Unsupervised Learning for Trustworthy IoT

Nikhil Banerjee
nb00227@surrey.ac.uk

Thanassis Giannetosos
a.giannetsos@surrey.ac.uk

Emmanouil Panaousis
e.panaousis@surrey.ac.uk

Clive Cheong Took
c.cheongtook@surrey.ac.uk

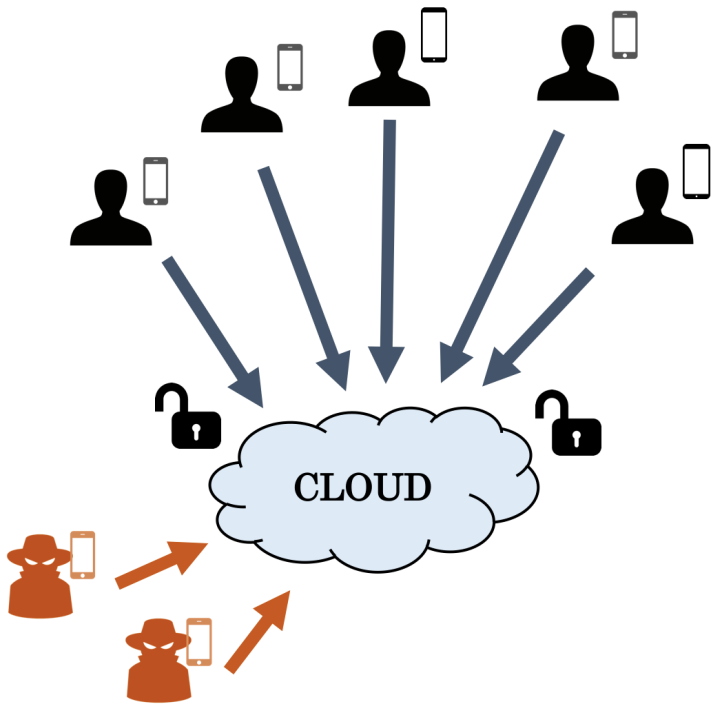
Department of Computer Science
University of Surrey

Overview

1. Introduction & Background
2. System Proposal
3. Experimental Setup & Results
4. Conclusion & Future Work

Mobile Crowd Sensing Trustworthiness

- Mobile Crowd Sensing for large scale data collection using common devices such as mobile phones
- Many participatory users feeding data into single database
- Desired openness means lack of control on user data:
- What if data originates from *untrustworthy* users in collaboration?
- **Need measures to prevent pollution of trusted data**.



System and Threat Models

- **System Model**: MCS sensing task with multiple users sending a stream of measurements $v_1, v_2, ..., v_n$.
- With timestamp t, location loc, and security measures in place (σ_{PrvKey}, certificate C).

$$r_i = \{[v_1, v_2, v_3, ..., v_n] \,||\, t \,||\, loc \,||\, \sigma_{PrvKey} \,||\, C\}$$

- **Threat Model**: Adversaries attempt to mislead system towards a value T compromising the system trustworthiness.

