On the Resilience and Uniqueness of CPA for Reliable Broadcast ☆

Chris Litsas [1], Aris Pagourtzis [1], Giorgos Panagiotakos [2], Dimitris Sakavalas [1]

[1] *School of Electrical and Computer Engineering*
National Technical University of Athens, 15780 Athens, Greece,
chlitsas@central.ntua.gr, pagour@cs.ntua.gr, sakaval@corelab.ntua.gr
[2] *Department of Informatics and Telecommunications*
University of Athens, 15784 Athens Greece.
g.panagiotakos@di.uoa.gr

Abstract

We consider the Reliable Broadcast problem in incomplete networks. We study the resilience of the Certified Propagation Algorithm (CPA), which is particularly suitable for *ad hoc* networks. We address the issue of determining the maximum number of corrupted players $t_{\max}^{\text{CPA}}$ that CPA can tolerate under the t-locally bounded adversary model, in which the adversary may corrupt at most t players in each player's neighborhood. For any graph G and dealer-node D we provide upper and lower bounds on $t_{\max}^{\text{CPA}}$ that can be efficiently computed in terms of a graph theoretic parameter that we introduce in this work. Along the way we obtain an efficient 2-approximation algorithm for $t_{\max}^{\text{CPA}}$. We further introduce two more graph parameters, one of which matches $t_{\max}^{\text{CPA}}$ exactly. Our approach exactly captures the information propagation of CPA and thus allows to provide intuitive and easily manageable conditions concerning the behavior of the algorithm. Furthermore we show that CPA is *unique*, in ad hoc networks, among all safe algorithms, i.e., algorithms which never cause a node to decide on an incorrect value. This means that CPA can tolerate as many local corruptions as any other safe algorithm and thus, our approach can be used to effectively describe the solvability of *ad hoc* Broadcast in general.

Keywords: Ad Hoc Networks, Reliable Broadcast, Byzantine Faults, Locally Bounded Adversary

1. Introduction

A fundamental problem in distributed networks is Reliable Broadcast, in which the goal is to distribute a message correctly despite the presence of Byzantine faults. That is, an adversary may control several nodes and be able to make them deviate from the protocol arbitrarily by blocking, rerouting, or even altering a message that they should normally relay intact to specific nodes. In general, agreement problems have been primarily studied under the threshold adversary model, where a fixed upper bound t is set for the number of corrupted players and broadcast can be achieved if and only if $t < n/3$, where n is the total number of players. The Broadcast problem has been extensively studied in complete networks under the threshold adversary model mainly in the period from 1982, when it was introduced by Lamport, Shostak and Pease [3], to 1998, when Garay and Moses [4] presented the first fully polynomial Broadcast protocol optimal in resilience and round complexity.

The case of a threshold adversary in incomplete networks has been studied to a much lesser extent [5, 6, 7, 8], mostly through protocols for Reliable Message Transmission which, combined with a Broadcast protocol for complete networks, yield Broadcast protocols for incomplete networks. Naturally, connectivity constraints are required to hold in addition to the $n/3$ bound. Namely, at most $t < c/2$ corruptions can be tolerated, where c is network connectivity [5].

In the case of an honest dealer, particularly useful in wireless networks, the impossibility threshold of $n/3$

☆ An earlier version of this paper has appeared as 'A Graph Parameter that Matches the Resilience of the Certified Propagation Algorithm', by Chris Litsas, Aris Pagourtzis, Dimitris Sakavalas, in Proceedings of ADHOC-NOW 2013, 12th International Conference, LNCS 7960, pp. 269-280, Springer. An extended version has appeared in [2].

Work supported by ALGONOW project of the Research Funding Program THALIS, co-financed by the European Union (European Social Fund – ESF) and Greek national funds through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework (NSRF).

does not hold; for example, in complete networks the problem becomes trivial. However, in incomplete networks the situation is different. A small number of traitors (corrupted players) may manage to block the entire protocol if they control a critical part of the network, e.g. if they form a separator of the graph. It therefore makes sense to define criteria depending on the structure on the graph (graph parameters), in order to bound the number or restrict the distribution of traitors that can be tolerated.

An approach in this direction is to consider topological restrictions on the adversary's corruption capacity. The importance of local restrictions comes, among others, from the fact that they may be used to derive local criteria which the players can employ in order to achieve Broadcast in *ad hoc* networks. Such an example is the *t-locally bounded adversary model*, introduced in [9], in which at most t-corruptions are allowed in the neighborhood of every node.

1.1. Related work

Koo [9] proposed a simple, yet powerful protocol for the t-locally bounded model, the *Certified Propagation Algorithm* (CPA) (a name coined by Pelc and Peleg in [1]), and applied it to networks of specific topology. In 2005 Pelc and Peleg [1] considered the t-locally bounded model in generic graphs and gave a sufficient topological condition for CPA to achieve Broadcast in such graphs. They also provided an upper bound on the number of corrupted players t that can be locally tolerated in order to achieve Broadcast by any protocol, in terms of an appropriate graph parameter; they left the deduction of tighter bounds as an open problem. To this end, Ichimura and Shigeno [10] proposed an efficiently computable graph parameter which implies a tighter, but not exact, characterization of the class of graphs on which CPA achieves Broadcast.

We would like to explain the contribution of this paper in more detail, especially in comparison to recent work of Tseng, Vaidya and Bhandari [11], which presents a necessary and sufficient condition for CPA correctness, and to the work in [12] which, among others, provides a necessary and sufficient condition for achieving reliable broadcast on any given network.

Two important open questions were stated in the study of [1] regarding reliable broadcast: (a) to derive a tight parameter revealing the maximum number of traitors that can be locally tolerated by CPA in a graph G with dealer D, in other words, to find a tight condition for CPA correctness, and (b) to check whether the *CPA Uniqueness* conjecture holds, which essentially states that whenever Broadcast is possible CPA will manage to achieve it; equivalently, that no *ad hoc* algorithm can tolerate more local corruptions than CPA on any instance (G, D). Both these open questions have mainly been addressed in [13, 2]; these results were later strengthened in [12].The approach followed in [12] is different from the one presented here.

