- introduction
  - anomaly detection definition
  - challenges
  - related work
    - hodge and austin 2004
      - survey on machine learning
      - survey on statistical domains
    - agyemang et al. 2006
      - review on numeric data
      - review on symbolic data
    - Markou and Singh 2003a/b
      - review on novelty detection techniques
        - using neural networks
        - using statistical approaches
    - Patcha and Park 2007; Snyder 2001
  - related work
    - related books
      - rousseeuw and Leroy 1987
      - Barnett and lewis 1994
        - review on statistics
      - Hawkins
  - related work
    - survey articles
      - Beckman and Cook 1983
      - Bakar et al. 2006
  - authors: CHANDOLA et al. contributions
    - Techniques + applications
- different aspects of an anomaly detection problem
  - Nature of input data
    - input is a collection of data instances
      - each data instance is described using a set of atributes
        - different types
          - binary
          - categorical
          - continuous
        - quantity of atributes
          - univariate
          - multivariate
            - all attributes might be the same type
            - or might be a mixture of different data types
    - the nature determines the applicability of anomaly detection techniques
      - for statistical techniques
        - different statistical models have to be used
          - for continuous
          - and categorical data
      - similarly for nearest-neighbour-based techniques
        - the nature of attributes would determine the distance measure to be used
      - often instead of the actual data, the pairwise distance between instances might be provided in the form of a distance or similarity matrix.
        - In such cases, techniques that require original data instances are not applicable, for example, many statistical and classification-based techniques.
    - can also be categorized
      - categorized based on the relationship present among data instances [Tan et al. 2005].
        - Most of the existing anomaly detection techniques deal with record data or point data, in which no relationship is assumed among the data instances
    - in general, data instances can be related to each other
      - Some examples are sequence data, spatial data, and graph data.
        - In sequence data, the data instances are linearly ordered, for example, time-series data, genome sequences, and protein sequences.
        - In spatial data, each data instance is related to its neighboring instances, for example, vehicular traffic data, and ecological data.
        - In graph data, data instances are represented as vertices in a graph and are connected to other vertices with edges.
  - Type of anomaly
    - Point Anomalies. If an individual data instance can be considered as anomalous with respect to the rest of data, then the instance is termed a point anomaly. This is the simplest type of anomaly and is the focus of majority of research on anomaly detection.
    - Contextual Anomalies. If a data instance is anomalous in a specific context, but not otherwise, then it is termed a contextual anomaly (also referred to as conditional anomaly [Song et al. 2007]).
      - The notion of a context is induced by the structure in the data set and has to be specified as a part of the problem formulation. Each data instance is defined using the following two sets of attributes:
        - Contextual attributes. The contextual attributes are used to determine the context (or neighborhood) for that instance. For example, in spatial data sets, the longitude and latitude of a location are the contextual attributes. In time-series data, time is a contextual attribute that determines the position of an instance on the entire sequence.
        - Behavioral attributes. The behavioral attributes define the noncontextual characteristics of an instance. For example, in a spatial data set describing the average rainfall of the entire world, the amount of rainfall at any location is a behavioral attribute.
    - Collective Anomalies. If a collection of related data instances is anomalous with respect to the entire data set, it is termed a collective anomaly.
      - The individual data instances in a collective anomaly may not be anomalies by themselves, but their occurrence together as a collection is anomalous.
        - Collective anomalies have been explored for sequence data [Forrest et al. 1999; Sun et al. 2006], graph data [Noble and Cook 2003], and spatial data [Shekhar et al. 2001]. It should be noted that while point anomalies can occur in any data set, collective anomalies can occur only in data sets in which data instances are related. In contrast, occurrence of contextual anomalies depends on the availability of context attributes in the data. A point anomaly or a collective anomaly can also be a contextual anomaly if analyzed with respect to a context. Thus a point anomaly detection problem or collective anomaly detection problem can be transformed to a contextual anomaly detection problem by incorporating the context information.
