1 Context

Following the setting of the seminal paper of Lamport et al. [13], many subsequent papers focusing on
Byzantine tolerance [2, 14, 15, 17, 18] study agreement and reliable communication primitives using
cryptography-free protocols in networks that are both static and fully connected. An important line
of research assumes the existence of $2k + 1$ node-disjoint paths from source to destination, in order
to provide reliable communication in the presence of up to $k$ Byzantine failure [10, 9, 19]. However,
these results rely on Menger’s theorem [3], which can be informally expressed as follows: we have $x$
disjoint paths between two nodes if and only if $x$ nodes must be removed to disconnect these two nodes.
This theorem only applies to static networks. None of the aforementioned papers considers genuinely
dynamic networks, i.e., where the topology evolves while the protocol executes.

In a seminal paper [16], Maurer et al. considered the following problem: two nodes want to reliably
communicate in a dynamic multi-hop network where a subset of the nodes are Byzantine. As Menger’s
theorem does not extend to dynamic networks [11], Maurer et al. [16] proved a new necessary and
sufficient condition (in other words, the weakest possible condition) for enabling reliable communication
in a dynamic multi-hop network where a subset of the nodes are Byzantine. Their proof is constructive,
as they provide a Byzantine-resilient algorithm for reliable communication that is optimal with respect
to their impossibility result. However, their algorithm requires an exponential computation at every node
upon receipt of every message, hindering its practical relevance.

Scientific lock: Overall, to date, for dynamic networks, no tractable (that is, polynomial) solution
exists for reliable communication with Byzantine attacks.

2 Methodology and Organization

The first challenge to solve is a tractable Byzantine broadcast algorithm. Although the condition pro-
vided by Maurer et al. [16] is the best possible from a theoretical point of view, it lacks practicality. That
is, verifying their condition requires to run at each node upon each message reception an exponential
time algorithm to compute the minimal node-cut of the received paths attached to received messages.
As our preliminary results suggest that computing the minimal dynamic cut in dynamic networks using
received paths attached to messages is at least NP-complete, one option is to investigate approxima-
tion algorithms. However, as we do not want to compromise safety, the approximation should always
be lower than the actual minimal dynamic cut. One trivial such approximation is the number of node
disjoint-paths among the received paths, but there exist dynamic networks where no two dynamic paths
are node-disjoint [11], so the computed dynamic minimal cut would be 1, resulting in no genuine mes-
sage being delivered even if at most one Byzantine node is in the network, that is, a loss of liveness.
Designing a polynomial approximation for the dynamic minimal cut problem that compromises neither safety nor liveness of the resulting broadcast algorithm is an obvious first goal.

The second goal is to investigate the orthogonal approach of using a purely local Byzantine-resilient broadcast algorithm, that is, an algorithm that does not store traversed paths with each message. In static networks, this approach was promoted as the Certified Propagation Algorithm (CPA) [12, 20, 21]: if sufficiently many neighbors broadcast the same message, then it is safe to re-broadcast it. For example, if at most \( k \) Byzantine nodes can be neighbors of a particular node, then it is safe to re-broadcast it once received \( k + 1 \) copies of the same message from different neighbors. Of course, the necessary and sufficient conditions induced by local algorithms are different from the global ones (we go from a global requirement on the number of Byzantine attackers to a local requirement about the neighborhood of each node), but not necessarily less useful as they are intrinsically polynomial locally. A first step in this direction was initiated by Bonomi et al. [5] for a limited set of (unpractical) dynamic networks. Another approach by Dobrev et al. [8] consider the broadcast problem in the context of dynamic edge faults, that are a strict subset of Byzantine failures. So, our second goal in this task will be to fully characterize the CPA approach in dynamic networks. This is likely to promote a new set of lower and upper bounds, expressed with local metrics, for polynomial broadcast algorithms.

We expect the outputs of the first two goals (a global approximation approach, and a local exact approach) to be incomparable from a theoretical point of view, as their constraints (on the number and placement of Byzantine) are not comparable. However, it makes sense to assess their relevance from a practical point of view, using data from real dynamic networks. We plan to devise a set of implementation-level optimizations for algorithms developed in goals 1 and 2, following the line of work initiated by our recent work [6, 4], but also general optimizations for long-lived executions [7]. Furthermore, we will first use the traces of dynamic networks available at the CRAWDAD [1] archive: e.g. mobility and connectivity traces extracted from GPS traces from the regional Fire Department of Asturias, social interactions and propinquity based on wireless and bluetooth, mobility traces of taxis in Rome, etc. Then, we will benchmark the algorithms obtained from Task 1.1 using the same set of traces for each algorithm, and measure the following metrics: (i) number of safety violations (that is, the number of fake messages delivered), (ii) number of liveness violations (that is, the number of nodes that do not deliver a genuine message), (iii) time to complete a single broadcast, (iv) time to complete a series of \( m \) broadcasts.

Obiously, a difficult setting in the evaluation is the placement of Byzantine attackers, as it may have a dramatic impact on the performance of the protocols. We expect to start with a random placement and run sufficiently many evaluations to have high confidence intervals. However, we also assume that the first results will mandate additional iterations of experiments as we gain insight about the worst case Byzantine placement.

3 Practicalities

The PhD will be located in LIP6 laboratory in Paris, France. Part of the research will be done in cooperation with colleagues in Japan (Xavier Défago at TokyoTech, Toshimitsu Masuzawa at Osaka University).

References


