錯誤診斷協議在處理器與通訊線路存在混合型錯誤模式的研究

計畫編號: 90-2213-E-003-004
執行期限: 90 年 8 月 1 日至 91 年 7 月 31 日
主持人: 蕭顯勝　國立台灣師範大學工業科技教育系
Email: hssiu@ite.ntnu.edu.tw

一. 中文摘要

在實際的分散式系統中，系統單元(處理機和通訊線路)是會有多種錯誤模式同時發生之情形(一般稱為混合錯誤模式)、網路之拓樸可能是非完全連結之架構、而且功能正常之處理機在一般情況下是不知道那一個系統單元是有錯誤情況發生的。為了維持系統的運作，系統必須有一個機制來檢查及定位(detect/locate)出錯誤的系統單元，這就是錯誤診斷問題的本質。在本計畫中，假設處理機與通訊線路都會發生混合錯誤模式的情況下，我們將提出一個通訊協定(稱為 GFDA—General Fault Diagnosis Agreement protocol)來解決錯誤診斷協議問題。GFDA 是一個以證據為基底(evidence-based)的通訊協定，首先每一處理機利用 GFDA 收集在拜占庭協議通訊協定(Byzantine agreement protocol)的訊息作為證據(evidence)，再檢查所收集的證據去檢查及定位共同的錯誤的系統單元。最後，每一良好處理機將檢查出的共同錯誤系統單元從系統中分離，重新計算出系統的組態，以維持系統的良好運作情況。我們亦會對 GFDA 作深入的研究分析及實作模擬。我們會證明 GFDA 能使每一處理器使用最少的通訊量來檢查出最多的共同錯誤系統單元。

關鍵字: 錯誤診斷協議、容錯分散式系統、混合錯誤模式、拜占庭協議

Abstract

In a real-life distributed system, the system components (either processors, communication links, or both) can be subjected to different types of failures simultaneously (also called hybrid fault model). The network topology may not be fully connected, and a fault-free processor does not know which component in the network is faulty. For such a network model, we propose a protocol, called GFDA (General Fault Diagnosis Agreement), for solving the *FDA* problem. GFDA is an *evidence-based* fault diagnosis approach [8]. GFDA first collects the messages that have accumulated in a Byzantine agreement (*BA*) protocol [10] as *evidence* and then detects/locates the common set of faulty processors by examining the collected evidence. After the common set of faulty components is detected/located, the system can be reconfigured by eliminating these detected/located faulty components. The proposed protocol can detect/locate the maximum number of tolerable faulty components to solve the *FDA* problem.

Keywords: *Fault Diagnosis Agreement, Fault tolerant distributed system, Mixed failure types, Byzantine agreement*.

二. 緣由與目的

在實際的分散式系統中，處理機和通訊線路是會有多種錯誤模式同時發生之情形(一般稱為混合錯誤模式)、網路之拓樸可能是非完全連結之架構、而且功能正常之處理機在一般情況下是不知道那一個系統單元是有錯誤情況發生的[5, 8, 9, 12, 13, 15]。我們可將處理機和傳輸線錯誤的型態分成兩大類: 任意錯誤(arbitrary fault)與靜止錯誤(dormant fault) [12,13]。任意錯誤型態指處理器或傳輸線能做出不可預期的錯誤行為；而靜止錯誤型態指處理器或傳輸線不會傳送任何訊息或延後訊息之傳送。在這樣的網路環境中，錯誤診斷的工作必須考慮下面的情況:

(1) 不同處理器必須相互配合來完成錯誤診斷之處理，而獲得一個共同的錯誤診斷結果來將錯誤單元從系統中隔離；

(2) 處理機與通訊線路均存在不同的錯誤模式，必須考慮兩者之間的錯誤行為所引起的影響，使得不會將正常的處理機或通訊線路誤判為錯誤單元。

(3) 錯誤的系統單元(如任意錯誤)會主動的發佈不正確資訊去影響錯誤診斷的結果，或因本身的錯誤模式(如靜止錯誤)而沒有將資訊送出。

(4) 因為因為網路不為全連式的，正常的訊息可能經過錯誤的處理器或傳輸線路而被破壞。例如一個訊息 m 從處理器 P 發出要到處理器 Q，其中經過任意錯誤處理器 R 而被改成訊息 m'。

因此，錯誤診斷問題的解決方案應該滿足下面兩個條件:

(1) 一致性(Consensus): 所有的良好處理機能檢查出一個共同的錯誤系統單元的集合。亦即是所有的良好處理機均會指認出一樣的錯誤單元數目與名稱。

(2) 公平性(Fairness): 沒有任何良好的系統單元會被指認成錯誤的。

到目前為止，沒有一個能解決一般化的情況下(處理機和通訊線路是會有混合錯誤模式、網路之拓樸可能是非完全連結)之錯誤診斷協議問題之方案。在本計畫中，在一般化的情況下考慮錯誤診斷協議問題，並提出對此問題之解決方案。

三. 結果與討論

在本計畫中，分散式系統是指一群能自主獨立的處理器，它們經由不規則的通訊線路連繫起來。處理機和傳輸線的錯誤型態分成兩類: 任意錯誤(arbitrary fault)與靜止錯誤(dormant fault)。錯誤診斷協議(FDA)問題的目的為使每一良好的處理機能共同的將錯誤系統單元檢查及定位出來。因為錯誤診斷的結果是每一個良好處理機都一樣的，所以被檢查出錯誤的系統單元能從系統中隔離，作系統組態重組的工作。我們列出系統中所有參數如下:

(1) N：所有處理器的集合，每一處理器均有獨一的名稱，系統中處理器數目為 n ($|N| = n$)。

(2) c：網路的連通數(connectivity)。根據 Menger 定理[4]，如果網路的連通數為 c，則任何一對處理器均存在 c 條不重疊的路徑。亦即是上述 c 條路徑只有開始點與結束點是相同的。

(3) P_a：系統中任意錯誤處理器的數目。

(4) P_d：系統中靜止錯誤處理器的數目。

(5) L_a：系統中任意錯誤通訊線的數目。

(6) L_d：系統中靜止錯誤通訊線的數目。

本計畫在上述的分散式系統中找出一個能解決錯誤診斷協議問題之通訊協定。首先，我們必須決定系統的最大容錯能力。因為錯誤診斷的結果必須在每一良好處理機間達成協議，所以錯誤診斷協議問題的最大容錯能力必然限制在協議問題(agreement problem)上。我們先前對上述網路環境對協議問題提出了一些限制條件[12]。要在上述網路中達成一致的協議之限制條件為:

(1) $n > 3P_a + P_d$

(2) $c > 2P_a + P_d + 2(L_a + L_d)$

為了要檢查出錯誤系統單元，我們提出了兩個檢查規則(rules)，稱為區域錯誤檢查規則(the local fault detection/location rule **LR**)和整體錯誤檢查規則(the global fault detection/location rule **GR**)。我們分成兩種規則之主要原因是要分別指示錯誤診斷的結果，如果被整體錯誤檢查規則檢查出的錯誤必定是被所有良好處理機判斷成錯誤；相反的，區域錯誤檢查規則檢查出的錯誤結果可能為不一致的。根據上述兩個規則，GFDA 將包括下列步驟來檢查錯誤系統單元，：

(1) 訊息收集步驟(message-collection step)
(2) 協議步驟(Agreed-on step)
(3) 錯誤診斷步驟(Fault-diagnose step)
(4) 系統重組態(System reconfiguration step)

上述主要步驟之功能顯示在圖一中。我們亦證明了 GFDA 為最佳化的通訊協定，它使用最少的通訊資料數量，而能檢查出最多數量的錯誤系統單元。

四. 參考文獻

[1] J. C. Adams and K. V. S. Ramarao, "Distributed diagnosis of Byzantine processors and links," in *Proc. Symp. on Distributed Computing Systems*, 1989, pp. 562-569.

[2] R. W. Buskens, and R. P. Bianchini, "Distributed on-line diagnosis in the presence of arbitrary faults," in *Proc. Symp. on Fault-Tolerant Computing*, 1993, 470-479.

[3] T. Chandra and S. Toueg, "Unreliable failure detectors for asynchronous systems," in *Proc. of the 10th ACM Symp. on Principles of Distributed Computing*, pp. 325-340, 1991.

[4] N. Deo, *GRAPH THEORY with Applications to Engineering and Computer Science*, Englewood Cliffs:Prentice-Hall, NJ, 1974.

[5] J. Martin, *Telecommunications and the Computer*, 3rd ed., Englewood Cliffs:Prentice-Hall, NJ, 1990.

[6] S. Mallela and G. M. Masson, "Diagnosable systems for intermittent faults," *IEEE Trans. on Computers*, vol. 27, no. 6, pp. 560-566, 1978.

[7] S. Mallela and G. M. Masson, "Diagnosis without repair for hybrid fault situations," *IEEE Trans. on Computers*, vol 29, no. 6, pp. 461-470, 1980.

