A Distributed Scheme of A Dynamic Entropy Based Method for Early Detection of Anomalous States in Sensor Network

A.A. Waskita, L.T. Handoko, H. Suhartanto

October 7, 2015

Agenda

Introduction

Model

Experiments

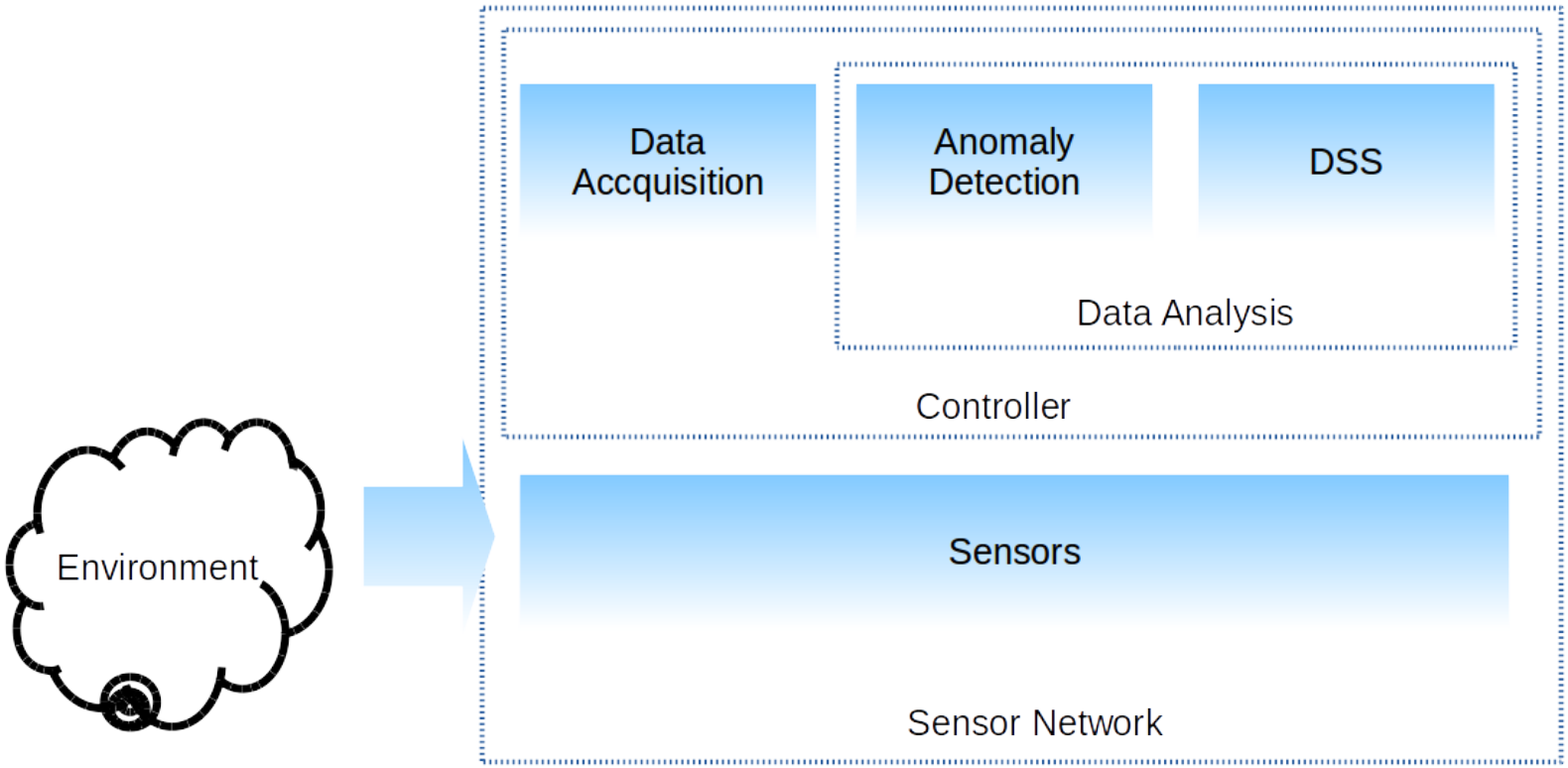