        - The techniques used for detecting collective anomalies are very different than the point and contextual anomaly detection techniques, and require a separate detailed discussion. Hence we chose to not cover them in this survey. For a brief review of the research done in the field of collective anomaly detection, the reader is referred to an extended version of this survey [Chandola et al. 2007].
  - data labels
    - The labels associated with a data instance denote whether that instance is normal or anomalous.1 It should be noted that obtaining labeled data that is accurate as well as representative of all types of behaviors, is often prohibitively expensive. Labeling is often done manually by a human expert and hence substantial effort is required to obtain the labeled training data set. Typically, getting a labeled set of anomalous data instances that covers all possible type of anomalous behavior is more difficult than getting labels for normal behavior. Moreover, the anomalous behavior is often dynamic in nature, for example, new types of anomalies might arise, for which there is no labeled training data. In certain cases, such as air traffic safety, anomalous instances would translate to catastrophic events, and hence are very rare.
      - Supervised anomaly detection
        - Techniques trained in supervised mode assume the availability of a training data set that has labeled instances for normal as well as anomaly classes. A typical approach in such cases is to build a predictive model for normal vs. anomaly classes. Any unseen data instance is compared against the model to determine which class it belongs to. There are two major issues that arise in supervised anomaly detection. First, the anomalous instances are far fewer compared to the normal instances in the training data. Issues that arise due to imbalanced class distributions have been addressed in the data mining and machine learning literature [Joshi et al. 2001, 2002; Chawla et al. 2004; Phua et al. 2004; Weiss and Hirsh 1998; Vilalta and Ma 2002]. Second, obtaining accurate and representative labels, especially for the anomaly class is usually challenging. A number of techniques have been proposed that inject artificial anomalies into a normal data set to obtain a labeled training data set [Theiler and Cai 2003; Abe et al. 2006; Steinwart et al. 2005]. Other than these two issues, the supervised anomaly detection problem is similar to building predictive models. Hence we will not address this category of techniques in this survey.
      - Semisupervised anomaly detection
        - Techniques that operate in a semisupervised mode, assume that the training data has labeled instances only for the normal class. Since they do not require labels for the anomaly class, they are more widely applicable than supervised techniques. For example, in spacecraft fault detection [Fujimaki et al. 2005], an anomaly scenario would signify an accident, which is not easy to model. The typical approach used in such techniques is to build a model for the class corresponding to normal behavior, and use the model to identify anomalies in the test data. A limited set of anomaly detection techniques exists that assumes availability of only the anomaly instances for training [Dasgupta and Nino 2000; Dasgupta and Majumdar 2002; Forrest et al. 1999]. Such techniques are not commonly used, primarily because it is difficult to obtain a training data set that covers every possible anomalous behavior that can occur in the data.
      - Unsupervised anomaly detection
        - Techniques that operate in unsupervised mode do not require training data, and thus are most widely applicable. The techniques in this category make the implicit assumption that normal instances are far more frequent than anomalies in the test data. If this assumption is not true then such techniques suffer from high false alarm rate. Many semisupervised techniques can be adapted to operate in an unsupervised mode by using a sample of the unlabeled data set as training data. Such adaptation assumes that the test data contains very few anomalies and the model learned during training is robust to these few anomalies.
  - output of anomaly detection
    - An important aspect for any anomaly detection technique is the manner in which the anomalies are reported. Typically, the outputs produced by anomaly detection techniques are one of the following two types:
      - Scores
        - 2.4.1. Scores. Scoring techniques assign an anomaly score to each instance in the test data depending on the degree to which that instance is considered an anomaly. Thus the output of such techniques is a ranked list of anomalies. An analyst may choose to either analyze the top few anomalies or use a cutoff threshold to select the anomalies.
          - Scoring-based anomaly detection techniques allow the analyst to use a domainspecific threshold to select the most relevant anomalies.
      - Labels
        - Techniques in this category assign a label (normal or anomalous) to each test instance.
          - Techniques that provide binary labels to the test instances do not directly allow the analysts to make such a choice, though this can be controlled indirectly through parameter choices within each technique.