Here, in order to address CPA correctness, we define a new graph parameter that captures exactly the number that can be locally tolerated by CPA, thus providing a tight condition as mentioned above. Very recently Tseng *et al.* [11] independently also gave a necessary and sufficient condition for CPA correctness; a corresponding tight parameter is implicit in their work. Our condition is therefore equivalent to that of [11]; however, no result concerning CPA Uniqueness, neither any necessary condition for Broadcast in general are given in [11]. On the other hand, our approach not only gives a faster way to check the tight condition for CPA correctness, most importantly it allows us to prove that the same condition is necessary for achieving Broadcast through *any safe*[1] algorithm in the *ad hoc* model, thus establishing that whenever Broadcast is possible by a safe algorithm, CPA can achieve it. This provides an affirmative answer to the second question of [1], namely we have proved that the *CPA Uniqueness* conjecture holds with respect to safe Broadcast algorithms. Note that an alternative proof for CPA Uniqueness, presented in [12], is essentially different than the one presented here. In particular, our approach allows to additionally obtain an efficient 2-approximation algorithm for the problem of determining the maximum local number of traitors that CPA (and by the uniqueness result any safe algorithm) can tolerate on a given instance (G, D). The significance of this approximability result comes from the fact that this number is NP-hard to compute as shown in [12]. Let us also mention that the equivalent condition presented in [12], while being more adaptable to different adversary models, does not yield an efficient approximation algorithm in any obvious way. Hence, the condition presented here is interesting *per se*.

1.2. Our results

In this paper we study the behavior of CPA in generic (incomplete) networks, with an honest dealer. As we will see in Section 7, this case essentially captures the difficulty of the general problem, where even the dealer may be corrupted. Our first contribution is the exact determination of the maximum number of corrupted players $t^{\mathrm{CPA}}_{\max}(G, D)$ that can be locally tolerated by CPA, for

[1] By the term 'safe' we refer to the notion of algorithms that never make a node take a wrong decision as explained in Section 1.3.

any graph G and dealer D. We do this by developing three graph parameters:

$\mathcal{K}(G, D)$ is determined via an appropriate *level-ordering* of the nodes of the graph. We show that $t < \mathcal{K}(G, D)/2$ is a sufficient condition for CPA to be t-locally resilient and that $t < \mathcal{K}(G, D)$ is a necessary condition, implying that $\lceil \mathcal{K}(G, D)/2 \rceil - 1 \leq t_{\max}^{\text{CPA}} < \mathcal{K}(G, D)$. We prove that our parameter coincides with the parameter $\widetilde{\mathcal{X}}(G, D)$ of [10]. We further propose an efficient algorithm for computing $\mathcal{K}(G, D)$ which is faster than the algorithm for computing $\widetilde{\mathcal{X}}(G, D)$ proposed in [10]. Note that this immediately gives an asymptotic 2-approximation for $t_{\max}^{\text{CPA}}$; we provide an example that shows that the ratio of this algorithm is tight.

$\mathcal{M}(G, D, t)$, depending also on a value t, is a parameter that immediately reveals whether CPA is t-locally resilient for graph G and dealer D, by simply checking whether $\mathcal{M}(G, D, t) \geq t + 1$. Therefore, via this parameter, we provide a *necessary and sufficient condition* for CPA to be t-locally resilient. Such a condition was not known until very recently, when a necessary and sufficient condition was independently given in [11]. However, the way in which the condition of [11] is defined implies a superexponential time algorithm to check it (actually no algorithm is given in [11]). On the other hand, we will see that even a naïve algorithm to compute $\mathcal{M}(G, D, t)$ would need single exponential time.

$\mathcal{T}(G, D) = \max\{t \in \mathbb{N} \mid \mathcal{M}(G, D, t) \geq t + 1\}$, gives the maximum number of corrupted players that CPA can tolerate in every node's neighborhood, hence exactly determining $t_{\max}^{\text{CPA}}(G, D)$.

In addition, using the $\mathcal{M}(G, D, t)$ parameter we prove that CPA is *unique* among the t-locally safe *ad hoc* broadcast algorithms. That is, if a t-locally safe *ad hoc* broadcast algorithm is t-resilient for a graph G with dealer D, then CPA is also t-resilient for G, D. Thus, we answer the question of CPA Uniqueness posed in [1] in the affirmative.

1.3. Problem and Model Definition

We will now formally define the adversary model and the CPA algorithm; both notions were developed in [9]; the term t-locally bounded is due to [1]. We will also define basic notions and terminology that we will use throughout the paper. We refer to the participants of the protocol by using the notions *node* and *player* interchangeably.

1.3.1. Reliable Broadcast with Honest Dealer.

We assume the existence of a designated honest player, called the *dealer*, who wants to broadcast a certain value x_D to all players. We say that a distributed protocol achieves Reliable Broadcast if by the end of the protocol every honest player has *decided on* x_D, i.e. has been able to deduce that x_D is the value originally sent by the dealer and output it as its own decision.

The above problem is trivial in complete networks and we will consider the case of incomplete networks here. In the sequel we will refer to the problem as the Broadcast problem.

1.3.2. t-locally bounded adversary model.

We consider a network where nodes may be corrupted, but at most t-corruptions are allowed in the neighborhood of every node. A corruption set with the above property is called *t-local set*. Given a graph G and dealer D, an algorithm which achieves Broadcast for any t-local corruption set is called t-locally resilient. An algorithm which achieves Broadcast in the t-locally bounded adversary model is called *t-locally resilient*. As stated in [1], a basic requirement of a broadcast algorithm is that it is *safe*, namely, it never causes a node to accept an incorrect message. Specifically an algorithm for graph G and dealer D is called *t-locally safe* if it never causes a node to decide on an incorrect message under any t-local set of Byzantine corruptions.

The previously mentioned Certified Propagation algorithm uses only local information and thus is particularly suitable for *ad hoc* networks. CPA is probably the only Broadcast algorithm known up to now for the t-locally bounded model, not requiring knowledge of the network topology.

