doi:10.1093/comjnl/bxm074

Capsule Reviews

FAIROUZ KAMAREDDINE

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. The Capsule Reviews were compiled by Fairouz Kamareddine. Professor Kamareddine is an Associate Editor of The *Computer Journal* and is based in the Department of Mathematical and Computer Science at Heriot-Watt University, Edinburgh, UK.

Service Availability in Concurrent Systems—Part I: A Theory of Hierarchical Services of Interacting Processes. M.S. FALLAH AND A.R. SHARAFAT

The paper introduces an axiomatic model of concurrent systems through which a number of issues related to service availability including mutual exclusion, deadlock/starvation freedom, denial/quality of services and fault tolerance can be described in a cohesive manner.

The paper starts from the claim that existing formal models of concurrent systems are not suited for the analysis of service availability. It develops the hierarchical services of interacting processes (HSIP) model which allows a system to be viewed both as a set of processes and as a set of services. Similarities between HSIP and CSP are outlined. The authors explain the three components that form a concurrent system in HSIP: the hierarchy, the timing and the computation model. The system hierarchy identifies the atomic services required in a system execution. The system timing and the system computation model enable the identification of the instants at which atomic services are requested. The paper gives the axioms that represent the availability of resources and atomic services and illustrates through examples the usefulness of HSIP in modelling concurrent systems. In a follow up [1], the authors analyse further the problem of system availability.

REFERENCE

[1] Fallah, M. and Sharafat, A. (2007) Service availability in concurrent systems Part II: analysis and case studies using HSIP. *The Computer Journal*, **50**, 535–554.

Service Availability in Concurrent Systems—Part II: Analysis and Case Studies Using HSIP. M.S. FALLAH AND A.R. SHARAFAT

This is a follow up of the earlier work of the authors [1] where they axiomatically developed the hierarchical services of interacting processes (HSIP) model which allows a system to be viewed both as a set of processes and as a set of services. The model was intended to describe a number of issues related to service availability. The current paper analyses in detail the problem of service availability using this HSIP model of [1] and establishes a number of results related to the (un)decidability of the service availability problem and to the flexibility of HSIP. First, the paper formalises the service availability problem in the HSIP model and shows that it is undecidable in general. In particular, the paper shows that it is undecidable whether a given service of a given system is available at a given time. Then, the paper shows that the service availability problem is decidable for a particular class of systems (scrupulous systems without precedence cycles) and has the worst-case complexity of $O(ne^n)$ where n is the number of configurations in the system, and that for a subclass of these systems, service availability is NP-complete. Having established such (un)decidability results, the authors move to study service availability in nondeterministic systems and then carry out a number of case studies which establish the usefulness and flexibility of the proposed HSIP model.

REFERENCE

[1] Fallah, M. and Sharafat, A. (2007) Service availability in concurrent systems Part I: A theory of hierarchical services of interacting processes. *The Computer Journal*, **50**, 522–534.

A High-Speed Link Layer Architecture for Low Latency and Memory Cost Reduction. J. LEE, H.-J. LEE AND C. LEE

InfiniBand is a system interconnection standard that improves the interconnectivity between servers and I/O devices. The link layer of InfiniBand is responsible for supporting the quality of service (QoS) mechanisms. However, efficient implementation of the link layer is problematic from the points of view of performance and cost. In order to achieve the InfiniBand QoS mechanisms, careful design and implementation of the InfiniBand link layer needs to be carried out.

This paper concentrates on such careful design and implementation with special emphasis on packet latency

reduction and buffer space optimization. First, the paper introduces the InfiniBand QoS mechanisms at the link layer which constitutes of: the virtual lane (VL), the link-level flow control, VL arbitration and the service level (SL)-to-VL mapping. Then, the hardware architecture of the InfiniBand link layer is proposed. The link layer consists of three main blocks: the transit block, the receiver block and the central control block. To support the InfiniBand QoS mechanisms with high-speed packet processing, the paper investigates the existing architectural candidates for conventional packet receivers to assess their suitability for high-speed packet receiving by InfiniBand. The paper proposes a candidate suitable for efficient high-speed packet receiving architecture and a FIFO that supports it. Thereafter, the paper estimates the maximum and minimum delays from an input to an output of a switch by statically modelling three candidates for the link layer. To estimate the effects of dynamic factors in normal cases, a number of network simulations are carried out to measure the dynamic effects by the earlier mentioned three candidates in a real environment. Emphasis is placed on latency and gate counts. The implementation details of the InfiniBand link layer core are also given.

