Data Intensive Mobile Sensornets: Killer Applications and Grand Deterrents

Panel Chair:

Vladimir Zadorozhny, University of Pittsburgh, Pittsburgh, USA
vladimir AT sis.pitt.edu

Panelists:

Karl Aberer, EPFL, Switzerland
karl.aberer AT epfl.ch
Dimitrios Gunopulos, University of California, Riverside, USA
dg AT cs.ucr.edu
Pedro Jose Marron, University of Stuttgart, Germany
pedro.marron AT ipvs.uni-stuttgart.de
Ouri Wolfson, University of Illinois at Chicago, USA
wolfson AT cs.uic.edu

Synopsis:

First the panel chair highlighted several potential *Killer Applications* of Data Intensive Mobile Sensor Networks. They included:

- A team of cooperative mobile robots deployed in conjunction with stationary sensor nodes to acquire and process data for surveillance, tracking, environmental monitoring, or execute search and rescue operations.
- Large-scale human health monitoring with body sensors reporting critical health parameters (e.g., blood pressure) to a processing station. More complicated version: monitoring the health of soldiers in a battlefield.
- Discovering traffic conditions under assumption that each vehicle is provided with a group of sensors that reports its local parameters (e.g., speed) and surrounding condition (e.g., snow, icy road, etc.). A complicated case: battlefield reports and extra speed (e.g., a swarm of jets).

Each of the panelist was asked to specify a list of challenges that hold a progress towards creating a sustained market utilizing suggested *Killer Apps*. Finally, the panelists were invited to vote on a final list of *really GRAND DETTERENTS* selected out of the specified challenges.

The panelists selected two groups of challenges (deterrents): technical and non-technical one. After that the panelists voted to assess each of those challenges if they are really grand deterrents. A vote is a number between 0 and 10 (0-definitely not, 10-definitely yes). One suggestion was that rating around 5 could be read as "requires still lots of work, but could be principally solved". Note, that in this voting we did not consider a time dimension. What is a grand deterrent at the current moment, could eventually be solved, but some more long-term problems might stay around for quite a while. This was a bit difficult to factor into the evaluation.

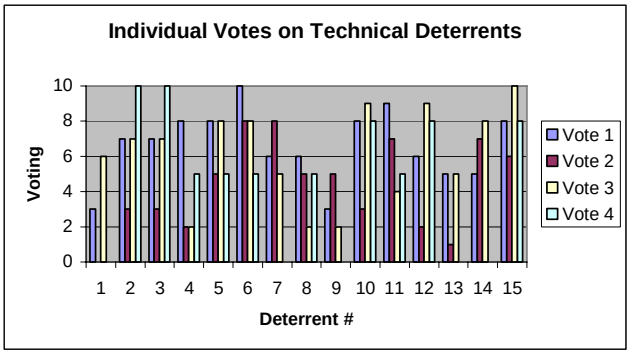
Technical Deterrents:

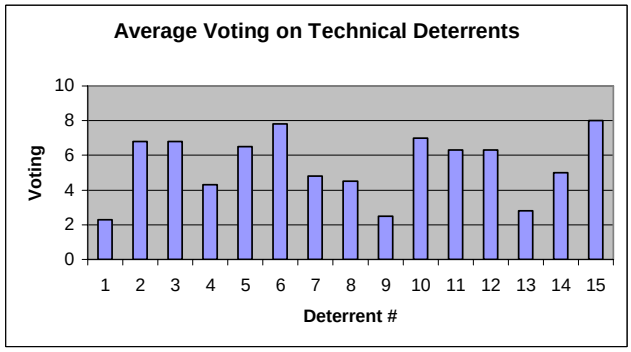
1. Lack of general approaches and theoretical foundations
2. Lack of techniques for getting information out of the sensor data
3. Lack of efficient techniques for storing and accessing the data
4. Difficulties with implementing sophisticated data analysis/mining
5. Difficulties with coping with redundant, inaccurate and false data
6. Lack of techniques for efficient deployment and maintenance
7. Lack of efficient engineering control and self-organization
8. Complex and expensive application development and evaluation
9. Lack of reliable localization techniques
10. Lack of efficient techniques to enforce privacy and security
11. Difficulties with handling heterogeneous hardware, protocols, data
12. Lack of proper resource management (e.g., long-time energy efficiency)
13. Inefficiency of lower layers of wireless networks (routing, MAC)
14. Lack of right abstraction (data location, query origination, moving patterns)
15. Alternative approaches (e.g central site database) can do it better

The results of voting on technical deterrents are represented in the following tables and graphs (the order of votes does not reflect the alphabetical order of the panelists above):

Table 1: Voting on Technical Deterrents

Deterrent#	*Vote 1*	*Vote 2*	*Vote 3*	*Vote 3*	*Average*
1	3	0	6	0	2.3
2	7	3	7	10	6.8
3	7	3	7	10	6.8
4	8	2	2	5	4.3
5	8	5	8	5	6.5
6	10	8	8	5	7.8
7	6	8	5	0	4.8
8	6	5	2	5	4.5
9	3	5	2	0	2.5
10	8	3	9	8	7
11	9	7	4	5	6.3
12	6	2	9	8	6.3
13	5	1	5	0	2.8
14	5	7	8	0	5
15	8	6	10	8	8





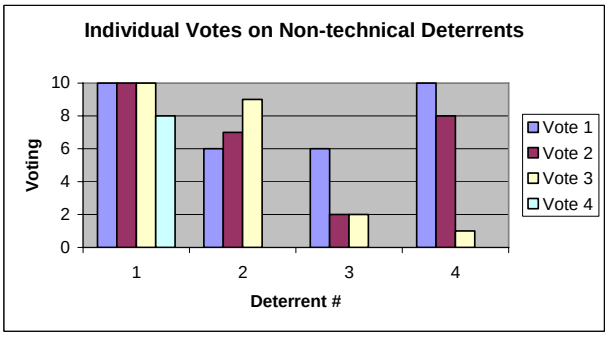
Non-technical Deterrents:

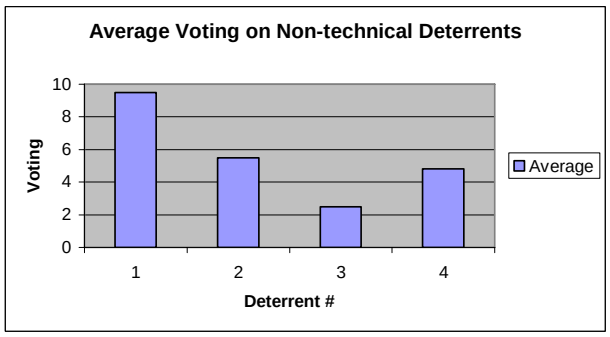
1. Not obvious business model (investment, economic return; different models for industry, military, government).
2. Difficulties with making technology accessible to non-IT specialists
3. The applications are not affordable for most of customers.
4. The general public is not ready for it.

The results of voting on technical deterrents are represented in the following tables and graphs (the order of votes does not reflect the alphabetical order of the panelists above):

Table 2: Voting on Non-technical Deterrents

Deterrent#	*Vote 1*	*Vote 2*	*Vote 3*	*Vote 4*	*Average*
1	10	10	10	8	9.5
2	6	7	9	0	5.5
3	6	2	2	0	2.5
4	10	8	1	0	4.8





Instead of Conclusion

At this point we would like to leave a conclusion open. We will appreciate any feedback from interested MDM participants. Please, send your comments to vladimir@sis.pitt.edu with the subject “MDM panel feedback”. All your feedbacks will be summarized in the concluding section of this summary.