Energy Trade-Offs in Resource-Constrained Multi-Agent Systems

Hugo Carr, Jeremy Pitt, Anthony Kleerekoper, and David Blancke

Electrical & Electronic Engineering Department,
Imperial College London, SW7 2BT, UK

1 Introduction

Sensor networks and mobile ad hoc networks are two types of open system with resource constraints, in which functionality may be compromised by a lack of resources. In this work, we investigate adaptive algorithms for power-challenged computing networks. Using simulations, we have studied how self-organization can be used to trade off energy for (acceptable) accuracy to improve longevity in a sensor network; and how perceived threat and information sensitivity can be used to trade-off energy for (acceptable) security risk in an ad hoc network.

2 Energy vs. Accuracy in Sensor Networks

In sensor networks, a trade off exists between accuracy and longevity for networks implementing in-network data aggregation functions. Given the following system:

- A set of sensor nodes $S = \{s_1, \ldots s_n, s_{sink}\}$ where s_{sink} is the sink node;
- Each sensor node, s_i, has some energy at time t, $en_i(t)$, and some, fixed, error value, er_i;
- Sensor nodes take readings such that $r_i(t) = R(t) \pm er_i$ where $R(t)$ is the correct value. The error value is applied positively or negatively at random;
- Sensor nodes form opinions such that $o_i(t) = O(\{r_1(t), r_2(t), ..., r_n(t)\})$ where $O(\ldots)$ is some aggregating function of the readings received from neighbours;
- Network error is defined as $NE(t) = abs(R(t) - o_{sink}(t))$;
- Network lifetime is defined as $NL = t$ such that $\sum_{i=0}^{n} en_i(t) > 0$ and $\sum_{i=0}^{n} en_i(t+1) \leq 0$ where the summations do not include the sink node;

The requirement is to derive a method for aggregation that enables the sensors to specify an upper accuracy bound for the network error such that the network lifetime increases as the upper bound is raised, i.e. derive an algorithm for $O(\{r_1(t), r_2(t), ..., r_n(t)\})$ such that we maximise NL while ensuring that $\forall t[NE(t) \leq \epsilon]$, where ϵ is some predefined error bound.

There are three main algorithmic aspects to our proposed solution: the clustering algorithm for routing and self-organization of the aggregation tree initiated by s_{sink}, the opinion formation algorithm for in-network data aggregation (i.e. computing $o_i(t)$, for each $i \in S$), and network reformation and 'intelligent' message casting.

H. Aldewereld, V. Dignum, and G. Picard (Eds.): ESAW 2009, LNAI 5881, pp. 113–115, 2009.

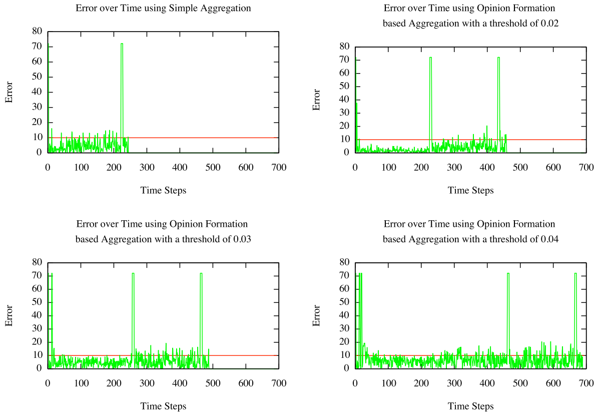

Fig. 1. Error in the aggregated reading over time under difference thresholds

The clustering algorithm is a minor variation of the protocol for forming an aggregation tree presented in [1], primarily in the assumption that transmission range is variable and the impact that data aggregation has on the cluster-head selection mechanism. We then adopt the opinion formation model of [4] for in-network data aggregation algorithm: treating the sensor nodes as agents, we can condition the interaction with social relations, such as trust and confidence thresholds, rather than simply averaging values. Finally we extend the message-passing protocols so agents (sensors) themselves determine the advisability on whether or not to transmit, and the extent whether or not it is appropriate (due to resource constraints) for the sink node to start re-dimensioning the network.

The algorithm has been simulated using the PreSage platform [2]. To test the longevity vs. accuracy trade-off, we used 500 nodes with a (max.) cluster size of 30 and ran the simulation recording the aggregated opinion at the sink node. Figure 1 compares the result of using simple aggregation against using opinion formation aggregation with different confidence thresholds. The results show that using a confidence threshold and network reformation can considerably extend the life-span of the network.

3 Energy vs. Security in Ad Hoc Networks

In ad hoc networks, a trade off exists between risk and longevity for networks implementing a number of different security policies, given that some policies require more computationally complex (and so high power) encryption algorithms. Given the following system:

- set of agents $A = \{a_1, a_2, \ldots, a_n\}$
- a set of clusters C satisfying $c_i \in C \rightarrow c_i \subseteq A$
- a pair of roles, *cluster-head* and *member*, such that there is one cluster-head per cluster and each agent is a member of at least one cluster;
- the set of social constraints (normative rules) as given by e.g. a specification in an action language (cf. [3]);

– environment variables, in particular a security level, *sl*, energy level *el*, and perceived threat level *tl* (derived from the information sensitivity and the detected interception rate).

The requirement is to derive a security policy that enables the agents to determine a network-level security policy from local, cluster-based interactions concerning the available energy and perceived threat.

Accordingly, we have developed an algorithm for selecting an appropriate security policy which inter-leaves data aggregation using 'gossiping' at the cluster and cluster-head level, and role-based norm-governed voting protocols for multi-agent systems [3]. We use opinion formation, based on the same model [4], to determine the need for change at the cluster level, followed by a vote (by the cluster members) for change at the cluster level; if there is a change then there is opinion formation at the cluster-head level, followed by votes within each cluster initiated by the cluster-heads. Simulation of this system is work in progress.

4 Conclusions

In both sensor networks and ad hoc networks, there is a resource-constrained environment limiting the effective computation of the constituent nodes. In both cases, we see 'brute' facts (the energy level), institutional facts determined by opinion formation (resp. data reading and perceived threat), and institutional facts determined by social rules (resp. accuracy bound and security level).

In order to trade-off the brute facts against the institutional facts to improve (resp.) accuracy and data integrity in such open systems (i.e. in the absence of global objects and common objectives), we have developed algorithms based on the interaction between and adaptation of an underlying social network with an overt organizational structure, where each informs, influences and interleaves with the other. This is the basis of what we call micro-social systems, which arise from the interleaving of social networks with norm-governed system, and may provide the basis of a common computational framework for self-organization in open resource-constrained networks.

References

1. Ding, M., Cheng, X., Xue, G.: Aggregation tree construction in sensor networks. In: IEEE Vehicular Technology Conference, vol. 4, pp. 2168–2172 (2003)
2. Neville, B., Pitt, J.: Presage: A programming environment for the simulation of agent societies. In: Hindriks, K., Pokahr, A., Sardina, S. (eds.) ProMAS 2009. LNCS (LNAI), vol. 5442, pp. 88–103. Springer, Heidelberg (2009)
3. Pitt, J., Kamara, L., Sergot, M., Artikis, A.: Formalization of a voting protocol for virtual organizations. In: Proceedings International Conference on Autonomous Agents and Multi-agent Systems (AAMAS), pp. 373–380 (2005)
4. Ramirez-Cano, D., Pitt, J.: Follow the Leader: Profiling Agents in an Opinion Formation Model of Dynamic Confidence and Individual Mind-Sets. In: Proceedings IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT), pp. 660–667. IEEE Computer Society, Los Alamitos (2006)