

Volume 1, Number 3, 2007

Contents

MINTCHEV, A. A prototype of an extension to the UDDI registry allowing publication and search based on subjective evaluations (pp. 229-240)

IVANOV P., S. ILIEVA. Agile case study evaluation in middle size project (pp. 241-254)

DIMOV, A., S. ILIEVA. Generalized nets model of an e-learning system software architecture (pp. 255-266)

DYACHUK, D., R. DETERS. Transparent scheduling of composite Web services (pp. 267-278)

STOICHEV, S. Algorithms for determining unitals and maximal arcs in projective planes of order 16 (pp. 279-292)

BRAYNOV, S., R. PAVLOV. Auction with untrustworthy bidders (pp. 293-312)

NIKOV V., S. NIKOVA, B. PRENEEL. On distributed oblivious transfer (pp. 313-336)

NIKOV V., S. NIKOVA, B. PRENEEL. On proactive verifiable secret sharing schemes (pp. 337-364)

SKALICZKI T., B. GOLDSCHMIDT, BÖSZÖRMENYI L. Algorithmic background of the host recommendation in the adaptive distributed multimedia server (pp. 365-386)

Abstracts

A PROTOTYPE OF AN EXTENSION TO THE UDDI REGISTRY ALLOWING PUBLICATION AND SEARCH BASED ON SUBJECTIVE EVALUATIONS*

Alexander Mintchev

e-mail: alexanderdm@fmi.uni-sofia.bg

ACM Computing Classification System (1998): D.2.11

Key words: UDDI, web-services, evaluations.

*The paper has been presented at the International Conference Pioneers of Bulgarian Mathematics, Dedicated to Nikola Obreshkff and Lubomir Tschakaloff, Sofia, July, 2006.

Abstract. The current paper introduces the usage of subjective evaluations by others as a tool that can support consumers' decisions. It summarizes the features of the main UDDI registry providers and presents an extension to any UDDI registry allowing users of the registry to publish subjective evaluations for any artifact found in it and to search for artifacts, based on subjective evaluations. The paper outlines some typical business scenarios, in which the proposed extension would be useful, and introduces some areas for feature work and improvement.

AGILE CASE STUDY EVALUATION IN MIDDLE SIZE PROJECT

Penko Ivanov, Sylvia Ilieva

e-mail: p.ivanov@prosyst.com, sylvia@acad.bg

ACM Computing Classification System (1998): K6.1, K6.3.

Key words: agile methodologies, agile management, software process, software metrics.

Abstract. In the last few years Agile methodologies appeared as a reaction to traditional ways of developing software and acknowledge the need for an alternative to documentation driven, heavyweight software development processes. This paper shortly presents a combination between Rational Unified Process and an agile approach for software development of e-business applications. The resulting approach is described stressing on the strong aspects of both combined methodologies. The article provides a case study of the proposed methodology which was developed and executed in a successful e-project in the area of the embedded systems.

GENERALIZED NETS MODEL OF AN E-LEARNING SYSTEM SOFTWARE ARCHITECTURE*

Aleksandar Dimov, Sylvia Ilieva

e-mail: aldi@fmi.uni-sofia.bg, sylvia@acad.bg

ACM Computing Classification System (1998): D.2.11.

Key words: Component-based software engineering; Software architecture; Generalized Nets; e-Learning systems.

*The paper has been presented at the International Conference Pioneers of Bulgarian Mathematics, Dedicated to Nikola Obreshkff and Lubomir Tschakaloff, Sofia, July, 2006.

Abstract. Component-based software engineering and software architecture are tightly connected areas in computer science. Software architecture presents the functionality of the system as decomposition into components, the properties of these components and the connectors between them. This paper illustrates a methodology for application of the theory of Generalized Nets (GNs) as a language for description of software systems architecture. According to this methodology, every component in the system, as well as every connector is represented by a single GN transition. This way the positions of the transition describe the ports of components and connectors in the system. This paper introduces a model of the component-based architecture of the e-learning system ARCADE, which is created, with respect to the proposed methodology for description with GNs. The four main subsystems are regarded as components in the GNs model. Their additional sub-modules are presented as the services provided by the components. Method calls are regarded as the connectors between these components. Further, the GNs model is compared with the existing UML diagrams, specifying the design of ARCADE.