Applications

Intrusion detection

Intrusion detection refers to detection of malicious activity (break-ins, penetrations, and other forms of computer abuse) in a computer related system [Phoha 2002]. These malicious activities or intrusions are interesting from a computer security perspective. An intrusion is different from the normal behavior of the system, and hence anomaly detection techniques are applicable in intrusion detection domain.

The key challenge for anomaly detection in this domain is the huge volume of data. The anomaly detection techniques need to be computationally efficient to handle these large sized inputs. Moreover the data typically comes in a streaming fashion, thereby requiring online analysis. Another issue that arises because of the large sized input is the false alarm rate. Since the data amounts to millions of data objects, a few percent of false alarms can make analysis overwhelming for an analyst. Labeled data corresponding to normal behavior is usually available, while labels for intrusions are not. Thus, semisupervised and unsupervised anomaly detection techniques are preferred in this domain.

CLASSIFICATION

Host-Based Intrusion Detection Systems.

Such systems (also referred to as system call intrusion detection systems) deal with operating system call traces. The intrusions are in the form of anomalous subsequences (collective anomalies) of the traces. The anomalous subsequences translate to malicious programs, unauthorized behavior and policy violations. While all traces contain events belonging to the same alphabet, it is the co-occurrence of events that is the key factor in differentiating between normal and anomalous behavior.

Network Intrusion Detection Systems

These systems deal with detecting intrusions in network data. The intrusions typically occur as anomalous patterns (point anomalies) though certain techniques model the data in a sequential fashion and detect anomalous subsequences (collective anomalies) [Gwadera et al. 2005b, 2004]. The primary reason for these anomalies is due to the attacks launched by outside hackers who want to gain unauthorized access to the network for information theft or to disrupt the network. A typical setting is a large network of computers connected to the rest of the world via the Internet.

Table II. Examples of Anomaly Detection Techniques Used for Host-Based Intrusion Detection

Technique Used	Section	References
Statistical Profiling using Histograms	Section 7.2.1	Forrest et al. [1996a, 1999, 2004, 1994, 1999], Hofmeyr et al. [1998], Kosoresow and Hofmeyr [1997], Jagadish et al. [1999], Cabrera et al. [2001], Gonzalez and Dasgupta [2003], Dasgupta 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]
Mixture of Models	Section 7.1.3	Eskin [2000]
Neural Networks	Section 4.1	Ghosh et al. [1998]
Support Vector Machines	Section 4.3	Hu et al. [2003], Heller et al. [2003]
Rule-Based Systems	Section 4.4	Lee et al. [1997, 1998, 2000]

Fraud detection

Fraud detection refers to detection of criminal activities occurring in commercial organizations such as banks, credit card companies, insurance agencies, cell phone companies, stock market, and so on. The malicious users might be the actual customers of the organization or might be posing as customers (also known as identity theft). The fraud occurs when these users consume the resources provided by the organization in an unauthorized way. The organizations are interested in immediate detection of such frauds to prevent economic losses.
Fawcett and Provost [1999] introduce the term activity monitoring as a general approach to fraud detection in these domains. The typical approach of anomaly detection techniques is to maintain a usage profile for each customer and monitor the profiles to detect any deviations. Some of the specific applications of fraud detection are discussed below.

Medical and public health anomaly detection

Anomaly detection in the medical and public health domains typically works with patient records. The data can have anomalies due to several reasons, such as abnormal patient condition, instrumentation errors, or recording errors. Several techniques have also focussed on detecting disease outbreaks in a specific area [Wong et al. 2003]. Thus the anomaly detection is a very critical problem in this domain and requires a high degree of accuracy.

The data typically consists of records that may have several different types of features, such as patient age, blood group, and weight. The data might also have a temporal as well as spatial aspect to it. Most of the current anomaly detection techniques in this domain aim at detecting anomalous records (point anomalies). Typically the labeled data belongs to the healthy patients, hence most of the techniques adopt a semisupervised approach. Another form of data handled by anomaly detection techniques in this domain is time-series data, such as Electrocardiograms (ECG) (Figure 4) and Electroencephalograms (EEG). Collective anomaly detection techniques have been applied to detect anomalies in such data [Lin et al. 2005].
The most challenging aspect of the anomaly detection problem in this domain is that the cost of classifying an anomaly as normal can be very high.

Table VII. Examples of Different Anomaly Detection Techniques Used in Medical and Public Health Domain

Technique Used	Section	References
Parametric Statistical Modeling	Section 7.1	Horn et al. [2001], Laurikkala et al. [2000], Solberg and Lahti [2005], Roberts [2002], Suzuki et al. [2003]
Neural Networks	Section 4.1	Campbell and Bennett [2001]
Bayesian Networks	Section 4.2	Wong et al. [2003]
Rule-Based Systems	Section 4.4	Aggarwal [2005]
Nearest Neighbor based Techniques	Section 5	Lin et al. [2005]
Mixture of Models	Section 7.1.3	Eskin [2000]
Neural Networks	Section 4.1	Ghosh et al. [1998]
Support Vector Machines	Section 4.3	Hu et al. [2003], Heller et al. [2003]
Rule-Based Systems	Section 4.4	Lee et al. [1997, 1998, 2000]

a

industrial damage detection

Industrial units suffer damage due to continuous usage and normal wear and tear. Such damage needs to be detected early to prevent further escalation and losses. The data in this domain is usually referred to as sensor data because it is recorded using different sensors and collected for analysis. Anomaly detection techniques have been extensively applied in this domain to detect such damage. Industrial damage detection can be further classified into two domains, one that deals with defects in mechanical components such as motors, engines, and so on, and the other that deals with defects in physical structures. The former domain is also referred to as system health management.

