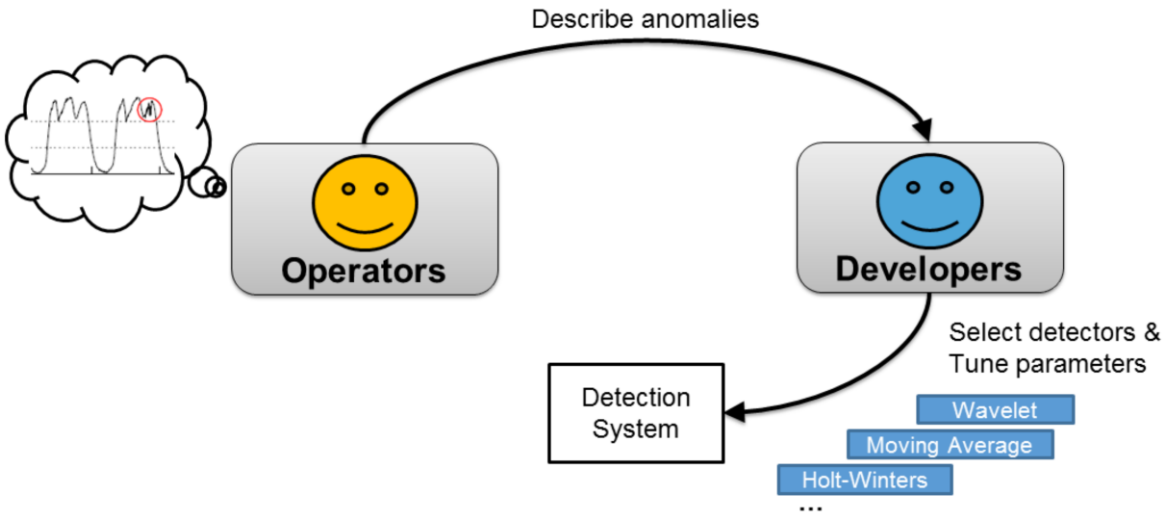
How to Build the Anomaly Detection System

In practice, it is more complex

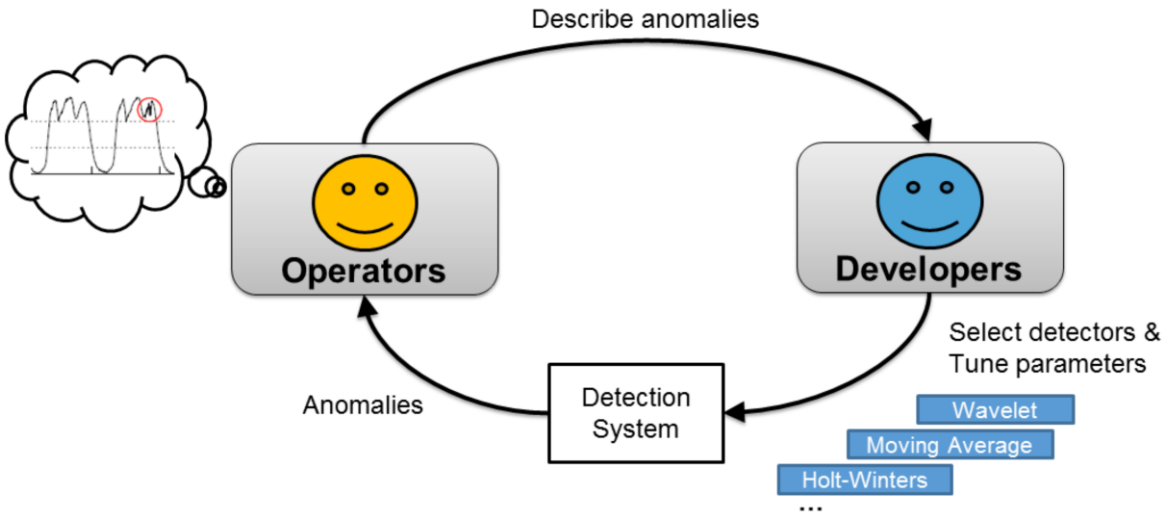


Then, to detect those anomalies, developers have to select suitable detectors and tune their internal parameters.

Sometimes, one detector is not sufficient enough, and they have to combine multiple detectors such as using majority-vote.

How to Build the Anomaly Detection System

In practice, it is more complex



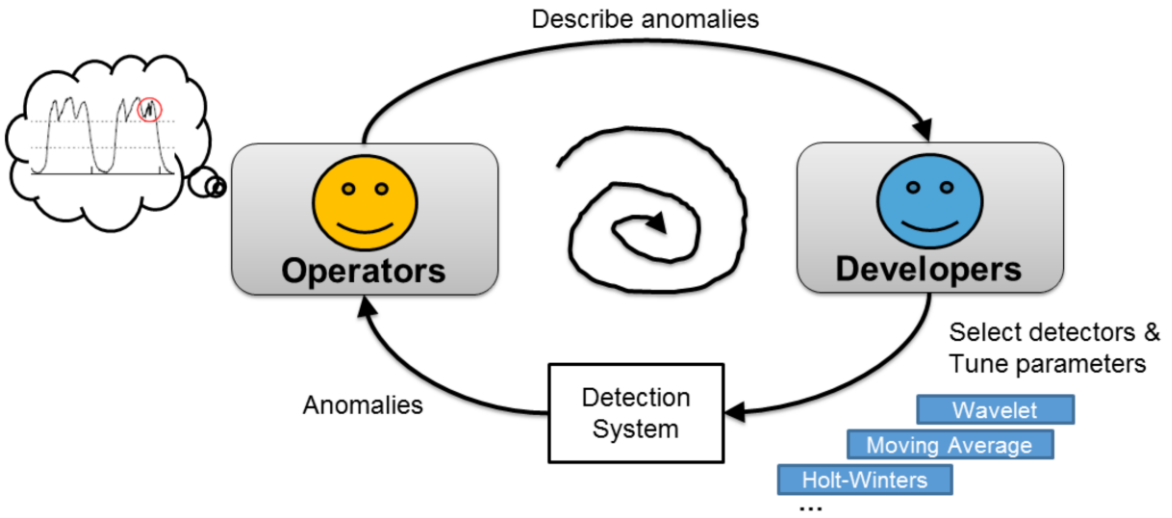
2015/12/15 Dapeng Liu (liudp10@mails.tsinghua.edu.cn) 7

