Preemptive Anomaly Prediction in IoT Components

Alhassan Boner Diallo, Hiroyuki Nakagawa, Tatsuhiro Tsuchiya

Graduate School of Information Science and Technology
Osaka University
Osaka, Japan

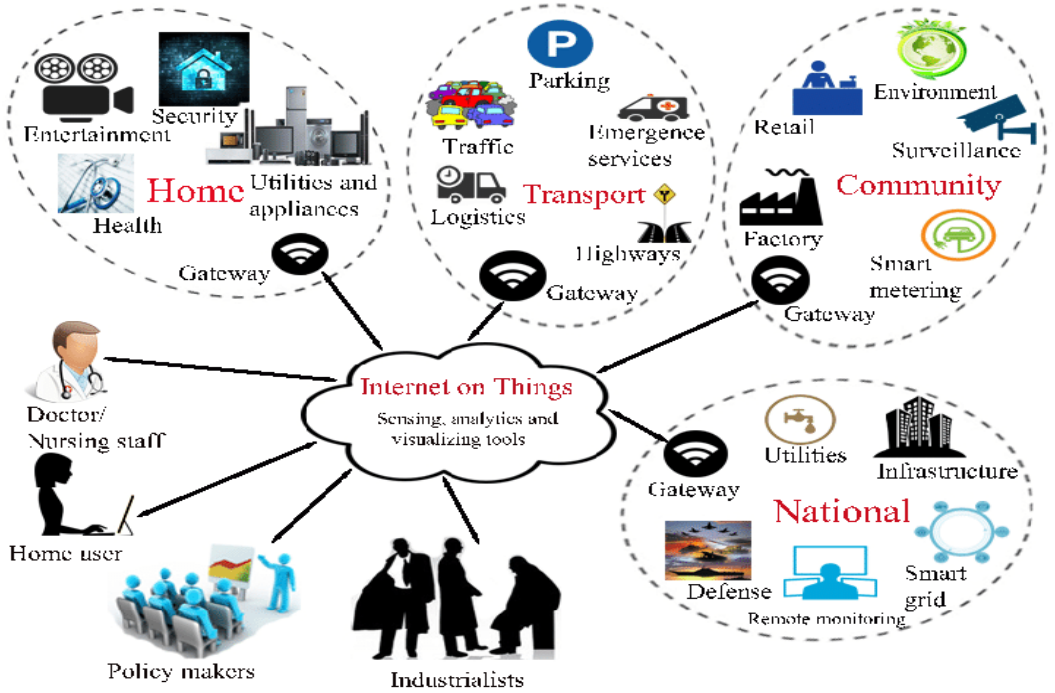
大阪大学
OSAKA UNIVERSITY

Content

- Introduction
- Background
- Case Study
  - DeltaIoT
- Research Question
- Approach
  - Reliability metrics quantification
  - Q-learning for time discovery
- Preliminary Results
- Discussions
- Conclusion

Introduction

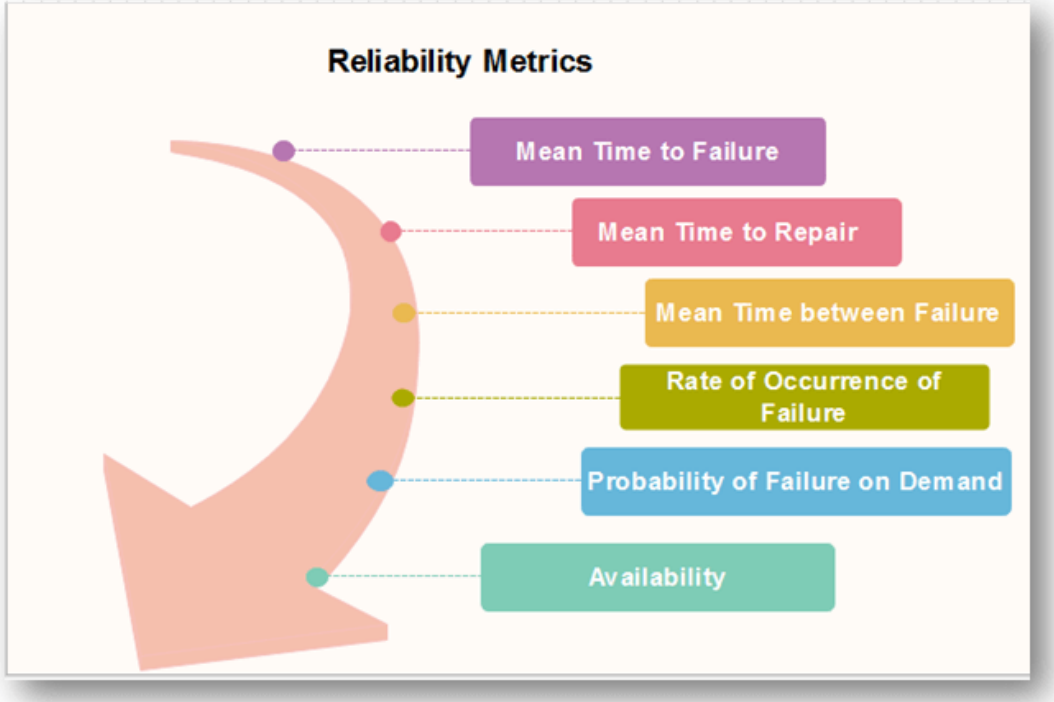
- IoT paradigm is applied to many safety-critical systems
  - factory management
  - personal body sensors in healthcare
  - surveillance systems in nuclear power plants
  - early warning systems for earthquakes
  - etc.
- Necessity to insure reliability and availability of the IoT system components



