

## 12. PCA / Anomaly Detection


Data Analysis for Networks - DataNets'19  
Anastasios Giovanidis

Sorbonne-LIP6



January 08, 2020

## Bibliography

- B.1** Gareth James, Daniela Witten, Trevor Hastie, Robert Tibshirani. “An introduction to statistical learning: with applications in R”. Springer Texts in Statistics.  
 **Chapter 10**  
ISBN 978-1-4614-7137-0 (DOI 10.1007/978-1-4614-7138-7)
- B.2** Qi Liao, and Slawomir Stanczak. “Network State Awareness and Proactive Anomaly Detection in Self-Organizing Networks”. IEEE Globecom 2015 Workshops,  
DOI: 10.1109/GLOCOMW.2015.7414141
- B.3** Anukool Lakhina, Mark Crovella, and Christophe Diot. “Diagnosing Network-Wide Traffic Anomalies”. SIGCOMM '04. pp. 219-230  
<https://doi.org/10.1145/1015467.1015492>

# PCA

A. Giovanidis 2019

The idea behind PCA is to find a **low-dimensional set of axes** that summarise data (unsupervised - no labels). Why?

- ▶ Many features in the data set can be **highly correlated**, so we need not keep both.
- ▶ Other features have very low variance and do not sufficiently differentiate between possible classes.
- ▶ We should remove the redundancy and describe the data-set with less properties.

☞ PCA only looks at **feature variance**: features that present high variance are more likely to have a good split between classes.

## How does it work? (I)

PCA **is not** feature selection.

☞ It rather constructs a new set of properties with reduced dimension based on a **linear combination** of the total number of features.

- ▶ PCA performs a linear transformation moving the original set of features to a new reduced space.
- ▶ The new space is composed by some principal components.
- ▶ These new features do not have any real meaning for us, only algebraic.

☞ Principal components are **all uncorrelated (orthogonal) to each other**.

## How does it work? (II)

The algorithm uses the concepts of variance matrix, covariance matrix, eigenvector and eigenvalues pairs to perform PCA, providing a set of **eigenvectors** and its respective **eigenvalues** as a result.

- ▶ The eigenvectors represent the new set of axes of the principal component space and the eigenvalues carry the information of quantity of variance that each eigenvector has.
- ▶ To reduce the dimension of the dataset we need to **keep those eigenvectors that have more variance and discard those with less variance.**

## Definitions

☞ The **first linear component** of a set of features  $X_1, \dots, X_p$  is the normalized linear combination of the features

$$Z_1 = \phi_{11}X_1 + \phi_{21}X_2 + \dots + \phi_{p1}X_p,$$

with the largest variance. Here  $\sum_{j=1}^p \phi_{j1}^2 = 1$ . Then,

$\phi_1 = (\phi_{11}, \phi_{21}, \dots, \phi_{p1})^T$  is the principal component, or the direction of maximum data variance.

We can solve to find the first and higher principal components by **eigen-decomposition**.

In total, there are  $\min(N - 1, p)$  principal components.

# Geometry

A. Giovanidis 2019

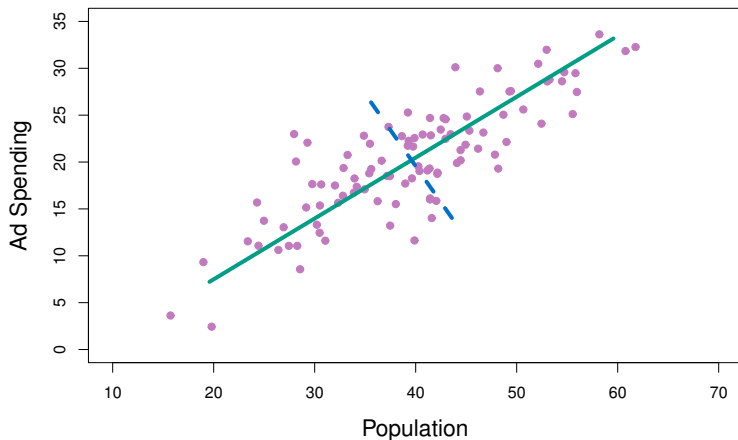
- ▶ The vector  $\phi_1$  defines a direction in feature space along which the data varies the most.
- ▶ If we project the  $N$  data points  $x_1, \dots, x_N$  onto this direction, the projected values are the principal components  $z_{11}, \dots, z_{N1}$ .

