Intrusion detection in unlabeled data with quarter-sphere Support Vector Machines

Pavel Laskov Christin Schäfer Igor Kotenko

Fraunhofer FIRST.IDA SPIIRAS

Berlin, Germany St. Petersburg, Russia

Fraunhofer Institut Rechnerarchitektur und Softwaretechnik FIRST

Unsupervised anomaly detection in IDS

- *Main idea*: search for anomalies in the data *without* training on the clean data.
- *Previous work*: (Eskin et al., 2002), (Lazarevic et al., 2003).
- *Advantages*: no need for training, no need for extensive amount of clean data.
- *Problems*: false alarm rates, performance.

Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

Motivation for our work

- Reproduce the state-of-the-art results on the KDD Cup (DARPA '98) dataset (with the main focus on one-class SVM).
- Investigate the methods from the machine learning point of view.
- Investigate the behavior of anomaly detection methods with varying outlier percentages.

Motivation for our work

- Reproduce the state-of-the-art results on the KDD Cup (DARPA '98) dataset (with the main focus on one-class SVM).
- Investigate the methods from the machine learning point of view.
- Investigate the behavior of anomaly detection methods with varying outlier percentages.

Main result: we propose a new anomaly detection technique, a quarter-sphere SVM, which is particularly geared for data used in intrusion detection and is significantly faster than other one-class SVM methods.

Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

KDD Cup data: summary of features

KDD Cup dataset contains the total of 42 features computed for connections of TCP data from the DARPA '98 evaluation.

Source	Sample attributes	Type
Basic connection properties	`duration, service, src_bytes, dest_bytes`	`int, bool, string`
Selected content features	`logged_in, root_shell, num_shells`	`int, bool`
Time window features	`count, srv_count, serror_rate, rerror_rate`	`int, float`
Connection window features	`dst_host_count, ...`	`int, float`

Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

KDD Cup data: normalization

- *Numerical attributes*: replace the values with distance from mean in the number of standard deviations.

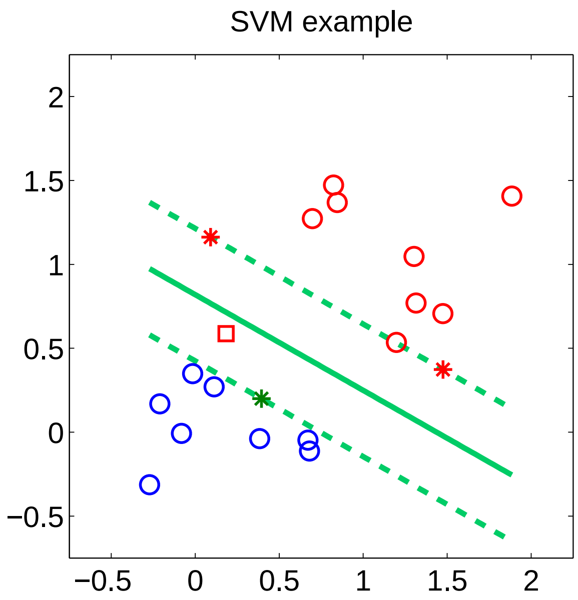
$$x_i^{(d)} \longleftarrow \frac{|x_i^{(d)} - \hat{\mu}^{(d)}|}{\hat{\sigma}^{(d)}}$$

- *Categorical attributes*: extend the space with $\mathrm{card}^{(d)}$ coordinates; assign the value of $\frac{1}{\mathrm{card}^{(d)}}$ to coordinates matching the attribute's value.

Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

Support Vector Machines (SVM)

The main idea of SVM: separation of examples of two classes with a hyperplane producing a large margin:



$$\min_{\mathbf{w},\xi,b} \quad \frac{1}{2}||\mathbf{w}||^2 + \frac{C}{l}\sum_{i=1}^{l}\xi_i$$

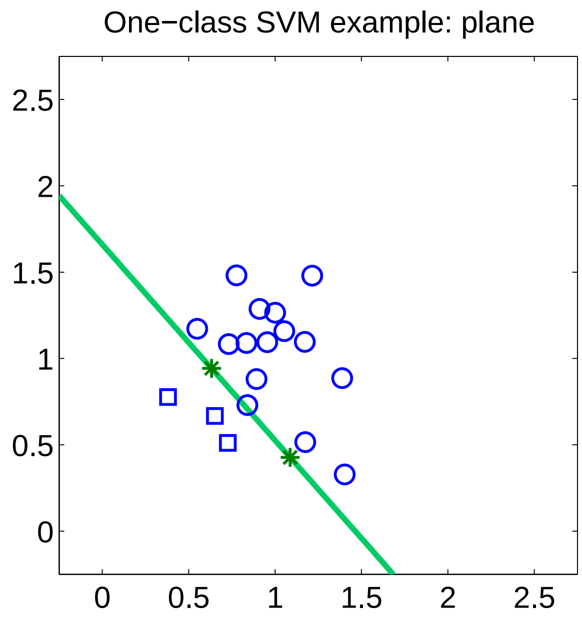
$$\text{subject to} \quad y_i((\mathbf{w}\cdot\mathbf{x}_i)+b) \geq 1-\xi_i,$$

$$\xi_i \geq 0.$$

Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

One-class SVM: plane formulation

The main idea of the plane one-class SVM: separate data from the origin with a hyperplane:

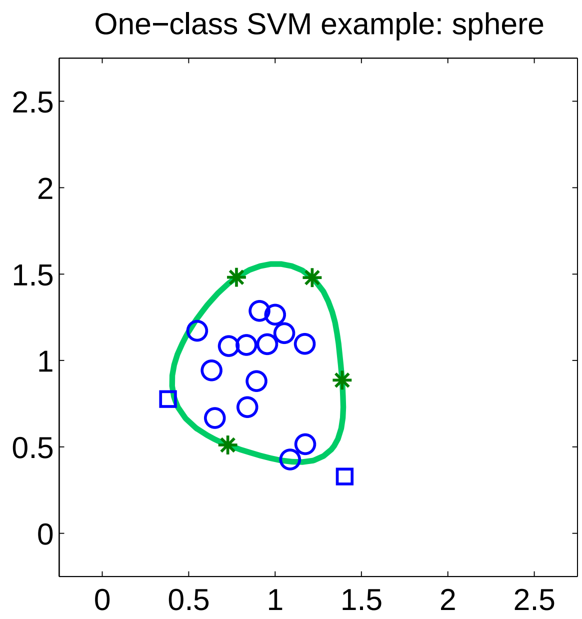


$$\begin{aligned} \min_{\mathbf{w},\xi,b} \quad & \frac{1}{2}||\mathbf{w}||^2 + \sum_{i=1}^{l} \xi_i - \nu\rho \\ \text{subject to} \quad & (\mathbf{w}\cdot\mathbf{x}_i) + b \geq \rho - \xi_i, \\ & \xi_i \geq 0. \end{aligned}$$

Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

One-class SVM: sphere formulation

The main idea of the sphere one-class SVM: fit a hypersphere around the data:

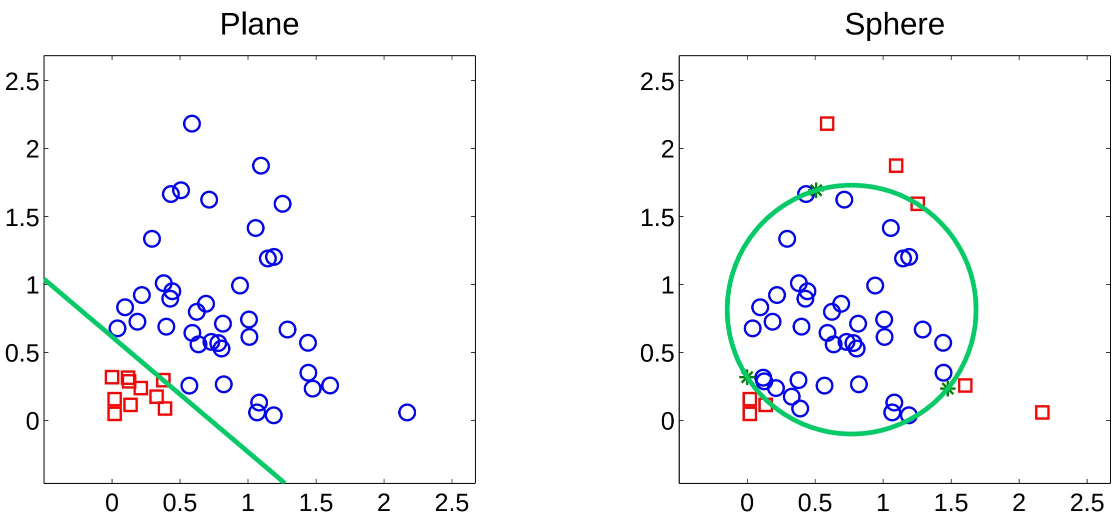


$$\min_{\mathbf{c},\xi,R^2} \quad R^2 + \frac{1}{\nu l}\sum_{i=1}^{l}\xi_i$$

$$\text{subject to} \quad ||\mathbf{c} - \mathbf{x}_i||^2 \le R^2 + \xi_i,$$
$$\xi_i \ge 0.$$

