科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　５　日現在

機関番号：１３３０２
研究種目：基盤研究(C)
研究期間：2011～2013
課題番号：２３５０００６０

研究課題名（和文）自律分散ロボット群向けの実用的非同期モデルの設計と耐故障分散アルゴリズムの研究

研究課題名（英文）Fault-tolerant distributed algorithms and realistic models for groups of autonomous mobile robots

研究代表者
ＤＥＦＡＧＯ　Ｘａｖｉｅｒ（DEFAGO, Xavier）

北陸先端科学技術大学院大学・情報科学研究科・准教授

研究者番号：７０３３３５５７

交付決定額（研究期間全体）：（直接経費）　　3,000,000円、（間接経費）　　900,000円

研究成果の概要（和文）：本研究では、フォールトトレラントで信頼性の高いマルチロボットシステムの開発を改善することを目指しています。そのため、移動ロボット群、フォールトトレラント分散システム、アルゴリズム等の分野の関連を研究します。特に、理論的なモデルと問題でも、その実用さを考え直す事が必要です。
本研究では、以下の結果も含む：①一部のロボットが故障しても全体が進めるアルゴリズム、②グラフ探検、③行動計画作成、④カスケード接続の障害。

研究成果の概要（英文）：This research aims at improving the development of fault-tolerant and reliable multi-robots systems. In particular, this includes relating formal models developed in the field of fault-tolerant distributed systems to the problem of mobile robot coordination. The purpose of such a model is to study the correctness of algorithms and identify the minimum capabilities (i.e., set of sensors) that the individual robots must have in order to reliably solve a given problem as a group. At the same time, it is essential that both model and problem be practically accurate so that results are directly applicable to real systems.
In particular, we have obtained important results for several problems, among which,
(1) gathering of robots when some robots or their sensors may fail, (2) exploration of a discrete environment, (3) motion planning of multiple-robots, and (4) cascading failures in large systems.

研究分野：分散システム

科研費の分科・細目：情報学、計算機システム・ネットワーク

キーワード：分散アルゴリズム　分散システム　ロボット群　モデル化　合意問題　自己安定　センサーネットワーク

１．研究開始当初の背景

The motivation for this research comes from the observation that there is a great need for guaranteed fault-tolerant operations of multi-robots systems, especially given the role as an infrastructure that such systems are envisioned to take in the future.

This research aims at improving the development of fault-tolerant and reliable multi-robots systems. In particular, this includes relating formal models developed in the field of fault-tolerant distributed systems to the problem of mobile robot coordination. As in most areas of engineering, agreement on a formal model in which one can design, study, evaluate, and prove the correctness of algorithms is essential for the maturity of a field, but is proving surprisingly elusive in this case.

It is especially important to obtain results that are theoretically sound and correct, yet practically relevant. In particular, we identify needs in the following areas:
(1) Multi-robots coordination algorithms
(2) Fault-tolerance mechanisms
(3) Fundamental limits and complexity

２．研究の目的

The goal of this project is to relate formal models developed in the field of fault-tolerant distributed systems to the problem of mobile robot coordination, with the objective of providing the basis for stronger and more reliable multi-robots systems.

Two important aspects are to define a formal model based on realistic assumptions for autonomous mobile robots, and to develop fault-tolerant decentralized algorithms for self-organizing groups of those robots. The purpose of such a model is to study the correctness of algorithms and identify the minimum capabilities (i.e., set of sensors) that the individual robots must have in order to reliably solve a given problem as a group. At the same time, it is essential that the model be practically accurate so that results obtained in the model are directly applicable to real systems.

Many projects aimed at swarms of mobile robots envision applications including exploration, emergency and disaster relief, as well as maintenance and monitoring tasks. All of these objectives assume systems that must operate non-stop, under harsh conditions, and with high safety and reliability requirements due to interactions with humans. Such systems require formal guarantees that cannot be provided by experimentation and simulation alone, but also require a rigorous model that allows for formal verification.
There is currently a very large gap between three different relevant approaches:

(1) **Empirical work on robotic swarms**
Most work focus on developing heuristics or observing spontaneous self-organization emerging out from the interactions of simple mechanisms. This provides very valuable insight on natural phenomena, but it fails to provide guarantees on the behavior of the system. Because of the lack of a formal model, it is impossible to prove that proposed solutions always operate as intended. The need for a formal system has been first stated by Cao et al. and is increasingly recognized in that community.

