A new parameter for a broadcast algorithm with locally bounded Byzantine faults

Akira Ichimura[a], Maiko Shigeno[a,1,*]

[a] *Graduate School of Systems and Information Engineering, University of Tsukuba, 305-8573, Japan.*

Abstract

This paper deals with broadcasting in a network with t-locally bounded Byzantine faults. One of the simplest broadcasting algorithms under Byzantine failures is referred to as a certified propagation algorithm (CPA), which is the only algorithm we know that does not use any global knowledge of the network topology. Hence, it is worth focusing on a graph-theoretic parameter such that CPA will work correctly. Using the theory of maximum adjacency (MA) ordering, a new graph-theoretic parameter for CPA is proposed. Within a factor of two, this parameter approximates the largest t such that CPA works for t-locally bounded Byzantine faults.

Keywords: graph algorithm, fault tolerance, broadcasting, Byzantine faults, MA ordering,

1. Introduction

In bidirectional communication network, it is important to analyze the parameters of the network for which a communication algorithm works correctly despite a limited number of failures and with no knowledge of their locations. Of all possible types of faults, Byzantine faults model the worst-case fault scenario. Byzantine failures demonstrate damaging behavior: they stop messages from being transmitted, and they transmit by false messages maliciously. We assume that Byzantine failures are restricted by the content of messages but they cannot affect schedules. Since Byzantine failures represent worst-case faults, some algorithms working correctly in networks with Byzantine failures can be safely used under any assumptions involving faults. Moreover, there are several other fault models depending on the number and location of faults. One of these models is t-locally bounded, in which at most t permanent malicious failures are permitted in the neighborhood of each vertex.

*Corresponding author

Email addresses: ichimu50(at) sk.tsukuba.ac.jp (Akira Ichimura), maiko(at) sk.tsukuba.ac.jp (Maiko Shigeno)

[1]Supported in part by the MEXT Grant-in-Aid for Scientific Research (C) No. 19510137 and by the Kayamori Foundation of Informational Science Advancement.

In this paper, we deal with broadcasting in a network with t-locally bounded Byzantine faults. Broadcasting is one of the most important procedures in communications. It involves the task of transmitting a message that has originated at one processor, called a source, to all other processors in the network. Fault-tolerant broadcasting has been extensively studied (e.g. Pelc [4]). Koo [2] investigated broadcasting in special networks under our fault model, and devised a simple broadcasting algorithm that is referred to as a Certified Propagation Algorithm (CPA). Pelc–Peleg [5] established a graph-theoretic parameter such that the CPA works correctly under our fault model in any network. They also found a graph-theoretic parameter such that no broadcast algorithm can work under our fault model. So far, CPA is the only broadcast algorithm we know that works under t-locally bounded Byzantine faults that does not use any global knowledge of the network topology. Hence, it is worth focusing on a graph-theoretic parameter such that CPA will work correctly. Using the theory of maximum adjacency (MA) ordering, we propose a new graph-theoretic parameter for CPA. Within a factor of two, this parameter approximates the largest t such that CPA works for t-locally bounded Byzantine faults.

2. Broadcast algorithm

We represent a communication network as a connected undirected graph $G = (V, E)$, where each vertex $v \in V$ corresponds to a processor and each edge $e \in E$ corresponds to a communication line between processors. For $v \in V$, let $\Gamma(v)$ be the neighborhood of v including v, i.e., $\Gamma(v) = \{u \in V \mid (v, u) \in E\} \cup \{v\}$. For a positive integer t, a subset W of V is called *t-local* if $|W \cap \Gamma(v)| \leq t$ holds for any $v \in V$. Let us consider a broadcast algorithm from an arbitrary source vertex under any t-local set of Byzantine faults. Two requirements of broadcast algorithms are that they never cause a vertex to accept an incorrect message from a given source and that they deliver the message to all the vertices. The assumption behind broadcast algorithms is that the source is fault-free and that all vertices know which vertex is the source. We call a broadcast algorithm *t-locally fault-tolerant* if it works correctly from an arbitrary source under any t-local set of Byzantine faults.