[8] A. Pelc, "Reliable communication in networks with Byzantine link failures," *NETWORKS*, vol. 22, no. 5, pp. 441-459, Aug. 1992.

[9] F. Preparata, G. Metze, and R. Chien, "On the connection assignment problem of diagnosable systems," *IEEE Trans. on Electronic Computing*,

vol. 16, no. 6, pp. 848-854, 1967.

[10] K. V. S. Ramarao and J. C. Adams, "On the diagnosis of Byzantine faults," in *Proc. Symp. on Reliable Distributed Systems*, 1988, pp. 144-153.

[11] K. Shin and P. Ramanathan, "Diagnosis of processors with Byzantine faults in a distributed computing systems," in *Proc. Symp. on Fault-Tolerate Computing*, 1987, pp. 55-60.

[12] H. S. Siu, Y. H. Chin, and W. P. Yang, "Byzantine agreement in the presense of mixed faults on processors and links," *IEEE Trans. on Parallel and Distributed Systems*, vol. 9, no. 4, pp.335-345, 1998.

[13] H. S. Siu, Y. H. Chin, and W. P. Yang, "A note on consensus on dual failure modes," *IEEE Tran. on Parallel and Distributed Systems*, vol. 7, no. 3, pp. 225-230, March 1996.

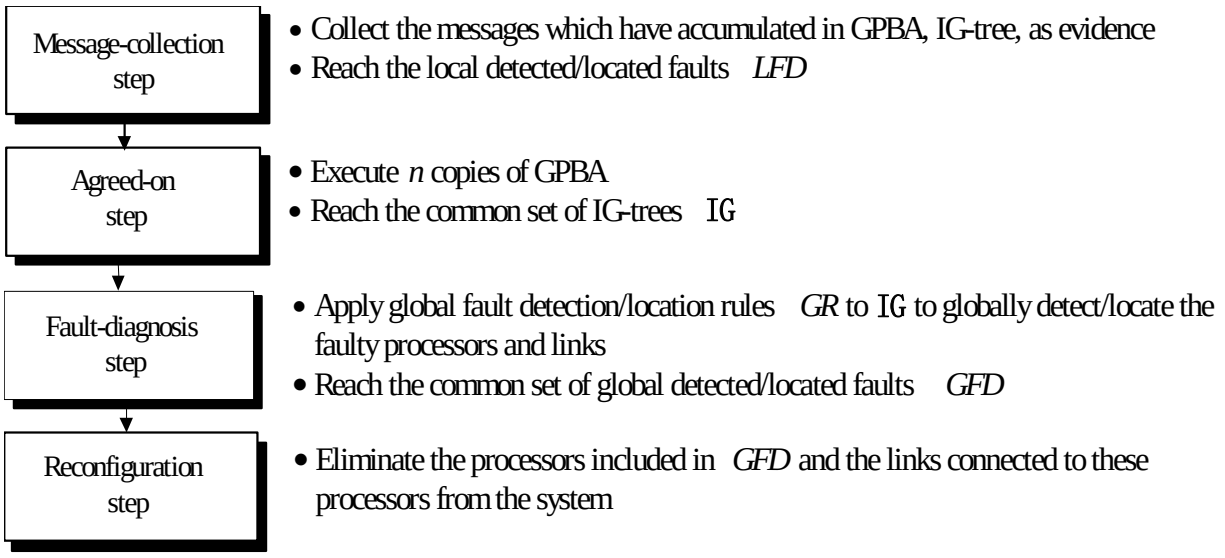
[14] H. S. Siu (also known as H. S. Hsiao), Y. H. Chin, and W. P. Yang, "Reaching fault diagnosis agreement under a hybrid fault model" *IEEE Tran. on Computers*, vol. 49, no. 9, pp. 980-986, Sept. 2000.

[15] M. Stahl, R. Buskens, and R. Bianchini, "On-line diagnosis in general topology networks," *Proc. of 1992 IEEE Workshop on Fault-Tolerant Parallel and Distributed Systems*, 1992, pp. 114-121.

[16] Nitin H. Vaidya and D. K. Pradhan, "Safe system level diagnosis," *IEEE Trans. on Computers*, vol. 43, no. 3, pp. 367-370, 1994.

[17] S. C. Wang, Y. H. Chin, and K. Q. Yan, "Reaching a fault detection agreement," in *Proc. Int. Conf. on Parallel Processing*, 1990, pp. 251-258.

[18] C. L. Yang and G. M. Masson, "A distributed algorithm for fault diagnosis in systems with soft failures," *IEEE Trans. on Computers*, vol. 37, no. 11, pp. 1476-1480, 1988.



圖一. GFDA 之處理程序