenciar entre comportamento normal e anômalo. Ao aplicar uma determinada técnica a um domínio específico, essas suposições podem ser usadas como diretrizes para avaliar a eficácia da técnica naquele domínio. Para cada categoria, fornecemos uma técnica básica de detecção de anomalias e, em seguida, mostramos como as diferentes técnicas existentes nessa categoria são variantes da técnica básica. Este modelo fornece uma compreensão mais fácil e sucinta das técnicas pertencentes a cada categoria. Além disso, para cada categoria, identificamos as vantagens e desvantagens das técnicas nessa categoria. Também fornecemos uma discussão sobre a complexidade computacional das técnicas, pois é uma questão importante em domínios de aplicação reais. Esperamos que esta pesquisa forneça uma melhor compreensão das diferentes direções em que a pesquisa foi feita sobre este tópico e como as técnicas desenvolvidas em uma área podem ser aplicadas em domínios para os quais não foram concebidas inicialmente.

Categorias e Descritores de Assuntos: H.2.8 **[Gerenciamento de Banco de Dados]:** Aplicações de Banco de Dados — Mineração de Dados

Termos Gerais: Algoritmos

Palavras-chave e frases adicionais: Detecção de anomalias, Detecção de outliers

---

1. INTRODUÇÃO

Detecção de anomalias refere-se ao problema de encontrar padrões em dados que não estão em conformidade com o comportamento esperado. Esses padrões não conformes são frequentemente chamados de anomalias, outliers, observações discordantes, exceções, aberrações, surpresas, peculiaridades ou contaminantes em diferentes domínios de aplicação. Destes, anomalias e outliers são dois termos usados mais comumente no contexto de detecção de anomalias; às vezes de forma intercambiável. A detecção de anomalias encontra amplo uso em uma ampla variedade de aplicações, como detecção de fraudes para cartões de crédito, seguros ou assistência médica, detecção de intrusão para segurança cibernética, detecção de falhas em sistemas críticos de segurança e vigilância militar para atividades inimigas.

A importância da detecção de anomalias se deve ao fato de que anomalias em dados se traduzem em informações acionáveis significativas (e frequentemente críticas) em uma ampla variedade de domínios de aplicação. Por exemplo, um padrão de tráfego anômalo em um computador

rede pode significar que um computador hackeado está enviando dados confidenciais para um destino não autorizado [Kumar 2005]. Uma imagem de ressonância magnética anômala pode indicar a presença de tumores malignos [Spence et al. 2001]. Anomalias em dados de transações de cartão de crédito podem indicar roubo de cartão de crédito ou de identidade [Aleskerov et al. 1997] ou leituras anômalas de um sensor de nave espacial podem significar uma falha em algum componente da nave espacial [Fujimaki et al. 2005].

A detecção de outliers ou anomalias em dados tem sido estudada na comunidade estatística já no século XIX [Edgeworth 1887]. Ao longo do tempo, uma variedade de técnicas de detecção de anomalias foi desenvolvida em várias comunidades de pesquisa. Muitas dessas técnicas foram desenvolvidas especificamente para certos domínios de aplicação, enquanto outras são mais genéricas.

Esta pesquisa tenta fornecer uma visão geral estruturada e abrangente da pesquisa sobre detecção de anomalias. Esperamos que ela facilite uma melhor compreensão das diferentes direções em que a pesquisa foi feita sobre este tópico, e como as técnicas desenvolvidas em uma área podem ser aplicadas em domínios para os quais não foram planejadas inicialmente.

1.1 O que são anomalias?

Anomalias são padrões em dados que não estão em conformidade com uma noção bem definida de comportamento normal. A Figura 1 ilustra anomalias em um conjunto de dados bidimensional simples. Os dados têm duas regiões normais, N1 e N2, já que a maioria das observações está nessas duas regiões. Pontos que estão suficientemente distantes das regiões, por exemplo, pontos o1 e o2, e pontos na região O3, são anomalias.

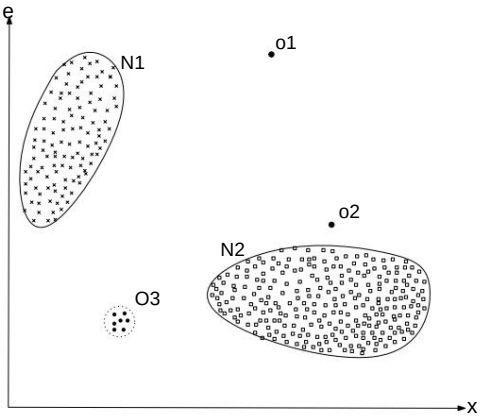


Fig. 1. Um exemplo simples de anomalias em um conjunto de dados bidimensionais.

Anomalias podem ser induzidas nos dados por uma variedade de razões, como atividade maliciosa, por exemplo, fraude de cartão de crédito, intrusão cibernética, atividade terrorista ou colapso de um sistema, mas todas as razões têm uma característica comum de que são interessantes para o analista. A “interesse” ou relevância da vida real das anomalias é uma característica fundamental da detecção de anomalias.

A detecção de anomalias está relacionada, mas é distinta da remoção de ruído [Teng et al. 1990] e da acomodação de ruído [Rousseeuw e Leroy 1987], ambas as quais lidam

com ruído indesejado nos dados. Ruído pode ser definido como um fenômeno em dados que não é de interesse do analista, mas atua como um obstáculo à análise de dados.
A remoção de ruído é motivada pela necessidade de remover os objetos indesejados antes que qualquer análise de dados seja realizada nos dados. Acomodação de ruído refere-se à imunização de uma estimativa de modelo estatístico contra observações anômalas [Huber 1974].

Outro tópico relacionado à detecção de anomalias é a detecção de novidades [Markou e Singh 2003a; 2003b; Saunders e Gero 2000], que visa detectar padrões não observados anteriormente (emergentes, novos) nos dados, por exemplo, um novo tópico de discussão em um grupo de notícias. A distinção entre novos padrões e anomalias é que os novos padrões são tipicamente incorporados ao modelo normal após serem detectados.

Vale ressaltar que as soluções para os problemas relacionados mencionados acima são frequentemente usadas para detecção de anomalias e vice-versa e, portanto, também são discutidas nesta análise.

1.2 Desafios Em um

nível abstrato, uma anomalia é definida como um padrão que não está em conformidade com o comportamento normal esperado. Uma abordagem direta de detecção de anomalias, portanto, é definir uma região que representa o comportamento normal e declarar qualquer observação nos dados que não pertença a essa região normal como uma anomalia. Mas vários fatores tornam essa abordagem aparentemente simples muito desafiadora:

—Definir uma região normal que engloba todo comportamento normal possível é muito difícil. Além disso, o limite entre comportamento normal e anômalo geralmente não é preciso. Assim, uma observação anômala que fica perto do limite pode realmente ser normal, e vice-versa.

—Quando anomalias são resultado de ações maliciosas, os adversários maliciosos geralmente se adaptam para fazer com que as observações anômalas pareçam normais, dificultando assim a tarefa de definir o comportamento normal.

—Em muitos domínios, o comportamento normal continua a evoluir e existe uma noção atual de normalidade. o comportamento pode não ser suficientemente representativo no futuro.

—A noção exata de uma anomalia é diferente para diferentes domínios de aplicação. Por exemplo, no domínio médico, um pequeno desvio do normal (por exemplo, flutuações na temperatura corporal) pode ser uma anomalia, enquanto um desvio semelhante no domínio do mercado de ações (por exemplo, flutuações no valor de uma ação) pode ser considerado normal. Portanto, aplicar uma técnica desenvolvida em um domínio a outro não é simples.

—Disponibilidade de dados rotulados para treinamento/validação de modelos usados por anomalia técnicas de detecção geralmente são um problema importante.

—Frequentemente os dados contêm ruído que tende a ser semelhante às anomalias reais e, portanto, é difícil de distinguir e remover.

Devido aos desafios acima, o problema de detecção de anomalias, em sua forma mais geral, não é fácil de resolver. Na verdade, a maioria das técnicas de detecção de anomalias existentes resolvem uma formulação específica do problema. A formulação é induzida por vários fatores, como a natureza dos dados, a disponibilidade de dados rotulados, o tipo de anomalias a serem detectadas, etc. Frequentemente, esses fatores são determinados pelo domínio de aplicação em

quais anomalias precisam ser detectadas. Pesquisadores adotaram conceitos de diversas disciplinas, como estatística, aprendizado de máquina, mineração de dados, teoria da informação, teoria espectral, e os aplicaram a formulações de problemas específicos.
A Figura 2 mostra os principais componentes mencionados acima associados a qualquer técnica de detecção de anomalias.

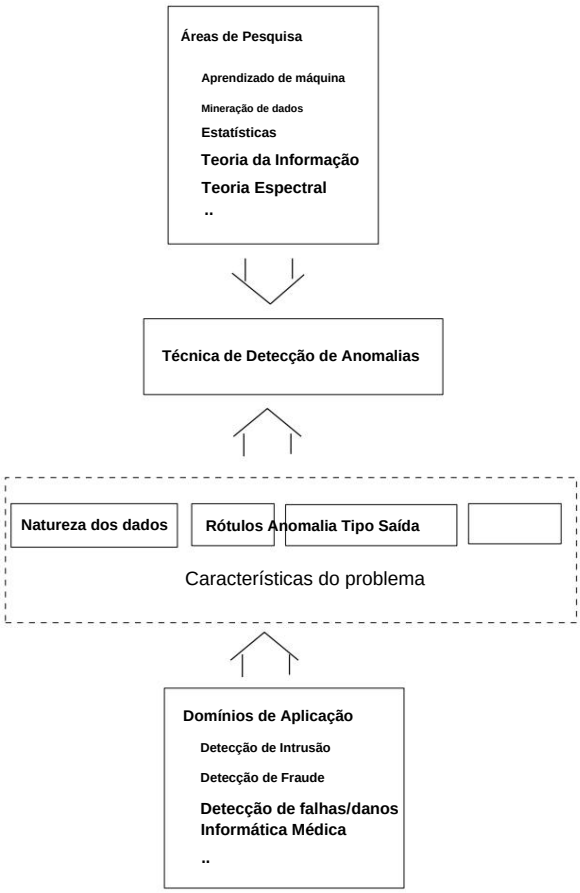


Fig. 2. Principais componentes associados a uma técnica de detecção de anomalias.

1.3 Trabalho relacionado

A detecção de anomalias tem sido o tópico de uma série de pesquisas e artigos de revisão, bem como livros. Hodge e Austin [2004] fornecem uma extensa pesquisa de técnicas de detecção de anomalias desenvolvidas em aprendizado de máquina e domínios estatísticos. Uma ampla revisão de técnicas de detecção de anomalias para dados numéricos e simbólicos é apresentada por Agyemang et al. [2006]. Uma extensa revisão de técnicas de detecção de novidades usando redes neurais e abordagens estatísticas foi apresentada em Markou e Singh [2003a] e Markou e Singh [2003b], respectivamente. Patcha e Park [2007] e Snyder [2001] apresentam uma pesquisa de técnicas de detecção de anomalias

usado especificamente para detecção de intrusão cibernética. Uma quantidade substancial de pesquisa sobre A detecção de outliers foi feita em estatística e foi revisada em vários livros
[Rousseeuw e Leroy 1987; Barnett e Lewis 1994; Hawkins 1980] bem como
outros artigos de pesquisa [Beckman e Cook 1983; Bakar et al. 2006].

A Tabela I mostra o conjunto de técnicas e domínios de aplicação abrangidos pelo nosso estudo
e os vários artigos de pesquisa relacionados mencionados acima.

		1	2	3	4	5	6	7	8
Técnicas	Classificação Baseada	ÿ	ÿ	ÿ	ÿ	ÿ	ÿ		ÿ
	Baseado em cluster								ÿ
	Vizinho mais próximo com base em	ÿ	ÿ	ÿ	ÿ	ÿ			ÿ ÿ
	Estatístico	ÿ						ÿ ÿ ÿ ÿ	
	Teórico da Informação	ÿ							
	Espectral	ÿ							
Aplicações	Detecção de intrusão cibernética								ÿ
	Detecção de Fraude	ÿ	ÿ						
	Detecção de anomalias médicas	ÿ							
	Detecção de Danos Industriais	ÿ							
	Processamento de Imagem	ÿ							
	Detecção de anomalias textuais	ÿ							
	Redes de Sensores	ÿ							

Tabela I. Comparação da nossa pesquisa com outros artigos de pesquisa relacionados.1 - Nossa pesquisa 2 - Hodge e Austin [2004], 3 - Agyemang et al. [2006], 4 - Markou e Singh [2003a], 5 - Markou e Singh [2003b], 6 - Patcha e Park [2007], 7 - Beckman e Cook [1983], 8 - Bakar et al [2006]

1.4 Nossas Contribuições

Este estudo é uma tentativa de fornecer uma visão geral estruturada e ampla de uma extensa
pesquisa sobre técnicas de detecção de anomalias abrangendo diversas áreas de pesquisa e
domínios de aplicação.

A maioria dos estudos existentes sobre detecção de anomalias concentra-se numa área específica
domínio de aplicação ou em uma única área de pesquisa. [Agyemang et al. 2006] e [Hodge
e Austin 2004] são dois trabalhos relacionados que agrupam a detecção de anomalias em múltiplos
categorias e discutir técnicas sob cada categoria. Esta pesquisa se baseia em
essas duas obras expandindo significativamente a discussão em diversas direções.

Adicionamos mais duas categorias de técnicas de detecção de anomalias, a saber, informação
técnicas teóricas e espectrais, para as quatro categorias discutidas em [Agyemang
et al. 2006] e [Hodge e Austin 2004]. Para cada uma das seis categorias, não
não apenas discutem as técnicas, mas também identificam suposições únicas sobre as
natureza das anomalias feitas pelas técnicas dessa categoria. Essas suposições
são essenciais para determinar quando as técnicas dessa categoria seriam capazes de
detectar anomalias e quando elas falhariam. Para cada categoria, fornecemos uma base
técnica de detecção de anomalias e, em seguida, mostrar como as diferentes técnicas existentes
essa categoria são variantes da técnica básica. Este modelo fornece uma maneira mais fácil
e compreensão sucinta das técnicas pertencentes a cada categoria. Além disso,
para cada categoria identificamos as vantagens e desvantagens das técnicas
nessa categoria. Também fornecemos uma discussão sobre a complexidade computacional de
as técnicas, pois é uma questão importante em domínios de aplicação reais.

Enquanto algumas das pesquisas existentes mencionam as diferentes aplicações da detecção de anomalias, fornecemos uma discussão detalhada dos domínios de aplicação onde técnicas de detecção de anomalias foram usadas. Para cada domínio, discutimos a noção de uma anomalia, os diferentes aspectos do problema de detecção de anomalias e os desafios enfrentados pelas técnicas de detecção de anomalias. Também fornecemos uma lista de técnicas que foram aplicadas em cada domínio de aplicação.

As pesquisas existentes discutem técnicas de detecção de anomalias que detectam a forma mais simples de anomalias. Nós distinguimos as anomalias simples das anomalias complexas. A discussão de aplicações de detecção de anomalias revela que, para a maioria dos domínios de aplicação, as anomalias interessantes são complexas por natureza, enquanto a maioria da pesquisa algorítmica se concentrou em anomalias simples.

1.5 Organização Esta

pesquisa é organizada em três partes e sua estrutura segue de perto a Figura 2. Na Seção 2, identificamos os vários aspectos que determinam a formulação do problema e destacamos a riqueza e a complexidade associadas à detecção de anomalias. Distinguimos anomalias simples de anomalias complexas e definimos dois tipos de anomalias complexas, a saber, anomalias contextuais e coletivas. Na Seção 3, descrevemos brevemente os diferentes domínios de aplicação onde a detecção de anomalias foi aplicada. Nas seções subsequentes, fornecemos uma categorização das técnicas de detecção de anomalias com base na área de pesquisa à qual pertencem. A maioria das técnicas pode ser categorizada em técnicas baseadas em classificação (Seção 4), baseadas no vizinho mais próximo (Seção 5), baseadas em agrupamento (Seção 6) e técnicas estatísticas (Seção 7). Algumas técnicas pertencem a áreas de pesquisa como teoria da informação (Seção 8) e teoria espectral (Seção 9). Para cada categoria de técnicas, também discutimos sua complexidade computacional para as fases de treinamento e teste. Na Seção 10, discutimos várias técnicas contextuais de detecção de anomalias. Discutimos várias técnicas coletivas de detecção de anomalias na Seção 11. Apresentamos algumas discussões sobre as limitações e o desempenho relativo de várias técnicas existentes na Seção 12. A Seção 13 contém observações finais.

2. DIFERENTES ASPECTOS DE UM PROBLEMA DE DETECÇÃO DE ANOMALIAS

Esta seção identifica e discute os diferentes aspectos da detecção de anomalias. Conforme mencionado anteriormente, uma formulação específica do problema é determinada por vários fatores diferentes, como a natureza dos dados de entrada, a disponibilidade (ou indisponibilidade) de rótulos, bem como as restrições e requisitos induzidos pelo domínio da aplicação. Esta seção traz à tona a riqueza no domínio do problema e justifica a necessidade do amplo espectro de técnicas de detecção de anomalias.

2.1 Natureza dos dados de

entrada Um aspecto fundamental de qualquer técnica de detecção de anomalias é a natureza dos dados de entrada. A entrada é geralmente uma coleção de instâncias de dados (também chamadas de objeto, registro, ponto, vetor, padrão, evento, caso, amostra, observação, entidade) [Tan et al. 2005, Capítulo 2]. Cada instância de dados pode ser descrita usando um conjunto de atributos (também chamados de variável, característica, recurso, campo, dimensão). Os atributos podem ser de diferentes tipos, como binário, categórico ou contínuo. Cada instância de dados pode consistir em apenas um atributo (univariado) ou múltiplos atributos (multivariados). Em

No caso de instâncias de dados multivariadas, todos os atributos podem ser do mesmo tipo ou podem ser uma mistura de diferentes tipos de dados.

A natureza dos atributos determina a aplicabilidade das técnicas de detecção de anomalias. Por exemplo, para técnicas estatísticas, diferentes modelos estatísticos devem ser usados para dados contínuos e categóricos. Da mesma forma, para técnicas baseadas no vizinho mais próximo, a natureza dos atributos determinaria a medida de distância a ser usada. Frequentemente, em vez dos dados reais, a distância em pares entre instâncias pode ser fornecida na forma de uma matriz de distância (ou similaridade). Nesses casos, técnicas que exigem instâncias de dados originais não são aplicáveis, por exemplo, muitas técnicas baseadas em estatística e classificação.

Dados de entrada também podem ser categorizados com base no relacionamento presente entre instâncias de dados [Tan et al. 2005]. A maioria das técnicas de detecção de anomalias existentes lida com dados de registro (ou dados de ponto), nos quais nenhum relacionamento é assumido entre as instâncias de dados.

Em geral, instâncias de dados podem ser relacionadas entre si. Alguns exemplos são dados de sequência, dados espaciais e dados de gráfico. Em dados de sequência, as instâncias de dados são ordenadas linearmente, por exemplo, dados de séries temporais, sequências de genoma, sequências de proteínas. Em dados espaciais, cada instância de dados é relacionada às suas instâncias vizinhas, por exemplo, dados de tráfego de veículos, dados ecológicos. Quando os dados espaciais têm um componente temporal (sequencial), eles são chamados de dados espaço-temporais, por exemplo, dados climáticos. Em dados de gráfico, as instâncias de dados são representadas como vértices em um gráfico e são conectadas a outros vértices com arestas. Mais adiante nesta seção, discutiremos situações em que tal relacionamento entre instâncias de dados se torna relevante para a detecção de anomalias.

2.2 Tipo de Anomalia Um

aspecto importante de uma técnica de detecção de anomalias é a natureza da anomalia desejada. Anomalias podem ser classificadas nas três categorias a seguir:

2.2.1 Anomalias de ponto. Se uma instância de dados individual pode ser considerada anômala em relação ao restante dos dados, então a instância é denominada anomalia de ponto. Este é o tipo mais simples de anomalia e é o foco da maioria das pesquisas sobre detecção de anomalias.

Por exemplo, na Figura 1, os pontos o1 e o2, bem como os pontos na região O3, ficam fora dos limites das regiões normais e, portanto, são anomalias de ponto, pois são diferentes dos pontos de dados normais.

Como um exemplo da vida real, considere a detecção de fraude de cartão de crédito. Deixe o conjunto de dados corresponder às transações de cartão de crédito de um indivíduo. Para simplificar, vamos supor que os dados sejam definidos usando apenas um recurso: valor gasto. Uma transação para a qual o valor gasto é muito alto em comparação com a faixa normal de gastos para essa pessoa será uma anomalia de ponto.

2.2.2 Anomalias contextuais. Se uma instância de dados for anômala em um contexto específico (mas não de outra forma), então ela é denominada anomalia contextual (também chamada de anomalia condicional [Song et al. 2007]).

A noção de um contexto é induzida pela estrutura no conjunto de dados e tem que ser especificada como parte da formulação do problema. Cada instância de dados é definida usando os dois conjuntos de atributos a seguir:

(1) Atributos contextuais. Os atributos contextuais são usados para determinar o contexto (ou vizinhança) para aquela instância. Por exemplo, em conjuntos de dados espaciais, a longitude e a latitude de um local são os atributos contextuais. Em dados de séries temporais, o tempo é um atributo contextual que determina a posição de uma instância na sequência inteira.

(2) Atributos comportamentais. Os atributos comportamentais definem as características não contextuais de uma instância. Por exemplo, em um conjunto de dados espaciais que descreve a precipitação média do mundo inteiro, a quantidade de precipitação em qualquer local é um atributo comportamental.

O comportamento anômalo é determinado usando os valores para os atributos comportamentais dentro de um contexto específico. Uma instância de dados pode ser uma anomalia contextual em um determinado contexto, mas uma instância de dados idêntica (em termos de atributos comportamentais) pode ser considerada normal em um contexto diferente. Essa propriedade é essencial para identificar atributos contextuais e comportamentais para uma técnica de detecção de anomalias contextuais.

Fig. 3. Anomalia contextual t2 em uma série temporal de temperatura. Note que a temperatura no tempo t1 é a mesma que no tempo t2 , mas ocorre em um contexto diferente e, portanto, não é considerada uma anomalia.

Anomalias contextuais têm sido mais comumente exploradas em dados de séries temporais [Weigend et al. 1995; Salvador e Chan 2003] e dados espaciais [Kou et al. 2006; Shekhar et al. 2001]. A Figura 3 mostra um exemplo para uma série temporal de temperatura que mostra a temperatura mensal de uma área nos últimos anos. Uma temperatura de 35F pode ser normal durante o inverno (no tempo t1) naquele lugar, mas o mesmo valor durante o verão (no tempo t2) seria uma anomalia.

Um exemplo semelhante pode ser encontrado no domínio de detecção de fraude de cartão de crédito. Um atributo contextual no domínio de cartão de crédito pode ser o momento da compra. Suponha que um indivíduo geralmente tenha uma conta de compras semanal de $ 100, exceto durante a semana do Natal, quando atinge $ 1.000. Uma nova compra de $ 1.000 em uma semana em julho será considerada uma anomalia contextual, pois não está em conformidade com o comportamento normal do indivíduo no contexto do tempo (embora o mesmo valor gasto durante a semana do Natal seja considerado normal).

A escolha de aplicar uma técnica de detecção de anomalias contextuais é determinada pela significância das anomalias contextuais no domínio da aplicação alvo.

Outro fator chave é a disponibilidade de atributos contextuais. Em vários casos definir um contexto é simples e, portanto, aplicar uma anomalia contextual técnica de detecção faz sentido. Em outros casos, definir um contexto não é fácil, dificultando a aplicação dessas técnicas.

2.2.3 Anomalias Coletivas. Se uma coleção de instâncias de dados relacionadas for anômala com relação ao conjunto de dados inteiro, é denominado como uma anomalia coletiva. As instâncias de dados individuais em uma anomalia coletiva podem não ser anomalias por si mesmas, mas sua ocorrência em conjunto como uma coleção é anômala. A Figura 4 ilustra uma exemplo que mostra uma saída de eletrocardiograma humano [Goldberger et al. 2000]. A região destacada denota uma anomalia porque o mesmo valor baixo existe para um tempo anormalmente longo (correspondendo a uma contração atrial prematura). Nota que esse valor baixo por si só não é uma anomalia.

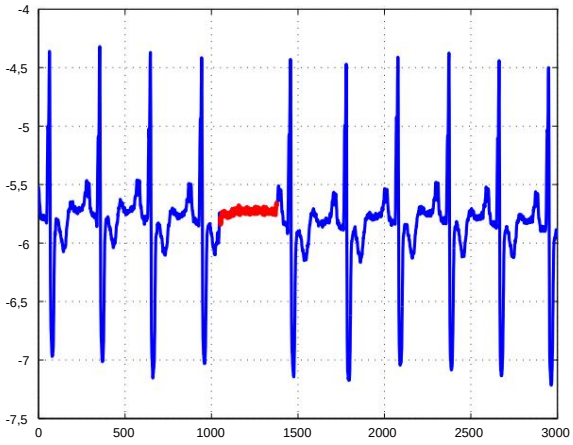


Fig. 4. Anomalia coletiva correspondente a uma Contração Atrial Prematura em um eletrocardiograma humano.

Como outro exemplo ilustrativo, considere uma sequência de ações que ocorrem em um computador conforme mostrado abaixo:

. . . http-web, estouro de buffer, http-web, http-web, smtp-mail, ftp, http-web, ssh, smtp-mail, http-web, ssh, estouro de buffer, ftp, http-web, ftp, smtp-mail,http-web . . .

A sequência de eventos destacada (buffer-overflow, ssh, ftp) corresponde a um ataque típico baseado na web por uma máquina remota seguido pela cópia de dados da computador host para destino remoto via ftp. Deve-se notar que esta coleção de eventos é uma anomalia, mas os eventos individuais não são anomalias quando ocorrem em outros locais na sequência.

Anomalias coletivas foram exploradas para dados de sequência [Forrest et al. 1999; Sun et al. 2006], dados gráficos [Noble e Cook 2003] e dados espaciais [Shekhar et al. [2001].

Deve-se notar que, embora anomalias pontuais possam ocorrer em qualquer conjunto de dados, anomalias coletivas podem ocorrer apenas em conjuntos de dados nos quais as instâncias de dados estão relacionadas. Em contraste, a ocorrência de anomalias contextuais depende da disponibilidade de atributos de contexto nos dados. Uma anomalia pontual ou uma anomalia coletiva também pode ser uma anomalia contextual se analisada com relação a um contexto. Assim, um problema de detecção de anomalia pontual ou problema de detecção de anomalia coletiva pode ser transformado em um problema de detecção de anomalia contextual ao incorporar as informações de contexto.

2.3 Rótulos de dados

Os rótulos associados a uma instância de dados denotam se essa instância é normal ou anômala[1]. Deve-se notar que obter dados rotulados que sejam precisos e representativos de todos os tipos de comportamentos, geralmente é proibitivamente caro.

A rotulagem é frequentemente feita manualmente por um especialista humano e, portanto, requer um esforço substancial para obter o conjunto de dados de treinamento rotulado. Normalmente, obter um conjunto rotulado de instâncias de dados anômalos que cubram todos os tipos possíveis de comportamento anômalo é mais difícil do que obter rótulos para comportamento normal. Além disso, o comportamento anômalo é frequentemente dinâmico por natureza, por exemplo, novos tipos de anomalias podem surgir, para os quais não há dados de treinamento rotulados. Em certos casos, como a segurança do tráfego aéreo, instâncias anômalas se traduziriam em eventos catastróficos e, portanto, serão muito cru.

Com base na extensão em que os rótulos estão disponíveis, as técnicas de detecção de anomalias podem operar em um dos três modos a seguir:

2.3.1 Detecção de anomalia supervisionada. Técnicas treinadas no modo supervisionado assumem a disponibilidade de um conjunto de dados de treinamento que tem instâncias rotuladas para classes normais e de anomalia. A abordagem típica em tais casos é construir um modelo preditivo para classes normais vs. de anomalia. Qualquer instância de dados não vista é comparada com o modelo para determinar a qual classe ela pertence. Existem dois problemas principais que surgem na detecção de anomalia supervisionada. Primeiro, as instâncias anômalas são muito menores em comparação com as instâncias normais nos dados de treinamento. Problemas que surgem devido a distribuições de classes desequilibradas foram abordados na literatura de mineração de dados e aprendizado de máquina [Joshi et al. 2001; 2002; Chawla et al. 2004; Phua et al. 2004; Weiss e Hirsh 1998; Vilalta e Ma 2002]. Segundo, obter rótulos precisos e representativos, especialmente para a classe de anomalias, geralmente é desafiador.

Várias técnicas foram propostas para injetar anomalias artificiais em um conjunto de dados normais para obter um conjunto de dados de treinamento rotulado [Theiler e Cai 2003; Abe et al. 2006; Steinwart et al. 2005]. Além dessas duas questões, o problema de detecção de anomalias supervisionadas é semelhante à construção de modelos preditivos. Portanto, não abordaremos essa categoria de técnicas nesta pesquisa.

2.3.2 Detecção de anomalias semi-supervisionadas. Técnicas que operam em um modo semi-supervisionado assumem que os dados de treinamento têm instâncias rotuladas somente para a classe normal. Como elas não exigem rótulos para a classe de anomalia, elas são mais amplamente aplicáveis do que técnicas supervisionadas. Por exemplo, na detecção de falhas em naves espaciais [Fujimaki et al. 2005], um cenário de anomalia significaria um acidente, o que não é fácil de modelar. A abordagem típica usada em tais técnicas é

[1]Também chamadas de classes normais e anômalas.

construa um modelo para a classe correspondente ao comportamento normal e use o modelo para identificar anomalias nos dados de teste.

Existe um conjunto limitado de técnicas de detecção de anomalias que assumem a disponibilidade apenas das instâncias de anomalias para treinamento [Dasgupta e Nino 2000; Dasgupta e Majumdar 2002; Forrest et al. 1996]. Tais técnicas não são comumente usadas, principalmente porque é difícil obter um conjunto de dados de treinamento que cubra todos os comportamentos anômalos possíveis que podem ocorrer nos dados.

2.3.3 Detecção de anomalias não supervisionadas. Técnicas que operam em modo não supervisionado não exigem dados de treinamento e, portanto, são mais amplamente aplicáveis. As técnicas nesta categoria fazem a suposição implícita de que instâncias normais são muito mais frequentes do que anomalias nos dados de teste. Se essa suposição não for verdadeira, essas técnicas sofrem de alta taxa de alarmes falsos.

Muitas técnicas semissupervisionadas podem ser adaptadas para operar em um modo não supervisionado usando uma amostra do conjunto de dados não rotulados como dados de treinamento. Tal adaptação pressupõe que os dados de teste contenham muito poucas anomalias e que o modelo aprendido durante o treinamento seja robusto a essas poucas anomalias.

2.4 Saída da Detecção de Anomalias Um

aspecto importante para qualquer técnica de detecção de anomalias é a maneira como as anomalias são relatadas. Normalmente, as saídas produzidas por técnicas de detecção de anomalias são um dos dois tipos a seguir:

2.4.1 Pontuações. Técnicas de pontuação atribuem uma pontuação de anomalia a cada instância nos dados de teste dependendo do grau em que essa instância é considerada uma anomalia.
Assim, a saída de tais técnicas é uma lista classificada de anomalias. Um analista pode escolher analisar as poucas anomalias principais ou usar um limite de corte para selecionar as anomalias.

2.4.2 Rótulos. Técnicas nesta categoria atribuem um rótulo (normal ou anômalo) a cada instância de teste.

Técnicas de detecção de anomalias baseadas em pontuação permitem que o analista use um limite específico de domínio para selecionar as anomalias mais relevantes. Técnicas que fornecem rótulos binários para as instâncias de teste não permitem diretamente que os analistas façam tal escolha, embora isso possa ser controlado indiretamente por meio de escolhas de parâmetros dentro de cada técnica.

