SUMMARIES

E. Vyšniauskas, L. Nemuraitė, B. Paradauskas. Quality Estimation of Speech Recognition Features for Dynamic Time Warping Classifier. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 2, 103 – 115.

The goal of the paper is to define requirements to OWL 2 ontologies, under which their semantics may be preserved in a relational database, and to demonstrate that the hybrid approach for transforming OWL 2 ontologies into relational databases possesses such capability. The hybrid approach maps part of ontology concepts to relational database concepts on the base of their common semantics; ontology constructs having no direct equivalents in databases are stored in metatables. The paper defines requirements for ontologies under transformation as ontology normalization and integrity rules, and presents a set of SQL queries for extracting rich data, covering semantics of source ontology, from the resulting database. The capability of the hybrid approach to preserve semantics of OWL 2 ontologies in relational databases is demonstrated with a representative example of a Vehicle ontology.

U. Legat, A. Biasizzo, F. Novak. On-Line Self-Recovery of Embedded Multi-Processor SOC on FPGA Using Dynamic Partial Reconfiguration. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 2, 116 – 124.

An error-recovery method for embedded multi-processor systems on SRAM-based FPGAs is proposed. This method is effective against soft-errors in the configuration memory, such as the errors caused by high energy radiation also known as Single Event Upsets. The error-recovery algorithm performs on-line test of the FPGA configuration memory and recovers errors using dynamic partial reconfiguration. Processor cores perform a distributed recovery procedure. If a failure occurs in the processor currently running the recovery algorithm, another processor core takes the role and performs reconfiguration. Presented case study demonstrates the advantage of the proposed approach.

S. Minkevičius, L. Sakalauskas. Modeling of the Phenomena in Multiserver Networks. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 2, 125 – 135.

The paper is devoted to the analysis of queueing systems in the context of the network and communications theory. We investigate a theorem on the law of the iterated logarithm for a queue of jobs in an open multiserver queueing network and its applications to the mathematical models of the generalized Internet system and a multiserver computer system.

R. Maskeliūnas, K. Ratkevičius. HMI Modelling for Multimodal Lithuanian Applications. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 2, 136 – 142.

Spoken dialogue based human-machine interfaces (HMI) are becoming more and more widely integrated in computer applications. Speech allows doing some task easier and faster. The combination with a more traditional means of inputs and outputs – i.e. the multimodality factor becomes more and more important allowing wider accessibility. It is important to model and design spoken language dialog trees to imitate the natural conversations in the human-computer interactions, especially in information retrieval systems and applications. The paper presents three algorithms of HMI dialogs and the results of their experimental evaluation. The results showed that it is possible to achieve about 97% recognition accuracy in simple phrase based dialog conversations and about 93% in a very naturally sounding keyword spotting based dialogs

H. Huang, Y. Zhuang, G. Ma., Y. Lv. Optimal Spacecraft Formation Reconfiguration with Collision Avoidance Using Particle Swarm Optimization. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 2, 143 – 150.

This paper presents an energy-optimal trajectory planning method for spacecraft formation reconfiguration in deep space environment using continuous low-thrust propulsion system. First, we employ the Legendre pseudospectral method (LPM) to transform the optimal reconfiguration problem to a parameter optimization nonlinear programming (NLP) problem. Then, to avoid the computational complexity for calculating the gradient information caused by traditional optimization methods, we use particle swarm optimization (PSO) algorithm to solve the NLP problem. Meanwhile, in order to avoid the collision between any pair of Legendre-Gauss-Lobatto (LGL) points, we insert some test points in the region where collision may happen most likely. What's more, the collision avoidance constraints are also checked at these test points. Finally, numerical simulation shows that the energy-optimal trajectories for spacecraft reconfiguration could be generated by the method we proposed in a relative short time, so that it could be adopted on-board for practical spacecraft formation problems.

M.-L. Chiang, H.-C. Hsieh. A New Approach to the Fault Detection Problem for Mobile P2P Network. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 2, 151 – 161.

To improve the performance of mobile P2P network systems, all the faulty-free peers must be able to function collaboratively. Regrettably, some peers may be untrustworthy and unwilling to cooperate with others. Some peers may even attack the network resulting in the performance degrades. For this reason, it is very important to provide a reliable protocol to detect and remove faulty peers. In the past, there have some traditional BA protocols been proposed for fault detection, in which

all peers require to exchange 2 * (⌊(*n*-1)/3⌋ +1) rounds of message to collect messages; and the complexity of messages is $O(n^{\lfloor (n-1)/3 \rfloor * \lfloor (n-1)/3 \rfloor})$. However, the previous protocols are inefficient and unsuitable for the mobile P2P network because most of the protocols do not concern the mobility issue, and can cause large number of message results in a large protocol overhead. In this study, we proposed a new fault detection protocol to detect/locate faulty peers by using only three rounds of message exchange. Furthermore, the complexity of protocol we proposed can be reduced to $O(n^2)$ even if some peers move around the network. Since, our proposed protocol is more suitable and efficient for mobile P2P network.

