SUMMARIES

P. Treigys, V. Marcinkevičius, A. Kaklauskas. Analysis of Iris and Pupil Parameters for Stress Recognition. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 1, 7 – 14.

The aim of this study is to automatically identify the iris and pupil of the eye in the video stream and to parameterize the identified structures in order to make assumptions if the subjected is stressed or not. During tests ,subjects were given a number of issues which they had to respond by selecting only one correct answer. Visual material was gathered using a helmet-fitted stationary near-infrared camera that recorded iris and pupil of the eye reactions to stimuli. Subsequently it was made an automatic iris and pupil recognition and approximation by curves in the gathered sequence of images. Each change in the pupil size is described by different time series length. Thus, it is impossible to compare the obtained data using the Euclidean distance measures. For this reason, the metrics based on periodograms were used to compare the data series. The differences calculated between the eye pupil reaction to stimuli and question show-up time was introduced in multidimensional scaling algorithms for dimension reduction. It was noticed that the stimuli to the false answers tend to cluster.

S. Tallapally. Security Enhancement on Simple Three Party PAKE Protocol. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 1, 15 – 22.

In the field of cryptography, the three-party authenticated key exchange protocol is an important tool, especially in the secure communication areas. In this protocol, two clients share a human-memorable password with a trusted server whereby the two clients receive a secure session key. Most recently, Huang proposed a simple and efficient three party password-based key exchange protocol. She claimed that the proposed protocol is secure against various attacks. However, Yoon and Yoo proved an undetectable online password guessing attack on Huang's protocol. In the present paper, an unknown key share attack on Huang's three party PAKE protocol using undetectable online password guessing attack is demonstrated. Additionally, an alternative protocol that eliminates this attack is proposed. Moreover, the proposed protocol requires only four message transmission rounds.

V. Štuikys, R. Damaševičius, G. Ziberkas, K. Valinčius. Understanding of Heterogeneous Multi-Stage Meta-Programs. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 1, 23 – 32.

The paper analyzes an approach to understanding heterogeneous meta-programs and multi-stage meta-programs. At the core of the approach is human-centred analysis combined with the Brook's program cognition theory and the concept of reverse engineering. The use of the approach leads to extracting higher-level models (graphs representing meta-parameter – meta-function relationship models, feature diagrams and algorithms) from correct meta-specifications. The models and processes enable not only to better understand the multi-stage heterogeneous meta-programs but also to contribute to their evolution. The paper describes some properties of the multi-stage heterogeneous meta-programs. The approach is supported by the case study and complexity evaluation.

E. Sakalauskas. The Multivariate Quadratic Power Problem over $\boldsymbol{Z}_n$ is NP-Complete. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 1, 33 – 39.

In this paper a new NP-complete problem, named as multivariate quadratic power (MQP) problem, is presented. This problem is formulated as a solution of multivariate quadratic power system of equations over the semigroup (monoid) $\boldsymbol{Z}_n$ and is denoted by MQP($\boldsymbol{Z}_n$), where n is a positive integer. Two sequential polynomial-time reductions from the known NP-complete multivariate quadratic (MQ) problem over the field $\boldsymbol{Z}_2$, i.e. MQ($\boldsymbol{Z}_2$) to MQP($\boldsymbol{Z}_n$), are constructed. It is proved that certain restricted MQP($\boldsymbol{Z}_n$) problem over some subgroup of $\boldsymbol{Z}_n$ is equivalent to MQ($\boldsymbol{Z}_2$) problem. This allows us to prove that MQP($\boldsymbol{Z}_n$) is NP-complete also. The MQP problem is related to matrix power function (MPF) which was used for construction of several cryptographic protocols. We expect that the NP-complete problem announced here could be used to create new candidate one-way functions (OWF) and to construct new cryptographic primitives.

V. Laurutis, I. Indrijauskienė, R. Zemblys S. Niauronis. Effects of Müller-Lyer Illusion on the Accuracy of Primary Saccades and Smooth Pursuit Eye Movements. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 1, 40 – 45.

