
Capsule Reviews

The Capsule Reviews are intended to provide a short succinct review of each paper in the issue, in order to bring the content to a wider readership. This issue's Capsule Reviews were compiled by Fairouz Kamarreddine. Professor Kamarreddine is an Associate Editor of *The Computer Journal* and is based in the Department of Computing and Electrical Engineering at Heriot-Watt University, Edinburgh, UK.

An object-oriented methodology for embedded real-time systems. J. M. ALVAREZ, M. DIAZ, L. LLOPIS, E. PIMENTEL AND J. M. TROYA

Real-time embedded systems can be found in all sorts of devices and in a large variety of fields. As a result of this, real-time embedded systems have an ever-increasing complexity and need to be robust, safe and be able to obey deadlines. This means that new methodologies need to be developed in order to deal with these requirements. This paper develops a new methodology based on the integration of rate-monotonic analysis (RMA) in the context of the Specification and Description Language (SDL) cycle, paying special attention to the transition system between the object and the process models. In order to get this integration, a real-time execution model for SDL is presented which allows the expression of real-time constraints. This model is based on transition priority, assignment and priority inheritance and considers hardware integration. Furthermore, as SDL has a clear formal semantic, this allows the usage of existing SDL-based simulation and validation tools. The paper gives a succinct survey of related work, of object-oriented methodologies for real-time systems and of SDL. The paper then presents the proposed methodology and applies it to a cordless telephone system.

On the structuring of reliable multicast protocols for distributed mobile systems. G. ANASTASI AND A. BARTOLI

Nowadays, it is essential to be able to deal with portable computers and wireless networking, where one needs to move freely with a hand-held computer, while maintaining connectivity with a wired computing infrastructure through a number of wireless cells. However, mobile devices have constraints in terms of power and memory availability. This paper deals with 'reliable multicast' in a group of processes comprising mobile hosts that communicate with a wired infrastructure by means of wireless links. The paper notes that not only are most existing proposals for reliable multicasts based on 'hand-off' (i.e. whenever a mobile host switches a cell, state information about this host travels across the wired network from the support station to the old cell to that of the new cell), but also most detailed analyses for these hand-off reliable multicast protocols focus on correctness rather than performance. Based on these observations, the paper takes an earlier proposal by the authors of a protocol which does not need any form of hand-off and provides a detailed cost and performance analysis

based on simulation experiments. These experiments show that the protocol which does not need any form of hand-off fares much better than the protocol based on hand-off in many respects: latency, scalability, bandwidth usage efficiency, and speed in managing cell switches of mobile hosts. This means that hand-off protocols are neither necessary nor sufficient to obtain good performance.

RCPCP: A ceiling-based protocol for multiple-disk environments. J. WU, T.-W. KUO AND C.-W. HSUEH

Real-time process scheduling has been a hot topic for the past few decades. Work on the feasibility and schedulability of real-time systems continues to pose many difficulties, and to propose many interesting approaches. This paper explores the real-time resource allocation problem under a realistic system architecture, where processes are sequences of CPU and I/O bursts. It proposes a methodology which is efficient and easy to implement for scheduling processes in multi-disk environments. The paper explores the balance between the management of priority inversion and the utilization of system resources. Simulation results for the proposed methodology are given and a simple deadlock-detection mechanism is derived leading to a deadlock-free version whose correctness is shown.

The impacts of write-through procedures and checkpointing on real-time concurrency control. T.-W. KUO, Y.-H. HOU, K.-Y. LAM

In order to maintain database consistency and to meet response-time requirements of real-time transactions, various efficient concurrency protocols have been proposed. On the other hand, in non-real-time main-memory database systems, much research effort has been devoted to recoverability and transaction durability. In particular, a write-through procedure (involving techniques such as fuzzy checkpointing) must be done to enforce the updating of transaction logs into stable storage. Such issues of maintaining transaction durability are often ignored in the design of real-time concurrency control protocols and in their performance evaluation. This paper explores the inter-activities of real-time concurrency control and the mechanisms in maintaining transaction durability under checkpointing and write-through procedures. The paper considers the RWPCP Read/Write Priority Ceiling Protocol proposed for hard real-time database systems and shows that schedules generated from RWPCP could be irrecoverable when transaction commitment is considered. Then the paper shows that different checkpointing granularities in

different variants of RWPCP impose different impacts on the adopted concurrency control protocol. The impacts of different checkpointing methods of RWPCP are evaluated through a simulation model which is implemented and tested on a series of simulation experiments. The simulation results showed that the impacts of checkpointing on real-time concurrency control highly depend on the granule size in checkpointing.

Robust and simple authentication protocol. H.-Y. CHIEN AND J.-K. JAN

Password-based protocols are currently the mainstream authentication protocols in many distributed systems. Passwords can either be weak (generated by user) or strong (generated by a computer program). Weak passwords are vulnerable to password-guessing attacks. Strong passwords are hard to memorize, and therefore, trusted devices like smart cards are used to store strong passwords. As password-guessing attacks are popular, various protocols operate to avoid these attacks. The paper examines three such protocols and shows their limitations. Then, the paper proposes the so-called RObust and SImple (ROSI) protocol which avoids these limitations. The security examination and the performance evaluation of the ROSI protocol are presented showing that ROSI achieves robust security with lower costs.

Hiding information in image mosaics. C. BLUNDO AND C. GALDI

In order to secure communication, two disciplines are usually used: 'cryptography' and 'information hiding'.

One of the basic goals of cryptography is the privacy of communication and hence the encryption procedure must be randomized to ensure privacy. However, this randomized encryption can sometimes give away the fact that a secret is being communicated. For this reason, hiding a secret message in an innocent-looking one may be more safe, as not only is the secret hidden, but also the fact that there is a secret is hidden too. However, information hiding faces similar problems as cryptography. This paper argues that using images in information hiding is a safer option and considers a particular class of pseudo-random images (the image mosaics). The paper gives algorithms for information hiding that allow different levels of security. These algorithms have not yet been implemented and hence the work leaves open the experimental verification.

Representing the dividing instant. J. MA AND B. KNIGHT

Puzzles concerning the dividing instant (DI) of when something holds and then it does not have fascinated philosophers since ancient times. Questions such as: 'what is the dividing moment between when the sun is shining and when the sun has set?' have come again and again in many modern day applications and systems. Such questions were attempted by a variety of logics and systems: temporal logics, point-based logics, interval-based logics, event-based logics, fuzzy logics, and many more varieties of systems. This paper investigates the DI problem by means of examining different responses from the point of view of different temporal approaches. The paper proposes a classification of assumptions about the DI and draws observations on the expressiveness of different approaches.