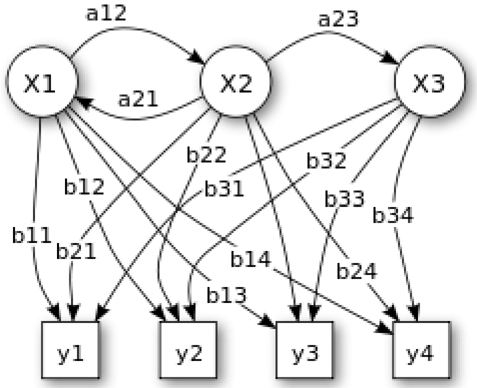
Markov Models

Applied to Anomaly Detection

By Saab Group

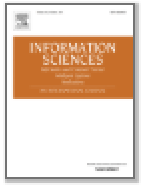


The paper

ELSEVIER

Information Sciences

Volume 411, October 2017, Pages 52-65



Anomaly detection based on a dynamic Markov model

Huorong Ren [a, b], Zhixing Ye [a, b], Zhiwu Li [c, a]

Show more

https://doi.org/10.1016/j.ins.2017.05.021

Get rights and content

THE HAGUE
UNIVERSITY OF
APPLIED SCIENCES

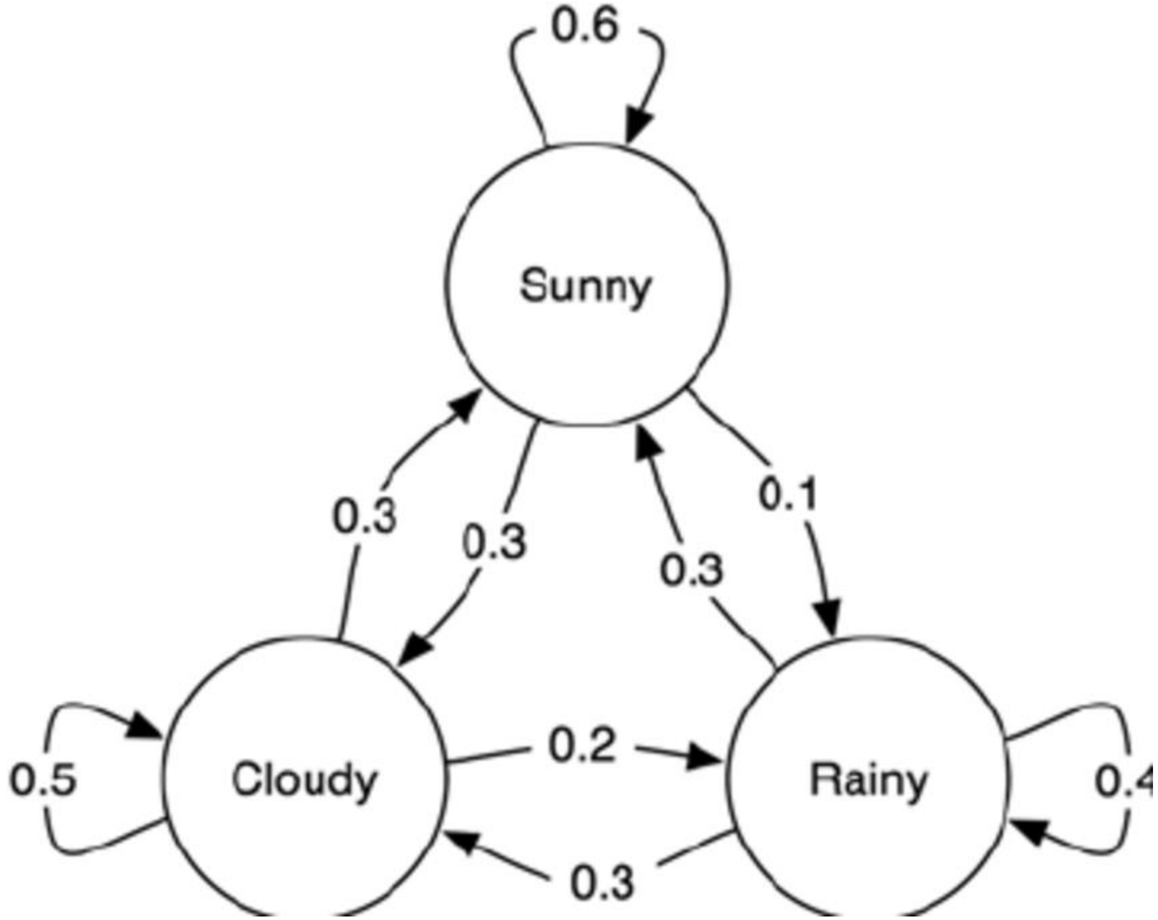
What is a Markov Model?

- In probability theory, a Markov model is a stochastic model **used to model randomly changing systems**.

- It is assumed that **future states depend only on the current state**, not on the events that occurred before it (that is, it assumes the Markov property).