(2) **Mobility work on mobile ad hoc networks (MANET) and sensor networks**.
Work on MANET and sensor networks (mesh networks) extend conventional distributed systems by considering that nodes are mobile. This mobility impacts the connectivity of the network and results in a system with a dynamic topology. Unlike with mobile robots, mobility here is not an output of the algorithms. The limited representation of mobility is thus inadequate for robot algorithms.

(3) **Theoretical work on cooperative mobile robotics**.
Pioneered by the work of Suzuki and Yamashita, a computational approach to cooperative mobile robotics provides a formal system model in which algorithms and minimal assumptions are being studied. Although this allows an investigation of the fundamental limits of coordination (e.g., coordination in the face of malicious robots), it is difficult to actually adapt the proposed algorithms for real systems due to the gap between assumptions made in the model and the reality in actual robotic systems. In particular, we find three important issues that contribute to this gap:

① *Sensors and motors have infinite accuracy.* It is natural to leave sensor accuracy issues out of a model aimed at studying higher-level issues. However, infinite accuracy has lead to focus on problem details that have little relevance in practice, such as an overemphasis on the difference between convergence and formation.

② *Explicit communication is left out of the model.* Although the models allow communication to be used implicitly as a means to provide some synchronization between robots, problems such as cooperative motion planning or global coordinate synchronization do require a model including both communication and mobility to be studied properly.

③ *Avoiding collisions*. The third issue is that, with very few exceptions, none of the theoretical work considers that robots may hide each other, and try to avoid the collisions of robots.

The originality of this research project is that we will consider both practical and theoretical aspects of the problem and try to close the gap between them.

3．研究の方法

Addressing the problem requires to consider many different aspects of multi-robots systems coordination. In order to study this, it is essential to progress one direction at a time. The general methodology is to start from existing theoretical results, and change one aspect of the model or problem with a more realistic one. There are several directions:

(1) ***Discrete environments***.
Since it is impossible in practice to rely on sensors with infinite accuracy, coordination algorithms must consider this aspect. There are three main approaches:
① *Redefine problems* to account for inaccuracies in the results, and take account of inaccuracies in computations at every stage.
② *Consider a discrete environment*, such that cell size is computed to cover sensor inaccuracies.
③ *Avoid using sensor information* where accuracy is critical. Of course, this solves the problem. This is however not always possible, and it boils down to finding what are the minimal assumptions to solve a given problem.

(2) ***Fault-tolerance***.
There are several general approaches to fault-tolerance, and how to cope with them (see Fig.1):
① *Masking fault-tolerance (Fig.1a)*. A masking fault-tolerant system continues operating as normal even after facing a bounded number of component failures (here, a component is a robot). This approach is strong to address permanent faults.
② *Non-masking fault-tolerance (Fig.1b)*. A non-masking fault-tolerant system may behave wrongly while faults occur, but always recovers a correct behavior after that. This addresses transient faults.
③ *Fail-safe behavior (Fig.1c)*. A fail-safe system is designed so that, when normal behavior cannot be guaranteed, the system avoids severe consequences by forcing itself into a fail-safe state.
④ *Graceful degradation (Fig.1d)*. A system may have several degraded operational states, in which, depending on the severity of faults, the system operates in a degraded mode (e.g., without ensuring some of the functionality) until recovery is possible. Thus, the system can still remain available for a subset of its operations, until it can fully recover.

