한국컴퓨터정보학회 동계학술대회 논문집 제27권 제1호 (2019. 1)

항공기 소프트웨어에서 동시성 오류를 자율적으로 수리하기 위한 함수 호출 기반 기법

김태형O, 최으뜸*, 전용기*
O*경상대학교 정보과학과
e-mail: miewcs2@gnu.ac.krO, {slateblue33, jun}@gnu.ac.kr*

A Method Call Based Technique for On-the-fly Repairing of Concurrency Errors in Airborne Software

Tae-Hyung KimO, Eu-Teum Choi*, Yong-Kee Jun*
O*Dept. of Informatics, Gyeongsang National University

● 요 약 ●

항공기 소프트웨어는 기능적 실패 시 인명피해나 재산피해와 같은 큰 사고로 이어질 수 있다. 따라서 항공기 소프트웨어 개발 과정에서 엄격한 검증 프로세스를 수행하지만 오류를 완벽히 제거하는 것은 어렵다. 병행 프로그램에서 발생하는 동시성 오류는 잘못된 동기화에 의하여 공유자원을 사용할 때 발생할 수 있다. 하지만 복잡한 인터리빙을 모두 고려하여 디버깅하기 어렵기 때문에 자율적으로 수리되어야 한다. 본 논문은 항공기 소프트웨어에서 함수 호출을 기반으로 동시성 오류를 자율적으로 수리하는 기법을 제시한다. 제시하는 기법은 모니터 및 컨트롤 엔진, 순차정보 제공 엔진, 건전성 관리시스템으로 구성된다.

키워드: 항공기 소프트웨어(airborne software), 동시성오류(concurrency error), 자율 수리(on-the-fly repairing), 건전성 관리시스템(health management system)

I. Introduction

항공기에서 안전한 소프트웨어 개발을 위해 검증 프로세스를 수행하고 있지만 검증 프로세스에서 소프트웨어 오류를 완벽하게 제거할 수 없다[1]. 동시성 오류는 잘못된 동기화로 공유자원을 사용할 때 발생한다. 하지만 복잡한 인터리빙을 모두 고려하여 디버깅할 수 없기 때문에 수행 중에 자율적으로 수리되어야 한다[2]. 자율 수리는 프로그램 수행 중에 오류가 발생하기 전에 예측하고 수리하는 기법이다.

본 논문에서는 동시성 오류를 자율적으로 수리하기 위해 함수 호출 기반의 기법을 제시한다. 제시하는 자율적 수리기법은 동시성 오류를 진단, 예측, 수리하고 건전성 관리시스템에 적용하여 관리한다.

II. Background

항공기의 기능을 소프트웨어로 구현하는 비중이 증가하고 있으며 안전한 항공기 소프트웨어 개발을 위해 검증 프로세스를 엄격하게 수행하고 있다. 하지만 항공기 소프트웨어의 개발과정 중 검증 프로세스에 시간 및 비용을 50%이상 사용해도 잠재적인 소프트웨어 오류를 완벽히 제거할 수 없다.

병행 프로그램에서 발생하는 동시성 오류는 잘못된 동기화에 의해 공유자원을 사용할 때 발생할 수 있다. 이러한 동시성 오류는 스레드들 간의 복잡한 인터리빙을 모두 고려할 수 없으므로 모든 오류를 디버깅할 수 없다. 따라서 프로그램 수행 중에 잠재적인 동시성 오류를 자율적으로 수리할 수 있어야 한다.

자율 수리는 병행 프로그램의 수행 중에 동시성 오류가 발생하면 지연 또는 재수행 등의 기법을 이용하여 프로그램이 올바르게 수행되도록 한다.

항공기 건전성 관리시스템은 항공기의 안전성을 위해 프로그램 수행 중에 발생하는 오류를 진단, 수리, 예측하는 기술이다. 규모가 크고 복잡하며 안전성이 중요한 항공기 소프트웨어 같은 경우에는 모든 잠재적 결함을 수리하기 어렵기 때문에 건전성 관리시스템의 역할이 중요하다.