The goal of the present investigation was to support or to oppose the two-visual-system (vision–for perception and vision-for action) hypothesis. Since illusions might be the subject of misinterpretation and the loss of presented information, we decided to examine how Müller-Lyer (M-L) illusion affects accuracy of double-step saccades and smooth pursuit eye movements and compare these results with those obtained during perceptual judgment of the length of the shaft of M-L illusion. Experimental investigation revealed that the primary saccades elicited in double-step mode were mostly affected by the M-L illusion. The position errors of the primary saccades elicited in the reflexive mode were affected by 4% for wings-in illusion and by 3.6% for wings-out illusion comparing with the 0.25% and 0.1% for the saccades elicited in the voluntary mode. The position errors of complete saccades (0.14% and 0.02%) and tracking errors obtained during the smooth pursuit (0.11% and 0.05%) were negligibly small. Nevertheless, experimental results obtained during perceptual judgment of M-L illusion were substantially

larger – 14% and 10%, respectively. Our experimental investigation of the accuracy of saccadic and smooth pursuit eye movements elicited to the stimulus with M-L illusion unfolded that the visuo-motor system is able to resist to the illusory stimulus and supported the two-visual-systems hypothesis. Obtained results have demonstrated that the main parameter, which plays the most important role on the precision of visuo-motor behavior, is the uncertainty of perception of the shape and the position of the illusionary stimulus.

K. Jonelis, K. Brazauskas, D. Levišauskas. A System for Dissolved Oxygen Control in Industrial Aeration Tank. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 1, 46 – 52.

The control system is developed for accurate set-point control of dissolved oxygen concentration in industrial aeration tank based on adaptation of PI controller to time-varying dynamics of the controlled process. The controller adaptation algorithm refers to the process state model-based transfer function that follows changes in process dynamics by updating the function parameters with on-line measurements of process variables, and the controller tuning rules developed for typical structure transfer function models.

The control system was investigated via computer simulation of the dissolved oxygen concentration set-point control in an industrial aeration tank under process disturbances and set-point step changes. The control system demonstrates fast adaptation of PI controller parameters and noticeably higher accuracy control compared to that of ordinary fixed gain PI controller.

B.L. Chen, W.-C. Kuo, L.-C. Wuu. A Secure Password-Based Remote User Authentication Scheme without Smart Cards. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 1, 53 – 59.

There are many remote user authentication schemes proposed in literature for preventing unauthorized parties from accessing resources in an insecure environment. Due to inherent tamper-resistance, most of them are based on smart card authentication schemes. Unfortunately, the cost of cards and readers makes these schemes costly. In the real world, common storage devices, such as universal serial bus (USB) thumb drives, portable HDDs, mobile phones, Laptop or Desktop PCs, are widely used, and they are much cheaper or more convenient for storing user authentication information. However, since these devices do not provide tamper-resistance, it is a challenge to design a secure authentication scheme using these kinds of memory devices. In this paper, we will propose a secure password-based remote user authentication and key agreement scheme without using smart cards. According to our analysis, the proposed scheme guarantees mutual authentication and also resists off-line dictionary, replay, forgery, and impersonation attacks. Compared to related scheme, the proposed scheme's computation cost is lower and the total message length is shorter. Therefore, our scheme is suitable even for applications in limited power computing environments.

Y.-F. Chang, W.-L. Tai, C.-Y. Lin. A Verifiable Proxy Signature Scheme Based on Bilinear Pairings with Identity-Based Cryptographic Approaches. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 1, 60 – 68.

Hu and Huang proposed an identity-based proxy signature scheme with bilinear pairings. By this approach, the extra burden of verifying a public key with a certificate can be eliminated, and the length of a digital signature can be 160 bits only. Later, Park et al. pointed out that Hu and Huang's scheme suffers from one serious problem, privacy problem, such that a proxy key is generated by using a designated proxy signer's private key without his agreement. To solve this problem, Park et al. also proposed an improvement. With deep insight into Park et al.'s improvement, two drawbacks are found. First, a designated proxy signer may be fooled. Second, the verification of the proxy key in Park et al.'s scheme will never succeed. To preserve advantages and overcome drawbacks, an enhancement will be proposed in this paper.

C.-T. Li. A More Secure and Efficient Authentication Scheme with Roaming Service and User Anonymity for Mobile Communications. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 1, 69 – 76.