The second principal component  $Z_2$  is again the linear combination of  $X_1, \dots, X_p$  that has maximal variance out of all linear combinations that are **uncorrelated with  $Z_1$** .

Uncorrelated with  $Z_1$  is equivalent to **constrain the direction  $\phi_2$  to be orthogonal (perpendicular) to  $\phi_1$** .

# Geometry of 2 components: 2 features

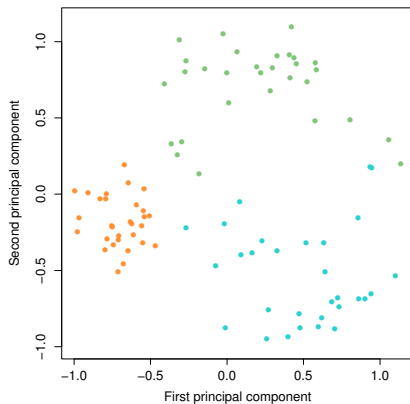
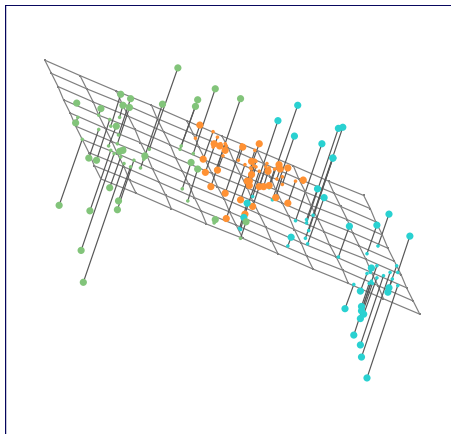
A. Giovanidis 2019





# Geometry of 2 components: 3 features

A. Giovanidis 2019



## Proportion of variance explained

👉 **Question:** How much of the information in a given data set is lost by projecting the observations onto the first few principal components?

- ▶ The **total variance** present in the (centered) data

$$\text{Total } V = \sum_{j=1}^p \text{Var}(X_j) = \sum_{j=1}^p \frac{1}{N} \sum_{i=1}^N x_{ij}^2$$

- ▶ The **variance** explained by the  $m$ -th principal component

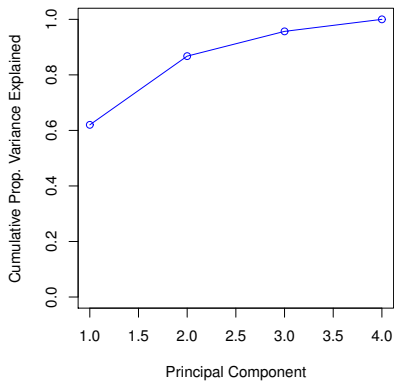
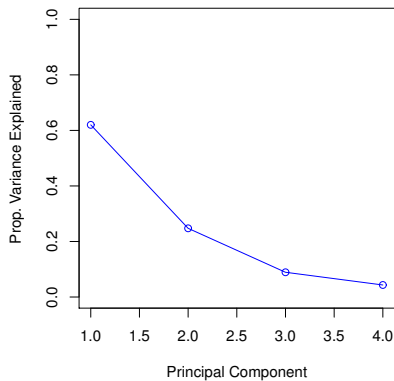
$$V_m = \frac{1}{N} \sum_{i=1}^N z_{im}^2 = \frac{1}{N} \sum_{i=1}^N \left( \sum_{j=1}^p \phi_{jm} x_{ij} \right)^2$$

☞ Hence, the cumulative prop. of variance explained (PVE) by  $r$  PCs is

$$PVE = \frac{\sum_{m=1}^r V_m}{\text{Total } V}$$

## PVA curves

A. Giovanidis 2019



## How many PCs to keep?

☞ If we use all  $\min(N - 1, p)$  PCs then we get a PVE equal to 1. But then we do not get any dimensionality reduction!

Actually, we want to use the smallest number of principal components required to get a good understanding of the data.

- ▶ We can choose the PCs by observing the PVA plot for an elbow.
- ▶ In unsupervised learning it depends on the application.
- ▶ In supervised learning the best number of PCs can be selected by cross-validation.