항공기 건전성 관리시스템에서 소프트웨어 동시성 오류를 자율적으로 수리하는 기존의 기법들은 load/ store instruction 수준의 병행 접근사건 정보를 통해 오류를 탐지하고 수리한다. 하지만 load/store 정보를 유지하기 위해 많은 시간 및 공간 오버헤드가 발생한다. 따라서 실시간성이 보장되어야 하는 항공기 소프트웨어에는 적용하기가 어렵다.

III. The Proposed Scheme

본 논문에서는 항공기 소프트웨어에서 함수 호출을 기반으로 동시

성 오류를 자율적으로 수리하는 기법을 제시한다. 제안하는 기법은 모니터 및 컨트롤 엔진, 순차정보 제공 엔진, 그리고 건전성 관리시스템으로 구성된다. 전체 구조는 Fig. 1과 같다.

모니터 및 컨트롤 엔진은 순차정보 제공 엔진으로부터 올바른 상태 및 함수 호출의 순차를 제공받아 잘못된 순차가 생기면 해당 함수 호출을 지연시키는 기능을 한다[3]. 또한 자율 수리를 실패하면 Health Monitor로 실패를 보고하여 기존의 오류 완화 기법을 실시한다.

순차정보 제공 엔진은 미리 등록된 정확한 상태 및 함수 호출 순서를 모니터 및 컨트롤 엔진에 전달한다. 해당 엔진은 configuration 파일로 미리 저장되어있다.

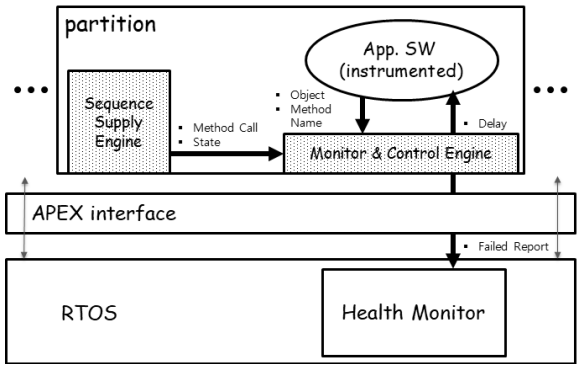

Fig. 1. Overall Architecture

건전성 관리시스템은 모니터 및 컨트롤 엔진이 동시성 오류에 대한 자율적인 수리를 실패하면 보고를 받는다. 보고를 받은 건전성 관리시스템은 기존에 정의된 오류 완화 기법을 실시하여 수리를 실시한다.

해당 기법의 진행 순서는 다음과 같다. 먼저 순차정보 제공 엔진은 모니터 및 컨트롤 엔진에게 올바른 상태 및 함수 호출의 순차를 제공한다. 그 후 모니터 및 컨트롤 엔진은 전달받은 올바른 순차를 이용하여 프로그램을 모니터링 한다. 모니터 및 컨트롤 엔진은 올바르지 않은 순차가 일어나기 전에 해당 함수 호출을 delay 시켜서 동시성 오류를 수리하게 된다. 만약 이러한 자율적 수리가 실패하게 되면 모니터 및 컨트롤 엔진은 Health Monitor로 보고하고, Health Monitor는 기존의 오류 완화 기법을 실시한다.

IV. Conclusions

본 논문에서는 항공기 소프트웨어에서 함수 호출을 기반으로 동시성 오류를 자율적으로 수리하는 기법을 제시하였다. 따라서 추후 실제 구현을 통해 수행 오버헤드를 줄이는 연구를 진행할 예정이다.

ACKNOWLEDGEMENT

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2018R1D1A3B07041838)

REFERENCES

[1] Mahadevan, Nagabhushan and Dubey, Abhishek and Karsai, Gabor. "Application of software health management techniques." Proceedings of the 6th international symposium on software engineering for adaptive and self-managing systems, pages 1-10, May 2011.

[2] Guy Martin Tchamgoue, Ok-Kyoon Ha, Kyong-Hoon Kim, and Yong-Kee Jun, “A framework for on-the-fly race healing in ARINC-653 applications,” International Journal of Hybrid Information Technology, SERSC 4.2 (2011): 1-12.

[3] Zhang, Lu, and Chao Wang. "Runtime prevention of concurrency related type-state violations in multithreaded applications." Proceedings of the 2014 International Symposium on Software Testing and Analysis. ACM, 2014.