Table VIII. Examples of Anomaly Detection Techniques Used for Fault Detection in Mechanical Units

Technique Used	Section	References
Parametric Statistical Modeling	Section 7.1	Guttormsson et al. [1999], Keogh et al. [1997, 2002, 2006]
Non-parametric Statistical Modeling	Section 7.2.2	Desforges et al. [1998]
Neural Networks	Section 4.1	Bishop [1994], Campbell and Bennett [2001], Diaz and Hollmen [2002], Harris [1993], Jakubek and Strasser [2002], King et al. [2002], Li et al. [2002], Petsche et al. [1996], Streifel et al. [1996], Whitehead and Hoyt [1993]
Spectral	Section 9	Parra et al. [1996], Fujimaki et al. [2005]
Rule Based Systems	Section 4.4	Yairi et al. [2001]

a

Table IX. Examples of Anomaly Detection Techniques Used for Structural Damage Detection

Technique Used	Section	References
Statistical Profiling using Histograms	Section 7.2.1	Manson [2002], Manson et al. [2001, 2000]
Parametric Statistical Modeling	Section 7.1	Ruotolo and Surace [1997]
Mixture of Models	Section 7.1.3	Hickinbotham et al. [2000a, 2000b], Hollier and Austin [2002]
Neural Networks	Section 4.1	Brotherton et al. [1998, 2001], Nairac et al. [1999, 1997], Surace et al. [1998, 1997], Sohn et al. [2001], Worden [1997]

Image processing

Anomaly detection techniques dealing with images are either interested in any changes in an image over time (motion detection) or in regions that appear abnormal on the static image. This domain includes satellite imagery [Augusteijn and Folkert 2002; Byers and Raftery 1998; Moya et al. 1993; Torr and Murray 1993; Theiler and Cai 2003], digit recognition [Cun et al. 1990], spectroscopy [Chen et al. 2005; Davy and Godsill 2002; Hazel 2000; Scarth et al. 1995], mammographic image analysis [Spence et al. 2001; Tarassenko 1995], and video surveillance [Diehl and Hampshire 2002; Singh and Markou 2004; Pokrajac et al. 2007]. The anomalies are caused by motion, or insertion of a foreign object, or instrumentation errors. The data has spatial as well as temporal characteristics. Each data point has a few continuous attributes such as color, lightness, texture, and so on. The interesting anomalies are either anomalous points or regions in the images (point and contextual anomalies).
One of the key challenges in this domain is the large size of the input. When dealing with video data, online anomaly detection techniques are required.

Table X. Examples of Anomaly Detection Techniques Used in Image Processing Domain

Technique Used	Section	References
Mixture of Models	Section 7.1.3	Byers and Raftery [1998], Spence et al. [2001], Tarassenko [1995]
Regression	Section 7.1.2	Chen et al. [2005], Torr and Murray [1993]
Bayesian Networks	Section 4.2	Diehl and Hampshire [2002]
Support Vector Machines	Section 4.3	Davy and Godsill [2002], Song et al. [2002]
Neural Networks	Section 4.1	Augusteijn and Folkert [2002], Cun et al. [1990], Hazel [2000], Moya et al. [1993], Singh and Markou [2004]
Clustering	Section 6	Scarth et al. [1995]
Nearest Neighbor-Based Techniques	Section 5	Pokrajac et al. [2007], Byers and Raftery [1998]

a

Anomaly detection in Text Data

Anomaly detection techniques in this domain primarily detect novel topics or events or news stories in a collection of documents or news articles. The anomalies are caused due to a new interesting event or an anomalous topic.
The data in this domain is typically high dimensional and very sparse. The data also has a temporal aspect since the documents are collected over time.
A challenge for anomaly detection techniques in this domain is to handle the large variations in documents belonging to one category or topic.