Conclusions

Further works

Agenda

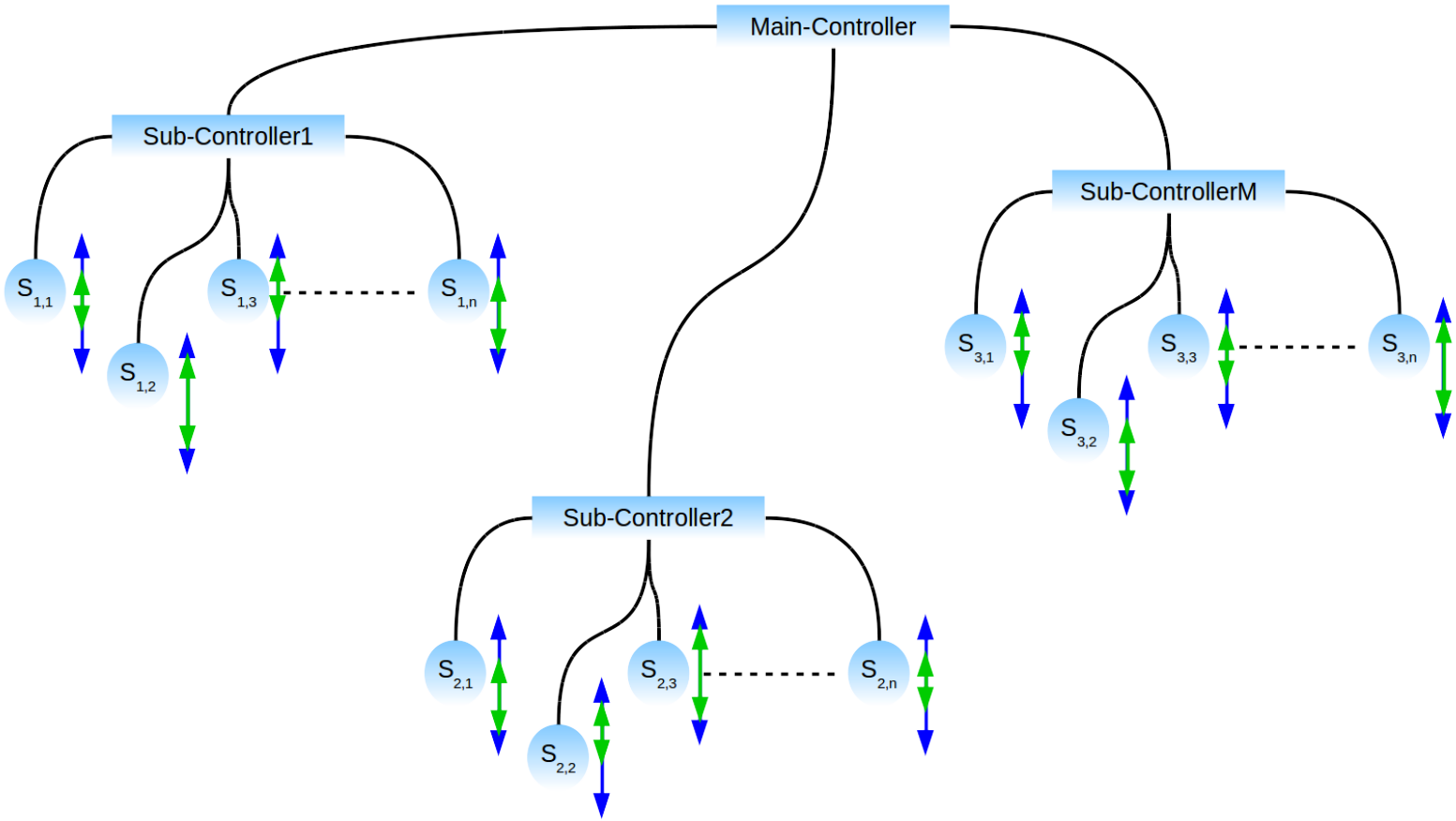
Backgroud

To keep a system performance, it is important to implement a monitoring system which is able to detect any anomalous state of a system