The detection system starts to work and report anomalies to operators.

However, because operators may not describe the anomalies precisely, or developers cannot select or tune detectors well, the detection system is often inaccurate at the beginning

How to Build the Anomaly Detection System

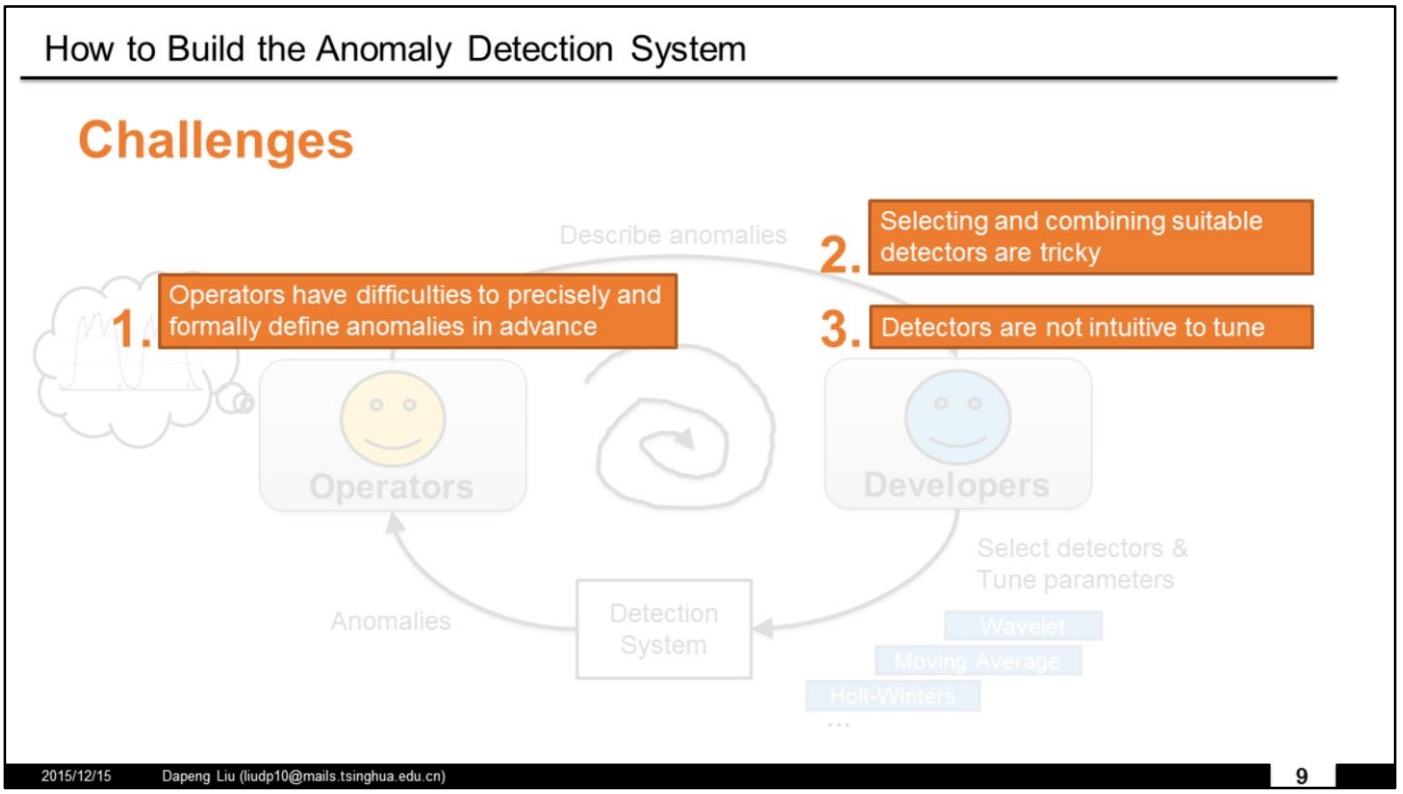
In practice, it is more complex



2015/12/15 Dapeng Liu (liudp10@mails.tsinghua.edu.cn) 8

So, it usually takes operators and developers a lot of efforts to iterate again and again, but at last the system may still not work, generating many false positives or false negatives, and operators are not willing to use it.

This is one important reason that many proposed detectors are not being used in practice.



In summary, there are three main challenges in building an anomaly detection system.
First, …
Second…
Third…(Especially for those complex dectors)

Because of these practical challenges, building an anomaly detection system requires a lot of manual efforts.

This is the problem we want to solve in this paper. We want to reduce the efforts of building an anomaly detection system. But how can we do that?