Table XI. Examples of Anomaly Detection Techniques Used for Anomalous Topic Detection in Text Data

Technique Used	Section	References
Mixture of Models	Section 7.1.3	Baker et al. [1999]
Statistical Profiling using Histograms	Section 7.2.1	Fawcett and Provost [1999]
Support Vector Machines	Section 4.3	Manevitz and Yousef [2002]
Neural Networks	Section 4.1	Manevitz and Yousef [2000]
Clustering Based	Section 6	Allan et al. [1998], Srivastava and Zane-Ulman [2005], Srivastava [2006]

a

Sensor networks

Sensor networks have lately become an important topic of research; more from the data analysis perspective, since the sensor data collected from various wireless sensors has several unique characteristics. Anomalies in data collected from a sensor network can either mean that one or more sensors are faulty, or they are detecting events (such as intrusions) that are interesting for analysts. Thus anomaly detection in sensor networks can capture sensor fault detection or intrusion detection or both.

A single sensor network might be comprised of sensors that collect different types of data, such as binary, discrete, continuous, audio, video, and so forth. The data is generated in a streaming mode. Often times the environment in which the various sensors are deployed, and the communication channel, induce noise and missing values in the collected data.

Anomaly detection in sensor networks poses a set of unique challenges. The anomaly detection techniques are required to operate online. Due to severe resource constraints, the anomaly detection techniques need to be lightweight. Another challenge is that data is collected in a distributed fashion, and hence a distributed data mining approach is required to analyze it [Chatzigiannakis et al. 2006]. Moreover, the presence of noise in the data collected from the sensor makes anomaly detection more challenging, since it has to now distinguish between interesting anomalies and unwanted noise/missing values.

Table XII. Examples of Anomaly Detection Techniques Used for Anomaly Detection in Sensor Networks

Technique Used	Section	References
Bayesian Networks	Section 4.2	Janakiram et al. [2006]
Rule-Based Systems	Section 4.4	Branch et al. [2006]
Parametric Statistical Modeling	Section 7.1	Phuong et al. [2006], Du et al. [2006]
Nearest Neighbor-Based Techniques	Section 5	Subramaniam et al. [2006], Zhang et al. [2007], Idé et al. [2007]
Spectral	Section 9	Chatzigiannakis et al. [2006]

a

Other Domains

Anomaly detection has also been applied to several other domains such as speech recognition [Albrecht et al. 2000; Emamian et al. 2000], novelty detection in robot behavior [Crook and Hayes 2001; Crook et al. 2002; Marsland et al. 1999, 2000b, 2000a], traffic monitoring [Shekhar et al. 2001], click-through protection [Ihler et al. 2006], detecting faults in Web applications [Ide and Kashima 2004; Sun et al. 2005], detecting anomalies in biological data [Kadota et al. 2003; Sun et al. 2006; Gwadera et al. 2005a; MacDonald and Ghosh 2007; Tomlins et al. 2005; Tibshirani and Hastie 2007], detecting anomalies in census data [Lu et al. 2003], detecting associations among criminal activities [Lin and Brown 2003], detecting anomalies in Customer Relationship Management (CRM) data [He et al. 2004b], detecting anomalies in astronomical data [Dutta et al. 2007; Escalante 2005; Protopapas et al. 2006] and detecting ecosystem disturbances [Blender et al. 1997; Kou et al. 2006; Sun and Chawla 2004].

CLASSIFICATION BASED

Classification [Tan et al. 2005; Duda et al. 2000] is used to learn a model (classifier) from a set of labeled data instances (training) and then, classify a test instance into one of the classes using the learned model (testing). Classification-based anomaly detection techniques operate in a similar two-phase fashion. The training phase learns a classifier using the available labeled training data. The testing phase classifies a test instance as normal or anomalous, using the classifier.
Classification based anomaly detection techniques operate under the following general assumption:

Assumption. A classifier that can distinguish between normal and anomalous classes can be learned in the given feature space.

Based on the labels available for the training phase, classification-based anomaly detection techniques can be grouped into two broad categories: multi-class and oneclass anomaly detection techniques.

Multi-class classification based anomaly detection techniques assume that the training data contains labeled instances belonging to multiple normal classes [Stefano et al. 2000; Barbara et al. 2001b]. Such anomaly detection techniques teach a classifier to distinguish between each normal class and the rest of the classes. See Figure 6(a) for illustration. A test instance is considered anomalous if it is not classified as normal by any of the classifiers. Some techniques in this subcategory associate a confidence score with the prediction made by the classifier. If none of the classifiers are confident in classifying the test instance as normal, the instance is declared to be anomalous.