The simplest t-locally fault-tolerant broadcast algorithm is CPA devised by Koo [2]. The following gives a precise formulation of CPA for a t-local set of faults.

Step 0 A given source s sends a message to all its neighbors $\Gamma(s) \setminus \{s\}$.

Step 1 Each vertex in $\Gamma(s) \setminus \{s\}$ accepts the message received from source s, and sends it to all its neighbors.

Step 2 If there is a vertex $v \in V \setminus \Gamma(s)$ which has not accepted any message yet and it receives $t + 1$ same messages from distinct neighbors, v accepts the message and sends it to all its neighbors.

Step 3 If all the vertices accept the message, then stop. Otherwise, go to Step 2.

Pelc-Peleg [5] found a graph-theoretic parameter such that CPA works correctly. For a graph G and for any $s, v \in V$, define $X_s(v) = |\{u \in V \mid d_s(u) < d_s(v)\}|$, where $d_s(v)$ is the shortest path length from s to v. Let $X(G) = \min\{X_s(v) \mid s \in V, v \in V \setminus \Gamma(s)\}$.

Lemma 1 ([5]Lemma 2.1). *For a graph G, CPA is t-locally fault-tolerant if $t < X(G)/2$.*

Pelc-Peleg [5] also established a different parameter $LPC(G)$ such that, for a graph G and for $t \geq LPC(G)$, no broadcast algorithm can work under t-locally bounded Byzantine faults. A subset C of vertices is called a *t-local pair cut* if a subgraph deleting C has at least two connected components and C can be partitioned into two t-local sets. The parameter $LPC(G)$ is defined by the smallest nonnegative integer t such that G has a t-local pair cut.

Property 2. *To compute $LPC(G)$ is NP-hard.*

Proof. We transform a set splitting problem known as NP-hard [1] to a problem to compute $LPC(G)$. Given a collection $\mathcal{S}$ of 3-element subsets of a finite set X, the set splitting problem decides whether there is a partition of X into two subsets X_1 and X_2 such that no subset in $\mathcal{S}$ is entirely contained in either X_1 or X_2.

Let $\mathcal{S}+$ be a multiple collection adding dummy subsets $\{v\}$ to $\mathcal{S}$ such that the cardinality of $\{s \in \mathcal{S}+ \mid s \ni v\}$ is at least six for each $v \in X$. A complete graph with vertex set $\mathcal{S}+$ and a copy of it are denoted by $K_{\mathcal{S}+}$ and $K'_{\mathcal{S}+}$, respectively. We construct a graph G^{SSP} with vertex set $V(G^{\mathrm{SSP}}) = V(K_{\mathcal{S}+}) \cup V(K'_{\mathcal{S}+}) \cup X$ and edge set $E(G^{\mathrm{SSP}}) = E(K_{\mathcal{S}+}) \cup E(K'_{\mathcal{S}+}) \cup \{(v, s), (v, s') | v \in X, s \in \mathcal{S}+, v \in s\}$, where s' is a node in $V(K'_{\mathcal{S}+})$ which is a copy of $s \in \mathcal{S}+$. If a subgraph of G^{SSP} deleting $C(\subseteq V(G^{\mathrm{SSP}}))$ has at least two connected components and $X \setminus C \neq \emptyset$, C contains $\Gamma(v) \cap V(K_{\mathcal{S}+})$ or $\Gamma(v) \cap V(K'_{\mathcal{S}+})$ for some $v \in X$. Since each $v \in X$ has at least six neighbor in both $V(K_{\mathcal{S}+})$ and $V(K'_{\mathcal{S}+})$, C is a t-local pair cut with $t \geq 3$. We next consider the case of $C = X$. We can partition X into two 2-local sets in G^{SSP}, if and only if the set splitting problem has a desired partition X_1 and X_2. Therefore, we have $LPC(G^{\mathrm{SSP}}) = 2$, if and only if the set splitting problem has a desired partition. □