In terms of convenience requirements, mobile communications have become one of the most important roaming services for wireless environments. Especially, how to prevent unauthorized users from illegitimate accesses in mobile communication systems has become an important issue. Password authentication with smart card is one of the mechanisms that were widely used to authenticate the validity of participants between a roaming user, the foreign agent and the home agent of a roaming user. In 2011, Yoon et al. proposed a user friendly authentication scheme with user anonymity for wireless communications and claimed that their scheme is secure and efficient using for battery-powered mobile devices in mobile communication systems. However, we observe that Yoon et al.'s scheme is vulnerable to insider attack, unfairness in session key computation, unable to provide user anonymity and is not easily reparable. In this paper, we offer a more secure and efficient authentication scheme to remedy its security weaknesses and provide reliable roaming accesses in mobile communication environments.

Z. Stanimirović, M. Marić, S. Božović, P. Stanojević. An Efficient Evolutionary Algorithm for Locating Long-Term Care Facilities. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 1, 77 – 89.

This paper deals with a variant of a discrete location problem of establishing long-term care facilities in a given network. The objective is to determine optimal locations for these facilities in order to minimize the maximum number of assigned patients to a single facility. We propose an efficient evolutionary approach (EA) for solving this problem, based on binary encoding, appropriate objective function and standard genetic operators. Unfeasible individuals in the population are corrected to be feasible, while applied EA strategies keep the feasibility of individuals and preserve the diversity of genetic material. The algorithm is benchmarked on a real-life test instance with 33 nodes and the obtained results are compared with the existing ones

from the literature. The EA is additionally tested on new problem instances derived from the standard ORLIB AP hub data set with up to 400 potential locations. For the first time in the literature we report verified optimal solutions for most of the tested problem instances with up to 80 nodes obtained by the standard optimization tool CPLEX. Exhaustive computational experiments show that the EA approach quickly returns all optimal solutions for smaller problem instances, while large-scale instances are solved in a relatively short CPU time. The results obtained on the test problems of practical sizes clearly indicate the potential of the proposed evolutionary-based method for solving this problem and similar discrete location problems.

SANTRAUKOS

P. Treigys, V. Marcinkevičius, A. Kaklauskas. Akies vyzdžio ir rainelės parametrų analizė siekiant atpažinti stresą. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 1, 7 – 14.

Atlikto tyrimo tikslas – automatiškai išskirti akies rainelę ir vyzdį apibūdinančius parametrus iš filmuotos ar filmuojamos medžiagos ir nustatyti, ar tiriamasis patiria stresą. Tyrimų metu buvo analizuojama, kaip laikui bėgant keičiasi biometriniai parametrai tiriamajam sprendžiant įvairius testus. Vaizdinė medžiaga buvo formuojama naudojant stacionarią ant šalmo pritvirtintą NIR kamerą rainelės ir vyzdžio reakcijai fiksuoti. Vėliau buvo atliktas automatinis rainelės ir vyzdžio atpažinimas kadrų sekoje ir šių akies struktūrų aproksimavimas kreivėmis. Buvo daroma prielaida, kad tiriamojo stresą testo metu galima įvertinti pagal tai, kaip laikui bėgant keičiasi akies vyzdžio plotas rainelės ploto atžvilgiu. Kadangi kiekvieną tiriamojo akies vyzdžio dydžio pokytį laikui bėgant apibūdina skirtingų ilgių variacinės eilutės, todėl naudojant euklidinį atstumą jų palyginti negalima. Dėl šios priežasties eilutėms palyginti tyrimuose buvo naudota metrika, paremta periodogramomis. Pastebėta, kad klaidingų atsakymų sukelti stimulai yra linkę grupuotis, priešingai nei teisingų atsakymų sukelti stimulai. Skirtingų tiriamųjų reakcijos į stimulą projekcijos, pritaikius Spencerio slenkamąjį vidurkį, duoda skirtingus rezultatus. Šie faktai rodo, kad suformuotos periodogramos gali būti panaudotos nustatyti ar tiriamasis patiria stresą.

S. Tallapally. Saugumo sustiprinimas paprastu trišaliu PAKE protokolu. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 1, 15 – 22.

