SUMMARIES

S. C. Shah, M.-S. Park, W. S. Choi, Z. H. Mir, S. H. Chauhdary, A. K. Bashir, F. H. Chandio. An Adaptive and Distance-based Resource Allocation Scheme for Interdependent Tasks in Mobile Ad Hoc Computational Grids. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 307 – 317.

Two key components contribute to task completion time: execution cost and communication cost. The communication cost is induced by data transfers between tasks residing on separate nodes. The communication is always expensive and unreliable in mobile ad hoc Grids and therefore plays a critical role in application performance. To reduce communication cost, interdependent tasks are allocated to nodes located close to one another. However, once the tasks have been allocated, nodes can move within a Grid. The movement of nodes within a Grid may result in multi-hop communication between nodes executing dependent tasks. In order to deal with node mobility within a Grid, an effective resource allocation scheme is required, but the design of such a scheme for mobile ad hoc computational Grids is challenging due to the constrained communication environment, node mobility, and infrastructure-less network environment. In this paper, we have developed an adaptive and distance-based resource allocation scheme which takes into account the characteristics of an application and nodes and applies migration heuristics to address the local node mobility problem. The scheme is validated in a simulated environment using various workloads and parameters.

J. Kapočiūtė-Dzikienė, G. Raškinis. Learning a Transferable World Model by Reinforcement Agent in Deterministic Observable Grid-World Environments. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 318 – 327.

Reinforcement-based agents have difficulties in transferring their acquired knowledge into new different environments due to the common identities-based percept representation and the lack of appropriate generalization capabilities. In this paper, the problem of knowledge transferability is addressed by proposing an agent dotted with decision tree induction and constructive induction capabilities and relying on decomposable properties-based percept representation. The agent starts without any prior knowledge of its environment and of the effects of its actions. It learns a world model (the set of decision trees) that corresponds to the set of explicit action definitions predicting action effects in terms of agent's percepts. Agent's planning component uses predictions of the world model to chain actions via a breadth-first search. The proposed agent was compared to the Q-learning and Adaptive Dynamic Programming based agents and demonstrated better ability to achieve goals in static observable deterministic grid-world environments different from those in which it has learnt its world model.

K. Kwon. Forward Reasoning via Sequential Queries in Logic Programming. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 328– 331.

Most Prolog implementations are based on backward chaining techniques. However, there are many applications in which forward chaining ones are desirable such as in dynamic programming. In this paper, we first introduce a variant of a Prolog interpreter that computes interpolations and then introduce the notion of sequential queries. These two notions allow a combination of both forms of reasoning in Prolog.

J. Mockus, R. Belevičius, D. Šešok, J. Kaunas, D. Mačiūnas. On Bayesian Approach to Grillage Optimization. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 332 – 339.

In this paper, a new simplified version of the Bayesian Approach to coordinate global optimization (BAcoor) is compared with the well-known algorithms. BAcoor is a method of multi-dimensional optimization by applying a sequence of one-dimensional global optimizers starting from the best points ob¬tained by previous one-dimensional optimization. The globality of one-dimension search is controlled by the only parameter. The new element is that observation points are defined by explicit formulas. In other similar methods this is performed by some numerical techniques that minimize the risk functions. The efficiency of suggested method is investigated and compared with other methods by solving a real-life civil engineering global optimization problem of pile placement schemes in grillage-type foundations. This problem is a good benchmark, because the minimal value of the objective function is known so the optimization error can be defined exactly.

H. Park, J. W. Lee. Task Assignment and Migration in Wireless Sensor Networks via Task Decomposition. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 340 – 348.

Energy consumption of sensor networks are largely affected by task assignments to the nodes in the network. In this paper, a task assignment method to improve the performance of wireless sensor networks, which exploits task decomposition and transformation, is presented. The task assignment is formulated as an optimization problem by providing a cost function incorporating the task decomposition and transformation at the same time. To show feasibility of our proposed method, simulated annealing approach is adopted. We also provided a distributed task migration method to support run-time of the given task on the network. While executing tasks in a node, if the remaining energy is less than pre-defined threshold level, the tasks in

the node will be migrated into a healthier neighbor node. The simulation results show that elaborate assignments and task decomposition can significantly improve performance of sensor networks.

