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 Enigneering at Heriot-Watt University, Edinburgh, UK.

Concept similarity in *SymOntos*: an enterprise ontology management tool. A. FORMICA AND M. MISSIKOFF

This paper deals with the similarity of concepts. Similarity reasoning is an important concept and represents one of the key mechanisms that humans use to organise their life. Given two concepts like 'car' and 'truck', how can we assess their similarity? The paper starts from these questions and proposes a method that allows assessing similarities of concepts using well-known notions in knowledge representation theory (inheritance hierarchy, similarity graph and structural forms). The paper gives the formal basis using an illustrative example establishing the concept similarity. Then the paper gives the conditions which must be satisfied for an ontology to be correct. Three kinds of similarity evaluation are proposed: flat structural similarity, hierarchical similarity and concept similarity. The paper is a welcome addition to research in the field and is very enjoyable to read.

Java for on-line distributed monitoring of heterogeneous systems and services. P. BELLAVISTA, A. CORRADI AND C. STEFANELLI

The Internet continues to dominate our daily lives with more and more people conducting more and more of their daily business on the Internet. This explosive use of the Internet requires more attention to the quality of service (QoS) provided by the Internet. It also requires ever more assurance of security and protection against misuse and attack. Previous approaches at solving these problems have their drawbacks. For example, the requirement that an intermediate router traversed by service packet flows implements a specific protocol which is likely to pass through a long process of acceptance (and hence affects the QoS). The paper claims that on-line monitoring components play a central role in any distributed infrastructure for QoS-enabled service provision in the Internet environment to achieve dynamic service adaptation, to enhance global performance and to detect possible denial-of-service attacks. For this reason, the authors introduce a tool for the design, implementation and deployment of Internet services. The paper also implements a tool which enforces distributed management policies. This tool results in a significant reduction in reaction time and traffic overhead. Performance results of these tools are very encouraging and further extensions are being studied by the authors.

Reverse execution of Java bytecode. J. J. COOK

This paper is concerned with debugging Java programs. Many such debuggers already exist but they mostly work in a forward manner. Sometimes, however, it is necessary for the debugger to move backwards. For example, imagine the scenario where the debugger has moved a few lines forwards of the bug and is in need now to go backwards. This paper proposes a debugger which can run Java code backwards. The author motivates the approach he considers (logging) for his debugger and discusses the implementation of reverse execution. Particular themes such as I/O, garbage collection and exception handling are discussed. A case study is provided and performance data is produced. The debugger is available on the web page of the author where it can be downloaded by the readers.

Practical Earley parsing. J. AYCOCK AND R. N. HORSPOOL

In the late sixties, Earley proposed a general context-free parsing algorithm. Earley's algorithm is general because it permits expressions of ambiguous grammar. However, Earley's algorithm suffers various problems related to grammar rules whose right-hand side is empty. As the two solutions proposed to this problem have their drawbacks, the authors study these problematic rules and propose a solution based on a new type of automaton which is suitable for Earley's parsing. First, the authors give a compact yet clear explanation of Earley's parsing and then outline the problem of the grammar rules with empty right-hand side and the drawbacks of the solutions proposed by Earley himself and later by Aho and Ullman. The authors propose what they call the 'ideal solution' and prove its correctness. This solution leads them to use an efficient deterministic automata in the general parsing algorithm. The authors devote considerable effort in finding a method to reconstruct derivations and then discuss the implementations of their two algorithms. Analysis of these implementations establish that the method of the paper is twice as fast as a standard Earley parser.

RASCAL: calculation of graph similarity using maximum common edge subgraphs. J. W. RAYMOND, E. J. GARDINER AND P. WILLETT

Comparing graph similarity has many important applications ranging from computer vision to video indexing. For this reason, research on graph similarity is quite popular. This paper is concerned with one approach in this area: the use of a maximum common subgraph (MCS) between the graphs being compared. The paper presents a new graph similarity calculation procedure based on MCS. The main

application of the new method is chemical similarity searching where molecular structures are represented as graphs, such that the atoms are labelled vertices and the chemical bonds are labelled edges. The representation of chemical information using MCS has advantages over other representation methods used in the literature. The method proposed in this paper gives a graph matching procedure called RASCAL (Rapid Similarity Calculation) which consists of screening (that rapidly determines whether the graphs being compared exceed some specified similarity threshold) and rigorous graph matching (which consists of an efficient determination of the MCS using the graph similarity concept). The nice thing about the proposed algorithm is that it uses various already established heuristics and introduces new ones as well. The authors believe that the procedure proposed can be applied in any other graph-based similarity application.