A monitoring System

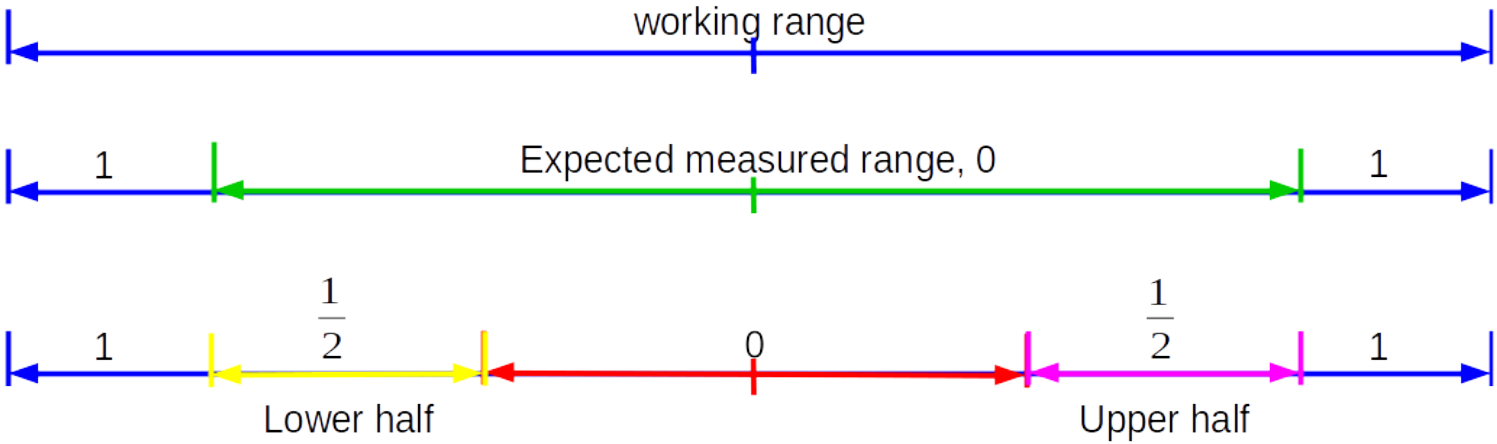
A monitoring system is a network of (though not necessarily) clusters of homogeneous or hybrid sensor, each with their operational specification



Operational Specification

An operational specification is a combination of

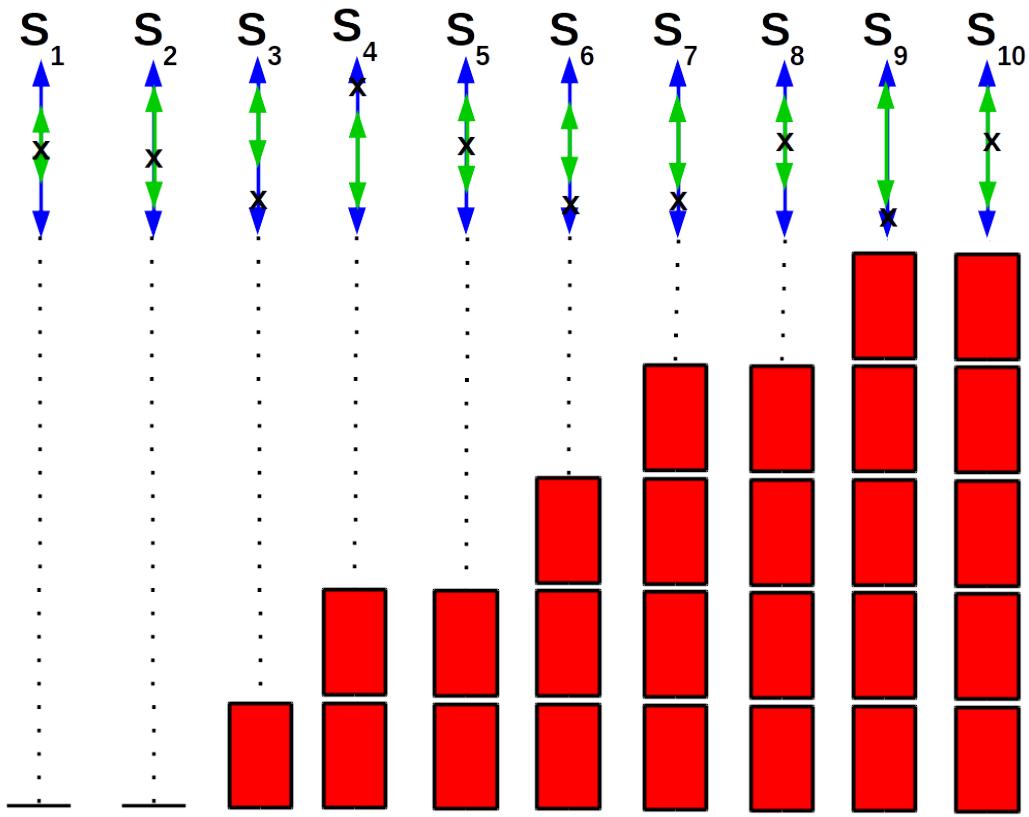
- a working range of each sensor involved and
- system design specification range where a sensor is placed $\rightarrow$ coded as 0 if it meet the specification, 1 if not