Kriptografijoje ir ypač saugioje komunikacijoje svarbi priemonė yra trišalio tapatybės nustatymo rakto pasikeitimo protokolas. Šiame protokole du klientai dalijasi žmogaus įsimenamu slaptažodžiu su patikimu serveriu, per kurį klientai gauna saugaus seanso raktą. Visai neseniai Huang pasiūlė paprastą ir veiksmingą trišalį slaptažodžiu grindžiamą rakto pasikeitimo protokolą. Jis teigė, kad siūlomas protokolas apsaugo nuo įvairių išpuolių. Tačiau Yoonas ir Yoo įrodė, kad internetinės slaptažodžių generavimo atakos Huango protokolas neaptinka. Šiame straipsnyje pateikiama nežinoma rakto pasikeitimo ataka, taikant neaptinkamą slaptažodžių generavimą, nukreipta prieš Huango trišalį PAKE protokolą. Be to, siūlomas alternatyvus protokolas, kuris šią ataką padaro neįmanomą. Siūlomam protokolui reikia tik keturių pranešimų perdavimo ciklų.

V. Štuikys, R. Damaševičius, G. Ziberkas, K. Valinčius. Heterogeninių daugiapakopių meta-programų suvokimo metodas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 1, 23 – 32.

Straipsnyje analizuojamas metodas heterogeninėms daugiapakopėms metaprogramoms suvokti. Metodas jungia Brookso programų pažinimo teorijos principus su apgrąžos inžinerijos principais. Įgalina iš korektiškos metaspecifikacijos išgauti aukštesnio lygmens modelius, t. y. metaparametrų ir metafunkcijų sąryšio grafus, požymių diagramas, programų generavimo procesų algoritmus. Modeliai ir procesai padeda ne tik geriau suvokti metaprogramas ir daugiapakopes metaprogramas, bet ir jas tobulinti. Straipsnyje taip pat pateikiamos kai kurios daugiapakopių programų savybės. Metodui pagrįsti analizuojami sukurtų dvipakopių metaprogramų variantai, ir įvertinamas jų sudėtingumas.

E. Sakalauskas. NP pilnoji daugelio kintamųjų laipsnių kvadratų problema virš $\boldsymbol{Z}_n$. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 1, 33 – 39.

Pateikiama nauja NP pilnoji problema, pavadinta daugelio kintamųjų laipsnių kvadratų problema. Šios problemos formuluotė paremta daugelio kintamųjų laipsninės lygčių sistemos sprendimu, kai nežinomieji kintamieji yra lygties konstantų laipsnių rodikliuose. Kiekvieną lygtį sudaro konstantų, apibrėžtų virš monoido $\boldsymbol{Z}_n$ sandaugos, o jų laipsnių rodikliai susideda iš bitiesinių nežinomųjų kintamųjų sandaugų (bitiesinių monomų) arba iš atskirų kintamųjų (tiesinių monomų). NP pilnumo įrodymas paremtas polinominio laiko redukcija iš žinomos NP pilnosios problemos, t. y. daugelio kintamųjų kvadratinės problemos, į daugelio kintamųjų laipsnių kvadratų problemą. Daugelio kintamųjų laipsnių kvadratų problema yra susieta su matricinio laipsnio problema, kuri buvo naudojama simetrinio šifravimo ir raktų pasikeitimo protokoluose.

V. Laurutis, I. Indrijauskienė, R. Zemblys S. Niauronis. Miulerio ir Lajerio iliuzijų įtaka pirminių sakadų ir tolygių sekamųjų akių judesių tikslumui. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 1, 40 – 45.

Šio tyrimo tikslas - patikrinti hipotezę, kad suvokimui ir veiksmams skirta vizualinė informacija yra apdorojama atskirai. Kadangi vizualinės iliuzijos yra suvokiamos netiksliai, o dalis pateiktos informacijos prarandama, buvo nuspręsta nustatyti Miulerio ir Lajerio iliuzijos įtaką sakadinių ir tolygių sekamųjų akių judesių tikslumui ir palyginti gautus rezultatus su rezultatais, gautais subjektyviai vertinant šios iliuzijos veikiamą objektą. Eksperimentinių tyrimų metu buvo nustatyta, kad Miulerio ir Lajerio iliuzija daugiausia įtakos turėjo pirminėms akių sakadoms, kurios buvo atliktos refleksiškai. Tokių sakadų paklaidos iliuzijai su sparneliais į vidų buvo 4 %, o iliuzijai su sparneliais į lauką – 3,6 %. Pirminių sakadų, atliktų savo noru, paklaidos atitinkamai buvo 0,25 % ir 0,1 %. Pilnų sakadų paklaidos (0,14 % ir 0,02 %) bei sekamųjų akių judesių paklaidos (0,11 % ir 0,05 %) buvo nereikšmingos. Tačiau eksperimentai, atlikti subjektyviai vertinant Miulerio ir Lajerio iliuzijos veikiamą

objektą, parodė, kad jos įtaka yra gerokai didesnė – atitinkamai 14 % ir 10 %. Tyrimo rezultatai leidžia teigti, kad okulomotorinė sistema yra atspari iliuzijos poveikiui, o kartu patvirtino dviejų regos sistemų hipotezę. Taip pat padaryta išvada, jog svarbiausias parametras, turintis įtakos okulomotorinės sistemos elgsenai, yra iliuzijos veikiamų objektų formos ir padėties neapibrėžtumas.