3. APLICAÇÕES DE DETECÇÃO DE ANOMALIAS

Nesta seção, discutimos várias aplicações de detecção de anomalias. Para cada domínio de aplicação, discutimos os quatro aspectos a seguir:

—A noção de anomalia.

—Natureza dos dados.

—Desafios associados à detecção de anomalias.

—Técnicas de detecção de anomalias existentes.

3.1 Detecção de intrusão

A detecção de intrusão refere-se à detecção de atividades maliciosas (invasões, penetrações, e outras formas de abuso de computador) em um sistema relacionado a computador [Phoha 2002]. Essas atividades maliciosas ou intrusões são interessantes do ponto de vista da segurança do computador perspectiva. Uma intrusão é diferente do comportamento normal do sistema e portanto, técnicas de detecção de anomalias são aplicáveis no domínio de detecção de intrusão.

O principal desafio para a detecção de anomalias neste domínio é o enorme volume de dados. As técnicas de detecção de anomalias precisam ser computacionalmente eficientes para lidar com essas entradas de grande porte. Além disso, os dados geralmente vêm em um streaming moda, exigindo assim uma análise on-line. Outra questão que surge devido a a entrada de grande porte é a taxa de alarme falso. Como os dados somam milhões de objetos de dados, uma pequena porcentagem de alarmes falsos pode tornar a análise opressiva para um analista. Dados rotulados correspondentes ao comportamento normal geralmente estão disponíveis, enquanto rótulos para intrusões não são. Assim, anomalias semi-supervisionadas e não supervisionadas técnicas de detecção são preferidas neste domínio.

Denning [1987] classifica os sistemas de detecção de intrusão em sistemas de detecção de intrusão baseados em host e em sistemas de detecção de intrusão baseados em rede.

3.1.1 Sistemas de detecção de intrusão baseados em host. Tais sistemas (também chamados de como sistemas de detecção de intrusão de chamadas de sistema) lidam com rastreamentos de chamadas do sistema operacional. As intrusões são na forma de subsequências anômalas (anomalias coletivas) de os rastros. As subsequências anômalas se traduzem em programas maliciosos, comportamento não autorizado e violações de políticas. Embora todos os rastros contenham eventos pertencentes para o mesmo alfabeto, é a co-ocorrência de eventos que é o fator-chave em diferenciando entre comportamento normal e anômalo.

Os dados são sequenciais por natureza e o alfabeto consiste em sistemas individuais chamadas conforme mostrado na Figura 5. Essas chamadas podem ser geradas por programas [Hofmeyr et al. 1998] ou por usuários [Lane e Brodley 1999]. O alfabeto é geralmente grande (183 chamadas do sistema para o sistema operacional SunOS 4.1x). Diferentes programas executam estes chamadas de sistema em sequências diferentes. O comprimento da sequência para cada programa varia. A Figura 5 ilustra um conjunto de amostra de sequências de chamadas do sistema operacional. Uma chave característica dos dados neste domínio é que os dados podem ser tipicamente perfilados em diferentes níveis, como nível de programa ou nível de usuário. Técnicas de detecção de anomalias

abrir, ler, abrir,	mmap, mmap, abrir, ler, mmap . . .		
mmap, mmap, ler,	abrir, fechar,	abrir, fechar	. . .
fechar,	abrir,	abrir, mmap, fechar	. . .

Fig. 5. Um conjunto de dados de amostra composto por três rastreamentos de chamadas do sistema operacional.

aplicados para detecção de intrusão baseada em host são necessários para lidar com o sequencial natureza dos dados. Além disso, as técnicas de detecção de anomalias pontuais não são aplicáveis neste domínio. As técnicas devem modelar os dados da sequência ou calcular similaridade entre sequências. Um levantamento de diferentes técnicas utilizadas para este problema é apresentado por Snyder [2001]. Uma avaliação comparativa da detecção de anomalias para detecção de intrusão baseada em host apresentada em Forrest et al. [1996] e Dasgupta e

Técnica Utilizada	Seção	Referências
Perfil estatístico usando histogramas	Seção 7.2.1	Forrest et al [1996; 2004; 1996; 1994; 1999], Hofmeyr et al. [1998] Kosoresow e Hofmeyr [1997] Jagadish et al. [1999] Cabrera et al. [2001] Gonzalez e Dasgupta [2003] Das-gupta et al [2000; 2002] Ghosh et al [1999a; 1998; 1999b] Debar et al. [1998] Eskin et al. [2001]
		Marceau [2000] Endler [1998] Lane et al [1999; 1997b; 1997a]
Mistura de modelos	Seção 7.1.3	Eskin [2000]
Redes Neurais	Seção 4.1	Ghosh et al. [1998]
Máquinas de vetores de suporte	Seção 4.3	Hu et al. [2003] Heller et al. [2003]
Sistemas baseados em regras	Seção 4.4	Lee et al[1997; 1998; 2000]

Tabela II. Exemplos de técnicas de detecção de anomalias usadas para detecção de intrusão baseada em host.

Nino [2000]. Algumas técnicas de detecção de anomalias utilizadas neste domínio são mostradas na Tabela II.

3.1.2 Sistemas de Detecção de Intrusão de Rede. Esses sistemas lidam com a detecção de intrusões em dados de rede. As intrusões ocorrem tipicamente como padrões anômalos (anomalias pontuais), embora certas técnicas modelem os dados de forma sequencial e detectem subsequências anômalas (anomalias coletivas) [Gwadera et al. 2005b; 2004]. A principal razão para essas anomalias é devido aos ataques lançados por hackers externos que querem obter acesso não autorizado à rede para roubo de informações ou para interromper a rede. Uma configuração típica é uma grande rede de computadores que está conectada ao resto do mundo pela Internet.

Os dados disponíveis para sistemas de detecção de intrusão podem estar em diferentes níveis de granularidade, por exemplo, rastreamentos de nível de pacote, dados de fluxos de rede CISCO, etc. Os dados têm um aspecto temporal associado a eles, mas a maioria das técnicas normalmente não lida com o aspecto sequencial explicitamente. Os dados são de alta dimensão, normalmente com uma mistura de atributos categóricos e contínuos.

Um desafio enfrentado pelas técnicas de detecção de anomalias neste domínio é que a natureza das anomalias continua mudando ao longo do tempo, à medida que os intrusos adaptam seus ataques de rede para escapar das soluções de detecção de intrusão existentes.

Algumas técnicas de detecção de anomalias utilizadas neste domínio são mostradas na Tabela III.

3.2 Detecção de Fraude

Detecção de fraude refere-se à detecção de atividades criminosas que ocorrem em organizações comerciais, como bancos, empresas de cartão de crédito, agências de seguros, empresas de telefonia celular, mercado de ações, etc. Os usuários mal-intencionados podem ser os clientes reais da organização ou podem estar se passando por clientes (também conhecido como roubo de identidade).
A fraude ocorre quando esses usuários consomem os recursos fornecidos pela organização de forma não autorizada. As organizações estão interessadas na detecção imediata de tais fraudes para evitar perdas econômicas.

Fawcett e Provost [1999] introduzem o termo monitoramento de atividade como uma abordagem geral para detecção de fraudes nesses domínios. A abordagem típica de anomalia

Técnica Utilizada	Seção	Referências
Perfil estatístico usando histogramas	Seção 7.2.1	NIDES [Anderson et al. 1994; Anderson et al. 1995; Javitz e Valdes 1991], EMERALD [Porras e Neumann 1997], Yamanishi et al [2001; 2004], Ho et al. [1999], Kruegel et al. [2002; 2003], Mahoney e outros [2002; 2003; 2003; 2007], Sargor [1998]
Modelagem Estatística Paramétrica	Seção 7.1	Gwadera et al [2005b; 2004], Ye e Chen [2001]
Modelagem Estatística Não Paramétrica	Seção 7.2.2	Chow e Yeung [2002]
Redes Bayesianas	Seção 4.2	Siaterlis e Maglaris [2004], Sebyala et al. [2002], Valdes e Skinner [2000], Bronstein et al.
Redes Neurais	Seção 4.1	HIDE [Zhang et al. 2001], NSOM [Labib e Ve-muri 2002], Smith et al. [2002], Kruegel et al. [2003], Manikopoulos e Papa-pavassiliou [2002], Ramadas et al. [2003]
Máquinas de vetores de suporte	Seção 4.3	Eskin et al. [2002]
Sistemas baseados em regras	Seção 4.4	ADAM [Barbara et al. 2001a; Bárbara et al. 2003; Bárbara et al. 2001b], Fan et al. [2001], Helmer et al. [1998], Qin e Hwang [2004], Salvador e Chan [2003], Otey et al. [2003]
Baseado em cluster	Seção 6	ADMIT [Sequeira e Zaki 2002], Eskin et al. [2002], Wu e Zhang [2003], Otey et al. [2003]
Mais próximo Vizinho baseado	Seção 5	MENTES [Ertoz et al. 2004; Chandola et al. 2006], Eskin e outros [2002]
Espectral	Seção 9	Shyu et al. [2003], Lakhina et al. [2005], Thottan e Ji [2003],Sun et al. [2007]
Teo-Informação retículo	Seção 8	Lee e Xiang [2001], Noble e Cook [2003]

Tabela III. Exemplos de técnicas de detecção de anomalias utilizadas para detecção de intrusão de rede.

Técnica Utilizada	Seção	Referências
Redes Neurais	Seção 4.1	CARDWATCH [Aleskerov et al. 1997], Ghosh e Reilly [1994],Brause et al. [1999],Dorronsoro et al. [1997]
Sistemas baseados em regras	Seção 4.4	Brause et al. [1999]
Agrupamento	Seção 6	Bolton e Hand [1999]

Tabela IV. Exemplos de técnicas de detecção de anomalias utilizadas para detecção de fraudes em cartões de crédito.

técnicas de detecção é manter um perfil de uso para cada cliente e monitorar os perfis para detectar quaisquer desvios. Algumas das aplicações específicas de fraude detecção são discutidos abaixo.

3.2.1 Detecção de Fraude de Cartão de Crédito. Neste domínio, técnicas de detecção de anomalias são aplicadas para detectar solicitações fraudulentas de cartão de crédito ou cartões de crédito fraudulentos. uso de cartão (associado a roubos de cartão de crédito). Detectando fraudes de cartão de crédito aplicações é semelhante à detecção de fraudes em seguros [Ghosh e Reilly 1994].

Técnica Utilizada	Seção	Referências
Perfil estatístico usando histogramas	Seção 7.2.1	Fawcett e Provost [1999], Cox et al. [1997]
Estatística Paramétrica-Modelagem cal	Seção 7.1	Agarwal [2005], Scott [2001]
Redes Neurais	Seção 4.1	Barson et al. [1996],Taniguchi et al. [1998]
Sistemas baseados em regras	Seção 4.4	Phua et al. [2004],Taniguchi et al. [1998]

Tabela V. Exemplos de técnicas de detecção de anomalias utilizadas para detecção de fraudes em celulares.

Os dados normalmente compreendem registros definidos em várias dimensões, como ID do usuário, valor gasto, tempo entre usos consecutivos do cartão, etc. As fraudes normalmente são refletidas em registros transacionais (anomalias de pontos) e correspondem a pagamentos altos, compra de itens nunca comprados pelo usuário antes, alta taxa de compra, etc. As empresas de crédito têm dados completos disponíveis e também têm registros rotulados. Além disso, os dados se enquadram em perfis distintos com base no usuário do cartão de crédito. Portanto, técnicas baseadas em criação de perfil e agrupamento são normalmente usadas neste domínio.

O desafio associado à detecção do uso não autorizado de cartão de crédito é que ela exige a detecção on-line da fraude assim que a transação fraudulenta ocorre.

Técnicas de detecção de anomalias foram aplicadas de duas maneiras diferentes para resolver esse problema. A primeira é conhecida como by-owner, na qual cada usuário de cartão de crédito é perfilado com base em seu histórico de uso do cartão de crédito. Qualquer nova transação é comparada ao perfil do usuário e sinalizada como uma anomalia se não corresponder ao perfil. Essa abordagem é normalmente cara, pois requer a consulta de um repositório central de dados, toda vez que um usuário faz uma transação. Outra abordagem conhecida como by-operation detecta anomalias entre transações que ocorrem em uma localização geográfica específica. Ambas as técnicas by-user e by-operation detectam anomalias contextuais. No primeiro caso, o contexto é um usuário, enquanto no segundo caso, o contexto é a localização geográfica.

Algumas técnicas de detecção de anomalias usadas neste domínio estão listadas na Tabela IV.

3.2.2 Detecção de fraude em telefone celular. A detecção de fraude em celular/celular é um problema típico de monitoramento de atividade. A tarefa é escanear um grande conjunto de contas, examinando o comportamento de chamada de cada uma, e emitir um alarme quando uma conta parece ter sido mal utilizada.

A atividade de chamada pode ser representada de várias maneiras, mas geralmente é descrita com registros de chamada. Cada registro de chamada é um vetor de recursos, tanto contínuos (por exemplo, CALL-DURATION) quanto discretos (por exemplo, CALLING-CITY). No entanto, não há representação primitiva inerente neste domínio. As chamadas podem ser agregadas por tempo, por exemplo, em chamadas-horas ou chamadas-dias ou usuário ou área, dependendo da granularidade desejada. As anomalias correspondem a alto volume de chamadas ou chamadas feitas para destinos improváveis.

Algumas técnicas aplicadas à detecção de fraudes em celulares estão listadas na Tabela V.

3.2.3 Detecção de Fraude de Reivindicação de Seguro. Um problema importante no setor de seguros de propriedade e acidentes é a fraude de reivindicações, por exemplo, fraude de seguro de automóvel. Indivíduos e grupos conspiratórios de requerentes e provedores manipulam a reivindicação

sistema de processamento para reivindicações não autorizadas e ilegais. A detecção de tais fraudes tem sido muito importante para as empresas associadas evitarem perdas financeiras.

Os dados disponíveis neste domínio são os documentos apresentados pelos requerentes. As técnicas extraem diferentes características (tanto categóricas quanto contínuas) desses documentos. Normalmente, os ajustadores de sinistros e investigadores avaliam essas reivindicações em busca de fraudes. Esses casos investigados manualmente são usados como instâncias rotuladas por técnicas supervisionadas e semissupervisionadas para detecção de fraudes de seguros.

A detecção de fraudes em reivindicações de seguros é frequentemente tratada como um problema genérico de monitoramento de atividades [Fawcett e Provost 1999]. Técnicas baseadas em redes neurais também foram aplicadas para identificar reivindicações de seguros anômalas [He et al. 2003; Brockett et al. 1998].

3.2.4 Detecção de Insider Trading. Outra aplicação recente de técnicas de detecção de anomalias tem sido na detecção precoce de Insider Trading. Insider trading é um fenômeno encontrado em mercados de ações, onde as pessoas obtêm lucros ilegais agindo com (ou vazando) informações privilegiadas antes que elas sejam tornadas públicas. As informações privilegiadas podem ser de diferentes formas [Donoho 2004]. Pode se referir ao conhecimento de uma fusão/aquisição pendente, um ataque terrorista afetando uma indústria específica, uma legislação pendente afetando uma indústria específica ou qualquer informação que afetaria os preços das ações em uma indústria específica. Insider trading pode ser detectado identificando atividades comerciais anômalas no mercado.

Os dados disponíveis são de várias fontes heterogêneas, como dados de negociação de opções, dados de negociação de ações, notícias. Os dados têm associações temporais, pois são coletados continuamente. A natureza temporal e de streaming também foi explorada em certas técnicas [Aggarwal 2005].

Técnicas de detecção de anomalias neste domínio são necessárias para detectar fraudes on-line e o mais cedo possível, para evitar que pessoas/organizações obtenham lucros ilegais.

Algumas técnicas de detecção de anomalias usadas neste domínio estão listadas na Tabela VI.

Técnica Utilizada	Seção	Referências
Perfil estatístico usando histogramas	Seção 7.2.1	Donoho [2004],Aggarwal [2005]
Teo-Informação	Seção 8	Arning e outros [1996]
retículo		

Tabela VI. Exemplos de diferentes técnicas de detecção de anomalias usadas para detecção de negociação com informações privilegiadas.

3.3 Detecção de anomalias médicas e de saúde pública A detecção de anomalias nos domínios médico e de saúde pública normalmente funciona com registros de pacientes. Os dados podem ter anomalias devido a vários motivos, como condições anormais do paciente ou erros de instrumentação ou erros de registro. Várias técnicas também se concentraram na detecção de surtos de doenças em uma área específica [Wong et al. [2003]. Assim, a detecção de anomalias é um problema muito crítico neste domínio e requer alto grau de precisão.

Os dados geralmente consistem em registros que podem ter vários tipos diferentes de características, como idade do paciente, grupo sanguíneo, peso. Os dados também podem ter

Técnica Utilizada	Seção	Referências
Estatística Paramétrica-Modelagem cal	Seção 7.1	Horn et al. [2001],Laurikkala et al. [2000],Solberg e Lahti [2005],Roberts [2002],Suzuki et al. [2003]
Redes Neurais	Seção 4.1	Campbell e Bennett [2001]
Redes Bayesianas	Seção 4.2	Wong et al. [2003]
Sistemas baseados em regras	Seção 4.4	Aggarwal [2005]
Mais próximo Técnicas baseadas em vizinhos	Seção 5	Lin et al. [2005]

Tabela VII. Exemplos de diferentes técnicas de detecção de anomalias utilizadas no domínio médico e de saúde pública.

aspecto temporal e espacial. A maioria das técnicas atuais de detecção de anomalias neste domínio visa detectar registros anômalos (anomalias pontuais).
Normalmente, os dados rotulados pertencem aos pacientes saudáveis, portanto, a maioria das técnicas adota uma abordagem semissupervisionada. Outra forma de dados manipulados por técnicas de detecção de anomalias neste domínio são dados de séries temporais, como eletrocardiogramas (ECG) (Figura 4) e eletroencefalogramas (EEG). Técnicas coletivas de detecção de anomalias foram aplicadas para detectar anomalias em tais dados [Lin et al. 2005].

O aspecto mais desafiador do problema de detecção de anomalias neste domínio é que o custo de classificar uma anomalia como normal pode ser muito alto.

Algumas técnicas de detecção de anomalias usadas neste domínio estão listadas na Tabela VII.

3.4 Detecção de Danos Industriais

Unidades industriais sofrem danos devido ao uso contínuo e ao desgaste normal. Tais danos precisam ser detectados precocemente para evitar mais escalada e perdas. Os dados neste domínio são geralmente chamados de dados do sensor porque são registrados usando diferentes sensores e coletados para análise. Técnicas de detecção de anomalias têm sido amplamente aplicadas neste domínio para detectar tais danos.
A detecção de danos industriais pode ser classificada em dois domínios, um que lida com defeitos em componentes mecânicos, como motores, etc., e o outro que lida com defeitos em estruturas físicas. O primeiro domínio também é conhecido como gerenciamento de saúde do sistema.

3.4.1 Detecção de Falhas em Unidades Mecânicas. As técnicas de detecção de anomalias neste domínio monitoram o desempenho de componentes industriais, como motores, turbinas, fluxo de óleo em oleodutos ou outros componentes mecânicos e detectam defeitos que podem ocorrer devido ao desgaste ou outras circunstâncias imprevistas.

Os dados neste domínio têm tipicamente um aspecto temporal e a análise de séries temporais também é usada em algumas técnicas [Keogh et al. 2002; Keogh et al. 2006; Basu e Meckesheimer 2007]. As anomalias ocorrem principalmente por causa de uma observação em um contexto específico (anomalias contextuais) ou como uma sequência anômala de observações (anomalias coletivas).

Normalmente, dados normais (pertencentes a componentes sem defeitos) estão prontamente disponíveis e, portanto, técnicas semissupervisionadas são aplicáveis. Anomalias precisam ser detectadas de forma on-line, pois medidas preventivas precisam ser tomadas assim que uma anomalia ocorre.

Algumas técnicas de detecção de anomalias usadas neste domínio estão listadas na Tabela VIII.

Técnica Utilizada	Seção	Referências
Estatística Paramétrica- Modelagem cal	Seção 7.1	Guttormsson et al. [1999], Keogh et al [1997; 2002; [2006]
Modelagem Estatística Não Paramétrica	Seção 7.2.2	Desforges et al. [1998]
Redes Neurais	Seção 4.1	Bishop [1994], Campbell e Bennett [2001], Diaz e Hollmen [2002], Harris [1993], Jakubek e Strasser [2002], King e outros [2002], Li e outros [2002], Petsche et al. [1996], Streifel et al. [1996], Whitehead e Hoyt [1993]
Espectral	Seção 9	Parra et al. [1996],Fujimaki et al. [2005]
Sistemas baseados em regras	Seção 4.4	Yairi e outros [2001]

Tabela VIII. Exemplos de técnicas de detecção de anomalias utilizadas para detecção de falhas em unidades mecânicas.

Técnica Utilizada	Seção	Referências
Perfil estatístico usando histogramas	Seção 7.2.1	Manson [2002],Manson et al. [2001], Manson et al. [2000]
Modelagem Estatística Paramétrica	Seção 7.1	Ruotolo e Surace [1997]
Mistura de modelos	Seção 7.1.3	Hickinbotham et al [2000a; 2000b], Hollier e Austin [2002]
Redes Neurais	Seção 4.1	Brotherton et al [1998; 2001], Nairac et al [1999; 1997], Surace et al [1998; 1997], Sohn et al. [2001], Palavras [1997]

Tabela IX. Exemplos de técnicas de detecção de anomalias utilizadas para detecção de danos estruturais.

3.4.2 Detecção de defeitos estruturais. As técnicas de detecção de defeitos e danos estruturais detectam anomalias estruturais em estruturas, por exemplo, fissuras em vigas, tensões em fuselagens.

Os dados coletados neste domínio têm um aspecto temporal. A detecção de anomalias as técnicas são semelhantes às técnicas de detecção de novidades ou de detecção de pontos de mudança pois tentam detectar mudanças nos dados coletados de uma estrutura. O normal dados e, portanto, os modelos aprendidos são tipicamente estáticos ao longo do tempo. Os dados podem têm correlações espaciais.

Algumas técnicas de detecção de anomalias usadas neste domínio estão listadas na Tabela IX.

3.5 Processamento de Imagem

As técnicas de detecção de anomalias que lidam com imagens são de interesse de qualquer mudanças em uma imagem ao longo do tempo (detecção de movimento) ou em regiões que parecem anormais na imagem estática. Este domínio inclui imagens de satélite [Augusteijn e Folkert 2002; Byers e Raftery 1998; Torr e Murray 1993; Theiler e Cai 2003], reconhecimento de dígitos [Cun et al. 1990], espectroscopia [Chen et al. 2005; Davy e Godsill 2002; Hazel 2000; Scarth et al. 1995], imagem mamográfica análise [Spence et al. 2001; Tarassenko 1995] e vigilância por vídeo [Diehl e Hampshire 2002; Singh e Markou 2004; Pokrajac et al. 2007]. As anomalias são causado por movimento ou inserção de objeto estranho ou erros de instrumentação. Os dados tem características espaciais e temporais. Cada ponto de dados tem algumas continuidades

Técnica Utilizada	Seção	Referências
Mistura de modelos	Seção 7.1.3	Byers e Raftery [1998], Spence et al. [2001],Tarassenko [1995]
Regressão	Seção 7.1.2	Chen et al. [2005], Torr e Murray [1993]
Redes Bayesianas	Seção 4.2	Diehl e Hampshire [2002]
Máquinas de vetores de suporte	Seção 4.3	Davy e Godsill [2002], Song et al. [2002]
Redes Neurais	Seção 4.1	Augusteijn e Folkert [2002],Cun et al. [1990],Hazel [2000],Moya et al. [1993],Singh e Markou [2004]
Agrupamento	Seção 6	Scarth e outros [1995]
Mais próximo Vizinho	Seção 5	Pokrajac et al. [2007], Byers e Raftery [1998]
Técnicas baseadas		

Tabela X. Exemplos de técnicas de detecção de anomalias utilizadas no domínio do processamento de imagens.

Técnica Utilizada	Seção	Referências
Mistura de modelos	Seção 7.1.3	Baker et al. [1999]
Perfil estatístico usando histogramas	Seção 7.2.1	Fawcett e Provost [1999]
Máquinas de vetores de suporte	Seção 4.3	Manevitz e Yousef [2002]
Redes Neurais	Seção 4.1	Manevitz e Yousef [2000]
Baseado em cluster	Seção 6	Allan et al. [1998], Srivastava e Zane-Ulman [2005], Srivastava [2006]

Tabela XI. Exemplos de técnicas de detecção de anomalias usadas para detecção de tópicos anômalos em texto dados.

atributos estranhos como cor, leveza, textura, etc. As anomalias interessantes são pontos ou regiões anômalas nas imagens (anomalias pontuais e contextuais).

Um dos principais desafios neste domínio é o grande tamanho da entrada. Quando ao lidar com dados de vídeo, são necessárias técnicas de detecção de anomalias online.

Algumas técnicas de detecção de anomalias usadas neste domínio estão listadas na Tabela X.

3.6 Detecção de anomalias em dados de texto

As técnicas de detecção de anomalias neste domínio detectam principalmente novos tópicos ou eventos ou notícias em uma coleção de documentos ou artigos de notícias. As anomalias são causado devido a um novo evento interessante ou um tópico anômalo.

Os dados neste domínio são tipicamente de alta dimensão e muito esparsos. Os dados também tem um aspecto temporal, pois os documentos são coletados ao longo do tempo.

Um desafio para as técnicas de detecção de anomalias neste domínio é lidar com grandes variações em documentos pertencentes a uma categoria ou tópico.

Algumas técnicas de detecção de anomalias usadas neste domínio estão listadas na Tabela XI.

3.7 Redes de Sensores

As redes de sensores tornaram-se recentemente um importante tópico de pesquisa; mais de a perspectiva da análise de dados, uma vez que os dados dos sensores coletados de vários dispositivos sem fio sensores tem várias características únicas. Anomalias em dados coletados de um sensor

Técnica Utilizada	Seção	Referências
Redes Bayesianas	Seção 4.2	Janakiram et al. [2006]
Sistemas baseados em regras	Seção 4.4	Branch et al. [2006]
Estatística Paramétrica-Modelagem cal	Seção 7.1	Phuong et al. [2006], Du et al. [2006]
Mais próximo Vizinho	Seção 5	Subramaniam et al. [2006], Kejia Zhang e Li [2007], Id´e et al. [2007]
Técnicas baseadas Espectral	Seção 9	Chatzigiannakis et al. [2006]

Tabela XII. Exemplos de técnicas de detecção de anomalias utilizadas para detecção de anomalias em redes de sensores.

rede pode significar que um ou mais sensores estão com defeito ou estão detectando eventos (como intrusões) que são interessantes para analistas. Assim, a detecção de anomalias em redes de sensores podem capturar detecção de falhas de sensores ou detecção de intrusão ou ambas.

Uma única rede de sensores pode ser composta por sensores que coletam diferentes tipos de dados, como binários, discretos, contínuos, áudio, vídeo, etc. Os dados são gerados em um modo de streaming. Muitas vezes, o ambiente em que os vários sensores estão implantado, bem como o canal de comunicação, induz ruído e valores ausentes nos dados coletados.

A detecção de anomalias em redes de sensores apresenta um conjunto de desafios únicos. técnicas de detecção de anomalias são necessárias para operar em uma abordagem online. Devido para severas restrições de recursos, as técnicas de detecção de anomalias precisam ser leves. Outro desafio é que os dados são coletados de forma distribuída e portanto, uma abordagem de mineração de dados distribuída é necessária para analisar os dados [Chatzi-giannakis et al. 2006]. Além disso, a presença de ruído nos dados coletados do sensor torna a detecção de anomalias mais desafiadora, pois agora ele precisa distinguir entre anomalias interessantes e ruído indesejado/valores ausentes.

A Tabela XII lista algumas técnicas de detecção de anomalias usadas neste domínio.

3.8 Outros Domínios

A detecção de anomalias também foi aplicada a vários outros domínios, como a fala reconhecimento [Albrecht et al. 2000; Emamian et al. 2000], detecção de novidades em robôs comportamento [Crook e Hayes 2001; Crook et al. 2002; Marsland et al. 1999; 2000b; 2000a], monitoramento de tráfego [Shekhar et al. 2001], proteção de cliques [Ihler et al. 2006], detectando falhas em aplicações web [Ide e Kashima 2004; Sun et al. 2005], detecção de anomalias em dados biológicos [Kadota et al. 2003; Sun et al. 2006; Gwadera et al. 2005a; MacDonald e Ghosh 2007; Tomlins et al. 2005; Tibshirani e Hastie 2007], detectando anomalias em dados censitários [Lu et al. 2003], detectando associações entre atividades criminosas [Lin e Brown 2003], detectando anomalias no Atendimento ao Cliente Dados de Gestão de Relacionamento (CRM) [He et al. 2004b], detectando anomalias em dados astronômicos [Dutta et al. 2007; Escalante 2005; Protopapas et al. 2006] e detecção de perturbações do ecossistema [Blender et al. 1997; Kou et al. 2006; Sun e [Châwla 2004].

4. TÉCNICAS DE DETECÇÃO DE ANOMALIAS COM BASE NA CLASSIFICAÇÃO

A classificação [Tan et al. 2005; Duda et al. 2000] é usada para aprender um modelo (classificador) de um conjunto de instâncias de dados rotuladas (treinamento) e, em seguida, classificar uma instância de teste em

uma das classes usando o modelo aprendido (teste). Técnicas de detecção de anomalias baseadas em classificação operam de forma semelhante em duas fases. A fase de treinamento aprende um classificador usando os dados de treinamento rotulados disponíveis. A fase de teste classifica uma instância de teste como normal ou anômala usando o classificador.

As técnicas de detecção de anomalias baseadas em classificação operam sob os seguintes suposição geral:

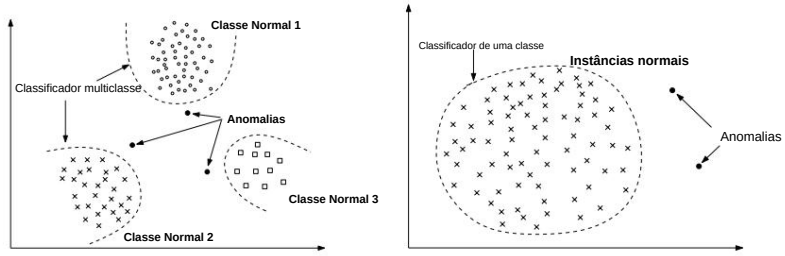
Suposição: Um classificador que pode distinguir entre classes normais e anômalas pode ser aprendido no espaço de características fornecido.

Com base nos rótulos disponíveis para a fase de treinamento, as técnicas de detecção de anomalias baseadas em classificação podem ser agrupadas em duas grandes categorias: técnicas de detecção de anomalias multiclasse e de classe única.

Técnicas de detecção de anomalias baseadas em classificação multiclasse assumem que os dados de treinamento contêm instâncias rotuladas pertencentes a múltiplas classes normais [Ste-fano et al. 2000; Barbara et al. 2001b]. Tais técnicas de detecção de anomalias aprendem um classificador para distinguir entre cada classe normal em relação ao restante das classes.

Veja a Figura 6(a) para ilustração. Uma instância de teste é considerada anômala se não for classificada como normal por nenhum dos classificadores. Algumas técnicas nesta subcategoria associam uma pontuação de confiança com a previsão feita pelo classificador. Se nenhum dos classificadores estiver confiante em classificar a instância de teste como normal, a instância é declarada anômala.

Técnicas de detecção de anomalias baseadas em classificação de uma classe assumem que todas as instâncias de treinamento têm apenas um rótulo de classe. Tais técnicas aprendem um limite discriminativo em torno das instâncias normais usando um algoritmo de classificação de uma classe, por exemplo, SVMs de uma classe [Sch¨olkopf et al. 2001], Kernel Fisher Discriminants de uma classe [Roth 2004; 2006], conforme mostrado na Figura 6(b). Qualquer instância de teste que não caia dentro do limite aprendido é declarada como anômala.