Certified Propagation Algorithm

1. The dealer D sends its initial value x_D to all of its neighbors, decides on x_D and terminates.
2. If a node is a neighbor of the dealer, then upon receiving x_D from the dealer, decides on x_D, sends it to all of its neighbors and terminates.
3. If a node is not a neighbor of the dealer, then upon receiving $t + 1$ copies of a value x from $t + 1$ distinct neighbors, it decides on x, sends it to all of its neighbors and terminates.

Definition 1 (Max CPA Resilience)**.** *For a graph G and dealer-node D, $t_{\max}^{\text{CPA}}(G, D)$ is the maximum t such that CPA is t-locally resilient.*

Whenever G and D are implied by the context, we will simply write $t_{\max}^{\text{CPA}}$.

1.3.3. Bounds vs Conditions.

Let us now make a simple but useful observation: for a graph-theoretic parameter X, showing that $t < X$ is a

sufficient topological condition for CPA to be t-locally resilient provides a lower bound of $\lceil X \rceil - 1$ on $t^{\text{CPA}}_{\max}$. Respectively, necessary conditions of similar form imply upper bounds on $t^{\text{CPA}}_{\max}$. We will often use this relation between bounds and conditions throughout the paper.

2. Lower Bounds on Max CPA Resilience

Pelc and Peleg [1] were the first to present a graph-theoretic parameter $\mathcal{X}(G, D)$ which gives a sufficient condition for CPA resilience, namely $\mathcal{X}(G, D) \geq 2t + 1$. However, as shown in the same paper, this condition is not necessary.

2.1. A new parameter for bounding Max CPA Resilience

In order to derive tighter bounds on $t^{\text{CPA}}_{\max}$ we introduce the notion of *minimum k-level ordering* of a graph which generalizes the level ordering that was implicit in [1]. Intuitively, a minimum k-level ordering is an arrangement of nodes into disjoint levels, such that every node has at least k neighbors in previous levels and belongs to the minimum level for which this property is satisfied for this node. Formally:

Definition 2. *A* Minimum k-Level Ordering $\mathcal{L}_k(G, D)$ *of a graph* $G = (V, E)$ *for a given dealer-node* D *is a partition* $V \setminus \{D\} = \bigcup_{i=1}^{m} L_i,\ m \in \mathbb{N}$ *s.t.*

$$L_1 = \mathcal{N}(D),$$
$$L_i = \{v \in V \setminus \bigcup_{j=1}^{i-1} L_j : |\mathcal{N}(v) \cap \bigcup_{j=1}^{i-1} L_j| \geq k\}, 2 \leq i \leq m$$

We next define the relaxed k-level ordering notion which will be useful for our proofs, by dropping the level minimality requirement for nodes.

Definition 3. *A* Relaxed k-Level Ordering *of a graph* $G = (V, E)$ *for a given dealer-node* D *is a partition* $V \setminus \{D\} = \bigcup_{i=1}^{m} L_i,\ m \in \mathbb{N}$ *s.t.*

$$L_1 = \mathcal{N}(D), \qquad \forall v \in L_i : |\mathcal{N}(v) \cap \bigcup_{j=1}^{i-1} L_j| \geq k$$

2.1.1. Properties of k-level orderings.

Note that while there may exist several relaxed k-level orderings of a graph, the minimum k-level ordering is unique, as can be shown by an easy induction. Let us also observe that a relaxed k-level ordering may be easily transformed to the unique minimum k-level ordering; to show this we will use a new notion: Given a relaxed k-level ordering $\mathcal{L}$: $V = \bigcup_{i=1}^{m} L_i,\ m \in \mathbb{N}$ we will refer to a player $u \in L_h \in \mathcal{L}$ as *delayed node* in $\mathcal{L}$ if $\exists\ d$ with $1 < d < h \leq m$ s.t. $|\mathcal{N}(u) \cap \bigcup_{j=1}^{d-1} L_j| \geq k$. The following is immediate from the previous definitions,

Fact. A relaxed k-level ordering with no delayed nodes is a minimum k-level ordering.

Now, given any relaxed k-level ordering $\mathcal{L}$ we can construct a minimum k-level ordering $\mathcal{L}_k$ simply by repeatedly moving every delayed node to the lowest level such that the partition remains a relaxed k-level ordering. It is easy to see that if there exists a minimum k-level ordering for a graph G with dealer D then it is actually unique. Therefore, the following holds,

Fact. Given a graph G and dealer D, for every $k \in \mathbb{N}$, if there exists a Relaxed k-Level Ordering for G, D then there exists a unique Minimum k-Level Ordering for G, D.

Definition 4 (Parameter $\mathcal{K}$)**.** *For graph G and dealer D,*

$$\mathcal{K}(G, D) \stackrel{def.}{=} \max\{k \in \mathbb{N} \mid \exists\ \textit{a Minimum k-Level Ordering } \mathcal{L}_k(G, D)\}$$

Theorem 1 (Sufficient Condition)**.** *For every graph G, dealer D and* $t \in \mathbb{N}$*, if* $t < \mathcal{K}(G, D)/2$ *then CPA is t-locally resilient.*

Proof. Observe that $2t < \mathcal{K}(G, D)$ implies the existence of a minimum $(2t + 1)$-level ordering $\mathcal{L}_{2t+1}(G, D)$. Let $\mathcal{L}_{2t+1}(G, D)$ be the partition $\{L_1, \ldots, L_m\}$ of V, i.e. $V = \bigcup_{i=1}^{m} L_i$. It suffices to show that for $1 \leq i \leq m$, every honest player $v \in L_i$ decides on the dealer's value x_D. By strong induction on i:

Every honest player $v \in L_1 = \mathcal{N}(D)$ decides on the dealer's value x_D due to the CPA steps 1 and 2. If all honest players $u \in L_i, 1 \leq i \leq h$, decide on x_D at some round, then every honest player $v \in L_{h+1}$ receives $|\bigcup_{j=1}^{h} L_j \cap \mathcal{N}(v)| \geq 2t + 1$ messages from its decided neighbors in previous levels and at least $t + 1$ of them are honest. Thus v decides on x_D.