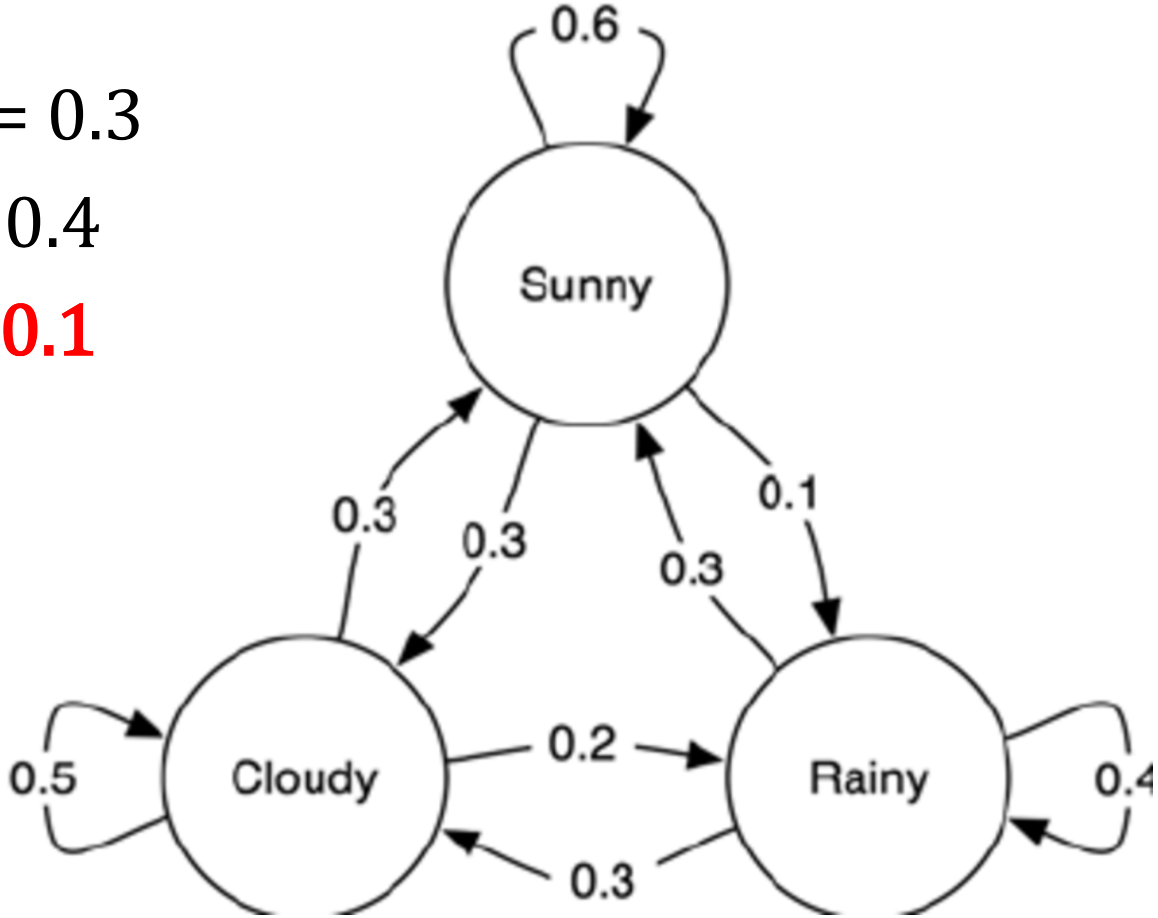
What is a Markov Model?

What is a Markov Model?



Why is this helpful in anomaly detection?

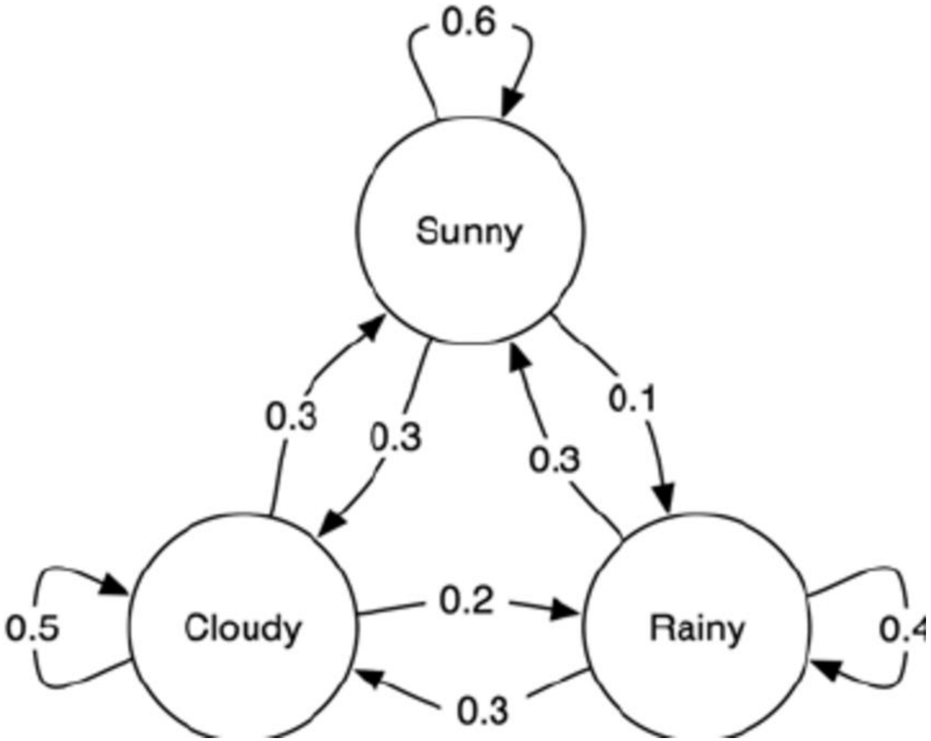
- P(sunny|cloudy) = 0.3
- P(rainy | rainy) = 0.4
- P(rainy|sunny) = **0.1**