# PCA Network Applications:

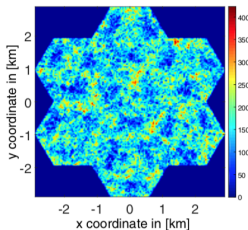
## PCA for 5G

# Application no.1: PCA for 5G

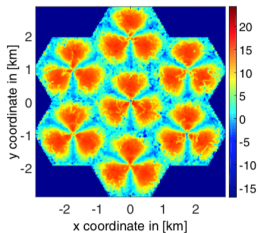
A. Giovanidis 2019

☞ We refer to the paper in reference [B.2]

**Aim:** In 5G cellular networks, to infer the network state and detect anomalous network behaviour.



(a) Number of UEs



(b) Average SINR

How: (2 step)

**Step.1** Dimension reduction through PCA (visualization)

**Step.2** Clustering and classification in low dimensions

☞ Dimensionality reduction can very much improve clustering and classification results.

# Input:16 data features

- ▶ Control Parameters
- ▶ Key Performance Indicators (KPI)
- ▶ Statistical Network Measurements

TABLE I: Selected 4 control parameters and 16 network metrics

Control Parameter	KPI	Statistical Network Measurements
1. antenna tilt	1. call drop rate (CDR)	11. number of UEs
2. transmit power	2. call blocking rate (CBR)	12. average UE arrival rate in neighboring cells
3. time-to-trigger (TTT)	3. incoming HO rate (HR <sub>in</sub> )	13. mean of RSRQ distribution
4. hysteresis	4. outgoing HO rate (HR <sub>out</sub> )	14. variance of RSRQ distribution
	5. HO ping-pong rate (HPPR)	15. mean of RSRQ distribution in neighboring cells
	6. Mobility success rate (MSR)	16. variance of RSRQ distribution in neighboring cells
	7. VoIP load	
	8. streaming load	
	9. average throughput of VoIP user	
	10. average throughput of streaming user	



## PCA Method

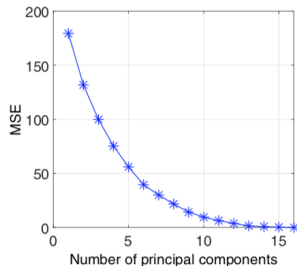
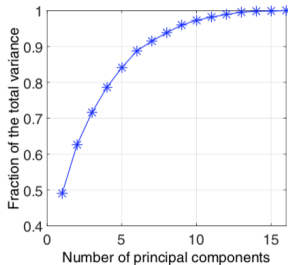
- ▶ Available data-set  $\{\mathbf{x}_i\}$ ,  $i = 1, \dots, N$ .
- ▶ Each measurement has  $p = 16$  features (dimensions)
- ▶ Let  $\mathbf{X} := [\mathbf{x}_1, \dots, \mathbf{x}_N]^T$  be the  $N \times p$  matrix.

### Method:

1. Center each row (feature) of the  $\mathbf{X}$  matrix.
2. Perform SVD of  $\mathbf{X}$ , i.e.  $\mathbf{X} = \mathbf{U}\mathbf{D}\mathbf{V}^T$ .
3. The columns of  $\mathbf{V}$  are the principal components.
4. Let  $d < p$  be the desired **new dimension**.
5. Compute the solution  $\mathbf{Z} = [\mathbf{z}_1, \dots, \mathbf{z}_N]^T$ , this is an  $N \times d$  matrix.  
How? Take the  $d$  first columns of  $\mathbf{U}$  and the  $d \times d$  upper left part of  $\mathbf{D}$ , so we get  $\mathbf{Z} = \mathbf{U}_d \mathbf{D}_d$  the data set with reduced dimension.

## How many principal components

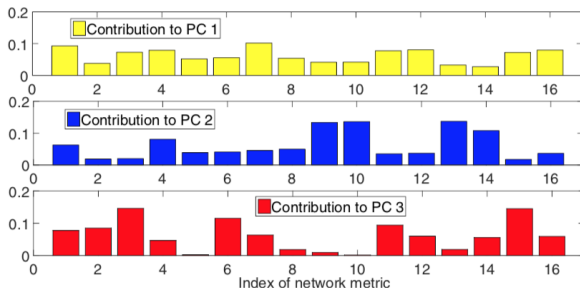
How much can the 3 principal components explain from the total variance?