K. Jonelis, K. Brazauskas, D. Levišauskas. Ištirpusio deguonies koncentracijos pramoniniame aerotanke valdymo sistema. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 1, 46 – 52.

Sukurta valdymo sistema, ištirpusio deguonies koncentracijai palaikyti pramoniniame aerotanke, paremta PI reguliatoriaus prisitaikymu prie kintamų sąlygų. Reguliatoriaus prisitaikymo algoritmas remiasi iš proceso būsenos modelio gaunama perdavimo funkcija, kuri yra atnaujinama atliekant būsenos kintamųjų matavimus ir geba sekti proceso dinamikos kitimą. Reguliatoriaus parametrai perskaičiuojami kiekviename valdymo diskretizavimo žingsnyje, taikant reguliatoriaus derinimo taisykles, sukurtas tipinės struktūros perdavimo funkcijos modeliams. Valdymo sistemos veikimo modeliavimas, veikiant procesą trikdantiems poveikiams ir šuoliniams nuostato pokyčiams, rodo greitą PI reguliatoriaus parametrų prisitaikymą ir pastebimai didesnį reguliavimo tikslumą, palyginti su pastoviai suderintu PI reguliatoriumi.

B. L. Chen, W.-C. Kuo, L.-C. Wuu. Saugi slaptažodžiu pagrįsta nutolusio vartotojo tapatybės nustatymo schema be išmaniųjų kortelių. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 1, 53 – 59.

Literatūroje pateikiama daug nutolusio vartotojo tapatybės nustatymo schemų, kurios padeda užkirsti kelią leidimo neturintiems asmenims prieiti prie išteklių nesaugiuose tinkluose. Dėl būdingo atsparumo klastojimui dauguma jų yra paremtos išmaniosios kortelės tapatybės nustatymo schemomis. Deja, išlaidos kortelėms ir skaitytuvams įsigyti didina šių schemų kainą. Įprasti informacijos saugojimo įrenginiai, pavyzdžiui, universaliosios nuosekliosios magistralės (USB) kaupikliai, nešiojamieji HDD, mobilieji telefonai, nešiojamieji arba asmeniniai kompiuteriai, yra plačiai naudojami ir gerokai pigesni arba patogesni vartotojo tapatybės nustatymo informacijai saugoti. Tačiau, kadangi šie įrenginiai nepadidina atsparumo klastojimui, juos naudojant sunku sukurti saugią tapatybės nustatymo schemą. Šiame straipsnyje siūloma saugi slaptažodžiu grindžiama nutolusio vartotojo tapatybės nustatymo schema be išmaniųjų kortelių. Mūsų atliktos analizės duomenimis, siūlomoji schema užtikrina abipusį tapatybės nustatymą ir taip pat yra atspari kartojimo, klastojimo ir apsimetimo atakoms. Palyginti su panašia schema, pasiūlytosios schemos skaičiavimo išlaidos yra mažesnės ir bendra žinutė trumpesnė. Todėl ši schema tinka net toms programoms, kurios veikia ribotų pajėgumų skaičiavimo terpėse.

Y.-F. Chang, W.-L. Tai, C.-Y. Lin. Įgaliotojo serverio tapatumo nustatymo schema, paremta asimetrinėmis poromis su kriptografiniu parašu. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 1, 60 – 68.