(a) Detecção de anomalias multiclasse (b) Detecção de anomalias de uma classe

Fig. 6. Usando classificação para detecção de anomalias.

Nas subseções a seguir, discutiremos uma variedade de técnicas de detecção de anomalias que usam diferentes algoritmos de classificação para construir classificadores:

4.1 Baseado em Redes Neurais

Redes neurais têm sido aplicadas à detecção de anomalias em ambientes multiclasse e também em ambientes de uma classe.

Referências de Rede Neural Usadas	
Perceptrons multicamadas	[Augusteijn e Folkert 2002; Cun et al. 1990; Sykacek 1997; Ghosh et al. 1999a; Ghosh et al. 1998; Barson et al. 1996; Ele e outros. 1997; Nairac et al. 1997; Hick-inbotham e Austin 2000b; Vasconcelos et al. 1995; 1994]
Árvores Neurais	[Martinez 1998]
Redes autoassociativas	[Aeyels 1991; Byungho e Sungzoon 1999; Japkow-icz et al. 1995; Hawkins et al. 2002; Ko e Jacyna 2000; Manevitz e Yousef 2000; Petsche et al. 1996; Sohn et al. 2001; Song et al. 2001; Streifel et al. 1996; Thompson et al. 2002; Worden 1997; Williams et al. 2002; Diaz e Hollmen 2002]
Baseado na Teoria da Ressonância Adaptativa	[Moya et al. 1993; Dasgupta e Nino 2000; Caudell e Newman 1993]
Função de base radial baseada em	[Albrecht et al. 2000; Bishop 1994; Brotherton et al. 1998; Brotherton e Johnson 2001; Li e outros 2002; Nairac e outros 1999; Nairac e outros 1997; Ghosh e Reilly 1994; Jakubek e Strasser 2002]
Redes Hopfield	[Jagota 1991; Crook e Hayes 2001; Crook et al. 2002; Addison et al. 1999; Murray 2001]
Redes oscilatórias	[Ho e Rouat 1997; 1998; Kojima e Ito 1999; Borisyuk et al. 2000; Martinelli e Perfetti 1994]

Tabela XIII. Alguns exemplos de técnicas de detecção de anomalias baseadas em classificação usando redes neurais.

Uma técnica básica de detecção de anomalias multiclasse usando redes neurais opera em duas etapas. Primeiro, uma rede neural é treinada nos dados de treinamento normais para aprender as diferentes classes normais. Segundo, cada instância de teste é fornecida como uma entrada para a rede neural. Se a rede aceitar a entrada de teste, ela é normal e se a rede rejeitar uma entrada de teste, ela é uma anomalia [Stefano et al. 2000; Odin e Addison 2000]. Várias variantes da técnica básica de rede neural foram propostas que usam diferentes tipos de redes neurais, conforme resumido na Tabela XIII.

Redes neurais replicadoras têm sido usadas para detecção de anomalias de uma classe [Hawkins et al. 2002; Williams et al. 2002]. Uma rede neural de feed forward multicamadas é construída que tem o mesmo número de neurônios de entrada e saída (correspondentes aos recursos nos dados). O treinamento envolve a compressão de dados em três camadas ocultas. A fase de teste envolve a reconstrução de cada instância de dados xi usando a rede aprendida para obter a saída reconstruída oi . O erro de reconstrução ÿi para a instância de teste xi é então computado como:

$$ÿi = \frac{1}{n} \sum_{j=1}^{não} (xij ÿ oij)^2$$

onde n é o número de características sobre as quais os dados são definidos. O erro de reconstrução ÿi é usado diretamente como uma pontuação de anomalia para a instância de teste.

4.2 Redes Bayesianas Redes

Bayesianas baseadas em redes Bayesianas têm sido usadas para detecção de anomalias em ambientes multiclasse.

Uma técnica básica para um conjunto de dados categóricos univariados usando uma rede bayesiana ingênua estima a probabilidade posterior de observar um rótulo de classe (de um conjunto

de rótulos de classe normais e do rótulo de classe de anomalia), dada uma instância de dados de teste. O rótulo de classe com o maior posterior é escolhido como a classe prevista para a instância de teste fornecida. A probabilidade de observar a instância de teste dada uma classe, e o prior nas probabilidades de classe, são estimados a partir do conjunto de dados de treinamento. As probabilidades zero, especialmente para a classe de anomalia, são suavizadas usando Laplace Smoothing.

A técnica básica pode ser generalizada para conjuntos de dados categóricos multivariados agregando as probabilidades posteriores por atributo para cada instância de teste e usando o valor agregado para atribuir um rótulo de classe à instância de teste.

Várias variantes da técnica básica foram propostas para detecção de intrusão de rede [Barbara et al. 2001b; Sebyala et al. 2002; Valdes e Skinner 2000; Mingming 2000; Bronstein et al. 2001], para detecção de novidades em vigilância por vídeo [Diehl e Hampshire 2002], para detecção de anomalias em dados de texto [Baker et al. 1999] e para detecção de surtos de doenças [Wong et al. 2002; 2003].

A técnica básica descrita acima assume independência entre os diferentes atributos. Várias variações da técnica básica foram propostas para capturar as dependências condicionais entre os diferentes atributos usando redes bayesianas mais complexas [Siaterlis e Maglaris 2004; Janakiram et al. 2006; Das e Schneider 2007].

4.3 Máquinas de Vetor de Suporte Baseadas

em Máquinas de Vetor de Suporte (SVMs) [Vapnik 1995] foram aplicadas à detecção de anomalias no cenário de uma classe. Tais técnicas usam técnicas de aprendizado de uma classe para SVM [Ratsch et al. 2002] e aprendem uma região que contém as instâncias de dados de treinamento (um limite). Kernels, como o kernel de função de base radial (RBF), podem ser usados para aprender regiões complexas. Para cada instância de teste, a técnica básica determina se a instância de teste cai dentro da região aprendida. Se uma instância de teste cai dentro da região aprendida, ela é declarada como normal, caso contrário, é declarada como anômala.

Variantes da técnica básica foram propostas para detecção de anomalias em dados de sinais de áudio [Davy e Godsill 2002], detecção de novidades em usinas de geração de energia [King et al. 2002] e detecção de intrusão de chamada de sistema [Eskin et al. 2002; Heller et al. 2003; Lazarevic et al. 2003]. A técnica básica também foi estendida para detectar anomalias em sequências temporais [Ma e Perkins 2003a; 2003b].

Uma variante da técnica básica [Tax e Duin 1999a; 1999b; Tax 2001] encontra a menor hiperesfera no espaço do kernel, que contém todas as instâncias de treinamento, e então determina de que lado dessa hiperesfera uma instância de teste está. Se uma instância de teste estiver fora da hiperesfera, ela é declarada anômala.

Song et al. [2002] usam Robust Support Vector Machines (RSVM) que são robustas à presença de anomalias nos dados de treinamento. RSVM foram aplicadas à detecção de intrusão de chamada de sistema [Hu et al. 2003].

4.4 Baseado em regras

Técnicas de detecção de anomalias baseadas em regras aprendem regras que capturam o comportamento normal de um sistema. Uma instância de teste que não é coberta por nenhuma dessas regras é considerada uma anomalia. Técnicas baseadas em regras foram aplicadas em configurações multiclasse e de uma classe.

Uma técnica básica baseada em regras multiclasse consiste em duas etapas. A primeira etapa é

aprenda regras a partir dos dados de treinamento usando um algoritmo de aprendizado de regras, como RIPPER, Decision Trees, etc. Cada regra tem um valor de confiança associado que é proporcional à razão entre o número de instâncias de treinamento corretamente classificadas pela regra e o número total de instâncias de treinamento cobertas pela regra. O segundo passo é encontrar, para cada instância de teste, a regra que melhor captura a instância de teste. O inverso da confiança associada à melhor regra é a pontuação de anomalia da instância de teste. Várias variantes menores da técnica básica baseada em regras foram propostas [Fan et al. 2001; Helmer et al. 1998; Lee et al. 1997; Salvador e Chan 2003; Teng et al. 1990].

A mineração de regras de associação [Agrawal e Srikant 1995] tem sido usada para detecção de anomalias de uma classe, gerando regras a partir dos dados de forma não supervisionada. Regras de associação são geradas a partir de um conjunto de dados categóricos. Para garantir que as regras correspondam a padrões fortes, um limite de suporte é usado para podar regras com baixo suporte [Tan et al. 2005]. Técnicas baseadas em mineração de regras de associação têm sido usadas para detecção de intrusão de rede [Mahoney e Chan 2002; 2003; Mahoney et al. 2003; Tandon e Chan 2007; Barbara et al. 2001a; Otey et al. 2003], detecção de intrusão de chamada de sistema [Lee et al. 2000; Lee e Stolfo 1998; Qin e Hwang 2004], detecção de fraude de cartão de crédito [Brause et al. 1999] e detecção de fraude em dados de manutenção de espaçonaves [Yairi et al. 2001]. Conjuntos de itens frequentes são gerados na etapa intermediária dos algoritmos de mineração de regras de associação. [2004a] propõe um algoritmo de detecção de anomalias para conjuntos de dados categóricos nos quais a pontuação de anomalia de uma instância de teste é igual ao número de conjuntos de itens frequentes em que ocorre.

Complexidade Computacional A
complexidade computacional de técnicas baseadas em classificação depende do algoritmo de classificação que está sendo usado. Para uma discussão sobre a complexidade de classificadores de treinamento, veja Kearns [1990]. Geralmente, árvores de decisão de treinamento tendem a ser mais rápidas, enquanto técnicas que envolvem otimização quadrática, como SVMs, são mais caras, embora SVMs de tempo linear [Joachims 2006] tenham sido propostas com tempo de treinamento linear. A fase de teste de técnicas de classificação é geralmente muito rápida, pois a fase de teste usa um modelo aprendido para classificação.

Vantagens e desvantagens das técnicas baseadas em classificação
As vantagens das técnicas baseadas em classificação são as seguintes:

(1) As técnicas baseadas em classificação, especialmente as técnicas multiclasse, podem fazer uso de algoritmos poderosos que podem distinguir entre instâncias pertencentes a classes diferentes.

(2) A fase de teste das técnicas baseadas em classificação é rápida, pois cada instância de teste precisa ser comparada com o modelo pré-calculado.

As desvantagens das técnicas baseadas em classificação são as seguintes:

(1) As técnicas de classificação multiclasse dependem da disponibilidade de rótulos precisos para várias classes normais, o que muitas vezes não é possível.

(2) Técnicas baseadas em classificação atribuem um rótulo a cada instância de teste, o que também pode se tornar uma desvantagem quando uma pontuação de anomalia significativa é desejada para as instâncias de teste. Algumas técnicas de classificação que obtêm uma probabilidade

a pontuação de previsão da saída de um classificador pode ser usada para resolver esse problema [Platt 2000].

5. TÉCNICAS DE DETECÇÃO DE ANOMALIA COM BASE NO VIZINHO MAIS PRÓXIMO O conceito de análise do vizinho mais próximo tem sido usado em várias técnicas de detecção de anomalias. Tais técnicas são baseadas na seguinte suposição-chave:

Suposição: Instâncias de dados normais ocorrem em vizinhanças densas, enquanto anomalias ocorrem longe de seus vizinhos mais próximos.

Técnicas de detecção de anomalias baseadas em vizinho mais próximo requerem uma medida de distância ou similaridade definida entre duas instâncias de dados. A distância (ou similaridade) entre duas instâncias de dados pode ser computada de diferentes maneiras. Para atributos contínuos, a distância euclidiana é uma escolha popular, mas outras medidas podem ser usadas [Tan et al. 2005, Capítulo 2]. Para atributos categóricos, o coeficiente de correspondência simples é frequentemente usado, mas medidas de distância mais complexas podem ser usadas [Boriah et al. 2008; Chandola et al. 2008]. Para instâncias de dados multivariados, a distância ou similaridade é geralmente computada para cada atributo e então combinada [Tan et al. 2005, Capítulo 2].

A maioria das técnicas que serão discutidas nesta seção, bem como as técnicas baseadas em clustering (Seção 6) não exigem que a medida de distância seja estritamente métrica. As medidas são tipicamente necessárias para serem positivas-definidas e simétricas, mas não são necessárias para satisfazer a desigualdade triangular.

As técnicas de detecção de anomalias baseadas no vizinho mais próximo podem ser amplamente agrupadas em duas categorias: (1)

Técnicas que usam a distância de uma instância de dados ao seu k como a pontuação de anomalia.

(2) Técnicas que calculam a densidade relativa de cada instância de dados para calcular sua pontuação de anomalia.

Além disso, existem algumas técnicas que usam a distância entre instâncias de dados de uma maneira diferente para detectar anomalias e serão brevemente discutidas mais tarde.

5.1 Usando Distância para k Uma técnica básica de detecção de anomalias de vizinho mais próximo é baseada na seguinte definição – A pontuação de anomalia de uma instância de dados é definida como sua distância para seu th k vizinho mais próximo em um determinado conjunto de dados. Esta técnica básica foi aplicada para detectar minas terrestres a partir de imagens terrestres de satélite [Byers e Raftery 1998] e para detectar espiras em curto (anomalias) nos enrolamentos de campo CC de grandes geradores de turbina síncronos [Guttormsson et al. 1999]. No último artigo, os autores usam k = 1. Normalmente, um limite é então aplicado na pontuação de anomalia para determinar se uma instância de teste é anômala ou não. Ramaswamy et al. [2000], por outro lado, selecionam n instâncias com as maiores pontuações de anomalia como anomalias.

o Vizinho mais próximo

A técnica básica foi estendida por pesquisadores de três maneiras diferentes. O primeiro conjunto de variantes modifica a definição acima para obter a pontuação de anomalia de uma instância de dados. O segundo conjunto de variantes usa diferentes medidas de distância/similaridade para lidar com diferentes tipos de dados. O terceiro conjunto de variantes foca em melhorar a eficiência da técnica básica (a complexidade da técnica básica é O(N2), onde N é o tamanho dos dados) de diferentes maneiras.

Eskin et al. [2002], Angiulli e Pizzuti [2002] e Zhang e Wang [2006] calculam a pontuação de anomalia de uma instância de dados como a soma de suas distâncias de seus k vizinhos mais próximos. Uma técnica semelhante foi aplicada para detectar fraudes de cartão de crédito por [Bolton e Hand 1999] chamada Análise de Grupo de Pares.

Uma maneira diferente de calcular a pontuação de anomalia de uma instância de dados é contar o número de vizinhos mais próximos (n) que não estão a mais de d de distância da instância de dados fornecida [Knorr e Ng 1997; 1998; 1999; Knorr et al. 2000]. Este método também pode ser visto como uma estimativa da densidade global para cada instância de dados, pois envolve a contagem do número de vizinhos em uma hiperesfera de raio d.
Por exemplo, em um conjunto de dados 2-D, a densidade de uma instância de dados $= \frac{\text{não}}{\pi d^2}$. O inverso da densidade é a pontuação de anomalia para a instância de dados. Em vez de calcular a densidade real, várias técnicas fixam o raio d e usam como pontuação de anomalia, enquanto $\frac{1}{\text{não}}$ várias técnicas fixam n e usam como pontuação de anomalia. $\frac{1}{\text{dia}}$

Embora a maioria das técnicas discutidas nesta categoria até agora tenham sido propostas para lidar com atributos contínuos, várias variantes foram propostas para lidar com outros tipos de dados. Uma técnica baseada em hipergráfico é proposta por [Wei et al. 2003] chamada HOT, onde os autores modelam os valores categóricos usando um hipergráfico e medem a distância entre duas instâncias de dados analisando a conectividade do gráfico. Uma medida de distância para dados contendo uma mistura de atributos categóricos e contínuos foi proposta para detecção de anomalias [Otey et al. 2006]. Os autores definem links entre duas instâncias adicionando distância para atributos categóricos e contínuos separadamente. Para atributos categóricos, o número de atributos para os quais as duas instâncias têm os mesmos valores define a distância entre eles. Para atributos contínuos, uma matriz de covariância é mantida para capturar as dependências entre os valores contínuos. Palshikar [2005] adapta a técnica proposta em [Knorr e Ng 1999] para sequências contínuas. Kou et al. [2006] estendem a técnica proposta em [Ramaswamy et al. 2000] para dados espaciais.

Várias variantes da técnica básica foram propostas para melhorar a eficiência. Algumas técnicas podam o espaço de busca ignorando instâncias que não podem ser anômalas ou focando em instâncias que têm mais probabilidade de ser anômalas. Bay e Schwabacher [2003] mostram que, para dados suficientemente randomizados, uma etapa de poda simples pode resultar na complexidade média da busca do vizinho mais próximo para ser quase linear. Após calcular os vizinhos mais próximos para uma instância de dados, o algoritmo define o limite de anomalia para qualquer instância de dados para a pontuação da anomalia mais fraca encontrada até o momento. Usando esse procedimento de poda, a técnica descarta instâncias que são próximas e, portanto, não interessantes.

Ramaswamy et al. [2000] propõem uma técnica baseada em partição, que primeiro agrupa as instâncias e calcula limites inferiores e superiores na distância de uma instância de seu vizinho mais próximo k para instâncias em cada partição. Essas informações são então usadas para identificar as partições que não podem conter as anomalias k superiores; tais partições são podadas. As anomalias são então computadas das instâncias restantes (pertencentes a partições não podadas) em uma fase final. Uma poda baseada em cluster semelhante foi proposta por Eskin et al. [2002], McCallum et al. [2000], Ghoting et al. [2006] e Tao et al. [2006].

Wu e Jermaine [2006] usam amostragem para melhorar a eficiência da técnica baseada no vizinho mais próximo. Os autores calculam o vizinho mais próximo de cada

instância dentro de uma amostra menor do conjunto de dados. Assim, a complexidade da técnica proposta é reduzida a O(MN) onde M é o tamanho da amostra escolhido.

Para podar o espaço de busca para vizinhos mais próximos, várias técnicas particionam o espaço de atributos em uma hipergrade consistindo de hipercubos de tamanhos fixos. A intuição por trás dessas técnicas é que se um hipercubo contém muitas instâncias, essas instâncias provavelmente serão normais. Além disso, se para uma instância dada, o hipercubo que contém a instância e seus hipercubos adjacentes contiverem muito poucas instâncias, a instância dada provavelmente será anômala. Técnicas baseadas nessa intuição foram propostas por Knorr e Ng [1998]. Angiulli e Pizzuti [2002] estendem linearizando o espaço de busca através da curva de preenchimento do espaço de Hilbert. O conjunto de dados d-dimensionais é ajustado em um hipercubo D = [0, 1]d . Este hipercubo é então mapeado para o intervalo I = [0, 1] usando a Curva de Preenchimento do Espaço de Hilbert e os k-vizinhos mais próximos de uma instância de dados são obtidos examinando seus sucessores e predecessores em I.

5.2 Usando Densidade Relativa

Técnicas de detecção de anomalias baseadas em densidade estimam a densidade da vizinhança de cada instância de dados. Uma instância que fica em uma vizinhança com baixa densidade é declarada anômala, enquanto uma instância que fica em uma vizinhança densa é declarada normal.

Para uma determinada instância de dados, a distância até seu k^{o} vizinho mais próximo é equivalente ao raio de uma hiperesfera, centralizada na instância de dados dada, que contém k outras instâncias. Assim, a distância até o k vizinho mais próximo para uma instância dados dada pode ser vista como uma estimativa do inverso da densidade da instância no conjunto de dados e a técnica básica baseada no vizinho mais próximo descrita na subseção anterior pode ser considerada como uma técnica de detecção de anomalias baseada na densidade.

Técnicas baseadas em densidade têm desempenho ruim se os dados tiverem regiões de densidades variadas. Por exemplo, considere um conjunto de dados bidimensional mostrado na Figura 7. Devido à baixa densidade do cluster C1, é aparente que para cada instância q dentro do cluster C1, a distância entre a instância q e seu vizinho mais próximo é maior do que a distância entre a instância p2 e o vizinho mais próximo do cluster C2, e a instância p2 não será considerada uma anomalia. Portanto, a técnica básica não conseguirá distinguir entre p2 e instâncias em C1. No entanto, a instância p1 pode ser detectada.

Para lidar com a questão das densidades variáveis no conjunto de dados, um conjunto de técnicas foi proposto para calcular a densidade de instâncias em relação à densidade de seus vizinhos.

Breunig et al [1999; 2000] atribuem uma pontuação de anomalia a uma instância de dados dada, conhecida como Fator de Outlier Local (LOF). Para qualquer instância de dados dada, a pontuação LOF é igual à razão da densidade local média dos k vizinhos mais próximos da instância e a densidade local da própria instância de dados. Para encontrar a densidade local para uma instância de dados, os autores primeiro encontram o raio da menor hiperesfera centrada na instância de dados, que contém seus k vizinhos mais próximos. A densidade local é então calculada dividindo k pelo volume desta hiperesfera. Para uma instância normal situada em uma região densa, sua densidade local será semelhante à de seus vizinhos, enquanto para uma instância anômala, sua densidade local será menor do que a de seus vizinhos mais próximos.

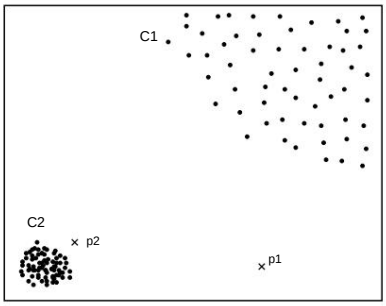


Fig. 7. Vantagem das técnicas baseadas na densidade local sobre as técnicas baseadas na densidade global.

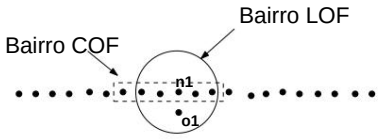


Fig. 8. Diferença entre os bairros calculados por LOF e COF.

vizinhos. Portanto, a instância anômala obterá uma pontuação LOF mais alta.

No exemplo mostrado na Figura 7, o LOF será capaz de capturar ambas as anomalias (p1 e p2) devido ao fato de considerar a densidade em torno das instâncias de dados.

Vários pesquisadores propuseram variantes da técnica LOF. Algumas dessas variantes estimam a densidade local de uma instância de uma maneira diferente. Algumas variantes adaptaram a técnica original a tipos de dados mais complexos. Como a técnica LOF original é O(N2) (N é o tamanho dos dados), várias técnicas foram propostas para melhorar a eficiência da LOF.

Tang et al. [2002] discutem uma variação do LOF, que eles chamam de Fator Outlier baseado em Conectividade (COF). A diferença entre LOF e COF é a maneira como a vizinhança k para uma instância é computada. No COF, a vizinhança para uma instância é computada em um modo incremental. Para começar, a instância mais próxima da instância fornecida é adicionada ao conjunto de vizinhança. A próxima instância adicionada ao conjunto de vizinhança é tal que sua distância para o conjunto de vizinhança existente é mínima entre todas as instâncias de dados restantes. A distância entre uma instância e um conjunto de instâncias é definida como a distância mínima entre a instância fornecida e qualquer instância pertencente ao conjunto fornecido. A vizinhança é aumentada dessa maneira até atingir o tamanho k. Uma vez que a vizinhança é computada, a pontuação de anomalia (COF) é computada da mesma maneira que o LOF. O COF é capaz de capturar regiões como linhas retas, conforme mostrado na Figura 8.

Uma versão mais simples do LOF foi proposta por Hautamaki et al. [2004] que calcula uma quantidade chamada Detecção de Outliers usando Número In-degree (ODIN) para cada instância de dados. Para uma dada instância de dados, ODIN é igual ao número de k vizinhos mais próximos da instância de dados que têm a dada instância de dados em sua lista de k vizinhos mais próximos. O inverso de ODIN é a pontuação de anomalia para a instância de dados. Uma técnica semelhante foi proposta por Brito et al. [1997].

Papadimitriou et al. [2002] propõem uma medida chamada Multi-granularity Deviation Factor (MDEF), que é uma variação do LOF. O MDEF para uma dada instância de dados é igual ao desvio padrão das densidades locais dos vizinhos mais próximos da dada instância de dados (incluindo a própria instância de dados). O inverso do desvio padrão é a pontuação de anomalia para a instância de dados. A técnica de detecção de anomalias apresentada no artigo é chamada LOCI, que não apenas encontra instâncias anômalas, mas também microclusters anômalos.

Várias variantes de LOF foram propostas para lidar com diferentes tipos de dados. Uma variante de LOF é aplicada para detectar anomalias espaciais em dados climáticos por Sun e Chawla [2004; 2006]. Yu et al. [2006] usam uma medida de similaridade em vez de distância para lidar com atributos categóricos. Uma técnica semelhante foi proposta para detectar anomalias sequenciais em sequências de proteínas por Sun et al. [2006]. Esta técnica usa Árvores de Sufixo Probabilísticas (PST) para encontrar os vizinhos mais próximos para uma determinada sequência.
Pokrajac et al. [2007] estendem o LOF para trabalhar de forma incremental para detectar anomalias em dados do sensor de vídeo.

Algumas variantes da técnica LOF foram propostas para melhorar sua eficiência.
Jin et al. [2001] propõem uma variante, na qual apenas as principais anomalias n são encontradas em vez de encontrar a pontuação LOF para cada instância de dados. A técnica inclui encontrar microclusters nos dados e, em seguida, encontrar o limite superior e inferior no LOF para cada um dos microclusters. Chiu e Chee Fu [2003] propuseram três variantes de LOF que melhoram seu desempenho ao fazer certas suposições sobre o problema para podar todos os clusters que definitivamente não contêm instâncias que figurarão na lista de anomalias n principais. Para os clusters restantes, uma análise detalhada é feita para encontrar a pontuação LOF para cada instância nesses clusters.

Complexidade Computacional Uma
desvantagem da técnica básica baseada no vizinho mais próximo e da técnica LOF é a complexidade O(N2) necessária. Como essas técnicas envolvem encontrar vizinhos mais próximos para cada instância, estruturas de dados eficientes, como árvores kd [Bentley 1975] e árvores R [Roussopoulos et al. 1995], podem ser usadas. Mas essas técnicas não escalam bem à medida que o número de atributos aumenta. Várias técnicas otimizaram diretamente a técnica de detecção de anomalias sob a suposição de que apenas as poucas anomalias principais são interessantes. Se uma pontuação de anomalia for necessária para cada instância de teste, essas técnicas não serão aplicáveis. Técnicas que particionam o espaço de atributos em uma hipergrade são lineares em tamanho de dados, mas são exponenciais no número de atributos e, portanto, não são adequadas para um grande número de atributos. Técnicas de amostragem tentam abordar o problema da complexidade O(N2) determinando os vizinhos mais próximos dentro de uma pequena amostra do conjunto de dados. Mas a amostragem pode resultar em pontuações de anomalia incorretas se o tamanho da amostra for muito pequeno.

Vantagens e Desvantagens das Técnicas Baseadas no Vizinho Mais Próximo As vantagens das técnicas baseadas no vizinho mais próximo são as seguintes: (1) Uma vantagem fundamental das

técnicas baseadas no vizinho mais próximo é que elas são de natureza não supervisionada e não fazem nenhuma suposição sobre a distribuição generativa dos dados. Em vez disso, elas são puramente orientadas por dados.

(2) As técnicas semissupervisionadas apresentam melhor desempenho do que as técnicas não supervisionadas em termos de anomalias perdidas, uma vez que a probabilidade de uma anomalia formar uma vizinhança próxima no conjunto de dados de treinamento é muito baixa.

(3) A adaptação de técnicas baseadas no vizinho mais próximo a um tipo de dados diferente é simples e requer principalmente a definição de uma medida de distância apropriada para os dados fornecidos.

As desvantagens das técnicas baseadas no vizinho mais próximo são as seguintes:

(1) Para técnicas não supervisionadas, se os dados tiverem instâncias normais que não

tem vizinhos próximos o suficiente ou se os dados têm anomalias que têm vizinhos próximos o suficiente, a técnica falha em rotulá-los corretamente, resultando em anomalias perdidas.

(2) Para técnicas semissupervisionadas, se as instâncias normais nos dados de teste não tiverem instâncias normais semelhantes suficientes nos dados de treinamento, a taxa de falsos positivos para tais técnicas será alta.

(3) A complexidade computacional da fase de teste também é um desafio significativo, pois envolve o cálculo da distância de cada instância de teste com todas as instâncias pertencentes aos próprios dados de teste ou aos dados de treinamento, para calcular os vizinhos mais próximos.

(4) O desempenho de uma técnica baseada no vizinho mais próximo depende muito de uma medida de distância, definida entre um par de instâncias de dados, que pode efetivamente distinguir entre instâncias normais e anômalas. Definir medidas de distância entre instâncias pode ser desafiador quando os dados são complexos, por exemplo, gráficos, sequências, etc.

6. TÉCNICAS DE DETECÇÃO DE ANOMALIAS BASEADAS EM CLUSTERING

Clustering [Jain e Dubes 1988; Tan et al. 2005] é usado para agrupar instâncias de dados semelhantes em clusters. Clustering é principalmente uma técnica não supervisionada, embora clustering semissupervisionado [Basu et al. 2004] também tenha sido explorado ultimamente. Embora clustering e detecção de anomalias pareçam ser fundamentalmente diferentes um do outro, várias técnicas de detecção de anomalias baseadas em clustering foram desenvolvidas. Técnicas de detecção de anomalias baseadas em clustering podem ser agrupadas em três categorias.

A primeira categoria de técnicas baseadas em agrupamento baseia-se na seguinte suposição:

Suposição: Instâncias de dados normais pertencem a um cluster nos dados, enquanto anomalias mentiras ou não pertencem a nenhum cluster.

Técnicas baseadas na suposição acima aplicam um algoritmo baseado em clustering conhecido ao conjunto de dados e declaram qualquer instância de dados que não pertença a nenhum cluster como anômala. Vários algoritmos de clustering que não forçam cada instância de dados a pertencer a um cluster, como DBSCAN [Ester et al. 1996], ROCK [Guha et al. 2000] e clustering SNN [Ert¨oz et al. 2003] podem ser usados. O algoritmo FindOut [Yu et al. 2002] é uma extensão do algoritmo WaveCluster [Sheik-holeslami et al. 1998] no qual os clusters detectados são removidos dos dados e as instâncias residuais são declaradas como anomalias.

Uma desvantagem dessas técnicas é que elas não são otimizadas para encontrar anomalias, já que o objetivo principal do algoritmo de agrupamento subjacente é encontrar clusters.

A segunda categoria de técnicas baseadas em agrupamento baseia-se na seguinte suposição:

Suposição: As instâncias de dados normais ficam próximas ao centróide do cluster mais próximo, enquanto as anomalias estão longe do centroide do seu aglomerado mais próximo.

Técnicas baseadas na suposição acima consistem em duas etapas. Na primeira etapa, os dados são agrupados usando um algoritmo de agrupamento. Na segunda etapa, para cada instância de dados, sua distância até seu centroide de cluster mais próximo é calculada como sua anomalia
pontuação.

Várias técnicas de detecção de anomalias que seguem essa abordagem de duas etapas foram propostas usando diferentes algoritmos de agrupamento. Smith et al. [2002] estudaram Mapas Auto-Organizáveis (SOM), Agrupamento K-means e Maximização de Expectativas (EM) para agrupar dados de treinamento e então usar os clusters para classificar dados de teste. Em particular, o SOM [Kohonen 1997] tem sido amplamente usado para detectar anomalias em um modo semissupervisionado em várias aplicações, como detecção de intrusão [Labib e Vemuri 2002; Smith et al. 2002; Ramadas et al. 2003], detecção de falhas [Harris 1993; Ypma e Duin 1998; Emamian et al. 2000] e detecção de fraudes [Brockett et al. 1998]. Barbara et al. [2003] propõem uma técnica que é robusta a anomalias nos dados de treinamento. Os autores primeiro separam instâncias normais de anomalias nos dados de treinamento, usando mineração frequente de conjunto de itens, e então usam a técnica baseada em clustering para detectar anomalias. Várias técnicas também foram propostas para lidar com dados de sequência [Blender et al. 1997; Bejerano e Yona 2001; Vinueza e Grudic 2004; Budalakoti et al. 2006].