M. Liu, B. Liu, Y. Liu, C. Sun. Data Evolvement Analysis Based on Topology Self-Adaptive Clustering Algorithm. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 2, 162 – 172.

Along with the fast advance of internet technique, internet users have to deal with tremendous data every day. One of the most useful knowledge exploited from web is about the transfer of the information expressed by two data sets collected in different time phases. With this kind of knowledge, we can further apprehend what information newly appears, what information is antiquated, and what information maintains unchanged along with time passing. The task aiming at acquiring this kind of knowledge is formally entitled as data evolvement analysis. Clustering is a good solution to this task. By comparing the clustering results respectively formed in different time phases, it is easy to acquire the transfer of the information. Unfortunately, aforementioned plan is time- consuming, since it needs to perform clustering algorithm once again, once input data are updated. Therefore, we need to design a dynamic clustering algorithm. Once input data are updated, it can form clustering results by adjusting the existent cluster partition instead of performing clustering algorithm again. For this reason, a novel Topology Self-Adaptive Clustering algorithm (abbreviated as TSAC) is proposed in this paper. This algorithm comes from Self Organizing Mapping algorithm (abbreviated as SOM), whereas, it doesn't need to make any assumption about neuron topology beforehand. Besides, when input data are updated, its topology remodels meanwhile. For further enhancing its performance, it imports minimum spanning tree to preserve its topology order, which is never performed by any traditional SOM based algorithms. For clearly measuring the magnitude of the transfer of the information, it partitions data space into several grids, and calculates the density of each grid to quantify the transfer. Experiment results demonstrate that TSAC can automatically tune its topology. By this algorithm and in addition to grid structure, the transfer of the information can be legibly visualized.

Y.–M. Tseng, C.–H. Yu, T.–Y. Wu. Towards Scalable Key Management for Secure Multicast Communication. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 2, 173 – 182.

Secure multicast communication allows a sender to deliver encrypted messages to a group of authorized receivers. A practical approach is that the sender uses a common key shared by the authorized receivers to encrypt the transmitted messages. The common key must be renewed to ensure forward/backward secrecy when group members leave/join the group, called the rekeying process. Thus, the rekeying problem is a critical issue for secure multicast communication. Many key management schemes have been proposed to improve the performance of the rekeying process. In 2010, Lin et al. proposed two key management schemes without the rekeying process. However, the transmission size required in their schemes increases linearly with the number of group members. In this article, we use the time-bound concept to propose two new key management schemes without the rekeying process. The point is that the required transmission size is constant. Performance analysis is given to demonstrate that our schemes have better performance as compared with the recently proposed key management schemes in terms of transmission size and computational cost. Under several security assumptions, we prove that the proposed schemes satisfy the requirements of secure multicast communication.

C.-F. Cheng, K.-T. Tsai, H.-C. Liao. A Simple and Efficient Signature-based Consensus Protocol in the Asynchronous Distributed System. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 2, 183 – 198.

The consensus problem in distributed systems is mainly solved by message exchange. Most of previous consensus algorithms rely on exchange of oral messages to achieve consensus among processors. As oral messages are susceptible to influences from malicious attackers, this type of consensus protocols usually requires a large number of rounds of message exchange, and the complexity of message exchange is also excessively high. In light of this drawback of oral message-based consensus algorithms, some scholars proposed signed message-based consensus algorithm to reduce the number of rounds of message exchange required. However, some signed message-based consensus algorithms still have certain drawbacks which make them ineffective in some conditions. To address this issue, we propose a new signed message-based consensus algorithm in this paper. We integrate the concept of grouping into the proposed algorithm and find the best number of groups through mathematical analysis to further reduce the rounds of message exchange required. In other words, the proposed algorithm makes use of digital signature and the concept of grouping to solve the consensus problem.

SANTRAUKOS

E. Vyšniauskas, L. Nemuraitė, B. Paradauskas. OWL 2 ontologijų semantikos išsaugojimas reliacinėse duomenų bazėse taikant hibridinį metodą. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 2, 103 – 115.