K. Lukšys, E. Sakalauskas. Matrix Power Cipher. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 349 – 355.

In this paper a new symmetric matrix power cipher is presented. The main component of this cipher is the key dependent S-box based on the matrix power function (MPF). We give the details of the cipher and explain how MPF can be used in multiple rounds. The matrix power cipher due to its special algebraic structure can be highly parallelized and each round can be separated into up to m2 distinct threads, where m is the order of square matrices used in the cipher. A security analysis and main security parameters are also provided.

T. Skersys, L. Tutkutė, R. Butleris, R. Butkienė. Extending BPMN Business Process Model with SBVR Business Vocabulary and Rules. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 356 – 367.

Despite the fact that business process (BP) modeling has its long-lasting traditions in various areas of application, this discipline remains in the constant process of improvement and issue-solving. The possibilities of synergy among business process models and business vocabularies and rules are analyzed in this paper. We emphasize the existing gap between business process modeling and specification of business vocabularies and rules. Such a situation may lead to misunderstandings while reading and interpreting business models and also miscommunication issues within and among the organizations. Some of these issues could be resolved by realizing the integration of BP modeling standards with business vocabularies and rules. The paper presents some argumentation to back such statements. Later, basic principles of the approach for BPMN (Business Process Model and Notation) Business process model integration with SBVR (Semantics of Business Vocabulary and Business Rules) business vocabulary & rules are presented and briefly described in this paper.

A. Venčkauskas, N.Jusas, I. Mikuckienė, S. Maciulevičius. Generation of the Secret Encryption Key Using the Signature of the Embedded System. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 368 – 375.

Program protection, programming code integrity and intellectual property protection are important problems in embedded systems. Security mechanisms for embedded systems have some specific restrictions related to limited resources, bandwidth requirements and security. In this paper we develop a secret encryption key generation algorithm by using the signature of the embedded system. We explore the qualitative characteristic of the generated keys - the entropy. Experiments showed that the generated secret keys have high entropy.

P. Paškevičius, R. Damaševičius, E. Karčiauskas, R. Marcinkevičius. Automatic Extraction of Features and Generation of Feature Models from Ja-va Programs. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 376 – 384.

Feature modelling is a key technique for identifying common and variable features in software (software component families). The result of feature modelling is a feature model: a concise specification of product features and their relationships. Feature models have been proven to be useful for software variability modelling and management. However, there is a wide gap between feature models and program source code. Here we focus on reverse engineering of source code to feature models. We present a framework for the automated derivation of feature models from the existing software artefacts (components, libraries, etc.), which includes a formal description of a feature model, a program-feature relation meta-model, and a method for feature model generation based on feature dependency extraction and clustering. Feature models are generated in Feature Description Language (FDL) and as Prolog rules.

G. Liutkus, A. Riškus, A. Tomkevičius, A. Lenkevičius. Issues with Exchange of Presentation Data Among CAD Systems. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 385 – 391.

Today exchange of data among CAD systems becomes more important. As each CAD system has its own flavor to represent the same objects, exchange of data among them is full of issues. Most common problems are incomplete transfer of presentation information, associativity between representation and presentation, usage of annotation planes and text. They are analyzed in details and possible solutions are suggested as well.

SANTRAUKOS

S. C. Shah, M.-S. Park, W. S. Choi, Z. H. Mir, S. H. Chauhdary, A. K. Bashir, F. H. Chandio. Adaptyvi ir atstumu paremta išteklių paskirstymo schema, skirta nepriklausomoms užduotims mobiliuosiuose Ad Hoc skaičiavimo tinkluose. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 4, 307–317.

