Report
Internship LIP6

August 11, 2021

Authors :
Osama Rashid
Hamed Nazim Mamache
Gabin Mazué

Tutor:
Maria Potop-Butucaru
Supervised by:
Gewu BU

Contents

Chapter 1

Fast Probabilistic Consensus

1.1 Parameters

- N : number of nodes of the network
- Quorum size : number of nodes that each node will have to query
- τ : initial threshold
- β : parameter of the uniform law
- l : number of rounds for a node to be finalized
- D : distance chosen for the random walks
- M : maximum number of rounds for the algorithm

1.2 Protocol of the Consensus

The Fast Probabilistic Consensus is a consensus algorithm based on queries. It has been proven in the Coordicide that this algorithm has a lot of potential, it was shown that in most cases, the network will converge towards the majority's opinion however, this is not mandatory. Each node will start with an initial opinion which corresponds to the round 0, this opinion will be chosen randomly given a probability P_0, then it will do the following actions:

- Launch a certain number of random walks at each discrete time t (the protocol of the random walk will be explained in details in the next section)

- Wait for the chosen nodes to respond and give their opinions
- Calculate the mean of the opinion received

One the node has calculated the mean, if it is the first round, he will compare it to the threshold τ, if the mean is bigger then his opinion becomes 1, otherwise it becomes 0. However, if it is not the first round, then the node will generate a random variable U_t following a uniform law between $[\beta, 1-\beta]$. If the mean is bigger than U_t, the opinion becomes 1, if it is smaller, the opinion becomes 0 and if it is equal, the opinion stays the same as the previous round. The node will then check whether its current opinion is the same as the previous one, if it is the same he wil increment a variable named "count", otherwise, he will reset it to 0. This variable will allow the node to finalize its opinion if the counter reaches L.

1.3 Protocol of the Random Walk

When a node will need to do a random walk of a certain distance, it will choose randomly between one of its neighbors and send a message containing the list of visited nodes and the distance decremented of 1. At this point , the list will only have the node that launched the random walk. Once the node receives that message, it will whether the distance remaining is greater than 0, if it is, he will add himself in the list of visited nodes, and send a message to one of its neighbors. This neighbor is chosen uniformly between the neighbors that have not already been visited so that no random walk can go through the same node twice. If all of the neighbors have already been visited, then the random walk stops. The random walk can also stop when the remaining distance reaches 0.

We also worked on randoms walks using Tabu lists, however this type of random walk did not improve the outcomes of the algorithm. This is easily explainable because the advantage of Tabu lists is that it prevents the visited list to be too big, however this problem does not happen here. Indeed the list is already restricted by the distance.

Chapter 2

Cellular Consensus

2.1 Presentation

The Cellular Consensus is a cellular automata based on the approach of majority dynamics. Each node acts as a cellular automaton, that changes its opinion in case of conflict with his neighbors and adopt the majority opinion. This cellular automata implementation brings the following novel key properties :

- During the execution of the algorithm, the network is supposed irremovable, so the set of neighbors of a node does not change too.
- When a node have to evaluate the opinion given by one of his neighbors, he needs a "proof" materialized by the opinions of the neighbor's neighbors. This will allow the network's nodes to monitor each other and to detect if someone is lying independently of its neighbors.
- If this "proof" shows that the neighbor is lying, it will immediately be blacklisted by the node and none of his opinions will be taken into account.
- Time is considered discrete so the algorithm works round by round.

At the beginning of each round, every node send a "heartbeat" of its signed current opinion and the opinions from the previous round of his neighbors, each signed by the issuing node.

Since the previous opinions of the neighbors cannot be faked, every nodes can validate that the received opinion is indeed correct.

We formalize the above ideas in the consensus protocol described below.

2.2 Algorithm and Parameters

Consider a network composed of N nodes, and suppose that each node is directly connected to its k neighbors. Let us note N_i the set of neighbors of the node i. The "automatic verification" mechanism is a key mechanism for the security of this algorithm, since a malicious node must not be able to influence its neighbors.
At each step of the algorithm, each node holds an opinion. The opinion can be 0, 1 or -1.

Indeed, if the majority opinion of N_i neighbors of i in round m is:

- 0, then the opinion of i in round $m + 1$ will be 0,
- 1, then the opinion of i in round $m + 1$ will be 1,
- non-existent (i.e. there is no majority opinion), then the opinion of i in round $m+$ 1 will be -1.

The opinion of node i at round m is then denoted $X_m(i) \in \{0, 1, -1\}$.

We suppose that the state of each node i is initialized to an opinion $X_0(i) \in \{0, 1\}$, according to a certain probability P_0 that we can vary.

The algorithm takes the following parameters as arguments:

- $N \in \mathbb{N}$, number of nodes,
- $k \in \mathbb{N}$, number of neighbors of each node,
- $M \in \mathbb{N}$, maximum number of rounds,
- $l \in \mathbb{N}$, the number of consecutive rounds with the same opinion before the opinion of a node becomes **final**.
- $p : \{0, ..., k\} \to \mathbb{R}_{\geq 0}$, increasing monotonic weight function n that maps the number of neighbors to a weight. This function **penalizes** the nodes with the fewest neighbors.

Each node i knows the opinions of its neighbors $j \in N_i$ as well as the opinions of all their neighbors N_j. Indeed, these opinions are necessary and imperative for the functioning of the mechanism formalized by the "heartbeat" algorithm, as we can see below.

Algorithm 1: Heartbeat, The Coordicide - IOTA

```
Input: Node i, Round m
Output:
for ∀ neighbor $j \in N_i$ do
    Send opinion $X_m(i)$ to neighbor $j$
    for ∀ $j' \in N_i \backslash \{j\}$ do
        Sending opinion $X_{m-1}(j')$ to neighbor $j$
    end
end
```

As we could see previously, the consensus mechanism is a cellular automaton where a node uses the opinions of its neighbors to update its own state:
When the majority of neighbors support either 0 or 1, the node adopts this opinion. If neither of these opinions has a majority, the node adopts third opinion -1 (i.e. none of them).
Knowing that we assume the set N_i known at least for all its neighbors i, any node can use these simple rules to validate whether the opinion of neighbor i is consistent with the majority opinion of the set nodes $\in N_i$.

The cellular consensus mechanism is more formally illustrated in the following algorithm:

Algorithm 2: Cellular Consensus, The Coordicide - IOTA

```
for each node $i$ do
    Send initial opinion $X_0(i)$ to neighbors $N_i$
end
for $m \in [1; M]$ do
    for each node $i$ do
        for each neighbor $j \in N_i$ do
            if $X_{m-1}(j)$ is inconsistent wrt $X_{m'}(j')$ for $j' \in N_j, m' < m-1$ then
                \\ drop neighbor $j$
                $N_i \leftarrow N_i \backslash \{j\}$
            end
        end
        if node $i$ is finalized then
            Opinion $X_m(i) \leftarrow X_{m-1}(i)$
        end
        else
            $total \leftarrow \sum_{j \in N_i} p(|N_j|)$
            if $\sum_{\{j \in N_i | X_{m-1}(j)=0\}} p(|N_j|) > \frac{total}{2}$ then
                $X_m(i) \leftarrow 0$
            end
            else
                if $\sum_{\{j \in N_i | X_{m-1}(j)=1\}} p(|N_j|) > \frac{total}{2}$ then
                    $X_m(i) \leftarrow 1$
                end
                else
                    $X_m(i) \leftarrow -1$
                end
            end
        end
        heartbeat($i$,$m$);
        if opinion $X(i)$ has not changed since $l$ tours then
            Mark node $i$ as finalized
        end
    end
end
```

Chapter 3

Topology Presentation

3.1 2D Grid

The first topology studied is the simplest of all. We consider a grid / "matrix", which contains nodes. Each nodes' neighbors will be those adjacent to them. Their number therefore varies according to the position of the node in the grid. Indeed, if a node ends up in a corner, it will only have 2 neighbors. Also, if it ends up on an edge, it will have 3 neighbors. Finally, if this one is in the "center" of the grid, it will have 4 neighbors.

3.2 Torus

The second topology studied is an improvement of the 2D grid and avoids getting stuck in the corners and on the edges. To do this we will transform our grid into a torus. We are therefore going to connect the top and bottom edges together, and repeat the same process for the right and left edges. By connecting the edges between them, we add neighbors to the nodes which are in the corners and on the edges. Indeed, if we are in the top left corner, we add the bottom left corner and the top right corner to the list of our neighbors. If we are on an edge, we add the node which is on the opposite edge. Finally, if we are located in the "center", nothing changes. The number of neighbors is therefore equal to 4 for any node in the network.

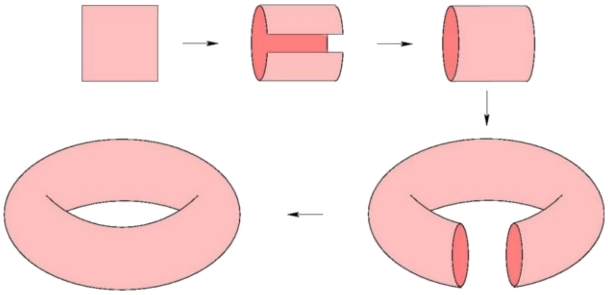


Figure 3.1: Transformation of a 2D grid into a torus

3.3 Watts-Strogatz model graphs

The Watts-Strogatz model is a graph generation model, possessing the small world property (the computation of the shortest path between two nodes is logarithmic). This method takes in parameters N the number of nodes, K the average degree of the nodes in the network and P the probability allowing to change the edges. The goal of the process is to start from a ring graph in order to process every edge of a node. Indeed, each edge can change recipient with the probability P passed as a parameter.

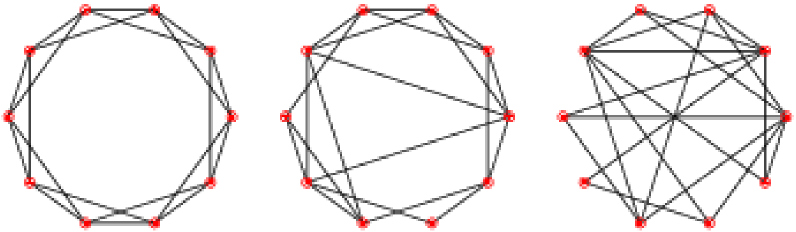


Figure 3.2: Watts-Strogatz method process

Chapter 4

Byzantines adversaries

In order to simulate possible attacks and predict critical security cases, three adversary profiles called malicious nodes, liars or byzantine nodes were imagined (and therefore implemented):

4.1 Cautious adverseries

These nodes are able to lie on every round of the process with a probability P_{lie}. However, the opinion sent during the different polls during a unique round is still the same. For example, if one of these nodes is requested during a poll and the opinion sent is 1, then if it is requested again during the same round, it will again send opinion 1. However, this opinion may therefore turn out to be false.

4.2 Semi-Cautious adverseries

This node will not lie, however, it is capable of not responding to a node during a poll, with a probability $P_{silence}$, thus delaying the process of network convergence. These nodes can also be assimilated to slow nodes that are not necessarily malicious but are still slowing down the network.

4.3 Berserk adversaries

This node is similar to Cautious adversaries except that it is able to give different responses in the same round. Thus, within the same round but in different polls, it can send his true opinion, then lie and give the wrong opinion. In theory, they represent the greatest threat because of their very unpredictable character and their great freedom.

