

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], Kawser and Hefsey [1997], Jagadeesh et al. [1999], Cabrera et al. [2001], Gonzalez and Dasgupta [2003], Dasgupta et al. [2000, 2002], Ghosh et al. [1998a, 1998, 1996b], 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]

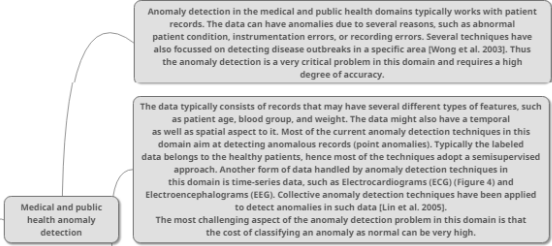
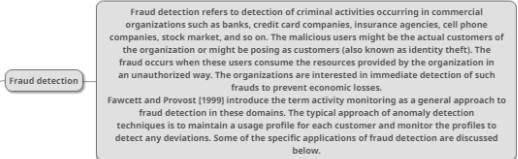


Table VII. Examples of Different Anomaly Detection Techniques Used in Medical and Public Health Domain

Technique Used	Section	References
Parametric Statistical Modeling	Section 7.1	Horn et al. [2001], Laurikkala et al. [2000], Salberg 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]

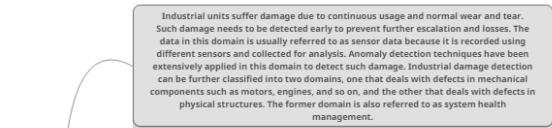


Table VIII. Examples of Anomaly Detection Techniques Used for Fault Detection in Mechanical Units

Technique Used	Section	References
Parametric Statistical Modeling	Section 7.1	Guttorfsson 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], Pelache et al. [1996], Strobel 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]

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	Rustolo and Sumac [1997]
Mixture of Models	Section 7.1.3	Hickinbotham et al. [2000a, 2000b], Hollier and Austin [2002]
Neural Networks	Section 4.1	Brodherton et al. [1998, 2001], Nairac et al. [1999, 1997], Surace et al. [1998, 1997], Sohn et al. [2001], Worden [1997]

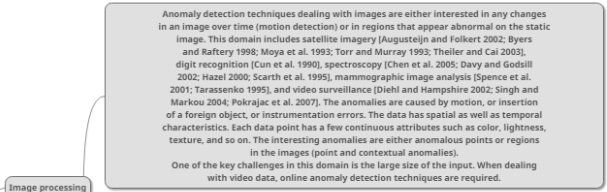


Table X. Examples of Anomaly Detection Techniques Used in Image Processing Domain

Technique Used	Section	References
Mixture of Models	Section 7.1.3	Byers and Raftery [1998], Spence et al. [2001], Tarasenko [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	Augustein 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	Pekarjac et al. [2007], Byers and Raftery [1998]

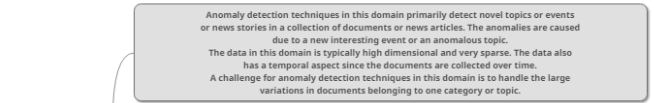


Table XI. Examples of Anomaly Detection Techniques Used for Anomalous Topic Detection in Text Data

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	Manovitz and Yousef [2002]
Neural Networks	Section 4.1	Manovitz and Yousef [2000]
Clustering Based	Section 6	Allan et al. [1998], Srivastava and Zane-Ulman [2005], Srivastava [2006]

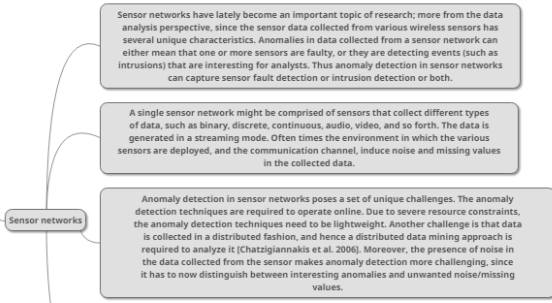
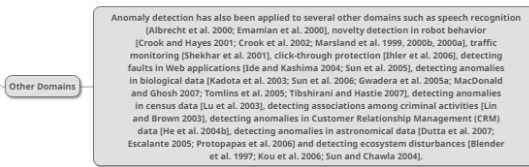


Table XII. Examples of Anomaly Detection Techniques Used for Anomaly Detection in Sensor Networks

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], Ide et al. [2007]
Spectral	Section 9	Chatzigiannakis et al. [2006]



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 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, x_i , using the learned network to obtain the reconstructed output, o_i . The reconstruction error, δ_i , for the test instance x_i 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 δ_i 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	[Augustejn 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] [Martinez 1998]
Neural Trees	[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]
Autoassociative Networks	[Moya et al. 1993; Dasgupta and Nino 2000; Caudell and Newman 1993]
Adaptive Resonance Theory 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]
Radial Basis Function-Based	[Jagota 1991; Crook and Hayes 2001; Crook et al. 2002; Addison et al. 1999; Murray 2001]
Hopfield Networks	[Ho and Rouat 1997, 1998; Kojima and Ito 1999; Borisjuk et al. 2000; Martinelli and Perfetti 1994]
Oscillatory Networks	

Bayesian networks have been used for anomaly detection in the multi-class setting. A basic technique for a univariate categorical data set using a naïve 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; Schyala 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 (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 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; Orey 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].