Agenda

Entrophy

- The acquisition value of each sensor in the format of the cumulative value formed a specific pattern
- A specific pattern shows irregularities of a system based on its specification



Entrophy

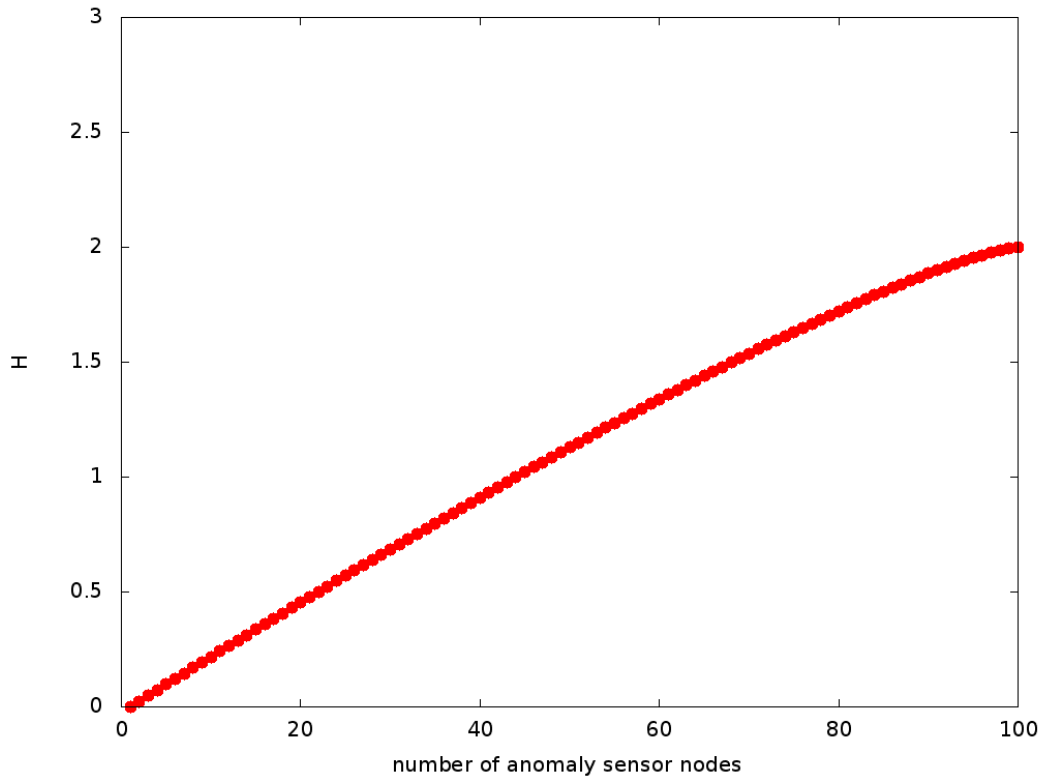
$$H = -\sum_{k=1}^{K} p_k \log(p_k) \tag{1}$$

For a case of previous figure

- Number of different accumulated state, K=6, each are 0, 1, 2, 3, 4, 5
- Number of each accumulated state are 2, 1, 2, 1, 2, 2
- Probability of each accumulated state, pk are 0.2, 0.1, 0.2, 0.1, 0.2, 0.2
- Entropy for a case in previous figure = 0.76