Chapter 5

Simulation results

Throughout this part, we will present the results of the 2 different algorithms by varying different parameters.
Note that, in the following simulations, we noticed that there was no difference between berserk adversaries and Cautious adversaries when considering the convergence results.
We therefore consider that berserk adversaries have the same convergence results as Cautious adversaries, which seems logical, because in the long run, both malicious nodes will have lied to the network the same amount of time. If we consider M the number of rounds and X the number of queries that the malicious node will receive per round on average, a Cautious adversary will lie in $\frac{M}{2}$ rounds which makes an average amount of lies of $\frac{MX}{2}$. As for the Berserk adversary, he will lie in average $\frac{X}{2}$ regardless of the round which also makes a total of $\frac{MX}{2}$ lies.

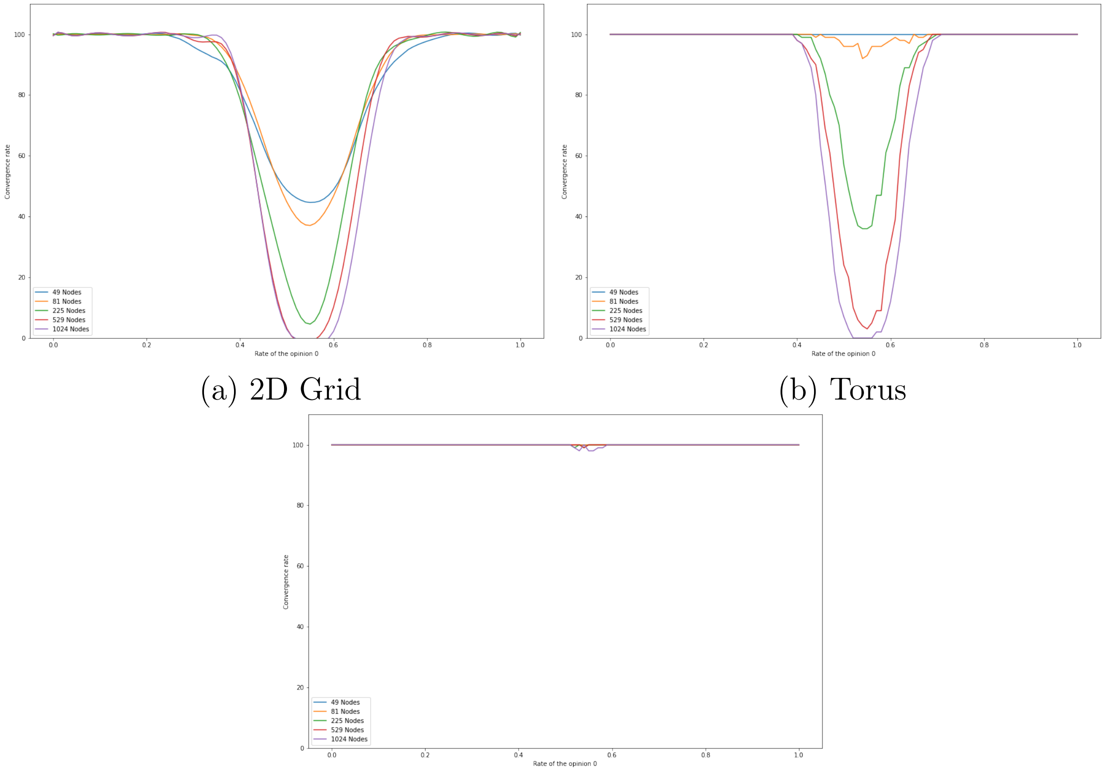
5.1 Fast Probabilistic results

5.1.1 Percentage of convergence according to the initial division probability P_0 for different network sizes without malicious nodes

Parameters

- Number of nodes of the network : $49 \leq N \leq 1024$,
- Distance of the random walks : $D = 4$
- Number of nodes queried by each node : Quorum size $= 10$

- Initial threshold : $\tau = 0.5$
- Uniform law parameter : $\beta = 0.25$
- Number of rounds : $M = 30$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 0\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 10$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

Figure 5.1: Percentage of convergence according to the initial division probability P_0 for different network sizes, without malicious nodes

In these graphs, we looked at the convergence rate according to the initial division probability P_0 in each topology and for different sizes, our goal was to see whether the size of the network had an influence on the convergence rate. As we can see in those graphs, for the grid and the torus, it does have a major impact, the more nodes we have, the less it converges. This means that if we want these network topologies to converge, we need to have smaller sizes. However, even with small sizes, it does not converge enough to be considered efficient. On the contrary, the Watts-Strogatz topology seems to be very powerful as the convergence rate is at 100% nearly all the time for every size which means that the size does not affect that topology (or at least it does not affect it enough to be seen here).

5.1.2 Percentage of convergence according to the initial division probability P_0 for different average number of neighbors K in a Watts-Strogatz graph without malicious nodes

Parameters

- Number of nodes of the network : $N = 225$,
- Distance of the random walks : $D = 4$
- Number of nodes queried by each node : Quorum size = 10
- Initial threshold : $\tau = 0.5$
- Uniform law parameter : $\beta = 0.25$
- Number of rounds : $M = 30$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 0\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $4 \leq K \leq 16$, $P = 1$.

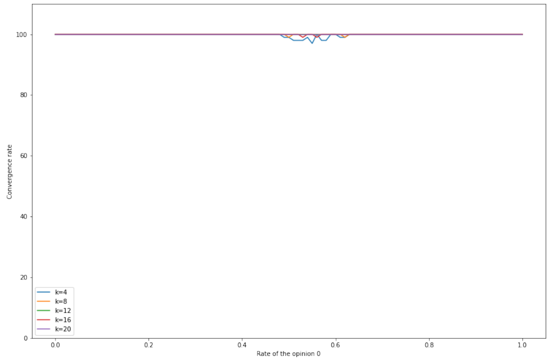


Figure 5.2: Percentage of convergence according to the initial division probability P_0 for different average number of neighbors K in a Watts-Strogatz without malicious nodes

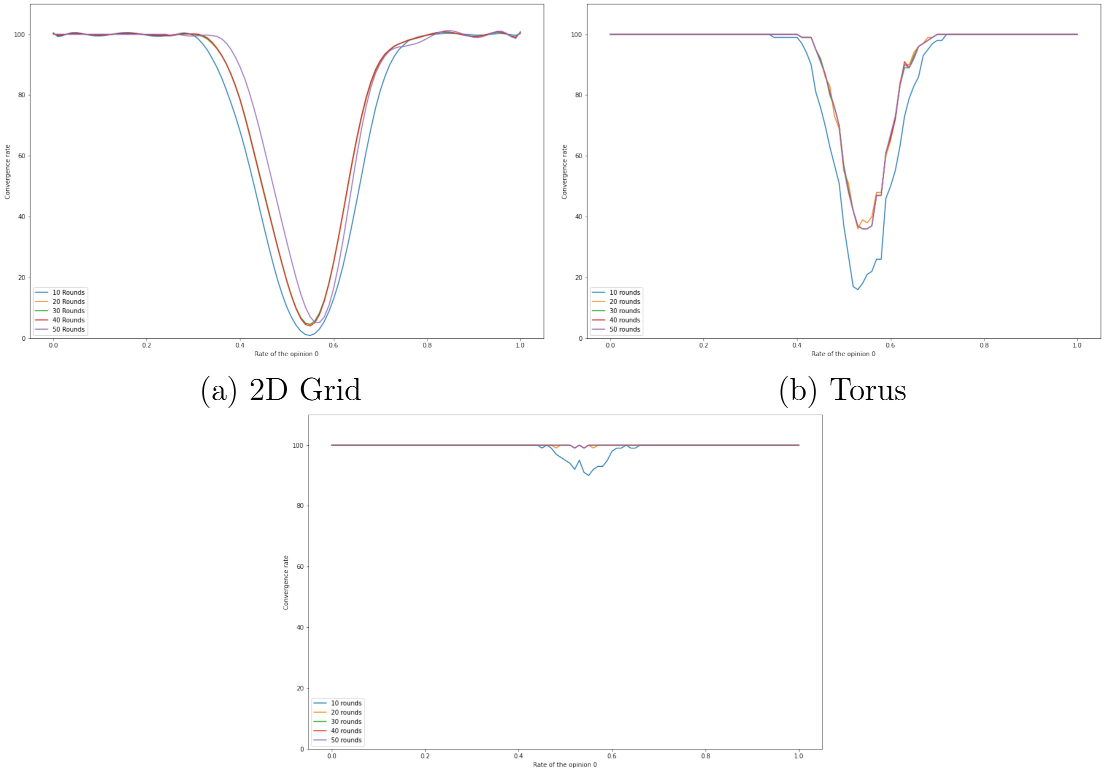
On this graph, we wanted to push the limits of the Watts-Strogatz topology by increasing the average number of neighbors of each node because, in theory, if a node has more neighbors then he should converge more easily towards the majority opinion of the network. We can see that this statement partially true because, for $K = 20$, the network always converges, however, the network had already a good rate of convergence with $K = 4$, this means that, perhaps, if we want to increase the convergence rate, we should look into another parameter.

5.1.3 Percentage of convergence according to the initial division probability P_0 for different number of rounds M without malicious nodes

Parameters

- Number of nodes of the network : $N = 225$,
- Distance of the random walks : $D = 4$
- Number of nodes queried by each node : Quorum size = 10
- Initial threshold : $\tau = 0.5$
- Uniform law parameter : $\beta = 0.25$
- Number of rounds : $10 \leq M \leq 50$,

- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 0\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 10$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

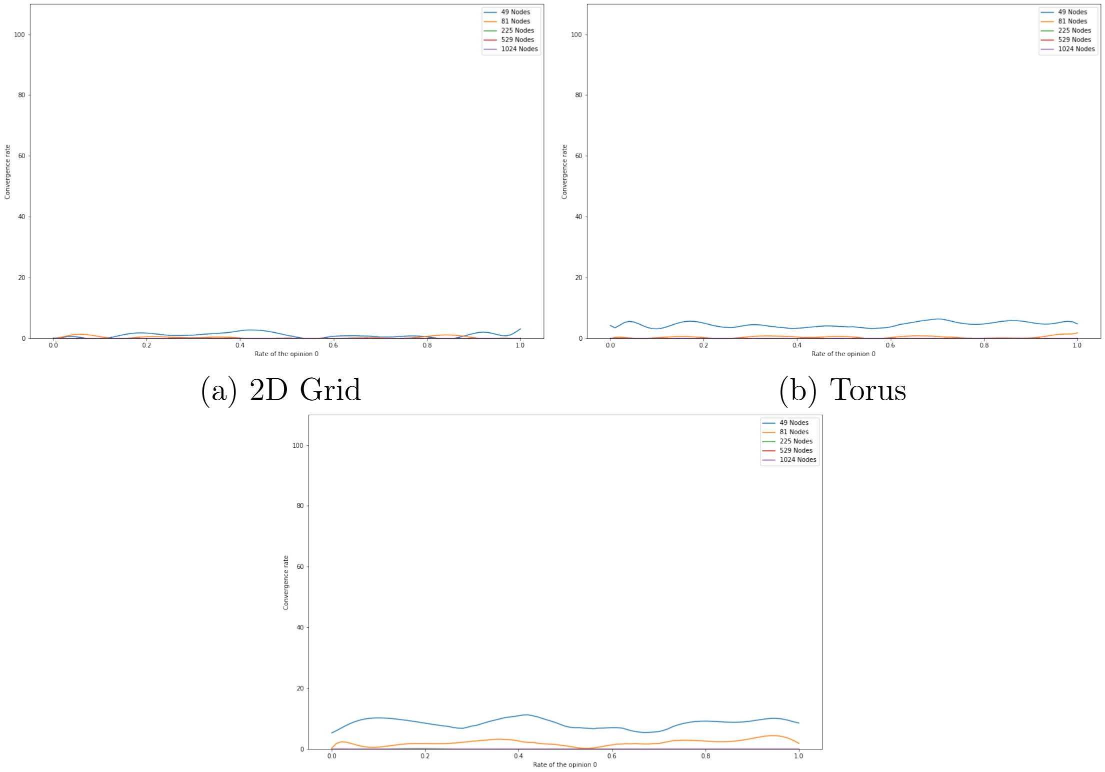
Figure 5.3: Percentage of convergence according to the initial division probability P_0 for different number of rounds M without malicious nodes

These graphs show how the number of rounds can affect the networks, we can observe that at 10 rounds, the network has not been able converge yet, however, from 20 rounds to 50 rounds, we don't see any noteworthy difference, this means that for every topology, 20 rounds is enough to get convergence. In further simulations, we kept 30 rounds just to be sure that the network will have enough time to converge (if it converges).