Du pagrindiniai komponentai – vykdymo išlaidos ir ryšių išlaidos – turi įtakos užduočių įvykdymo laikui. Ryšių sąnaudos sukeliamos perduodant duomenis užduotims, kurios priklauso atskiriems mazgams. Ryšiai visada yra brangūs ir nepatikimi mobiliuosiuose Ad Hoc tinkluose. Jie atlieka svarbų vaidmenį užtikrinant programos efektyvumą. Siekiant sumažinti ryšio išlaidas, tarpusavyje susijusios užduotys turi įtakos mazgams, esantiems arti vienas kito. Tačiau, kai užduotys būna paskirstytos, mazgai gali judėti tinklo viduje. Mazgų judėjimas tinkle gali sukelti daugiašuolį ryšį tarp mazgų, kurie vykdo vieną nuo kitos priklausančias užduotis. Siekiant spręsti mazgų judrumo tinkle problemą, reikalinga efektyvi išteklių priskyrimo schema. Tačiau kurti tokias schemas mobiliesiems Ad Hoc skaičiavimo tinklams yra gana sunku dėl apribotos ryšių aplinkos, mazgo judrumo ir tinklo su mažesne infrastruktūra aplinkos. Straipsnyje sukurta adaptyvi ir atstumu grindžiama išteklių paskirstymo schema, kuri apima programos savybes bei mazgus ir pritaiko judrumo euristiką atkreipiant dėmesį į vietinio mazgo judrumo problemą. Schema patikrinta imitacinėje aplinkoje naudojant įvairiausias darbines apkrovas ir parametrus.

J. Kapočiūtė-Dzikienė, G. Raškinis. Pastiprinimu paremto agento gebėjimas mokytis ir perkelti išmoktą pasaulio modelį į kitas pasiekiamas deterministines iš laukelių sudarytas aplinkas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 4, 318–327.

Pastiprinimu paremti agentai mokytis susiduria su problemomis perkeldami vienoje aplinkoje įgytas žinias į naujas aplinkas: taip nutinka dėl receptorių pateikimų interpretavimo būdo ir mechanizmų, leidžiančių tinkamai apibendrinti receptorių pateikimus, trūkumo. Straipsnyje ši žinių perkeliamumo problema yra sprendžiama pasiūlius agentą, kuris taiko sprendimų medžio indukcijos ir konstrukcinės indukcijos metodus, o receptorių pateikimus interpretuoja kaip paskirstytą savybių rinkinį. Pradėdamas darbą agentas neturi jokių žinių nei apie aplinką, nei apie savo veiksmų pasekmes. Jis išmoksta pasaulio modelį (sprendimų medžių rinkinį), atitinkantį išsamius veiksmų aprašymus, pagal kurį turint konkrečius receptorių pateikimus, galima prognozuoti veiksmų pasekmes. Agento planavimo komponentė, paremta paieškos platyn metodu: ji ieško veiksmų grandinių nuo vienos aplinkos situacijos iki kitos naudodama pasaulio modelį ir pagal jį suprognozuotus receptorių pateikimus. Pasiūlytas metodas palygintas su Q-mokymo ir Adaptyvaus dinaminio programavimo metodais: pateiktos metodų galimybės siekti tikslų statinėse stebimose deterministinėse iš laukelių sudarytose aplinkose, taikant ne toje pačioje aplinkoje išmoktus pasaulio modelius.

K. Kwon. Argumentų perdavimas loginiame programavime naudojant nuoseklias užklausas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 4, 328–331.

Dauguma prologo kalbos realizacijų grindžiamos atgaliniais grupavimo būdais. Tačiau yra daug programų, kuriose pageidaujami tokie pirminiai grupavimo būdai, kokie taikomi dinamiškame programavime. Šiame straipsnyje iš pradžių pristatomas Prologo vertėjo variantas, kuris apskaičiuoja interpoliacijas, paskui pateikiama nuoseklių užklausų sąvoka. Vartojant šias dvi sąvokas galima abiejų formų samprotavimo Prologe kombinacija.