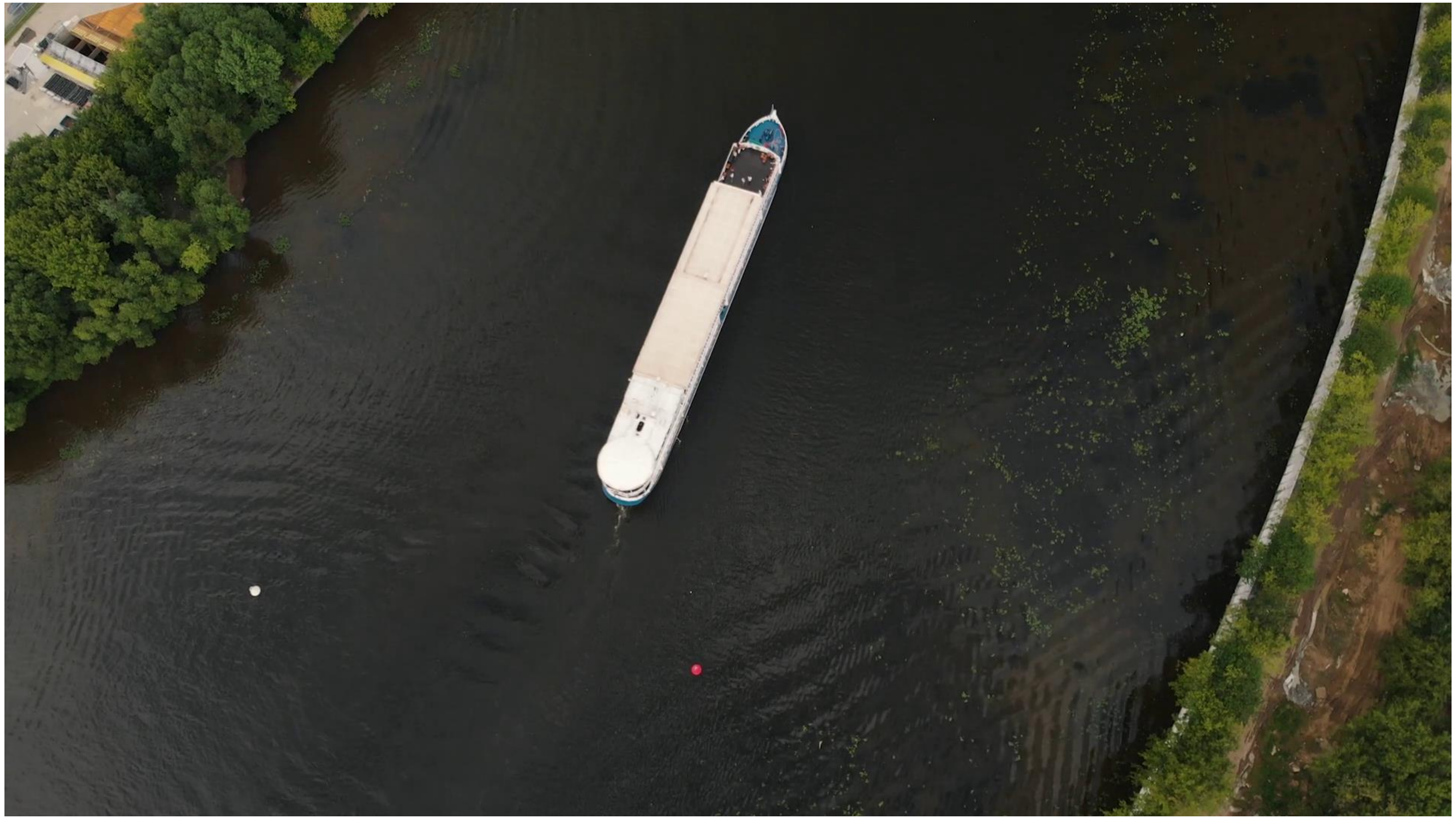
Why is this helpful in anomaly detection?