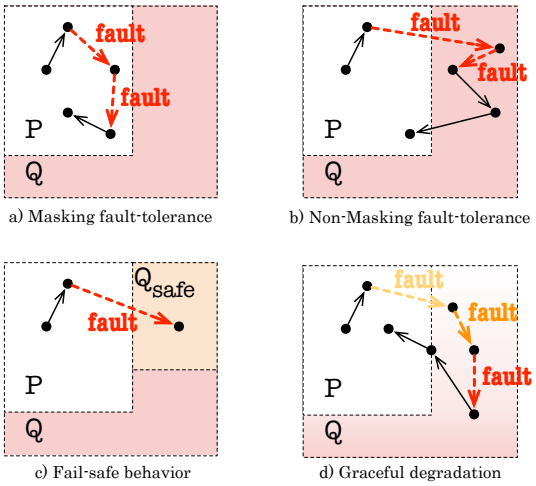


Fig. 1 Modes of fault-tolerance

(3) ***Cascading failures and error propagation***.
In large systems, the failure of a robot can trigger the failure of its neighbors. It is thus important to find a way to contain it. In particular, if a robot gets erratic due to, say, cosmic rays or radiation, it may affect its neighbors by sending them corrupted messages, or simply through its own behavior.

４．研究成果

The results that we have obtained can be classified into the three categories described in the previous section.

(1) ***Discrete environments***.
We have considered several problems in which robots evolve in a discrete environment. In particular, we have studied the following problems under the assumptions that robots have no orientation and are active independently:
① Exploring the environment [7,9]. The problem is to ensure that all places are visited infinitely often. We have been able to characterize the problem in a ring topology, when robots cannot rely on orientation. We have identified the algorithms that can solve the problem, and some of the conditions under which the problem cannot possibly be solved.
② Collision-avoiding motion planning. Each robot must reach its own destination, which is distinct from but unknown to the other robots. We have found some interesting necessary conditions for general graphs, and almost completely characterized the problem in the case of a grid. One of the core sub-problems is the ability to exchange information between robots, in particular on their destinations. These results are currently under review for publication.

2) ***Fault-tolerance***.
Algorithms designed for the model of Suzuki and Yamashita are often self-stabilizing, due to the common assumption that robots discard memory of past actions. Self-stabilization is a desired property because it provides some level of non-masking fault-tolerance.
① Non-terminating executions come of often as a result of being unable to break symmetries. One approach to breaking symmetries consists in relying on some compass information. The drawback is that compasses are extremely inaccurate sensors. With others, we have thus studied the problem of achieving gathering using compasses that are potentially inaccurate. We have found bounds on how much the compasses can differ for the problem to be still achievable [5].
② By introducing the notion of permanent faults (crash and Byzantine), we have found that such algorithms are particularly weak with respect to permanent faults. However, two methods can help address this situation:
a) Synchrony assumptions, such as, bounded activations or mutually exclusive one can help greatly in solving basic agreement problems in the face of permanent faults.
b) Randomization provides a way to break symmetries and solve the problems in usually constant expected time, even under a large number of permanent crash faults. E.g., Figure 2 depicts all state transitions of a probabilistic gathering algorithm that tolerates any number of permanent (or transient) crash faults, as long as at least one robot is not crashed permanently. From all possible states there is a strictly positive probability to reach the only absorbing state, in which the robots are gathered.

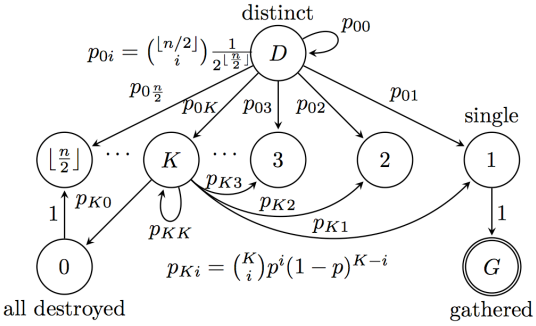
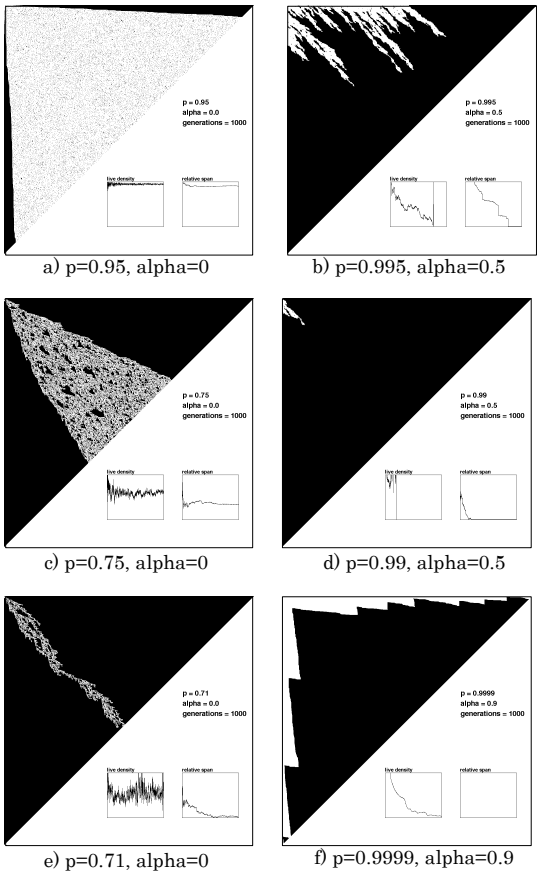