3. MA ordering parameter

Using the theory of a maximum adjacency (MA) ordering [3], we establish a new upper bound on t for which CPA is t-locally fault-tolerant. For any vertex $v \in V$ and subset $W \subseteq V$ of vertices, let $\delta(W, v) = |\{(w, v) \in E \mid w \in W\}|$. An MA ordering is defined by a total ordering $\sigma = (v_1, v_2, \ldots, v_n)$ of vertices in V such that $\delta(W_{i-1}, v_i) \geq \delta(W_{i-1}, v_j)$ holds for all i, j with $1 \leq i < j \leq n$, where $W_0 = \emptyset$ and $W_i = \{v_1, v_2, \ldots, v_i\}$. This ordering is also referred to as a legal ordering and as a max-back ordering. In our case, with respect to source s, let $W_0^s = \Gamma(s)$ and

$\sigma^s = (v_1^s, v_2^s, \dots)$ be an MA ordering for $V \setminus \Gamma(s)$, i.e., $\delta(W_{i-1}^s, v_i^s) \geq \delta(W_{i-1}^s, v_j^s)$ holds for all i, j with $1 \leq i < j \leq |V \setminus \Gamma(s)|$, where $W_i^s = \{v_1^s, v_2^s, \dots, v_i^s\}$. Although such an ordering is not unique, we can define a graph-theoretical parameter from arbitrary MA ordering.

Lemma 3. *Let $\sigma^s = (v_1^s, v_2^s, \dots)$ be an MA ordering with respect to source s. Then, the value of $\min\{\delta(W_{k-1}^s, v_k^s) \mid k = 1, 2, \dots\}$ is uniquely determined regardless of the MA ordering.*

Proof. For distinct MA orderings $\sigma^s = (v_1^s, v_2^s, \dots)$ and $\hat{\sigma}^s = (\hat{v}_1^s, \hat{v}_2^s, \dots)$, assume that $\min\{\delta(W_{k-1}^s, v_k^s) \mid k = 1, 2, \dots\} < \min\{\delta(\hat{W}_{k-1}^s, \hat{v}_k^s) \mid k = 1, 2, \dots\}$, where $\hat{W}_k^s = \{\hat{v}_1^s, \hat{v}_2^s, \dots, \hat{v}_k^s\}$. Let $\min\{\delta(W_{k-1}^s, v_k^s) \mid k = 1, 2, \dots\} = \delta(W_{\ell-1}^s, v_\ell^s)$ and $v_\ell^s = \hat{v}_j^s$. Since $\delta(W_{\ell-1}^s, v_\ell^s) < \delta(\hat{W}_{j-1}^s, \hat{v}_j^s) = \delta(\hat{W}_{j-1}^s, v_\ell^s)$, we have $\hat{W}_{j-1}^s \setminus W_{\ell-1}^s \neq \emptyset$. Let $\hat{v}_m^s$ be the vertex which has the smallest index in $\hat{\sigma}^s$ among $\hat{W}_{j-1}^s \setminus W_{\ell-1}^s$. From the rule of choosing m, we obtain $(\hat{W}_{j-1}^s \setminus W_{\ell-1}^s) \cap \hat{W}_{m-1}^s = \emptyset$, i. e. $\hat{W}_{m-1}^s \subseteq W_{\ell-1}^s$. Thus

$$\min\{\delta(\hat{W}_{k-1}^s, \hat{v}_k^s) \mid k = 1, 2, \dots\} \leq \delta(\hat{W}_{m-1}^s, \hat{v}_m^s) \leq \delta(W_{\ell-1}^s, \hat{v}_m^s) \leq \delta(W_{\ell-1}^s, v_\ell^s)$$

holds, which contradicts our assumption. □

Hence, a parameter $\tilde{X}(G) = \min\{\delta(W_{k-1}^s, v_k^s) \mid s \in V, k = 1, 2, \dots\}$ is well-defined.

