Finding the Truth: Towards Robust Aggregation of Inconsistent Information

UNSW | Faculty of Engineering | School of Computer Science and Engineering

Mohsen Rezvani

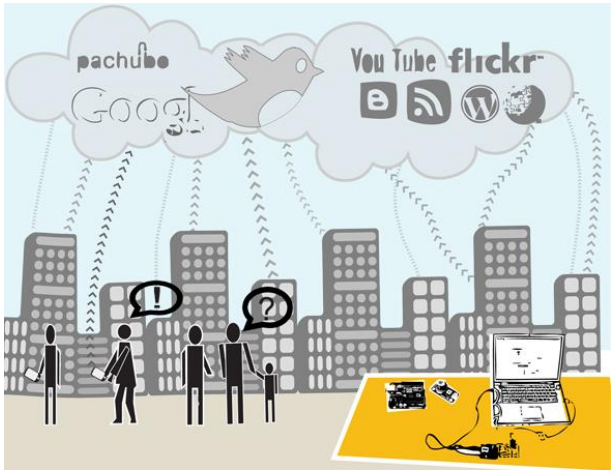
PhD Student in Network Research Lab

18 November 2014

What is this talk about?

- how to improve reliability of information obtained in an automated way from multiple sources

- possible sources: a sensor network or multiple websites or a large number of users of a web service or a social network



What is this talk about? – cont.

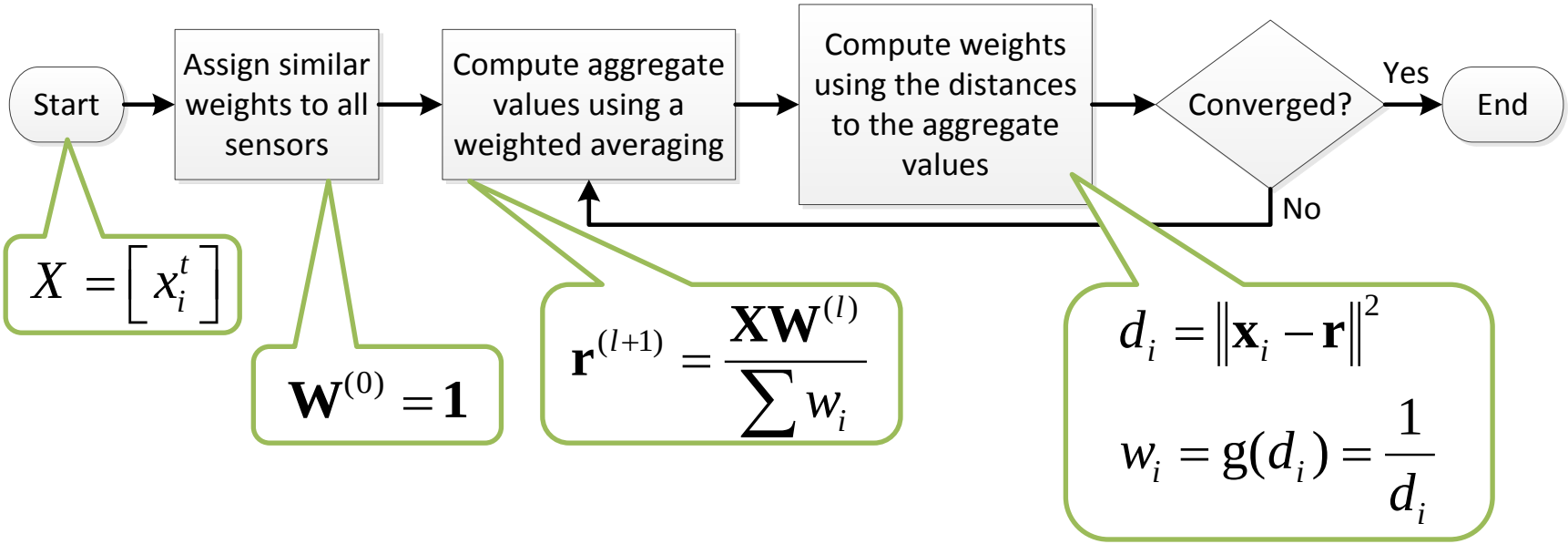
- the problem: multiple sources are often inconsistent, because of:
  - errors, noise, hardware faults
  - being out of date
  - differences of opinion
  - might be maliciously supplying false information

- Reputation and Trust Systems
  - Aggregate the reports to obtain a belief about a source / object within a context / community

- Iterative filtering algorithms

Iterative Filtering Algorithms

- IF Property: *Sensors whose readings often are far from those of others are assigned less weights*



[Kerchove and Dooren, Iterative filtering in reputation systems. SIAM J. Matrix Anal. Appl., 2010.]