5.1.4 Percentage of convergence according to the initial division probability P_0 for different network sizes, with Cautious Adversaries

Parameters

- Number of nodes of the network : $49 \leq N \leq 1024$,
- Distance of the random walks : $D = 4$
- Number of nodes queried by each node : Quorum size $= 10$
- Initial threshold : $\tau = 0.5$
- Uniform law parameter : $\beta = 0.25$
- Number of rounds : $M = 30$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 33\%$,
- The lying probability : $P_{lie} = 50\%$
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 10$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

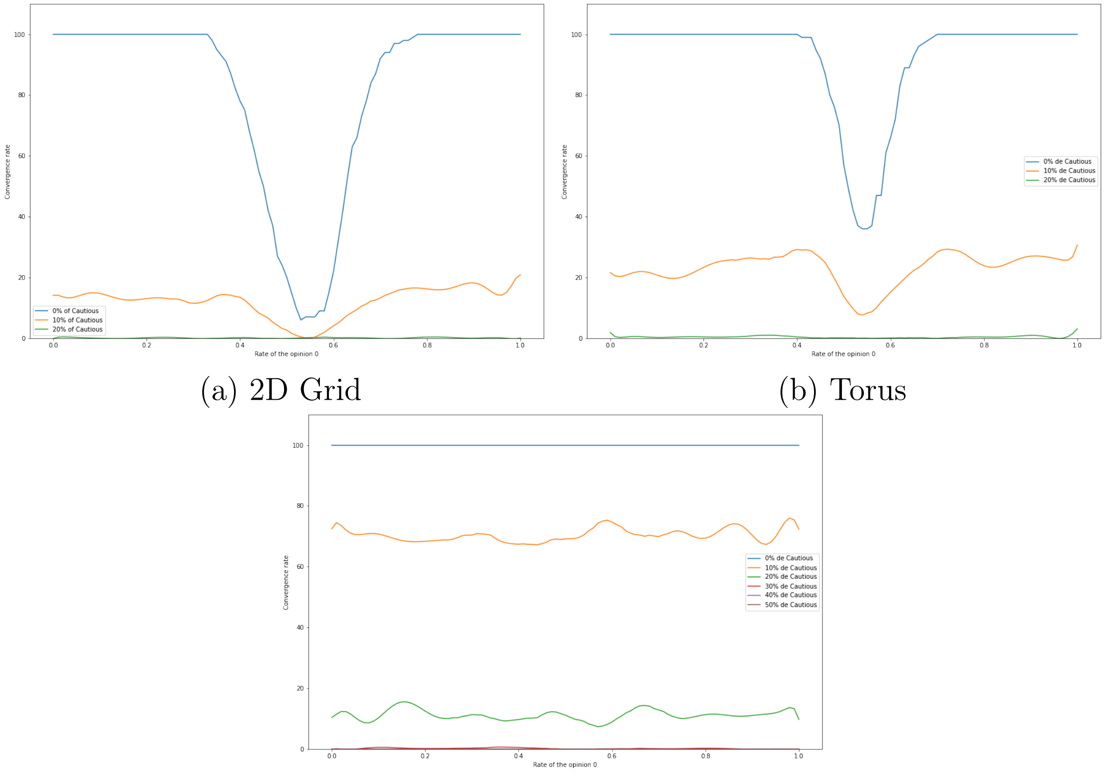
Figure 5.4: Percentage of convergence according to the initial division probability P_0 for different network sizes, with Cautious Adversaries

As we can see on these graph, when the network has 33% of Cautious adversaries, the convergence rate drops dramatically for every topology, this shows a significant weakness of the FPC, this consensus algorithm does not work if the network is corrupted with an important amount of malicious nodes. This is due to the fact that the Cautious adversaries have the time to spread their lies across the network when nodes asks their opinions by queries. Now that we saw the impact of a certain percentage of Cautious adversaries, we are going to look at how the networks reacts as we introduce more and more malicious nodes.

5.1.5 Percentage of convergence according to the initial division probability P_0 for different percentage of Cautious adversaries $P_{malicious}$

Parameters

- Number of nodes of the network : $N = 225$,
- Distance of the random walks : $D = 4$
- Number of nodes queried by each node : Quorum size $= 10$
- Initial threshold : $\tau = 0.5$
- Uniform law parameter : $\beta = 0.25$
- Number of rounds : $M = 30$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $0\% \leq P_{malicious} \leq 20\%$ (to 50% for Watt-Strogatz),
- The lying probability : $P_{lie} = 50\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 20$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

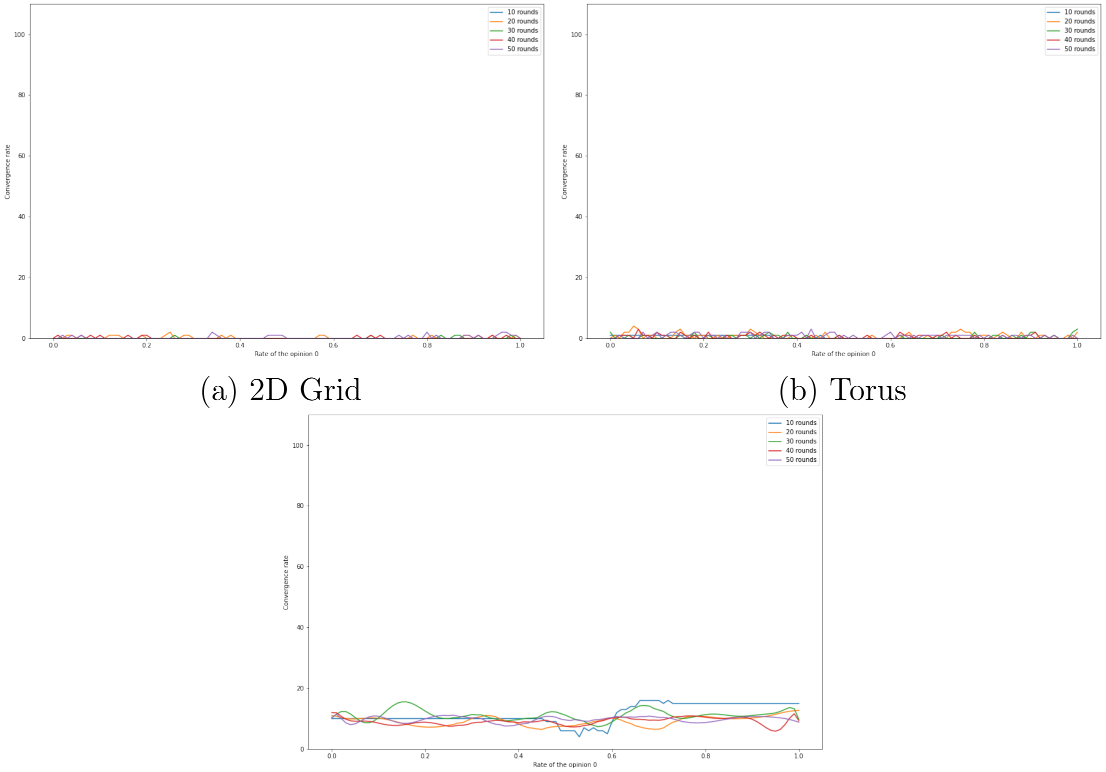
Figure 5.5: Percentage of convergence according to the initial division probability P_0 for different percentage of Cautious adversaries $P_{malicious}$

On these graphs, we can clearly notice a very big difference between 0% and 10% of Cautious adversaries, it shows that the network is already corrupted with only 10% for the grid and the torus, whereas it is just under 80% for Watts-Strogatz graphs, it supports more and more the argument that Watts-Strogatz is the best topology for networks even though the convergence rate is catastrophic at 20% of malicious nodes for all topologies. This is a proof that the network cannot withstand more than 10% of Cautious adversaries which is clearly not secure enough.

5.1.6 Percentage of convergence according to the initial division probability P_0 for different number of rounds M, with Cautious adversaries

Parameters

- Number of nodes of the network : $N = 225$,
- Distance of the random walks : $D = 4$
- Number of nodes queried by each node : Quorum size $= 10$
- Initial threshold : $\tau = 0.5$
- Uniform law parameter : $\beta = 0.25$
- Number of rounds : $10 \leq M \leq 50$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 20\%$,
- The lying probability : $P_{lie} = 50\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 20$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

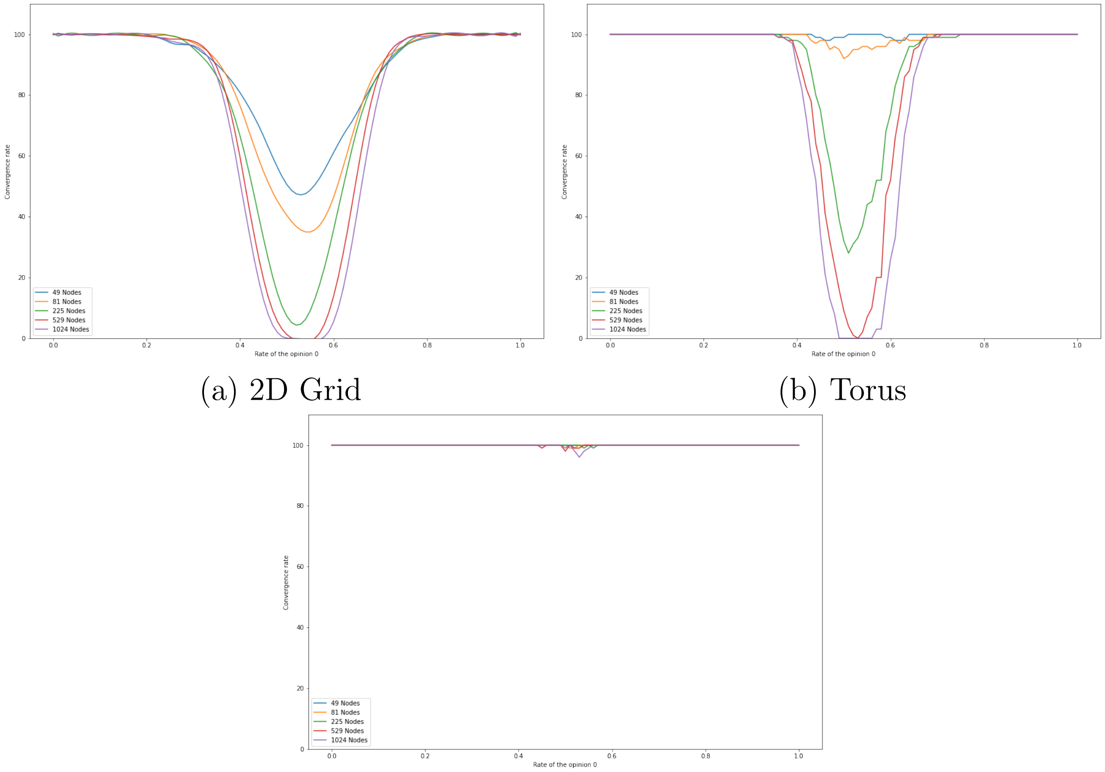
Figure 5.6: Percentage of convergence according to the initial division probability P_0 for different number of rounds M, with Cautious adversaries