Straipsnio tikslas – apibrėžti sąlygas, kurioms esant OWL 2 ontologijų semantiką galima išsaugoti reliacinėse duomenų bazėse ir parodyti, kad hibridinis OWL 2 ontologijų saugojimo reliacinėse duomenų bazėse metodas šią galimybę teikia. Straipsnyje analizuojamos ontologijų normalizavimo ir vientisumo užtikrinimo taisyklės bei jas atitinkanti transporto ontologija ir duomenų bazė, sugeneruota taikant hibridinį metodą, kai dalis ontologijos darinių tiesiogiai vaizduojama reliacine schema, o kita dalis, neturinti tiesioginio atvaizdžio duomenų bazėje, saugoma metalentelėse. Pateikiamos SQL užklausos rodo, kaip metalentelės padeda išgauti vertingesnę informaciją, atitinkančią ontologijos semantiką

U. Legat, A. Biasizzo, F. Novak. Aktyvus įterptųjų sistemų, sudarytų iš daugiaprocesorės SOC sistemos FPGA pagrindu, atsikūrimas naudojant dinaminį dalinį pertvarkymą. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 2, 116 – 124.

Siūlomas klaidos atitaisymo metodas, skirtas įterptinėms daugiaprocesorėms sistemoms atkurti naudojant SRAM grindžiamas FPGA. Šis metodas tinka šalinti nedidelėms klaidoms, atsirandančioms konfigūracijos atmintyje, pavyzdžiui, dėl didelės energijos spinduliuotės, taip pat vadinamoms vieno įvykio sutrikimais. Klaidos atkūrimo algoritmas tinkle atlieka FPGA konfigūracijos atminties testą ir ištaiso klaidas dinaminio dalinio pertvarkymo būdu. Procesoriaus branduoliai įvykdo paskirstytą atitaisymo procedūrą. Jei atitaisymo algoritmą vykdančiame procesoriuje įvyksta klaida, kitas procesoriaus branduolys perima algoritmo vykdymą ir atlieka pertvarkymą. Pateiktas pavyzdinio atvejo tyrimas parodo siūlomo metodo pranašumus.

S. Minkevičius, L. Sakalauskas. Apie netiesinius reiškinius skaitmeniniuose tinkluose. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 2, 125 – 135.

Šio aptarnavimo teorijos tyrimo tikslas yra teorema, pateikianti dvigubo logaritmo dėsnį paraiškų eilės ilgiui atvirame daugiakanaliame aptarnavimo tinkle, taip pat šios teoremos taikymas, kuriant matematinius kompiuterio ir interneto pranešimų siuntimo sistemų modelius.

R. Maskeliūnas, K. Ratkevičius. Žmogaus ir mašinos sąsajos, skirtos multimodaliems taikymams Lietuvoje, modeliavimas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 2, 136 – 142.

Vartotojo ir kompiuterio tarpusavio sąsaja, dar vadinama žmogaus ir mašinos sąsaja, tampa vis svarbesne komunikacinių paslaugų dalimi. Naudojant tokią sąsają galima sėkmingiau ir efektyviau atlikti daugelį pagrindinių telekomunikacinėms paslaugoms keliamų užduočių, kurių svarbiausia yra sujungti ir leisti tarpusavyje bendrauti asmenims bet kurioje pasaulio vietoje bet kuriuo metu. Tai gali užtikrinti tiktai mobilūs įrenginiai. Tokie įrenginiai turi nedidelę klaviatūrą ir nedidelį ekraną, todėl balsinė sąsaja daugeliu atvejų yra pranašesnė. Straipsnyje pateikiami trys multimodalios sąsajos modeliai ir jų eksperimentinio įvertinimo rezultatai. Parodyta, kad galima gauti apie 97 % lietuviškų skaičių pavadinimų atpažinimo tikslumą, kai skaičiai yra ilgose frazėse, ir apie 93 % atpažinimo tikslumą, kai skaičiai yra trumpuose natūraliai skambančiuose balso dialoguose ir vyksta raktažodžių paieška.

H. Huang, Y. Zhuang, G. Ma., Y. Lv. Optimalus erdvėlaivio sandaros pertvarkymas susidūrimui išvengti optimizuojant dalelių spiečių. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 2, 143 – 150.