👉 **Answer:** Over 70% !

## Explained variance per feature per PC

Interestingly, different components can explain better different features.



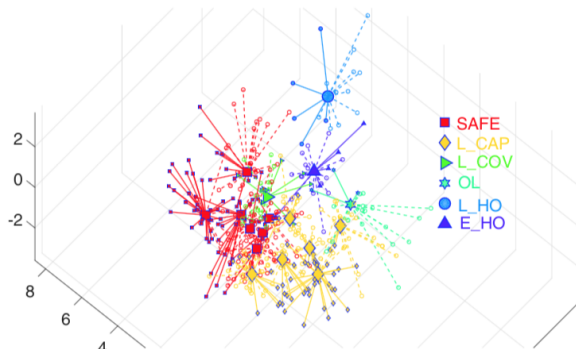
(d) Contribution of 16 network metrics to the top 3 PCs

Some features are more pronounced so the 1st PC explains most, but others are more subtle.

## Visualisation in 3D

A. Giovanidis 2019

In the 3D-plane the data points can be visualised



## Clustering and Anomaly detection

The network states can be clustered in low dimension.

These classes can be used for anomaly detection:

- ▶ One class for SAFE state
- ▶ Various classes for various types of anomalous states

TABLE II: Supervised classes based on a priori knowledge

Class	A priori knowledge
1. SAFE	all KPIs satisfy the requirements of QoS
2. L_COV	high CDR, low average throughput, low mean of RSRQ, high variance of RSRQ
3. L_CAP	low average throughput, normal CDR
4. OL	high CBR, high load, low average throughput
5. E_HO	high HPPR, high HR_in and HR_out
6. L_HO	low MSR, low HPPR

**Note:** RSRQ is Reference Signal Received Quality. For CDR, CBR, HPPR, HR-in, HR-out, MSR see feature table above.

## Clustering method

One can use [K-means](#), with  $K = 6$  equal to the number of various states-modes. As an interesting hint, one can use an even larger  $K$  and after this, group back together as in [hierarchical clustering](#).

☞ Very often some data are labeled empirically, so we can characterise which cluster refers to which class-mode.

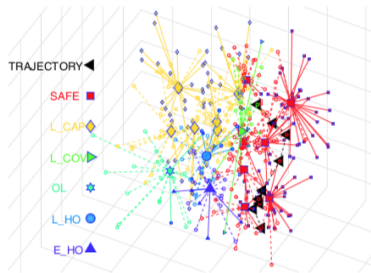
After having clustered, we can use a classifier to predict the class of future network states, and track the status of the network.

This approach is very similar to Exercise 1 in the TP11 : clustering.

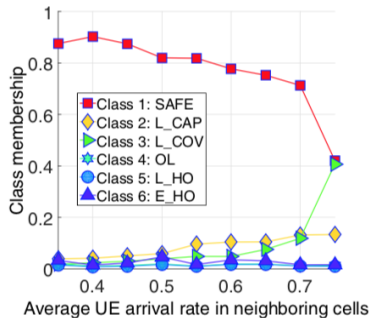
# Anomaly Visualisation in 3D

A. Giovanidis 2019

In the 3D-plane we can see the evolution towards an anomalous state



(a) Trajectory of network state.



(b) Class memberships.

# PCA Network Applications:

## Network-traffic anomaly detection



## Network-traffic anomaly

Source material from [B.3]

In network applications it is very important to detect anomalies.

An **anomaly** is characterised by unusual and significant changes in a network's traffic levels, which can often span multiple links.

Anomalies need to be diagnosed. One must extract and interpret anomalous patterns from large amounts of high-dimensional noisy data.

Anomaly causes may be due to:

- ▶ Denial of Service (DoS) attacks,
- ▶ Router misconfigurations.

# Anomaly detection

A. Giovanidis 2019

- ☞ Anomalies can create congestion in the network and stress resource utilisation in a router. This is bad from an operational standpoint.
- ☞ Some anomalies may have dramatic impact on the end user customer, without being dangerous for the networks.

Anomaly detection designates those points in time at which the network is experiencing an anomaly. The algorithm should have a high detection probability and a low false alarm probability.