Técnicas baseadas na segunda suposição também podem operar no modo semissupervisionado, no qual os dados de treinamento são agrupados e instâncias pertencentes aos dados de teste são comparadas com os clusters para obter uma pontuação de anomalia para a instância de dados de teste [Marchette 1999; Wu e Zhang 2003; Vinueza e Grudic 2004; Allan et al. 1998]. Se os dados de treinamento tiverem instâncias pertencentes a várias classes, o agrupamento semissupervisionado pode ser aplicado para melhorar os clusters. He et al. [2002] incorporam o conhecimento de rótulos para melhorar sua técnica de detecção de anomalias baseada em agrupamento não supervisionado [He et al. 2003] calculando uma medida chamada fator de anomalia semântica que é alta se o rótulo de classe de um objeto em um cluster for diferente da maioria dos rótulos de classe naquele cluster.

Note que se as anomalias nos dados formarem clusters por si só, as técnicas discutidas acima não serão capazes de detectar tais anomalias. Para abordar esse problema, uma terceira categoria de técnicas baseadas em clustering foi proposta, que se baseia na seguinte suposição:

Suposição: Instâncias de dados normais pertencem a clusters grandes e densos, enquanto anomalias pertencem a aglomerados pequenos ou esparsos.

Técnicas baseadas na suposição acima declaram instâncias pertencentes a clusters cujo tamanho e/ou densidade está abaixo de um limite como anômalas.

Várias variações da terceira categoria de técnicas foram propostas [Pires e Santos-Pereira 2005; Otey et al. 2003; Eskin et al. 2002; Mahoney et al. 2003; Jiang et al. 2001; He et al. 2003]. A técnica proposta por [He et al. 2003], chamada FindCBLOF, atribui uma pontuação de anomalia conhecida como Cluster-Based Local Outlier Factor (CBLOF) para cada instância de dados. A pontuação CBLOF captura o tamanho do cluster ao qual a instância de dados pertence, bem como a distância da instância de dados ao seu centroide de cluster.

Várias técnicas baseadas em clustering foram propostas para melhorar a eficiência das técnicas existentes discutidas acima. O clustering de largura fixa é um algoritmo de aproximação de tempo linear (O(N d)) usado por várias técnicas de detecção de anomalias [Eskin et al. 2002; Portnoy et al. 2001; Mahoney et al. 2003; He et al. 2003]. Uma instância é atribuída a um cluster cujo centro está dentro de uma distância pré-especificada para a instância fornecida. Se nenhum cluster desse tipo existir, então um novo cluster com a instância como

centro é criado. Então eles determinam quais clusters são anomalias com base em sua densidade e distância de outros clusters. A largura pode ser um parâmetro especificado pelo usuário [Eskin et al. 2002; Portnoy et al. 2001] ou pode ser derivada dos dados [Mahoney et al. 2003]. Chaudhary et al. [2002] propõem uma técnica de detecção de anomalias usando árvores kd que fornecem um particionamento dos dados em tempo linear.
Eles aplicam sua técnica para detectar anomalias em conjuntos de dados astronômicos onde a eficiência computacional é um requisito importante. Outra técnica que aborda essa questão é proposta por Sun et al. [2004]. Os autores propõem uma técnica de indexação chamada CD-trees para particionar dados em clusters de forma eficiente. As instâncias de dados que pertencem a clusters esparsos são declaradas como anomalias.

6.1 Distinção entre técnicas baseadas em clustering e técnicas baseadas no vizinho mais próximo Várias técnicas baseadas em clustering exigem computação de distância entre um par de instâncias. Assim, nesse aspecto, elas são semelhantes às técnicas baseadas no vizinho mais próximo. A escolha da medida de distância é crítica para o desempenho da técnica; portanto, a discussão na seção anterior sobre as medidas de distância também se aplica às técnicas baseadas em clustering. A principal diferença entre as duas técnicas, no entanto, é que as técnicas baseadas em clustering avaliam cada instância com relação ao cluster ao qual ela pertence, enquanto as técnicas baseadas no vizinho mais próximo analisam cada instância com relação à sua vizinhança local.

Complexidade Computacional A
complexidade computacional do treinamento de uma técnica de detecção de anomalias baseada em cluster depende do algoritmo de cluster usado para gerar clusters a partir dos dados. Assim, tais técnicas podem ter complexidade quadrática se a técnica de cluster exigir computação de distâncias em pares para todas as instâncias de dados, ou linear quando usar técnicas baseadas em heurística, como k-means [Hartigan e Wong 1979] ou técnicas de cluster aproximadas [Eskin et al. 2002]. A fase de teste de técnicas baseadas em cluster é rápida, pois envolve a comparação de uma instância de teste com um pequeno número de clusters.

Vantagens e desvantagens das técnicas baseadas em clustering
As vantagens das técnicas baseadas em agrupamento são as seguintes:

(1) As técnicas baseadas em agrupamento podem operar em modo não supervisionado.

(2) Essas técnicas podem frequentemente ser adaptadas a outros tipos de dados complexos, bastando para isso conectar um algoritmo de agrupamento que possa manipular o tipo de dados específico.

(3) A fase de teste para técnicas baseadas em agrupamento é rápida, pois o número de agrupamentos com os quais cada instância de teste precisa ser comparada é uma pequena constante.

As desvantagens das técnicas baseadas em agrupamento são as seguintes:

(1) O desempenho das técnicas baseadas em agrupamento depende muito da eficácia do algoritmo de agrupamento na captura da estrutura do agrupamento de instâncias normais.

(2) Muitas técnicas detectam anomalias como um subproduto do agrupamento e, portanto, não são otimizadas para detecção de anomalias.

(3) Vários algoritmos de agrupamento forçam cada instância a ser atribuída a algum cluster.
Isso pode fazer com que anomalias sejam atribuídas a um grande cluster, sendo consideradas instâncias normais por técnicas que operam sob a suposição de que anomalias não pertencem a nenhum cluster.

(4) Várias técnicas baseadas em agrupamento são eficazes apenas quando as anomalias não existem.
não formam aglomerados significativos entre si.

(5) A complexidade computacional para agrupar os dados é frequentemente um gargalo, especialmente se forem usados algoritmos de agrupamento O(N2d) .

7. TÉCNICAS DE DETECÇÃO DE ANOMALIA ESTATÍSTICA

O princípio subjacente de qualquer técnica de detecção de anomalia estatística é: “Uma anomalia é uma observação que é suspeita de ser parcial ou totalmente irrelevante porque não é gerada pelo modelo estocástico assumido” [Anscombe e Guttman 1960]. As técnicas de detecção de anomalia estatística são baseadas na seguinte suposição-chave:

Suposição: Instâncias de dados normais ocorrem em regiões de alta probabilidade de um modelo estocástico, enquanto anomalias ocorrem em regiões de baixa probabilidade do modelo estocástico.

Técnicas estatísticas ajustam um modelo estatístico (geralmente para comportamento normal) aos dados fornecidos e então aplicam um teste de inferência estatística para determinar se uma instância não vista pertence a esse modelo ou não. Instâncias que têm baixa probabilidade de serem geradas a partir do modelo aprendido, com base na estatística de teste aplicada, são declaradas como anomalias. Técnicas paramétricas e não paramétricas foram aplicadas para ajustar um modelo estatístico. Enquanto técnicas paramétricas assumem o conhecimento da distribuição subjacente e estimam os parâmetros a partir dos dados fornecidos [Eskin 2000], técnicas não paramétricas geralmente não assumem o conhecimento da distribuição subjacente [Desforges et al. 1998]. Nas próximas duas subseções, discutiremos técnicas de detecção de anomalias paramétricas e não paramétricas.

7.1 Técnicas Paramétricas

Como mencionado antes, as técnicas paramétricas assumem que os dados normais são gerados por uma distribuição paramétrica com parâmetros ÿ e função de densidade de probabilidade f(x, ÿ), onde x é uma observação. A pontuação de anomalia de uma instância de teste (ou observação) x é o inverso da função de densidade de probabilidade, f(x, ÿ). Os parâmetros ÿ são estimados a partir dos dados fornecidos.

Alternativamente, um teste de hipótese estatística (também conhecido como teste de discordância na literatura de detecção de outliers estatísticos [Barnett e Lewis 1994]) pode ser usado. A hipótese nula (H0) para tais testes é que a instância de dados x foi gerada usando a distribuição estimada (com parâmetros ÿ). Se o teste estatístico rejeitar H0, x é declarado como anomalia. Um teste de hipótese estatística é associado a uma estatística de teste, que pode ser usada para obter uma pontuação de anomalia probabilística para a instância de dados x.

Com base no tipo de distribuição assumido, as técnicas paramétricas podem ser categorizadas da seguinte forma:

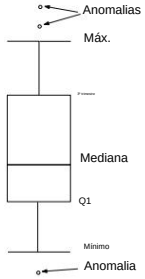


Fig. 9. Um gráfico de caixa para um conjunto de dados univariados.

7.1.1 Baseado em Modelo Gaussiano. Tais técnicas assumem que os dados são gerados a partir de uma distribuição Gaussiana. Os parâmetros são estimados usando Estimativas de Máxima Verossimilhança (MLE). A distância de uma instância de dados para a média estimada é a pontuação de anomalia para essa instância. Um limite é aplicado às pontuações de anomalia para determinar as anomalias. Diferentes técnicas nesta categoria calculam a distância para a média e o limite de diferentes maneiras.

Uma técnica simples de detecção de outliers, frequentemente usada no domínio de controle de qualidade de processos [Shewhart 1931], é declarar todas as instâncias de dados que estão a mais de 3ÿ de distância da média da distribuição µ, onde ÿ é o desvio padrão da distribuição.
A região µ ± 3ÿ contém 99,7% das instâncias de dados.

Testes estatísticos mais sofisticados também foram usados para detectar anomalias, conforme discutido em [Barnett e Lewis 1994; Barnett 1976; Beckman e Cook 1983]. Descreveremos alguns testes aqui.

A regra do box plot (Figura 9) é a técnica estatística mais simples que foi aplicada para detectar anomalias univariadas e multivariadas em dados de domínio médico [Laurikkala et al. 2000; Horn et al. 2001; Solberg e Lahti 2005] e dados de rotores de turbina [Guttormsson et al. 1999]. Um box-plot descreve graficamente os dados usando atributos de resumo, como a menor observação não anômala (min), quartil inferior (Q1), mediana, quartil superior (Q3) e a maior observação não anômala (max).

A quantidade Q3 ÿQ1 é chamada de Intervalo Interquartil (IQR). Os diagramas de caixa também indicam os limites além dos quais qualquer observação será tratada como uma anomalia. Uma instância de dados que esteja mais de 1,5 ÿ IQR abaixo de Q1 ou 1,5 ÿ IQR acima de Q3 é declarada como uma anomalia. A região entre Q1 ÿ 1,5IQR e Q3 + 1,5IQR contém 99,3% das observações e, portanto, a escolha do limite de 1,5IQR torna a regra do diagrama de caixa equivalente à técnica 3ÿ para dados gaussianos.

O teste de Grubb (também conhecido como teste residual máximo normalizado) é usado para detectar anomalias em um conjunto de dados univariados [Grubbs 1969; Stefansky 1972; Anscombe e Guttman 1960] sob a suposição de que os dados são gerados por uma distribuição gaussiana. Para cada instância de teste x, sua pontuação z é computada da seguinte forma:

$$z = \frac{|x - \bar{x}|}{s} \quad (1)$$

onde $\bar{x}$ e s são a média e o desvio padrão da amostra de dados, respectivamente.

Uma instância de teste é declarada anômala se:

$$z > \frac{N \ddot{y} 1}{\ddot{y} N} \sqrt{\frac{t^2 \ddot{y}/(2N),N\ddot{y}2}{N \ddot{y} 2 + t^2 \ddot{y}/(2N),N\ddot{y}2}} \quad (2)$$

onde N é o tamanho dos dados e tÿ/(2N),Nÿ2 é um limite usado para declarar uma instância como anômala ou normal. Este limite é o valor tomado por uma distribuição t em um nível de significância de ÿ 2N . O nível de significância reflete a confiança associada ao limite e controla indiretamente o número de instâncias declaradas como anômalas.

Uma variante do teste de Grubb para dados multivariados foi proposta por Laurikkala et al. [2000], que usa a distância de Mahalanobis de uma instância de teste x para a média da amostra ¯x, para reduzir observações multivariadas a escalares univariados.

$$^{2}_{\text{anos}} = (x \ddot{y} \bar{x}) S^{-1} (x \ddot{y} \bar{x}), \quad (3)$$

onde S é a matriz de covariância da amostra. O teste de Grubb univariado é aplicado a y para determinar se a instância x é anômala ou não. Várias outras variantes do teste de Grubb foram propostas para lidar com conjuntos de dados multivariados [Aggarwal e Yu 2001; 2008; Laurikkala et al. 2000], dados estruturados em gráfico [Shekhar et al. 2001] e cubos de dados de Processamento Analítico Online (OLAP) [Sarawagi et al. 1998].

O teste t de Student também foi aplicado para detecção de anomalias em [Surace e Worden 1998; Surace et al. 1997] para detectar danos em vigas estruturais. Uma amostra normal, N1, é comparada com uma amostra de teste, N2, usando o teste t. Se o teste mostrar diferença significativa entre elas, isso significa a presença de uma anomalia em N2.

A versão multivariada do teste t de Student, chamada de Hotelling t 2 -teste também é usado como uma estatística de teste de detecção de anomalias em [Liu e Weng 1991] para detectar anomalias em estudos de biodisponibilidade/bioequivalência. estatística para

Ye e Chen [2001] usam um ÿ 2 determinar anomalias em dados de chamada do sistema operacional. A fase de treinamento assume que os dados normais têm uma distribuição normal multivariada. O valor da estatística ÿ 2 é determinado como:

$$^{2}\ddot{y} = \sum_{eu=1}^{não} \frac{(Xi \ddot{y} Ei)^2}{Ei} \quad (4)$$

onde Xi é o valor observado da i-ésima variável, Ei é o valor esperado da i-ésima variável (obtido dos dados de treinamento) e n é o número de variáveis. Um valor grande de X2 denota que a amostra observada contém anomalias.

Várias outras técnicas de detecção de anomalias estatísticas que assumem que os dados seguem uma distribuição gaussiana foram propostas e usam outros testes estatísticos, como: teste de Rosner [Rosner 1983], teste de Dixon [Gibbons 1994], teste de detecção de deslizamento [Hawkins 1980], etc.

7.1.2 Baseado em Modelo de Regressão. A detecção de anomalias usando regressão foi extensivamente investigada para dados de séries temporais [Abraham e Chuang 1989; Abraham e Box 1979; Fox 1972].

A técnica básica de detecção de anomalias baseada no modelo de regressão consiste em duas etapas. Na primeira etapa, um modelo de regressão é ajustado aos dados. Na segunda etapa, para cada instância de teste, o resíduo para a instância de teste é usado para determinar o

pontuação de anomalia. O resíduo é a parte da instância que não é explicada pelo modelo de regressão. A magnitude do resíduo pode ser usada como pontuação de anomalia para a instância de teste, embora testes estatísticos tenham sido propostos para determinar anomalias com certa confiança [Anscombe e Guttman 1960; Beckman e Cook 1983; Hawkins 1980; Torr e Murray 1993]. Certas técnicas detectam a presença de anomalias em um conjunto de dados analisando o Conteúdo de Informação de Akaike (AIC) durante o ajuste do modelo [Kitagawa 1979; Kadota et al. 2003].

A presença de anomalias nos dados de treinamento pode influenciar os parâmetros de regressão e, portanto, o modelo de regressão pode não produzir resultados precisos. Uma técnica popular para lidar com tais anomalias ao ajustar modelos de regressão é chamada de regressão robusta [Rousseeuw e Leroy 1987] (estimativa de parâmetros de regressão ao acomodar anomalias). Os autores argumentam que as técnicas de regressão robusta não apenas escondem as anomalias, mas também podem detectá-las, porque as anomalias tendem a ter resíduos maiores do ajuste robusto. Uma abordagem de detecção de anomalia robusta semelhante foi aplicada em modelos de Média Móvel Integrada Autorregressiva (ARIMA) [Bianco et al. 2001; Chen et al. 2005].

Variantes da técnica baseada em modelos básicos de regressão foram propostas para lidar com dados de séries temporais multivariadas. Tsay et al. [2000] discutem a complexidade adicional em séries temporais multivariadas sobre as séries temporais univariadas e apresentam estatísticas que podem ser aplicadas para detectar anomalias em modelos ARIMA multivariados.
Esta é uma generalização das estatísticas propostas anteriormente por Fox [1972].

Outra variante que detecta anomalias em dados de séries temporais multivariadas gerados por um modelo de Média Móvel Autorregressiva (ARMA) foi proposta por Galeano et al. [2004]. Nessa técnica, os autores transformam as séries temporais multivariadas em séries temporais univariadas combinando linearmente os componentes das séries temporais multivariadas. As combinações lineares interessantes (projeções no espaço 1-d) são obtidas usando uma técnica de busca de projeção [Huber 1985] que maximiza o coeficiente de curtose (uma medida para o grau de pico/planicidade na distribuição variável) dos dados da série temporal. A detecção de anomalias em cada projeção é feita usando estatísticas de teste univariadas, conforme proposto por Fox [1972].

7.1.3 Mistura de Distribuições Paramétricas Baseadas. Tais técnicas usam uma mistura de distribuições estatísticas paramétricas para modelar os dados. Técnicas nesta categoria podem ser agrupadas em duas subcategorias. A primeira subcategoria de técnicas modela as instâncias normais e anomalias como distribuições paramétricas separadas, enquanto a segunda subcategoria de técnicas modela apenas as instâncias normais como uma mistura de distribuições paramétricas.

Para a primeira subcategoria de técnicas, a fase de teste envolve determinar a qual distribuição — normal ou anômala — a instância de teste pertence. Abraham e Box [1979] assumem que os dados normais são gerados a partir de uma distribuição gaussiana (N(0,ÿ com a mesma média, mas com maior ^{2})) e as anomalias também são geradas a partir de uma distribuição gaussiana). Uma variância, N(0,k 2ÿ 2 usando o teste de Grubb em ambas as instância de teste é testada distribuições e, consequentemente, rotulados como normais ou anômalos. Técnicas semelhantes foram propostas em [Lauer 2001; Eskin 2000; Abraham e Box 1979; Box e Tiao 1968; Agarwal 2005]. Eskin [2000] usa o algoritmo Expectation Maximization (EM) para desenvolver uma mistura de modelos para as duas classes, assumindo que cada ponto de dados é uma anomalia com probabilidade a priori ÿ, e

normal com probabilidade a priori 1 ÿ ÿ. Assim, se D representa a distribuição de probabilidade real de todos os dados, e M e A representam as distribuições dos dados normais e anômalos, respectivamente, então D = ÿA + (1 ÿ ÿ)M. M é aprendido usando qualquer técnica de estimativa de distribuição, enquanto A é assumido como uniforme.
Inicialmente, todos os pontos são considerados como estando em M. A pontuação de anomalia é atribuída a um ponto com base em quanto as distribuições mudam se esse ponto for removido de M e adicionado a A.

A segunda subcategoria de técnicas modela as instâncias normais como uma mistura de distribuições paramétricas. Uma instância de teste que não pertence a nenhum dos modelos aprendidos é declarada como anomalia. Modelos de mistura gaussiana têm sido usados principalmente para tais técnicas Agarwal [2006], e têm sido usados para detectar tensões em dados de fuselagem [Hickinbotham e Austin 2000a; Hollier e Austin 2002], para detectar anomalias em análise de imagens mamográficas [Spence et al. 2001; Tarassenko 1995] e para detecção de intrusão de rede [Yamanishi e ichi Takeuchi 2001; Yamanishi et al. 2004]. Técnicas semelhantes têm sido aplicadas para detectar anomalias em dados de sinais biomédicos [Roberts e Tarassenko 1994; Roberts 1999; 2002], onde estatísticas de valores extremos2 são usadas para determinar se um ponto de teste é uma anomalia com relação à mistura aprendida de modelos ou não. Byers e Raftery [1998] usam uma mistura de distribuições de Poisson para modelar os dados normais e então detectar anomalias.

7.2 Técnicas não paramétricas

As técnicas de detecção de anomalias nesta categoria usam modelos estatísticos não paramétricos, de modo que a estrutura do modelo não é definida a priori, mas é determinada a partir de dados fornecidos. Essas técnicas geralmente fazem menos suposições sobre os dados, como suavidade de densidade, quando comparadas a técnicas paramétricas.

7.2.1 Baseado em histograma. A técnica estatística não paramétrica mais simples é usar histogramas para manter um perfil dos dados normais. Tais técnicas também são chamadas de baseadas em frequência ou baseadas em contagem. Técnicas baseadas em histograma são particularmente populares na comunidade de detecção de intrusão [Eskin 2000; Eskin et al.
[2001; Denning 1987] e detecção de fraudes [Fawcett e Provost 1999], uma vez que o comportamento dos dados é governado por certos perfis (usuário, software ou sistema) que podem ser capturados de forma eficiente usando o modelo de histograma.

Uma técnica básica de detecção de anomalias baseada em histograma para dados univariados consiste em duas etapas. A primeira etapa envolve a construção de um histograma com base nos diferentes valores tomados por esse recurso nos dados de treinamento. Na segunda etapa, a técnica verifica se uma instância de teste cai em qualquer um dos compartimentos do histograma. Se cair, a instância de teste é normal, caso contrário, é anômala. Uma variante da técnica básica baseada em histograma é atribuir uma pontuação de anomalia a cada instância de teste com base na altura (frequência) do compartimento em que cai.

2Teoria do Valor Extremo (EVT) [Pickands 1975] é um conceito similar ao da detecção de anomalias e lida com desvios extremos de uma distribuição de probabilidade. A EVT foi aplicada ao gerenciamento de risco [McNeil 1999] como um método para modelar e medir riscos extremos. A principal diferença entre valores extremos e anomalias estatísticas é que valores extremos são conhecidos por ocorrerem nas extremidades de uma distribuição de probabilidade, enquanto anomalias são mais gerais. Anomalias também podem ser geradas a partir de uma distribuição completamente diferente.

O tamanho do compartimento usado na construção do histograma é fundamental para a detecção de anomalias. Se os bins forem pequenos, muitas instâncias de teste normais cairão em bins vazios ou raros, resultando em uma alta taxa de alarmes falsos. Se os bins forem grandes, muitas instâncias de teste anômalas cairão em bins frequentes, resultando em uma alta taxa de falsos negativos. Portanto, um desafio fundamental para técnicas baseadas em histograma é determinar um tamanho ideal dos bins para construir o histograma que mantenha uma baixa taxa de alarmes falsos e uma baixa taxa de falsos negativos.

Técnicas baseadas em histogramas requerem dados normais para construir os histogramas [Anderson et al. 1994; Javitz e Valdes 1991; Helman e Bhangoo 1997]. Algumas técnicas até constroem histogramas para as anomalias [Dasgupta e Nino 2000], se instâncias anômalas rotuladas estiverem disponíveis.

Para dados multivariados, uma técnica básica é construir histogramas por atributos.
Durante o teste, para cada instância de teste, a pontuação de anomalia para cada valor de atributo da instância de teste é calculada como a altura do bin que contém o valor do atributo. As pontuações de anomalia por atributo são agregadas para obter uma pontuação de anomalia geral para a instância de teste.

A técnica básica baseada em histograma para dados multivariados foi aplicada à detecção de intrusão de chamada de sistema Endler [1998], detecção de intrusão de rede [Ho et al.
1999; Yamanishi e ichi Takeuchi 2001; Yamanishi et al. 2004], detecção de fraudes [Fawcett e Provost 1999], detecção de danos em estruturas [Manson 2002; Manson et al. 2001; Manson et al. 2000], detecção de ataques baseados na web [Kruegel e Vigna 2003; Kruegel et al. 2002] e detecção de tópicos anômalos em dados de texto [Allan et al.
[1998]. Uma variante da técnica simples é usada em Detecção de Anomalias de Cabeçalho de Pacote (PHAD) e Detecção de Anomalias de Camada de Aplicação (ALAD) [Mahoney e Chan 2002], aplicada à detecção de intrusão de rede.

Sistema de detecção de intrusão de rede em tempo real (NIDES) da SRI International
[Anderson et al. 1994; Anderson et al. 1995; Porras e Neumann 1997] tem um subsistema que mantém perfis estatísticos de longo prazo para capturar o comportamento normal de um sistema de computador [Javitz e Valdes 1991]. Os autores propõem uma estatística Q para comparar um perfil de longo prazo com um perfil de curto prazo (observação). A estatística é usada para determinar outra medida chamada estatística S, que reflete a extensão em que o comportamento em um recurso específico é uma anomalia em relação ao perfil histórico. As estatísticas S por recurso são combinadas para obter um único valor chamado estatística IS, que determina se uma instância de teste é anômala ou não. Uma variante foi proposta por Sargor [1998] para detecção de anomalias em protocolos de roteamento de estado de link.

7.2.2 Baseado em função kernel. Uma técnica não paramétrica para estimativa de densidade de probabilidade é a estimativa de janelas de Parzen [Parzen 1962]. Isso envolve o uso de funções kernel para aproximar a densidade real. Técnicas de detecção de anomalias baseadas em funções kernel são semelhantes aos métodos paramétricos descritos anteriormente. A única diferença é a técnica de estimativa de densidade usada. Desforges et al. [1998] propuseram uma técnica estatística semissupervisionada para detectar anomalias que usa funções kernel para estimar a função de distribuição de probabilidade (pdf) para as instâncias normais. Uma nova instância que se encontra na área de baixa probabilidade desta pdf é declarada anômala.

Aplicação semelhante de janelas parzen é proposta para detecção de intrusão de rede
[Chow e Yeung 2002], para detecção de novidades em dados de fluxo de óleo [Bishop 1994], e

para análise de imagens mamográficas [Tarassenko 1995].

Complexidade Computacional A
complexidade computacional das técnicas de detecção de anomalias estatísticas depende da natureza do modelo estatístico que é necessário para ser ajustado aos dados. Ajustar distribuições paramétricas únicas da família exponencial, por exemplo, Gaussiana, Poisson, Multinomial, etc., é tipicamente linear em tamanho de dados, bem como em número de atributos.
Ajustar distribuições complexas (como modelos de mistura, HMM, etc.) usando técnicas de estimativa iterativas como Expectation Maximization (EM), também são tipicamente lineares por iteração, embora possam ser lentas na convergência dependendo do problema e/ou critério de convergência. Técnicas baseadas em kernel podem potencialmente ter complexidade de tempo quadrática em termos do tamanho dos dados.

Vantagens e desvantagens das técnicas estatísticas
As vantagens das técnicas estatísticas são:

(1) Se as suposições relativas à distribuição de dados subjacentes forem verdadeiras, as técnicas estatísticas fornecem uma solução estatisticamente justificável para a detecção de anomalias.
(2) A pontuação de anomalia fornecida por uma técnica estatística está associada a um intervalo de confiança, que pode ser usado como informação adicional ao tomar uma decisão sobre qualquer instância de teste.
(3) Se a etapa de estimativa da distribuição for robusta a anomalias nos dados, as técnicas estatísticas podem operar em um ambiente não supervisionado sem qualquer necessidade de dados de treinamento rotulados.

As desvantagens das técnicas estatísticas são:

(1) A principal desvantagem das técnicas estatísticas é que elas dependem da suposição de que os dados são gerados a partir de uma distribuição particular. Essa suposição frequentemente não é verdadeira, especialmente para conjuntos de dados reais de alta dimensão.
(2) Mesmo quando a suposição estatística pode ser razoavelmente justificada, há várias estatísticas de teste de hipóteses que podem ser aplicadas para detectar anomalias; escolher a melhor estatística geralmente não é uma tarefa simples [Motulsky 1995]. Em particular, construir testes de hipóteses para distribuições complexas que são necessárias para ajustar conjuntos de dados de alta dimensão não é trivial.
(3) Técnicas baseadas em histogramas são relativamente simples de implementar, mas uma deficiência fundamental dessas técnicas para dados multivariados é que elas não conseguem capturar as interações entre diferentes atributos. Uma anomalia pode ter valores de atributos que são individualmente muito frequentes, mas sua combinação é muito rara, mas uma técnica baseada em histogramas por atributos não seria capaz de detectar tais anomalias.

8. TÉCNICAS DE DETECÇÃO DE ANOMALIAS TEÓRICAS DA INFORMAÇÃO

Técnicas teóricas da informação analisam o conteúdo de informação de um conjunto de dados usando diferentes medidas teóricas da informação, como Complexidade de Kolomogorov, entropia, entropia relativa, etc. Tais técnicas são baseadas na seguinte suposição-chave:

Suposição: Anomalias nos dados induzem irregularidades no conteúdo de informação do conjunto de dados.

Seja C(D) a complexidade de um dado conjunto de dados, D. Uma técnica básica de teoria da informação pode ser descrita como segue. Dado um conjunto de dados D, encontre o subconjunto mínimo de instâncias, I, tal que C(D)ÿC(DÿI) seja máximo. Todas as instâncias no subconjunto assim obtido são consideradas anômalas. O problema abordado por esta técnica básica é encontrar uma solução pareto-ótima, que não tenha um único ótimo, uma vez que há dois objetivos diferentes que precisam ser otimizados.

Na técnica descrita acima, a complexidade de um conjunto de dados (C) pode ser medida de diferentes maneiras. A complexidade de Kolomogorov [Li e Vitanyi 1993] foi usada por várias técnicas [Arning et al. 1996; Keogh et al. 2004]. Arning et al. [1996] usam o tamanho da expressão regular para medir a Complexidade de Kolomogorov dos dados (representada como uma string) para detecção de anomalias. Keogh et al. [2004] usam o tamanho do arquivo de dados compactado (usando qualquer algoritmo de compactação padrão), como uma medida da Complexidade de Kolomogorov do conjunto de dados. Outras medidas teóricas da informação, como entropia, incerteza relativa, etc., também foram usadas para medir a complexidade de um conjunto de dados categóricos [Lee e Xiang 2001; He et al. 2005; He et al. 2006; Ando 2007].

A técnica básica descrita acima envolve otimização dupla para minimizar o tamanho do subconjunto e maximizar a redução na complexidade do conjunto de dados.
Assim, uma abordagem exaustiva na qual cada subconjunto possível do conjunto de dados é considerado seria executada em tempo exponencial. Várias técnicas foram propostas que realizam busca aproximada para o subconjunto mais anômalo. He et al. [2006] usam um algoritmo aproximado chamado Local Search Algorithm (LSA) [He et al. 2005] para determinar aproximadamente tal subconjunto de forma linear, usando entropia como medida de complexidade. Uma técnica semelhante que usa uma medida de gargalo de informação foi proposta por [Ando 2007].

Técnicas de teoria da informação também foram usadas em conjuntos de dados nos quais instâncias de dados são naturalmente ordenadas, por exemplo, dados sequenciais, dados espaciais. Em tais casos, os dados são divididos em subestruturas (segmentos para sequências, subgráficos para gráficos, etc.), e a técnica de detecção de anomalias encontra a subestrutura, I, tal que C(D) ÿ C(D ÿ I) é máximo. Esta técnica foi aplicada a sequências [Lin et al. 2005; Chakrabarti et al. 1998; Arning et al. 1996], dados de gráfico [Noble e Cook 2003] e dados espaciais [Lin e Brown 2003]. Um desafio fundamental de tais técnicas é encontrar o tamanho ideal da subestrutura que resultaria na detecção de anomalias.

Complexidade Computacional Como
mencionado anteriormente, a técnica básica de detecção de anomalias da teoria da informação tem complexidade de tempo exponencial, embora tenham sido propostas técnicas aproximadas que têm complexidade de tempo linear.

Vantagens e desvantagens das técnicas teóricas da informação
As vantagens das técnicas teóricas da informação são as seguintes:

(1) Eles podem operar em um ambiente não supervisionado.

