Anomaly Detection in Urban Sensor Networks
An approach for increased situational awareness

C. Brax (Saab) and M. Fredin (Saab)

Introduction

- More and more sensors are deployed in surveillance systems
- One goal with a surveillance system is to increase the situational awareness and find threats at an early stage
- Threats are hard to define and does not follow well defined doctrines
- Manual analysis of surveillance information can be hard
  - E.g. much information, boredom, inconsistent analysis, lack of experience, fatigue, etc.

→ Automated support for analyzing surveillance information is needed

Experimental System

- An anomaly detection system
- Integration of different modules

Scenario

A road block

Area of interest

Scenario used for evaluating the Tree Anomaly Detector

Locations of sensors

Results

- A simulation platform and a number of scenarios have been developed and used for a number of experiments
- Four different approaches for anomaly detection evaluated
  - Gaussian Anomaly Detector (detects anomalies in geographical areas)
  - SAX Anomaly Detector (detects anomalies in geographical areas)
  - Tree Anomaly Detector (detects anomalies in single object behavior)
  - Behavioral Anomaly Detector (detects anomalies in single object behavior)

Summary

- No significant difference in performance between using ground truth data and using data from a simulated sensor network
- The result of anomaly detection can be used directly to alert an operator as well as for input to other fusion systems such as ontological reasoning systems