- P(sunny|cloudy) = 0.3
- P(rainy | rainy) = 0.4
- P(cloudy|sunny) = **0.1**

ANOMALY
DETECTED

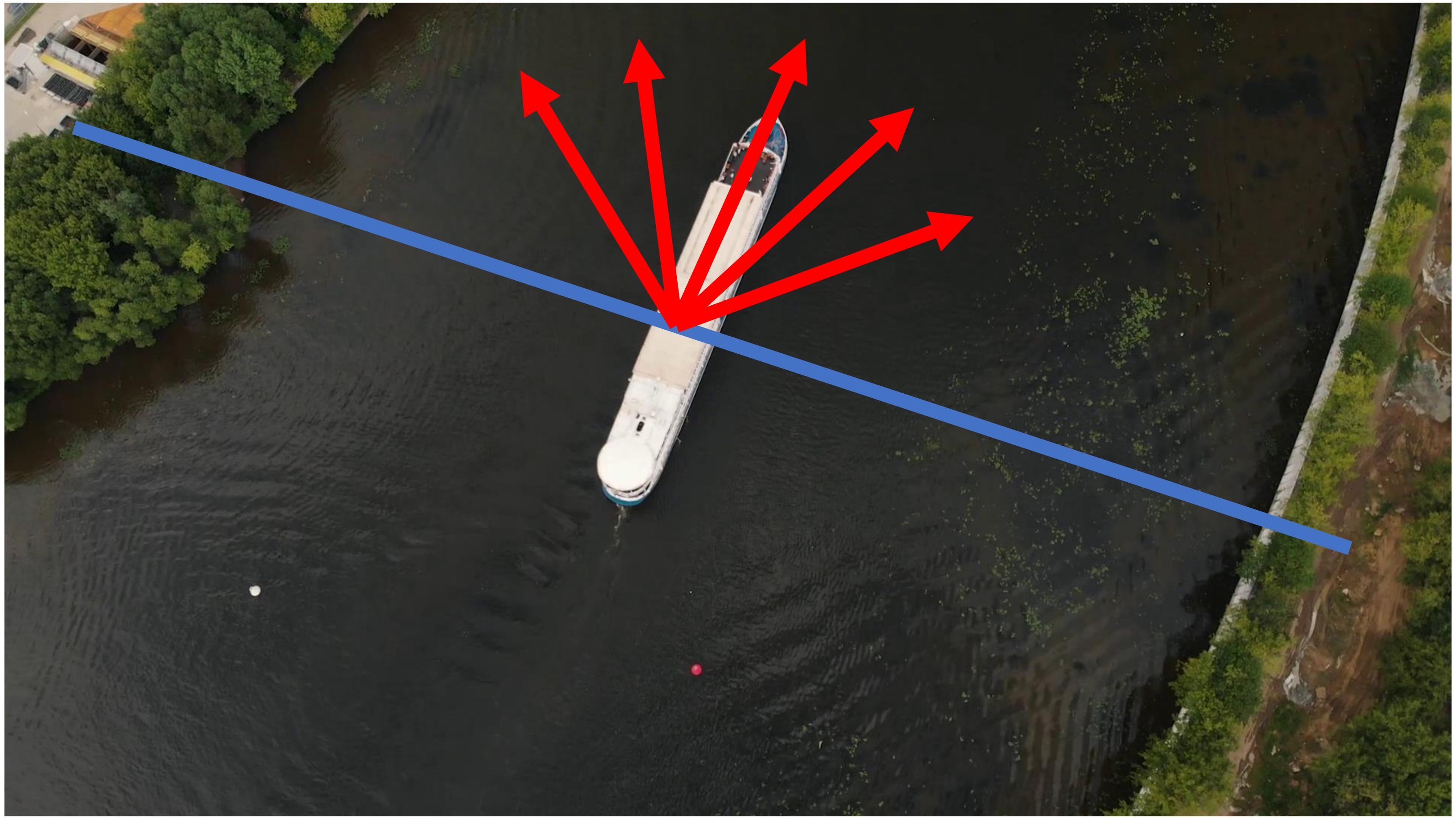


Why can this be applied to our Project?