(2) Não fazem quaisquer suposições sobre a distribuição estatística subjacente para os dados.

As desvantagens das técnicas teóricas da informação são as seguintes:

(1) O desempenho de tais técnicas é altamente dependente da escolha da medida teórica da informação. Frequentemente, tais medidas podem detectar a presença de anomalias somente quando há um número significativamente grande de anomalias presentes nos dados.

(2) As técnicas teóricas da informação aplicadas a sequências e conjuntos de dados espaciais dependem do tamanho da subestrutura, que muitas vezes não é trivial de obter.

(3) É difícil associar uma pontuação de anomalia a uma instância de teste usando uma informação técnica teórica de informação.

9. TÉCNICAS DE DETECÇÃO DE ANOMALIAS ESPECTRAIS

Técnicas espectrais tentam encontrar uma aproximação dos dados usando uma combinação de atributos que capturam a maior parte da variabilidade nos dados. Tais técnicas são baseadas na seguinte suposição-chave:

Suposição: os dados podem ser incorporados em um subespaço dimensional inferior no qual instâncias normais e anomalias parecem significativamente diferentes.

Assim, a abordagem geral adotada pelas técnicas de detecção de anomalias espectrais é determinar tais subespaços (embeddings, projeções, etc.) nos quais as instâncias anômalas podem ser facilmente identificadas [Agovic et al. 2007]. Tais técnicas podem funcionar em um ambiente não supervisionado, bem como semi-supervisionado.

Várias técnicas usam a Análise de Componentes Principais (PCA) [Jolliffe 2002] para projetar dados em um espaço de dimensão inferior. Uma dessas técnicas [Parra et al. 1996] analisa a projeção de cada instância de dados ao longo dos componentes principais com baixa variância. Uma instância normal que satisfaz a estrutura de correlação dos dados terá um valor baixo para tais projeções, enquanto uma instância anômala que se desvia da estrutura de correlação terá um valor grande. Dutta et al. [2007] adotam essa abordagem para detectar anomalias em catálogos de astronomia.

Ide e Kashima [2004] propõem uma técnica espectral para detectar anomalias em uma série temporal de gráficos. Cada gráfico é representado como uma matriz de adjacência para um determinado tempo. Em cada instância de tempo, o componente principal da matriz é escolhido como o vetor de atividade para o gráfico fornecido. A série temporal dos vetores de atividade é considerada como uma matriz e o vetor singular esquerdo principal é obtido para capturar as dependências normais ao longo do tempo nos dados. Para um novo gráfico (teste), o ângulo entre seu vetor de atividade e o vetor singular esquerdo principal obtido dos gráficos anteriores é calculado e usado para determinar a pontuação de anomalia do gráfico de teste. Em uma abordagem semelhante, Sun et al. [2007] propõem uma técnica de detecção de anomalias em uma sequência de gráficos realizando a Decomposição de Matriz Compacta (CMD) na matriz de adjacência para cada gráfico e, assim, obtendo uma aproximação da matriz original. Para cada gráfico na sequência, os autores realizam a CMD e calculam o erro de aproximação entre a matriz de adjacência original e a matriz aproximada. Os autores constroem uma série temporal dos erros de aproximação e detectam anomalias na série temporal de erros; o gráfico correspondente ao erro de aproximação anômalo é declarado anômalo.

Shyu et al. [2003] apresentam uma técnica de detecção de anomalias onde os autores realizam PCA robusta [Huber 1974] para estimar os componentes principais da matriz de covariância dos dados de treinamento normais. A fase de teste envolve comparações

ing cada ponto com os componentes e atribuindo uma pontuação de anomalia com base na distância do ponto dos componentes principais. Assim, se a projeção de x nos componentes principais for y1, y2, . . ., yp e os autovalores correspondentes forem ÿ1, ÿ2, . . ., ÿp, então

$$\sum_{eu=1}^{q} \frac{e_{eu}^{2}}{eu} = \frac{2\,e\,1}{2} + \frac{2\,e}{\ldots} + \ddot{y}1\,\ddot{y}2 \qquad \frac{2\,e\,q}{\ddot{y}q}, \; q \ddot{y} p \tag{5}$$

tem uma distribuição qui-quadrado [Hawkins 1974]. Usando este resultado, os autores propõem que, para um dado nível de significância ÿ, a observação x é uma anomalia se

$$\sum_{eu=1}^{q} \frac{2_{eu}}{e\,\ddot{y}i} > \ddot{y}2_{q}\,(a) \tag{6}$$

Pode ser demonstrado que a quantidade calculada na Equação 5 é igual à distância de Maha-lanobis da instância x da média da amostra (ver Equação 3) quando q = p [Shyu et al. 2003]. Assim, a técnica baseada em PCA robusta é a mesma que uma técnica estatística discutida na Seção 7.1.1 em um subespaço menor.

A técnica robusta baseada em PCA foi aplicada ao domínio de detecção de intrusão de rede [Shyu et al. 2003; Lakhina et al. 2005; Thottan e Ji 2003] e para detectar anomalias em componentes de naves espaciais [Fujimaki et al. 2005].

As técnicas baseadas em PCA padrão
de complexidade computacional são tipicamente lineares em tamanho de dados, mas frequentemente quadráticas no número de dimensões. Técnicas não lineares podem melhorar a complexidade de tempo para ser linear no número de dimensões, mas polinomial no número de componentes principais [Gunter et al. 2007]. Técnicas que realizam SVD nos dados tipicamente quadráticas em tamanho de dados.

Vantagens e desvantagens das técnicas espectrais
As vantagens das técnicas de detecção de anomalias espectrais são as seguintes:

(1) Técnicas espectrais realizam automaticamente a redução de dimensionalidade e, portanto, são adequadas para lidar com conjuntos de dados de alta dimensão. Além disso, elas também podem ser usadas como uma etapa de pré-processamento seguida pela aplicação de qualquer técnica de detecção de anomalia existente no espaço transformado.

(2) As técnicas espectrais podem ser usadas em um ambiente não supervisionado.

As desvantagens das técnicas de detecção de anomalias espectrais são as seguintes:

(1) As técnicas espectrais são úteis apenas se as instâncias normais e anômalas forem separáveis na incorporação dimensional inferior dos dados.

(2) As técnicas espectrais geralmente apresentam alta complexidade computacional.

10. LIDANDO COM ANOMALIAS CONTEXTUAIS

As técnicas de detecção de anomalias discutidas nas seções anteriores focam principalmente na detecção de anomalias pontuais. Nesta seção, discutiremos técnicas de detecção de anomalias que lidam com anomalias contextuais.

Conforme discutido na Seção 2.2.2, as anomalias contextuais exigem que os dados tenham um conjunto de atributos contextuais (para definir um contexto) e um conjunto de atributos comportamentais (para

detectar anomalias dentro de um contexto). Song et al. [2007] usam os termos atributos ambientais e indicadores que são análogos à nossa terminologia. Algumas das maneiras pelas quais os atributos contextuais podem ser definidos são:

(1) Espacial: Os dados têm atributos espaciais, que definem a localização de uma instância de dados e, portanto, uma vizinhança espacial. Várias técnicas de detecção de anomalias baseadas em contexto [Lu et al. 2003; Shekhar et al. 2001; Kou et al. 2006; Sun e Chawla 2004] foram propostas para dados com dados espaciais.

(2) Gráficos: As arestas que conectam os nós (instâncias de dados) definem a vizinhança para cada nó. Técnicas de detecção de anomalias contextuais foram aplicadas a dados baseados em gráficos por Sun et al. [2005].

(3) Sequencial: Os dados são sequenciais, ou seja, os atributos contextuais de um dado instância é sua posição na sequência.

Dados de séries temporais foram amplamente explorados na categoria de detecção de anomalias contextuais [Abraham e Chuang 1989; Abraham e Box 1979; Rousseeuw e Leroy 1987; Bianco et al. 2001; Fox 1972; Salvador e Chan 2003; Tsay et al. 2000; Galeano et al. 2004; Zeevi et al. 1997].

Outra forma de dados sequenciais para os quais técnicas de detecção de anomalias foram desenvolvidas são os dados de eventos, nos quais cada evento tem um registro de data e hora (como dados de chamada do sistema operacional ou dados da web [Ilgun et al. 1995; Vilalta e Ma 2002; Weiss e Hirsh 1998; Smyth 1994]). A diferença entre dados de séries temporais e sequências de eventos é que, para as últimas, o tempo entre chegadas entre eventos consecutivos é irregular.

(4) Perfil: Muitas vezes, os dados podem não ter uma estrutura espacial ou sequencial explícita, mas ainda podem ser segmentados ou agrupados em componentes usando um conjunto de atributos contextuais. Esses atributos são normalmente usados para criar perfis e agrupar usuários em sistemas de monitoramento de atividades, como detecção de fraudes em celulares [Fawcett e Provost 1999; Teng et al. 1990], bancos de dados de CRM [He et al. 2004b] e detecção de fraudes em cartões de crédito [Bolton e Hand 1999]. Os usuários são então analisados dentro de seu grupo para anomalias.

Em comparação com a rica literatura sobre técnicas de detecção de anomalias pontuais, a pesquisa sobre detecção de anomalias contextuais tem sido limitada. Em termos gerais, tais técnicas podem ser classificadas em duas categorias. A primeira categoria de técnicas reduz um problema de detecção de anomalias contextuais a um problema de detecção de anomalias pontuais, enquanto a segunda categoria de técnicas modela a estrutura nos dados e usa o modelo para detectar anomalias.

10.1 Redução ao problema de detecção de anomalias pontuais

Como anomalias contextuais são instâncias de dados individuais (como anomalias pontuais), mas são anômalas apenas em relação a um contexto, uma abordagem é aplicar uma técnica conhecida de detecção de anomalias pontuais dentro de um contexto.

Uma técnica genérica baseada em redução consiste em duas etapas. Primeiro, identifique um contexto para cada instância de teste usando os atributos contextuais. Segundo, calcule a pontuação de anomalia para a instância de teste dentro do contexto usando uma técnica de detecção de anomalia de ponto conhecida.

Um exemplo da técnica de redução genérica foi proposto para o cenário em que a identificação do contexto não é direta [Song et al. 2007].
Os autores assumem que os atributos já estão particionados em atributos contextuais e comportamentais. Assim, cada instância de dados d pode ser representada como [x, y].
Os dados contextuais são particionados usando uma mistura de modelos gaussianos, digamos U. Os dados comportamentais também são particionados usando outra mistura de modelos gaussianos, digamos V. Uma função de mapeamento, p(Vj |Ui) também é aprendida. Esse mapeamento indica a probabilidade da parte indicadora de um ponto de dados y ser gerada a partir de um componente de mistura Vj , quando a parte ambiental x é gerada por Ui . Assim, para uma dada instância de teste d = [x, y], a pontuação de anomalia é dada por:

$$\text{Pontuação de anomalia} = \sum_{eu=1}^{nU} p(x \ddot{y} Ui) \sum_{j=1}^{nV} p(y \ddot{y} Vj)p(Vj|Ui)$$

onde nU é o número de componentes da mistura em U e NV é o número de componentes da mistura em V . p(x ÿ Ui) indica a probabilidade de um ponto de amostra x ser gerado a partir do componente da mistura Ui enquanto p(y ÿ Uj) indica a probabilidade de um ponto de amostra y ser gerado a partir do componente da mistura Vj .

Outro exemplo da técnica genérica é aplicado à detecção de fraudes em celulares [Fawcett e Provost 1999]. Os dados neste caso consistem em registros de uso de celulares. Um dos atributos nos dados é o usuário do celular, que é usado como atributo contextual. A atividade de cada usuário é então monitorada para detectar anomalias usando outros atributos. Uma técnica semelhante é adotada para segurança de computadores [Teng et al. 1990], onde os atributos contextuais são: ID do usuário, hora do dia. Os atributos restantes são comparados com regras existentes que representam o comportamento normal para detectar anomalias. A análise de grupo de pares [Bolton e Hand 1999] é outra técnica semelhante, onde os usuários são agrupados como pares e analisados dentro de um grupo para fraude. He et al. [2004b] propõem o conceito de detecção de anomalias de classe, que é essencialmente segmentar os dados usando os rótulos de classe e, em seguida, aplicar uma técnica conhecida de detecção de anomalias baseada em agrupamento [He et al. 2002] para detectar anomalias dentro deste subconjunto.

Para dados espaciais, as vizinhanças são intuitivas e diretas de detectar [Ng e Han 1994] usando as coordenadas de localização. A detecção de anomalias baseada em gráficos [Shekhar et al. 2001; Lu et al. 2003; Kou et al. 2006] usa a pontuação de Grubb [Grubbs 1969] ou técnicas de detecção de anomalias de pontos estatísticos semelhantes para detectar anomalias dentro de uma vizinhança espacial. Sun e Chawla [2004] usam uma medida baseada em distância chamada SLOM (Spatial Local Outlier Measure [Sun e Chawla 2006]) para detectar anomalias espaciais dentro de uma vizinhança.

Outro exemplo da técnica genérica aplicada a dados de séries temporais é proposto por Basu e Meckesheimer [2007]. Para uma dada instância em uma série temporal, os autores comparam o valor observado à mediana dos valores de vizinhança. Uma técnica de transformação para dados de séries temporais foi proposta usando espaços de fase [Ma e Perkins 2003b]. Essa técnica converte uma série temporal em um conjunto de vetores desdobrando a série temporal em um espaço de fase usando um processo de incorporação de atraso de tempo.
As relações temporais em qualquer instância de tempo são incorporadas no vetor de fase para essa instância. Os autores usam essa técnica para transformar uma série temporal em espaço de características e, em seguida, usam SVMs de uma classe para detectar anomalias. Cada anomalia pode ser

traduzido para um valor em determinada instância de tempo na série temporal original.

10.2 Utilizando a Estrutura em Dados Em

vários cenários, dividir dados em contextos não é simples. Isso é tipicamente verdadeiro para dados de séries temporais e dados de sequência de eventos. Em tais casos, técnicas de modelagem de séries temporais e de sequência são estendidas para detectar anomalias contextuais nos dados.

Uma técnica genérica nesta categoria pode ser descrita como segue. Um modelo é aprendido a partir dos dados de treinamento que podem prever o comportamento esperado com relação a um determinado contexto. Se o comportamento esperado for significativamente diferente do comportamento observado, uma anomalia é declarada. Um exemplo simples desta técnica genérica é a regressão na qual os atributos contextuais podem ser usados para prever o atributo comportamental ajustando uma linha de regressão nos dados.

Para dados de séries temporais, várias técnicas baseadas em regressão para modelagem de séries temporais, como regressão robusta [Rousseeuw e Leroy 1987], modelos autorregressivos [Fox 1972], modelos ARMA [Abraham e Chuang 1989; Abraham e Box 1979; Galeano et al. 2004; Zeevi et al. 1997] e modelos ARIMA [Bianco et al. 2001; Tsay et al. 2000], foram desenvolvidas para detecção de anomalias contextuais. Técnicas baseadas em regressão foram estendidas para detectar anomalias contextuais em um conjunto de sequências coevolutivas modelando a regressão, bem como a correlação entre as sequências [Yi et al. 2000].

Um dos primeiros trabalhos em detecção de anomalias de séries temporais foi proposto por Fox [1972], onde uma série temporal foi modelada como um processo auto-regressivo estacionário. Qualquer observação é testada para ser uma anomalia comparando-a com a matriz de covariância do processo auto-regressivo. Se a observação cair fora do erro modelado para o processo, ela é declarada como uma anomalia. Uma extensão para esta técnica é feita usando a Regressão de Vetor de Suporte para estimar os parâmetros de regressão e então usando o modelo aprendido para detectar novidades nos dados [Ma e Perkins 2003a].

Uma técnica para detectar uma única anomalia (discordância) em uma sequência de alfabetos foi proposta por Keogh et al. [2004]. A técnica adota uma abordagem de dividir e conquistar. A sequência é dividida em duas partes e a Complexidade de Kolmogorov é calculada para cada uma. Aquela com maior complexidade contém a anomalia. A sequência é dividida recursivamente até que reste um único evento que é declarado como a anomalia na sequência.

Weiss e Hirsh [1998] propõem uma técnica para detectar eventos raros em dados sequenciais, onde eles usam eventos que ocorrem antes de um tempo específico para prever o evento que ocorre naquela instância de tempo. Se a previsão não corresponder ao evento real, ele é declarado raro. Essa ideia é estendida em outras áreas, onde os autores usaram Frequent Itemset Mining [Vilalta e Ma 2002], Finite State Automaton (FSA) [Ilgun et al. 1995; Salvador e Chan 2003] e Markov Models [Smyth 1994] para determinar probabilidades condicionais para eventos com base no histórico de eventos.

Marceau [2000] usa FSA para prever o próximo evento de uma sequência com base nos n eventos anteriores. Eles aplicam essa técnica ao domínio de detecção de intrusão de chamada de sistema. Hollmen e Tresp [1999] empregam HMM para detecção de fraude em telefones celulares.
Os autores usam um modelo de chamada de comutação de regime hierárquico para modelar a atividade de telefone celular de um usuário. O modelo prevê a probabilidade de uma fraude ocorrer para uma chamada usando o modelo aprendido. A estimativa de parâmetros é feita usando o EM

algoritmo.

Um modelo para detectar intrusões em redes telefônicas foi proposto por Scott [2001] e para modelar dados de cliques na web por Ihler et al. [2006]. Ambos os artigos seguem uma técnica na qual assumem que o comportamento normal em uma série temporal é gerado por um processo de Poisson não estacionário enquanto as anomalias são geradas por um processo de Poisson homogêneo. A transição entre comportamento normal e anômalo é modelado usando um processo de Markov. As técnicas propostas em cada um desses artigos use a técnica de estimativa de Markov Chain Monte Carlo (MCMC) para estimar os parâmetros para esses processos. Para teste, uma série temporal é modelada usando este processo e os períodos de tempo em que o comportamento anômalo esteve ativo são considerados como anomalias.

A estrutura do gráfico bipartido em redes P2P foi usada para primeiro identificar uma vizinhança para qualquer nó no gráfico [Sun et al. 2005] e, em seguida, detectar a relevância desse nó dentro da vizinhança. Um nó com uma pontuação de relevância baixa é tratado como uma anomalia. Os autores também propõem uma técnica aproximada onde o o gráfico é primeiro particionado em subgráficos não sobrepostos usando o particionamento de gráfico algoritmo como METIS [Karypis e Kumar 1998]. A vizinhança de um nó é então computado dentro de sua partição.

Complexidade Computacional

A complexidade computacional da fase de treinamento em técnicas de detecção de anomalias contextuais baseadas em redução depende da técnica de redução, bem como a técnica de detecção de anomalias pontuais usada em cada contexto. Enquanto as técnicas de segmentação/ particionamento têm uma etapa de redução rápida, as técnicas que usam clustering, ou estimativa de mistura de modelos, são relativamente mais lentas. Como a redução simplifica o problema de detecção de anomalias, técnicas rápidas de detecção de anomalias pontuais pode ser usado para acelerar a segunda etapa. A fase de testes é relativamente cara já que para cada instância de teste, seu contexto é determinado e, então, um rótulo de anomalia ou a pontuação é atribuída usando uma técnica de detecção de anomalias pontuais.

A complexidade computacional da fase de treinamento na detecção de anomalias contextuais técnicas que utilizam a estrutura dos dados para construir modelos, normalmente é mais alto que de técnicas que reduzem o problema à detecção de anomalias pontuais. Uma vantagem para tais técnicas é que a fase de teste é relativamente rápida, uma vez que cada instância é apenas comparado ao modelo único e recebe uma pontuação de anomalia ou uma pontuação de anomalia rótulo.

Vantagens e desvantagens das técnicas de detecção de anomalias contextuais

A principal vantagem das técnicas de detecção de anomalias contextuais é que elas permitem uma definição natural de uma anomalia em muitas aplicações da vida real onde instâncias de dados tendem a ser semelhantes dentro de um contexto. Tais técnicas são capazes de detectar anomalias que podem não ser detectadas por técnicas de detecção de anomalias pontuais que tomam uma visão global dos dados.

A desvantagem das técnicas de detecção de anomalias contextuais é que elas são aplicável somente quando um contexto pode ser definido.

11. LIDANDO COM ANOMALIAS COLETIVAS

Esta seção discute as técnicas de detecção de anomalias que focam na detecção de anomalias coletivas. Conforme mencionado anteriormente, anomalias coletivas são um subconjunto de instâncias que ocorrem juntas como uma coleção e cuja ocorrência não é normal com relação a um comportamento normal. As instâncias individuais pertencentes a esta coleção não são necessariamente anomalias por si mesmas, mas é sua coocorrência em uma forma particular que as torna anomalias. O problema de detecção de anomalias coletivas é mais desafiador do que a detecção de anomalias pontuais e contextuais porque envolve explorar a estrutura nos dados para regiões anômalas.

Um requisito primário de dados para detecção de anomalias coletivas é a presença de relacionamento entre instâncias de dados. Três tipos de relações que foram exploradas com mais frequência são sequenciais, espaciais e gráficos:

—Técnicas de Detecção de Anomalias Sequenciais: Essas técnicas trabalham com dados sequenciais e encontram subsequências como anomalias (também chamadas de anomalias sequenciais). Conjuntos de dados típicos incluem dados de sequência de eventos, como dados de chamada de sistema [Forrest et al. 1999] ou dados de séries temporais numéricas [Chan e Mahoney 2005].

—Técnicas de Detecção de Anomalias Espaciais: Essas técnicas trabalham com dados espaciais e encontram sub-regiões conectadas dentro dos dados como anomalias (também chamadas de anomalias espaciais). Técnicas de detecção de anomalias foram aplicadas a dados de imagens multiespectrais [Hazel 2000].

—Técnicas de detecção de anomalias de gráficos: Essas técnicas funcionam com dados de gráficos e encontram subgráficos conectados dentro dos dados como anomalias (também chamadas de anomalias de gráficos). Técnicas de detecção de anomalias foram aplicadas a dados de gráficos [Noble e Cook 2003].

Pesquisas substanciais foram feitas no campo de detecção de anomalias sequenciais; isso pode ser atribuído à existência de dados sequenciais em vários domínios de aplicação importantes. A detecção de anomalias espaciais foi explorada principalmente no domínio de processamento de imagens. As subseções a seguir discutem cada uma dessas categorias em detalhes.

11.1 Lidando com anomalias sequenciais

Conforme mencionado anteriormente, a detecção coletiva de anomalias em dados de sequência envolve a detecção de sequências que são anômalas em relação a uma definição de comportamento normal. Dados de sequência são muito comuns em uma ampla gama de domínios onde uma ordenação natural é imposta em instâncias de dados por tempo ou posição. Na literatura de detecção de anomalias, dois tipos de sequências são tratados. O primeiro tipo de sequências são simbólicas, como uma sequência de chamadas de sistema operacional ou uma sequência de entidades biológicas. O segundo tipo de sequências são contínuas ou séries temporais. As sequências também podem ser univariadas, nas quais cada evento na sequência é uma observação univariada, ou multivariadas, nas quais cada evento na sequência é uma observação multivariada.

O problema de detecção de anomalias para sequências pode ser definido de diferentes maneiras e são discutidos abaixo.

11.1.1 Detecção de sequência anômala em um conjunto de sequências. O objetivo das técnicas nesta categoria é detectar sequências anômalas de um determinado conjunto de

sequências. Tais técnicas podem operar em um modo semi-supervisionado ou em um modo não supervisionado.

Os principais desafios enfrentados pelas técnicas nesta categoria são:

—As sequências podem não ter o mesmo comprimento.

—As sequências de teste podem não estar alinhadas entre si ou com sequências normais.

Por exemplo, o primeiro evento em uma sequência pode corresponder ao terceiro evento em outra sequência. Comparar tais sequências é um problema fundamental com sequências biológicas [Gusfield 1997], onde diferentes técnicas de alinhamento de sequências e correspondência de sequências são exploradas.

As técnicas para abordar esse problema seguem uma das duas abordagens a seguir:

Redução ao Problema de Detecção de Anomalias Pontuais Uma
abordagem geral para resolver o problema acima seria transformar as sequências em um espaço de características finito e então usar uma técnica de detecção de anomalias pontuais no novo espaço para detectar anomalias.

Certas técnicas assumem que todas as sequências têm comprimentos iguais. Assim, elas tratam cada sequência como um vetor de atributos e empregam uma técnica de detecção de anomalias pontuais para detectar anomalias. Por exemplo, se um conjunto de dados contém sequências de comprimento 10, elas podem ser tratadas como registros de dados com 10 características. Uma medida de similaridade ou distância pode ser definida entre um par de sequências e qualquer técnica de detecção de anomalias pontuais pode ser aplicada a tais conjuntos de dados. Essa abordagem foi adotada para conjuntos de dados de séries temporais [Caudell e Newman 1993; Blender et al. 1997].
No primeiro artigo, os autores aplicam a técnica de detecção de anomalias baseada em redes neurais ART (Teoria de Ressonância Adaptativa) para detectar anomalias em um conjunto de dados de séries temporais, enquanto o último artigo usa uma técnica de detecção de anomalias baseada em agrupamento para identificar regimes de ciclones (anomalias) em dados meteorológicos.

Conforme mencionado anteriormente, as sequências fornecidas podem não ter o mesmo comprimento. Certas técnicas abordam esse problema transformando cada sequência em um registro de número igual de atributos. Uma técnica de transformação foi proposta para dados de várias séries temporais [Chan e Mahoney 2005], conhecida como Box Modeling. Em um modelo de caixa, para cada série temporal, cada instância dessa série temporal é atribuída a uma caixa dependendo de seu valor. Essas caixas são então tratadas como recursos (o número de caixas é o número de recursos no espaço de recursos transformado). Os autores então aplicam técnicas de detecção de anomalias pontuais — uma técnica baseada em distância euclidiana e uma técnica baseada em classificação usando RIPPER para detectar séries temporais anômalas nos dados.

Várias técnicas abordam a questão do comprimento desigual de sequências usando uma métrica de similaridade ou distância que pode calcular similaridade ou distância entre duas sequências de comprimento desigual. Por exemplo, [Budalakoti et al. 2006] empregam o comprimento da maior subsequência comum como medida de similaridade para sequências simbólicas. Os autores subsequentemente aplicam uma técnica de detecção de anomalias baseada em agrupamento, usando essa medida de similaridade.

11.1.1.1 Modelagem de Sequências. As transformações discutidas na seção anterior são apropriadas quando todas as sequências estão alinhadas corretamente. Muitas vezes, a suposição de alinhamento se torna muito proibitiva. Pesquisas lidando com dados de chamada de sistema, dados biológicos, etc., exploram outras alternativas para detectar anomalias coletivas.

Essas técnicas operam em modo semissupervisionado e, portanto, exigem um conjunto de treinamento de sequências normais.

A modelagem de associação sequencial foi usada para gerar regras sequenciais a partir de sequências [Teng et al. 1990]. Os autores usam uma abordagem chamada aprendizado indutivo baseado em tempo para gerar regras a partir do conjunto de sequências normais. A sequência de teste é comparada a essas regras e é declarada uma anomalia se contiver padrões para os quais nenhuma regra foi gerada.

A modelagem Markoviana de sequências tem sido a abordagem mais popular nesta categoria. As técnicas de modelagem usadas nesta categoria variam de Autômatos de Estado Finito (FSA) a modelos de Markov. FSA têm sido usados para detectar anomalias em dados de protocolo de rede [Sekar et al. 2002; Sekar et al. 1999]. Anomalias são detectadas quando uma dada sequência de eventos não resulta em atingir um dos estados finais.
Os autores também aplicam sua técnica à detecção de intrusão de chamadas do sistema operacional [Sekar et al. 2001].

Ye [2004] propõe uma abordagem simples de modelagem de cadeia de Markov de 1 ordem para detectar se uma dada sequência S é uma anomalia. O autor determina a probabilidade de S, P(S) usando a seguinte equação

$$P(S) = qS1 \prod_{t=2}^{|E|} pStÿ1St$$

onde qS1 é a probabilidade de observar o símbolo S1 no conjunto de treinamento e pStÿ1St é a probabilidade de observar o símbolo St após o símbolo Stÿ1 no conjunto de treinamento. O inverso de P(S) é a pontuação de anomalia para S. A desvantagem dessa técnica é que a cadeia de Markov de ordem única não pode modelar dependências de ordem superior nas sequências.

Forrest et al. [1999] propõem uma técnica baseada no Modelo Oculto de Markov (HMM) para detectar rastros de programas anômalos em dados de chamadas do sistema operacional. Os autores treinam um HMM usando as sequências de treinamento. Os autores propõem duas técnicas de teste. Na primeira técnica, eles calculam a probabilidade de uma sequência de teste S ser gerada pelo HMM aprendido usando o algoritmo de Viterbi. A segunda técnica é usar o Autômato de Estado Finito (FSA) subjacente do HMM.
As transições de estado e as saídas feitas pelo HMM para produzir a sequência de teste são registradas. Os autores contam o número de vezes que o HMM teve que fazer uma transição de estado improvável ou produzir um símbolo improvável (usando um limite definido pelo usuário) como incompatibilidades. O número total de incompatibilidades denota a pontuação de anomalia para essa sequência.

Uma Probabilistic Suffix Trees (PST) é outra ferramenta de modelagem que foi aplicada para detectar anomalias coletivas em bancos de dados sequenciais. Uma PST é uma representação compacta de uma cadeia de Markov de ordem variável. Yang e Wang [2003] usam PST para agrupar sequências e detectar sequências anômalas como um subproduto. Da mesma forma, Smyth [1997] e Cadez et al. [2000] usam HMMs para agrupar o conjunto de sequências e detectar quaisquer sequências que não pertencem a nenhum cluster como anomalias.

Outra ferramenta de modelagem usada para detecção de anomalias sequenciais é a Sparse Markov Trees (SMT), que é semelhante a uma PST com a diferença de que permite símbolos curinga dentro de um caminho. Essa técnica foi usada por Eskin et al. [2001], que treinam uma mistura de SMT usando o conjunto de treinamento. Cada SMT tem uma localização diferente de

curingas. A fase de teste envolve prever a probabilidade P(Sn|Snÿ1 . . . S1) usando o melhor SMT da mistura. Se essa probabilidade estiver abaixo de um certo limite, a sequência de teste é declarada como uma anomalia.

11.1.2 Detectando subsequências anômalas em uma sequência longa. O objetivo das técnicas pertencentes a esta categoria é detectar uma subsequência dentro de uma dada sequência que seja anômala em relação ao resto da sequência. Tais subsequências anômalas também foram referidas como discordâncias [Bu et al. 2007; Fu et al. 2006; Keogh et al. 2005; Yankov et al. 2007].

Essa formulação de problema ocorre em conjuntos de dados de eventos e séries temporais onde os dados estão na forma de uma longa sequência e contêm regiões anômalas.
As técnicas que abordam esse problema, normalmente funcionam em um modo não supervisionado, devido à falta de quaisquer dados de treinamento. A suposição subjacente é que o comportamento normal da série temporal segue um padrão definido. Uma subsequência dentro da sequência longa que não está em conformidade com esse padrão é uma anomalia.

Os principais desafios enfrentados pelas técnicas nesta categoria são:

—O comprimento da subsequência anômala a ser detectada não é geralmente definido.
Uma sequência longa pode conter regiões anômalas de comprimentos variáveis. Assim, a segmentação de comprimento fixo da sequência geralmente não é útil.

—Como a sequência de entrada contém regiões anômalas, torna-se desafiador criar um modelo robusto de normalidade.

Chakrabarti et al. [1998] propõem uma técnica de detecção de surpresa em transações de cesta de mercado. Os dados são uma sequência de conjuntos de itens, ordenados por tempo. Os autores propõem segmentar a sequência de conjuntos de itens de modo que a soma do número de bits necessários para codificar cada segmento (usando o Teorema da Informação clássico de Shannon) seja minimizada. Os autores mostram que existe uma solução ótima para encontrar tal segmentação. Os segmentos que requerem o maior número de bits para codificação são tratados como anomalias.