Theorem 4. *For a graph G, CPA is t-locally fault-tolerant if $t < \tilde{X}(G)/2$.*

Proof. With respect to a given source s, let $\sigma^s = (v_1^s, v_2^s, \dots)$ be an MA ordering and $W_i^s = \{v_1^s, v_2^s, \dots, v_i^s\}$. We have $|W_{i-1}^s \cap \Gamma(v_i^s)| = \delta(W_{i-1}^s, v_i^s) \geq \tilde{X}(G) > 2t$, for any vertex $v_i^s \in V \setminus \Gamma(s)$. Thus, at the first iteration of CPA, Step 2 can select v_1^s, which receives at least $t + 1$ same messages. By induction, we can show that, at the ith iteration, Step 2 can select v_i^s and that, at the end of the ith iteration, W_i^s is a set of vertices that accept the message. Hence, CPA works correctly. □

The following property shows that parameter $\tilde{X}(G)$ is more efficient than $X(G)$ for the upper bound on t for which CPA is t-locally fault-tolerant.

Property 5. *For any graph G, $\tilde{X}(G) \geq X(G)$ holds.*

Proof. Note that, for any s' and $v' \in V \setminus \Gamma(s')$, $X_{s'}(v') \geq X(G)$ holds. Let $\tilde{X}(G) = \delta(W_{\ell-1}^s, v_\ell^s)$. If we assume $\tilde{X}(G) < X(G)$, we obtain $X_s(v_\ell^s) > \delta(W_{\ell-1}^s, v_\ell^s)$, which implies that there exists $\hat{v}$ that does not belong to $W_{\ell-1}^s$ and that is nearer from s than v_ℓ^s. If there are many such vertices, we choose the one whose distance from s is minimum, i.e., we choose a vertex attaining $\min\{d_s(v) \mid v \in X_s(v_\ell^s) \setminus W_{\ell-1}^s\}$.

Let the order of $\hat{v}$ in σ^s be v^s_m. From the definition of MA ordering, we have $\delta(W^s_{\ell-1}, v^s_\ell) \geq \delta(W^s_{\ell-1}, v^s_m)$. Hence, we obtain

$$X_s(v^s_m) \geq X(G) > \tilde{X}(G) = \delta(W^s_{\ell-1}, v^s_\ell) \geq \delta(W^s_{\ell-1}, v^s_m).$$

Thus, there exists a vertex v that does not belong to $W^s_{\ell-1}$ and that is nearer from s than v^s_m. This fact contradicts the choice of v^s_m. □

Moreover, we can show a graph G so that the difference between $\tilde{X}(G)$ and $X(G)$ is large.

Example 1. *For a positive integer h, graph G^h has vertex set $V(G^h) = \{w_1, w_2, \ldots, w_h\} \cup \{u_1, u_2, \ldots, u_h\}$ and edge set $E(G^h) = \{(w_i, u_j) \mid 1 \leq i < j \leq h\} \cup \{(u_i, u_j) \mid 1 \leq i < j \leq h\} \cup \{(w_i, w_j) \mid 1 \leq i < j \leq h\}$. Obviously, we obtain $X(G^h) = X_{u_1}(w_{h-1}) = 1$ and $\tilde{X}(G^h) = h - 1$. Figure 1 shows graph G^h with $h = 5$. Indeed, CPA works correctly on graph G^h for $t \leq \lceil (h-1)/2 \rceil - 1$. However, for $t \geq \lceil (h-1)/2 \rceil$, CPA stops before all the vertices accept the message if u_1 is the source and $u_2, \ldots, u_{\lceil (h-1)/2 \rceil + 1}$ are Byzantine failures.*

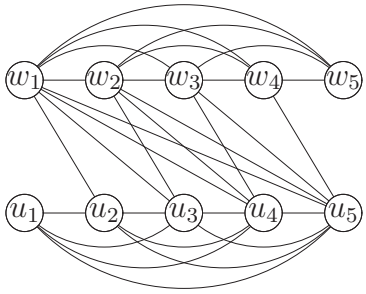

Figure 1: Graph G^h with $h = 5$

The parameter $\tilde{X}(G)$ also establishes a lower bound on t for which CPA does not work correctly under any t-local set of Byzantine faults.