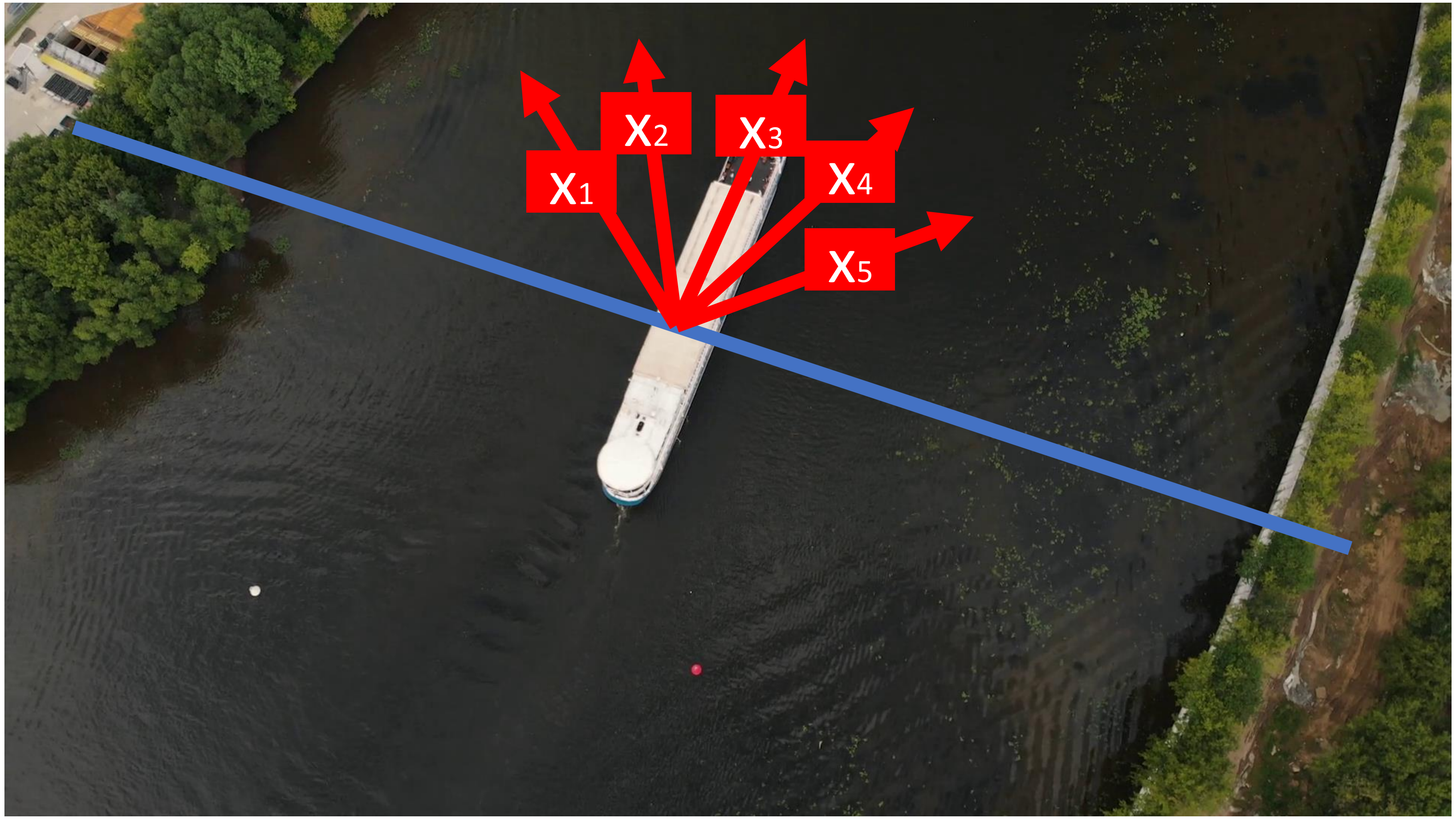


Why can this be applied to our Project?

Why can this be applied to our Project?

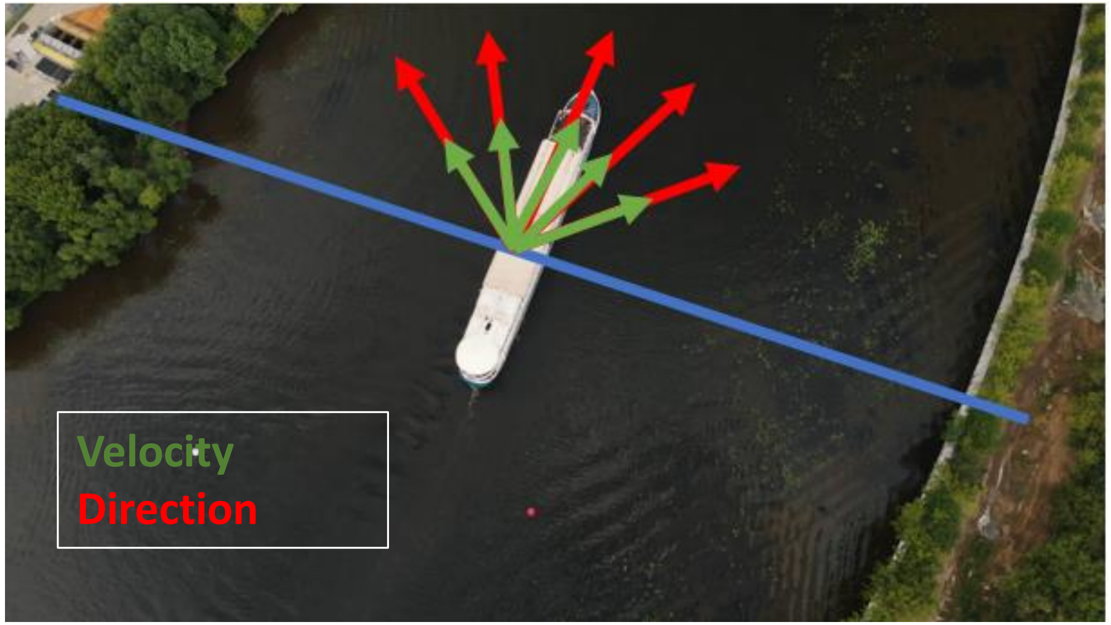


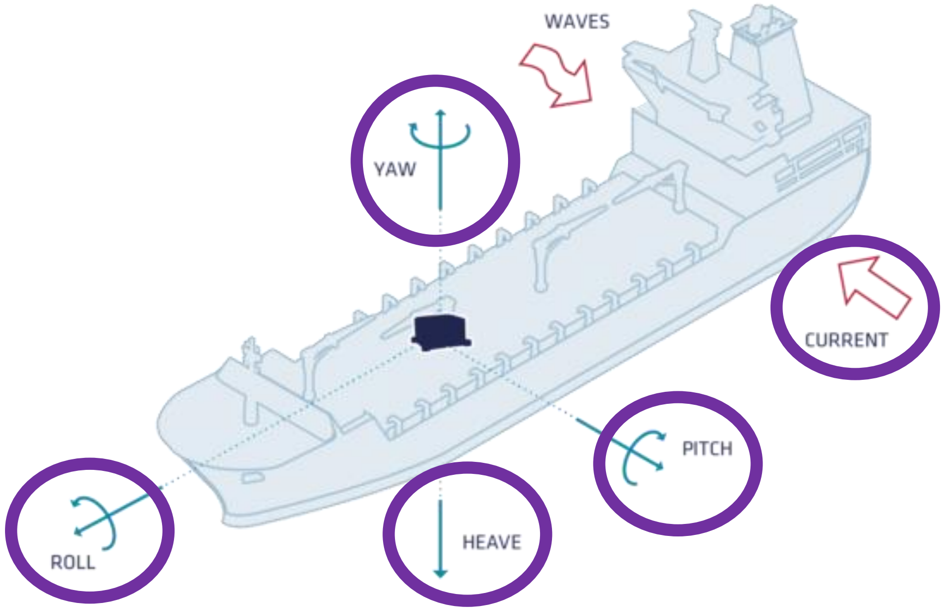
Why can this be applied to our Project?