After we saw that a percentage beyond 10% of Cautious adversaries was too much for the network, we wanted to see whether it was because the network did not have enought time to converge or if the number of rounds did not matter and the network would never converge even with a high number of rounds. As we can see, the number of rounds does not have an impact on the convergence, the Cautious adversaries are too powerful and will not let the network converge in either topology. It confirms the fact that beyond 10%, the network cannot have a good rate of convergence with these parameters.

5.1.7 Percentage of convergence according to the initial division probability P_0 for different network sizes, with Semi-Cautious Adversaries

Parameters

- Number of nodes of the network : $49 \leq N \leq 1024$,
- Distance of the random walks : $D = 4$
- Number of nodes queried by each node : Quorum size $= 10$
- Initial threshold : $\tau = 0.5$
- Uniform law parameter : $\beta = 0.25$
- Number of rounds : $M = 30$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 33\%$,
- The lying probability : $P_{lie} = 50\%$
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 10$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

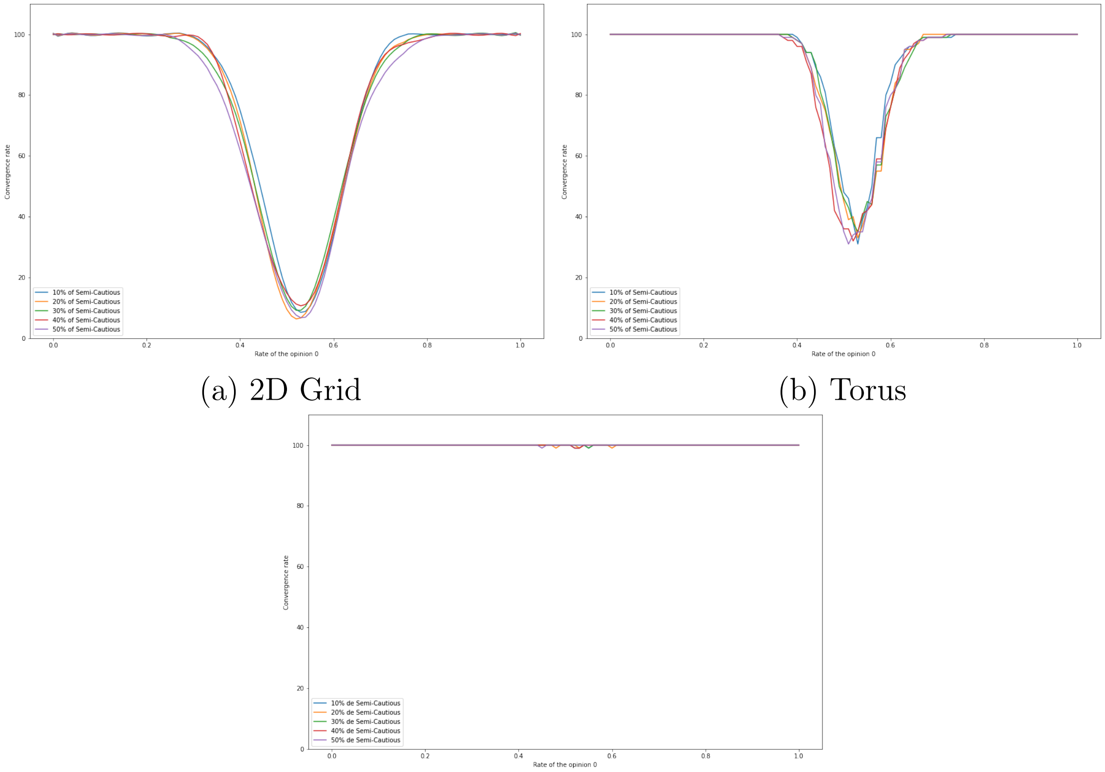
Figure 5.7: Percentage of convergence according to the initial division probability P_0 for different network sizes, with Semi-Cautious Adversaries

Previously, we saw the impact of Cautious adversaries on the different topologies, now we are going to study the impact of Semi-Cautious adversaries. We an observe that for each topology, Semi-Cautious adversaries do not have much of an impact, it seems that the curves are the same as when they were no malicious nodes, this can be explained by the fact that Semi-Cautious adversaries do not lie, they just do not answer sometimes which does not corrupt the network. In theory, it should only slow down the network so the next graphs that we will see are going to make the percentage of Semi-Cautious vary and see if a big amount makes a difference or not.

5.1.8 Percentage of convergence according to the initial division probability P_0 for different percentage of Semi-Cautious adversaries $P_{malicious}$

Parameters

- Number of nodes of the network : $N = 225$,
- Distance of the random walks : $D = 4$
- Number of nodes queried by each node : Quorum size = 10
- Initial threshold : $\tau = 0.5$
- Uniform law parameter : $\beta = 0.25$
- Number of rounds : $M = 30$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $0\% \leq P_{malicious} \leq 50\%$
- The silence probability : $P_{lie} = 50\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 20$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

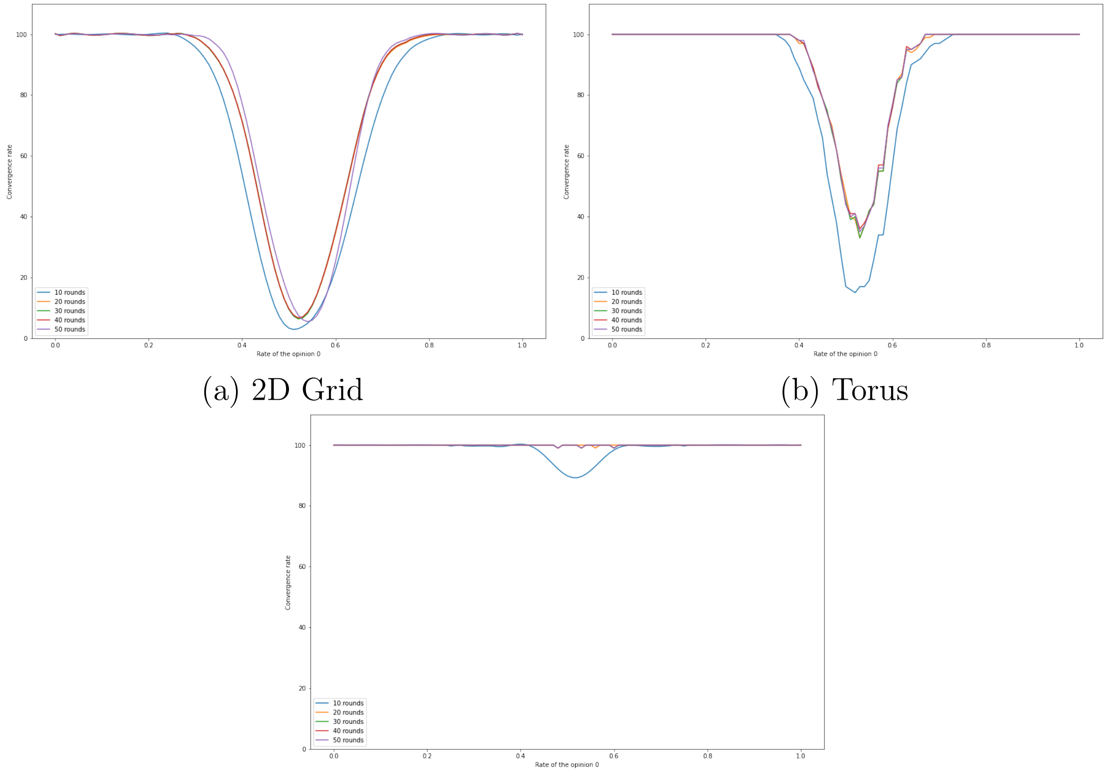
Figure 5.8: Percentage of convergence according to the initial division probability P_0 for different percentage of Semi-Cautious adversaries $P_{malicious}$

When the percentage of Semi-Cautious adversaries increases, we do not see any notable difference in the convergence rate, apart from a slight decrease. This means that the number of Semi-Cautious adversaries in the network does not affect the convergence, hence we can conclude on the fact that these types of malicious nodes are the least dangerous for the network. It also shows that if some devices are slow and they can't respond to the queries in time (this type of behaviour is similar to being a Semi-Cautious adversary), the network will not be put at disadvantage because of these devices. Moreover, we think that the slight decrease is due to the fact that Semi-Cautious adversaries might slow down the network so, maybe, 30 rounds is not enough anymore for the network to converge. This is why we will see the impact of the maximum number of rounds on the next graphs.

