

Detection of DoS attacks using a Naive Bayesian Classifier

Agenda

- Naive Bayesian Classifier
- Orange
- Testing
- Results
- Summary

Naive Bayesian Classifier

- Bayes Theorem
- Properties
 - Quick
 - Low resources
 - Large training set

$$\Pr(A|B) = \frac{\Pr(B|A) \Pr(A)}{\Pr(B)}.$$

Orange

- C++ basert
- Python scripts
- Orange widgets
 - Visual programming
 - Intuitive

Requirements

- Orange
 - Ease of use
 - Statistical output
- Success rate
 - 95%

Implementation

- Orange
- Dataset
 - MIT
 - Moonshine
 - Size: 30,000 (36%)
 - Size: 20,000 (1%)
- Attributes

Testing

- Test 1
 - Training: 70%
 - Classifying: 30%
- Test 2 and 3
 - Training: 50% and 10%
 - Classifying: 50% and 90%

Testing

- Test 4
 - Change of attributes
 - Training: 70%
 - Classifying: 30%

Testing

- Test 5
 - New set: 1% DoS
 - Training: 70%
 - Classifying: 30%
- Test 6
 - Training: 10%
 - Classifying: 90%

Results

- Test results
- Data set inaccuracy
- Lab vs. real world

Summary

- Naive bayesian classifier
- Orange
- Requirements
- Implementation
- Testing
- Results