Theorem 6. *For any graph G, CPA is not t-locally fault-tolerant if $t > \tilde{X}(G)$.*

Proof. Assume that CPA is t-locally fault-tolerant for $t > \tilde{X}(G)$. Let $\tilde{X}(G) = \delta(W^s_{\ell-1}, v^s_\ell)$. With W, we denote a set of vertices that accept the message from s before Step 2 of CPA selects v^s_ℓ. Since v^s_ℓ receives $t+1$ same messages, $\delta(W, v^s_\ell) > t$ holds. The fact $\delta(W, v^s_\ell) > \delta(W^s_{\ell-1}, v^s_\ell)$ implies $W \setminus W^s_{\ell-1} \neq \emptyset$. Let $\hat{v}$ be a vertex selected first at Step 2 from $W \setminus W^s_{\ell-1}$, and let $\widehat{W}$ be a set of vertices that accept the message before Step 2 selects $\hat{v}$. From the definition of $\hat{v}$, we have $\widehat{W} \subseteq W^s_{\ell-1}$. Therefore, we obtain $\delta(\widehat{W}, \hat{v}) \leq \delta(W^s_{\ell-1}, \hat{v}) \leq \delta(W^s_{\ell-1}, v_\ell) = \tilde{X}(G) < t$, which contradicts that $\hat{v}$ receives at least $t+1$ messages. □

Pelc-Peleg[5] established by $LPC(G)$ a lower bound on t for which there was no t-locally fault-tolerant algorithm. Since $\tilde{X}(G)$ gives a lower bound for only CPA, $\tilde{X}(G)$ is expected to a better lower bound than $LPC(G)$. However, there exists no relation between $\tilde{X}(G)$ and $LPC(G)$.

Example 2. *Let $G_{n'}$ be the cartesian product of the n'-complete graph $K_{n'}$ and the 2-path P_2. That is to say, the vertex set $V(G_{n'})$ is $V(K^1_{n'}) \cup V(K^2_{n'}) \cup V(K^3_{n'})$, where $K^i_{n'}$ $(i = 1, 2, 3)$ are copies of $K_{n'}$, and the edge set $E(G_{n'})$ is $E(K^1_{n'}) \cup E(K^2_{n'}) \cup E(K^3_{n'}) \cup \{(v^1, v^2), (v^2, v^3) \mid v \in V(K_{n'})\}$, where v^i denotes a copy vertex of v in $K^i_{n'}$. Figure 2 shows graph $G_{n'}$ with $n' = 5$. For a source node s^1 in $V(K^1_{n'})$, $\Gamma(s^1) = V(K^1_{n'}) \cup \{s^2\}$ and $W_{n'-1} = V(K^1_{n'}) \cup V(K^2_{n'})$ holds. Hence, we have $\delta(W_{n'-1}, v_{n'}) = 1$ and $\tilde{X}(G) = 1$. Meanwhile, we shall show $LPC(G_{n'}) \geq \lceil n'/4 \rceil$. When a subgraph deleting $C(\subseteq V(G_{n'}))$ has at least two connected components, $|C \cap (V(K^1_{n'}) \cup V(K^2_{n'}))| \geq n'$ or $|C \cap (V(K^2_{n'}) \cup V(K^3_{n'}))| \geq n'$ holds. Without loss of generality we assume that $|C \cap (V(K^1_{n'}) \cup V(K^2_{n'}))| \geq n'$. If C can be partitioned into two t-local sets, we have $|C \cap V(K^i_{n'})| \leq 2t$ for $i = 1, 2$, since there exists a vertex being adjacent to all of $C \cap V(K^i_{n'})$. Thus, we obtain $n' \leq |C \cap (V(K^1_{n'}) \cup V(K^2_{n'}))| = |C \cap V(K^1_{n'})| + |C \cap V(K^2_{n'})| \leq 4t$, which implies that $t \geq \lceil n'/4 \rceil$. Therefore, this graph $G_{n'}$ with $n' > 4$ shows an example where $\tilde{X}(G)$ is smaller than $LPC(G)$.*