One-class SVM on non-negative data

Previous methods

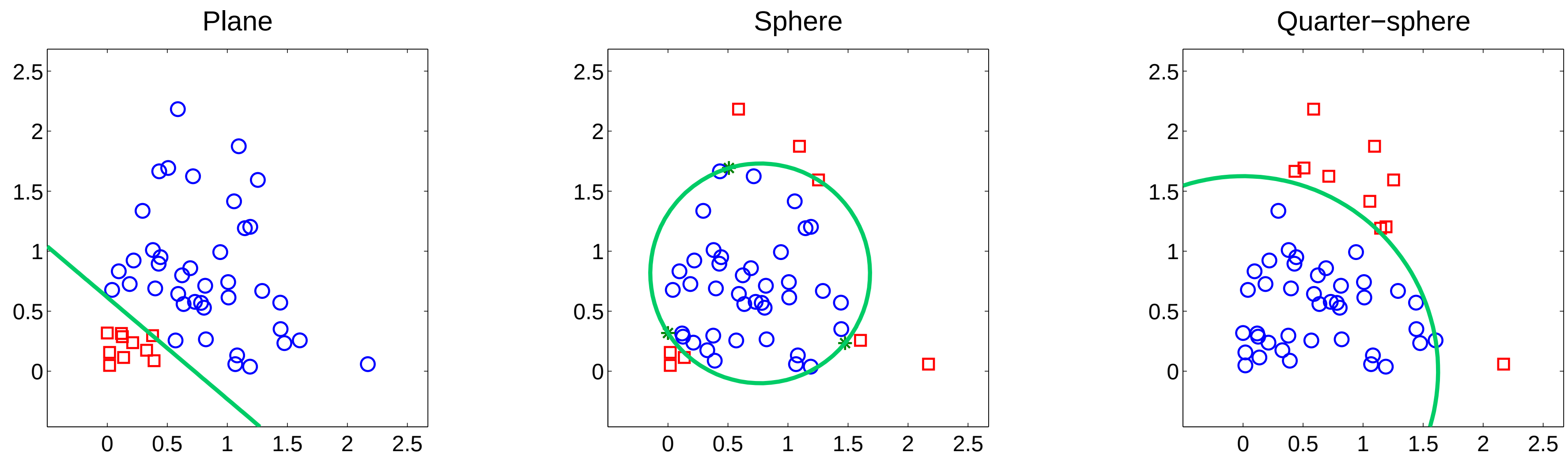


Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

One-class SVM on non-negative data

Previous methods

New method



Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

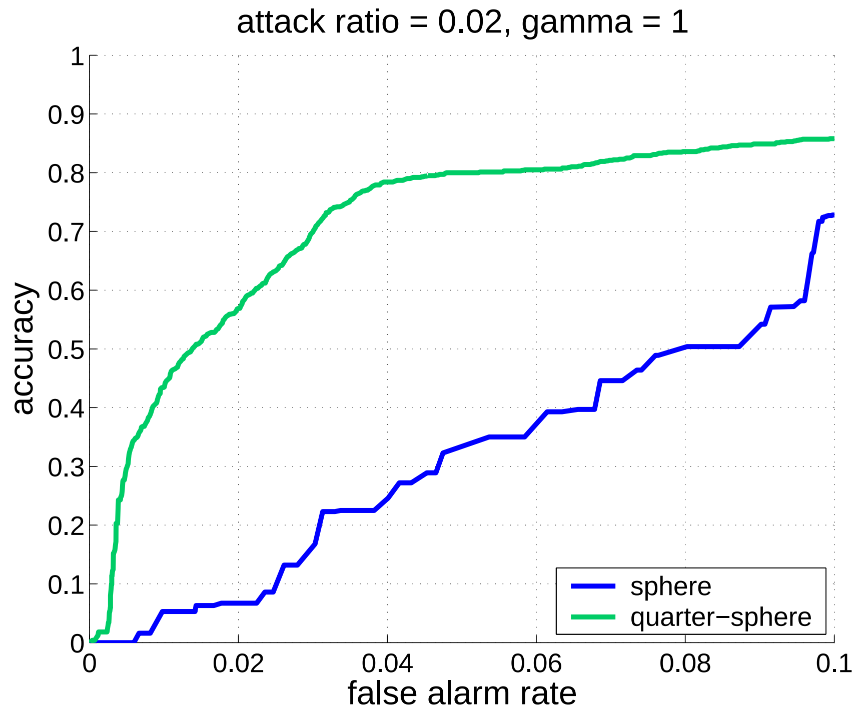
Quarter-sphere SVM: dual formulation

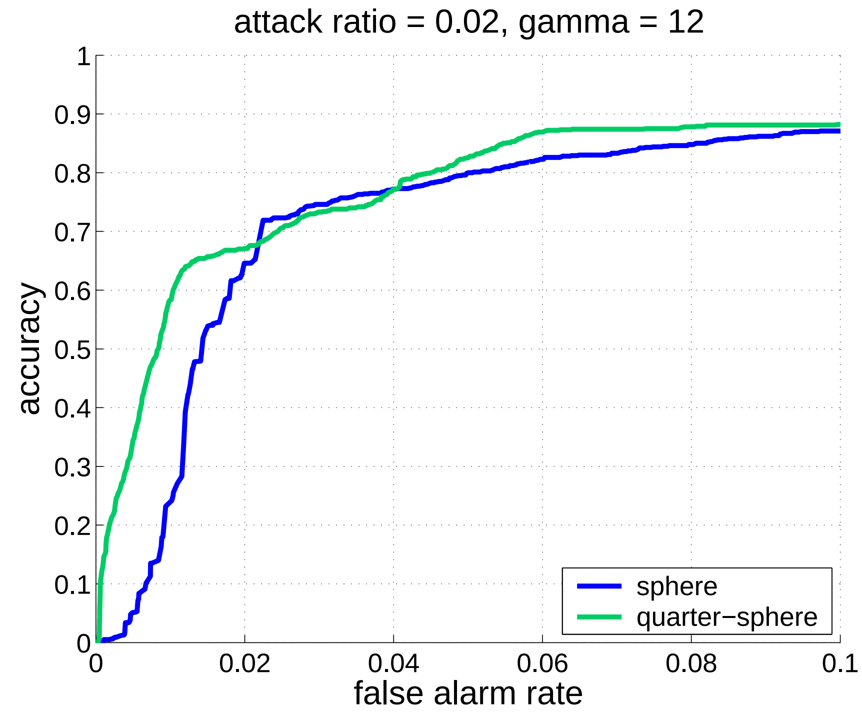
Algorithmically, the following *linear program* must be solved to apply a quarter-sphere SVM:

$$\begin{aligned} \max_{\boldsymbol{\alpha}} \quad & \sum_{i=1}^{l} \alpha_i \, \mathrm{k}(\mathbf{x}_i, \mathbf{x}_i), \\ \text{subject to} \quad & 0 \leq \alpha_i \leq C, \; i = 1, \ldots, l, \\ & \sum_{i=1}^{l} \alpha_i = 1. \end{aligned}$$

FIRST
Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

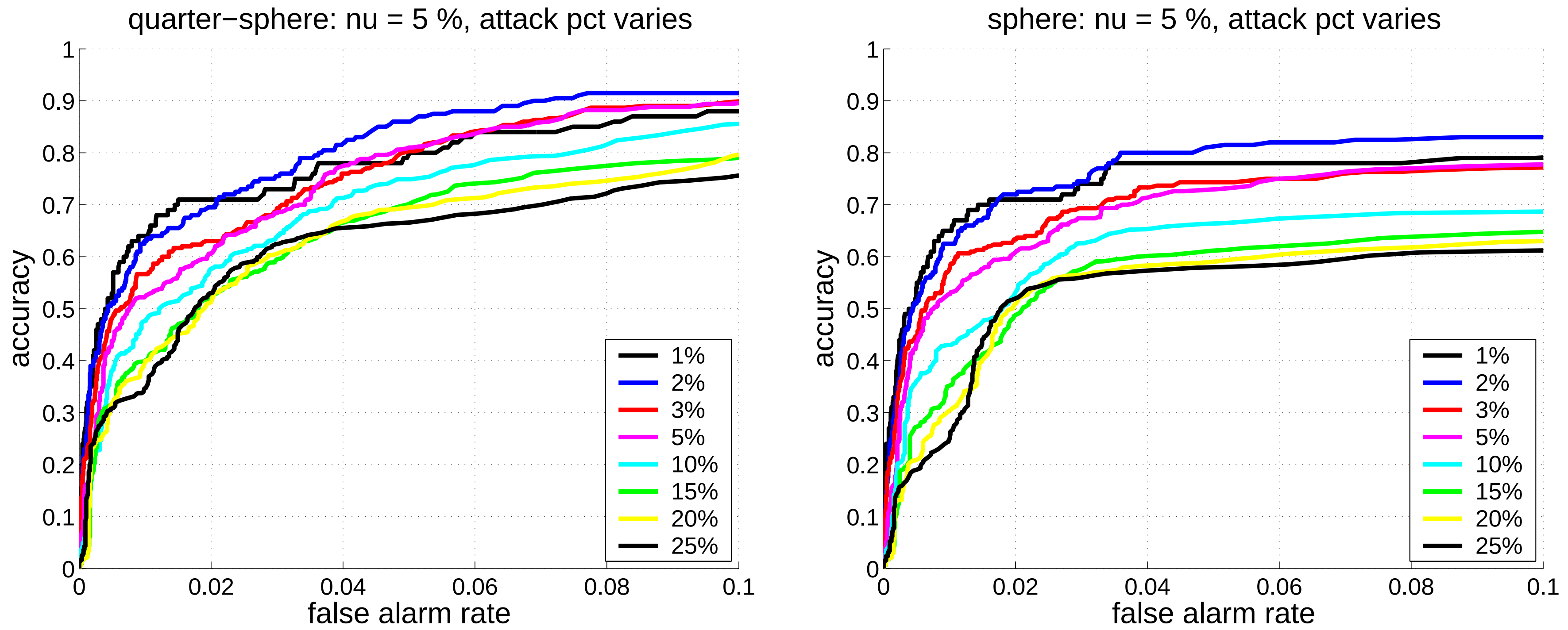
Results: Quarter-sphere vs. Sphere





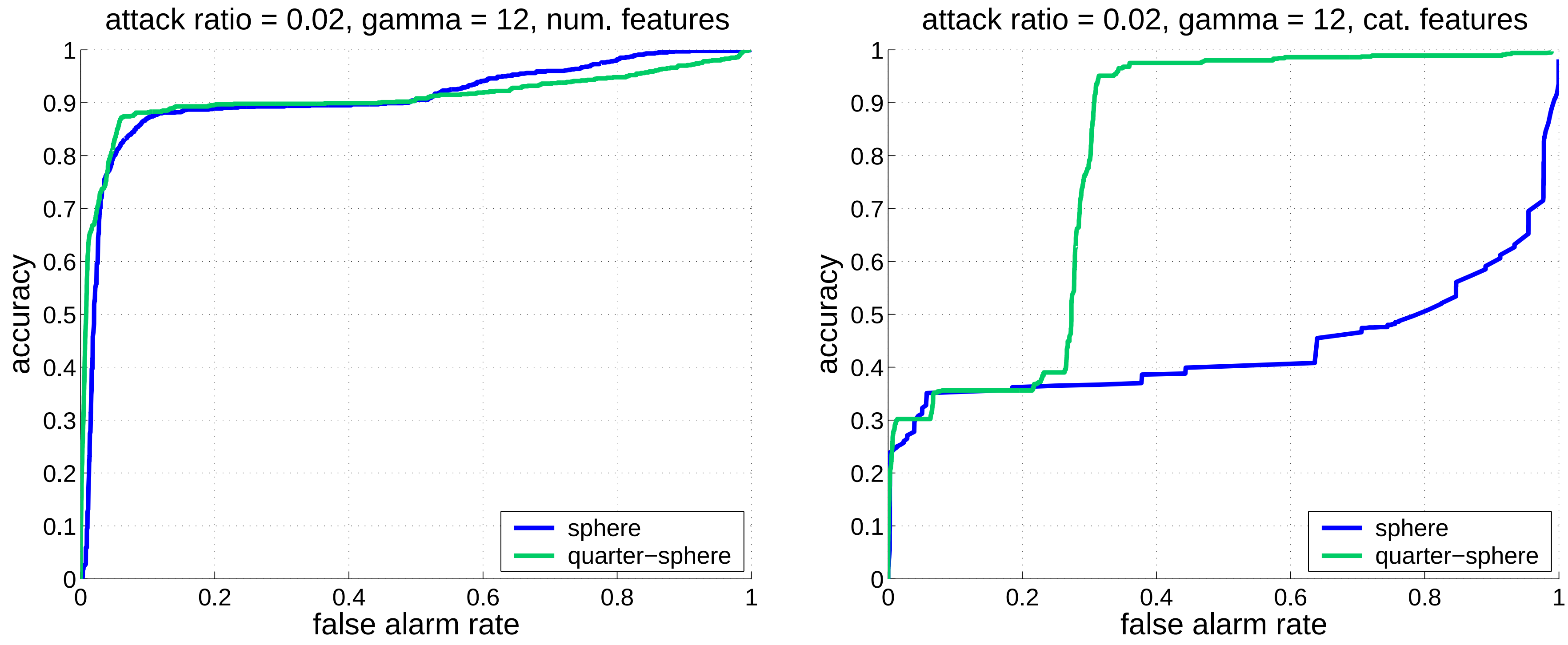
Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

Results: varying attack percentage



Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

Results: numerical vs. categorical features



Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

Conclusions

- Designing special-purpose anomaly detection techniques, suited for the data arising in IDS, can significantly decrease false alarm rates.
- What is most needed for the success of anomaly detection:
  - Precise understanding of *how* different mechanisms of anomaly detection work on the data arising in IDS.
  - Critical analysis with respect to *robustness*, i.e. operation under conditions that anomalies are not rare or their impact can significantly tilt the decision toward the anomaly.