Roy, Sandip, et al. "Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing Internet of Things." *IEEE Internet of Things Journal* 5.4 (2017): 2884-2895.

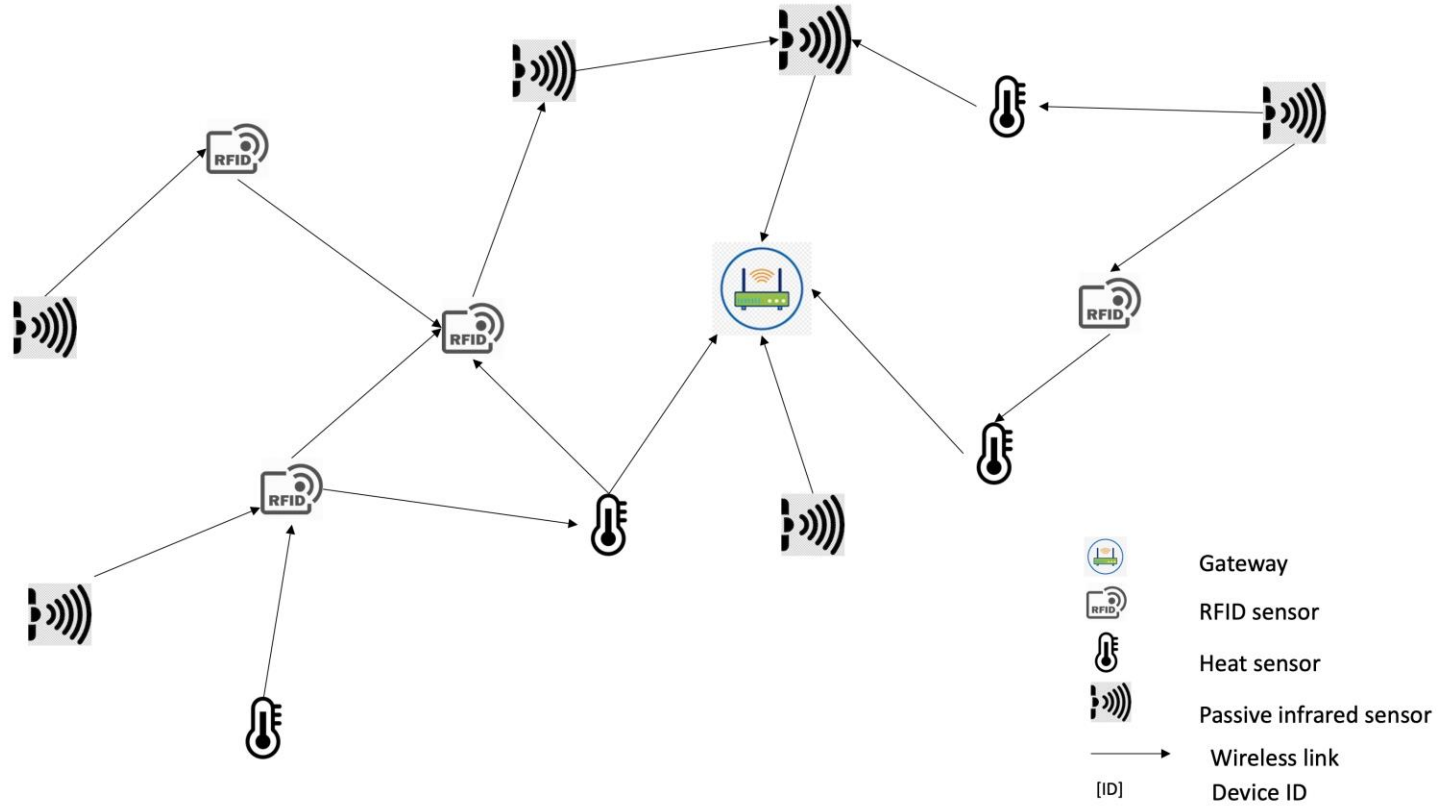
Background

- IoT systems reliability
  - Quality decay over time
- Metrics for reliability quantification
  - mean time to anomaly, anomaly rate, probability of anomaly
- Focus: ***Anomaly prediction***
  - cyclic and random anomalies on sensor components