How well do IF algorithms perform?

- Simultaneously produce approximations of:
  - the final aggregate values
  - Trustworthiness ranks of the sensors

- Outliers get penalized but never entirely excluded; no need to determine who is an outlier!

- If errors are independent and normally distributed, the variance of the estimate is close to the Cramer-Rao lower bound (CRLB).

How well do IF algorithms perform?

- If aggregate values get sufficiently close to the values of a particular sensor, iterative procedure converges fast to these particular values.
  - The discriminant function $g(d) = \frac{1}{d}$ has a pole at $d = 0$.

- Attack scenario
  - $c - 1$ attacker report far values s_t instead of r_t
  - The last node reports the skewed average value

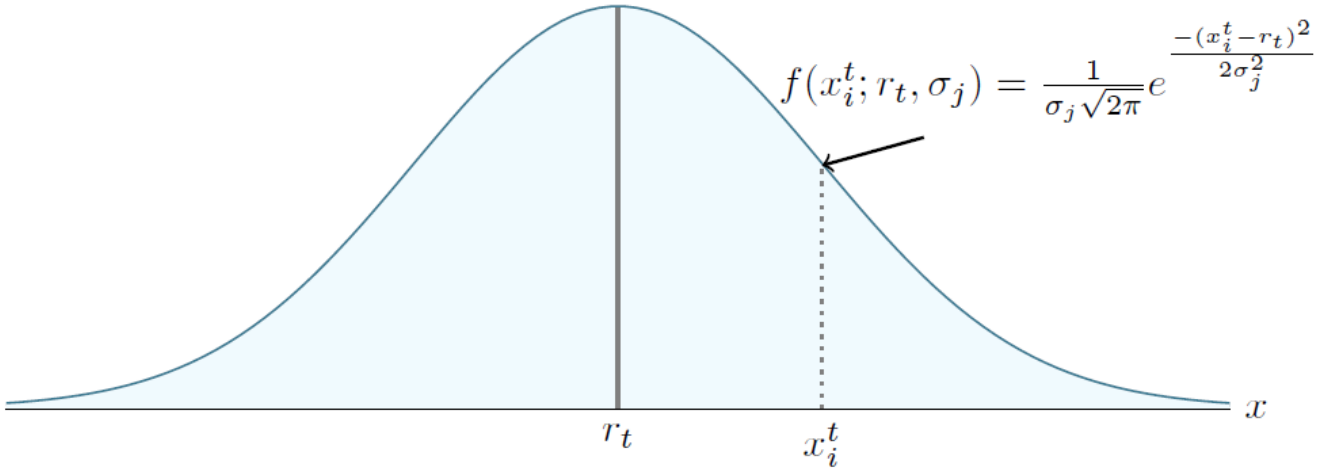
$$\left(\left(n-c+1\right)\ r_t + \left(c-1\right)\ s_t\ \right) / \left(n-1\right)$$

- M. Rezvani, A. Ignjatovic, E. Bertino and S. Jha, “A Robust Iterative Filtering Technique for Wireless Sensor Networks in the Presence of Malicious Attacks”, SenSys 2013
- M. Rezvani, A. Ignjatovic, E. Bertino and S. Jha, “Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks”, IEEE TDSC, 2014

Credibility Propagation (CRPR)

- **Idea:** the trustworthiness of a sensor node is evaluated from the amount of credibility that such a node collects from other nodes.

- ***Credibility*** of a sensor node is the likelihood that other nodes can make the readings of such a node.



Credibility Propagation – cont.