□

Corollary 2 (Lower Bound)**.** *For any graph G and dealer D it holds that* $t^{\text{CPA}}_{\max} \geq \lceil \mathcal{K}(G, D)/2 \rceil - 1$

2.2. Non-tightness of the lower bound

In Theorem 1 we proved that $t < \mathcal{K}(G, D)/2$ is sufficient for CPA to be t-locally resilient; we next prove that it is not a necessary condition. Intuitively, the reason is that the topology of the graph may prevent the adversary from corrupting t players in *each* player's neighborhood, hence some players will correctly decide by

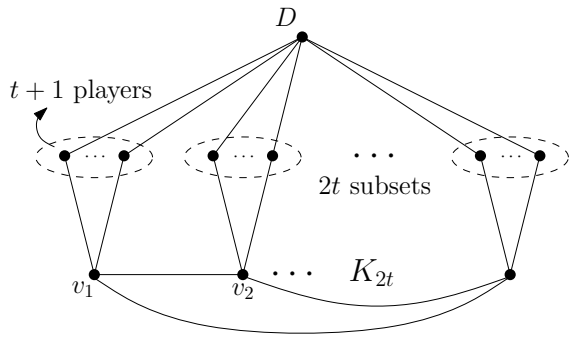

Figure 1: Graph with $\mathcal{K}(G, D) = t + 1$, for which CPA is t-locally resilient.

executing CPA even if they have only $t + 1$ neighbors in previous levels.

Proposition 3. *There exists a family of instances (G, D), such that CPA is $(\mathcal{K}(G, D) - 1)$-locally resilient for (G, D).*

Proof. Figure 1 provides such an instance for each value of t. In this instance the neighborhood of D consists of $2t^2 + 2t$ nodes, nodes $v_1, \ldots, v_{2t}$ form a clique of size $2t$ and are connected with $\mathcal{N}(D)$ as shown in the figure. We can easily check that $t = \mathcal{K}(G, D) - 1$. If we run CPA on G then any player $v_i \in \{v_1, \ldots, v_{2t}\}$ receives M correct messages, with

$$M = M_A + M_B \tag{1}$$

where, M_A = number of messages received from $\mathcal{N}(D)$ and M_B = number of messages received from $B = \{v_1, \ldots, v_{2t}\} \setminus \{v_i\}$. Let $T_i = T \cap \mathcal{N}(D) \cap \mathcal{N}(v_i)$ be the set of traitors that are common neighbors of D and v_i. Then

$$M_A = |\mathcal{N}(D) \cap \mathcal{N}(v_i) \setminus T_i| = t + 1 - |T_i| \tag{2}$$

In order to compute the number of correct messages that v_i receives from players in B, we define the set $C_B = C_{B_1} \cup C_{B_2}$ where the sets C_{B_1}, C_{B_1} are defined as:

$$C_{B_1} = \{v \in B \;\big|\; v \text{ receives at most } t \text{ messages from } \mathcal{N}(D)\}$$
$$C_{B_2} = \{v \in B \;\big|\; v \text{ is corrupted}\}$$

We observe that C_{B_1} becomes maximum in cardinality if the adversary corrupts exactly one player in every set $\mathcal{N}(v_j) \cap \mathcal{N}(D), \forall v_j \in B$. Therefore $\max_{T:t\text{-local set}} |C_{B_1}| = \max_{T:t\text{-local set}} |T \cap (\mathcal{N}(D) \setminus \mathcal{N}(v_i))| = t - |T_i|$. Also $|C_{B_2}| \leq t - |T_i|$ because B and $\mathcal{N}(v_i) \cap \mathcal{N}(D)$ form the neighborhood of v_i where the corruptions can be at most t. Next we compute an upper bound on C_B. Namely, $|C_B| = |C_{B_1} \cup C_{B_2}| \leq |C_{B_1}| + |C_{B_2}| \leq (t - |T_i|) + (t - |T_i|) = 2t - 2|T_i|$ and thus, $M_B = 2t - 1 - |C_B| = 2t - 1 - 2t + 2|T_i| = 2|T_i| - 1$. Finally from the last equation and equations (1), (2) we compute the total number of messages $M = M_A + M_B \geq t + 1 - |T_i| + 2|T_i| - 1 = t + |T_i|$.

For any v_i, if $|T_i| > 0$ then $M \geq t + 1$. Otherwise $|T_i| = 0$ and v_i receives $t + 1$ correct messages from $\mathcal{N}(D)$. Thus CPA successfully achieves Broadcast on (G, D).

□

3. An Upper Bound on Max CPA Resilience

In the previous section we have shown that $t^{\text{CPA}}_{\max} \geq \lceil \mathcal{K}(G, D)/2 \rceil - 1$; we have also demonstrated cases in which $\mathcal{K}(G, D) - 1$ traitors are locally tolerated by CPA. In this section we will show that the latter is the best possible: $\mathcal{K}(G, D) - 1$ is an upper bound on the number of local traitors for any G and D. We do this by proving a necessary condition for CPA to be t-locally resilient.

Theorem 4 (Necessary Condition)**.** *For any graph G, dealer D and $t \geq \mathcal{K}(G, D)$, CPA is not t-locally resilient.*

Proof. Assume that CPA is t-locally resilient, with $t \geq \mathcal{K}(G, D)$. Since, by assumption, CPA is t-locally resilient there must be a positive integer, let s, so that the algorithm terminates after s steps in G. Consider now the operation of CPA on graph G in terms of sets. Let L_i denote the set of nodes that decide in the i-th round. Since every node in L_i decides at the i-th round we get that it has at least $t + 1$ neighbors in sets $L_1, \ldots, L_{i-1}$. That is, $\forall v \in L_i \Rightarrow |\mathcal{N}(v) \cap \bigcup_{j=1}^{i-1} L_j| \geq t + 1$. Observe that the above sequence is a relaxed $(t+1)$-level ordering for G, D. From the above observation and according to the Proposition 2.1.1 we get that there must be a minimum $(t+1)$-level ordering for G, D. But this is a contradiction since we assumed that $t \geq \mathcal{K}(G, D)$.