TRANSPARENT SCHEDULING OF COMPOSITE WEB SERVICES*

Dmytro Dyachuk, Ralph Deters

e-mail: dod401@mail.usask.ca, deters@cs.usask.ca

ACM Computing Classification System (1998): H.3.5; F.2.2.

Key words: Web Services, Composite Web Service, LWKR, SJF, Scheduling, Admission Control.

The paper has been presented at the International Conference Pioneers of Bulgarian Mathematics, Dedicated to Nikola Obreshkff and Lubomir Tschakaloff, Sofia, July, 2006.

Abstract. Composite Web Services (CWS) aggregate multiple Web Services in one logical unit to accomplish a complex task (e.g. business process). This aggregation is achieved by defining a workflow that orchestrates the underlying Web Services in a manner consistent with the desired functionality. Since CWS can aggregate atomic and other CWS they foster the development of service layers and reuse of already existing functionality. An important issue in the deployment of services is their run-time performance under various loads. Due to the complex interactions of the underlying services, a CWS they can exhibit problematic and often difficult to predict behaviours in overload situations. This paper focuses on the use of request scheduling for improving CWS performance in overload situations. Different scheduling policies are investigated in regards to their effectiveness in helping with bulk arrivals.

ALGORITHMS FOR FINDING UNITALS AND MAXIMAL ARCS IN PROJECTIVE PLANES OF ORDER 16*

Stoicho D. Stoichev
e-mail: stoi@tu-sofia.bg

ACM Computing Classification System (1998): G.2.1.

Key words: Unital, Maximal arc, Projective plane, Graph isomorphism, Graph automorphism group, Algorithm.

The paper has been presented at the International Conference Pioneers of Bulgarian Mathematics, Dedicated to Nikola Obreshkoff and Lubomir Tschakaloff, Sofia, July, 2006.

Abstract. Two heuristic algorithms (M65 and M52) for finding respectively unital and maximal arcs in projective planes of order 16 are described. The exact algorithms based on exhaustive search are impractical because of the combinatorial explosion (huge number of combinations to be checked). Algorithms M65 and M52 use unions of orbits of different subgroups of the automorphism group of the 273×273 bipartite graph of the projective plane. Two very efficient algorithms (developed by the author and not described the generators, orbits and order of the graph automorphism group; (ii) graph isomorphism algorithm derived from VSEPARN. Four properties are proved and used to speed up the algorithms M65 and M52. The results of these algorithms are published. After changing only the parameters of these algorithms they can be used for determining unital in projective planes of different orders.

AUCTIONS WITH UNTRUSTWORTHY BIDDERS

Sviatoslav Braynov, Radoslav Pavlov
e-mail: sbray2@uis.edu, radko@cc.bas.bg

ACM Computing Classification System (1998): I.2.11

Key words: auctions, e-commerce, mechanism design, trust.

Abstract. The paper analyzes auctions which are not completely enforceable. In such auctions, economic agents may fail to carry out their obligations, and parties involved cannot rely on external enforcement or control mechanisms for backing up a transaction. The first mechanism is based on discriminating bidding schedules that separate trustworthy from untrustworthy bidders. The second mechanism is a generalization of the Vickrey auction to the case of untrustworthy bidders. We prove that, if the winner is considered to have the trustworthiness of the second-highest bidder, truthfully declaring one's trustworthiness becomes a dominant strategy. We expect the proposed mechanisms to reduce the cost of trust management and to help agent designers avoid many market failures caused by lack of trust.