Straipsnyje pristatomas optimalus energijos vartojimo trajektorijos planavimo metodas, skirtas erdvėlaivio sandarai pertvarkyti kosminėje aplinkoje, naudojant nuolatinę silpnos jėgos impulso sistemą. Pirma, optimaliai pertvarkymo problemai pakeisti į parametrų optimizavimo netiesinę programavimo problemą (NLP) taikomas Legendre pseudo-spektrinis metodas (LPM). Tuomet, siekiant išvengti sudėtingų tradicinio optimizavimo metodų sukeltų gradiento skaičiavimų, naudojamas dalelių spiečiaus optimizavimo (PSO) algoritmas NLP problemai spręsti, o kad būtų galima išvengti susidūrimo tarp bet kokios poros Legendre, Gausso ir Lobatto (LGL) taškų, įterpiami kai kurie testavimo taškai į tą sritį, kur susidūrimas yra labiausiai tikėtinas. Taip pat yra tikrinami susidūrimo vengimo apribojimai šiuose testavimo taškuose. Galiausiai skaitmeninis modeliavimas parodo, kad erdvėlaiviui pertvarkyti optimalias energijos trajektorijas galėtų generuoti metodas, pasiūlytas per palyginti trumpą laiką, taigi, tai galėtų būti pritaikyta praktinėms erdvėlaivio sandaros problemoms spręsti.

M.-L. Chiang, H.-C. Hsieh. Naujas požiūris į judriojo ryšio P2P tinklo klaidų aptikimo problemą. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 2, 151 – 161.

Siekiant pagerinti judriojo ryšio P2P tinklo sistemų darbą, visi neturintys klaidų lygiarangiai turi gebėti veikti bendrai. Gaila, bet kai kurie lygiarangiai gali būti nepatikimi ir nenorėti bendradarbiauti su kitais arba gali net atakuoti tinklą, o dėl to mažėja efektyvumas. Dėl šios priežasties labai svarbu turėti patikimą protokolą, kuris aptiktų ir pašalintų klaidingus lygiarangius. Anksčiau buvo pasiūlyti keli tradiciniai klaidų aptikimo BA protokolai, pagal kuriuos visiems lygiarangiams reikėjo apsikeisti 2 * (⌊(*n*-1)/3⌋ +1) žinučių ciklais, kad sukauptų žinutes, ir žinučių sudėtingumas yra O($n^{\lfloor (n-1)/3 \rfloor * \lfloor (n-1)/3 \rfloor}$). Tačiau ankstesni protokolai yra neefektyvūs ir netinkami judriojo ryšio P2P tinklui, nes dauguma protokolų neapima judrumo problemos, ir žinučių gali būti daug, o dėl to protokole labai padaugėja papildomos informacijos. Šiame moksliniame tyrime pasiūlytas naujas klaidų aptikimo protokolas, kad būtų galima aptikti/nustatyti klaidingus lygiarangius, atliekant tik tris apsikeitimo žinutėmis ciklus. Be to, pasiūlytąjį protokolą galima supaprastinti iki O(n2), net jei kai kurie lygiarangiai juda aplink tinklą. Vadinasi, mūsų pasiūlytas protokolas judriojo ryšio P2P tinklui yra tinkamesnis ir efektyvesnis.

M. Liu, B. Liu, Y. Liu, C. Sun. Duomenų plėtros analizė pagrįsta topologiniu prisitaikančių sankaupų formavimo algoritmu. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 2, 162 – 172.

Interneto technologijoms sparčiai tobulėjant, interneto vartotojai kiekvieną dieną susiduria su didžiuliais duomenų kiekiais. Viena iš naudingiausių žinių, išgautų iš tinklo, yra žinia apie informacijos perkėlimą, išreikštą dviem duomenų rinkiniais, surinktais skirtingose laiko fazėse. Šios rūšies žinios leidžia nuspėti, kuri informacija pasirodo naujai, kuri yra pasenusi ir kuri informacija laikui bėgant neesikeičia. Užduotis, kuria siekiama įgyti šios rūšies žinių, formaliai yra vadinama duomenų plėtros analize. Sankaupų formavimas yra tinkamas šios užduoties sprendimo būdas. Lyginant sankaupų suformavimo skirtingose laiko fazėse rezultatus, lengva sukombinuoti informacijos perkėlimą. Deja, tam planui reikia daug laiko sąnaudų, nes jis turi įvykdyti sankaupų formavimo algoritmą dar kartą po to, kai atnaujinami įvestieji duomenys. Todėl turime suprojektuoti dinamišką sankaupų formavimo algoritmą. Kai įvesties duomenys atnaujinti, algoritmas gali suformuoti sankaupų formavimo rezultatus reguliuodamas esamą sankaupos padalijimą, užuot vėl vykdęs sankaupų formavimo algoritmą. Dėl šios priežasties šiame darbe siūlomas neįprastas topologinis prisitaikančių sankaupų formavimo algoritmas (angl. santrumpa TSAC). Šis algoritmas kilo iš savaime susitvarkančiojo žemėlapio algoritmo (angl. santrumpa SOM), tačiau iš anksto nereikia daryti jokių prielaidų apie neuronų topologiją. Be to, kai įvesties duomenys atnaujinami, jų topologija atsikuria. Atlikimui toliau gerinti importuojamas minimalus apimties medis, kad būtų išsaugota jo topologijos tvarka, o to neatlieka joks tradicinis SOM pagrįstas algoritmas. Informacijos perkėlimo dydžiui tiksliai išmatuoti jis padalija duomenų erdvę į kelis tinklelius ir apskaičiuoja kiekvieno tinklelio tankumą, kad nustatytų perkėlimo kiekį. Bandymo rezultatai rodo, kad TSAC gali automatiškai suderinti savo topologiją. Šis algoritmas ir jo papildymas tinklelių struktūra leidžia tinkamai vizualizuoti informacijos perkėlimą.