Transitions

And… if we have other interesting features?





Since all measurements are bounded

- We can partitionate them and classify them
- E.g:

So what's the average speed of a sailboat? **Most sailboats cruise at a speed of 4-6 knots (4.5-7 mph), with a top speed of 7 knots (8 mph or 13 km/h). Larger racing yachts can easily reach speeds up to 15 knots (17 mph or 28 km/h), with an average cruising speed between 6-8 knots (7-9 mph). Cruising speeds of over 8 knots are uncommon.**

Since all measurements are bounded

- We can partitionate them and classify them
- E.g:

So what's the average speed of a sailboat? **Most sailboats cruise at a speed of 4-6 knots (4.5-7 mph), with a top speed of 7 knots (8 mph or 13 km/h). Larger racing yachts can easily reach speeds up to 15 knots (17 mph or 28 km/h), with an average cruising speed between 6-8 knots (7-9 mph). Cruising speeds of over 8 knots are uncommon.**

0 km/h

30 km/h

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Since all measurements are bounded

- We can partitionate them and classify them
- E.g:

So what's the average speed of a sailboat? **Most sailboats cruise at a speed of 4-6 knots (4.5-7 mph), with a top speed of 7 knots (8 mph or 13 km/h). Larger racing yachts can easily reach speeds up to 15 knots (17 mph or 28 km/h), with an average cruising speed between 6-8 knots (7-9 mph). Cruising speeds of over 8 knots are uncommon.**

0 km/h

30 km/h

slow

normal

fast

Since all measurements are bounded

- We can partitionate them and classify them.

- Now each classification is a substate of the measurement, so that for speed we have both slow, normal and fast sub-states.

- Position could be partitioned into **suspicious** and **non-suspicious** according to the history of anomalies detected in a certain port.

- The direction can also be partitioned(we Will see it in the following slides).

Since all measurements are bounded

- So if we use in out model 3 states representing the speed, 2 states representing the position and 5 states representing the direction, there Will be:

$$\binom{10}{3} = 120\ states$$

Since all measurements are bounded

- So if we use in out model 3 states representing the speed, 2 states representing the position and 5 states representing the direction, there Will be:

$$\binom{10}{3} = 120\ states$$

- **This might be too much (or not)**

?