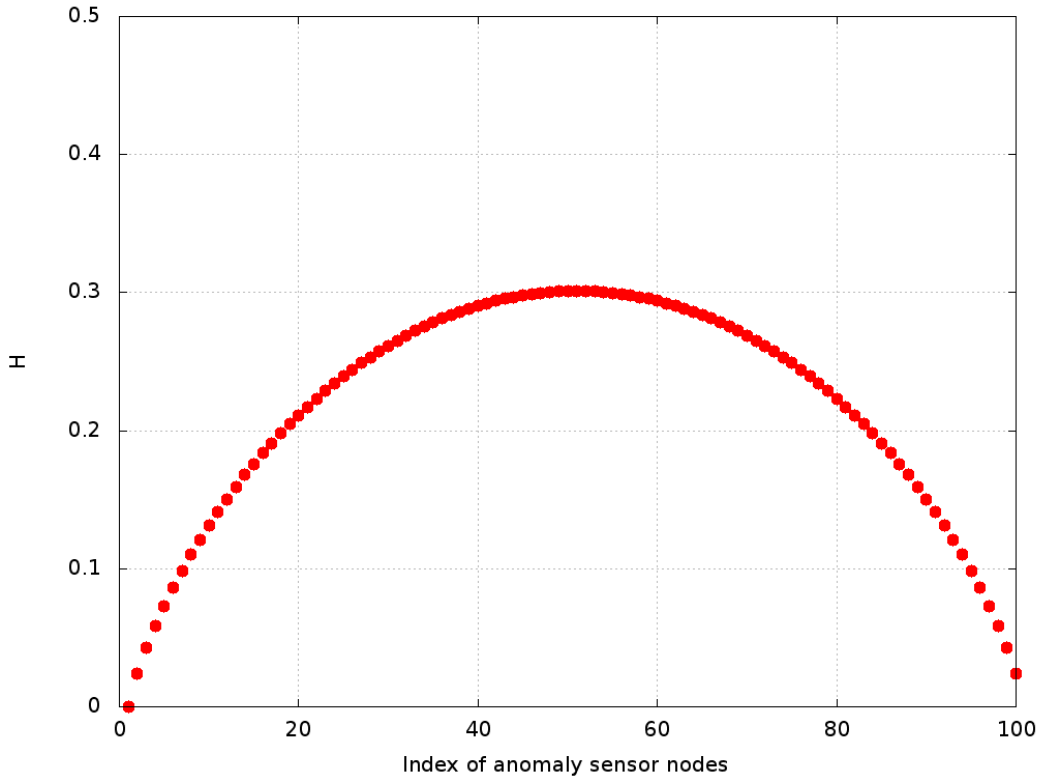
Agenda

Entropy based model characteristics



The more anomalous state sensor, the greater entrophy

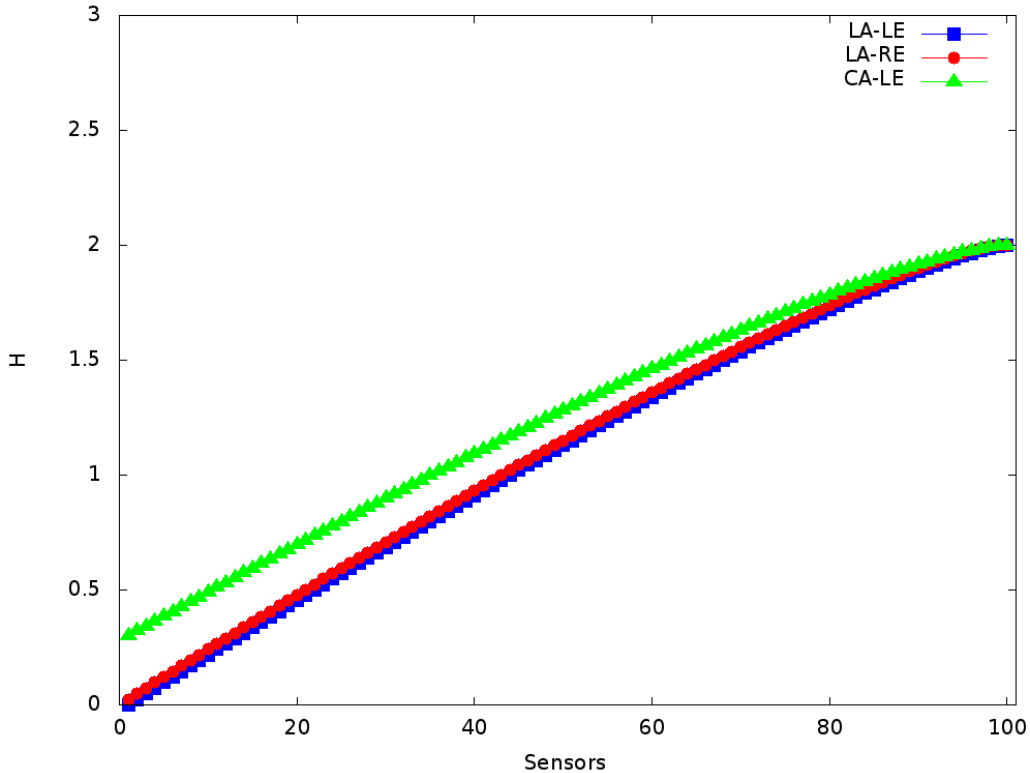
Entropy based model characteristics



The differences in position of anomalous sensor resulted in differences in the value of entrophy $\rightarrow$ it is better to