Keogh et al. [2004] propõem um algoritmo chamado Window Comparison Anomaly Detection (WCAD), onde os autores extraem subsequências de uma dada sequência de observações contínuas usando uma janela deslizante. Os autores comparam cada subsequência com a sequência inteira usando uma medida de dissimilaridade baseada em compressão.
A pontuação de anomalia de cada subsequência é sua dissimilaridade com a sequência inteira.
Keogh et al [2005; 2006] propõem uma técnica relacionada (HOT SAX) para resolver o problema acima para séries temporais contínuas. A abordagem básica seguida pelos autores é extrair subsequências da sequência dada usando janela deslizante e, em seguida, calcular a distância de cada subsequência para sua subsequência não sobreposta mais próxima dentro da sequência original. A pontuação de anomalia de uma subsequência é proporcional à sua distância de seus vizinhos mais próximos. A distância entre duas sequências é medida usando medida euclidiana. Abordagem semelhante também é aplicada ao domínio de dados médicos por Lin et al. [2005]. Os mesmos autores propõem o uso da transformação baseada em Wavelet de Haar para tornar a técnica anterior mais eficiente [Fu et al. 2006; Bu et al. 2007].

Modelos de Markov de Máxima Entropia (Maxent) [McCallum et al. 2000; Pavlov e Pennock 2002; Pavlov 2003] assim como Campos Aleatórios Condicionais (CRF) [Lafferty et al. 2001], foram usados para segmentar dados de texto. A formulação do problema

é preciso prever a sequência de estados mais provável para uma determinada sequência de observação. Qualquer segmento anômalo dentro da sequência de observação terá uma baixa probabilidade condicional para qualquer sequência de estados.

11.1.3 Determinar se a frequência de um padrão de consulta em uma sequência dada é anômala em relação à sua frequência esperada. Tal formulação do problema de detecção de anomalias é motivada pelo tipo de dados caso vs controle [Helman e Bhangoo 1997; Gwadera et al. 2005b; 2004]. A ideia é detectar padrões cuja ocorrência em um dado conjunto de dados de teste (caso) seja diferente de sua ocorrência em um conjunto de dados normal (controle). Keogh et al. [2002] extraem substrings de uma dada string de alfabetos usando uma janela deslizante. Para cada uma dessas substrings, eles determinam se essa substring é anômala em relação a um banco de dados normal de strings. Os autores usam árvores de sufixos para estimar a frequência esperada de uma substring no banco de dados normal de strings. Em uma abordagem semelhante [Gwadera et al. 2005a], os autores usam Modelos de Markov Interpolados (IMM) para estimar a frequência esperada.

11.2 Lidando com Anomalias Espaciais a

detecção coletiva de anomalias em dados espaciais envolve encontrar subgráficos ou subcomponentes nos dados que são anômalos. Uma quantidade limitada de pesquisa foi feita nesta categoria, então as discutiremos individualmente.

Hazel [2000] propõe uma técnica para detectar regiões em uma imagem que são anômalas em relação ao resto da imagem. A técnica proposta faz uso de Campos de Markov Aleatórios Gaussianos Multivariados (MGMRF) para segmentar uma determinada imagem. Os autores fazem uma suposição de que cada pixel pertencente a uma região anômala da imagem também é uma anomalia contextual dentro de seu segmento. Esses pixels são detectados como anomalias contextuais em relação aos segmentos (estimando a probabilidade condicional de cada pixel) e, então, conectados usando uma estrutura espacial disponível, para encontrar as anomalias coletivas.

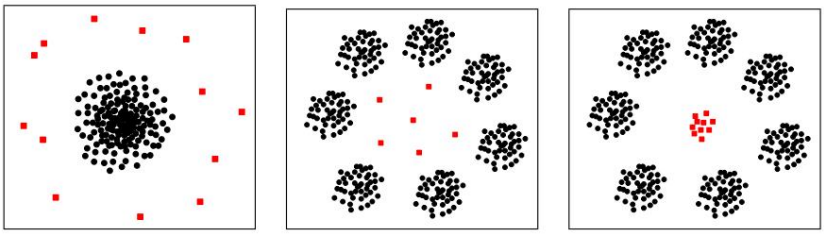
A detecção de anomalias para gráficos foi explorada em domínios de aplicação onde os dados podem ser modelados como gráficos. Noble e Cook [2003] abordam dois problemas distintos de detecção de anomalias coletivas para dados de gráficos. O primeiro problema envolve a detecção de subgráficos anômalos em um determinado gráfico grande. Os autores usam uma técnica de enumeração de subgráficos de baixo para cima e analisam a frequência de um subgráfico no gráfico fornecido para determinar se é uma anomalia ou não. O tamanho do subgráfico também é levado em consideração, uma vez que um subgráfico grande (como o próprio gráfico) está fadado a ocorrer muito raramente no gráfico, enquanto um subgráfico pequeno (como um nó individual) será mais frequente. O segundo problema envolve a detecção se um determinado subgráfico é uma anomalia em relação a um gráfico grande. Os autores medem a regularidade ou entropia do subgráfico no contexto de todo o gráfico para determinar sua anomalia

pontuação.

12. PONTOS FORTES E FRACOS RELATIVOS DA DETECÇÃO DE ANOMALIAS TÉCNICAS

Cada uma das muitas técnicas de detecção de anomalias discutidas nas seções anteriores tem seus pontos fortes e fracos exclusivos. É importante saber qual técnica de detecção de anomalias é mais adequada para um determinado problema de detecção de anomalias.
Dada a complexidade do espaço do problema, não é viável fornecer tal

entendimento para cada problema de detecção de anomalias. Nesta seção, analisamos os pontos fortes e fracos relativos de diferentes categorias de técnicas para algumas configurações de problemas simples.



(a) Conjunto de dados 1 (b) Conjunto de dados 2 (c) Conjunto de dados 3

Fig. 10. Conjuntos de dados 2-D. Instâncias normais são mostradas como círculos e anomalias são mostradas como quadrados.

Por exemplo, vamos considerar o seguinte problema de detecção de anomalias. A entrada são dados contínuos 2D (Figura 10(a)). As instâncias de dados normais são geradas a partir de uma distribuição gaussiana e estão localizadas em um cluster compacto no espaço 2D. As anomalias são muito poucas instâncias geradas a partir de outra distribuição gaussiana cuja média está muito longe da primeira distribuição. Um conjunto de dados de treinamento representativo que contém instâncias do conjunto de dados normais também está disponível. Assim, as suposições feitas pelas técnicas nas Seções 4–9 são válidas para este conjunto de dados e, portanto, quaisquer técnicas de detecção de anomalias pertencentes a essas categorias detectarão as anomalias em tal cenário.

Agora, vamos considerar outro conjunto de dados 2D (Figura 10(b)). Deixe que as instâncias normais sejam tais que sejam geradas por um grande número de diferentes distribuições gaussianas com médias dispostas em um círculo e variância muito baixa. Assim, os dados normais serão um conjunto de clusters compactos dispostos em um círculo. Uma técnica baseada em classificação de uma classe pode aprender um limite circular ao redor de todo o conjunto de dados e, portanto, não será capaz de detectar as anomalias que estão dentro do círculo de clusters. Por outro lado, se cada cluster fosse rotulado como uma classe diferente, uma técnica baseada em classificação multiclasse pode ser capaz de aprender limites ao redor de cada cluster e, portanto, ser capaz de detectar as anomalias no centro. Uma técnica estatística que usa uma abordagem de modelo de mistura para modelar os dados pode ser capaz de detectar as anomalias.

Da mesma forma, técnicas baseadas em clustering e no vizinho mais próximo serão capazes de detectar as anomalias, uma vez que elas estão longe de todas as outras instâncias. Em um exemplo semelhante (Figura 10(c)), se as instâncias anômalas formarem um cluster compacto de tamanho significativo no centro do círculo, tanto as técnicas baseadas em clustering quanto as baseadas no vizinho mais próximo tratarão essas instâncias como normais, exibindo, portanto, desempenho ruim.

Para conjuntos de dados mais complexos, diferentes tipos de técnicas enfrentam desafios diferentes. Técnicas baseadas em vizinho mais próximo e agrupamento sofrem quando o número de dimensões é alto porque as medidas de distância em um grande número de dimensões não são capazes de diferenciar entre instâncias normais e anômalas. Técnicas espectrais abordam explicitamente o problema de alta dimensionalidade mapeando dados para uma projeção dimensional inferior. Mas seu desempenho é altamente dependente da suposição de que as instâncias normais e anomalias são distinguíveis no espaço projetado.

Técnicas baseadas em classificação podem ser uma escolha melhor em tal cenário. Mas para ser

as técnicas mais eficazes baseadas em classificação exigem rótulos para instâncias normais e anômalas, que geralmente não estão disponíveis. Mesmo que os rótulos para instâncias normais e anômalas estejam disponíveis, o desequilíbrio na distribuição dos dois rótulos geralmente torna o aprendizado de um classificador bastante desafiador. Técnicas semissupervisionadas de vizinho mais próximo e agrupamento, que usam apenas os rótulos normais, geralmente podem ser mais eficazes do que as técnicas baseadas em classificação. Técnicas estatísticas, embora não supervisionadas, são eficazes apenas quando a dimensionalidade dos dados é baixa e as suposições estatísticas são válidas. Técnicas de teoria da informação exigem uma medida que seja sensível o suficiente para detectar os efeitos de até mesmo uma única anomalia. Caso contrário, tais técnicas só poderão detectar anomalias quando houver um número significativamente suficiente delas.

Técnicas baseadas em vizinho mais próximo e clustering exigem computação de distância entre um par de instâncias de dados. Assim, tais técnicas assumem que a medida de distância pode discriminar entre as anomalias e instâncias normais bem o suficiente.
Em situações em que é difícil identificar uma boa medida de distância, técnicas baseadas em classificação ou estatísticas podem ser uma escolha melhor.

A complexidade computacional de uma técnica de detecção de anomalias é um aspecto fundamental, especialmente quando a técnica é aplicada a um domínio real. Enquanto técnicas baseadas em classificação, baseadas em cluster e estatísticas têm tempos de treinamento caros, os testes geralmente são rápidos. Muitas vezes isso é aceitável, já que os modelos podem ser treinados de forma off-line enquanto os testes precisam ser em tempo real. Em contraste, técnicas como técnicas baseadas em vizinho mais próximo, teoria da informação e técnicas espectrais que não têm uma fase de treinamento, têm uma fase de teste cara que pode ser uma limitação em um ambiente real.

Técnicas de detecção de anomalias geralmente assumem que anomalias em dados são raras quando comparadas a instâncias normais. Embora essa suposição seja geralmente verdadeira, anomalias nem sempre são raras. Por exemplo, ao lidar com detecção de worms em redes de computadores, o tráfego anômalo (worm) é na verdade mais frequente do que o tráfego normal. Técnicas não supervisionadas não são adequadas para tal detecção de anomalias em massa. Técnicas operando em modos supervisionados ou semissupervisionados podem ser aplicadas para detectar anomalias em massa [Sun et al. 2007; Soule et al. 2005].

13. CONSIDERAÇÕES FINAIS E TRABALHO FUTURO

Nesta pesquisa, discutimos diferentes maneiras pelas quais o problema da detecção de anomalias foi formulado na literatura e tentamos fornecer uma visão geral da enorme literatura sobre várias técnicas. Para cada categoria de técnicas de detecção de anomalias, identificamos uma suposição única sobre a noção de dados normais e anômalos. Ao aplicar uma determinada técnica a um domínio específico, essas suposições podem ser usadas como diretrizes para avaliar a eficácia da técnica naquele domínio. Idealmente, uma pesquisa abrangente sobre detecção de anomalias deve permitir que o leitor não apenas entenda a motivação por trás do uso de uma técnica específica de detecção de anomalias, mas também forneça uma análise comparativa de várias técnicas. Mas a pesquisa atual foi feita de forma não estruturada, sem depender de uma noção unificada de anomalias, o que torna o trabalho de fornecer uma compreensão teórica do problema de detecção de anomalias muito difícil. Um possível trabalho futuro seria unificar as suposições feitas por diferentes técnicas sobre o comportamento normal e anômalo em uma estatística ou ma-

estrutura de aprendizagem de chine. Uma tentativa limitada nessa direção é fornecida por Knorr e Ng [1997], onde os autores mostram a relação entre a distância baseada e anomalias estatísticas para conjuntos de dados bidimensionais.

Há várias direções promissoras para pesquisas futuras em detecção de anomalias. As técnicas de detecção de anomalias contextuais e coletivas estão começando a encontrar aplicabilidade crescente em vários domínios e há muito espaço para desenvolvimento de novas técnicas nesta área. A presença de dados em diferentes sistemas distribuídos locais motivou a necessidade de técnicas de detecção de anomalias distribuídas [Zim-mermann e Mohay 2006]. Embora tais técnicas processem informações disponíveis em vários locais, muitas vezes eles têm que proteger simultaneamente as informações presentes em cada local, exigindo assim técnicas de detecção de anomalias que preservem a privacidade [Vaidya e Clifton 2004]. Com o surgimento das redes de sensores, o processamento de dados à medida que chega tornou-se uma necessidade. Muitas técnicas discutidas nesta pesquisa exigem todos os dados de teste antes de detectar anomalias. Recentemente, as técnicas foi proposto que pode operar de forma online [Pokrajac et al. 2007]; tal técnicas não apenas atribuem uma pontuação de anomalia a uma instância de teste conforme ela chega, mas também atualizar incrementalmente o modelo. Outra área futura onde a detecção de anomalias está encontrando cada vez mais aplicabilidade em sistemas complexos. Um exemplo de tal sistema seria um sistema de aeronave com múltiplos componentes. A detecção de anomalias em tais sistemas envolve a modelagem da interação entre vários componentes [Bronstein e outros 2001].

AGRADECIMENTOS

Os autores agradecem a Shyam Boriah e Gang Fang pelos comentários detalhados sobre o rascunho final do artigo.

Este trabalho foi apoiado pela NASA sob o prêmio NNX08AC36A, NSF grant número CNS-0551551, NSF ITR Grant ACI-0325949, NSF IIS-0713227 e NSF Grant IIS-0308264. O acesso às instalações de computação foi fornecido pela Tecnologia Digital Consórcio.

REFERÊNCIAS

Abe, N., Zadrozny, B., e Langford, J. 2006. Detecção de outliers por aprendizagem ativa. Em Anais da 12ª Conferência Internacional ACM SIGKDD sobre Descoberta de Conhecimento e Mineração de Dados. ACM Press, Nova York, NY, EUA, 504–509.

Abraham, B. e Box, GEP 1979. Análise bayesiana de alguns problemas discrepantes em séries temporais. Biometria 66, 2, 229–236.

Abraham, B. e Chuang, A. 1989. Detecção de outliers e modelagem de séries temporais. Tecnometrics 31, 2, 241–248.

Addison, J., Wermter, S., e MacIntyre, J. 1999. Eficácia da extração de características em redes neurais arquiteturas de rede para detecção de novidades. Em Anais da 9ª Conferência Internacional sobre Redes Neurais Artificiais. Vol. 2. 976–981.

Aeyels, D. 1991. Sobre o comportamento dinâmico do detector de novidades e do filtro de novidades. Em Análise de Sistemas Dinâmicos Controlados - Progresso em Sistemas e Teoria de Controle, B. Bon-nard, B. Bride, J. Gauthier e I. Kupka, Eds. Vol. 8. Springer, Berlim, 1–10.

Agarwal, D. 2005. Uma abordagem bayesiana empírica para detectar anomalias em matrizes multidimensionais dinâmicas. Em Anais da 5ª Conferência Internacional IEEE sobre Mineração de Dados. IEEE Computer Society, Washington, DC, EUA, 26–33.

Agarwal, D. 2006. Detectando anomalias em fluxos de classificação cruzada: uma abordagem bayesiana. Knowl-edge and Information Systems 11, 1, 29–44.

Aggarwal, C. 2005. Sobre detecção de anormalidades em fluxos de dados espúriamente povoados. Em Anais do 5º SIAM Data Mining. 80–91.

Aggarwal, C. e Yu, P. 2001. Detecção de outliers para dados de alta dimensão. Em Proceedings of the ACM SIGMOD International Conference on Management of Data. ACM Press, 37–46.

Aggarwal, CC e Yu, PS 2008. Detecção de outliers com dados incertos. Em SDM. 483–493.

Agovic, A., Banerjee, A., Ganguly, AR, e Protopopescu, V. 2007. Detecção de anomalias em corredores de transporte usando incorporação de manifold. Em First International Workshop on Knowledge Discovery from Sensor Data. ACM Press.

Agrawal, R. e Srikant, R. 1995. Padrões sequenciais de mineração. Em Anais da 11ª Conferência Internacional sobre Engenharia de Dados. IEEE Computer Society, Washington, DC, EUA, 3–14.

Agyemang, M., Barker, K. e Alhajj, R. 2006. Uma pesquisa abrangente de dados numéricos e técnicas de mineração de outliers simbólicos. Intelligent Data Analysis 10, 6, 521–538.

Albrecht, S., Busch, J., Kloppenburg, M., Metze, F., e Tavan, P. 2000. Redes de funções de base radial generalizadas para classificação e detecção de novidades: auto-organização de decisão bayesiana opcional. Neural Networks 13, 10, 1075–1093.

Aleskerov, E., Freisleben, B., e Rao, B. 1997. Cardwatch: Um sistema de mineração de banco de dados baseado em rede neural para detecção de fraude de cartão de crédito. Em Proceedings of IEEE Computational Intelligence for Financial Engineering. 220–226.

Allan, J., Carbonell, J., Doddington, G., Yamron, J., e Yang, Y. 1998. Estudo piloto de detecção e rastreamento de tópicos. Em Proceedings of DARPA Broadcast News Transcription and Understanding Workshop. 194–218.

Anderson, Lunt, Javitz, Tamaru, A., e Valdes, A. 1995. Detectando comportamento incomum de programa usando os componentes estatísticos do NIDES. Tech. Rep. SRI–CSL–95–06, Laboratório de Ciência da Computação, SRI International. maio.

Anderson, D., Frivold, T., Tamaru, A., e Valdes, A. 1994. Sistema especialista em detecção de intrusão de próxima geração (nides), manual do usuário de software, versão beta-atualização. Tech. Rep. SRI– CSL–95–07, Laboratório de Ciência da Computação, SRI International. maio.

Ando, S. 2007. Agrupando agulhas em um palheiro: Uma análise teórica da informação de detecção de minorias e outliers. Em Anais da 7ª Conferência Internacional sobre Mineração de Dados. 13–22.

Angiulli, F. e Pizzuti, C. 2002. Detecção rápida de outliers em espaços de alta dimensão. Em Proceedings of the 6th European Conference on Principles of Data Mining and Knowledge Discovery. Springer-Verlag, 15–26.

Anscombe, FJ e Guttman, I. 1960. Rejeição de outliers. Technometrics 2, 2, 123–147.

Arning, A., Agrawal, R., e Raghavan, P. 1996. Um método linear para detecção de desvio em grandes bancos de dados. Em Anais da 2ª Conferência Internacional de Descoberta de Conhecimento e Mineração de Dados. 164–169.

Augusteijn, M. e Folkert, B. 2002. Classificação de redes neurais e detecção de novidades. Revista Internacional de Sensoriamento Remoto 23, 14, 2891–2902.

Bakar, Z., Mohemad, R., Ahmad, A., e Deris, M. 2006. Um estudo comparativo para técnicas de detecção de outliers em mineração de dados. Cybernetics and Intelligent Systems, 2006 IEEE Conference on, 1–6.

Baker, D., Hofmann, T., McCallum, A., e Yang, Y. 1999. Um modelo probabilístico hierárquico para detecção de novidades em texto. Em Proceedings of International Conference on Machine Learning.

Barbara, D., Couto, J., Jajodia, S., e Wu, N. 2001a. Adam: um banco de testes para explorar o uso de mineração de dados na detecção de intrusão. SIGMOD Rec. 30, 4, 15–24.

Barbara, D., Couto, J., Jajodia, S., e Wu, N. 2001b. Detectando novas intrusões de rede usando estimadores bayesianos. Em Anais da Primeira Conferência Internacional SIAM sobre Mineração de Dados.

Barbara, D., Li, Y., Couto, J., Lin, J.-L., e Jajodia, S. 2003. Bootstrapping de um sistema de detecção de intrusão de mineração de dados. Em Anais do simpósio ACM de 2003 sobre computação aplicada. Imprensa ACM, 421–425.

Barnett, V. 1976. A ordenação de dados multivariados (com discussão). Journal of the Royal Statistical Society. Série A 139, 318–354.

Barnett, V. e Lewis, T. 1994. Outliers em dados estatísticos. John Wiley e filhos.

Barson, P., Davey, N., Field, SDH, Frank, RJ e McAskie, G. 1996. A detecção de fraude em redes de telefonia móvel. Neural Network World 6, 4.

Basu, S., Bilenko, M. e Mooney, RJ 2004. Uma estrutura probabilística para clustering semi-supervisionado. Em Anais da décima conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, Nova York, NY, EUA, 59–68.

Basu, S. e Meckesheimer, M. 2007. Detecção automática de outliers para séries temporais: uma aplicação para dados de sensores. Knowledge and Information Systems 11, 2 (fevereiro), 137–154.

Bay, SD e Schwabacher, M. 2003. Mineração de outliers baseados em distância em tempo quase linear com randomização e uma regra de poda simples. Em Anais da nona conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, 29–38.

Beckman, RJ e Cook, RD 1983. Outliers...s. Technometrics 25, 2, 119–149.

Bejerano, G. e Yona, G. 2001. Variações em árvores de sufixos probabilísticos: modelagem estatística e predição de famílias de proteínas. Bioinformática 17, 1, 23–43.

Bentley, JL 1975. Árvores de busca binárias multidimensionais usadas para busca associativa. Com-munications of the ACM 18, 9, 509–517.

Bianco, AM, Ben, MG, Martinez, EJ e Yohai, VJ 2001. Detecção de outliers em modelos de regressão com erros arima usando estimativas robustas. Journal of Forecasting 20, 8, 565–579.

Bishop, C. 1994. Detecção de novidades e validação de rede neural. Em Proceedings of IEEE Visão, Imagem e Processamento de Sinais. Vol. 141. 217–222.

Blender, R., Fraedrich, K., e Lunkeit, F. 1997. Identificação de regimes de trilhas de ciclones no Atlântico Norte. Quarterly Journal of the Royal Meteorological Society 123, 539, 727–741.

Bolton, R. e Hand, D. 1999. Métodos de criação de perfil não supervisionados para detecção de fraudes. Em Crédito Pontuação e Controle de Crédito VII.

Boriah, S., Chandola, V., e Kumar, V. 2008. Medidas de similaridade para dados categóricos: Uma avaliação comparativa. Em Anais da oitava Conferência Internacional SIAM sobre Mineração de Dados. 243–254.

Borisyuk, R., Denham, M., Hoppensteadt, F., Kazanovich, Y. e Vinogradova, O. 2000. Um modelo de rede neural oscilatória de memória distribuída esparsa e detecção de novidades. Biosistemas 58, 265–272.

Box, GEP e Tiao, GC 1968. Análise bayesiana de alguns problemas discrepantes. Biometria 55, 1, 119–129.

Branch, J., Szymanski, B., Giannella, C., Wolff, R., e Kargupta, H. 2006. Detecção de outliers na rede em redes de sensores sem fio. Na 26ª Conferência Internacional IEEE sobre Sistemas de Computação Distribuída.

Brause, R., Langsdorf, T., e Hepp, M. 1999. Mineração de dados neurais para detecção de fraudes de cartão de crédito. Em Proceedings of IEEE International Conference on Tools with Artificial Intelligence. 103–106.

Breunig, MM, Kriegel, H.-P., Ng, RT e Sander, J. 1999. Óptica de: Identificando outliers locais. Em Anais da Terceira Conferência Europeia sobre Princípios de Mineração de Dados e Descoberta de Conhecimento. Springer-Verlag, 262–270.

Breunig, MM, Kriegel, H.-P., Ng, RT e Sander, J. 2000. Lof: identificando outliers locais baseados em densidade. Em Anais da Conferência Internacional ACM SIGMOD de 2000 sobre Gerenciamento de Dados. ACM Press, 93–104.

Brito, MR, Chavez, EL, Quiroz, AJ e Yukich, JE 1997. Conectividade do gráfico k-vizinho-mais-próximo mútuo em clusterização e detecção de outliers. Statistics and Probability Letters 35, 1, 33–42.

Brockett, PL, Xia, X., e Derrig, RA 1998. Usando o mapa de características auto-organizável de Kohonen para descobrir fraudes em reivindicações de danos corporais em automóveis. Journal of Risk and Insurance 65, 2 (junho), 245–274.

Bronstein, A., Das, J., Duro, M., Friedrich, R., Kleyner, G., Mueller, M., Singhal, S., e Cohen, I. 2001. Redes bayesianas para detecção de anomalias em serviços baseados na internet. Em Simpósio Internacional sobre Gerenciamento Integrado de Redes,.

Brotherton, T. e Johnson, T. 2001. Detecção de anomalias para aeronaves militares avançadas usando redes neurais. Em Proceedings of 2001 IEEE Aerospace Conference.

Brotherton, T., Johnson, T., e Chadderdon, G. 1998. Classificação e detecção de novidades usando modelos lineares e uma rede neural de função de base elíptica dependente de classe. Em Proceedings of the IJCNN Conference. Anchorage AL.

Bu, Y., Leung, T.-W., Fu, A., Keogh, E., Pei, J., e Meshkin, S. 2007. Wat: Encontrando discordâncias top-k em banco de dados de séries temporais. Em Anais da 7ª Conferência Internacional SIAM sobre Mineração de Dados.

Budalakoti, S., Srivastava, A., Akella, R., e Turkov, E. 2006. Detecção de anomalias em grandes conjuntos de sequências de símbolos de alta dimensão. Rep. Técnico NASA TM-2006-214553, NASA Ames Research Center.

Byers, SD e Raftery, AE 1998. Remoção de desordem do vizinho mais próximo para estimar características em processos de pontos espaciais. Journal of the American Statistical Association 93, 577–584.

Byungho, H. e Sungzoon, C. 1999. Características do mlp autoassociativo como um detector de novidades. Em Proceedings of IEEE International Joint Conference on Neural Networks. Vol. 5. 3086–3091.

Cabrera, JBD, Lewis, L., e Mehra, RK 2001. Detecção e classificação de intrusões e falhas usando sequências de chamadas de sistema. Registros SIGMOD 30, 4, 25–34.

Cadez, I., Heckerman, D., Meek, C., Smyth, P., e White, S. 2000. Visualização de padrões de navegação em um site usando clustering baseado em modelo. Em Anais da sexta conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, Nova York, NY, EUA, 280–284.

Campbell, C. e Bennett, K. 2001. Uma abordagem de programação linear para detecção de novidades. Em Proceedings of Advances in Neural Information Processing. Vol. 14. Cambridge Press.

Caudell, T. e Newman, D. 1993. Uma arquitetura de ressonância adaptativa para definir normalidade e detectar novidades em séries temporais e bancos de dados. Em IEEE World Congress on Neural Networks. IEEE, Portland, OR, 166–176.

Chakrabarti, S., Sarawagi, S., e Dom, B. 1998. Mineração de padrões surpreendentes usando comprimento de descrição temporal. Em Anais da 24ª Conferência Internacional sobre Bancos de Dados Muito Grandes. Morgan Kaufmann Publishers Inc., São Francisco, CA, EUA, 606–617.

Chan, PK e Mahoney, MV 2005. Modelagem de múltiplas séries temporais para detecção de anomalias. Em Anais da Quinta Conferência Internacional IEEE sobre Mineração de Dados. IEEE Computer Society, Washington, DC, EUA, 90–97.

Chandola, V., Boriah, S., e Kumar, V. 2008. Compreendendo medidas de similaridade categórica para detecção de outliers. Tech. Rep. 08-008, Universidade de Minnesota. Mar.

Chandola, V., Eilertson, E., Ertoz, L., Simon, G., e Kumar, V. 2006. Mineração de dados para segurança cibernética. Em Data Warehousing e técnicas de mineração de dados para segurança de computadores, A. Singhal, Ed. Springer.

Chatzigiannakis, V., Papavassiliou, S., Grammatikou, M., e Maglaris, B. 2006. Detecção de anomalias hierárquicas em redes de sensores distribuídas em larga escala. Em ISCC '06: Anais do 11º Simpósio IEEE sobre Computadores e Comunicações. IEEE Computer Society, Washington, DC, EUA, 761–767.

Chaudhary, A., Szalay, AS, e Moore, AW 2002. Detecção de outliers muito rápida em grandes conjuntos de dados multidimensionais. Em Anais do ACM SIGMOD Workshop em Questões de Pesquisa em Mineração de Dados e Descoberta de Conhecimento (DMKD). ACM Press.

Chawla, NV, Japkowicz, N., e Kotcz, A. 2004. Editorial: edição especial sobre aprendizagem com conjuntos de dados desbalanceados. SIGKDD Explorations 6, 1, 1–6.

Chen, D., Shao, X., Hu, B., e Su, Q. 2005. Seleção simultânea de comprimento de onda e detecção de outliers em regressão multivariada de espectros de infravermelho próximo. Analytical Sciences 21, 2, 161–167.

Chiu, A. e chee Fu, AW 2003. Melhorias na detecção de outliers locais. Em Proceedings of 7º Simpósio Internacional de Engenharia e Aplicações de Banco de Dados. 298–307.

Chow, C. e Yeung, D.-Y. 2002. Detectores de intrusão de rede de janela de Parzen. Em Anais da 16ª Conferência Internacional sobre Reconhecimento de Padrões. Vol. 4. IEEE Computer Society, Washington, DC, EUA, 40385.

Cox, KC, Eick, SG, Wills, GJ e Brachman, RJ 1997. Mineração de dados visual: Reconhecimento de fraudes em chamadas telefônicas. Journal of Data Mining and Knowledge Discovery 1, 2, 225–231.

Crook, P. e Hayes, G. 2001. Uma implementação robótica de um método biologicamente inspirado para detecção de novidades. Em Proceedings of Towards Intelligent Mobile Robots Conference. Manchester, Reino Unido.

Crook, PA, Marsland, S., Hayes, G., e Nehmzow, U. 2002. Um conto de dois filtros - detecção de novidades on-line. Em Proceedings of International Conference on Robotics and Automation. 3894–3899.

Cun, YL, Boser, B., Denker, JS, Howard, RE, Habbard, W., Jackel, LD e Henderson, D. 1990. Reconhecimento de dígitos manuscritos com uma rede de retropropagação. Avanços em sistemas de processamento de informações neurais, 396–404.

Das, K. e Schneider, J. 2007. Detectando registros anômalos em conjuntos de dados categóricos. Em Anais da 13ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press.

Dasgupta, D. e Majumdar, N. 2002. Detecção de anomalias em dados multidimensionais usando algoritmo de seleção negativa. Em Proceedings of the IEEE Conference on Evolutionary Computation. Havaí, 1039–1044.

Dasgupta, D. e Nino, F. 2000. Uma comparação de algoritmos de seleção negativa e positiva na detecção de novos padrões. Em Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics. Vol. 1. Nashville, TN, 125–130.

Davy, M. e Godsill, S. 2002. Detecção de mudanças espectrais abruptas usando máquinas de vetores de suporte. uma aplicação para segmentação de sinal de áudio. Em Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing. Orlando, EUA.

Debar, H., Dacier, M., Nassehi, M., e Wespi, A. 1998. Padrões de comprimento fixo vs. variável para detectar comportamento suspeito de processo. Em Anais do 5º Simpósio Europeu sobre Pesquisa em Segurança de Computadores. Springer-Verlag, Londres, Reino Unido, 1–15.

Denning, DE 1987. Um modelo de detecção de intrusão. IEEE Transactions of Software Engineering 13, 2, 222–232.

Desforges, M., Jacob, P., e Cooper, J. 1998. Aplicações da estimativa de densidade de probabilidade para a detecção de condições anormais em engenharia. Em Proceedings of Institute of Mechanical Engineers. Vol. 212. 687–703.