Using Bloom filters to speed-up name lookup in distributed systems. M. C. LITTLE, S. K. SHRIVASTAVA AND N. A. SPEIRS

Imagine a large-scale distributed system with billions of objects scattered over nodes separated by large physical distances. Consider locating objects in such a system. This location of objects takes the form of a naming service that maps an object name to its location. Achieving good performance and reliability of naming services in such a large-scale system is very difficult. But, naming services play a central role in computing systems. This paper presents a speed-up technique based on hashing that is applicable in any stage of the name to location resolution process. But a hash function requires space to store the keys to be hashed and the entities to be stored. Bloom filters which are based on a probabilistic hash-coding method reduce the space required to store a hash set. This paper gives a good overview of Bloom filters, their use in naming services and of the related work based on Bloom filters. The paper illustrates the effectiveness of Bloom filters to locate objects by performing some experiments and by analysing the performance results. These experiments lead the authors to provide feedback on how to use Bloom filters to obtain trade-offs between performance and resource utilization.

A comparison of random binary tree generators. J. SILTANEVA AND E. MÄKINEN

Binary trees are essential in various branches of computer science and randomly generating binary trees is a very common operation. For this reason, efficient generation of random binary trees is desirable. But random generation of binary trees is computationally complicated. This paper compares five linear time algorithms for generating unbiased random binary trees, and gives a ranking of these algorithms with respect to their asymptotic performance in terms of the numbers of the basic operations executed on average per tree node. The paper starts by introducing these five algorithms and then compares them with respect to their execution time, counting the number of various types of operations executed and also taking the weight of different types of operations into account. The algorithms are then ranked following these different measures. As a definite absolute ranking of these algorithm is very difficult, this paper makes an interesting step towards comparing them.

A key escrow scheme with time-limited monitoring for one-way communication. M. ABE AND M. KANDA

There is a strong demand for monitoring communication to combat crime, while at the same time a large amount of work takes place on securing and protecting information. In order to reach a compromise, a trusted third party is involved. In a key escrow scheme, users deposit their private keys to the escrew agency (EA) which discloses the key only to the law enforcement party (LEP) and only if lawfully requested. But then again, the question of trusting the EA arises and hence the need for weakening the power of the EA arises. Various solutions have been proposed to solve this problem. In particular, the private key is divided between a number of EAs and it is only disclosed if all the EAs co-operate. Sometimes, only a part of the private key is passed to the EAs which will then have to construct the whole key. Often, the monitoring period of the LEA is limited too. This shows that there are many approaches at reaching a compromise between securing and protecting information on one hand, and making it available when needed. Such is the case when investigating crimes. The paper points out that each of these approaches have their limitations in one sense or another. For this reason, a novel key escrow approach is presented. This approach is shown to satisfy most desired properties except for one: namely, target hiding. The paper is honest about the drawbacks of the new approach and discusses various open problems. This paper is a useful step in an area that is of extreme importance and that affects our lives. We want private information to be secure, yet we also want to retrieve vital information.

A verifiable multi-authority secret election allowing abstention from voting. W.-S. JUANG, C.-L. LEI AND H.-T. LIAW

Nowadays, more and more of our activities are done on the web. This paper deals with voting on the web. Networked elections will not be accepted unless there is a protocol which protects the voter's privacy and which prevents cheating (e.g. duplication of votes). There are many other problems faced by networked voting which have occupied many researchers. This paper overviews some of the previous work in this area and outlines some of its drawbacks. Then the paper proposes a robust and verifiable multi-authorities secret voting scheme for real-world environments with many desirable and important properties such as the fairness of the lobbying process, the strict monitoring of the voting process, the privacy of the voter, etc. Correctness of the proposed scheme is shown and its security analyzed. The scheme allows a voter to abstain from voting and to openly complain if his/her vote has not been taken into account. The paper is thorough and very interesting to read.