$$\max f[x^t - x^{(a)}(\tau)] \qquad \text{s.t.} \quad f \leq T$$

Concept Drift

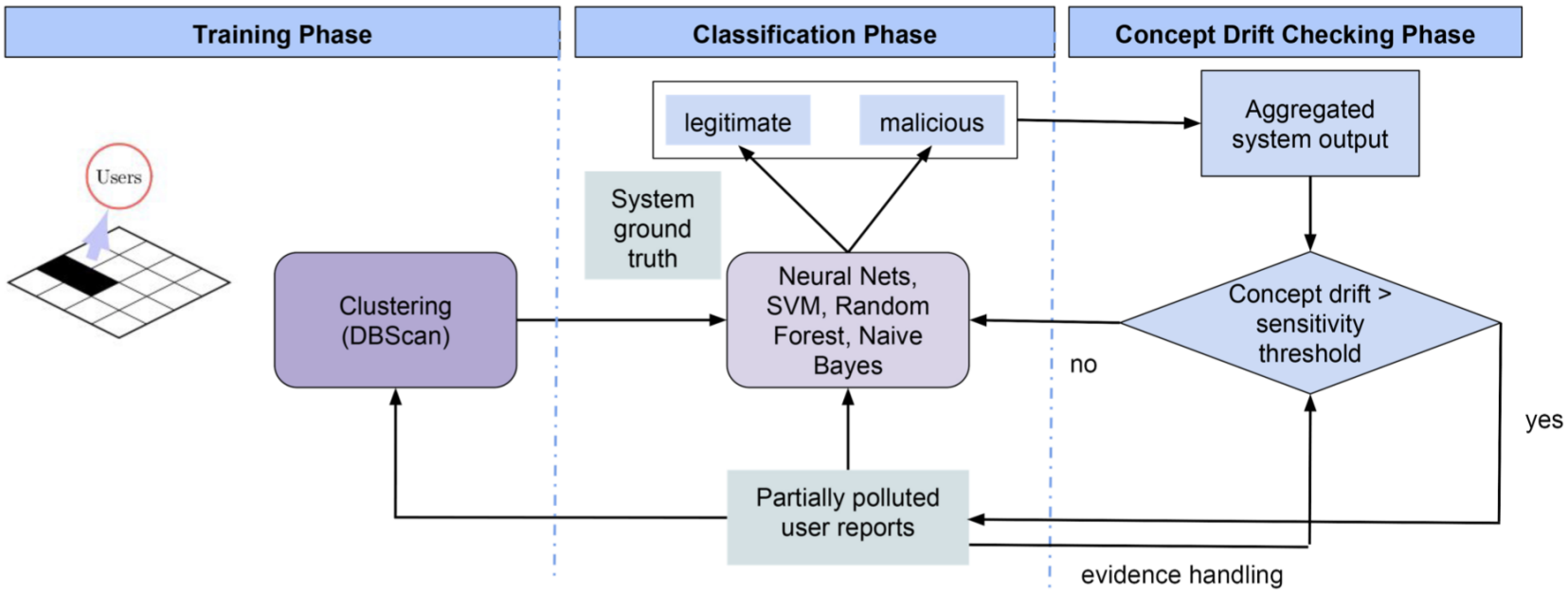
- An unforseen change in statistical properties of over time.
- Can be natural (e.g. environmental change) or malicious (e.g. malicious attack strategy).
- Must be taken into account to prevent false positives.

$$x_i^{(a)}(\tau) = \min(x_i^t + \tau\delta + \eta_i(\tau), T), \quad \forall\ i = \{1, ..., N_a\},$$

such that

$$\begin{aligned}
\tau = 0 \qquad & x_i^{(a)} = x_i^t + \eta_i(0) \approx x_i^t \\
\tau = 1 \qquad & x_i^{(a)} = \min(x_i^t + \delta + \eta_i(1), T) \\
\tau = 2 \qquad & x_i^{(a)} = \min(x_i^t + 2\delta + \eta_i(2), T) \\
\cdots & \\
\tau \to \infty \qquad & x^{(a)} = T
\end{aligned}$$

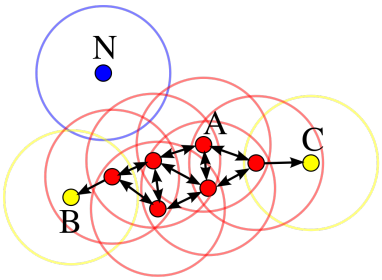
Proposed System Design



- Clustering slow; classification faster but dependent on clustering.
- Re-clustering only triggered if potential natural concept drift occurs.

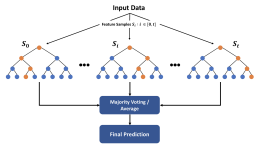
Chosen Algorithms

Arthur P. Dempster and Glenn Shafer - **Dempster-Shafer Theory**

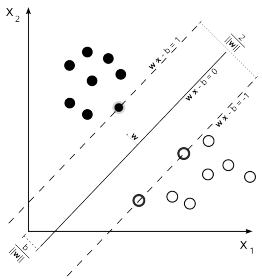


DBSCAN Clustering

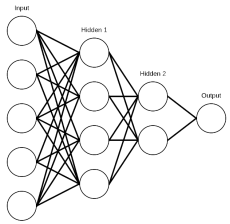
- Naive Bayes
- Random Forest



- Support Vector Machines



- Artificial Neural Networks



Experimental Setup

Data:

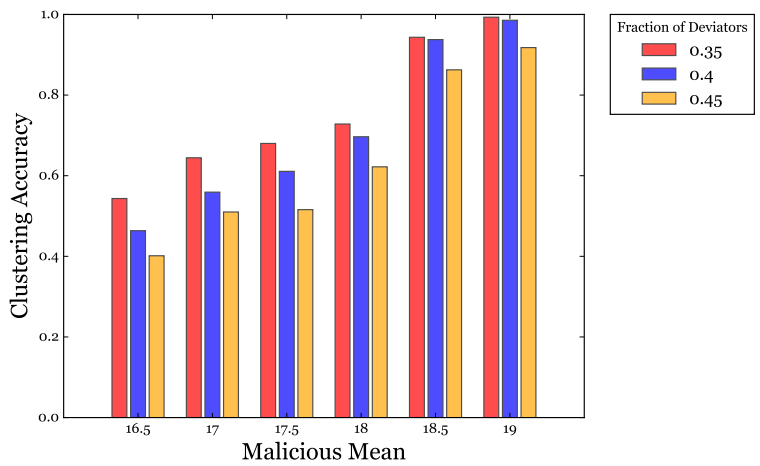
- Evaluation of real world (source: Data Sensing Lab) and synthetic (random normal distribution).
- 5 sensor values: Temperature, Humidity, Passive IR, Motion & Microphone.
- Target measurement: Temperature

Experiments:

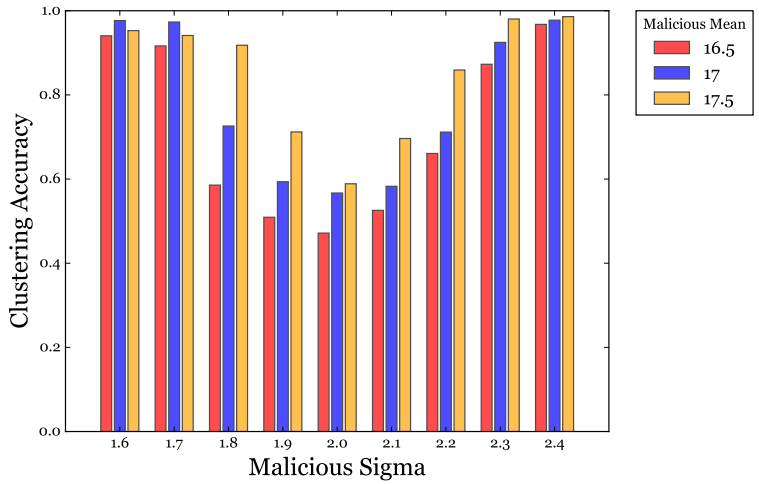
- Initial experiments to select topology and hyperparameters.
- Then determine clustering, classification and overall accuracy for varying malicious distributions and fraction of deviating users.
- *Demonstrate system effectiveness facing varying adversarial strategies.*

Clustering accuracy for various outlier distributions

The accuracy of clustering increases as the mean of malicious data becomes distant from that of the legitimate.

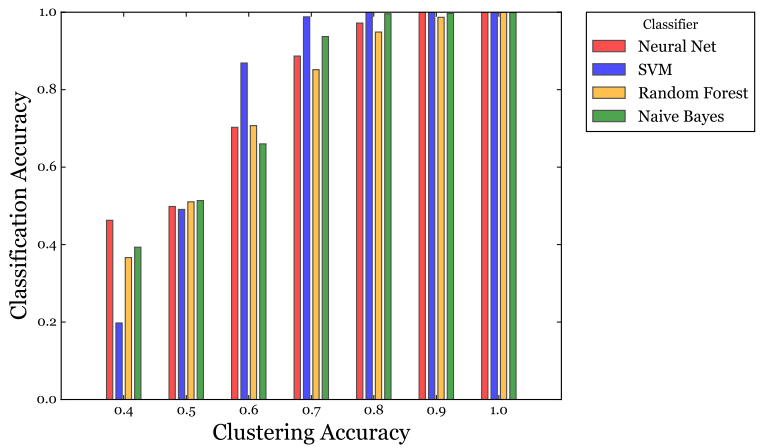


The clustering accuracy increases as the standard deviation distances itself from the legitimate deviation.