- The credibility of sensor i given by sensor j

$$\mathrm{L}(j,i) = \left(\prod_{t=1}^{m} \frac{1}{\sigma_j \sqrt{2\pi}} e^{\frac{-(x_i^t - r_t)^2}{2\sigma_j^2}} \right)^{\frac{1}{m}} = \frac{1}{\sigma_j \sqrt{2\pi}} e^{\frac{-\frac{1}{m}\sum_{t=1}^{m}(x_i^t - r_t)^2}{2\sigma_j^2}}$$

- The total credibility of sensor i

$$\mathrm{cr}(i) = \left(\prod_{\substack{j=1 \\ j \neq i}}^{n} \mathrm{L}(j,i) \right)^{\frac{1}{n-1}} = \left(\prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{1}{\sigma_j \sqrt{2\pi}} e^{\frac{-\frac{1}{m}\sum_{t=1}^{m}(x_i^t - r_t)^2}{2\sigma_j^2}} \right)^{\frac{1}{n-1}} = \left(\prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{1}{\sigma_j \sqrt{2\pi}} e^{\frac{-\sigma_i^2}{2\sigma_j^2}} \right)^{\frac{1}{n-1}}$$

Credibility Propagation – cont.

- The aggregate value at time t

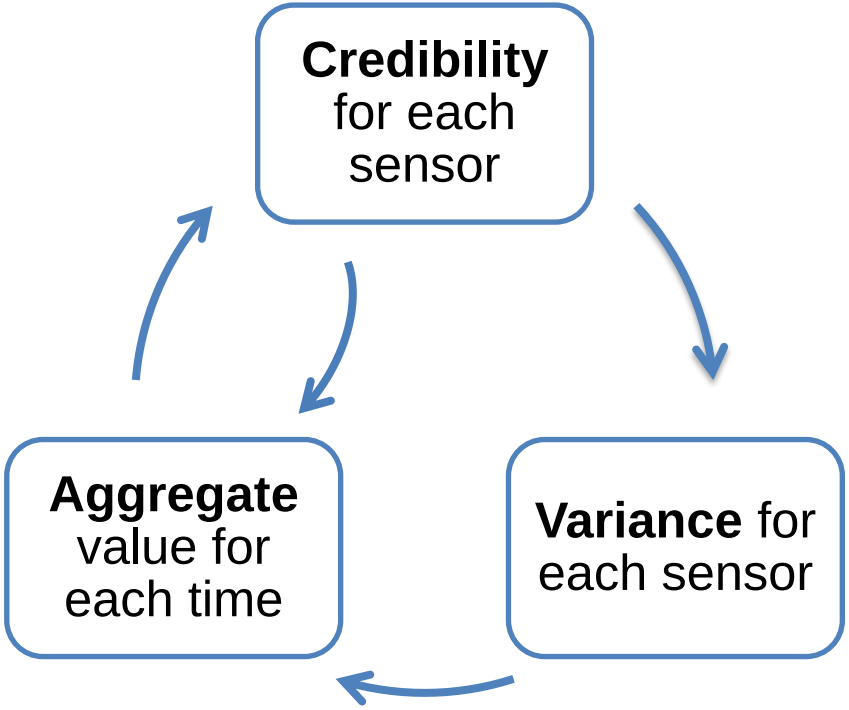
$$r_t = \sum_{i=1}^{n} \frac{\mathrm{cr}(i)}{\sum_{k=1}^{n} \mathrm{cr}(k)} x_i^t$$

- The variance of sensor i

$$\sigma_i^2 = \frac{1}{m} \sum_{t=1}^{m} (x_i^t - r_t)^2$$

Credibility Propagation – cont.

- Recursive relationship among credibility, aggregate value and variance



Credibility Propagation – cont.

- Each iteration of CrPr consisted of:
  - Updating all credibility values given the variances and aggregate values.
  - Updating all aggregate values given the credibility values.
  - Update all variances given the aggregate values.

- When does the algorithm terminate?
  - after changes in the variances fall below a threshold.
  - after a fixed number of iterations.

Credibility Propagation – cont.