https://www.javatpoint.com/software-engineering-software-reliability-metrics

Case Study: DeltaIoT



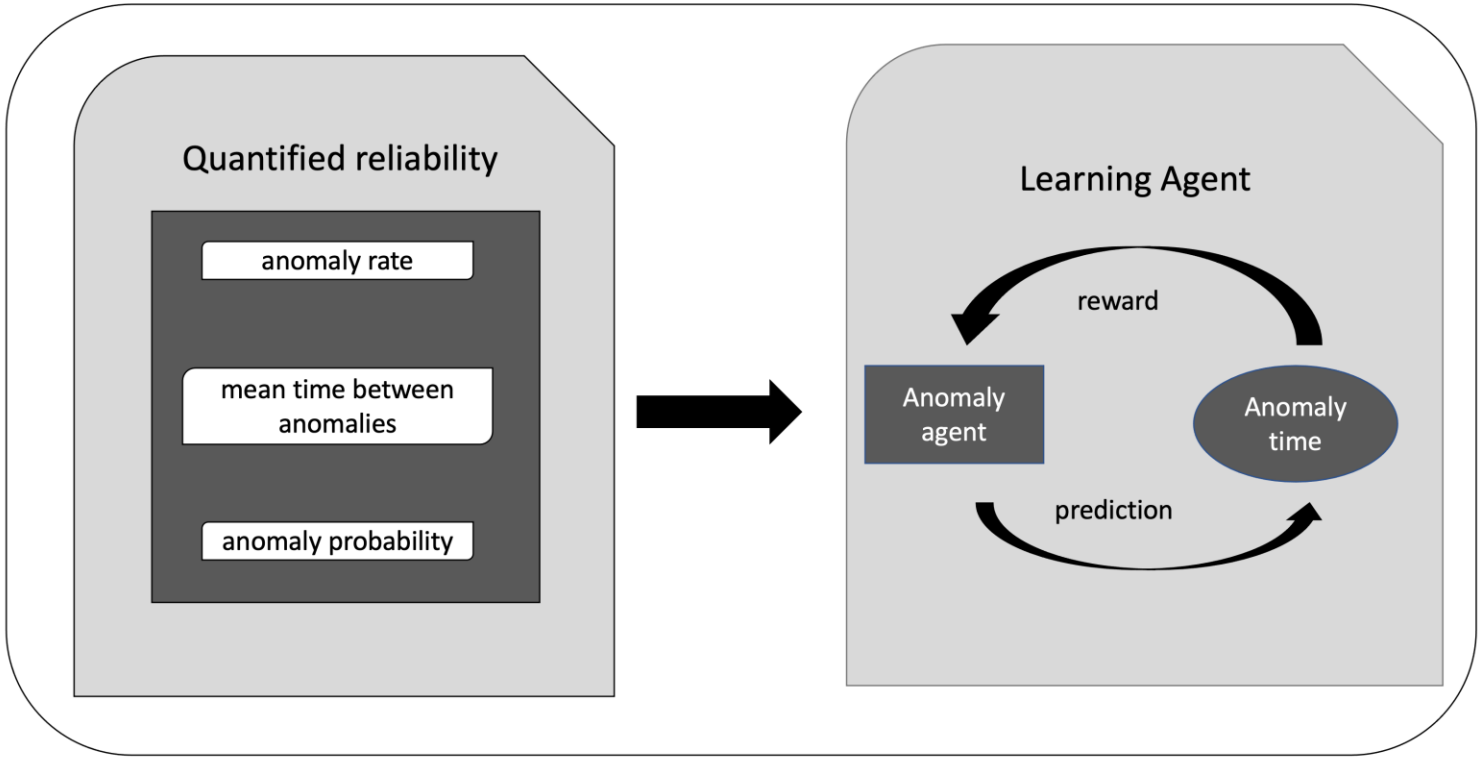
- Smart environment monitoring
- *15* Long-Range devices
  - Multi-hop communication
  - Communication in cycles
  - Cycle of 570s
- ***Sensor anomaly***
  - Loss of sensitivity
  - Loss in accuracy

Research Question

- How can we predict an accurate anomaly time for the IoT sensors based on their reliability metrics?