More Data

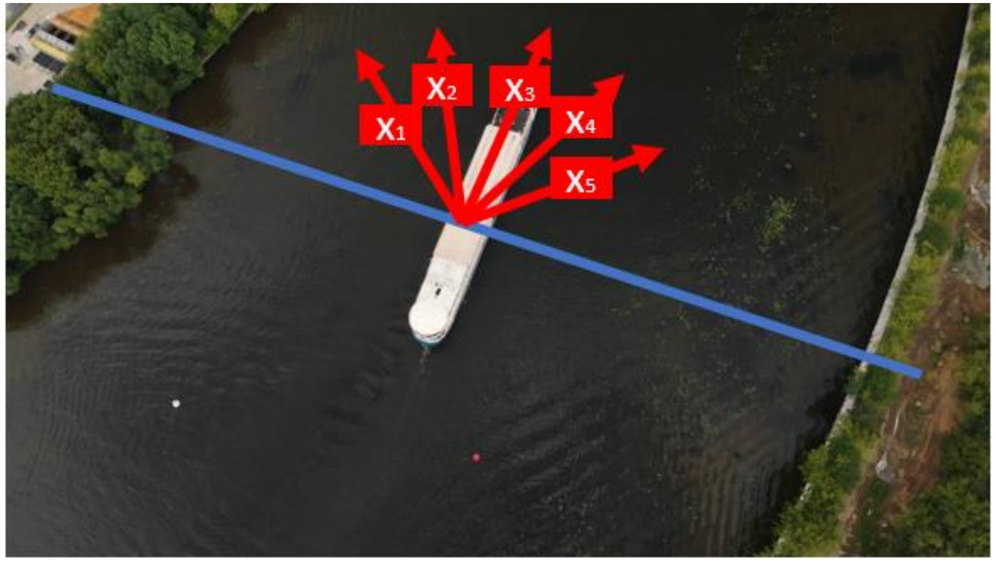
=

More information
per state

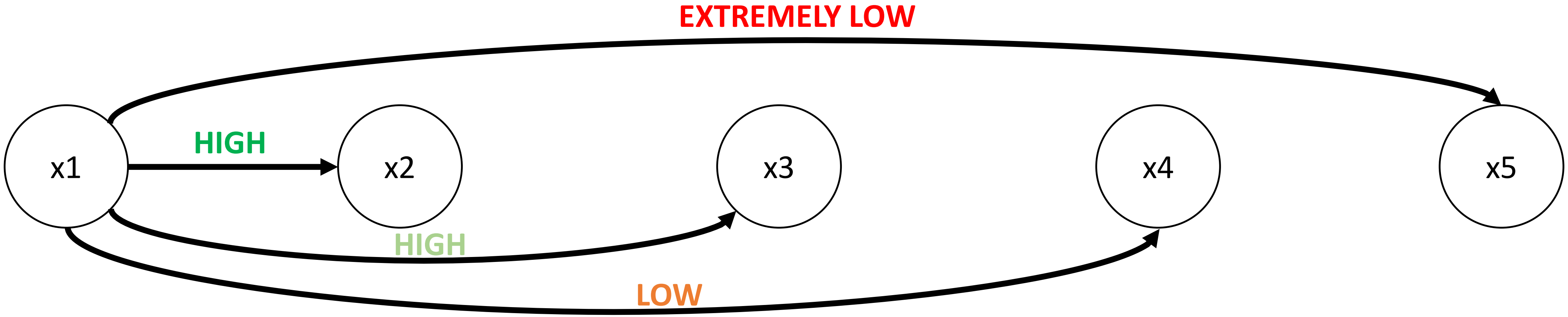
An example focusing only in direction

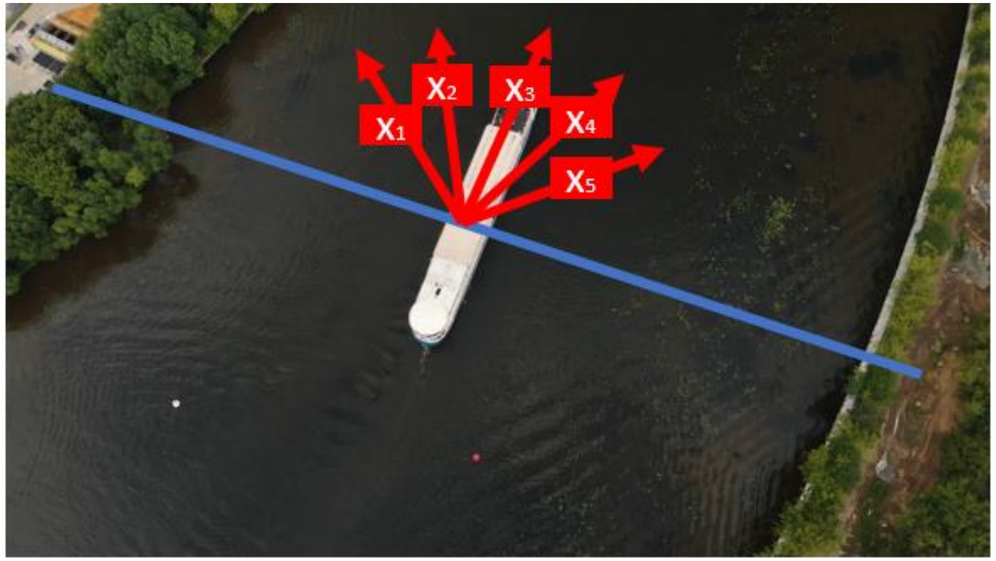
- We can extract much more features (depends on the data)