Fig. 2 State transitions of probabilistic gathering with crash faults.

3) ***Cascading failures***.
Consider a very large system in which a faulty robot may become faulty yet remain operational with a corrupted behavior (e.g., state corrupted by radiations, code infected by a virus or compromised by an intruder). With some probability p, the corrupted robot may affect some of its neighbors. Conversely, a sane robot may detect the attempt with probability q, and start a containment strategy by warning its own neighbors of the situation. When the precedence of warning messages over corruption messages is given by a probability alpha, the question is under what values of the parameters p, q, alpha can the cascading be contained or not.
We have considered simple containment strategies, in which the warning message is given a maximum hop-count, and studied the problem in various classes of graphs: finite grid, infinite grid, unit disc geometric random graphs, and small-world graphs.
We have found that, in each case, there is a threshold, above which the cascading is

containment with probability 1, and below which it is contained with probability close to 0. We have also found that cascading can be contained in many cases in regular graphs and, in particular, in the grid.
Figure 3 illustrates the propagation in the case of an infinite grid, for various values of p and alpha, but when q=1, and when warning messages propagate forever. The propagation begins from the upper left corner and advances toward the lower right corner, until the center. A white pixel is a faulty robot and a black pixel one that contributed to the containment.



a) p=0.95, alpha=0　b) p=0.995, alpha=0.5
c) p=0.75, alpha=0　d) p=0.99, alpha=0.5
e) p=0.71, alpha=0　f) p=0.9999, alpha=0.9

Fig. 3 Cascading failures in a grid: propagation patterns according to infection rate (p) and priority of containment messages (alpha). Cascading starts from the upper left corner (shows one of four quadrants). White pixels represent faulty nodes.

Depending on the values of the parameters p and alpha, the propagation has good chance of being contained (3b,3d,3f) or of continuing at infinity (3a,3c). It is however less clear in some limit cases (3b). In particular, and among many other results, we have been able to find limit values of the parameters experimentally, and also an analytical upper bound (above which propagation cannot be stopped) and a lower bound (under which propagation is always stopped).
Our work on cascading failures and propagation in small-world graphs have taught us that, in such topologies, propagation can be stopped only if each individual node has a very low probability of failing. This has lead us to study the problem more reliable software, so that this does not come as a weak point. We have obtained some promising results in this line of work [1,2,4,8].

