GEORGETOWN UNIVERSITY

Nitin H Vaidya <nv198@georgetown.edu>

[PODC 2019] Submission #138 "Exact Byzantine Consensus on Undirected..."

1 message

PODC 2019 HotCRP <noreply@podc19.hotcrp.com> Sun, May 5, 2019 at 9:10 PM
Reply-To: faith@cs.toronto.edu
To: Muhammad Khan <mskhan6@illinois.edu>, Nitin Vaidya <nitin.vaidya@georgetown.edu>

Dear authors,

The program committee for the 38th ACM Symposium on Principles of Distributed Computing (PODC 2019) is happy to inform you that your paper

#138 Exact Byzantine Consensus on Undirected Graphs under Local Broadcast Model

has been accepted. Only 50 regular papers from among 173 submissions were accepted. Your paper will be allocated a 20 minute talk at the conference and up to 10 (double column) pages in the proceedings. The camera ready version of your paper is due by May 27.

Reviews of your paper are appended to this email.

Contact Faith Ellen <faith@cs.toronto.edu> with any questions or concerns.

-PODC 2019 Program Committee

Review #138A
==========

Paper summary

Considers Byzantine agreement in an incomplete graph with local broadcast, which means that any message sent by a process (including by faulty processes) is delivered to all neighbors. Shows that with f faults, Byzantine agreement is possible if and only if the minimum degree is at least $2f$ and the vertex connectivity is at least $\lfloor 3f/2 \rfloor + 1$. For the upper bound, the paper gives an exponential-time algorithm that exactly matches the lower bound, and a linear-time algorithm that works with vertex connectivity $2f$. Some additional results are provided for a hybrid model that allows some faulty nodes to deliver different messages to different neighbors.

Positive Qualities of the Paper

Solid, well-written paper that gives a tight characterization of solvability of Byzantine agreement in a natural model.

* *

Review #138B
==========

Paper summary

This paper investigates binary consensus in an arbitrary network where nodes may be Byzantine and communication proceeds in synchronous broadcasts with neighbors, i.e., the local model.
It provides necessary conditions on the graph G for solving consensus in the local broadcast model: 1) node degree of at least 2f and 2) connectivity of at least floor(3f/2)+1.
Those conditions are shown to be sufficient as they describe an exponential algorithm that solve consensus under the 2f-degree and floor(3d/2)+1 condition. Additionally, when the underlying communication graph is 2f-connected, a linear algorithm algorithm. The main construction of the algorithm is to show that it is possible to implement reliable communication between any two nodes in at least one direction, using a clever observation on the failure model combined with the communication model.

The paper also introduces equivocation in a hybrid model where a new parameter, t, counts the number of nodes that may equivocate, i.e., not using local broadcast. Equivocation is not a classical notion, and the definition: "a message sent by any node is received identically by all of its neighbors in the communication network. Thus, under the local broadcast model, attempts by a node to equivocate (i.e., send conflicting information to its neighbors) can be detected by its neighbors." is not really clear at first sight. The hybrid model gives a "slider" between t=0, the local model, and t=f, the classical byzantine model with point to point communication. In the hybrid model, they also provide necessary and sufficient conditions for solving consensus: 1) floor((3(f-t)/2)+2t+1)-connectivity, 2) 2f degree if t=0 and 3) every nonempty set of at most t nodes has at least 2f+1 neighbors when t>0.

The main paper (excluding the appendices) is nicely structured and explains the main results on well chosen examples, in a didactic way. The observation that 1 way reliable communication can be implemented should be made more explicit since it is crucial for the results and the provided algorithm.

To conclude, the article presents strong results on an important problem covering two traditionally disjoint communities (consensus/local). As the authors point, their result help to understand different tradeoffs and their hybrid model provides interesting insights on the relationship between point to point and local models.

Positive Qualities of the Paper

- The paper is clear and nicely structured.
- Strong results on an important problem covering two traditionally disjoint communities (consensus/local)

Negative Qualities of the Paper

- The appendices are very long (full paper is 29 pages) and raise the question of what could and should be published in the proceedings.

* *

Review #138C
==========

Paper summary

The authors study Byzantine consensus in arbitrary graphs under the constraint that (some or all) of the faulty nodes communicate by broadcasts, i.e., cannot equivocate. They establish tight bounds on the resilience that can be achieved and (as the corresponding positive result has exponential running time) provide polynomial time algorithm under a slightly stronger bound on the number of faulty nodes.

Positive Qualities of the Paper
---
1. The paper is well-written, which (based on some sampling) appears to extend to the proofs in the appendix.
2. I found it interesting and somewhat surprising that connectivity of 2f or 2f+1 is not needed. The paper does a good job in clarifying why this initial expectation is incorrect, by providing intuition for how a smaller bound can be achieved (and, of course, an algorithm and proof).

Negative Qualities of the Paper

I find it difficult to get excited about the novelty and technical contribution of the paper. Phrased negatively, the paper studies yet another variant of consensus, applies the standard tools, and then gets the respective results. (Nonetheless, I'd like to stress that the technical contribution is solid.)

Detailed technical comments

As (regrettably) I did not spend a lot of time with the appendix, I have few remarks here.

- While I can see why you define disjointness of uv-paths and Uv-paths as you do, this results in disjointness of paths depending on which specialization is currently used: Two disjoint uv-paths are not disjoint {u}v-paths. Do you see a way out of this that does not become to cumbersome?
- After Theorem 6.1, when discussing the case of t=f, you state that "condition (iii) combined with (i) is equivalent to n >= 3f+1." This is incorrect, as the former does not follow from n >= 3f+1, so I assume that you're actually trying to say that the former *implies* the latter. But even then (i) is not required: Applying (iii) to the empty set (or a singleton) shows that there are at least 2f+1 nodes, and applying it again for |S|=f yields that there are at least 3f+1 nodes.

Committee Decision

The reviewers largely agreed in their evaluation. However, the second reviewer's criticism about the length of the appendix was opposed by some PC members. The paper was discussed in the
PC meeting and was accepted, although it did not have very strong support.