Diaz, I. e Hollmen, J. 2002. Geração residual e visualização para entender novas condições de processo. Em Proceedings of IEEE International Joint Conference on Neural Networks. IEEE, Honolulu, HI, 2070–2075.

Diehl, C. e Hampshire, J. 2002. Classificação de objetos em tempo real e detecção de novidades para vigilância colaborativa por vídeo. Em Proceedings of IEEE International Joint Conference on Neural Networks. IEEE, Honolulu, HI.

Donoho, S. 2004. Detecção precoce de negociação com informações privilegiadas em mercados de opções. Em Anais da décima conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, Nova York, NY, EUA, 420–429.

Dorronsoro, JR, Ginel, F., Sanchez, C., e Cruz, CS 1997. Detecção de fraude neural em operações de cartão de crédito. IEEE Transactions On Neural Networks 8, 4 (julho), 827–834.

Du, W., Fang, L. e Peng, N. 2006. Lad: detecção de anomalias de localização para sensores sem fio redes. J. Parallel Distrib. Comput. 66, 7, 874–886.

Duda, RO, Hart, PE, e Stork, DG 2000. Classificação de padrões (2ª edição). Wiley-Interciência.

Dutta, H., Giannella, C., Borne, K., e Kargupta, H. 2007. Detecção distribuída de outliers top-k em catálogos de astronomia usando o sistema demac. Em Proceedings of 7th SIAM International Conference on Data Mining.

Edgeworth, FY 1887. Sobre observações discordantes. Philosophical Magazine 23, 5, 364–375.

Emamian, V., Kaveh, M., e Tewfik, A. 2000. Agrupamento robusto de sinais de emissão acústica usando a rede kohonen. Em Anais da IEEE International Conference of Acoustics, Speech and Signal Processing. IEEE Computer Society.

Endler, D. 1998. Detecção de intrusão: aplicando aprendizado de máquina a dados de auditoria do Solaris. Em Anais da 14ª Conferência Anual de Aplicações de Segurança de Computadores. IEEE Computer Society, 268.

Ertoz, L., Eilertson, E., Lazarevic, A., Tan, P.-N., Kumar, V., Srivastava, J., e Dokas, P. 2004. MINDS - Sistema de Detecção de Intrusão de Minnesota. Em Mineração de Dados - Desafios da Próxima Geração e Direções Futuras. MIT Press.

Ertoz, L. , Steinbach, M., e Kumar, V. 2003. Encontrar tópicos em coleções de documentos: A compartilhou abordagem do vizinho mais próximo. Em Clustering and Information Retrieval. 83–104.

Escalante, HJ 2005. Uma comparação de algoritmos de detecção de outliers para machine learning. Em Proceedings of the International Conference on Communications in Computing.

Eskin, E. 2000. Detecção de anomalias em dados ruidosos usando distribuições de probabilidade aprendidas. Em Anais da Décima Sétima Conferência Internacional sobre Aprendizado de Máquina. Morgan Kauf-mann Publishers Inc., 255–262.

Eskin, E., Arnold, A., Prerau, M., Portnoy, L., e Stolfo, S. 2002. Uma estrutura geométrica para detecção de anomalias não supervisionadas. Em Proceedings of Applications of Data Mining in Computer Security. Kluwer Academics, 78–100.

Eskin, E., Lee, W. e Stolfo, S. 2001. Modelagem de chamada de sistema para detecção de intrusão usando tamanhos de janelas dinâmicos. Em Proceedings of DISCEX.

Ester, M., Kriegel, H.-P., Sander, J., e Xu, X. 1996. Um algoritmo baseado em densidade para descobrir clusters em grandes bancos de dados espaciais com ruído. Em Anais da Segunda Conferência Internacional sobre Descoberta de Conhecimento e Mineração de Dados, E. Simoudis, J. Han, e U. Fayyad, Eds. AAAI Press, Portland, Oregon, 226–231.

Fan, W., Miller, M., Stolfo, SJ, Lee, W., e Chan, PK 2001. Usando anomalias artificiais para detectar intrusões de rede conhecidas e desconhecidas. Em Anais da Conferência Internacional IEEE de 2001 sobre Mineração de Dados. IEEE Computer Society, 123–130.

Fawcett, T. e Provost, F. 1999. Monitoramento de atividade: notando mudanças interessantes no comportamento. Em Anais da 5ª Conferência Internacional ACM SIGKDD sobre Descoberta de Conhecimento e Mineração de Dados. ACM Press, 53–62.

Forrest, S., D'haeseleer, P., e Helman, P. 1996. Uma abordagem imunológica para detecção de mudanças: Algoritmos, análise e implicações. Em Anais do Simpósio IEEE de 1996 sobre Segurança e Privacidade. IEEE Computer Society, 110.

Forrest, S., Esponda, F., e Helman, P. 2004. Uma estrutura formal para esquemas de detecção positiva e negativa. Em IEEE Transactions on Systems, Man and Cybernetics, Parte B. IEEE, 357–373.

Forrest, S., Hofmeyr, SA, Somayaji, A., e Longstaff, TA 1996. Um senso de identidade para processos unix. Em Proceedinges do ISRSP96. 120–128.

Forrest, S., Perelson, AS, Allen, L., e Cherukuri, R. 1994. Discriminação self-nonself em um computador. Em Proceedings of the 1994 IEEE Symposium on Security and Privacy. IEEE Computer Society, Washington, DC, EUA, 202.

Forrest, S., Warrender, C., e Pearlmutter, B. 1999. Detectando intrusões usando chamadas de sistema: Modelos de dados alternativos. Em Proceedings of the 1999 IEEE ISRSP. IEEE Computer Society, Washington, DC, EUA, 133–145.

Fox, AJ 1972. Outliers em séries temporais. Journal of the Royal Statistical Society. Série B(Metodológico) 34, 3, 350–363.

Fu, AW-C., Leung, OT-W., Keogh, EJ, e Lin, J. 2006. Encontrando discordâncias de séries temporais com base na transformação de Haar. Em Anais da 2ª Conferência Internacional sobre Mineração de Dados Avançada e Aplicações. Springer Verlag, 31–41.

Fujimaki, R., Yairi, T., e Machida, K. 2005. Uma abordagem para o problema de detecção de anomalias em naves espaciais usando espaço de recursos do kernel. Em Anais da décima primeira conferência internacional ACM SIGKDD sobre descoberta de conhecimento em mineração de dados. ACM Press, Nova York, NY, EUA, 401–410.

Galeano, P., Pea, D. e Tsay, RS 2004. Detecção de outliers em séries temporais multivariadas por meio de busca de projeção. Documentos de Trabalho de Estatística e Econometria ws044211, Universidad Carlos III, Departamento de Estadística y Econometrónica. Setembro.

Ghosh, AK, Schwartzbard, A., e Schatz, M. 1999a. Perfis de comportamento de programas de aprendizagem para detecção de intrusão. Em Anais do 1º Workshop USENIX sobre Detecção de Intrusão e Monitoramento de Rede. 51–62.

Ghosh, AK, Schwartzbard, A., e Schatz, M. 1999b. Usando perfis de comportamento de programa para detecção de intrusão. Em Proceedings of SANS Third Conference and Workshop on Intrusion Detection and Response.

Ghosh, AK, Wanken, J., e Charron, F. 1998. Detectando intrusões anômalas e desconhecidas contra programas. Em Anais da 14ª Conferência Anual de Aplicações de Segurança de Computadores. IEEE Computer Society, 259.

Ghosh, S. e Reilly, DL 1994. Detecção de fraude de cartão de crédito com uma rede neural. Em Anais da 27ª Conferência Internacional Anual do Havaí sobre Ciência de Sistemas. Vol. 3.
Los Alamitos, Califórnia.

Ghoting, A., Parthasarathy, S., e Otey, M. 2006. Mineração rápida de outliers baseados em distância em conjuntos de dados de alta dimensão. Em Proceedings of the SIAM International Conference on Data Mining.

Gibbons, RD 1994. Métodos estatísticos para monitoramento de águas subterrâneas. John Wiley & Sons, Inc.

Goldberger, AL, Amaral, LAN, Glass, L., Hausdorff, JM, Ivanov, PC, Mark, RG, Mietus, JE, Moody, GB, Peng, C.-K., e Stanley, HE 2000. Phys-ioBank, PhysioToolkit e PhysioNet: Componentes de um novo recurso de pesquisa para sinais fisiológicos complexos. Circulation 101, 23, e215–e220. Páginas eletrônicas de circulação: http://circ.ahajournals.org/cgi/content/full/101/23/e215.

Gonzalez, FA e Dasgupta, D. 2003. Detecção de anomalias usando seleção negativa de valor real. Programação genética e máquinas evolutivas 4, 4, 383–403.

Grubbs, F. 1969. Procedimentos para detectar observações atípicas em amostras. Technometrics 11, 1, 1–21.

Guha, S., Rastogi, R. e Shim, K. 2000. ROCK: Um algoritmo de agrupamento robusto para categorias atributos. Sistemas de Informação 25, 5, 345–366.

Gunter, S., Schraudolph, NN e Vishwanathan, SVN 2007. Kernel iterativo rápido análise de componentes principais. J. Mach. Learn. Res. 8, 1893–1918.

Gusfield, D. 1997. Algoritmos em strings, árvores e sequências: ciência da computação e computação biologia internacional. Cambridge University Press, Nova York, NY, EUA.

Guttormsson, S., II, RM e El-Sharkawi, M. 1999. Agrupamento de novidades elípticas para detecção on-line de curto-turno de rotores excitados em funcionamento. IEEE Transactions on Energy Conversion 14, 1 (março).

Gwadera, R., Atallah, MJ, e Szpankowski, W. 2004. Detecção de conjuntos significativos de episódios em sequências de eventos. Em Anais da Quarta Conferência Internacional IEEE sobre Mineração de Dados. IEEE Computer Society, Washington, DC, EUA, 3–10.

Gwadera, R., Atallah, MJ, e Szpankowski, W. 2005a. Modelos de Markov para identificação de episódios significativos. Em Anais da 5ª Conferência Internacional SIAM sobre Mineração de Dados.

Gwadera, R., Atallah, MJ, e Szpankowski, W. 2005b. Detecção confiável de episódios em sequências de eventos. Knowledge and Information Systems 7, 4, 415–437.

Harris, T. 1993. Rede neural em monitoramento de saúde de máquina. Engenharia Profissional.

Hartigan, JA e Wong, MA 1979. Um algoritmo de agrupamento k-means. Estatística Aplicada 28, 100–108.

Hautamaki, V., Karkkainen, I., e Franti, P. 2004. Detecção de outliers usando gráfico k-vizinhos mais próximos. Em Anais da 17ª Conferência Internacional sobre Reconhecimento de Padrões. Vol. 3. IEEE Computer Society, Washington, DC, EUA, 430–433.

Hawkins, D. 1980. Identificação de outliers. Monografias sobre Probabilidade Aplicada e Estatística.

Hawkins, DM 1974. A detecção de erros em dados multivariados usando componentes principais. Journal of the American Statistical Association 69, 346 (junho), 340–344.

Hawkins, S., He, H., Williams, GJ e Baxter, RA 2002. Detecção de outliers usando redes neurais replicadoras. Em Anais da 4ª Conferência Internacional sobre Data Warehousing e Descoberta de Conhecimento. Springer-Verlag, 170–180.

Hazel, GG 2000. MRF gaussiana multivariada para segmentação de cena multiespectral e detecção de anomalias. GeoRS 38, 3 (maio), 1199–1211.

Ele, H., Wang, J., Graco, W., e Hawkins, S. 1997. Aplicação de redes neurais à detecção de fraude médica. Expert Systems with Applications 13, 4, 329–336.

He, Z., Deng, S., e Xu, X. 2002. Detecção de outliers integrando conhecimento semântico. Em Anais da Terceira Conferência Internacional sobre Avanços em Gerenciamento de Informação na Era da Web. Springer-Verlag, Londres, Reino Unido, 126–131.

Ele, Z., Deng, S., Xu, X., e Huang, JZ 2006. Um algoritmo rápido e ganancioso para mineração de outliers. Em Anais da 10ª Conferência Pacífico-Ásia sobre Conhecimento e Descoberta de Dados. 567–576.

He, Z., Xu, X., e Deng, S. 2003. Descobrindo outliers locais baseados em cluster. Pattern Recognition Letters 24, 9-10, 1641–1650.

He, Z., Xu, X., e Deng, S. 2005. Um modelo de otimização para detecção de outliers em dados categóricos. Em Proceedings of International Conference on Intelligent Computing. Vol. 3644. Springer.

Ele, Z., Xu, X., Huang, JZ e Deng, S. 2004a. Um método de descoberta de padrões frequentes para detecção de outliers. 726–732.

Ele, Z., Xu, X., Huang, JZ, e Deng, S. 2004b. Mineração de outliers de classe: Conceitos, algoritmos e aplicações. 588–589.

Heller, KA, Svore, KM, Keromytis, AD e Stolfo, SJ 2003. Uma classe de máquinas de vetores de suporte para detectar acessos anômalos ao registro do Windows. Em Proceedings of the Workshop on Data Mining for Computer Security.

Helman, P. e Bhangoo, J. 1997. Um sistema baseado em estatística para priorizar a exploração de informações sob incerteza. Em IEEE International Conference on Systems, Man, and Cybernetics. Vol. 27. IEEE, 449–466.

Helmer, G., Wong, J., Honavar, V., e Miller, L. 1998. Agentes inteligentes para intrusão detecção. Em Anais da IEEE Information Technology Conference. 121–124.

Hickinbotham, SJ e Austin, J. 2000a. Detecção de novidades em dados de deformação de fuselagem. Em Anais da 15ª Conferência Internacional sobre Reconhecimento de Padrões. Vol. 2. 536–539.

Hickinbotham, SJ e Austin, J. 2000b. Detecção de novidades em dados de deformação de fuselagem. Em Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks. Vol. 6. 24–27.

Ho, LL, Macey, CJ e Hiller, R. 1999. Uma plataforma distribuída e confiável para detecção de anomalias adaptáveis em redes IP. Em Anais do 10º Workshop Internacional IFIP/IEEE sobre Sistemas Distribuídos: Operações e Gerenciamento. Springer-Verlag, Londres, Reino Unido, 33–46.

Ho, TV e Rouat, J. 1997. Um detector de novidades usando uma rede de neurônios de integração e disparo. Anotações de aula em Ciência da Computação 1327, 103–108.

Ho, TV e Rouat, J. 1998. Detecção de novidades com base no tempo de relaxamento de uma rede de neurônios integrais e disparados. Em Proceedings of Second IEEE World Congress on Computational Intelligence. Anchorage, AK, 1524–1529.

Hodge, V. e Austin, J. 2004. Uma pesquisa de metodologias de detecção de outliers. Artificial Intelligence Review 22, 2, 85–126.

Hofmeyr, SA, Forrest, S., e Somayaji, A. 1998. Detecção de intrusão usando sequências de chamadas de sistema. Journal of Computer Security 6, 3, 151–180.

Hollier, G. e Austin, J. 2002. Detecção de novidades para degradação de strain gauge usando componentes maximamente correlacionados. Em Proceedings of the European Symposium on Artificial Neural Networks. 257–262–539.

Hollmen, J. e Tresp, V. 1999. Detecção de fraude baseada em chamadas em redes de comunicação móvel usando um modelo de troca de regime hierárquico. Em Anais da conferência de 1998 sobre Avanços em sistemas de processamento de informações neurais II. MIT Press, Cambridge, MA, EUA, 889–895.

Horn, PS, Feng, L., Li, Y., e Pesce, AJ 2001. Efeito de outliers e indivíduos não saudáveis na estimativa do intervalo de referência. Clinical Chemistry 47, 12, 2137–2145.

Hu, W., Liao, Y. e Vemuri, VR 2003. Detecção robusta de anomalias usando máquinas de vetores de suporte. Em Proceedings of the International Conference on Machine Learning. Morgan Kaufmann Publishers Inc., São Francisco, CA, EUA, 282–289.

Huber, P. 1974. Estatísticas Robustas. Wiley, Nova York.

Huber, PJ 1985. Projeção de busca (com discussões). The Annals of Statistics 13, 2 (junho), 435–475.

Ide, T. e Kashima, H. 2004. Detecção de anomalias baseada em eigenspace em sistemas de computador. Em Anais da 10ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, Nova York, NY, EUA, 440–449.

Ide, T. , Papadimitriou, S., e Vlachos, M. 2007. Computando pontuações de anomalias de correlação usando vizinhos mais próximos estocásticos. Em Proceedings of International Conference Data Mining. 523–528.

Ihler, A., Hutchins, J., e Smyth, P. 2006. Detecção adaptativa de eventos com processos de Poisson de variação temporal. Em Anais da 12ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, Nova York, NY, EUA, 207–216.

Ilgun, K., Kemmerer, RA, e Porras, PA 1995. Análise de transição de estado: Uma abordagem de detecção de intrusão baseada em regras. IEEE Transactions on Software Engineering 21, 3, 181–199.

Jagadish, HV, Koudas, N., e Muthukrishnan, S. 1999. Desviantes de mineração em um banco de dados de séries temporais. Em Anais da 25ª Conferência Internacional sobre Bancos de Dados Muito Grandes. Editora Morgan Kaufmann Inc., 102–113.

Jagota, A. 1991. Detecção de novidades em um número muito grande de memórias armazenadas em uma rede estilo hopfield. Em Proceedings of the International Joint Conference on Neural Networks. Vol. 2. Seattle, WA, 905.

Jain, AK e Dubes, RC 1988. Algoritmos para Clusterização de Dados. Prentice-Hall, Inc.

Jakubek, S. e Strasser, T. 2002. Diagnóstico de falhas usando redes neurais com base elipsoidal funções. Em Anais da American Control Conference. Vol. 5. 3846–3851.

Janakiram, D., Reddy, V., e Kumar, A. 2006. Detecção de outliers em redes de sensores sem fio usando redes de crenças bayesianas. Em Primeira Conferência Internacional sobre Software e Middleware de Sistemas de Comunicação. 1–6.

Japkowicz, N., Myers, C., e Gluck, MA 1995. Uma abordagem de detecção de novidade para classificação. Em Proceedings of International Joint Conference on Artificial Intelligence. 518–523.

Javitz, HS e Valdes, A. 1991. O detector de anomalias estatísticas sri ides. Em Anais do Simpósio IEEE de 1991 sobre Pesquisa em Segurança e Privacidade. IEEE Computer Society.

Jiang, MF, Tseng, SS e Su, CM 2001. Processo de agrupamento de duas fases para outliers detecção. Cartas de reconhecimento de padrões 22, 6-7, 691–700.

Jin, W., Tung, AKH e Han, J. 2001. Mineração de outliers locais top-n em grandes bancos de dados. Em Anais da sétima conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, 293–298.

Joachims, T. 2006. Treinamento de svms lineares em tempo linear. Em KDD '06: Anais da 12ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM, Nova York, NY, EUA, 217–226.

Jolliffe, IT 2002. Análise de Componentes Principais, 2ª ed. Springer.

Joshi, MV, Agarwal, RC e Kumar, V. 2001. Mineração de agulha em palheiro: classificação de classes raras por indução de regra de duas fases. Em Anais da conferência internacional ACM SIGMOD de 2001 sobre Gerenciamento de dados. ACM Press, Nova York, NY, EUA, 91–102.

Joshi, MV, Agarwal, RC e Kumar, V. 2002. Prevendo classes raras: o boosting pode tornar qualquer aluno fraco forte? Em Anais da oitava conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM, Nova York, NY, EUA, 297–306.

Kadota, K., Tominaga, D., Akiyama, Y., e Takahashi, K. 2003. Detectando amostras discrepantes em dados de microarray: Uma avaliação crítica do efeito de discrepantes na classificação de amostras. Chem-Bio Informatics 3, 1, 30–45.

Karypis, G. e Kumar, V. 1998. Esquema de particionamento k-way multinível para grafos irregulares. Revista de Computação Paralela e Distribuída 48, 1, 96–129.

Kearns, MJ 1990. Complexidade Computacional da Aprendizagem de Máquina. MIT Press, Cambridge, MA, EUA.

Kejia Zhang, Shengfei Shi, HG e Li, J. 2007. Detecção de outliers não supervisionados em redes de sensores usando árvore de agregação. Advanced Data Mining and Applications 4632, 158–169.

Keogh, E., Lin, J., e Fu, A. 2005. Hot sax: Encontrando eficientemente a subsequência de série temporal mais incomum. Em Proceedings of the Fifth IEEE International Conference on Data Mining. IEEE Computer Society, Washington, DC, EUA, 226–233.

Keogh, E., Lin, J., Lee, S.-H., e Herle, HV 2006. Encontrando a subsequência de série temporal mais incomum: algoritmos e aplicações. Knowledge and Information Systems 11, 1, 1–27.

Keogh, E., Lonardi, S., e chi' Chiu, BY 2002. Encontrando padrões surpreendentes em um banco de dados de séries temporais em tempo e espaço lineares. Em Anais da oitava conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, Nova York, NY, EUA, 550– 556.

Keogh, E., Lonardi, S., e Ratanamahatana, CA 2004. Rumo à mineração de dados sem parâmetros. Em Anais da 10ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, Nova York, NY, EUA, 206–215.

Keogh, E. e Smyth, P. 1997. Uma abordagem probabilística para correspondência rápida de padrões em bancos de dados de séries temporais. Em Anais da Terceira Conferência Internacional sobre Descoberta de Conhecimento e Mineração de Dados, D. Heckerman, H. Mannila, D. Pregibon e R. Uthurusamy, Eds. AAAI Press, Menlo Park, Califórnia., Newport Beach, CA, EUA, 24–30.

King, S., King, D., P. Anuzis, KA, Tarassenko, L., Hayton, P., e Utete, S. 2002. O uso de técnicas de detecção de novidades para monitorar plantas de alta integridade. Em Anais da Conferência Internacional de 2002 sobre Aplicações de Controle. Vol. 1. Cancun, México, 221–226.

Kitagawa, G. 1979. Sobre o uso de aic para a detecção de outliers. Technometrics 21, 2 (maio), 193–199.

Knorr, EM e Ng, RT 1997. Uma abordagem unificada para mineração de outliers. Em Anais da conferência de 1997 do Centro de Estudos Avançados sobre Pesquisa Colaborativa. IBM Press, 11.

Knorr, EM e Ng, RT 1998. Algoritmos para mineração de outliers baseados em distância em grandes conjuntos de dados. Em Anais da 24ª Conferência Internacional sobre Bancos de Dados Muito Grandes. Editora Morgan Kaufmann Inc., 392–403.

Knorr, EM e Ng, RT 1999. Encontrando conhecimento intensional de outliers baseados em distância. No The VLDB Journal. 211–222.

Knorr, EM, Ng, RT e Tucakov, V. 2000. Outliers baseados em distância: algoritmos e aplicações. The VLDB Journal 8, 3-4, 237–253.

Ko, H. e Jacyna, G. 2000. Comportamento dinâmico da memória autoassociativa realizando novidade filtragem. Em IEEE Transactions on Neural Networks. Vol. 11. 1152–1161.

Kohonen, T., Ed. 1997. Mapas auto-organizáveis. Springer-Verlag New York, Inc., Secaucus, NJ, EUA.

Kojima, K. e Ito, K. 1999. Aprendizagem autônoma de novos padrões utilizando dinâmica caótica. Em IEEE International Conference on Systems, Man, and Cybernetics. Vol. 1. IEEE, Tóquio, Japão, 284–289.

Kosoresow, AP e Hofmeyr, SA 1997. Detecção de intrusão via rastreamentos de chamada de sistema. IEEE Software 14, 5, 35–42.

Kou, Y., Lu, C.-T., e Chen, D. 2006. Detecção de outliers ponderados espacialmente. Em Proceedings of Conferência SIAM sobre Mineração de Dados.

Kruegel, C., Mutz, D., Robertson, W., e Valeur, F. 2003. Classificação de eventos bayesianos para detecção de intrusão. Em Anais da 19ª Conferência Anual de Aplicações de Segurança de Computadores. IEEE Computer Society, 14.

Kruegel, C., Toth, T., e Kirda, E. 2002. Detecção de anomalias específicas de serviço para detecção de intrusão de rede. Em Proceedings of the 2002 ACM symposium on Applied computing. ACM Press, 201–208.

Kruegel, C. e Vigna, G. 2003. Detecção de anomalias em ataques baseados na web. Em Anais da 10ª conferência da ACM sobre segurança de computadores e comunicações. ACM Press, 251–261.

Kumar, V. 2005. Computação paralela e distribuída para segurança cibernética. Sistemas Distribuídos On-line, IEEE 6, 10.

Labib, K. e Vemuri, R. 2002. Nsom: Uma detecção de intrusão baseada em rede em tempo real usando mapas auto-organizáveis. Redes e Segurança.

Lafferty, JD, McCallum, A., e Pereira, FCN 2001. Campos aleatórios condicionais: modelos probabilísticos para segmentação e rotulagem de dados de sequência. Em Anais da Décima Oitava Conferência Internacional sobre Aprendizado de Máquina. Morgan Kaufmann Publishers Inc., São Francisco, CA, EUA, 282–289.

Lakhina, A., Crovella, M., e Diot, C. 2005. Anomalias de mineração usando distribuições de recursos de tráfego. Em Anais da conferência de 2005 sobre Aplicações, tecnologias, arquiteturas e protocolos para comunicações de computador. ACM Press, Nova York, NY, EUA, 217–228.

Lane, T. e Brodley, CE 1997a. Uma aplicação de aprendizado de máquina para detecção de anomalias. Em Anais da 20ª Conferência Nacional de Segurança de Sistemas de Informação do NIST-NCSC. 366–380.

Lane, T. e Brodley, CE 1997b. Correspondência de sequência e aprendizado em detecção de anomalias para segurança de computadores. Em Proceedings of AI Approaches to Fraud Detection and Risk Management, Fawcett, Haimowitz, Provost e Stolfo, Eds. AAAI Press, 43–49.

Lane, T. e Brodley, CE 1999. Aprendizado de sequência temporal e redução de dados para detecção de anomalias. ACM Transactions on Information Systems and Security 2, 3, 295–331.

Lauer, M. 2001. Uma abordagem de mistura para detecção de novidades usando dados de treinamento com outliers. Em Proceedings of the 12th European Conference on Machine Learning. Springer-Verlag, Londres, Reino Unido, 300–311.

Laurikkala, J., Juhola1, M., e Kentala., E. 2000. Identificação informal de outliers em dados médicos. Em Fifth International Workshop on Intelligent Data Analysis in Medicine and Pharmacology. 20–24.

Lazarevic, A., Ertoz, L., Kumar, V., Ozgur, A., e Srivastava, J. 2003. Um estudo comparativo de esquemas de detecção de anomalias na detecção de intrusão de rede. Em Proceedings of SIAM International Conference on Data Mining. SIAM.

Lee, W. e Stolfo, S. 1998. Abordagens de mineração de dados para detecção de intrusão. Em Anais do 7º Simpósio de Segurança USENIX. San Antonio, TX.

Lee, W., Stolfo, S., e Chan, P. 1997. Padrões de aprendizagem de rastreamentos de execução de processos unix para detecção de intrusão. Em Anais do workshop AAAI 97 sobre métodos de IA em Fraude e gerenciamento de risco.

Lee, W., Stolfo, SJ e Mok, KW 2000. Detecção de intrusão adaptativa: Uma mineração de dados abordagem. Artificial Intelligence Review 14, 6, 533–567.

Lee, W. e Xiang, D. 2001. Medidas de teoria da informação para detecção de anomalias. Em Anais do Simpósio IEEE sobre Segurança e Privacidade. IEEE Computer Society, 130.

Li, M. e Vitanyi, PMB 1993. Uma introdução à complexidade de Kolmogorov e suas aplicações cátions. Springer-Verlag, Berlim.

Li, Y., Pont, MJ e Jones, NB 2002. Melhorando o desempenho de classificadores de função de base radial em aplicações de monitoramento de condições e diagnóstico de falhas onde falhas desconhecidas podem ocorrer. Pattern Recognition Letters 23, 5, 569–577.

Lin, J., Keogh, E., Fu, A. e Herle, HV 2005. Aproximações à mágica: Encontrando séries temporais médicas incomuns. Em Anais do 18º Simpósio IEEE sobre Sistemas Médicos Baseados em Computador. IEEE Computer Society, Washington, DC, EUA, 329–334.

Lin, S. e Brown, DE 2003. Um método de associação de dados baseado em outliers para vincular crimes incidentes. Em Anais da 3ª Conferência de Mineração de Dados SIAM.

Liu, JP e Weng, CS 1991. Detecção de dados atípicos em estudos de biodisponibilidade/bioequivalência. Statistics Medicine 10, 9, 1375–89.

Lu, C.-T., Chen, D., e Kou, Y. 2003. Algoritmos para detecção de outliers espaciais. Em Proceedings da 3ª Conferência Internacional sobre Mineração de Dados. 597–600.

Ma, J. e Perkins, S. 2003a. Detecção de novidades on-line em sequências temporais. Em Anais da 9ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, Nova York, NY, EUA, 613–618.

Ma, J. e Perkins, S. 2003b. Detecção de novidades em séries temporais usando máquinas de vetores de suporte de uma classe. Em Proceedings of the International Joint Conference on Neural Networks. Vol. 3. 1741– 1745.

MacDonald, JW e Ghosh, D. 2007. Análise de perfil de outliers de Copa–câncer. Bioinformat-ics 22, 23, 2950–2951.

Mahoney, MV e Chan, PK 2002. Aprendizagem de modelos não estacionários de tráfego de rede normal para detecção de novos ataques. Em Anais da 8ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, 376–385.

Mahoney, MV e Chan, PK 2003. Regras de aprendizado para detecção de anomalias de tráfego de rede hostil. Em Proceedings of the 3rd IEEE International Conference on Data Mining. IEEE Computer Society, 601.

Mahoney, MV, Chan, PK e Arshad, MH 2003. Uma abordagem de aprendizado de máquina para detecção de anomalias. Tech. Rep. CS–2003–06, Departamento de Ciência da Computação, Florida Institute of Technology Melbourne FL 32901. março.

Manevitz, LM e Yousef, M. 2000. Aprendendo com dados positivos para classificação de documentos usando redes neurais. Em Proceedings of Second Bar-Ilan Workshop on Knowledge Discovery and Learning. Jerusalém.

Manevitz, LM e Yousef, M. 2002. SVMs de uma classe para classificação de documentos. Journal of Pesquisa em Aprendizado de Máquina 2, 139–154.

Manikopoulos, C. e Papavassiliou, S. 2002. Intrusão de rede e detecção de falhas: uma abordagem de anomalia estatística. IEEE Communication Magazine 40.

Manson, G. 2002. Identificação de características sensíveis a danos e insensíveis ao ambiente para danos detecção. Em Proceedings of the IES Conference. Swansea, Reino Unido.

Manson, G., Pierce, G., e Worden, K. 2001. Sobre a estabilidade de longo prazo da condição normal para detecção de danos em um painel composto. Em Anais da 4ª Conferência Internacional sobre Avaliação de Danos em Estruturas. Cardiff, Reino Unido.

Manson, G., Pierce, SG, Worden, K., Monnier, T., Guy, P. e Atherton, K. 2000. Estabilidade de longo prazo de dados de condições normais para detecção de novidades. Em Proceedings of Smart Structures and Integrated Systems. 323–334.

Marceau, C. 2000. Caracterizando o comportamento de um programa usando n-grams de comprimento múltiplo. Em Proceedings of the 2000 workshop on New Security Paradigms. ACM Press, Nova York, NY, EUA, 101–110.

Marchette, D. 1999. Um método estatístico para criar perfis de tráfego de rede. Em Anais do 1º Workshop USENIX sobre Detecção de Intrusão e Monitoramento de Rede. Santa Clara, CA, 119–128.

Markou, M. e Singh, S. 2003a. Detecção de novidades: uma revisão - parte 1: abordagens estatísticas. Processamento de sinais 83, 12, 2481–2497.