5.1.9 Percentage of convergence according to the initial division probability P_0 for different number of rounds M, with Semi-Cautious adversaries

Parameters

- Number of nodes of the network : $N = 225$,
- Distance of the random walks : $D = 4$
- Number of nodes queried by each node : Quorum size = 10
- Initial threshold : $\tau = 0.5$
- Uniform law parameter : $\beta = 0.25$
- Number of rounds : $10 \leq M \leq 50$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 20\%$,
- The silence probability : $P_{lie} = 50\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 20$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

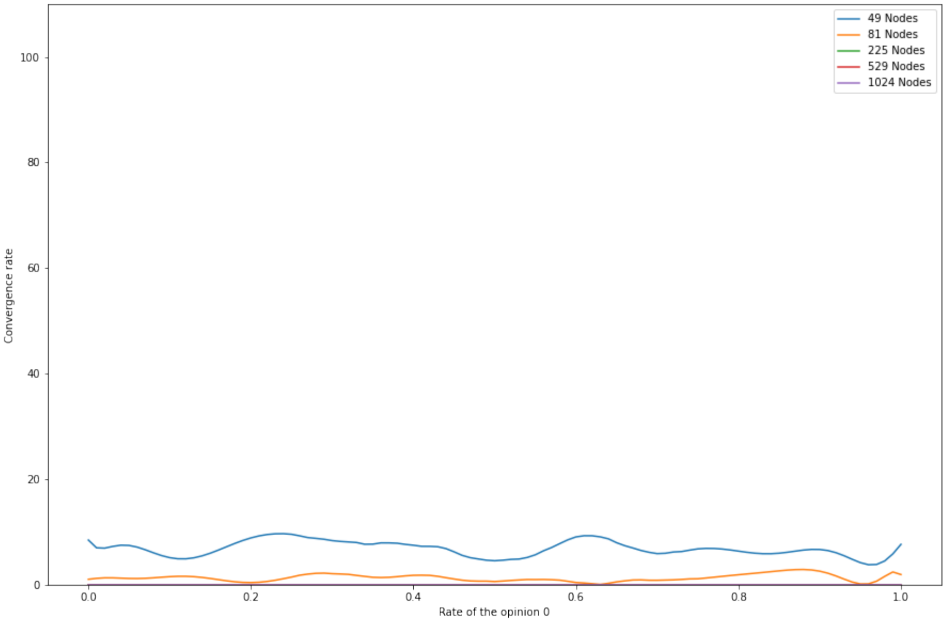
Figure 5.9: Percentage of convergence according to the initial division probability P_0 for different number of rounds M, with Semi-Cautious adversaries

Previously, we saw that the number of rounds did not matter with Cautious adversaries because they corrupted the network anyways, so in this figure we are going to check if it matters with Semi-Cautious adversaries. We also saw that with Semi-Cautious adversaries, the network acted like they were not any malicious nodes, this is again verified because we can notice that from 20 to 50 rounds, there is not any noticeable difference for either topology which is the same observation we got without malicious nodes. To conclude on Semi-Cautious adversaries, we can say that they are the least dangerous malicious nodes, they do not corrupt the network even though they can slightly decrease the convergence rate.

5.1.10 Percentage of convergence according to the initial division probability P_0 for different network sizes, with Berserk Adversaries

Parameters

- Number of nodes of the network : $49 \leq N \leq 1024$,
- Distance of the random walks : $D = 4$
- Number of nodes queried by each node : Quorum size $= 10$
- Initial threshold : $\tau = 0.5$
- Uniform law parameter : $\beta = 0.25$
- Number of rounds : $M = 30$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 33\%$,
- The lying probability : $P_{lie} = 50\%$
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 10$, $P = 1$.



(a) Torus

Figure 5.10: Percentage of convergence according to the initial division probability P_0 for different network sizes, with Berserk Adversaries

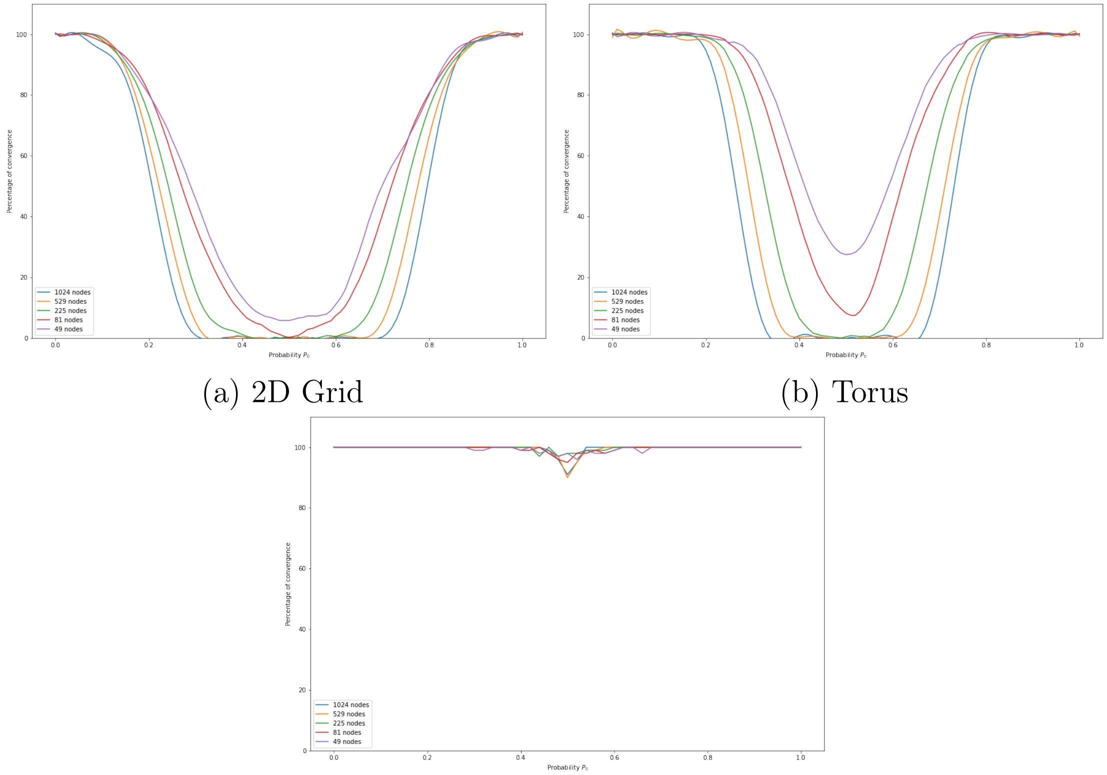
We said that the Berserk adversaries worked the same say as Cautious adversaries, so in this graph, we check that our theory was true, we can see that the graph is very similar to the one with Cautious adversaries, this supports our theory that both have the same effect on the network, this is why we decided not to other graph with Berserk adversaries since it would have been very similar results.

5.2 Cellular Consensus results

5.2.1 Percentage of convergence according to the initial division probability P_0 for different network sizes N, without malicious nodes

Parameters

- Number of nodes of the network : $49 \leq N \leq 1024$,
- Number of rounds : $M = 20$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 0\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 10$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

Figure 5.11: Percentage of convergence according to the initial division probability P_0 for different network sizes N, without malicious nodes

Here, for the three topologies, the number of nodes is an important parameter for the convergence of the network. Indeed, when the number of nodes increases, the percentage of convergence decreases. We can also see that the 2D Grid is the worst topology behind the Torus and Watts-Strogatz. It is noteworthy to recall that the Cellular Consensus is based on the communication between neighbors and that we have the average number of neighbors $K < 4$ for the 2D Grid, $K = 4$ for the Torus and $K = 10$ for Watts-Strogatz. We could then ask ourselves if the average number of neighbors is a convergence factor ?

5.2.2 Percentage of convergence according to the initial division probability P_0 for different average number of neighbors K, in Watts-Strogatz graph without malicious nodes

Parameters

- Number of nodes of the network : $N = 225$,
- Average number of neighbors : $4 \leq K \leq 16$
- Number of rounds : $M = 20$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 0\%$,
- 100 simulations for each initial division probability P_0.

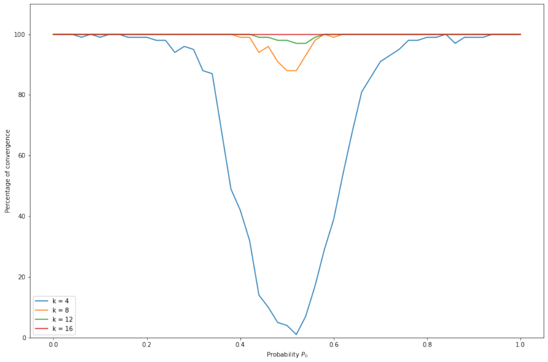


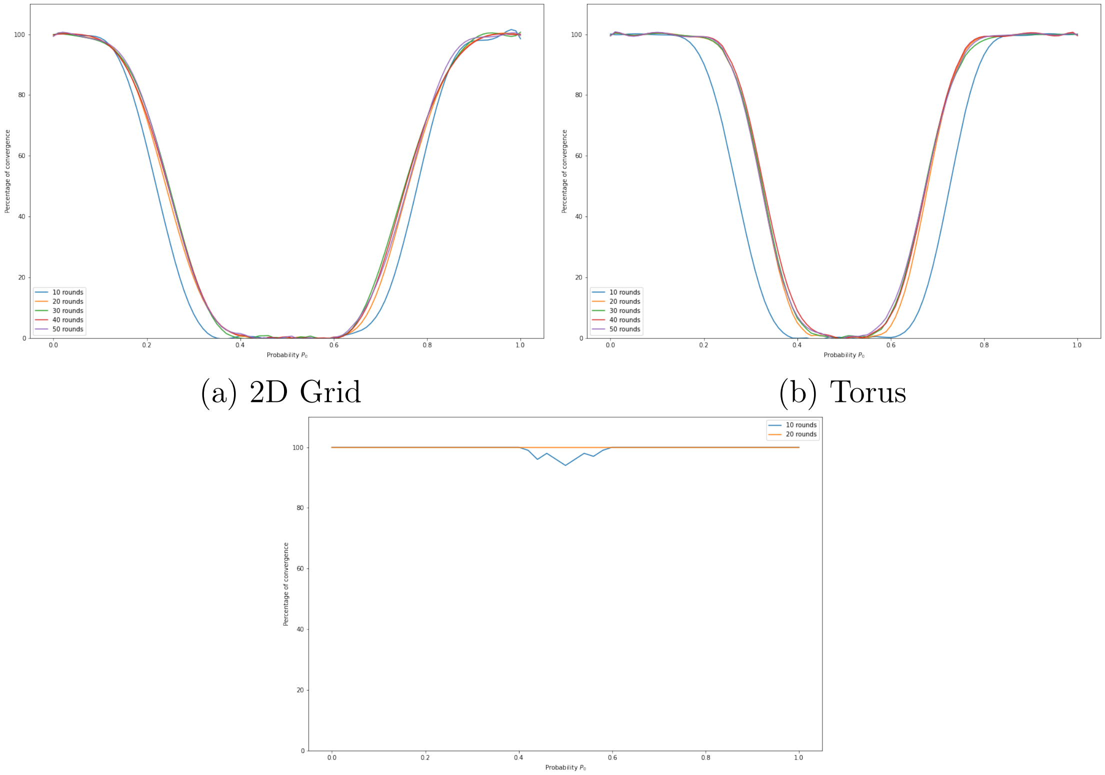
Figure 5.12: Percentage of convergence according to the initial division probability P_0 for different average number of neighbors K, in Watts-Strogatz graph without malicious nodes

According to this graph, our theory is confirmed and we can also notice that for $K \geq 16$, we have always convergence for the topology Watts-Strogatz.

5.2.3 Percentage of convergence according to the initial division probability P_0 for different number of rounds M, without malicious nodes

Parameters

- Number of nodes of the network : $N = 225$,
- Number of rounds : $10 \leq M \leq 50$, ($10 \leq M \leq 20$ for Watts-Strogatz),
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 0\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 10$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

Figure 5.13: Percentage of convergence according to the initial division probability P_0 for different number of rounds M, without malicious nodes

We can see in the previous figures that, to judge the convergence, 10 rounds are not sufficient to obtain concrete results. However, from 20 rounds, we seem to get the same results as 50 rounds. This confirms the following conjecture: for the Cellular Consensus, when there is convergence, it appears relatively quickly (after 20 rounds).