One-class classification based anomaly detection techniques assume that all training instances have only one class label. Such techniques learn a discriminative boundary around the normal instances using a one-class classification algorithm, for example, one-class SVMs [Scholkopf et al. 2001], one-class Kernel Fisher Discriminants [Roth ¨ 2004, 2006], as shown in Figure 6(b). Any test instance that does not fall within the learned boundary is declared as anomalous.

Neural Networks-Based

Neural networks have been applied to anomaly detection in multi-class as well as oneclass settings. A basic multi-class anomaly detection technique using neural networks operates in two steps. First, a neural network is trained on the normal training data to learn the different normal classes. Second, each test instance is provided as an input to the neural network. If the network accepts the test input, it is normal and if the network rejects a test input, it is an anomaly [Stefano et al. 2000; Odin and Addison 2000]. Several variants of the basic neural network technique have been proposed that use different types of neural networks, as summarized in Table XIII.
Replicator Neural Networks have been used for one-class anomaly detection [Hawkins et al. 2002; Williams et al. 2002]. A multi-layer feed forward neural network is constructed that has the same number of input and output neurons (corresponding to the features in the data). The training involves compressing data into three hidden layers. The testing phase involves reconstructing each data instance, xi, using the learned network to obtain the reconstructed output, oi. The reconstruction error, δi, for the test instance xi is then computed as:

$$\delta_i = \frac{1}{n}\sum_{j=1}^{n}(x_{ij} - o_{ij})^2,$$

where n is the number of features over which the data is defined. The reconstruction error δi is directly used as an anomaly score for the test instance.

Table XIII. Some Examples of Classification-Based Anomaly Detection Techniques Using Neural Networks

Neural Network Used	References
Multi layered Perceptrons	[Augusteijn and Folkert 2002; Cun et al. 1990; Sykacek 1997; Ghosh et al. 1999a, 1998; Barson et al. 1996; He et al. 1997; Nairac et al. 1997; Hickinbotham and Austin 2000b; Vasconcelos et al. 1995, 1994]
Neural Trees	[Martinez 1998]
Autoassociative Networks	[Aeyels 1991; Byungho and Sungzoon 1999; Japkowicz et al. 1995; Hawkins et al. 2002; Ko and Jacyna 2000; Manevitz and 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 and Hollmen 2002]
Adaptive Resonance Theory Based	[Moya et al. 1993; Dasgupta and Nino 2000; Caudell and Newman 1993]
Radial Basis Function-Based	[Albrecht et al. 2000; Bishop 1994; Brotherton et al. 1998; Brotherton and Johnson 2001; Li et al. 2002; Nairac et al. 1999, 1997; Ghosh and Reilly 1994; Jakubek and Strasser 2002]
Hopfield Networks	[Jagota 1991; Crook and Hayes 2001; Crook et al. 2002; Addison et al. 1999; Murray 2001]
Oscillatory Networks	Ho and Rouat 1997, 1998; Kojima and Ito 1999; Borisyuk et al. 2000; Martinelli and Perfetti 1994]

a

Bayesian Networks-Based

Bayesian networks have been used for anomaly detection in the multi-class setting. A basic technique for a univariate categorical data set using a na¨ ıve Bayesian network estimates the posterior probability of observing a class label from a set of normal class labels and the anomaly class label, given a test data instance. The class label with largest posterior is chosen as the predicted class for the given test instance. The likelihood of observing the test instance given a class and the prior on the class probabilities, is estimated from the training data set. The zero probabilities, especially for the anomaly class, are smoothed using Laplace Smoothing.

The basic technique can be generalized to multivariate categorical data sets by aggregating the per-attribute posterior probabilities for each test instance and using the aggregated value to assign a class label to the test instance.
Several variants of the basic technique have been proposed for network intrusion detection [Barbara et al. 2001b; Sebyala et al. 2002; Valdes and Skinner 2000; Mingming 2000; Bronstein et al. 2001], for novelty detection in video surveillance [Diehl and Hampshire 2002], for anomaly detection in text data [Baker et al. 1999], and for disease outbreak detection [Wong et al. 2002, 2003].