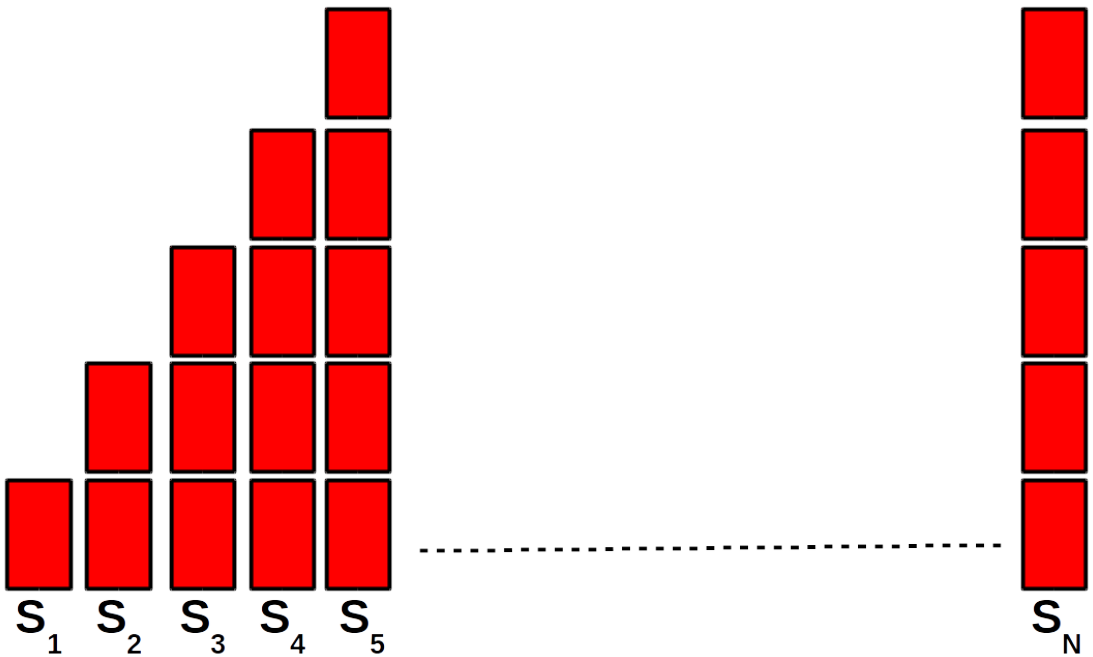
- put the more critical sensor in the middle of the sensor index
- separate the more critical sensors in different cluster

Entropy based model characteristics



The number of anomalous state sensor and the startng point of evaluation resulted different value of entrophy

