Anomaly Detection in Urban Sensor Networks

An approach for increased situational awareness

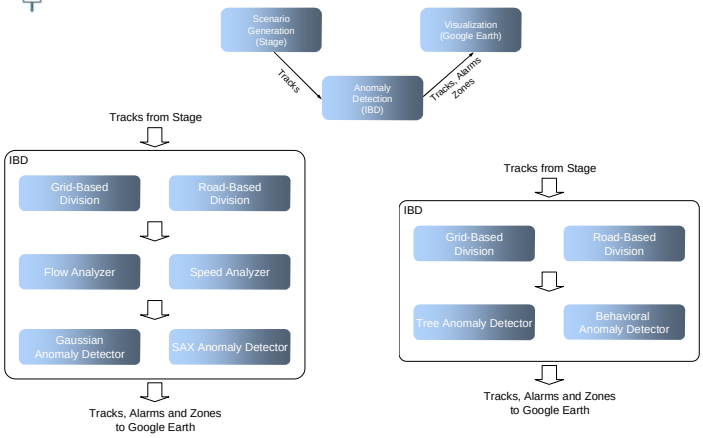
C. Brax (Saab) and M. Fredin (Saab)

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.

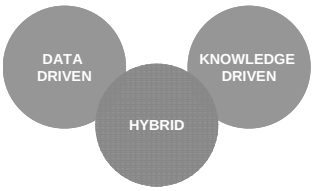
→ Automated support for analyzing surveillance information is needed

Experimental System

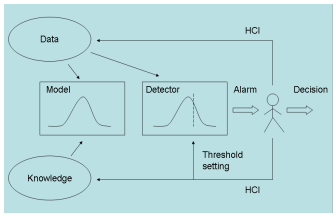


Anomaly Detection

- An approach for finding threats at an early stage
- Automatic analysis of the behavior of surveyed objects

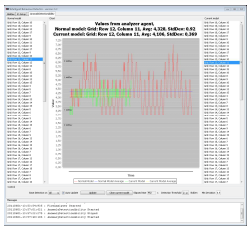


Different categories of detection mechanisms



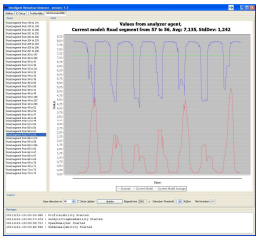
Anomaly detection concepts

Results

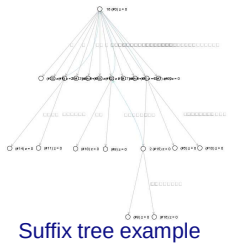


Gaussian Anomaly Detector

Output from the anomaly detection system



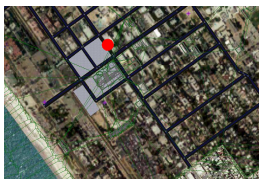
SAX Anomaly Detector



Suffix tree example

Scenario

Area of interest



A road block

Scenario used for evaluating the Tree Anomaly Detector

Locations of sensors

Summary

- 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)
    - Two types of division into geographical areas evaluated, using a linear grid and using contextual information about the road network
    - Two measures for traffic in a geographical area evaluated, average flow and average speed
    - Using road based division together with average flow or average speed gave best results
  - SAX Anomaly Detector (detects anomalies in geographic areas)
    - Uses a richer normal model
    - Can capture relative changes in traffic flows
    - Issues regarding pre-processing and threshold settings remains
  - Tree Anomaly Detector (detects anomalies in single object behavior)
    - Requires tracking of single objects
    - Evaluated based on a number of parameters on five scenarios
    - With the recommended parameter setup, the detector found four out of five scenarios with vehicles taking anomalous routes through the area-of-interest
    - Approach only evaluated in batch-mode, a method for on-line detection remains to be developed
  - Behavioral Anomaly Detector (detects anomalies in single object behavior)
    - The detector was able to find a number of typical behaviors in the data
    - These behaviors can be used for classification and anomaly detection
- 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

The R&T Project D-FUSE (Data Fusion in Urban Sensor Networks) is contracted by the European Defence Agency on behalf of Members States contributing to the Joint Investment Programme on Force Protection

For information contact: christoffer.brax@saabgroup.com