Hu ir Huangas pasiūlė tapatybe grindžiamą įgaliotojo serverio parašo schemą su asimetrinėmis poromis. Taikant šį metodą galima atsisakyti papildomo viešojo rakto su sertifikatu patikrinimo, todėl skaitmeninio parašo ilgis gali būti tik 160 bitų. Vėliau Parkas ir kt. nurodė, kad Hu ir Huango schemose yra viena nemaža privatumo problema, nes įgaliotojo serverio raktas generuojamas naudojant paskirto įgaliotojo serverio pasirašančiojo asmens privatų raktą be jo sutikimo. Parkas ir kt. pasiūlė sprendimą, kaip šią problemą pašalinti. Atlikus Parko ir kt. pasiūlymo analizę, rasti du trūkumai. Pirma, paskirtas įgaliotojo serverio pasirašantysis asmuo gali būti apgautas. Antra, pagal Parko ir kt. schemą įgaliotojo serverio rakto patvirtinti niekada nepavyks. Siekiant išlaikyti schemos privalumus ir pašalinti trūkumus, šiame straipsnyje pateikiamas schemos patobulinimas.

C.-T. Li. Saugesnė ir veiksmingesnė tapatumo nustatymo schema mobiliosioms komunikacijoms, teikiančioms tarptinklines paslaugas ir užtikrinančioms vartotojo anonimiškumą. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 1, 69 – 76.

Dėl patogumo, mobiliosios komunikacijos yra viena iš svarbiausių bevielių tinklų tarptinklinių paslaugų. Ypač svarbu tapo užkirsti kelią neteisėtai leidimo neturinčių vartotojų prieigai mobiliųjų ryšių sistemose. Slaptažodžio tapatumo nustatymas, naudojant išmaniąją kortelę, yra vienas iš būdų, kurie buvo plačiai taikomi vartotojo registravimo sistemos, tinklo vartotojų registro ir vartotojo namų agento tapatumui nustatyti. 2011 m. Yoonas ir kiti pasiūlė vartotojui draugišką tapatumo nustatymo schemą, suteikiančią bevielių ryšių vartotojui anonimiškumą, ir teigė, kad jų schema yra saugi ir efektyvi, naudojant baterijomis maitinamus mobiliuosius prietaisus mobiliojo ryšio sistemose. Tačiau pastebėjome, kad Yoono ir kt. schemą gali pažeisti vidinio tinklo vartotojo ataka, seanso rakto skaičiavimo klaidos, nesugebėjimas suteikti vartotojui anonimiškumo. Ji nėra lengvai pataisoma. Šiame straipsnyje siūloma saugesnė efektyvi tapatumo nustatymo schema, leidžianti pašalinti saugumo trūkumus ir suteikti vartotojams patikimą tarptinklinių paslaugų prieinamumą mobiliojo ryšio tinkluose.

Z. Stanimirović, M. Demiri, S. Božović, P. Stanojević. Veiksmingas evoliucinis ilgalaikių priežiūros paslaugų paieškos algoritmas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 1, 77 – 89.

Šiame straipsnyje nagrinėjamas diskrečiojo nustatymo problemos variantas, įgyvendinant ilgalaikės priežiūros infrastruktūrą tam tikrame tinkle. Darbo tikslas nustatyti šioms infrastruktūroms optimalias vietas, kad būtų sumažintas didžiausias vienai infrastruktūrai paskiriamų vartotojų skaičius. Pateikiamas efektyvus evoliucinis metodas (EM) šiai problemai spręsti remiantis dvejetainiu kodavimu, atitinkamomis objektinėmis funkcijomis ir standartiniais genetiniais operatoriais. Negalimi populiacijos individai paverčiami į galimus, nes taikomos EM strategijos išlaiko individų tinkamumą ir išsaugo genetinių duomenų įvairovę. Algoritmas yra testuojamas realiomis sąlygomis, naudojant 33 tinklo mazgus, ir gauti rezultatai yra lyginami su pateikiamais literatūroje. EM yra papildomai testuota naujais probleminiais atvejais iš standartinio ORLIB AP

duomenų rinkinio su iki 400 galimų vietų. Pirmą kartą pateikiami daugumos testuotų atvejų patikrinti optimalūs sprendimai, gauti esant iki 80 mazgų ir naudojant standartinį optimizavimo įrankį CPLEX. Išsamūs skaičiavimo eksperimentai rodo, kad naudojant EM greitai surandami visi optimalūs mažesnių problemų sprendimai, o didelės problemos išsprendžiamos per palyginti trumpą CPU darbo laiką. Testuojant praktinio dydžio problemas gauti rezultatai aiškiai rodo, kad pasiūlytu evoliuciniu metodu galima spręsti šią ir panašias diskrečiojo nustatymo problemas.