Pontifícia Universidade Católica
do Rio de Janeiro

Francisco Figueiredo Goytacaz Sant'Anna

Safe System-Level Concurrency on Resource-Constrained Nodes with Céu

Tese de Doutorado

Thesis presented to the Programa de Pós-Graduação em Informática of the Departamento de Informática, PUC–Rio as partial fulfillment of the requirements for the degree of Doutor em Informática

Advisor : Prof. Roberto Ierusalimschy
Co–Advisor: Prof. Noemi de La Roque Rodriguez

Rio de Janeiro
September 2013

Pontifícia Universidade Católica
do Rio de Janeiro

Francisco Figueiredo Goytacaz Sant'Anna

Safe System-Level Concurrency on Resource-Constrained Nodes with Céu

Thesis presented to the Programa de Pós-Graduação em Informática of the Departamento de Informática do Centro Técnico Científico da PUC–Rio, as partial fulfillment of the requirements for the degree of Doutor em Informática. Approved by the following commission:

Prof. Roberto Ierusalimschy
Advisor
Departamento de Informática — PUC–Rio

Prof. Noemi de La Roque Rodriguez
Co–Advisor
Departamento de Informática — PUC–Rio

Prof. Renato Fontoura de Gusmão Cerqueira
Departamento de Informática — PUC-Rio

Prof. Markus Endler
Departamento de Informática — PUC-Rio

Prof. Silvana Rossetto
UFRJ

Prof. Roberto da Silva Bigonha
UFMG

Prof. José Eugenio Leal
Head of the Centro Técnico Científico — PUC–Rio

Rio de Janeiro, September 12, 2013

Francisco Figueiredo Goytacaz Sant'Anna

He completed his undergraduate studies in Computer Engeneering at the the Pontifical Catholic University of Rio de Janeiro (PUC–Rio) in 2003. He received his Master degree in Computer Science from PUC–Rio in 2009.

Bibliographic data

Sant'Anna, Francisco Figueiredo Goytacaz

Safe System-Level Concurrency on Resource-Constrained Nodes with Céu / Francisco Figueiredo Goytacaz Sant'Anna; advisor: Roberto Ierusalimschy; co–advisor: Noemi de La Roque Rodriguez. — Rio de Janeiro : PUC–Rio, Departamento de Informática, 2013.

88f. : il.; 30 cm

1. Tese de Doutorado - Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Informática.

Bibliography included.

1. Computer Science – Thesis. 2. Concurrency. 3. Determinism. 4. Embedded Systems. 5. Esterel. 6. Reactivity. 7. Synchronous. 8. Wireless Sensor Networks. I. Ierusalimschy, Roberto. II. Rodriguez, Noemi de La Roque. III. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Informática. IV. Title.

CDD: 004

Acknowledgments

I would like to thank Roberto and Noemi for giving me freedom to make hits and misses for the last six years. Also, Phillippas and Olaf for kindly receiving me in Chalmers, Sweden. Luiz Fernando and Cerqueira for my period in the Telemídia Lab, where I started as a researcher. Finally, all my teachers in CAp-UERJ, responsible for my education before college.

My studies were funded by CNPq and SAAB.

Abstract

Sant'Anna, Francisco Figueiredo Goytacaz; Ierusalimschy, Roberto; Rodriguez, Noemi de La Roque. **Safe System-Level Concurrency on Resource-Constrained Nodes with Céu**. Rio de Janeiro, 2013. 88p. Tese de Doutorado — Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Despite the continuous research to facilitate Wireless Sensor Networks development, most safety analysis and mitigation efforts in concurrency are still left to developers, who must manage synchronization and shared memory explicitly. We propose a system language that ensures safe concurrency by handling threats at compile time, rather than at runtime. The synchronous and static foundation of our design allows for a simple reasoning about concurrency that enables compile-time analysis resulting in deterministic and memory-safe programs. As a trade-off, our design imposes limitations on the language expressiveness, such as doing computationally-intensive operations and meeting hard real-time responsiveness. To show that the achieved expressiveness and responsiveness is sufficient for a wide range of WSN applications, we implement widespread network protocols and the CC2420 radio driver. The implementations show a reduction in source code size, with a penalty of memory increase below 10% in comparison to *nesC*. Overall, we ensure safety properties for programs relying on high-level control abstractions that also lead to concise and readable code.

Keywords

Concurrency. Determinism. Embedded Systems. Esterel. Reactivity. Synchronous. Wireless Sensor Networks.

Resumo

Sant'Anna, Francisco Figueiredo Goytacaz; Ierusalimschy, Roberto; Rodriguez, Noemi de La Roque. **Concorrência Segura em Nível de Sistema para Nós com Restrições de Recursos em Céu**. Rio de Janeiro, 2013. 88p. Tese de Doutorado — Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Apesar da pesquisa contínua para facilitar a programação de redes de sensores sem fio, a análise de perigos de concorrência ainda é de responsabilidade do programador, que deve tratar manualmente de questões como sincronização e memória compartilhada. Nós apresentamos uma linguagem de sistema que garante concorrência segura tratando ameaças em tempo de compilação. A fundamentação estática e síncrona da nossa abordagem permite um raciocínio mais simples sobre questões de concorrência, permitindo uma análise em tempo de compilação que garante programas determinísticos. Como contra-partida, nosso modelo impõe em termos da expressividade da linguagem, tais como para efetuar cálculos demorados, ou atender prazos estritos em tempo real. Nós implementamos diversos protocolos de rede conhecidos e o driver para o rádio CC2420 para mostrar que a expressividade e responsividade obtida com a linguagem é suficiente para uma gama considerável de aplicações para redes de sensores. As implementaçẽs mostram uma redução de tamanho de código, com um aumento de memória abaixo de 10% em comparação com nesC. O uso da linguagem proposta implica em diversas propriedades de segurança que se baseiam em abstrações de controle de alto nível, também resultando em código mais conciso e legível.

Palavras–chave

Concorrência. Determinismo. Sistemas Embarcados. Esterel. Síncrono. Reativo. Redes de Sensores sem Fio.

Contents

List of Figures