This basic technique assumes independence between the different attributes. Several variations of the basic technique have been proposed that capture the conditional dependencies between the different attributes using more complex Bayesian networks [Siaterlis and Maglaris 2004; Janakiram et al. 2006; Das and Schneider 2007]

PROPOSTA PARA WSN

Support Vector Machines-Based

Support Vector Machines (SVMs) [Vapnik 1995] have been applied to anomaly detection in the one-class setting. Such techniques use one class learning techniques for SVM [Ratsch et al. 2002] and learn a region that contains the training data instances (a boundary). Kernels, such as radial basis function (RBF) kernel, can be used to learn complex regions. For each test instance, the basic technique determines if the test instance falls within the learned region. If a test instance falls within the learned region, it is declared as normal, else it is declared as anomalous.
Variants of the basic technique have been proposed for anomaly detection in audio signal data [Davy and Godsill 2002], novelty detection in power generation plants [King et al. 2002] and system call intrusion detection [Eskin et al. 2002; Heller et al. 2003; Lazarevic et al. 2003]. The basic technique has also been extended to detect anomalies in temporal sequences [Ma and Perkins 2003a, 2003b].
A variant of the basic technique [Tax and Duin 1999a, 1999b; Tax 2001] finds the smallest hypersphere in the kernel space that contains all training instances, and then determines on which side of that hypersphere a test instance lies. If a test instance lies outside the hypersphere, it is declared to be anomalous.
Song et al. [2002] use Robust Support Vector Machines (RSVM), which are robust to the presence of anomalies in the training data. RSVM have been applied to system call intrusion detection [Hu et al. 2003].

Rule-Based

Rule-based anomaly detection techniques learn rules that capture the normal behavior of a system. A test instance that is not covered by any such rule is considered as an anomaly. Rule-based techniques have been applied in multi-class as well as one-class settings.
A basic multi-class rule-based technique consists of two steps. The first step is to learn rules from the training data using a rule learning algorithm, such as RIPPER, Decision Trees, and so on. Each rule has an associated confidence value that is proportional to ratio between the number of training instances correctly classified by the rule and the total number of training instances covered by the rule. The second step is to find, for each test instance, the rule that best captures the test instance. The inverse of the confidence associated with the best rule is the anomaly score of the test instance.
Several minor variants of the basic rule-based technique have been proposed [Fan et al. 2001; Helmer et al. 1998; Lee et al. 1997; Salvador and Chan 2003; Teng et al. 1990].
Association rule mining [Agrawal and Srikant 1995] has been used for one-class anomaly detection by generating rules from the data in an unsupervised fashion. Association rules are generated from a categorical data set. To ensure that the rules correspond to strong patterns, a support threshold is used to prune out rules with low support [Tan et al. 2005]. Association rule mining-based techniques have been used for network intrusion detection [Mahoney and Chan 2002, 2003; Mahoney et al. 2003; Tandon and Chan 2007; Barbara et al. 2001a; Otey et al. 2003, system call intrusion detection [Lee et al. 2000; Lee and Stolfo 1998; Qin and Hwang 2004], credit card fraud detection [Brause et al. 1999], and fraud detection in spacecraft housekeeping data [Yairi et al. 2001]. Frequent itemsets are generated in the intermediate step of association rule mining algorithms. He et al. [2004a] propose an anomaly detection algorithm for categorical data sets in which the anomaly score of a test instance is equal to the number of frequent itemsets in which it occurs.

PROPOSTA PARA WSN

Computational Complexity. The computational complexity of classification-based techniques depends on the classification algorithm being used. For a discussion on the complexity of training classifiers, see Kearns [1990]. Generally, training decision trees tends to be faster, while techniques that involve quadratic optimization, such as SVMs, are more expensive; though linear time SVMs [Joachims 2006] have been proposed that have linear training time. The testing phase of classification techniques is usually very fast since the testing phase uses a learned model for classification.

Advantages and Disadvantages of Classification-Based Techniques. The advantages of classification-based techniques are as follows:
(1) Classification-based techniques, especially the multi-class techniques, can make use of powerful algorithms that can distinguish between instances belonging to different classes.
(2) The testing phase of classification-based techniques is fast, since each test instance needs to be compared against the precomputed model.

The disadvantages of classification-based techniques are as follows:
(1) Multi-class classification-based techniques rely on the availability of accurate labels for various normal classes, which is often not possible.
(2) Classification-based techniques assign a label to each test instance, which can also become a disadvantage when a meaningful anomaly score is desired for the test instances. Some classification techniques that obtain a probabilistic prediction score from the output of a classifier, can be used to address this issue [Platt 2000].