Approach
Component-level mechanism

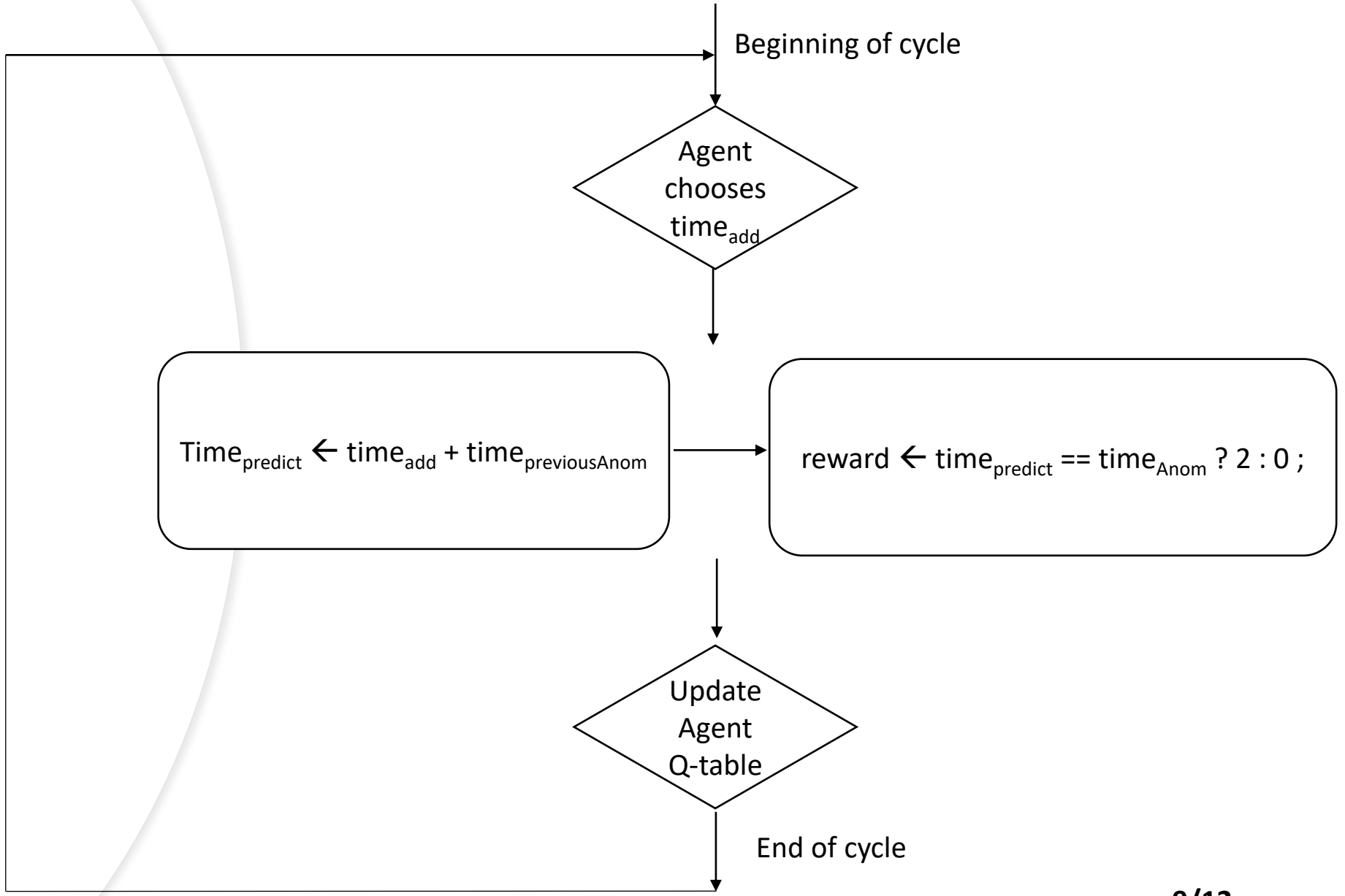
- Anomaly Prediction
  - Reliability quantification mechanism
    - Component quality over time
  - Q-learning agent
    - Estimate anomaly time