□

Corollary 5 (Upper bound on $t^{\text{CPA}}_{\max}$)**.** *For any graph G and dealer D it holds that $t^{\text{CPA}}_{\max} < \mathcal{K}(G, D)$*

3.1. Comparison with the Ichimura-Shigeno parameter

In [10], Ichimura and Shigeno introduce a graph theoretic parameter $\widetilde{\mathcal{K}}(G, D)$ which can be used to obtain a sufficient condition for CPA resilience. For a graph $G = (V, E)$ and dealer D, they consider a total ordering $\sigma = (v_1, v_2, \ldots)$ of the set $V \setminus (\mathcal{N}(D) \cup D)$, and use $\delta(W_i, v)$ to denote the number of neighbors that v has in the set $\mathcal{N}(D) \cup \{v_1, \ldots, v_{i-1}\}$. The total ordering σ has

the property that $\forall i, j$, *with* $1 \leq i < j \leq |V \setminus (\mathcal{N}(D) \cup D)|$ it holds that $\delta(W_{i-1}, v_i) \geq \delta(W_{i-1}, v_j)$. This ordering is also referred to as *max-back ordering*. They define parameter $\widetilde{\mathcal{X}}(G, D) = \min\{\delta(W_{i-1}, v_i) \mid i = 1, 2, \ldots\}$. and prove that it is unique, i.e., is the same for all max-back orderings. They essentially prove that,[2]

$$\lceil \widetilde{\mathcal{X}}(G, D)/2 \rceil - 1 \leq t_{\max}^{\text{CPA}} < \widetilde{\mathcal{X}}(G, D). \tag{1}$$

Hence, their parameter gives similar bounds as ours. We next show that there is a good reason for this coincidence: despite the different way of defining the parameters $\mathcal{K}(G, D)$ and $\widetilde{\mathcal{X}}(G, D)$, they prove to be equal.

Proposition 6. $\mathcal{K}(G, D) = \widetilde{\mathcal{X}}(G, D)$

Proof. Consider the max-back ordering $\sigma = (v_1, v_2, \ldots)$. Then the sequence $\{L_1 = \mathcal{N}(D), L_2 = \{v_1\}, L_3 = \{v_2\}, \ldots\}$ is trivially a relaxed $\widetilde{\mathcal{X}}(G, D)$-level ordering, because the minimum connectivity between a level and its predecessors is $\widetilde{\mathcal{X}}(G, D)$. Thus, due to Proposition 2.1.1, there exists a minimum $\widetilde{\mathcal{X}}(G, D)$-level ordering, therefore $\mathcal{K}(G, D) \geq \widetilde{\mathcal{X}}(G, D)$. Thus, combining the last inequality with inequality (1) we get the following:

$$t_{\max}^{\text{CPA}} < \widetilde{\mathcal{X}}(G, D) \leq \mathcal{K}(G, D)$$

Since Proposition 3 implies that there is a graph for which CPA is $(\mathcal{K}(G, D) - 1)$-locally resilient the above relation yields the equality of $\mathcal{K}(G, D)$ and $\widetilde{\mathcal{X}}(G, D)$, since $\widetilde{\mathcal{X}}(G, D) < \mathcal{K}(G, D)$ would lead to $t_{\max}^{\text{CPA}} < \mathcal{K}(G, D) - 1$, a contradiction.

□

Although the two parameters $\mathcal{K}(G, D)$ and $\widetilde{\mathcal{X}}(G, D)$ are equal, the fact that $\mathcal{K}(G, D)$ is defined in a completely different way leads to an improved complexity of computing it, as we will see in the next section.

4. Approximation of Max CPA Resilience

Let us now consider the approximability of computing the *Max CPA Resilience*; we will give an efficient 2-approximation algorithm. We first show how to check if there exists a minimum m-level ordering, for a graph G and dealer D, using a slight variation of the standard BFS algorithm. Subsequently, we obtain the approximation by simply computing $\mathcal{K}(G, D)$, using the above check. The ratio follows immediately, by combining Corollaries 2 and 5.

[2]Note that the condition $t \leq \widetilde{\mathcal{X}}(G, D)$ was given as necessary in [10]; however their proof can be easily modified to show the tighter bound $t < \widetilde{\mathcal{X}}(G, D)$, implying the right part of (1).

Existence check of a minimum m-level ordering for (G, D).

1. Assign a zero counter to each node.
2. Enqueue the dealer and every one of its neighbors.
3. Dequeue a node and increase the counters of all its neighbors. Enqueue a neighbor only if its counter is at least m.
4. Repeat Step 3 until the queue is empty.
5. If all nodes have been enqueued then output '*True*' (a minimum m-level ordering exists); otherwise, output '*False*'.

Note that the above algorithm can be modified to compute the minimum m-level ordering $\mathcal{L}_m(G, D)$.

2-Approximation of $t_{\max}^{\text{CPA}}$.

1. Compute $\mathcal{K}(G, D)$: since $\mathcal{K}(G, D) < \min_{v \in V \setminus (\mathcal{N}(D) \cup D)} \deg(v) = \delta$, the exact value of $\mathcal{K}(G, D)$ is computed by $\log \delta$ repetitions of the existence check, by simple binary search.
2. Return $\lceil \mathcal{K}(G, D)/2 \rceil - 1$

Since $t \geq \mathcal{K}(G, D) \Rightarrow$ CPA is not t-locally resilient, it holds that $t_{\max}^{\text{CPA}} < \mathcal{K}(G, D)$, consequently, the returned value is at least $\lceil t_{\max}^{\text{CPA}}/2 \rceil - 1$.

A tight example for the approximation ratio of the algorithm is in fact given by the instance in Figure 1 in which we present a graph for which $\mathcal{K}(G, D) = t + 1$ and CPA is t-locally resilient.

The complexity of the above approximation algorithm is obviously given by the complexity of the computation of $\mathcal{K}(G, D)$. As explained above the algorithm requires at most $\log \delta$ executions of the existence check. The latter requires $O(|E|)$ time (same complexity as BFS). Altogether, we get that the time complexity of the algorithm is $O(|E| \log \delta)$, which significantly improves upon the complexity bound for the equivalent parameter $\widetilde{\mathcal{X}}(G, D)$ given in [10]; the complexity stated there is $O(|V|(|V| + |E|))$.

5. Determining $t_{\max}^{\text{CPA}}$ Exactly

In this section we present a procedure to compute the exact value of $t_{\max}^{\text{CPA}}$. To this end, we introduce two new graph parameters.