x1 x2 x3 x4 x5



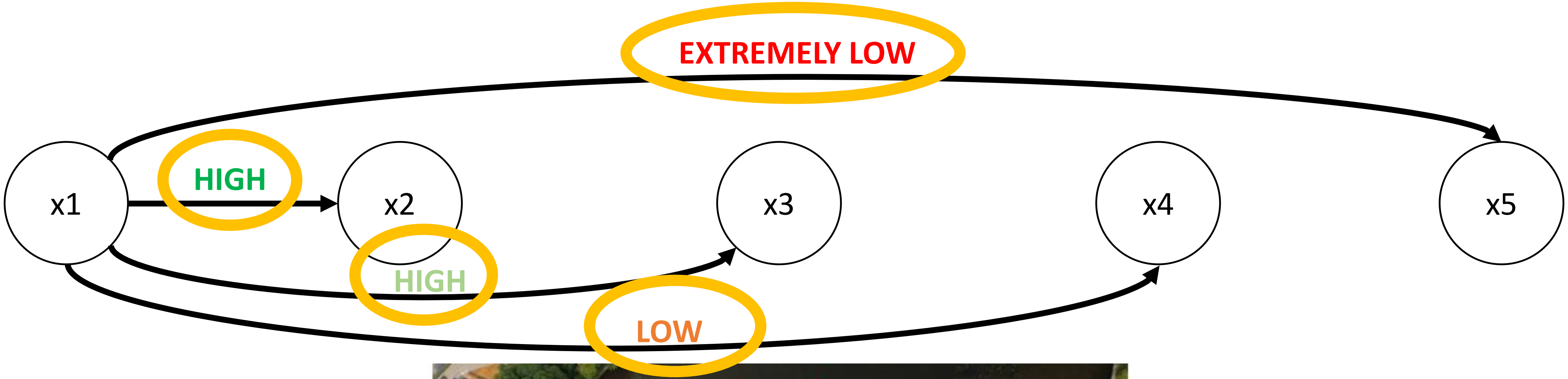
Basic Model

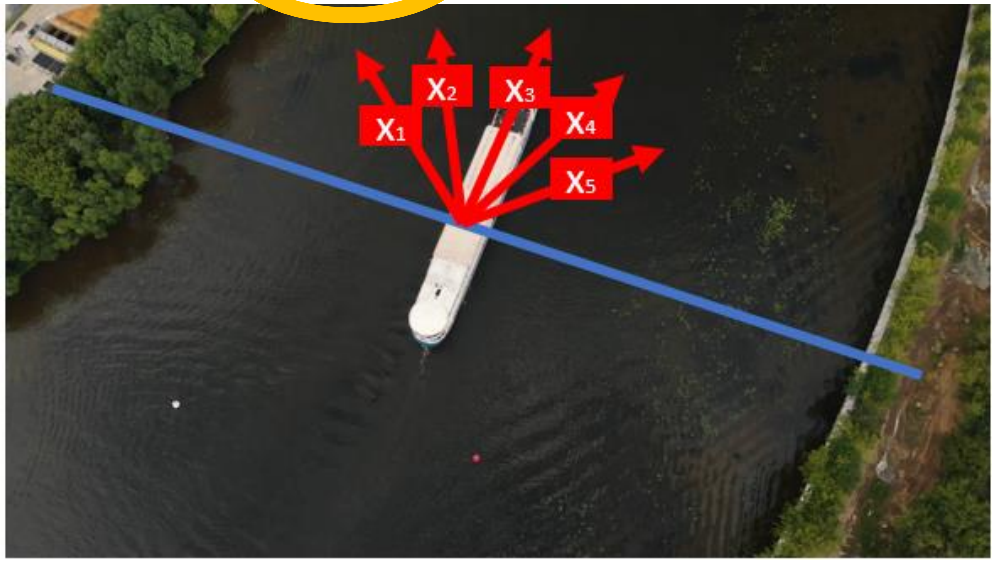




Basic Model

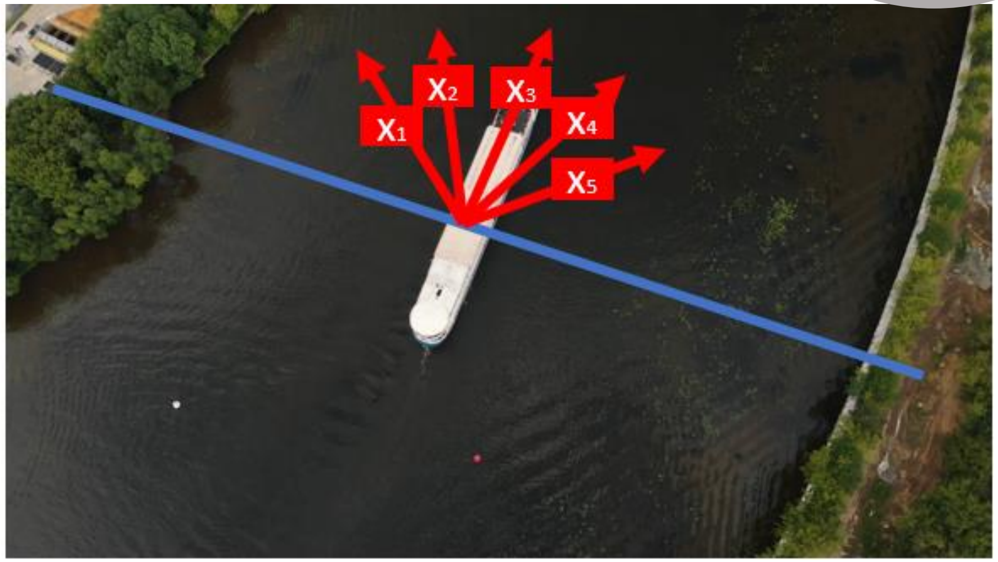
What could we extract from the





Basic Model

Finally...



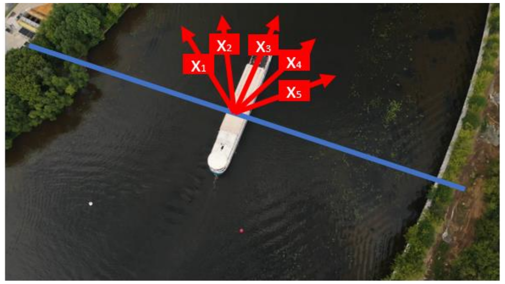
If there is a transition from x1 to x5:

WE ARE JUST IN FRONT OF AN

Implementation

Finally...

Once defined the states, we can compute probabilities of transition between one state to another and represent them on a matrix



Transition Probability Matrix

$$\begin{array}{cc} & \begin{array}{cccc} 1 & 2 & \cdots & n \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ \vdots \\ m \end{array} & \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \end{array}$$

a_{ij} = Probability of transition from i to j

Idea:

- Get the probability values from a training set
- Evaluate the model with the test set
  - Whenever a transition happen, check the probability of that to have ocurred and if it is under a tested threshold → ANOMALY

Also Interesting

- **Problem**
  - Speed and size of the ships should get evaluated in conjunction.
    - Higher speeds are supossed to be adopted by smaller ships
    - High speeds are not anomalous for big ships
- **Markov Models allow us to evaluate speed and length together**
  - Given a range of posible values for speed and length, we can partitionate both so that given a **transition pair**

(speed1, length)→ (speed1, length)

Initially: (100km/h, 500m) → → (type 7, type 5) → STATE 4

Finally: (20 km/h, 500m) → → (type 4, type 5) → STATE 7

SO

STATE 4 to STATE 7

THE HAGUE
UNIVERSITY OF
APPLIED SCIENCES