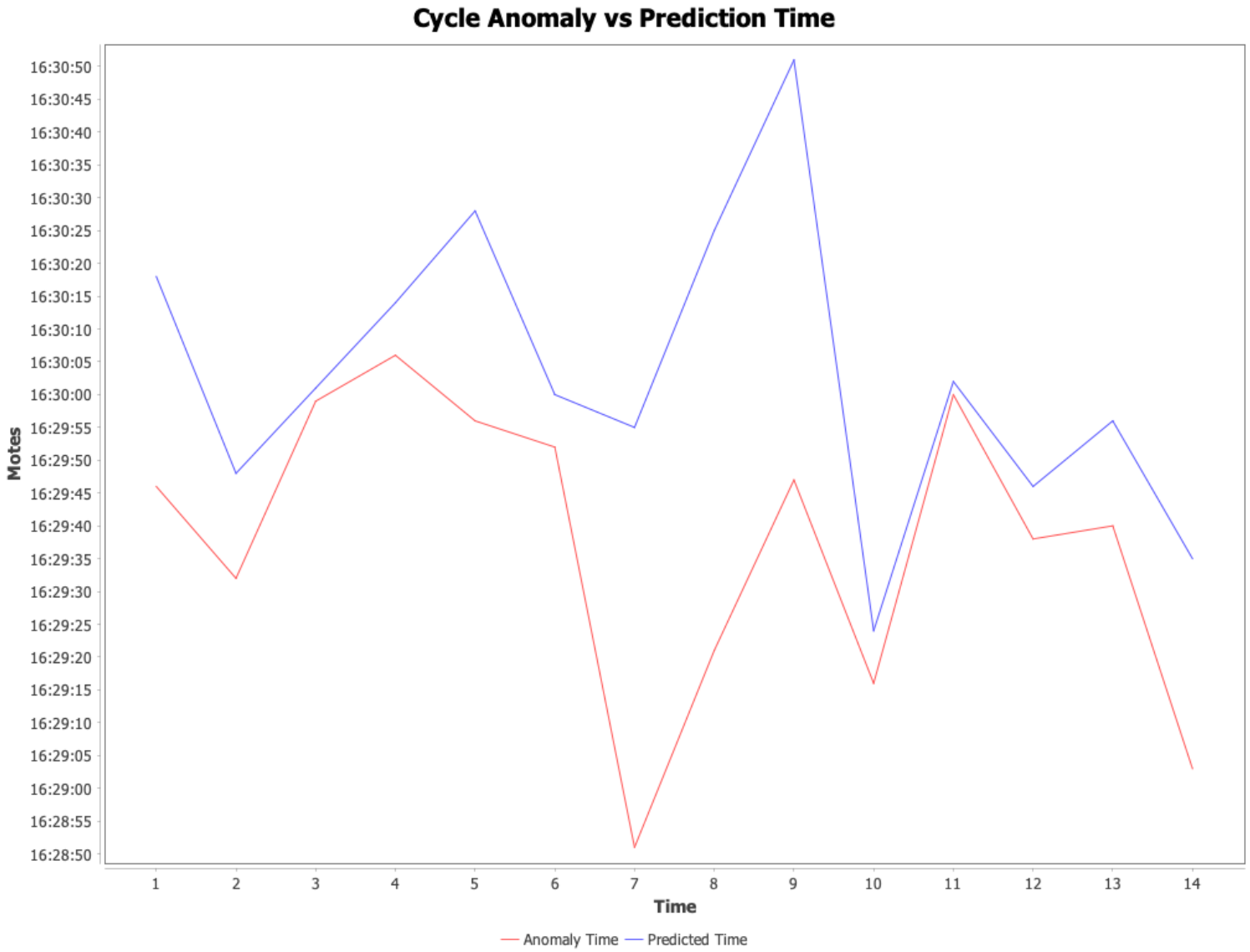
Approach
Q-learning Agent

- $state_i$
  - value of the probability of anomaly
- $action_i$
  - amount of time to add to the previous anomaly time
  - $\mathbf{time_{add}}$
- ***Q-value***
  - quality of the state-action combination

Approach
Q-Agent training



Preliminary Results



Discussions

- The estimation of the predicted time seemed to follow the anomaly time for some devices
- There is a need to better calibrate the way the agent learn, for example, by changing the interaction between the reward and the action

Conclusion

- In this research , we tried to solve the anomaly prediction problem for IoT sensor components using Q-learning
- Our approach produced contrasting results depending on the sensor component