For a corruption set (t-local set) T and graph $G = (V, E)$ we will denote with $G_{\bar{T}} = (V \setminus T, E')$ the node induced subgraph of G on the node set $V \setminus T$.

Definition 5. *For any graph G, dealer D and positive integer t, the* t-safety threshold *is the quantity* $\mathcal{M}(G, D, t) = \min_{T:\ t\text{-local set}} \mathcal{K}(G_{\bar{T}}, D)$.

Theorem 7 (Necessary and Sufficient Condition)**.** *For a graph $G = (V, E)$ and dealer D, CPA is t-locally resilient iff $\mathcal{M}(G, D, t) \geq t + 1$.*

Proof. ($\Leftarrow$) Assume $\mathcal{M}(G, D, t) \geq t + 1$ and let $T \subseteq V \setminus D$ be any t-local corruption set. It must hold that $\mathcal{K}(G_{\bar{T}}, D) \geq t+1$. Hence, there exists a minimum $(t+1)$-level ordering $\mathcal{L}_{t+1}(G_{\bar{T}}, D) = \{L_1, \ldots, L_m\}$. Therefore every honest player v has at least $t + 1$ honest neighbors in previous levels of $\mathcal{L}_{t+1}(G_{\bar{T}}, D)$; by a simple induction we can show that v will decide on the dealer's value x_D.

($\Rightarrow$) If CPA is t-locally resilient then for any t-local corruption set, T, we have that every honest player in $G_{\bar{T}}$ decides on x_D and let the total number of rounds for the termination of the protocol is $m \in \mathbb{N}$. Define the sequence of sets $L_i = \{v \in V \setminus T \;\big|\; v \text{ decides in round } i \text{ of CPA }\}, i \in \{1, \ldots, m\}$. Then we will show by induction that the sequence $(L_i)_{i=1}^{m}$ is the (unique) minimum $(t + 1)$-level ordering on graph $G_{\bar{T}}$ with dealer D. Note first that $L_1 = \mathcal{N}(D) \setminus T$ because the players that decide in round 1 are exactly the neighborhood of the dealer. For the induction basis, we observe that $L_2 = \{v \in V \setminus T \;\big|\; \mathcal{N}(v) \cap L_1 \geq t + 1\}$ because the players that decide in round 2 are exactly those who will receive $t + 1$ identical messages from decided players in round 1. Assuming now that $L_k = \{v \in V \setminus \{T \cup \bigcup_{j=1}^{k-1} L_j\} : |\mathcal{N}(v) \cap \bigcup_{j=1}^{k-1} L_j| \geq t + 1\}$ it turns out that $L_{k+1} = \{v \in V \setminus \{T \cup \bigcup_{j=1}^{k} L_j\} : |\mathcal{N}(v) \cap \bigcup_{j=1}^{k} L_j| \geq t + 1\}$ due to the fact that the players that decide in round $k + 1$ are exactly the players who receive at least $t + 1$ messages from previously decided players. Since the above hold for any T, the claim follows. □

For exactly determining the maximum CPA resilience $t_{\max}^{\text{CPA}}$ we need the parameter,

$$\mathcal{T}(G, D) = \max\{t \in \mathbb{N} \;\big|\; \mathcal{M}(G, D, t) \geq t + 1\}$$

It should be clear by the above discussion that $\mathcal{T}(G, D)$ is exactly the maximum CPA resilience:

Corollary 8. $t_{\max}^{\text{CPA}}(G, D) = \mathcal{T}(G, D)$

A simple algorithm to compute the t-safety threshold requires exponential time (consider all the t-local corruption sets and compute $\mathcal{K}(G_{\bar{T}}, D)$ as in Section 4). Note that a different necessary and sufficient condition for CPA to be t-locally resilient was independently given in [11]. However, a superexponential time to check that condition is implicit (no algorithm is given in [11]).

Moreover, for computing $t_{\max}^{\text{CPA}} = \mathcal{T}(G, D)$ it suffices to perform at most $\log \delta \; \mathcal{M}(G, D, t)$ computations, where δ is the minimum degree of any node in $V \setminus (\mathcal{N}(D) \cup D)$.

6. CPA Uniqueness in *Ad Hoc* Networks

Based on the necessary and sufficient condition for CPA to be t-locally resilient in a graph G with dealer D we can now prove the *CPA uniqueness conjecture* for *ad hoc* networks, which was posed as an open problem in [1]. Another proof was first presented in [12], a subsequent work which was based on the preliminary version of this paper. The conjecture states that no algorithm can locally tolerate more traitors than CPA in networks of unknown topology.

We consider only the class of *t-locally safe* Broadcast algorithms which never cause a node to decide on an incorrect message under any t-local corruption set, cf.[1]

We assume the *ad hoc* network model, e.g. [1]. In particular we assume that nodes know only their own labels, the labels of their neighbors and the label of the dealer. We call a distributed Broadcast algorithm that operates under these assumptions an *ad hoc algorithm*.

Theorem 9. *Let $\mathcal{A}$ be a t-locally safe ad hoc Broadcast algorithm. If A is t-locally resilient for a graph G with dealer D then CPA is t-locally resilient for G, D.*

Proof. From Theorem 7 we have that, if CPA is not t-locally resilient in (G, D) then, $\mathcal{M}(G, D, t) = \min_{T:\ t\text{-local set}} \mathcal{K}(G_{\bar{T}}, D) \leq t$ which implies that there exists a t-local corruption set T s.t. in the remaining graph $G_{\bar{T}}$ a minimum $(t + 1)$-level ordering does not exist. From the definition of the $(t+1)$-level ordering we have that given the sequence of subsets of the nodes $V_{\bar{T}} = V \setminus (T \cup \{D\})$,

$$L_1 = \mathcal{N}_{G_T}(D),$$

$$L_i = \{v \in V_{\bar{T}} \setminus \bigcup_{j=1}^{i-1} L_j : |\mathcal{N}_{G_T}(v) \cap \bigcup_{j=1}^{i-1} L_j| \geq t + 1\}, 2 \leq i \leq m\}$$

there exists $h \in \mathbb{N}$ s.t. $\forall\, j \geq h,\ L_j = \emptyset$ and $\bigcup_{i=1}^{h} L_i \subsetneq V_{\bar{T}}$. We denote with $h_{\min}$ the minimum $h \in \mathbb{N}$ with the above property. We can assume wlog that $h_{\min} \geq 2$, because $h = 1$ implies that in the graph $G_{\bar{T}}$ the dealer D is disconnected from the rest of the graph which in turn, trivially implies that no algorithm will achieve Broadcast under the corruption of set T.