Graph G_c in Figure 2 shows an example where $\tilde{X}(G)$ is larger than $LPC(G)$. We can verify $\tilde{X}(G_c) = 2$. However, since $C_1 \cup C_2$ is a 1-local pair cut for $C_1 = \{x, x'\}$ and $C_2 = \{y, y'\}$, we obtain $LPC(G_c) = 1$. Thus, when there exists one Byzantine faulty vertex, no broadcast algorithm works. Hence, CPA does not work correctly with one faulty Byzantine vertex.

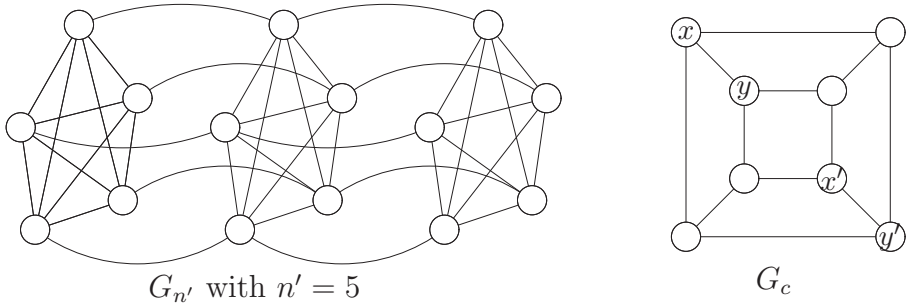

Figure 2: Examples of difference in inequality relation between $\tilde{X}(G)$ and $LPC(G)$

From the above example, both $\tilde{X}(G)$ and $LPC(G)$ are used to determine whether CPA is t-locally fault-tolerant. However, we can conclude that $\tilde{X}(G)$ is most useful than $LPC(G)$. Although to compute $LPC(G)$ is NP-hard as proved in Property 2, $\tilde{X}(G)$ is calculated efficiently. Indeed, an MA ordering with respect to a source can be found in linear time [3]. So, we can obtain $\tilde{X}(G)$ in $O(|V|(|V| + |E|))$ time.

4. Conclusion

We presented new upper and lower bounds on t for which CPA is t-locally fault-tolerant, using the theory of an MA ordering. Theorems 4 and 6 imply that $\tilde{X}(G)$ approximates the largest t such that CPA is t-locally fault-tolerant within a factor of two. The MA ordering is known to derive algorithmic results attained in the area of graph connectivity, where some other total orderings of vertices are also introduced. It is open whether these total orderings get tighter bounds on t for which CPA is t-locally fault-tolerant.

References

[1] M. R. Garey, D. S. Johnson, *Computers and Intractability*, Freeman, 1979.

[2] C. Y. Koo, Broadcast in radio networks tolerating Byzantine adversarial behavior, Proc. PODC, 2004.

[3] H. Nagamochi, T. Ibaraki, *Algorithmic Aspects of Graph Connectivity*, Cambridge University Press, 2008.

[4] A. Pelc, Fault-tolerant broadcasting and gossiping in communication networks, Networks 28 (1996), 143-156.

[5] A. Pelc, D. Peleg, Broadcasting with locally bounded Byzantine faults, Inf. Process. Lett. 93 (2005), 109-115.