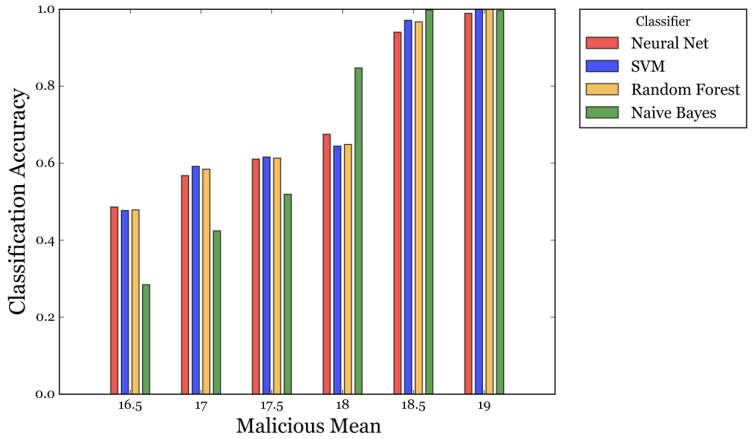


.. and for classification using various classifiers.

Using generated fixed clustering results (with given accuracy) to evaluate the classifiers dependence on clustering results.



Overall system accuracy for clustering and classification phases of varying malicious means.



Remarks and Conclusions

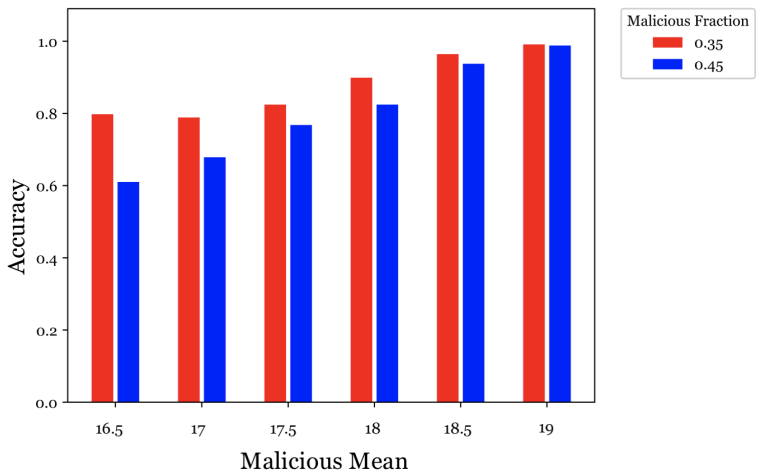
- Classification accuracy very dependent on results of clustering.
  - Drawback: Sparse initial clusters can produce worse results.
- Outlier detection accuracy increases as distribution of malicious values distances from the legitimate distribution.
- Can detect concept drift through tuning of sensitivity parameter.

$$x_i^{(a)}(\tau) = \min(x_i^t + \tau\delta + \eta_i(\tau), T), \quad \forall\ i = \{1, ..., N_a\},$$

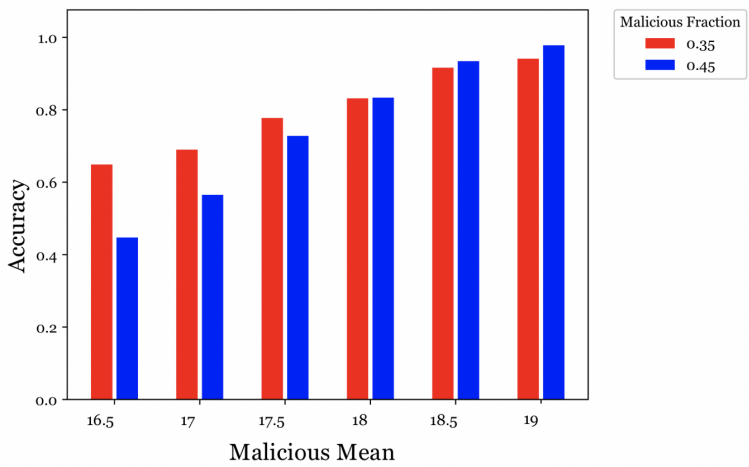
Future Work

- Evaluation of additional clustering techniques, ensemble methods for classification and sensitivity parameter for concept drift detection.
- Alternate Methods: Impact of correlation between sensors values for outlier detection. *Removes reliance on clustering.*

Predicting the *expected* value of another highly correlated sensor.



Less correlated sensors obtain lower prediction accuracy.



Thank you!