Let $A = \bigcup_{i=1}^{h_{\min}} L_i$ and $B = V_{\bar{T}} \setminus A$. It is now obvious from the definition of the minimum $(t + 1)$-level ordering that

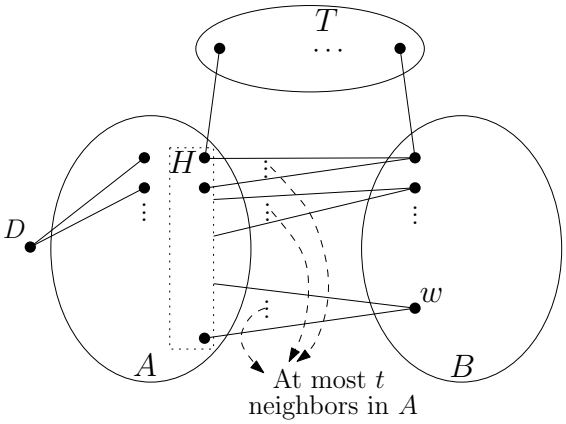

Figure 2: Partition of G in the subgraphs A, B, T

$\forall w \in B$, $|\mathcal{N}_{G_{\bar{T}}}(w) \cap A| \leq t$. Moreover $\bigcup_{i=1}^{h_{\min}} L_i \subsetneq V_{\bar{T}}$ implies that $B \neq \emptyset$. Finally let $H = \bigcup_{w \in B} (\mathcal{N}_{G_{\bar{T}}}(w) \cap A)$ and observe that H constitutes a node-cut in graph $G_{\bar{T}}$ separating the dealer D from the subgraph B. The partition of graph G in the three subgraphs A, B, T is depicted in Figure 2.

Let G' be a graph that results from G if we remove edges (u, v) from the set $E' = \{(u, v) | u, v \in A \cup T\}$ s.t. the set H becomes t-local in G' (e.g. we can remove all edges that connect nodes in the set $A \cup T$). The existence of a set of edges that guarantees such a property is implied by the fact that $\forall w \in B$, $|\mathcal{N}_{G_{\bar{T}}}(w) \cap H| \leq t$.

The proof is by contradiction. Suppose that there exists a t-locally safe Broadcast algorithm $\mathcal{A}$ which is t-locally resilient in graph G with dealer D. We consider the following executions σ and σ' of $\mathcal{A}$,

- Execution σ is on the graph G with dealer D, for the dealer's value we have that $x_D = 0$, the corruption set is the set T and in each round, all the players in this set perform the actions that are instructed to perform in the respective round of execution σ' where T is a set of honest players.

- Execution σ' is on the graph G' with dealer D, for the dealer's value we have that $x_D = 1$, the corruption set is the set H and in each round, all the players in this set perform the actions that are instructed to perform in the respective round of execution σ where H is a set of honest players.

Note that the corruption sets T, H are admissible corruption sets in G, G' respectively due to their t-locality. It is easy to see that the set $H \cup T$ is a node-cut which separates D from B in both G and G' and actions of all nodes of this cut are identical in both executions σ, σ'. Consequently the actions of any honest node $w \in B$ must be identical in both executions. Since by our assumption algorithm $\mathcal{A}$ is t-locally resilient on G with dealer D, w must decide on the dealer's message 0 in execution σ on G with dealer D. It must perform the same action in execution σ' on G' with dealer D. However, in this execution the dealer's message is 1. This contradicts the assumption that $\mathcal{A}$ is t-locally safe. □

We can observe that if the requirement for t-local safety is omitted, then the theorem does not hold. Intuitively we can use a protocol that assumes certain topological properties for the network such that this protocol is t-locally resilient in a family of graphs that have the same topological properties as the ones assumed.

More formally, in [1], Pelc and Peleg introduced another algorithm, the *Relaxed Propagation Algorithm*(RPA) which uses knowledge of the topology of the network and they proved that there exists a graph G with dealer D for which RPA is 1-locally resilient and CPA is not. So if we use RPA in an *ad hoc* setting assuming that the network is G then this algorithm will be t-locally resilient in G with dealer D while CPA won't. Non-t-local safety of RPA can easily be shown. This simple observation shows that the theorem does not hold if we consider algorithms which are not t-locally safe.

7. Conclusions

In this paper we developed three new graph parameters, depending on graph G and dealer-node D, for bounding the maximum resilience $t_{\max}^{\text{CPA}}$ of CPA. The first parameter, $\mathcal{K}(G, D)$, can be efficiently computed and can be used for approximating $t_{\max}^{\text{CPA}}$ within a factor of 2. The t-safety threshold, $\mathcal{M}(G, D, t)$, may be used as a test to check whether CPA is t-locally resilient for a certain graph G with dealer D and integer t. The third parameter, $\mathcal{T}(G, D)$, coincides with $t_{\max}^{\text{CPA}}$ and thus provides an exact characterization of the resilience of CPA as a function of the graph G and dealer D.

Finally, using the $\mathcal{M}(G, D, t)$ parameter we also prove that CPA is *unique* among the t-locally safe ad hoc broadcast algorithms, in a sense that for a graph G and dealer D if there exists a t-locally resilient, t-locally safe ad hoc broadcast algorithm, then CPA is also t-resilient in G, D thus answering the open problem of *CPA Uniqueness* posed in [1] in the affirmative.