Comparing Typical Opening Move Choices Made by Humans and Chess Engines. M. LEVENE AND J. BAR-ILAN

Games have received much attention in both theoretical and applied computer science where algorithms, search strategies, automation and efficiency all play a role in improving the games (as an example of a particular study, see [1]). This paper is concerned with computer chess games and observes that with machines having ever growing computing resources, the future looks bleak for human contestants in man-machine chess matches. The paper considers the research question whether the opening books used by modern chess engines in machine versus machine competitions are comparable to those used by chess players in human versus human competitions. Opening theory is an advanced topic of its own and many expert chess players usually memorise the first few moves from well documented material on chess openings. Moreover, automated methods have been developed for improving the quality of opening books for computer chess programmers.

To compare the choices of humans to those of engines, the paper uses two opening books: Powerbook 2005 (for humans versus humans) and Comp2005 (for machine versus machine). Several measures are used to test the correspondence between the two opening books and a number of tests and experiments are carried out. The test results show a close association between humans and machines opening books. The paper analyses these results and discusses a number of extensions and applications of the comparison techniques proposed.

REFERENCE

[1] Chen, S.T. and Lin, S.S. (2004) Optimal Algorithms for 2xn Mastermind Games -a Graph-Partition Approach. *The Computer Journal*, **47**, 602–611.

Provably Efficient Authentication Key Agreement Protocol for Multi-Servers. R.-J. HWANG AND S.-H. SHIAU

Network security has attracted much attention in the past years (see for example [1–3]). An authenticated key agreement (AKE) protocol is a total solution for providing identity authentication and message confidentiality security services. This paper proposes an efficient AKE protocol for a multi-server architecture. Each user keeps one identity, one smart card and one password which he uses to log into many different servers using the proposed protocol. This proposed protocol is more efficient than other approaches and can resist a number of attacks. This protocol is shown to be secure and correct. After introducing the necessary backgrounds and preliminaries, the proposed AKE protocol for multi-servers is introduced through three stages: the registration phase, the login phase and the password change phase. Then, the proposed protocol is shown to be secure using the random oracle model, and is shown to be correct using a simple logic analysis method.

Furthermore, the author shows that the proposed protocol can prevent replay attacks, unknown key share attacks, stolen verifier attacks and insider attacks. The proposed protocol is also compared to a number of other proposed protocols from the point of view of security properties, computational costs and communicational costs. From all these points of view, the proposed protocol is shown to outperform these other proposals.

REFERENCES

[1] Hanaoka, G., Shikata, J., Hanaoka, Y. and Imai, H. (2006) Unconditionally Secure Anonymous Encryption and Group Authentication. *The Computer Journal*, **49**, 310–321.

[2] Huang, C.-M. (200?) Efficient and Provably Secure IP Multimedia Subsystem Authentication for UMTS. *The Computer Journal*, bxm029.

[3] Tseng, Y.-M. (2007) A secure Authenticated Group Key Agreement Protocol for Resource-Limited Mobile Devices. *The Computer Journal*, **50**, 41–52.

Some Generalisations of a Simion—Schmidt Bijection. A. JUARNA AND V. VAJNOVSZKI

Let $[n] = \{1, 2, \ldots, n\}$. A permutation of the set $[n]$ is a bijection from $[n]$ to $[n]$. Let S_n be the set of all permutations of $[n]$. A pattern is a certain kind of a permutation. If T is a set of patterns, the set of permutations that avoid the patterns in T is denoted as $S_{n(T)}$. Enumerations of permutations avoiding certain patterns have been studied in the literature (see for instance [1].

Let F(n-1) be the set of all length (n-1) binary strings with no consecutive 1s. Simion-Schmidt gave a constructive bijection from F(n-1) to S_n(123, 132, 213). This paper generalises this Simion-Schmidt bijection to an injection from (n-1)-tuples of {0,1} to S_n and derives four further bijections which are shown to be combinatorial isomorphisms. Graph-theoretical interpretations of the results of the paper are also given.

REFERENCE

[1] Pallo, J.M. (1988) Some properties of the rotation lattice of binary trees. *Comput. J.*, **31**, 564–565.

