An Integrated Framework for Optimizing Automatic Monitoring Systems in Large IT Infrastructures
Liang Tang, Tao Li, Larisa Shwartz, Florian Pinel, Genady Ya. Grabarnik
Florida International University, IBM Watson Research Center, St. John’s University

Introduction
Automatic Monitoring System: monitor those servers, notify the system administrator only when a problem happens.

How to Detect False Positives and False Negatives
False positive and false negatives are identified by system administrators and recorded in tickets (ground truth). Can the monitoring system learn from these tickets?

Configuration is Complicated

What is Misconfiguration?
• False Positive: A CPU utilization situation with 50% threshold on an intensive DB server (50% is normal for an intensive DB server, it is not a problem).
• False Negative: Installed a new web server, but forget to add it into the monitoring situation. If this web server has a problem, it would not be captured by the monitoring system.

Online Evaluation

Offline Evaluation

Our goal: eliminate false positives and false negatives

Labeled Domain Words (Labeled Features)