5.2.4 Percentage of convergence according to the initial division probability P_0 for different network sizes N, with Cautious Adversaries

Parameters

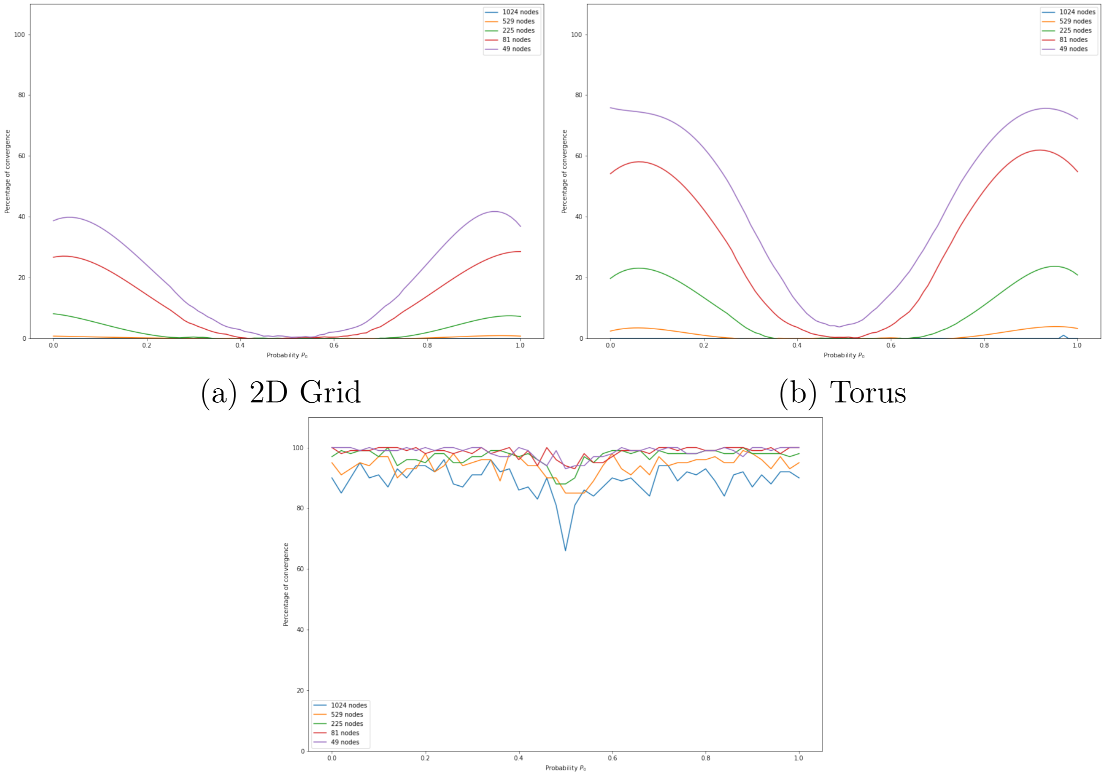
- Number of nodes of the network : $49 \leq N \leq 1024$,
- Number of rounds : $M = 20$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 33.333\%$,
- The lying probability : $P_{lie} = 50\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 10$, $P = 1$.

When we introduce Cautious adversaries in the network, we observe the same phenomenon as without malicious nodes. However, the percentage of convergence appears to be much lower. Indeed when the malicious nodes are detected, they are immediately blacklisted and this means that the nodes concerned lost a neighbor, which leads to this decrease. We saw previously, without malicious nodes, that bigger was the average number of neighbors, better was the percentage of convergence. It would be interesting to see whether this is also true with Cautious adversaries.

5.2.5 Percentage of convergence according to the initial division probability P_0 for different average number of neighbors K, in Watts-Strogatz graph with Cautious adversaries

Parameters

- Number of nodes of the network : $N = 225$,
- Average number of neighbors : $4 \leq K \leq 16$
- Number of rounds : $M = 20$,



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

Figure 5.14: Percentage of convergence according to the initial division probability P_0 for different network sizes N, with Cautious Adversaries

- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 33\%$,
- The lying probability : $P_{lie} = 50\%$,
- 100 simulations for each initial division probability P_0.

Here, the results confirm that the average number of neighbors influence the percentage of convergence. Moreover, we see that the Cautious adversaries lower the convergence. Indeed, previously, with $K = 16$, we had full convergence whereas now, we need $K = 20$ to have it. In the next subsection we will see the importance of Cautious adversaries in the network.

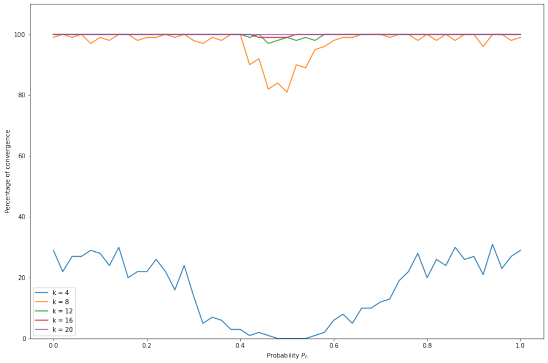
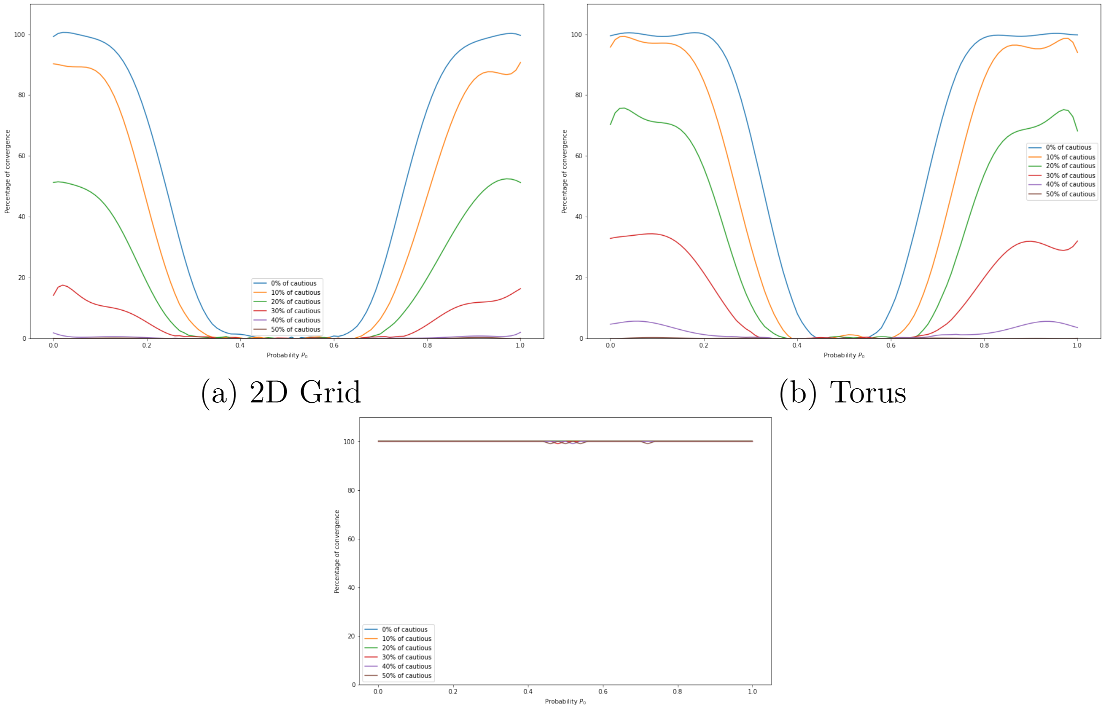


Figure 5.15: Percentage of convergence according to the initial division probability P_0 for different average number of neighbors K, in Watts-Strogatz graph with Cautious adversaries

5.2.6 Percentage of convergence according to the initial division probability P_0 for different percentage of Cautious adversaries $P_{malicious}$

Parameters

- Number of nodes of the network : $N = 225$,
- Number of rounds : $M = 20$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $0\% \leq P_{malicious} \leq 50\%$,
- The lying probability : $P_{lie} = 50\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 20$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

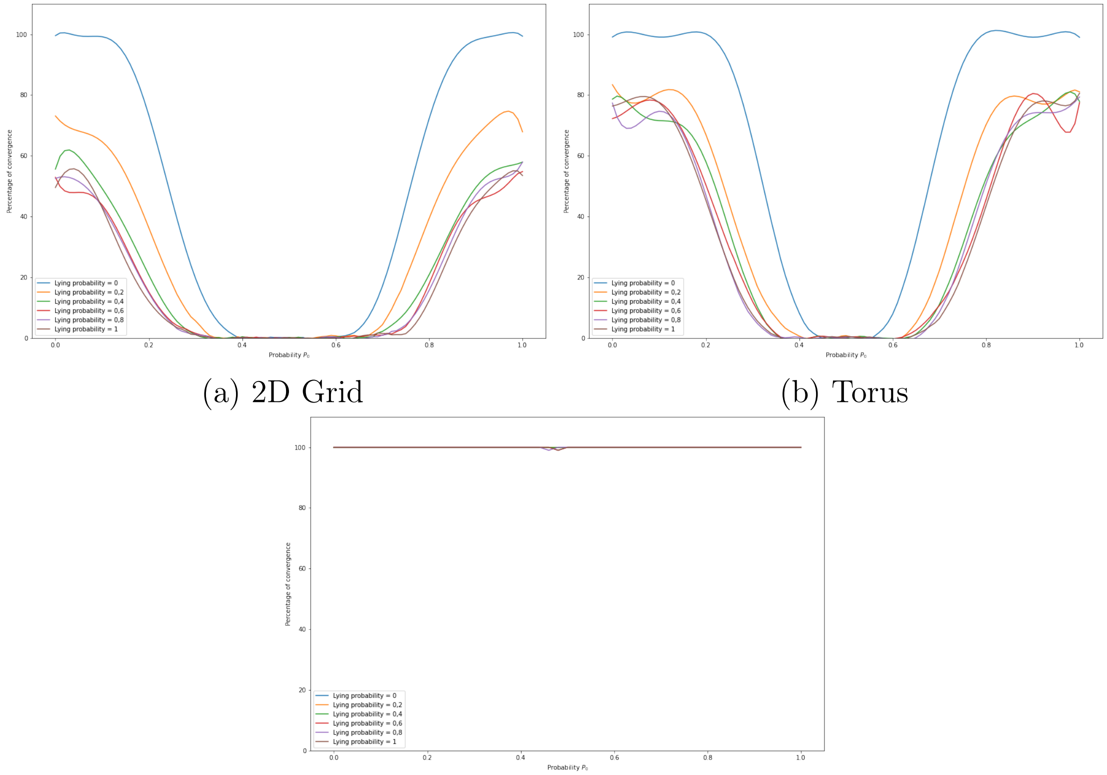
Figure 5.16: Percentage of convergence according to the initial division probability P_0 for different percentage of Cautious adversaries $P_{malicious}$

When we vary the percentage of chance that a node is a Cautious adversary, we observe a decrease in the convergence which seems quite logical. By comparing the different topologies, we observe that the results obtained with the torus are better than those obtained with the 2D grid. As for the results obtained with the Watts-Strogatz topology, they are consistently good and sometimes even excellent. Moreover, we notice, in the case of the torus and the 2D grid, a small difference between the curve of 10% and that of 20%. However, this is no longer the case from 20% and 30%. We saw also that when the number of byzantines nodes is low ($0\% \leq P_{malicious} \leq 10\%$) or high ($30\% \leq P_{malicious} \leq 50\%$) the percentage of convergence does not evolve a lot. In addition, when $10\% \leq P_{malicious} \leq 30\%$, this one change significantly due to the fact that we go from a network without too many malicious to one which has a consequent amount of them.