Markou, M. e Singh, S. 2003b. Detecção de novidades: uma revisão - parte 2: rede neural baseada abordagens. Processamento de Sinais 83, 12, 2499–2521.

Marsland, S., Nehmzow, U., e Shapiro, J. 1999. Um modelo de habituação aplicado a robôs móveis. Em Proceedings of Towards Intelligent Mobile Robots. Departamento de Ciência da Computação, Universidade de Manchester, Série de Relatórios Técnicos, ISSN 1361-6161, Relatório UMCS-99-3-1.

Marsland, S., Nehmzow, U., e Shapiro, J. 2000a. Detecção de novidades para neotaxis de robôs. Em Anais do 2º Simpósio Internacional sobre Computação Neural. 554 – 559.

Marsland, S., Nehmzow, U., e Shapiro, J. 2000b. Um detector de novidades em tempo real para um dispositivo móvel robô. Em Anais da Conferência EUREL sobre Sistemas Robóticos Avançados.

Martinelli, G. e Perfetti, R. 1994. Rede neural celular generalizada para detecção de novidades. Transações IEEE em Sistemas de Circuitos I: Aplicação da Teoria Fundamental 41, 2, 187–190.

Martinez, D. 1998. Estimativa de densidade de árvore neural para detecção de novidades. Transações IEEE em Redes Neurais 9, 2, 330–338.

McCallum, A., Freitag, D., e Pereira, FCN 2000. Modelos de Markov de máxima entropia para extração e segmentação de informações. Em Anais da 17ª Conferência Internacional sobre Aprendizado de Máquina. Morgan Kaufmann Publishers Inc., São Francisco, CA, EUA, 591–598.

McCallum, A., Nigam, K., e Ungar, LH 2000. Clusterização eficiente de conjuntos de dados de alta dimensão com aplicação à correspondência de referência. Em Anais da 6ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, 169–178.

McNeil, A. 1999. Teoria do valor extremo para gerentes de risco. Modelagem interna e CAD II , 93–113.

Mingming, NY 2000. Redes probabilísticas com links não direcionados para detecção de anomalias. Em Anais do IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop. 175–179.

Motulsky, H. 1995. Bioestatística intuitiva: escolhendo um teste estatístico. Oxford University Press, Capítulo 37.

Moya, M., Koch, M., e Hostetler, L. 1993. Redes classificadoras de uma classe para aplicações de reconhecimento de alvos. Em Proceedings on World Congress on Neural Networks, International Neural Network Society. Portland, OR, 797–801.

Murray, AF 2001. Detecção de novidades usando produtos de especialistas simples - uma arquitetura potencial para sistemas embarcados. Redes Neurais 14, 9, 1257–1264.

Nairac, A., Corbett-Clark, T., Ripley, R., Townsend, N., e Tarassenko, L. 1997. Escolhendo um modelo apropriado para detecção de novidades. Em Anais da 5ª Conferência Internacional IEEE sobre Redes Neurais Artificiais. 227–232.

Nairac, A., Townsend, N., Carr, R., King, S., Cowley, P., e Tarassenko, L. 1999. Um sistema para análise de dados de vibração de motores a jato. Engenharia Assistida por Computador Integrada 6, 1, 53–56.

Ng, RT e Han, J. 1994. Métodos de clusterização eficientes e eficazes para mineração de dados espaciais. Em Anais da 20ª Conferência Internacional sobre Bancos de Dados Muito Grandes. Morgan Kaufmann Publishers Inc., São Francisco, CA, EUA, 144–155.

Noble, CC e Cook, DJ 2003. Detecção de anomalias baseada em gráficos. Em Anais da 9ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, 631–636.

Odin, T. e Addison, D. 2000. Detecção de novidades usando tecnologia de rede neural. Em Proceed- reuniões da Conferência COMADEN. Houston, TX.

Otey, M., Parthasarathy, S., Ghoting, A., Li, G., Narravula, S. e Panda, D. 2003. Rumo à detecção de intrusão baseada em nic. Em Proceedings of the 9th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM Press, Nova York, NY, EUA, 723– 728.

Otey, ME, Ghoting, A., e Parthasarathy, S. 2006. Detecção rápida de outliers distribuídos em conjuntos de dados de atributos mistos. Data Mining and Knowledge Discovery 12, 2-3, 203–228.

Palshikar, GK 2005. Outliers baseados em distância em sequências. Notas de aula em Ciência da Computação referência 3816, 547–552.

Papadimitriou, S., Kitagawa, H., Gibbons, PB, e Faloutsos, C. 2002. Loci: Detecção rápida de out-lier usando a integral de correlação local. Tech. Rep. IRP-TR-02-09, Intel Research Laboratory, Pittsburgh, PA. Julho.

Parra, L., Deco, G., e Miesbach, S. 1996. Independência estatística e detecção de novidades com mapas não lineares de preservação de informações. Computação Neural 8, 2, 260–269.

Parzen, E. 1962. Sobre a estimativa de uma função de densidade de probabilidade e moda. Anais de Estatística Matemática 33, 1065–1076.

Patcha, A. e Park, J.-M. 2007. Uma visão geral das técnicas de detecção de anomalias: Existente soluções e últimas tendências tecnológicas. Comput. Networks 51, 12, 3448–3470.

Pavlov, D. 2003. Modelagem de sequência com misturas de distribuições de entropia máxima condicional. Em Anais da Terceira Conferência Internacional IEEE sobre Mineração de Dados. IEEE Computer Society, Washington, DC, EUA, 251.

Pavlov, D. e Pennock, D. 2002. Uma abordagem de entropia máxima para filtragem colaborativa em domínios dinâmicos, esparsos e de alta dimensão. Em Proceedings of Advances in Neural Information Processing. MIT Press.

Petsche, T., Marcantonio, A., Darken, C., Hanson, S., Kuhn, G., e Santoso, I. 1996.
Um autoassociador de rede neural para predição de falha de motor de indução. Em Proceedings of Advances in Neural Information Processing. Vol. 8. 924–930.

Phoha, VV 2002. Dicionário Springer de Segurança na Internet. Springer-Verlag.

Phua, C., Alahakoon, D., e Lee, V. 2004. Relatório minoritário na detecção de fraudes: classificação de dados distorcidos. SIGKDD Explorer Newsletter 6, 1, 50–59.

Phuong, TV, Hung, LX, Cho, SJ, Lee, Y., e Lee, S. 2006. Um algoritmo de detecção de anomalias para detectar ataques em redes de sensores sem fio. Intelligence and Security Informat-ics 3975, 735–736.

Pickands, J. 1975. Inferência estatística usando estatísticas de ordem extrema. The Annals of Statistics 3, 1 (janeiro), 119–131.

Pires, A. e Santos-Pereira, C. 2005. Usando clustering e estimadores robustos para detectar outliers em dados multivariados. Em Proceedings of International Conference on Robust Statistics. Finlândia.

Platt, J. 2000. Saídas probabilísticas para máquinas de vetores de suporte e comparação com métodos de verossimilhança regularizados. A. Smola, P. Bartlett, B. Schoelkopf e D. Schuurmans, Eds. 61–74.

Pokrajac, D., Lazarevic, A., e Latecki, LJ 2007. Detecção incremental de outliers locais para fluxos de dados. Em Proceedings of IEEE Symposium on Computational Intelligence and Data Mining.

Porras, PA e Neumann, PG 1997. EMERALD: Monitoramento de eventos que permite respostas a perturbações anômalas ao vivo. Em Anais da 20ª Conferência Nacional de Segurança de Sistemas de Informação do NIST-NCSC. 353–365.

Portnoy, L., Eskin, E., e Stolfo, S. 2001. Detecção de intrusão com dados não rotulados usando clustering. Em Proceedings of ACM Workshop on Data Mining Applied to Security.

Protopapas, P., Giammarco, JM, Faccioli, L., Struble, MF, Dave, R., e Alcock, C.
2006. Encontrando curvas de luz atípicas em catálogos de estrelas variáveis periódicas. Monthly Notices of the Royal Astronomical Society 369, 2, 677–696.

Qin, M. e Hwang, K. 2004. Frequent episode rules for internet anomaly detection. Em Anais do 3º Simpósio Internacional IEEE sobre Computação em Rede e Aplicações.
Sociedade de Computação IEEE.

Ramadas, M., Ostermann, S., e Tjaden, BC 2003. Detectando tráfego de rede anômalo com mapas auto-organizáveis. Em Proceedings of Recent Advances in Intrusion Detection. 36–54.

Ramaswamy, S., Rastogi, R., e Shim, K. 2000. Algoritmos eficientes para mineração de outliers de grandes conjuntos de dados. Em Anais da conferência internacional ACM SIGMOD de 2000 sobre Gerenciamento de dados. ACM Press, 427–438.

Ratsch, G., Mika, S., Scholkopf, B., e Muller, K.-R. 2002. Construindo algoritmos de boosting a partir de svms: Uma aplicação para classificação de uma classe. IEEE Transactions on Pattern Analysis and Machine Intelligence 24, 9, 1184–1199.

Roberts, S. 1999. Detecção de novidades usando estatísticas de valores extremos. Em Proceedings of IEEE - Visão, Imagem e Processamento de Sinais. Vol. 146. 124–129.

Roberts, S. 2002. Estatísticas de valor extremo para detecção de novidades em processamento de sinais biomédicos. Em Anais da 1ª Conferência Internacional sobre Avanços em Processamento de Sinais e Informações Médicas. 166–172.

Roberts, S. e Tarassenko, L. 1994. Uma rede de alocação de recursos probabilísticos para detecção de novidades. Neural Computing 6, 2, 270–284.

Rosner, B. 1983. Pontos percentuais para um procedimento generalizado esd many-outlier. Tecnometrics 25, 2 (maio), 165–172.

Roth, V. 2004. Detecção de outliers com discriminantes de fisher de kernel de uma classe. Em NIPS.

Roth, V. 2006. Kernel Fisher discriminantes para detecção de outliers. Computação Neural 18, 4, 942–960.

Rousseeuw, PJ e Leroy, AM 1987. Regressão robusta e detecção de outliers. John Wiley & Sons, Inc., Nova York, NY, EUA.

Roussopoulos, N., Kelley, S., e Vincent, F. 1995. Consultas de vizinhos mais próximos. Em Anais da Conferência Internacional ACM-SIGMOD sobre Gerenciamento de Dados.

Ruotolo, R. e Surace, C. 1997. Uma abordagem estatística para detecção de danos por meio do monitoramento de vibração. Em Anais do 5º Congresso Pan-Americano de Mecânica Aplicada. Porto Rico.

Salvador, S. e Chan, P. 2003. Estados de aprendizagem e regras para detecção de anomalias em séries temporais. Tech. Rep. CS–2003–05, Departamento de Ciência da Computação, Instituto de Tecnologia da Flórida Melbourne FL 32901. março.

Sarawagi, S., Agrawal, R., e Megiddo, N. 1998. Exploração orientada à descoberta de cubos de dados olap. Em Proceedings of the 6th International Conference on Extending Database Technology. Springer-Verlag, Londres, Reino Unido, 168–182.

Sargor, C. 1998. Detecção de anomalias estatísticas para protocolos de roteamento link-state. Em Anais da Sexta Conferência Internacional sobre Protocolos de Rede. IEEE Computer Society, Washington, DC, EUA, 62.

Saunders, R. e Gero, J. 2000. A importância de ser emergente. Em Proceedings of Artificial Intelligence in Design.

Scarth, G., McIntyre, M., Wowk, B., e Somorjai, R. 1995. Detecção de novidade em imagens funcionais usando agrupamento fuzzy. Em Anais do 3º Encontro da Sociedade Internacional de Ressonância Magnética em Medicina. Niçe, França, 238.

Scholkopf, B. , Platt, JC, Shawe-Taylor, JC, Smola, AJ e Williamson, RC 2001. Estimando o suporte de uma distribuição de alta dimensão. Neural Comput. 13, 7, 1443–1471.

Scott, SL 2001. Detectando intrusão de rede usando um processo de Poisson não homogêneo modulado por Markov. Enviado para o Journal of the American Statistical Association.

Sebyala, AA, Olukemi, T., e Sacks, L. 2002. Segurança de plataforma ativa por meio de detecção de intrusão usando rede bayesiana ingênua para detecção de anomalias. Em Proceedings of the 2002 London Communications Symposium.

Sekar, R., Bendre, M., Dhurjati, D., e Bollineni, P. 2001. Um método rápido baseado em autômato para detectar comportamentos anômalos de programas. Em Proceedings of the IEEE Symposium on Security and Privacy. IEEE Computer Society, 144.

Sekar, R., Guang, Y., Verma, S., e Shanbhag, T. 1999. Um sistema de detecção de intrusão de rede de alto desempenho. Em Anais da 6ª conferência da ACM sobre segurança de computadores e comunicações. ACM Press, 8–17.

Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H., e Zhou, S. 2002. Detecção de anomalias baseada em especificações: uma nova abordagem para detectar intrusões de rede. Em Proceedings of the 9th ACM conference on Computer and communications security. ACM Press, 265–274.

Sequeira, K. e Zaki, M. 2002. Admit: mineração de dados baseada em anomalias para intrusões. Em Anais da 8ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, 386–395.

Sheikholeslami, G., Chatterjee, S., e Zhang, A. 1998. Wavecluster: Uma abordagem de clustering multirresolução para bancos de dados espaciais muito grandes. Em Anais da 24ª Conferência Internacional sobre Bancos de Dados Muito Grandes. Morgan Kaufmann Publishers Inc., São Francisco, CA, EUA, 428–439.

Shekhar, S., Lu, C.-T., e Zhang, P. 2001. Detectando outliers espaciais baseados em gráficos: algoritmos e aplicações (um resumo dos resultados). Em Anais da 7ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, Nova York, NY, EUA, 371– 376.

Shewhart, WA 1931. Controle Econômico da Qualidade do Produto Manufaturado. D. Van Nostrand Empresa, Nova York NY.

Shyu, M.-L., Chen, S.-C., Sarinnapakorn, K., e Chang, L. 2003. Um novo esquema de detecção de anomalias baseado no classificador de componentes principais. Em Anais da 3ª Conferência Internacional IEEE sobre Mineração de Dados. 353–365.

Siaterlis, C. e Maglaris, B. 2004. Rumo à fusão de dados multissensor para detecção de dos. Em Anais do simpósio ACM de 2004 sobre computação aplicada. ACM Press, 439–446.

Singh, S. e Markou, M. 2004. Uma abordagem para detecção de novidades aplicada à classificação de regiões de imagem. IEEE Transactions on Knowledge and Data Engineering 16, 4, 396–407.

Smith, R., Bivens, A., Embrechts, M., Palagiri, C., e Szymanski, B. 2002. Abordagens de clusterização para detecção de intrusão baseada em anomalias. Em Proceedings of Intelligent Engineering Systems through Artificial Neural Networks. ASME Press, 579–584.

Smyth, P. 1994. Monitoramento de Markov com estados desconhecidos. IEEE Journal on Selected Areas in Communications, Edição Especial sobre Processamento Inteligente de Sinais para Comunicações 12, 9 (dezembro), 1600–1612.

Smyth, P. 1997. Sequências de agrupamento com modelos ocultos de Markov. Em Advances in Neural Information Processing. Vol. 9. MIT Press.

Snyder, D. 2001. Detecção de intrusão online usando sequências de chamadas de sistema. Tese de mestrado, Departamento de Ciência da Computação, Universidade Estadual da Flórida.

Sohn, H., Worden, K., e Farrar, C. 2001. Detecção de novidades sob condições ambientais em mudança. Em Anais do Oitavo Simpósio Internacional Anual SPIE sobre Estruturas e Materiais Inteligentes. Newport Beach, CA.

Solberg, HE e Lahti, A. 2005. Detecção de outliers em distribuições de referência: Desempenho do algoritmo de Horn. Química Clínica 51, 12, 2326–2332.

Song, Q., Hu, W., e Xie, W. 2002. Máquina de vetor de suporte robusto com classificação de imagem de buraco de bala. IEEE Transactions on Systems, Man, and Cybernetics – Parte C:Aplicações e revisões 32, 4.

Song, S., Shin, D., e Yoon, E. 2001. Análise de propriedades de detecção de novidades de autoassociadores. Em Proceedings of Condition Monitoring and Diagnostic Engineering Management.
577–584.

Song, X., Wu, M., Jermaine, C., e Ranka, S. 2007. Detecção de anomalia condicional. IEEE Transações em Engenharia de Conhecimento e Dados 19, 5, 631–645.

Soule, A., Salamatian, K., e Taft, N. 2005. Combinando filtragem e métodos estatísticos para detecção de anomalias. Em IMC '05: Anais da 5ª conferência ACM SIGCOMM sobre medição da Internet. ACM, Nova York, NY, EUA, 1–14.

Spence, C., Parra, L., e Sajda, P. 2001. Detecção, síntese e compressão em análise de imagem mamográfica com um modelo de probabilidade de imagem hierárquica. Em Proceedings of the IEEE Workshop on Mathematical Methods in Biomedical Image Analysis. IEEE Computer Society, Washington, DC, EUA, 3.

Srivastava, A. 2006. Habilitando a descoberta de anomalias recorrentes em relatórios de problemas aeroespaciais usando técnicas de clusterização de alta dimensão. Aerospace Conference, 2006 IEEE, 17–34.

Srivastava, A. e Zane-Ulman, B. 2005. Descobrindo anomalias recorrentes em relatórios de texto sobre sistemas espaciais complexos. Conferência Aeroespacial, 2005 IEEE, 3853–3862.

Stefano, C., Sansone, C., e Vento, M. 2000. Rejeitar ou não rejeitar: essa é a questão– uma resposta no caso de classificadores neurais. IEEE Transactions on Systems, Management and Cybernetics 30, 1, 84–94.

Stefansky, W. 1972. Rejeitando outliers em designs fatoriais. Technometrics 14, 2, 469–479.

Steinwart, I., Hush, D., e Scovel, C. 2005. Uma estrutura de classificação para detecção de anomalias. Revista de Pesquisa em Aprendizado de Máquina 6, 211–232.

Streifel, R., Maks, R., e El-Sharkawi, M. 1996. Detecção de espiras em curto no campo de rotores de turbina-gerador usando detectores de novidades–desenvolvimento e testes de campo. IEEE Transac-tions on Energy Conversations 11, 2, 312–317.

Subramaniam, S., Palpanas, T., Papadopoulos, D., Kalogeraki, V., e Gunopulos, D.
2006. Detecção de outliers online em dados de sensores usando modelos não paramétricos. Em VLDB '06: Anais da 32ª conferência internacional sobre bancos de dados muito grandes. VLDB Endowment, 187–198.

Sun, H., Bao, Y., Zhao, F., Yu, G. e Wang, D. 2004. Cd-trees: Uma estrutura de índice eficiente para detecção de outliers. 600–609.

Sun, J., Qu, H., Chakrabarti, D., e Faloutsos, C. 2005. Formação de vizinhança e detecção de anomalias em grafos bipartidos. Em Anais da 5ª Conferência Internacional IEEE sobre Mineração de Dados. IEEE Computer Society, Washington, DC, EUA, 418–425.

Sun, J., Xie, Y., Zhang, H., e Faloutsos, C. 2007. Menos é mais: representação matricial compacta de grandes gráficos esparsos. Em Anais da 7ª Conferência Internacional SIAM sobre Mineração de Dados.

Sun, P. e Chawla, S. 2004. Sobre outliers espaciais locais. Em Proceedings of 4th IEEE International Conferência sobre Mineração de Dados. 209–216.

Sun, P. e Chawla, S. 2006. Slom: uma nova medida para outliers espaciais locais. Conhecimento e Sistemas de Informação 9, 4, 412–429.

Sun, P., Chawla, S., e Arunasalam, B. 2006. Mineração de outliers em bancos de dados sequenciais. Em Na Conferência Internacional SIAM sobre Mineração de Dados.

Surace, C. e Worden, K. 1998. Um método de detecção de novidades para diagnosticar danos em estruturas: uma aplicação a uma plataforma offshore. Em Anais da Oitava Conferência Internacional de Engenharia Off-shore e Polar. Vol. 4. Colorado, EUA, 64–70.

Surace, C., Worden, K. e Tomlinson, G. 1997. Uma abordagem de detecção de novidades para diagnosticar dano em uma viga rachada. Em Proceedings of SPIE. Vol. 3089. 947–953.

Suzuki, E., Watanabe, T., Yokoi, H., e Takabayashi, K. 2003. Detectando exceções interessantes de dados de testes médicos com sumarização visual. Em Proceedings of the 3rd IEEE International Conference on Data Mining. 315–322.

Sykacek, P. 1997. Barras de erro equivalentes para classificadores de redes neurais treinados por inferência bayesiana. Em Proceedings of the European Symposium on Artificial Neural Networks. 121–126.

Tan, P.-N., Steinbach, M., e Kumar, V. 2005. Introdução à Mineração de Dados. Addison-Wesley.

Tandon, G. e Chan, P. 2007. Ponderação versus poda na validação de regras para detecção de anomalias de rede e host. Em Anais da 13ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press.

Tang, J., Chen, Z., chee Fu, AW e W. Cheung, D. 2002. Melhorando a eficácia de detecções de outliers para padrões de baixa densidade. Em Proceedings of the Pacific-Asia Conference on Knowledge Discovery and Data Mining. 535–548.

Taniguchi, M., Haft, M., Hollmn, J., e Tresp, V. 1998. Detecção de fraude em redes de comunicação usando métodos neurais e probabilísticos. Em Anais da IEEE International Con-ference in Acoustics, Speech and Signal Processing. Vol. 2. IEEE Computer Society, 1241–1244.

Tao, Y., Xiao, X. e Zhou, S. 2006. Mineração de outliers baseados em distância de grandes bancos de dados em qualquer espaço métrico. Em Anais da 12ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, Nova York, NY, EUA, 394–403.

Tarassenko, L. 1995. Detecção de novidades para a identificação de massas em mamografias. Em Anais da 4ª Conferência Internacional IEEE sobre Redes Neurais Artificiais. Vol. 4. Cambridge, Reino Unido, 442–447.

Tax, D. e Duin, R. 1999a. Descrição de domínio de dados usando vetores de suporte. Em Proceedings of the European Symposium on Artificial Neural Networks, M. Verleysen, Ed. Bruxelas, 251–256.

Tax, D. e Duin, R. 1999b. Descrição de dados de vetores de suporte. Pattern Recognition Letters 20, 11-13, 1191–1199.

Imposto, DMJ 2001. Classificação de uma classe; aprendizagem de conceitos na ausência de contra-exemplos. Tese de doutorado, Universidade de Tecnologia de Delft.

Teng, H., Chen, K., e Lu, S. 1990. Detecção adaptativa de anomalias em tempo real usando padrões sequenciais gerados indutivamente. Em Proceedings of IEEE Computer Society Symposium on Re-search in Security and Privacy. IEEE Computer Society Press, 278–284.

Theiler, J. e Cai, DM 2003. Abordagem de reamostragem para detecção de anomalias em multiespectrais imagens. Em Anais do SPIE 5093, 230-240, Ed.

Thompson, B., II, RM, Choi, J., El-Sharkawi, M., Huang, M., e Bunje, C. 2002. Aprendizagem implícita na avaliação de novidade do autocodificador. Em Anais da Conferência Conjunta Internacional sobre Redes Neurais. Honolulu, 2878–2883.

Thottan, M. e Ji, C. 2003. Detecção de anomalias em redes ip. IEEE Transactions on Signal Processing 51, 8, 2191–2204.

Tibshirani, R. e Hastie, T. 2007. Somas de outliers para análise de expressão gênica diferencial. Bioestatística 8, 1, 2–8.

Tomlins, SA, Rhodes, DR, Perner, S., Dhanasekaran, SM, Mehra, R., Sun, XW, Varambally, S., Cao, X., Tchinda, J., Kuefer, R., Lee, C. , Montie, JE, Shah, R., Pienta, KJ, Rubin, M., e Chinnaiyan, AM 2005. Fusão recorrente de genes do fator de transcrição tmprss2 e ets no câncer de próstata. Ciência 310, 5748, 603–611.

Torr, P. e Murray, D. 1993. Detecção de outliers e segmentação de movimento. Em Proceedings of SPIE, Fusão de Sensores VI, Paul S. Schenker; Ed. Vol. 2059. 432–443.

Tsay, RS, Pea, D., e Pankratz, AE 2000. Valores discrepantes em séries temporais multivariadas. Biometria 87, 4, 789–804.

Vaidya, J. e Clifton, C. 2004. Detecção de outliers que preservam a privacidade. Em Proceedings of the 4th Conferência Internacional IEEE sobre Mineração de Dados. 233–240.

Valdes, A. e Skinner, K. 2000. Monitoramento adaptativo baseado em modelos para detecção de ataques cibernéticos. Nos Anais do 3º Workshop Internacional sobre Avanços Recentes em Detecção de Intrusão. Editora Springer, 80–92.

Vapnik, VN 1995. A natureza da teoria da aprendizagem estatística. Springer-Verlag New York, Inc., Nova York, NY, EUA.

Vasconcelos, G., Fairhurst, M., e Bisset, D. 1994. Reconhecendo a novidade em tarefas de classificação. Em Proceedings of Neural Information Processing Systems Workshop on Novelty Detec-tion and Adaptive Systems monitoring. Denver, CO.

Vasconcelos, GC, Fairhurst, MC e Bisset, DL 1995. Investigando redes neurais feedforward com relação à rejeição de padrões espúrios. Pattern Recognition Letters 16, 2, 207–212.

Vilalta, R. e Ma, S. 2002. Prevendo eventos raros em domínios temporais. Em Anais da Conferência Internacional IEEE de 2002 sobre Mineração de Dados. IEEE Computer Society, Washington, DC, EUA, 474.

Vinueza, A. e Grudic, G. 2004. Detecção de outliers não supervisionada e aprendizagem semi-supervisionada. Rep. Técnico CU-CS-976-04, Univ. do Colorado em Boulder. Maio.

Wei, L., Qian, W., Zhou, A. e Jin, W. 2003. Hot: Teste de outlier baseado em hipergrafo para dados categóricos. Em Anais da 7ª Conferência Pacífico-Ásia sobre Conhecimento e Descoberta de Dados. 399–410.

Weigend, AS, Mangeas, M., e Srivastava, AN 1995. Especialistas não lineares com gate para séries temporais - descobrindo regimes e evitando overfitting. International Journal of Neural Systems 6, 4, 373–399.

Weiss, GM e Hirsh, H. 1998. Aprendendo a prever eventos raros em sequências de eventos. Em Anais da 4ª Conferência Internacional sobre Descoberta de Conhecimento e Mineração de Dados, R. Agrawal, P. Stolorz e G. Piatetsky-Shapiro, Eds. AAAI Press, Menlo Park, CA, Nova York, NY, 359–363.

Whitehead, B. e Hoyt, W. 1993. Uma abordagem de aproximação de função para detecção de anomalias em dados de teste de sistema de propulsão. Em Anais da 29ª Conferência Conjunta de Propulsão AIAA/SAE/ASME/ASEE. IEEE Computer Society, Monterey, CA, EUA.

Williams, G., Baxter, R., He, H., Hawkins, S., e Gu, L. 2002. Um estudo comparativo de rnn para detecção de outliers em mineração de dados. Em Proceedings of the 2002 IEEE International Conference on Data Mining. IEEE Computer Society, Washington, DC, EUA, 709.

Wong, W.-K., Moore, A., Cooper, G., e Wagner, M. 2002. Detecção de padrões de anomalias baseada em regras para detecção de surtos de doenças. Em Proceedings of the 18th Na-tional Conference on Artificial Intelligence. MIT Press. Também disponível online em http://www.cs.cmu.edu/simawm/antiterror.

Wong, W.-K., Moore, A., Cooper, G., e Wagner, M. 2003. Detecção de padrão de anomalia de rede bayesiana para surtos de doenças. Em Anais da 20ª Conferência Internacional sobre Aprendizado de Máquina. AAAI Press, Menlo Park, Califórnia, 808–815.

Worden, K. 1997. Detecção de falhas estruturais usando uma medida de novidade. Journal of Sound Vibração 201, 1, 85–101.

Wu, M. e Jermaine, C. 2006. Detecção de outliers por amostragem com garantias de precisão. Em Anais da 12ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM, Nova York, NY, EUA, 767–772.

Wu, N. e Zhang, J. 2003. Detecção de anomalias baseada em análise fatorial. Em Proceedings of IEEE Workshop on Information Assurance. Academia Militar dos Estados Unidos, West Point, NY, EUA.

Yairi, T., Kato, Y., e Hori, K. 2001. Detecção de falhas por regras de associação de mineração a partir de dados de manutenção. Em Anais do Simpósio Internacional sobre Inteligência Artificial, Robótica e Automação no Espaço.

Yamanishi, K. e ichi Takeuchi, J. 2001. Descobrindo regras de filtragem de outliers a partir de dados não rotulados: combinando um aprendiz supervisionado com um aprendiz não supervisionado. Em Anais da 7ª conferência internacional ACM SIGKDD sobre descoberta de conhecimento e mineração de dados. ACM Press, 389–394.

Yamanishi, K., Takeuchi, J.-I., Williams, G., e Milne, P. 2004. Detecção de outliers não supervisionada on-line usando misturas finitas com algoritmos de aprendizado de desconto. Data Mining and Knowledge Discovery 8, 275–300.

Yang, J. e Wang, W. 2003. Cluseq: Clusterização de sequência eficiente e eficaz. Em Anais da Conferência Internacional sobre Engenharia de Dados. 101–112.

Yankov, D., Keogh, EJ, e Rebbapragada, U. 2007. Descoberta de discórdia com reconhecimento de disco: Encontrando séries temporais incomuns em conjuntos de dados de tamanho terabyte. Em Proceedings of International Conference on Data Mining. 381–390.

Ye, N. 2004. Um modelo de cadeia de markov de comportamento temporal para detecção de anomalias. Em Proceedings do 5º Workshop Anual de Garantia de Informação do IEEE. IEEE.

Ye, N. e Chen, Q. 2001. Uma técnica de detecção de anomalias baseada em uma estatística qui-quadrado para detectar intrusões em sistemas de informação. Quality and Reliability Engineering International 17, 105–112.

Yi, B.-K., Sidiropoulos, N., Johnson, T., Jagadish, HV, Faloutsos, C., e Biliris, A. 2000. Mineração de dados on-line para sequências de tempo coevolutivas. Em Proceedings of the 16th Inter-national Conference on Data Engineering. IEEE Computer Society, Washington, DC, EUA, 13.

Ypma, A. e Duin, R. 1998. Detecção de novidades usando mapas auto-organizáveis. Em andamento em Sistemas de Informação Baseados em Conexionismo. Vol. 2. Springer, 1322–1325.

Yu, D., Sheikholeslami, G., e Zhang, A. 2002. Descoberta: encontrando valores discrepantes em conjuntos de dados muito grandes. Conhecimento e Sistemas de Informação 4, 4, 387–412.

Yu, JX, Qian, W., Lu, H. e Zhou, A. 2006. Encontrando outliers locais centrados em categorias espaços numéricos/cal. Knowledge and Information Systems 9, 3, 309–338.

Zeevi, AJ, Meir, R., e Adler, R. 1997. Previsão de séries temporais usando misturas de especialistas. Em Avanços em Processamento de Informação Neural. Vol. 9. MIT Press.

Zhang, J. e Wang, H. 2006. Detectando subespaços periféricos para dados de alta dimensão: a nova tarefa, algoritmos e desempenho. Knowledge and Information Systems 10, 3, 333–355.

Zhang, Z., Li, J., Manikopoulos, C., Jorgenson, J., e Ucles, J. 2001. Hide: um sistema hierárquico de detecção de intrusão de rede usando pré-processamento estatístico e classificação de rede neural. Em Anais do IEEE Workshop on Information Assurance and Security. West Point, 85–90.

Zimmermann, J. e Mohay, G. 2006. Detecção de intrusão distribuída em clusters com base em não interferência. Em ACSW Frontiers '06: Anais dos workshops australianos de 2006 sobre computação em grade e e-pesquisa. Australian Computer Society, Inc., Darlinghurst, Austrália, Austrália, 89–95.