

**IEEE / IST Workshop on
Monitoring, Attack Detection and Mitigation**
Tuebingen, Germany

**Robust Methods for Unsupervised PCA-based
Anomaly Detection**

Roland Kwitt

September 28-29, 2006

Overview

- 1 Problem Definition
- 2 Anomaly Detection based on Principal Components
- 3 Robust Estimators
- 4 Examples

Problem Definition

- Anomaly detection usually requires anomaly-free training data
- This can only be guaranteed in very few cases
- A separate cleaning step is required (\Rightarrow supervised anomaly detection)
- Don't waste the administrators time
- **Aim:** Unsupervised anomaly detection, even if the training data set is contaminated
- We need robust methods in the training phase of a detector

Anomaly Detection based on Principal Components

- We usually have a high-dimensional data set with n points in p dimensions
- Graphical methods are often not convenient to identify outliers
- The idea to use principal components to identify outliers in multivariate data is not new
- Principal components are linear combinations of the original variables
- **Example:** Let $\mathbf{x}_i^T = (x_{i1}, \dots, x_{ip})$ denote the i -th observation, then the sample PC score of the \mathbf{x}_i on the k -th PC is defined by

$$z_{ik} = \mathbf{a}_k^T \mathbf{x}_i = a_{k1}x_{i1} + a_{k2}x_{i2} + \dots + a_{kp}x_{ip}$$

- \mathbf{a}_k is the eigenvector corresponding to the k -th largest eigenvalue l_k of the sample covariance matrix \mathbf{S} .

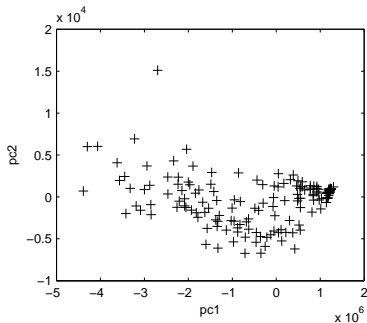
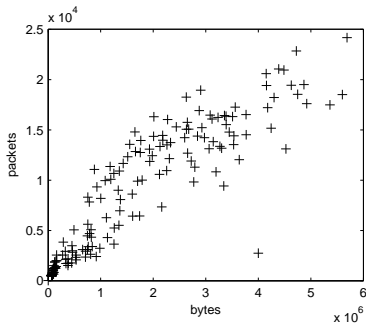
Anomaly Detection based on Principal Components

- The PCs are uncorrelated
- The question is, what types of outliers can be detected by PCs
- Outliers, which inflate variance or covariance are detectable by the **major** PCs
- Outliers, violating the correlation structure of the data are detectable by the **minor** PCs (see next slide)
- Shyu et al. introduces two measures to detect anomalies

$$v_{i1}^2 = \sum_{k=1}^q \frac{z_{ik}^2}{l_k} \quad \text{and} \quad v_{i2}^2 = \sum_{k=p-r+1}^p \frac{z_{ik}^2}{l_k}$$

A Special Outlier Example

- #Bytes, #Packets measured over consecutive time intervals



- These distances are a special version of the outlier measure

$$d_i^2 = \sum_{k=p-q+1}^p \frac{z_{ik}^2}{l_k},$$

which was first introduced by Gnanadesikan and Kettenring in 1972. If we set $p = q$, d_i^2 results in the squared Mahalanobis distance of observation \mathbf{x}_i .

Squared Mahalanobis Distance

$$MD^2(\mathbf{x}_i, \mathbf{X}) = (\mathbf{x}_i - T(\mathbf{X}))^T C(\mathbf{X})^{-1} (\mathbf{x}_i - T(\mathbf{X}))$$

- **Problem:** The classic estimators for location (denoted by \mathbf{T}) and covariance (denoted by \mathbf{C}) are very susceptible to the presence of outliers.

Robust Estimators

Breakdown Point

Smallest fraction of outliers that can cause \mathbf{T} to take on arbitrary values.

- Arithmetic Mean and the classic sample covariance matrix estimator have both breakdown 0%
- Two Alternatives:
 - Minimum Covariance Determinant (MCD) estimator
 - Minimum Volume Ellipsoid (MVE) estimator
- We propose to use high-breakdown estimators for location and covariance

MCD and MVE

Minimum Covariance Determinant (MCD) Estimator

$\mathbf{T}(\mathbf{X})$: Mean of the h points of \mathbf{X} for which the determinant of the covariance matrix is minimal

Minimum Volume Ellipsoid (MVE) Estimator

$\mathbf{T}(\mathbf{X})$: Center of the minimum volume ellipsoid covering (at least) h points of \mathbf{X}

- For both MCD and MVE, $\mathbf{C}(\mathbf{X})$ is the classic estimate, based on the h points
- Breakdown is 50% as $n \rightarrow \infty$.

Classic vs. Robust Mahalanobis Distance

- Shown here are the 97.5% classic/robust confidence ellipses, defined by the set of points whose distance is $\leq \sqrt{\chi_{p,0.975}^2}$

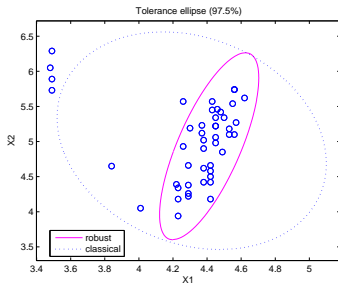
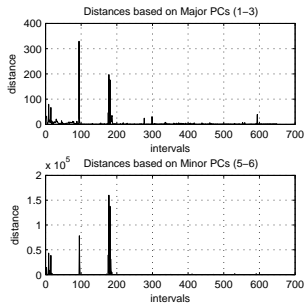


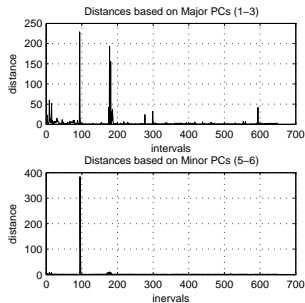
Figure: A classic example of the **masking effect** (Robust Distance obtained with MCD)

DARPA 1999 IDS Example

- Data Source: First 12 hours of day 4, Week 2 (Training data, with embedded attacks)



(a) MCD



(b) Standard

Thanks for your attention!