5.2.7 Percentage of convergence according to the initial division probability P_0 for different lying probability P_{lie}, with Cautious adversaries

Parameters

- Number of nodes of the network : $N = 225$,
- Number of rounds : $M = 20$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 20\%$,
- The lying probability : $0\% \leq P_{lie} \leq 100\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 20$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

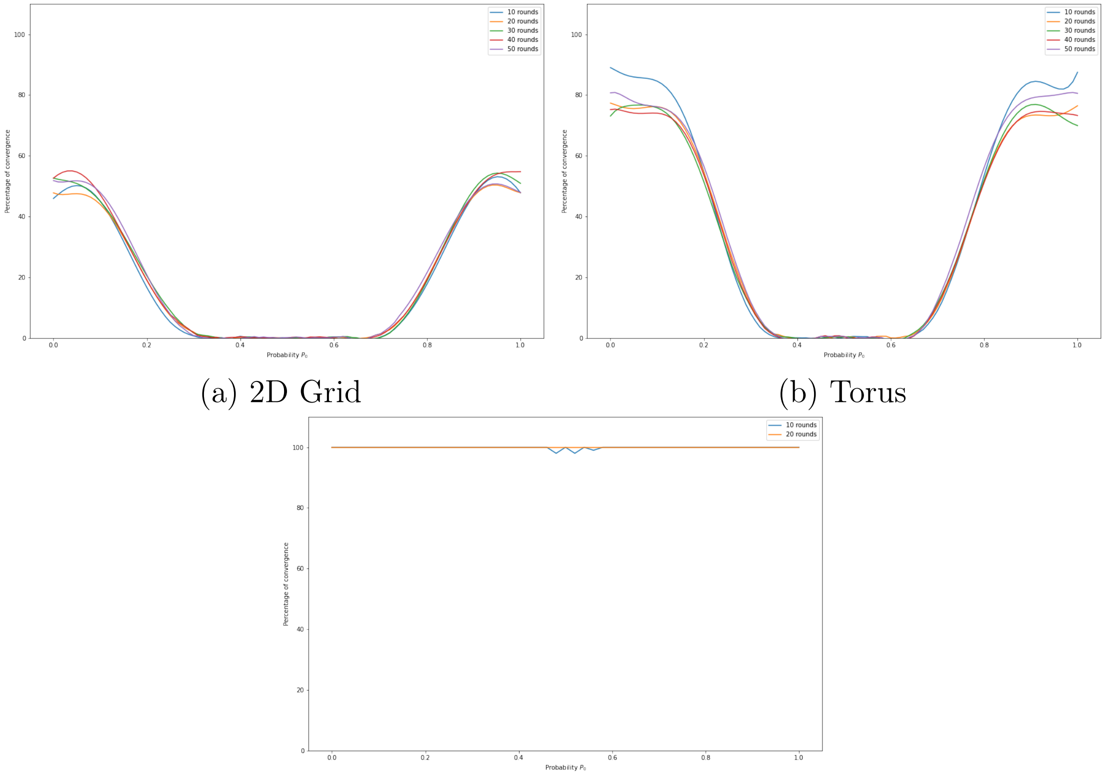
Figure 5.17: Percentage of convergence according to the initial division probability P_0 for different lying probability P_{lie}, with Cautious adversaries

Those graphs show us that the lying probability offer two aspects. First, when P_{lie} is low, the byzantines nodes rarely lie so there is a high probability that they would not lie and not be blacklisted until the end of the process, so the network act as there were no malicious nodes. Secondly, when $P_{lie} \geq 20\%$, there is a high probability that the malicious nodes will lie at least once during the twenty rounds, which explains the fact that there is not such a difference in term of convergence for $P_{lie} = 20\%$ and $P_{lie} = 100\%$. For Watts-Strogatz graphs, their is always convergence except for $P_{lie} = 80\%$ and $P_{lie} = 100\%$ because the malicious nodes lie a lot so they are blacklisted at the beginning of the process, so the network act like one with $K = 20 - (20\% \text{ of } 20) = 20 - 4 = 16$, which is not converging 100% of the time.

5.2.8 Percentage of convergence according to the initial division probability P_0 for different number of rounds M, with Cautious adversaries

Parameters

- Number of nodes of the network : $N = 225$,
- Number of rounds : $10 \leq M \leq 50$, ($10 \leq M \leq 20$ for Watts-Strogatz),
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 20\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 10$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

Figure 5.18: Percentage of convergence according to the initial division probability P_0 for different number of rounds M, with Cautious adversaries

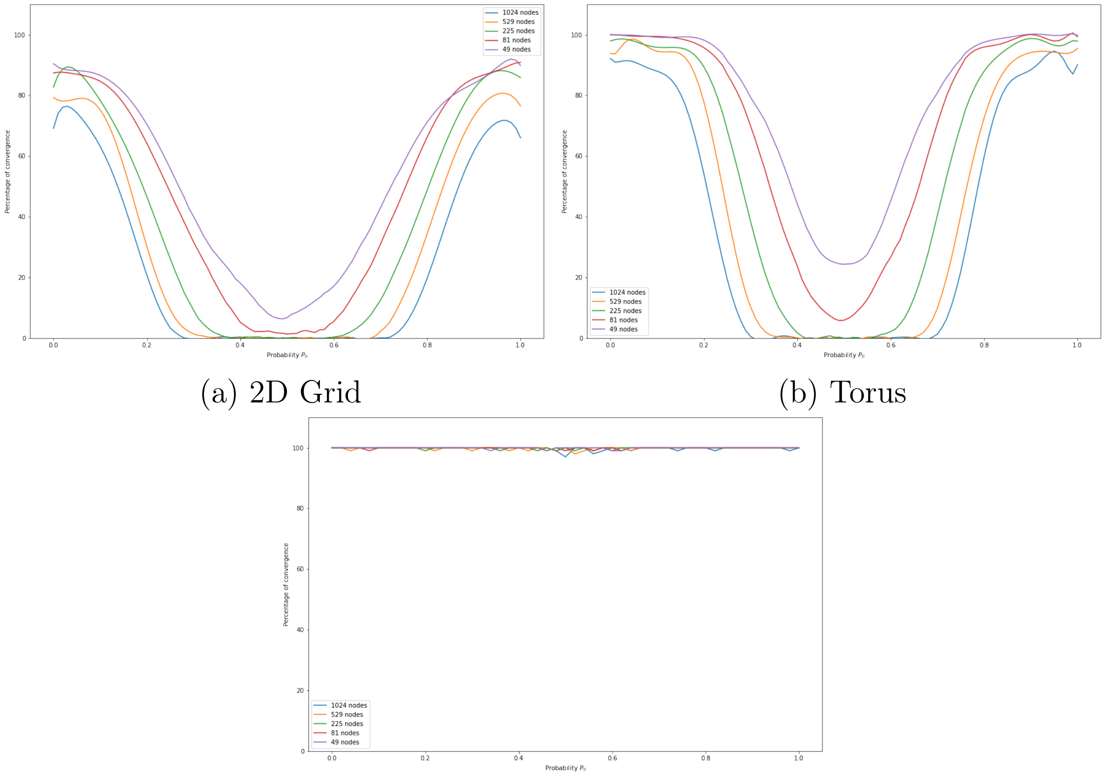
Here, we can see that 10 rounds are not sufficient to obtain concrete results of convergence. However, from 20 rounds, we seem to get the same results as 50 rounds. This confirms the following conjecture: for the Cellular Consensus, when there is convergence, it appears relatively quickly (after 20 rounds).

5.2.9 Percentage of convergence according to the initial division probability P_0 for different network sizes N, with Semi-Cautious Adversaries

Parameters

- Number of nodes of the network : $49 \leq N \leq 1024$,

- Number of rounds : $M = 20$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 33.333\%$,
- The silence probability : $P_{silence} = 50\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 10$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

Figure 5.19: Percentage of convergence according to the initial division probability P_0 for different network sizes N, with Semi-Cautious Adversaries

When we introduce Semi-Cautious adversaries in the network, we observe that when $0,3 \leq P_0 \leq 0,7$, the percentage of convergence is the same than without malicious nodes for 2D Grid and Torus topologies. In addition, for Watts-Strogatz topology, when P_0 is in this interval, we have better results that without byzantines nodes. This phenomenon is explained by the fact that when a network is in disagreement, the nodes which do not respond, make it possible to take a decision on the opinion, and therefore to promote convergence. It seems that this process, appears only when the average number of neighbors is high. However, when $0 \leq P_0 < 0,3$ or $0,7 < P_0 \leq 1$, the percentage of convergence is lower than normal, which seems quite logical. Indeed, when the network is in agreement, the Semi-Cautious adversaries disturb him and cause a drop of the percentage of convergence. So we could ask ourselves, what is the effect of Semi-Cautious on a larger average number of neighbors ?

5.2.10 Percentage of convergence according to the initial division probability P_0 for different average number of neighbors K, in Watts-Strogatz graph with Semi-Cautious adversaries

Parameters

- Number of nodes of the network : $N = 225$,
- Average number of neighbors : $4 \leq K \leq 16$
- Number of rounds : $M = 20$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 33.333\%$,
- The silence probability : $P_{silence} = 50\%$,
- 100 simulations for each initial division probability P_0.