Parallel Generation of *t*-Ary Trees in A-order: Parallel Tree Generation. H. AHRABIAN AND A. NOWZARI-DALINI

The problem of generating rooted ordered trees has been extensively studied in the literature (see for example [1–3]). In some of the tree generation algorithms proposed in the literature, the so-called A- and B-orders are used. The A-order uses global information of tree nodes whereas the B-order uses local information. This paper concentrates on the A-order (which is said to be more natural). First, the definition of A-order is given along with other necessary background notation. Then, a general successor algorithm to generate trees in A-order is given along with a successor algorithm for the so-called z-sequences which returns the successor sequence in A-order for a given z-sequence. Afterwards, a parallel version of the successor algorithm for z-sequences is given. This is the parallel generation algorithm of tree sequences. This algorithm is proved to be cost-optimal and adaptive. Finally, ranking and unranking algorithms for z-sequences in A-order are given.

REFERENCES

[1] Er, M.C. (1992) Efficient generation of k-ary trees in natural order. *The Computer Journal*, **35**, 306–308.

[2] Xiang, L., Tang, C. and Ushijima, K. (1997) Grammar-oriented enumeration of binary trees. *The Computer Journal*, **40**, 278–291.

[3] Xiang, L., Ushijima, K. and Akl, S. (2000) Generating regular k-ary trees efficiently. *The Computer Journal*, **43**, 290–300.

On the Security of a Group Key Agreement Protocol. Q. TANG

In [1], Tseng proposed a group key agreement protocol for a particular kind of wireless networks. [1] claimed a number of properties of the proposed protocol including security against impersonation attacks and passive attackers. The present paper explains that the security analysis in [1] is performed heuristically and the protocol cannot be proven secure in known security models. In particular, the present paper briefly shows that the protocol of [1] suffers from a number of security vulnerabilities.

REFERENCE

[1] Tseng, T. (2007) A secure authenticated group key agreement protocol for resource-limited mobile devices. *The Computer Journal*, **50**, 41–52.

A Proof of Revised Yahalom Protocol in the Bellare and Rogaway (1993) Model. K.-K.R. CHOO

The design of secure interactive cryptographic protocols (or key establishment protocols) is notoriously hard. The paper argues that mathematical proofs are sought to establish that a particular protocol behaves as intended, but points out that although many mathematical proofs are rife in errors (witness Euler's formulations in algebraic topology), they remain an invaluable tool for reasoning about protocols. The paper attempts to remedy the lack of a security proof within a computational complexity framework of the Yahalom protocol.

To do so, the paper gives within the Bellare and Rogaway (BR93) model and the random oracle model, a revised version of the Yahalom protocol and a formal statement of its security. First, the paper introduces the 1993 Bellare and Rogaway model of adversary capabilities with an associated definition of security. Then, the Yahalom protocol is presented together with its simplified version. The author proceeds by presenting a revised version of the Yahalom protocol where the users and the server can contribute to the value of the session key (whereas in the Yahalom protocol, the server was the only contributor), where a partnership mechanism is specified, and where an authenticated encryption scheme is used. The author proves that protocol 2 is secure if a number of conditions are met. Finally, the author reflects on the partnership mechanism that is part of his revised protocol and the role that session identifiers could play. A brief comparative study is also given.

An In–Out Combined Dynamic Weighted Round-Robin Method for Network Load Balancing. D.-C. LI AND F.M. CHANG

The high growth rate of internet applications decreases the quality of service and slows down response. In order to avoid this problem, multiple-internet-links are built and a number of load-balancing methods for networks with multiple-links have been proposed. In some of these methods, control algorithms such as the Round-Robin (RR) and the weighted Round-Robin (WRR) are used. This paper gives another algorithm (called CDWRR for combined dynamic weighted Round-Robin) where the need to measure, trace, rank and calculate links' performance is minimized for multiple incoming and outgoing network links. CDWR is applied in real network environments where the loads for multiple links with both incoming and outgoing interfaces are considered simultaneously. CDWRR determines the optimal detecting frequency or time instant for both in and out links. First, the load balance is evaluated, then the paper gives a dynamic weighted Round-Robin for incoming link balancing

and another for outgoing link balancing. Then a two-dimensional weight table that combines incoming and outgoing link weights is set for the combined dynamic weighted Round-Robin algorithm. Mathematical equations to determine the best detecting interval are given via studies of the smallest, longest and range detecting intervals for both incoming and outgoing link balancing. Simulations results are provided and discussed.