ON DISTRIBUTED OBLIVIOUS TRANSFER*

Ventzislav Nikov, Svetla Nikova, Bart Preneel
e-mail: ventzi.nikov@gmail.com, svetla.nikova, bart.preneel@esat.kuleuven.be

ACM Computing Classification System (1998): D.4.6.

Key words: Cryptographic Protocols, Oblivious Transfer.

*The paper has been presented at the International Conference Pioneers of Bulgarian Mathematics, Dedicated to Nikola Obreshkoff and Lubomir Tschakaloff, Sofia, July, 2006.

The material in this paper was presented in part at INDOCRYPT 2002 [18]

Abstract. This paper is about unconditionally secure distributed protocols for oblivious transfer, as proposed by Naor and Pinkas and generalized by Blundo et al. In this setting a Sender has ζ secrets and a Receiver is interested in one of them. The Sender distributes the information about the secrets to n servers, and a Receiver must contact a threshold of the servers in order to compute the secret. We present a non-existence result and a lower bound for the

existence of one-round, threshold, distributed oblivious transfer protocols, generalizing the results of Blundo et al. A threshold based construction implementing 1-out-of- ζ distributed oblivious transfer achieving this lower bound is described. A condition for existence of distributed oblivious transfer schemes based on general access structures is proven. We also present a general access structure protocol implementing 1-out-of- ζ distributed oblivious transfer.

ON PROACTIVE VERIFIABLE SECRET SHARING SCHEMES*

Ventzislav Nikov, Svetla Nikova, Bart Preneel

e-mail: venti.nikov@gmail.com, svetla.nikova, bart.preneel@esat.kuleuven.be

ACM Computing Classification System (1998): D.4.6.

Key words: Secret Sharing Schemes, Proactive Security.

*The paper has been presented at the International Conference Pioneers of Bulgarian Mathematics, Dedicated to Nikola Obreshkoff and Lubomir Tschakaloff, Sofia, July, 2006.

The material in this paper was presented in part at the 11th Workshop on Selected Areas in Cryptography (SAC) 2004 [13].

Abstract. This paper investigates the security of Proactive Secret Sharing Schemes. We first consider the approach of using commitment to 0 in the renewal phase in order to refresh the player's shares and we present two types of attacks in the information theoretic case. Then we prove the conditions for the security of such a proactive scheme. Proactivity can be added also using re-sharing instead of commitment to 0. We investigate this alternative approach too and describe two protocols. We also show that both techniques are not secure against a mobile adversary. To summarize we generalize the existing threshold protocols to protocols for general access structure. Besides this, we propose attacks against the existing proactive verifiable secret sharing schemes, and give modifications of the schemes that resist these attacks.

ALGORITHMIC BACKGROUND OF THE HOST RECOMMENDATION IN THE ADAPTIVE DISTRIBUTED MULTIMEDIA SERVER

Tibor Szkaliczki*, Balázs Goldschmidt, Laszlo Böszörményi

e-mail: sztibor@sztaki.hu, balage@iit.bme.hu, laszlo@itec.uni-klu.ac.at

ACM Computing Classification System (1998): H.3.4, G.2.2, G.2.3.

Key words: distributed video server, host recommendation, optimisation, facility location problem.

*Partial support of the Hungarian State Eötvös Scholarship, the Hungarian National Science Fund (Grant No. OTKA 42559 and 42706) and the Mobile Innovation Center, Hungary is gratefully acknowledged.

Abstract. In a distributed server architecture an obvious question is where to deploy the components. Host recommendation, which gives the answer, faces problems such as server selection, host deployment and, in case of multimedia servers, video replication. It is especially relevant for the Adaptive Distributed Multimedia Server (ADMS) which is dynamically able to add and remove its components to different nodes of the network. The present survey paper introduces the different variants of host recommendation and gives an overview of its possible mathematical approaches. Emphasis is put on the facility location problem and the related approximation algorithms. Finally some algorithms selected for implementation are presented.