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）
〔雑誌論文〕（計 9 件）

1. Reliability Prediction for Component-based Software Dealing with Concurrent Propagating Errors, T.-T. Pham, X. Défago, Q.-T. Huynh, Science of Computer Programming, Elsevier. In print. (refereed)
2. Reliability Prediction for Component-based Software Systems with Architectural-level Fault-tolerance Mechanisms (extended version), T.-T. Pham, F. Bonnet, X. Defago, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 5(1):4-36, 2014. http://isyou.info/jowua/abstracts/jowua-v5n1-1.htm (refereed)
3. A Taxonomy of Congestion Control Techniques for TCP in Wired and Wireless Networks, K.C. Lee, X. Defago, Y. Tan, A.O. Lim, IEEE Symp. on Wireless Technology & Applications (ISWTA), pp.147-152, 2013, 10.1109/ISWTA.2013.6688758 (refereed)
4. Reliability Prediction for Component-Based Software Systems with Architectural-Level Fault Tolerance Mechanisms, T.-T. Pham, X. Defago. In Proc. 8th Intl. Conf. on Availability, Reliability and Security (ARES 2013), pp.11-20, 2013, 10.1109/ARES.2013.8 (refereed)
5. The Gathering Problem for Two Oblivious Robots with Unreliable Compasses, T. Izumi, S. Souissi, Y. Katayama, N. Inuzuka, X. Defago, K. Wada, M. Yamashita, SIAM J. Comput., 41(1):26-46, 2012, 10.1137/100797916 (refereed)
6. A Fast and Robust Optimistic Total Order Broadcast for Online Video Games, S. Bernard, X. Defago, S. Tixeuil. In Proc. 26th Intl. Conf. on Advanced Information Networking and Applications Workshops, WAINA 2012, pp.189-196, 2012, 10.1109/WAINA.2012.105 (refereed)

7. Brief Announcement: Discovering and Assessing Fine-Grained Metrics in Robot Networks Protocols, F. Bonnet, X. Defago, F. Petit, M. Gradinariu Potop-Butucaru, S. Tixeuil, In Proc. Stabilization, Safety, and Security of Distributed Systems (SSS), LNCS 7596, pp.282-284. 2012, 10.1007/978-3-642-33536-5_28 (refereed)
8. Reliability Prediction for Component-Based Systems: Incorporating Error Propagation Analysis and Different Execution Models, T.-T. Pham, X. Defago, In Proc. 12th International Conference on Quality Software (QSIC-12), pp.106-115, 2012, 10.1109/QSIC.2012.20 (refereed)
9. Exploration and Surveillance in Multi-robots Networks (invited paper), F. Bonnet, X. Defago. In Proc. 2nd Intl. Conf. on Networking and Computing, ICNC 2011, Workshop on Frontiers of Distributed Computing, pp.342-344, 2011, 10.1109/ICNC.2011.66 (non-refereed)

〔学会発表〕（計 8 件）

1. Bridging the Chasm between Theory and Practice of Multi-Robots Systems (invited), X. Defago, JAIST-LORIA Workshop, 2014/04/01-02, Kanazawa, Ishikawa, Japan.
2. Self-stabilizing crash tolerant gathering with daemons and dice (invited), X. Defago, Research meeting on Distributed Computing by Mobile Robots (MAC 2013), 2013/07/04~05, Ischia, Italy.
3. Reaching Group Agreement in Spite of Faulty Robots, X. Defago, Research Seminar at Research into Artefacts, Center for Engineering (RACE), Univ. Tokyo, 2013/05/31, Kashiwa, Chiba, Japan.
4. Byzantine Fault Tolerant Protocols for TaskManagement in Mobile Robots (fast abstract), T. D. Nguyen, F. Bonnet, X. Defago, 18th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2012), 2012 年 11 月 18 日~2012 年 11 月 19 日, Niigata, Japan.
5. Making Reliability Modeling of Component-based Systems Usable in Practice (fast abstract), T.-T. Pham, Q.-T. Huynh, X. Defago, 18th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2012), 2012 年 11 月 18 日~2012 年 11 月 19 日, Niigata, Japan.
6. Reliable Micro-protocols Composition and Combination (fast abstract), D. Higashihara, X. Defago, 18th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2012), 2012 年 11 月 18 日~2012 年 11 月 19 日, Niigata, Japan.
7. A Fast and Robust Optimistic Total Order Broadcast for Online Video Games, S. Bernard, X. Defago, S. Tixeuil, 26th Intl. Conf. on Advanced Information Networking and Applications Workshops, WAINA 2012, 2012/03/24, Fukuoka, Japan.
8. Cooperative Mobile Robots in a Planar Environment, X. Defago, INRIA Sophia-Antipolis, 2012/03/13, Sophia-Antipolis, France.

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
DEFAGO, Xavier （DEFAGO, Xavier）
北陸先端科学技術大学院大学・情報研究科・准教授
研究者番号：７０３３３５５７

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：