J. Mockus, R. Belevičius, D. Šešok, J. Kaunas, D. Mačiūnas. Sijyno optimizavimas Bajeso metodu. Informacinės technologijos ir valdymas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 4, 332–339.

Straipsnyje pristatoma nauja supaprastinta Bajeso metodo versija koordinačių globaliajam optimizavimui (Bacoor) aptarti, kuri palyginama su kitais gerai žinomais algoritmais. Bacoor – tai daugiakriterio optimizavimo metodas, taikantis vienakriterių globaliojo optimizavimo algoritmų seką, pradedant nuo ankstesnio vienakriterio optimizavimo proceso metu gautų geriausių taškų. Vienakriterės paieškos globalumas yra kontroliuojamas vieninteliu parametru. Nauja yra tai, kad paieškos taškai apibrėžiami tiksliomis formulėmis. Taikant kitus panašius metodus, tai atliekama tam tikrais skaitiniais metodais, kurie minimizuoja rizikos funkcijas. Pasiūlyto metodo efektyvumas nagrinėjamas su kitais metodais ir lyginamas su jais, sprendžiant realius statybos inžinerijos polių išdėstymo schemų rostverkiniuose pamatuose globaliojo optimizavimo uždavinius. Tai itin tinkama metodams palyginti, nes tikslo funkcijos minimali reikšmė yra žinoma iš anksto, ir optimizavimo paklaida gali būti tiksliai įvertinta.

H. Park, J. W. Lee. Užduoties priskyrimas ir perkėlimas naudojant užduoties dekompoziciją belaidžiuose sensoriniuose tinkluose. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 4, 340–348.

Sensorinių tinklų energijos sunaudojimas daugiausia priklauso nuo užduoties priskyrimo taškams tinkle. Straipsnyje pateikiama užduoties priskyrimo metodika, siekiant pagerinti belaidžių sensorinių tinklų, kurie naudoja užduoties dekompoziciją

ir transformaciją, eksploatacijos savybes. Užduoties priskyrimas yra suformuluojamas kaip optimizavimo problema, pateikiant kainos funkciją, kuri kartu įtraukia užduoties dekompoziciją ir transformaciją. Pasiūlyto metodo pagrįstumui įrodyti parinktas imitacinis atkaitinimo metodas. Taip pat pateikiamas paskirstytas užduoties perkėlimo metodas, siekiant išlaikyti nustatytos užduoties atlikimo laiką tinkle. Atliekant užduotis mazge, jei likusi energija mažesnė negu iš anksto nustatyta riba lygmenyje, užduotys mazge bus perkeltos į sveikesnį kaimyninį mazgą. Imitavimo rezultatai rodo, kad sudėtingos užduotys ir užduoties dekompozicija gali žymiai pagerinti sensorinių tinklų veikimą.

K. Lukšys, E. Sakalauskas. Matricinio laipsnio šifras. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 4, 349–355.

Straipsnyje pateikiamas naujas simetrinis matricinio laipsnio šifras. Pagrindinis šio šifro elementas yra sukeitimo blokas, kuris paremtas matricinio laipsnio funkcija ir priklauso nuo slaptųjų šifravimo raktų. Straipsnyje pateikiamas šifro aprašas ir paaiškinama, kaip matricinio laipsnio funkcija gali būti panaudota iteraciniame šifre. Matricinio laipsnio šifras dėl savo specifinės algebrinės struktūros gali būti efektyviai lygiagretinamas. Kiekviena iteracija gali būti išskaidyta iki m^2 skirtingų gijų (m yra šifre naudojamų kvadratinių matricų eilė). Taip pat pateikiami šifro saugumo analizė ir pagrindiniai saugumo parametrai.

T. Skersys, L. Tutkutė, R. Butleris, R. Butkienė. BPMN veiklos procesų modelio praplėtimas SBVR veiklos žodynu ir taisyklėmis. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 356–367.