Entropy based model characteristics



Total sensor	Entropy
10	0.53
20	0.34
50	0.17
100	0.10

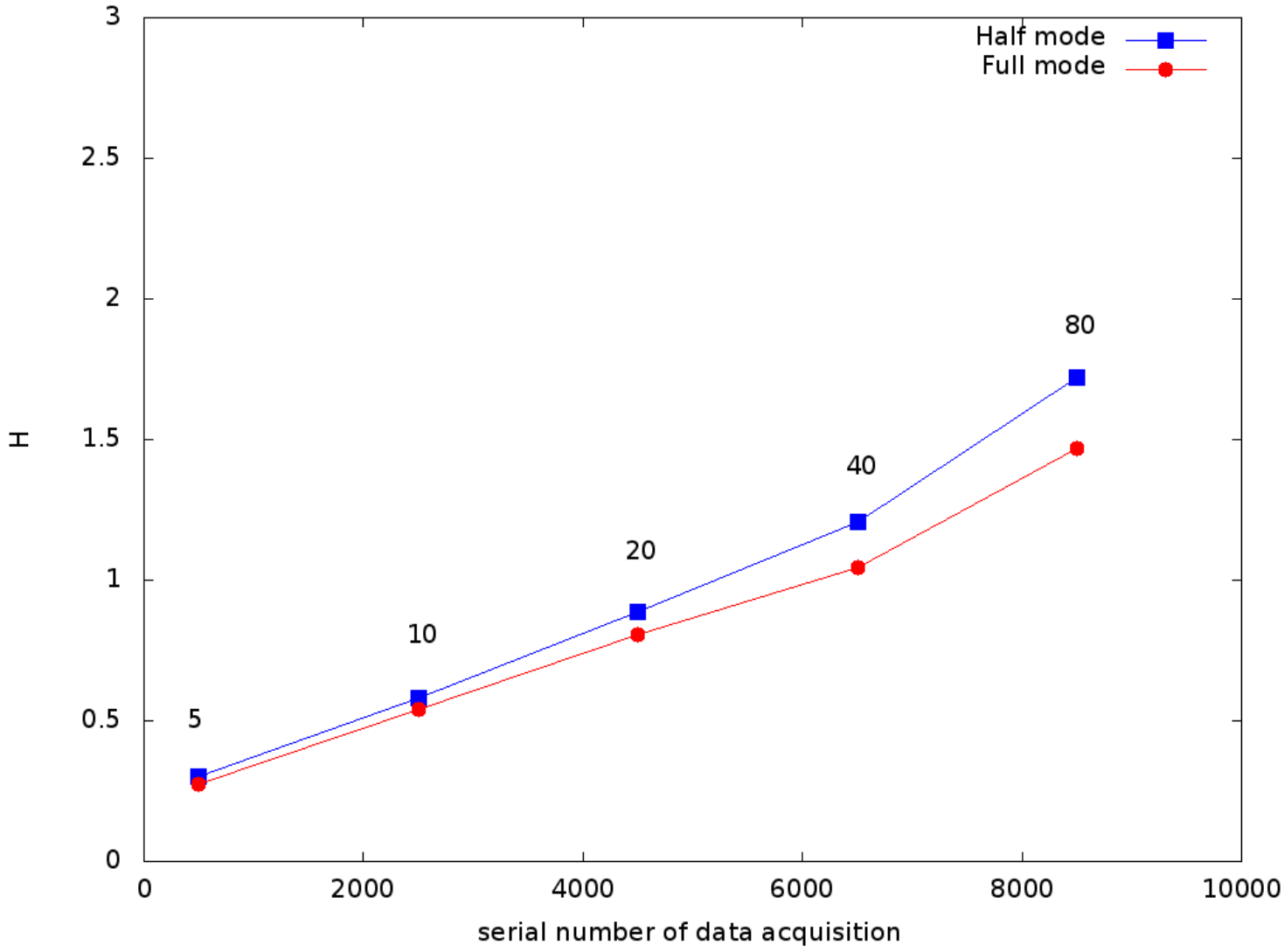
Data set

- Defines involving sensors, each with their operational characteristics $\rightarrow$ 100 sensors & 4 clusters involved (@25 sensors in each cluster)
- Create accquisition value for each sensor in a range of expected measurement randomly for a number of accquisitions phase
- Each accquisition was assumed to be made evary certain minutes, which is longer than time needed to communicate a physical parameter between sensors and controller
- Create some accquisition value in the outside of expected measurement to simulate anomalous state of a sensor network, either full or half mode
  - ✓ Full mode, state of a sensor is divided into 2, a normal and anomalous state
  - ✓ Half mode, a nomal state of a sensor is divided into 2, each with 0 and 0.5 encoding number