Y.–M. Tseng, C.–H. Yu, T.–Y. Wu. Keičiamo dydžio rakto valdymo schema saugiam daugiataškiam sujungimui sudaryti. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 2, 173 – 182.

Saugus daugiataškis sujungimas leidžia siuntėjui nusiųsti užšifruotas žinutes grupei įgaliotų priėmėjų. Praktiškai tai reiškia, kad siuntėjas naudoja bendrą raktą, kurį turi įgaliotieji gavėjai perduodamoms žinutėms užšifruoti. Bendras raktas turi būti atnaujinamas siekiant užtikrinti slaptumą perdavimo ir priėmimo metu, kai grupės nariai palieka/prisijungia prie grupės. Toks procesas vadinamas raktų pakeitimu. Taigi, raktų pakeitimo problema yra esminė siekiant saugaus daugiataškio sujungimo. Buvo pasiūlyta daug rakto valdymo schemų be raktų pakeitimo proceso. 2010 m. Lin ir kt. pasiūlė dvi rakto valdymo schemas be raktų pakeitimo proceso. Tačiau jų schemose daugėjant grupės narių skaičiui reikalaujamas perdavimo dydis tiesiškai didėja. Šiame straipsnyje naudotasi laiko apribojimo sąvoka siūlant dvi naujas rakto valdymo schemas be rakto pakeitimo. Esmė yra ta, kad reikiamas perdavimo dydis yra pastovus. Veiklos analizė pateikiama parodant, kad mūsų schemos veikia geriau palyginant su neseniai siūlytomis rakto valdymo schemomis, atsižvelgiant į perdavimo dydį ir skaičiavimo sąnaudas. Darant kelias saugumo prielaidas, įrodyta, kad siūlomos schemos tenkina saugaus daugiataškio sujungimo reikalavimus.

C.-F. Cheng, K.-T. Tsai, H.-C. Liao. Paprastas ir veiksmingas parašu pagrįstas susitarimo protokolas asinchroniškoje paskirstytojoje sistemoje. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 2, 183 – 198.

Susitarimo problema paskirstytosiose sistemose daugiausia yra sprendžiama apsikeitimu žinutėmis. Dauguma ankstesnių susitarimo algoritmų priklauso nuo žodinių apsikeitimų žinutėmis, kad pasiektų susitarimą tarp procesorių. Kadangi žodinės žinutės yra pasiduodančios kenkėjiškų puolėjų įtakoms, šio tipo susitarimo protokolams paprastai reikia daug apsikeitimo žinutėmis ciklų, ir apsikeitimas žinutėmis taip pat yra pernelyg sudėtingas. Atsižvelgdami į šį žodine žinute pagrįstų sutarimo algoritmų trūkumą, kai kurie mokslo žmonės pasiūlė pasirašyta žinute pagrįstą susitarimo algoritmą, kad sumažintų reikalingą apsikeitimo žinutėmis ciklų skaičių. Tačiau, kai kurie pasirašyta žinute pagrįsti susitarimo algoritmai vis dar turi trūkumų, kurie tam tikromis sąlygomis padaro juos neefektyvius. Siekdami atkreipti dėmesį į šią problemą, šiame straipsnyje siūlome pasirašyta žinute pagrįstą susitarimo algoritmą. Į pasiūlytąjį algoritmą integruojame grupavimo koncepciją ir, siekdami sumažinti reikalingus apsikeitimo žinutėmis ciklus, matematinės analizės būdu randame geriausią grupių skaičių. Kitaip tariant, pasiūlytas algoritmas naudoja skaitmeninį parašą ir grupavimo sąvoką, kad išspręstų sutarimo problemą. Šis algoritmas gali ne tik padidinti paskirstytųjų sistemų klaidos toleranciją, bet ir gerokai sumažinti susitarimui pasiekti reikalingą apsikeitimo žinutėmis ciklų skaičių.