Nepaisant to, kad veiklos procesų modeliavimas turi senas tradicijas įvairiose taikymo srityse, ši disciplina nuolatos tobulinama ir sprendžiamos vis naujai iškylančios problemos, susijusios su ja. Straipsnyje tiriamos veiklos procesų integravimo su veiklos žodynais ir veiklos taisyklėmis galimybės. Straipsnio autoriai pabrėžia, kad šiuo metu vis dar egzistuoja atotrūkis tarp šių veiklos konceptų. Esama situacija gali daryti įtaką netinkamam veiklos modelių skaitymui, jų interpretavimui, taip pat nesusikalbėjimui tiek pačios organizacijos viduje, tiek ir tarp skirtingų organizacijų. Straipsnyje identifikuoto atotrūkio tarp veiklos procesų ir veiklos žodynų bei veiklos taisyklių problemai spręsti, taikomas autorinis šių veiklos konceptų integracijos metodas. Šis metodas grindžiamas inovatyviais OMG grupės standartais BPMN (*Business Process Model and Notation*) ir SBVR (*Semantics of Business Vocabulary and Business Rules*).

A. Venčkauskas, N. Jusas, I. Mikuckienė, S. Maciulevičius. Slaptojo šifravimo rakto generavimas, naudojant įterptosios sistemos parašą. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 368–375.

Įterptųjų sistemų programų apsauga, programinio kodo vientisumo ir intelektinės nuosavybės užtikrinimas yra svarbios problemos. Įterptųjų sistemų saugumo mechanizmams būdingi tam tikri specifiniai apribojimai, sąlygoti ribotų išteklių, skaičiavimo pajėgumų ir saugumo reikalavimų. Straipsnyje pateiktas slaptų šifravimo raktų generavimo algoritmas, naudojant įterptosios sistemos parašą. Ištirta generuojamų raktų kokybinė charakteristika – entropija. Eksperimentai parodė, kad generuojami slapti raktai turi aukštą entropiją.–

P. Paškevičius, R. Damaševičius, E. Karčiauskas, R. Marcinkevičius. Automatinio Java programų požymių gavimo ir požymių modelių kūrimo metodas. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 376–384.

Požymių modeliavimo tikslas – nustatyti pastovius ir kintamus programų (ar programų šeimynų) požymius. Požymių modeliavimo rezultatas yra požymių modelis, kurį naudojant trumpai aprašomi programos požymiai ir jų sąryšiai. Požymių modeliai naudojami programų variantiškumui modeliuoti ir valdyti, tačiau šiuo metu tarp programos išeities tekstų ir požymių modelių yra spraga. Straipsnyje nagrinėjamas požymių modelių gavimas iš turimo programos (komponentų bibliotekos) išeities teksto taikant apgražos inžinerijos metodą. Siūlomas automatinio požymių modelių kūrimo metodas pagrįstas formaliu požymių modelio aprašu, programos-požymių sąryšio metamodeliu, požymių sąryšio grafo radimu ir požymių grupavimu. Požymių modeliai kuriami FDL ir Prolog kalbomis.

G. Liutkus, A. Riškus, A. Tomkevičius, A. Lenkevičius. Uždavinių, iškylančių apsikeitus pateikiamiems duomenims tarp CAD sistemų, sprendimas. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 4, 385–391.

Pastaruoju metu duomenims apsikeisti tarp CAD sistemų tampa vis svarbiau. Kadangi kiekviena CAD sistema turi savitą tų pačių objektų modeliavimo ir vaizdavimo būdą, apsikeisti duomenimis tampa problemiška. Tenka spręsti daug ir įvairių uždavinių. Viena iš problemų – nevisa informacija apie pateikiamus duomenis ir šių duomenų perdavimas. Kiti spręstini uždaviniai: ryšių tarp pateikiamų ir vaizdavimo duomenų atkūrimas, anotacijų plokštumų ir teksto vartojimas. Straipsnyje visi šie uždaviniai yra detaliai išnagrinėti, pasiūlyti galimi jų sprendimo būdai.