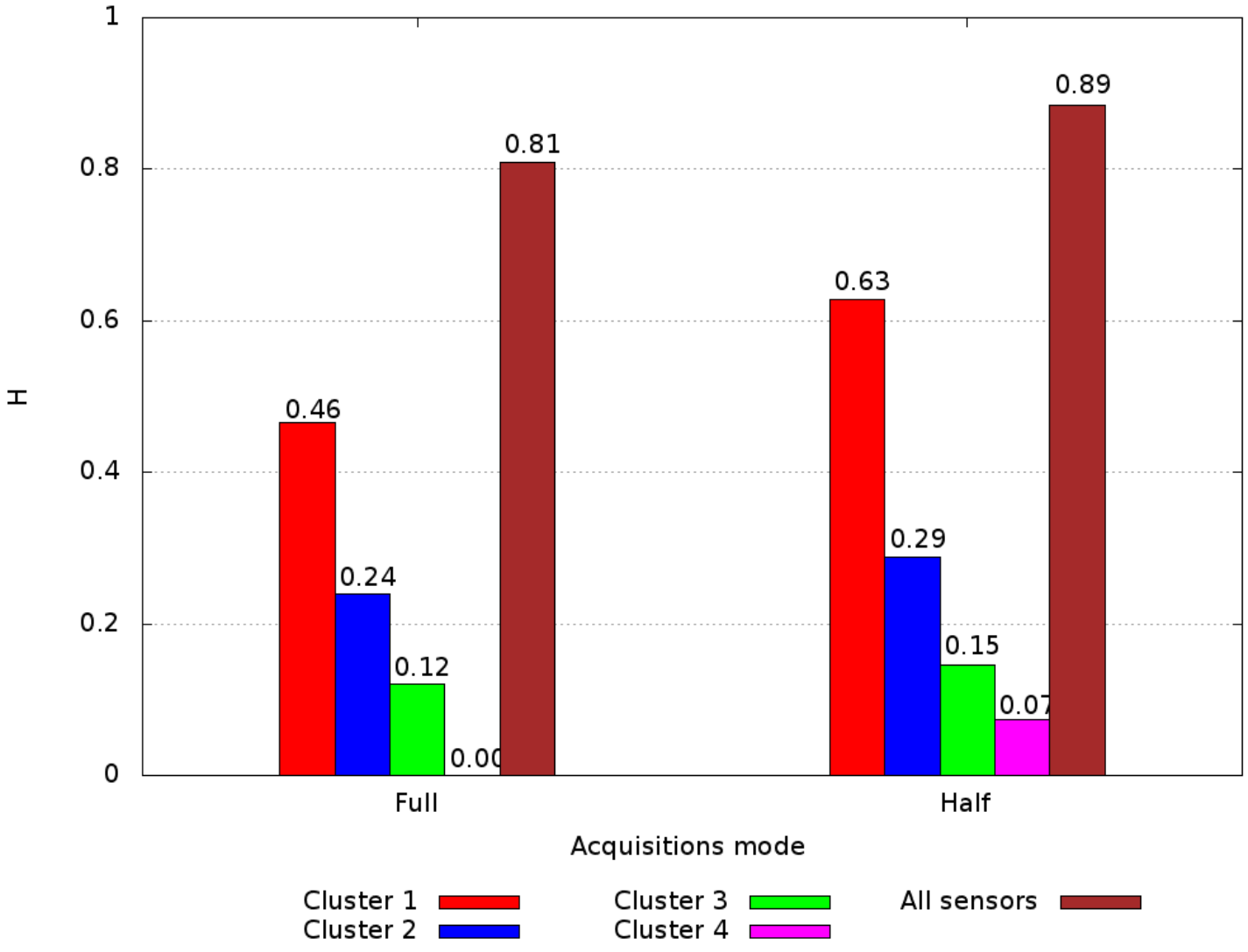
Data set

# of acc	Cluster1	Cluster2	Cluster3	Cluster4
1	3	2	0	0
2	5	3	2	0
3	10	5	3	2
4	20	10	6	4
5	25	25	25	5

From a data set



From a data set



Agenda

Conclusions

- An anomalous sensor in a middle of the index will resulting higher entropy than if the sensors are the edge
- A more critical sensor should be placed in the middle index to provide more sensitivity
- It is better to separate a more critical sensors to a different cluster than to combine them with the less critical one
- Total entropy which is obtained from clusters is larger than from a single network
- Entropy is larger for a half mode than a full mode because of more anomalous state detected

Agenda

Further works

- Compare this entropy based method to other similar one
- Develop a decission support system that involving this anomaly detection approach to a certain case


Thank you for your attention