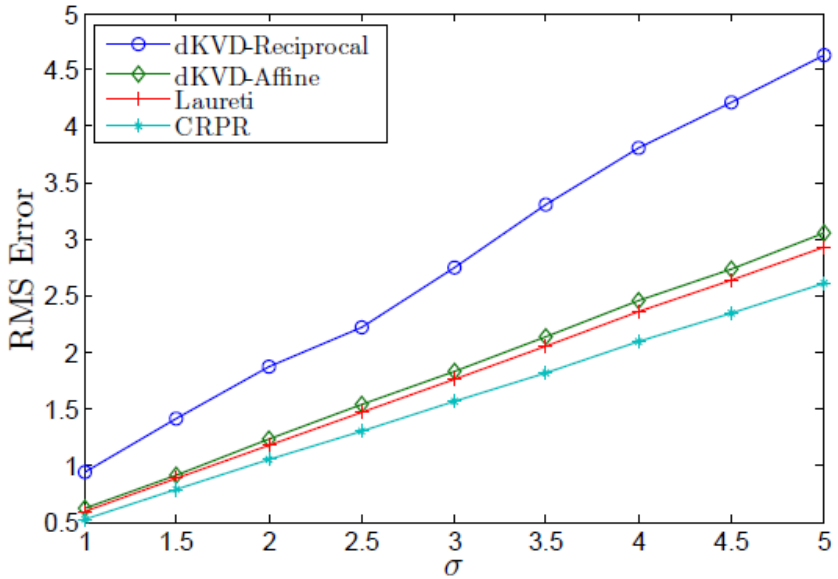
- Computing final aggregate values using MLE with the estimate variance values from the iterative algorithm

$$r_t = \sum_{i=1}^{n} \frac{\frac{1}{\mathrm{var}(i)}}{\sum_{k=1}^{n} \frac{1}{\mathrm{var}(k)}} x_i^t \quad \text{for all } t=1,\cdots,m.$$

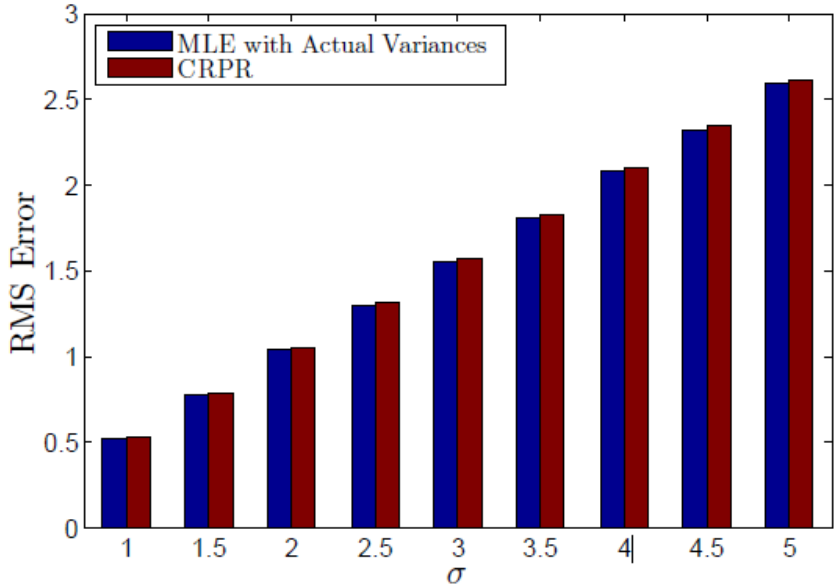
CrPr Extensions

- Sparse readings
- Compromised Node Detection and Revocation
- High credibility to sensors with more readings
- Credibility propagation to data streaming

Experiments: No Attack



(a) Unbiased error



(b) Unbiased error

Experiments: Attack

$$\left\|\mathbf{r}-\hat{\mathbf{r}}\right\|_1 = \sum_{t=1}^{m}\left|r_t-\hat{r}_t\right|$$

$$\frac{100}{m}\left\|\mathbf{r}-\hat{\mathbf{r}}\right\|_1$$

	Random Readings	Promoting Attack	Collusion Attack
Average	143.32 (19.91)	881.37 (122.41)	730.25 (101.42)
dKVD-Reciprocal	76.20 (10.58)	49.30 (6.85)	714.34 (99.21)
dKVD-Affine	101.82 (14.14)	119.85 (16.65)	131.96 (18.33)
Laureti	70.32 (9.77)	221.77 (30.80)	741.31 (102.96)
Robust-Reciprocal	76.20 (10.58)	49.30 (6.85)	69.90 (9.71)
Robust-Affine	101.82 (14.14)	119.85 (16.65)	131.96 (18.33)
CrPr	23.52 (3.27)	15.15 (2.10)	51.06 (7.09)

Conclusion

- CrPr provides more robustness against faults and false data injection

- Prove the convergence of CrPr
- Security analysis of CrPr through finding the best strategy of an attacker for launching a collusion attack

Thanks for your attention