Since the existence of a t-locally resilient Broadcast algorithm in a graph G with dealer D obviously depends on the topology of G, for a given local number of corruptions t we may define and compare the classes of

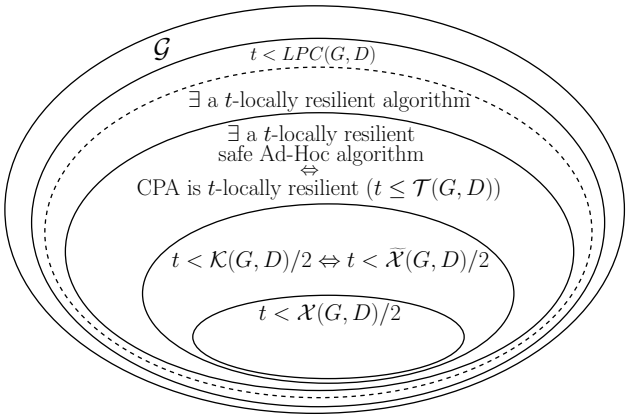

Figure 3: Overview of conditions related to the existence of t-locally resilient algorithms. Parameters $LPC(G, D)$ and $\mathcal{X}(G, D)$ are defined in [1] and $\bar{\mathcal{X}}(G, D)$ is from [10]. Continuous lines show strict inclusions.

graphs (with a designated dealer-node) determined by the properties and topological conditions that have appeared in the literature so far, including the ones defined in this paper. An overview of the corresponding classes and their relation is depicted in Figure 3.

The General Case (Corrupted Dealer) . It is well known that CPA works under the assumption that the dealer is honest. In order to address the case in which the dealer is corrupted one may observe that if the total number of traitors is strictly less than $n/3, n = |V|$, and the number of traitors in each node's neighborhood is bounded by $\min_{D \in V} \mathcal{T}(G, D)$ then we can achieve Reliable Broadcast by simulating any protocol for complete graphs as follows: each one-to-many (or even one-to-one) transmission is simulated by an execution of CPA. We observe that $\min_{D \in V} \mathcal{T}(G, D)$ may not be tight in this case. We can obtain a better bound if we define $\mathcal{M}(G, D, t)$ by considering only corruption sets of size strictly less than $n/3$. Subsequently, we derive an upper bound for Broadcast with corrupted dealer, namely $t \leq \min\left(\lceil n/3 \rceil - 1, \min_{D \in V} \mathcal{T}(G, D)\right)$. The deduction of a tight bound on the number of corrupted players as well as the study of more efficient algorithms for this problem are interesting open questions. Some remaining open problems are discussed below.

Approximation of $t_{\max}^{\text{CPA}}$. As was proved in subsequent work ([12]) the computation of $t_{\max}^{\text{CPA}}$ is NP-hard. It therefore makes sense to define another efficiently computable parameter yielding more tight bounds than $\mathcal{K}(G, D)$ in order to obtain an efficient approximation algorithm for $t_{\max}^{\text{CPA}}$ of ratio smaller than 2. Another direction which was proposed in [12] was to consider a varying bound $t(v)$ for the traitors of every neighborhood $\mathcal{N}(v)$; it seems that generalizing our approach of parameter $\mathcal{K}$ could provide an approximation scheme for this case too but even the definition of a meaningful approximation objective for this case is still an open question.

Wireless Networks. CPA is particularly suited for *ad hoc* networks, however it does not deal with radio network collisions. Only few articles have addressed the problem of reliable broadcast in radio networks so far and only for restricted graph topologies (e.g. [9], which deals with Byzantine failures, and [14], which studies the problem in the fault-tolerant model). It would therefore make sense to develop locally resilient protocols for the radio network model. To this end, one would have to consider models where the adversary cannot produce unlimited number of collisions otherwise it may block some messages permanently.

[1] A. Pelc, D. Peleg, Broadcasting with locally bounded byzantine faults, Inf. Process. Lett. 93 (3) (2005) 109–115.

[2] C. Litsas, A. Pagourtzis, G. Panagiotakos, D. Sakavalas, On the resilience and uniqueness of CPA for secure broadcast, IACR Cryptology ePrint Archive 2013 (2013) 738.
URL `http://eprint.iacr.org/2013/738`

[3] L. Lamport, R. Shostak, M. Pease, The byzantine generals problem, ACM Trans. Program. Lang. Syst. 4 (3) (1982) 382–401.

[4] J. A. Garay, Y. Moses, Fully polynomial byzantine agreement for $n > 3t$ processors in $t + 1$ rounds, SIAM J. Comput. 27 (1) (1998) 247–290.

[5] D. Dolev, The byzantine generals strike again, J. Algorithms 3 (1) (1982) 14–30.

[6] D. Dolev, C. Dwork, O. Waarts, M. Yung, Perfectly secure message transmission, J. ACM 40 (1) (1993) 17–47.

[7] M. Franklin, R. N. Wright, Secure communication in minimal connectivity models, Journal of Cryptology 13 (2000) 9–30.

[8] M. V. N. A. Kumar, P. R. Goundan, K. Srinathan, C. P. Rangan, On perfectly secure communication over arbitrary networks, in: PODC, ACM, New York, NY, USA, 2002, pp. 193–202.

[9] C.-Y. Koo, Broadcast in radio networks tolerating byzantine adversarial behavior, in: PODC, ACM, 2004, pp. 275–282.

[10] A. Ichimura, M. Shigeno, A new parameter for a broadcast algorithm with locally bounded byzantine faults, Inf. Process. Lett. 110 (12-13) 382–401.

[11] L. Tseng, N. Vaidya, V. Bhandari, Broadcast using certified propagation algorithm in presence of byzantine faults, Information Processing Letters 115 (4) (2015) 512 – 514. doi:http://dx.doi.org/10.1016/j.ipl.2014.11.010.

[12] A. Pagourtzis, G. Panagiotakos, D. Sakavalas, Reliable broadcast with respect to topology knowledge, in: DISC, Austin, TX, USA, 2014, pp. 107–121.

[13] C. Litsas, A. Pagourtzis, D. Sakavalas, A graph parameter that matches the resilience of the certified propagation algorithm, in: ADHOC-NOW, Wrocław, Poland, 2013, Springer, 2013, pp. 269–280.

[14] E. Kranakis, D. Krizanc, A. Pelc, Fault-tolerant broadcasting in radio networks, Journal of Algorithms 39 (1) (2001) 47 – 67.