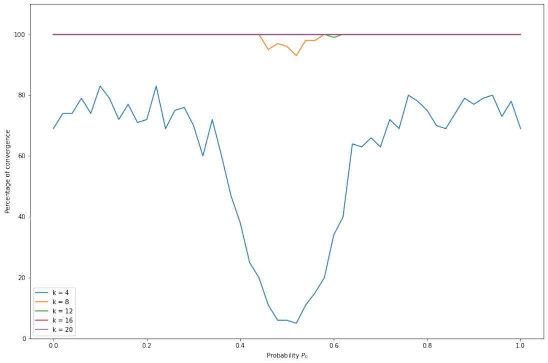


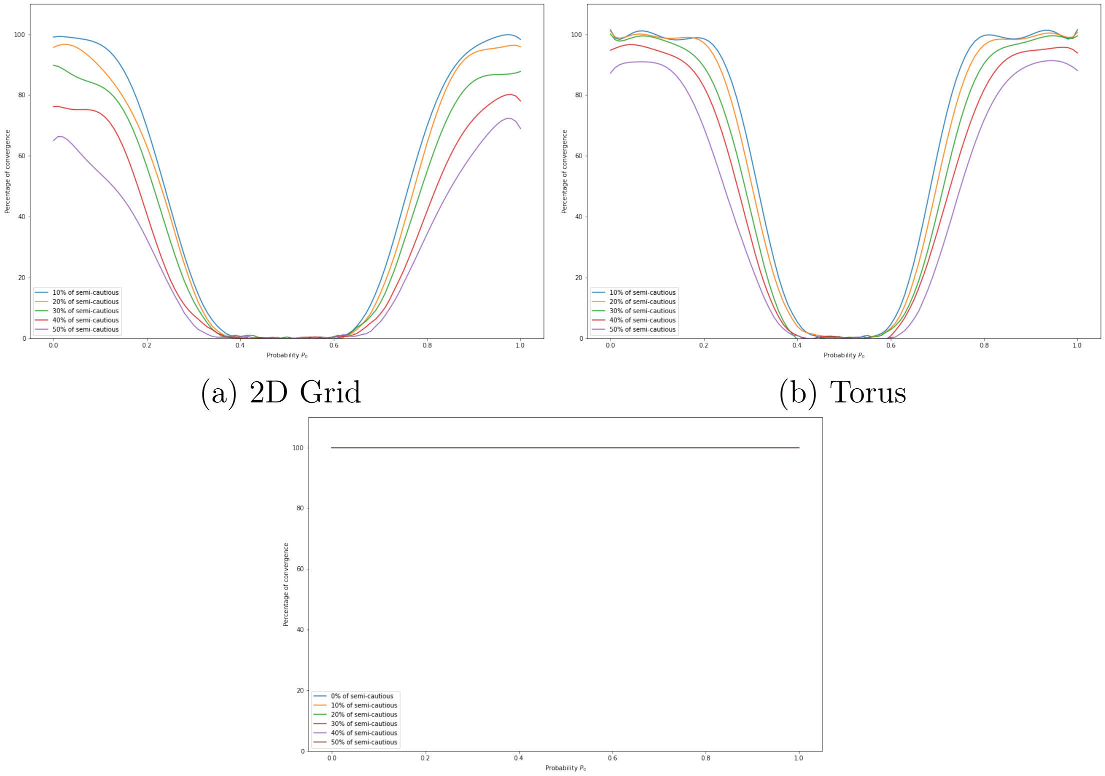
Figure 5.20: Percentage of convergence according to the initial division probability P_0 for different average number of neighbors K, in Watts-Strogatz graph with Semi-Cautious adversaries

Here, the results confirm our previous theory. Indeed, when the average number of neighbors is low, $K <= 4$ (2D Grid and Torus), the percentage of convergence is relatively low for $0 \leq P_0 < 0,3$ or $0,7 < P_0 \leq 1$ and similar to a network without malicious nodes for $0,3 \leq P_0 \leq 0,7$. When the average number of neighbors is higher, $K \geq 8$, the results seems to be better with an increase of a few percent.

5.2.11 Percentage of convergence according to the initial division probability P_0 for different percentage of Semi-Cautious adversaries $P_{malicious}$

Parameters

- Number of nodes of the network : $N = 225$,
- Number of rounds : $M = 20$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $0\% \leq P_{malicious} \leq 50\%$,
- The silence probability : $P_{silence} = 50\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 20$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

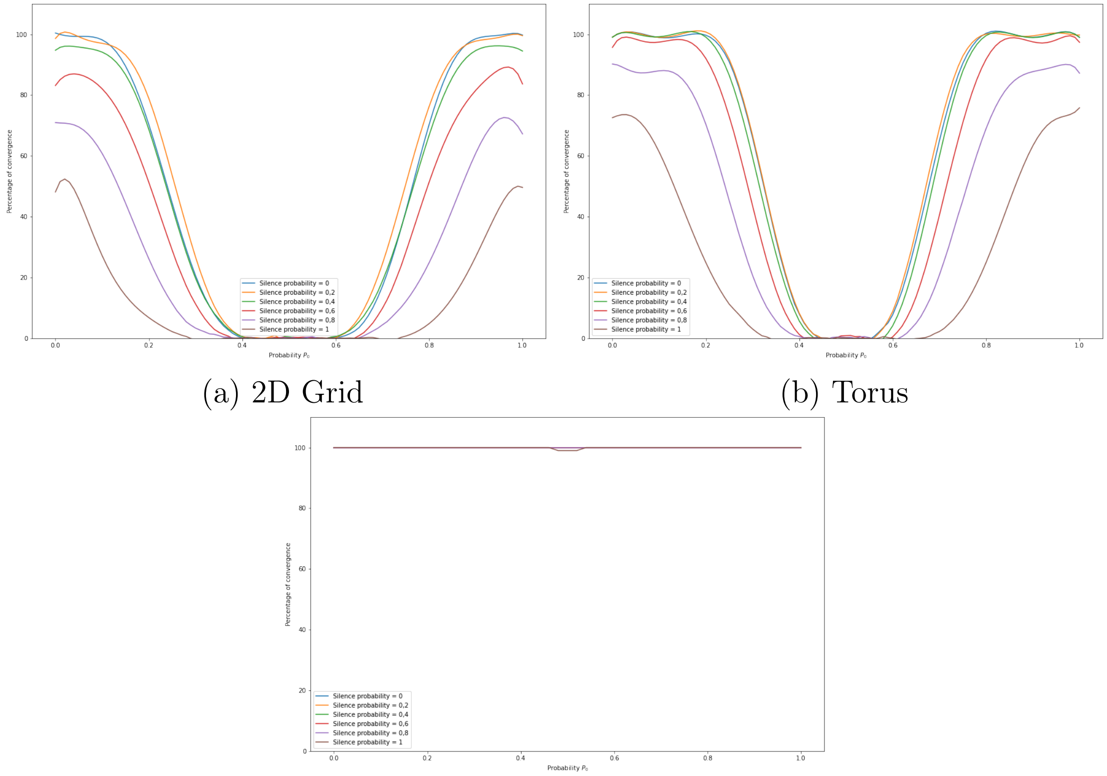
Figure 5.21: Percentage of convergence according to the initial division probability P_0 for different percentage of Semi-Cautious adversaries $P_{malicious}$

When we vary the percentage of chance that a node is a Semi-Cautious adversary, we observe a decrease in convergence which seems quite logical. By comparing the different topologies, we observe that the results obtained with the torus are better than those obtained with the 2D grid. As for the results obtained with the Watts-Strogatz topology, they are consistently excellent. As we have seen in the case of Cautious adversaries, we see that when the number of byzantines nodes is low ($0\% \leq P_{malicious} \leq 10\%$) or high ($30\% \leq P_{malicious} \leq 50\%$) the percentage of convergence does not evolve a lot. In addition, when $10\% \leq P_{malicious} \leq 30\%$, this one change significantly due to the fact that we go from a network without too many malicious to one which is full of them.
However, these last observations are much less obvious in the case of Semi Cautious adversaries.

5.2.12 Percentage of convergence according to the initial division probability P_0 for different silence probability $P_{silence}$, with Semi-Cautious adversaries

Parameters

- Number of nodes of the network : $N = 225$,
- Number of rounds : $M = 20$,
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 20\%$,
- The silence probability : $0\% \leq P_{silence} \leq 100\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 20$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

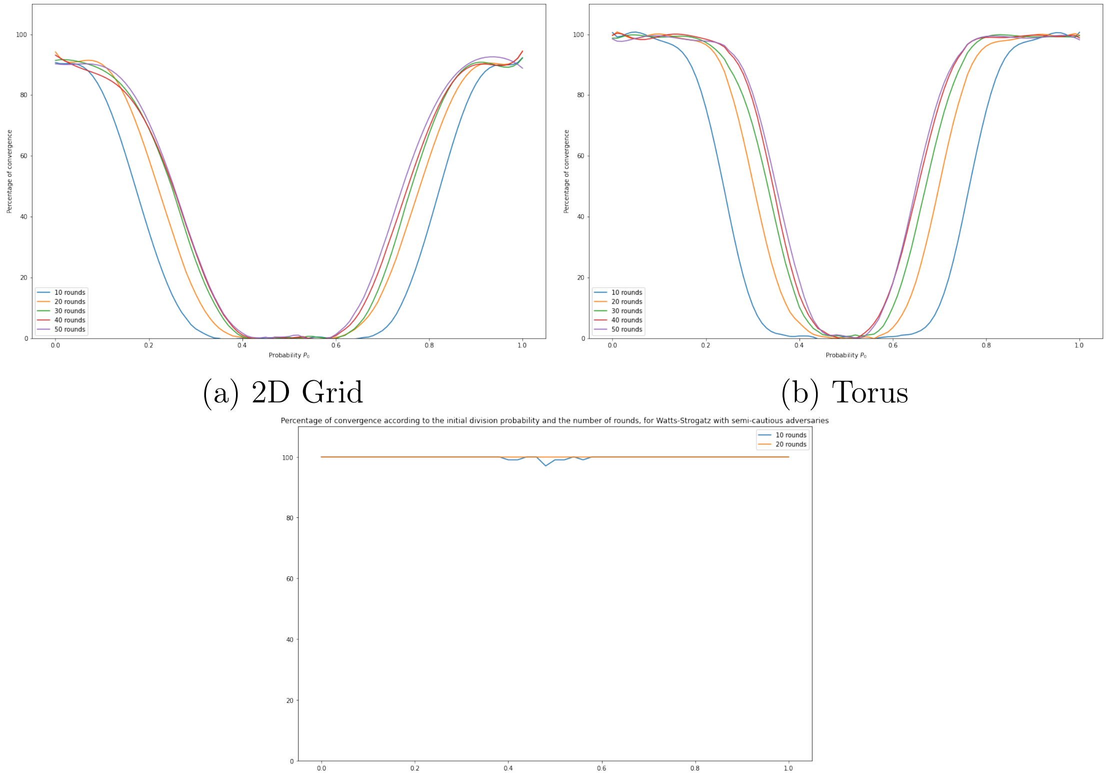
Figure 5.22: Percentage of convergence according to the initial division probability P_0 for different silence probability $P_{silence}$, with Semi-Cautious adversaries

Unlike the lying probability of Cautious adversaries, the silence probability has a little impact on the percentage of convergence when it is low. Indeed, when it varies from 0 to 0,4, there is almost no impact. However, from $P_{silence} = 0,6$ to $P_{silence} = 1$, the impact on the percentage of convergence is blatant. This tendency can be explained by the fact that the Semi-Cautious are not blacklisted, which means that when they lie rarely, there is no influence on the percentage of convergence.

5.2.13 Percentage of convergence according to the initial division probability P_0 for different number of rounds M, with Semi-Cautious adversaries

Parameters

- Number of nodes of the network : $N = 225$,
- Number of rounds : $10 \leq M \leq 50$, ($10 \leq M \leq 20$ for Watts-Strogatz),
- The number of consecutive rounds with the same opinion before the opinion of a node becomes **finalized** : $l = 10$,
- The probability that a node is malicious : $P_{malicious} = 20\%$,
- The silence probability : $P_{silence} = 50\%$,
- 100 simulations for each initial division probability P_0,
- For Watts-Strogatz : $K = 10$, $P = 1$.



(a) 2D Grid

(b) Torus

(c) Watts-Strogatz

Figure 5.23: Percentage of convergence according to the initial division probability P_0 for different number of rounds M, with Semi-Cautious adversaries

Here, we can see that 10 rounds are not sufficient to obtain concrete results of convergence. Moreover, we have almost the same results when $20 \leq M \leq 50$. This confirms the conjecture done when we did the same simulation with the Cautious adversaries.

Bibliography

[1] Coordicide, PDF
https://files.iota.org/papers/20200120_Coordicide_WP.pdf

[2] Our implementations, Github (August 2021)
https://github.com/IOTA-Internship/programs

[3] Torus model (May 2021)
https://urlz.fr/geqN

[4] Watts-Strogatz Graph (May 2021)
https://runestone.academy/runestone/books/published/complex/SmallWorldGraphs/WSGraphs.html