Available online at www.sciencedirect.com
SCIENCE DIRECT®
Theoretical Computer Science 322 (2004) 423–426
Theoretical Computer Science
www.elsevier.com/locate/tcs

Preface

This issue of Theoretical Computer Science contains five of the best contributions to "*F-WAN*, *Foundations of Wide Area Network Computing*." The meeting was held in Málaga Spain, on 12–13 July 2002, under the auspices of EATCS, the European Association for Theoretical Computer Science, and colocated with the 29th International Colloquium on Automata, Languages and Programming, ICALP 2002.

"Foundations of Wide Area Network Computing" focused on semantic aspects of global computing, motivated by the growing diffusion of internet services and applications, which is promoting global computing as an emerging model of computation. Based on mobility of code and computation on networks with highly dynamic topologies, the model needs effective infrastructures to support the coordination and control of components loaded at runtime from untrusted sources, as well as semantic frameworks to reason on the behaviour and properties of applications.

The themes of the meeting included research on calculi, models, and semantic theories of distributed, mobile, global computing systems; and languages, security and types for global computing. The selection of papers presented here comprises three invited talks, and the two best contributed papers. All of the papers included here, including the ones contributed by the invited speakers, were refereed to journal standard.

The *invited speakers* for F-WAN were:

Martín Abadi (UC Santa Cruz)
Luca Cardelli (Microsoft)
Andy Gordon (Microsoft)
Matthew Hennessy (Sussex)

and its *programme committee* consisted of:

Cédric Fournet (Microsoft)
Andrew Gordon (Microsoft)
Alan Jeffrey (De Paul, Chicago)
Ugo Montanari (Pisa)
Catuscia Palamidessi (PennState)
Benjamin Pierce (UPenn)
Davide Sangiorgi (INRIA)
Vladimiro Sassone (Sussex, chair)
Peter Sewell (Cambridge)

The proceedings have appeared in Elsevier's *ENTCS*, *Electronic Notes in Theoretical Computer Science*, vol. 66(3).

I wish to thank very warmly the *referees* of the papers in this special issue, who have contributed a very substantial and valuable effort. They were: Mikael Buchholtz, Michele Bugliesi, Cédric Fournet, Daniel Hirschkoff, Sergio Maffeis, Rosario

0304-3975/$ - see front matter
doi:10.1016/j.tcs.2004.03.001

Pugliese, Bernhard Reus, Alan Schmitt, Francesco Zappa Nardelli, and Pascal Zimmer. I am also grateful to *EATCS*, for its generous support to F-WAN, and to the *ICALP 2002* organiser, Inmaculada Fortes Ruiz, Llanos Mora, Rafael Morales, Francisco Triguero.

An invitation to the reader

This collection of selected papers from F-WAN offers results on an excellent variety of research topics in foundations of wide area network computing and global computing. These range from specification and correctness analysis of distributed (security) protocols (Abadi and Fournet); to logic languages, systems and calculi to express spatial properties of distributed systems (Caires and Cardelli); from comparative studies of the expressiveness of models and formalisms of computation (Busi and Zavattaro); to robustness and distribution transparency in the presence of faults (Chothia and Duggan), and resource-aware semantic analyses of migration calculi (Hennessy et al). I will provide below a brief synopsis of each of these papers, as an invitation for the casual reader to undertake the reading of this volume.

PRIVATE AUTHENTICATION, *Martín Abadi and Cédric Fournet*

Private authentication is the problem of authenticating principals on an insecure network without revealing their identities to outsiders, and has number of clear applications in distributed and mobile systems.

Abadi and Fournet describe two protocols for private authentication, making use public key cryptography. They formalise one of them in the applied π-calculus, and prove it enjoys the required guarantees of secrecy, authentication and privacy. The security properties studied in the paper are new and original. Remarkably, the relevant privacy properties can only be established in full when the presence of 'user' processes and their interaction with the protocol are formalised appropriately. The authors deal with such a requirement very elegantly.

ON THE EXPRESSIVE POWER OF MOVEMENT AND RESTRICTION IN PURE MOBILE AMBIENTS, *Nadia Busi and Gianluigi Zavattaro*

The comparison of computational constructs and mechanisms in terms of their relative expressiveness is a very interesting and traditionally complex task.

Busi and Zavattaro focus here on the expressiveness of the calculus of pure mobile ambients, i.e. the ambient calculus stripped down to its mobility primitives. The paper proceeds by comparing several subcalculi on the issue of decidability of termination, so as to assess, indirectly, the expressive power of combinations of name restriction and mobility operators. The main findings are that both movement (*in* and *out* capabilities) and name restriction can be dispensed with without altering the calculus' expressiveness, but not at the same time. One of the hot spots of the paper is the insight it provides into the expressiveness gap between replication and recursion. To establish

their decidability results, the authors make use of interesting techniques, to be noted from the technical point of view.

A Spatial logic for concurrency (part II), *Luís Caires and Luca Cardelli*

Spatial logics are a recent addition to the field of system specification and verification, and are rapidly finding application. They are logics aimed at describing both systems' behaviour and spatial structure.

Caires and Cardelli introduced in recent work a spatial logic for concurrent, mobile systems. Centred on the π-calculus, its fundamental ingredients are temporal and spatial modalities, as well as freshness quantifiers, which together yield a powerful, yet difficult to treat, combination. The paper in this collection carries forward the innovative developments on such a logic, focusing on its proof theory. In particular, the authors provide a sound sequent calculus, and investigate proof theoretical properties, such as cut-elimination.

Abstractions for fault tolerant global computing, *Tom Chothia and Dominic Duggan*

This paper investigates foundational calculi for the all-important problem of fault-tolerance in global computing, where systems are massively distributed and lack all forms of centralisation and trusted authority.

Chothia and Duggan introduce a family of π-calculi enriched with tools to support network-transparent, fault-tolerant applications. These consist of 'logs,' used to specify protocols for global agreement, and 'conclaves,' i.e. process groups sharing a log. The paper focuses on a calculus of atomic failures and commitment, and on its extension with anticommitment (the possibility to withdraw a previous commitment), and proves that they enjoy a subject-reduction property which guarantees the consistency of logs. The problem tackled in this paper is a very complex one, as it rides at the border of well known impossibility results (e.g., atomic commitment in asynchronous system with failures). The authors' approach is both novel and technically strong.

Towards a behavioural theory of access and mobility in distributed systems, *Matthew Hennessy, Massimo Merro, and Julian Rathke*

DPI is a reference calculus of distributed, mobile processes based on the π-calculus. Its processes execute in distributed locations, and migrate from place to place in order to interact with each other.

Hennessy, Merro and Rathke describe in this paper a sophisticated type system for selective access and mobility control in DPI. The core of the paper is devoted to identify suitable typed contextual equivalences, and characterise them via bisimulation on labelled transitions systems. Although the approach is traditional, the results are original and innovative, as the semantic theory is informed by access control policies in a very specific way. Namely, by barring access to certain locations, systems may keep processes from making certain observations. The resulting contextual equivalence

is more realistic, but correspondingly more complex to capture coinductively, and the authors make a excellent job of that.

Vladimiro Sassone
Guest Editor

Sussex, UK
January 2004