## Network and traffic volume

The studied network has the following structure:

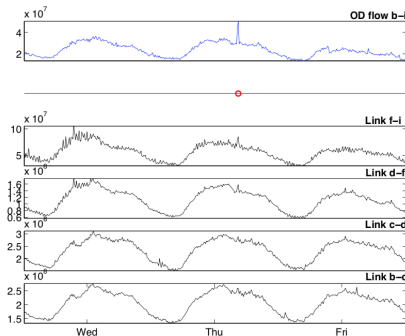
- ▶ Nodes are the PoP (Point of Presence)
- ▶ Origin-Destination (OD) flows
- ▶ The path followed by each OD flow is determined by routing tables.

The traffic observed on each link is the superposition of these OD flows.

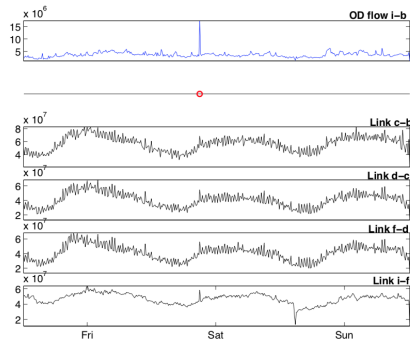
**Volume anomaly** is a sudden (with respect to time-step) positive or negative change in an OD flow's traffic. Such an anomaly originates outside the network, so it propagates from the origin PoP to the destination PoP.

👉 Networks: Sprint (13 PoPs, 49 Links), Abilene (11 PoPs, 41 Links).

# Traffic Anomaly by an OD flow



(a) Example 1



(b) Example 2

Figure 1: Examples of anomalies at the OD flow level (top row) that we want to diagnose from link traffic.

## Method (I)

- ☞ The anomaly detection method uses PCA to separate **normal** and **residual** network-wide traffic conditions.
- ▶ The measurement matrix  $\mathbf{X}$  is of dimension  $T \times M$ , where  $T$  is the number of successive time intervals of interest, and  $M$  the number of links in the network.
  - ▶ Each column  $i$  denotes the sampled time-series of the  $i$ -th link, each row  $j$  represents an instance of all the links at time  $j$ .
  - ▶ Here  $T = 1008$  of 10-min bins in a week long time-series, and  $M$  the number of links ( 41 or 49 depending on the studied network).

PCA is a coordinate transformation method that maps a given set of data points onto new axes, the principal components.

## Method (II)

A. Giovanidis 2019

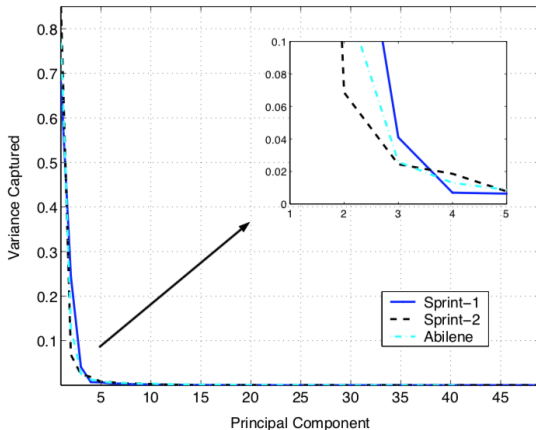
- ▶ Adjust  $\mathbf{X}$  so that its columns have zero mean (centered).
- ▶ Choose a number of principal components that capture the maximum variance from the original data, but still have a reduced dimension.

☞ The first principal component captures the variance of the data to the greatest degree possible on a single axis.

The next principal components then each capture the maximum variance among the remaining orthogonal directions.

Thus, the principal axes are ordered by the amount of data variance that they capture.

## Variance captured per PC



**Figure 2: Fraction of total link traffic variance captured by each principal component.**

## PC definition

We can find  $M$  principal components (directions)  $\mathbf{v}_i$ ,  $i = 1, \dots, M$

- ▶ The first PC points in the direction of maximum variance

$$\mathbf{v}_1 = \arg \max_{\|\mathbf{v}\|=1} \|\mathbf{X}\mathbf{v}\|$$

- ▶ Once the  $k - 1$  PCs have been determined, the  $k$ -th PC corresponds to the maximum variance of the residual

$$\mathbf{v}_k = \arg \max_{\|\mathbf{v}\|=1} \left\| \left( \mathbf{X} - \sum_{i=1}^{k-1} \mathbf{X}\mathbf{v}_i\mathbf{v}_i^T \right) \mathbf{v} \right\|$$



## Normal and Anomalous Set

As the above Figure shows, the first 4 PCs capture most of the variance and hence the most significant temporal patterns common to the ensemble of all link traffic time-series.

The current method works by separating the principal axes into two sets, corresponding to

- ▶ normal part ( $y^*$ ) and
- ▶ residual variation ( $\tilde{y}$ ) in traffic.

$$y = y^* + \tilde{y}$$

## Anomaly detection

Suppose we keep  $r < M$  dimensions that sufficiently capture the variance. These components are characterised by the vectors  $(\mathbf{v}_1, \dots, \mathbf{v}_r)$ .

We can form the matrix  $P = (\mathbf{v}_1, \dots, \mathbf{v}_r)$  of size  $M \times r$ . Then

$$(normal) \quad y^* = \mathbf{P}\mathbf{P}^T y = \mathbf{C}y$$

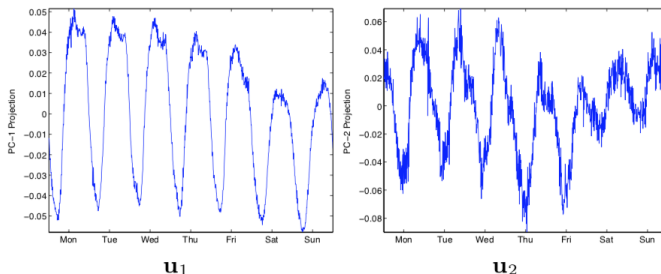
$$(residue) \quad y^* = (\mathbf{I} - \mathbf{P}\mathbf{P}^T) y = \tilde{\mathbf{C}}y$$

The information about the anomaly is found in the residue. If

$$||\tilde{y}||^2 = ||\tilde{\mathbf{C}}y||^2 > \delta$$

then an anomaly is declared! (threshold rule)

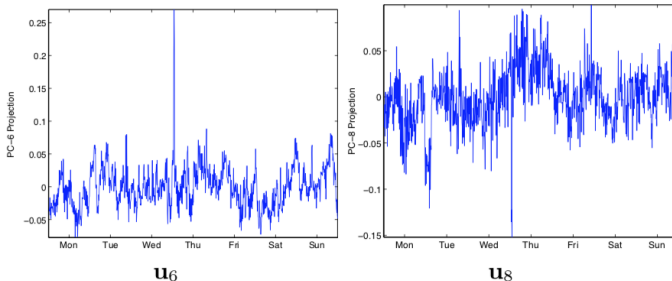
## Example: normal part



(a) Normal Behavior

This part of the data variance is described by the  $r$  principal components. We do not expect to find anomalies in this part. ( $\mathbf{u}_1 = \mathbf{X}\mathbf{v}_1$ ,  $\mathbf{u}_2 = \mathbf{X}\mathbf{v}_2$ )

## Example: residue part

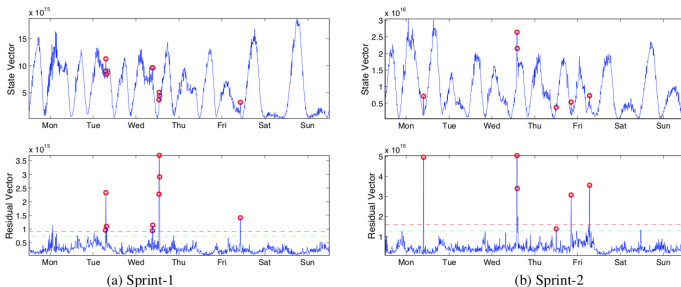


(b) Anomalous Behavior

This part of the data variance is the residue, described by the  $M - r$  remaining components, or by  $\mathbf{X}$  after subtracting the first  $r$  components. It is where [anomalies live](#).

## Example: anomaly detection

A. Giovanidis 2019



**Figure 4:** Timeseries plots of state vector squared magnitude ( $\|y\|^2$ , upper) and residual vector squared magnitude ( $\|\tilde{y}\|^2$ , lower) for two weeks of Sprint data.

An example of anomaly detection on time-series, by observing the residue and using a threshold rule. All time instants when the threshold is exceeded are declared anomalous.

**END**