SUMMARIES

L. Savulioniene, L. Sakalauskas. A Stochastic Algorithm of Frequent Set Search for Mining Association Rules. *Information Technology and Control, Kaunas, Technologija,* 2014, Vol. 43, No. 2, 121–132.

Data mining is discovery of unknown, nontrivial, practically useful and easy to interpret knowledge in chaotic data. The information, found by application of data mining techniques, is unknown in advance. Knowledge is described by relationships of new features that distinguish one attribute value from other set attributes. The new knowledge set must be applied to new information with some degree of reliability. Current algorithms for finding association rules require several passes over the analysed database. The paper presents a stochastic algorithm for mining association rules in large data sets. Our stochastic algorithm reduces the database activity considerably, because the database is analysed only once. The algorithm allows us to measure two significant criteria, i.e. time and accuracy. We analyse a large database of transactions. Each transaction consists of items purchased by a customer in a visit. The algorithm yields conclusions about association rules using the analysis of randomly selected subsequences. Our experiments show that the proposed algorithm can find association rules efficiently in only one database scan.

H. Pranevicius, M. Pranevicius, O. Pranevicius, M. Snipas, N. Paulauskas, F. Bukauskas. Continuous Time Markov Chain Models of Voltage Gating of Gap Junction Channels. *Information Technology and Control, Kaunas, Technologija,* 2014, Vol. 43, No. 2, 133–142.

The major goal of this study was to create a continuous time Markov chain (CTMC) models of voltage gating of gap junction (GJ) channels formed of connexin protein. This goal was achieved by using the Piece Linear Aggregate (PLA) formalism to describe the function of GJs and transforming PLA into Markov process. Infinitesimal generator of CTMC was used to automate construction of Markov chain model from description of the system using PLA formalism. Developed Markov chain models were used to simulate gap junctional conductance dependence on transjunctional voltage. The proposed method was implemented to create models of voltage gating of GJ channels containing 4 and 12 gates. CTMC modeling results were compared with the results obtained using a discrete time Markov chain (DTMC) model. It was shown that CTMC modeling requires less CPU time than an analogous DTMC model.

M. S. Farash, M. A. Attari. An Enhanced and Secure Three-Party Password-based Authenticated Key Exchange Protocol without Using Server's Public-Keys and Symmetric Cryptosystems. *Information Technology and Control, Kaunas, Technologija*, 2014, Vol. 43, No. 2, 143–150.

Password-based authenticated key exchange protocol is a type of authenticated key exchange protocols which enables two or more communication entities, who only share weak, low-entropy and easily memorable passwords, to authenticate each other and establish a high-entropy secret session key. In 2012, Tallapally proposed an enhanced three-party password-based authenticated key exchange protocol to overcome the weaknesses of Huang's scheme. However, in this paper, we indicate that the Tallapally's scheme not only is still vulnerable to undetectable online password guessing attack, but also is insecure against off-line password guessing attack. Therefore, we propose a more secure and efficient scheme to overcome the security flaws.

W.-C. Kuo, H.-J. Wei, J.-C. Cheng. Enhanced Secure Authentication Scheme with Anonymity for Roaming in Mobility Networks. *Information Technology and Control, Kaunas, Technologija,* 2014, Vol. 43, No. 2, 151–156.

In 2012, Kim and Kwak proposed an anonymous authentication scheme for mobility networks which claimed to improve upon the weakness of replay attack and man-in-the-middle attack in Mun *et al.*'s scheme. However, their proposed scheme is still vulnerable to replay and DoS attacks. A serious problem in their scheme is that FA cannot get the session key K_{MF}. In order to improve these shortcomings, we propose an enhanced secure authentication scheme with anonymity for roaming in mobility networks. The security analysis of our scheme demonstrates maintaining all of the security in Mun *et al.*'s scheme, but also efficiently improves upon the weaknesses in Kim-Kwak scheme.

P. Teppa-Garran, G. Garcia. ADRC Tuning Employing the LQR Approach for Decoupling Uncertain MIMO Systems. *Information Technology and Control, Kaunas, Technologija,* 2014, Vol. 43, No. 2, 157–165.

Active Disturbance Rejection Control (ADRC) tuning employing the LQR approach is applied for decoupling uncertain MIMO systems. This is done by considering all the coupling and interference interactions between the channels of the system as disturbances, using an Extended State Observer (ESO) to estimate them in real time and then canceling its effect employing the estimate as part of the control signal. The ADRC tuning is essentially a pole-placement technique and the desired performance is indirectly achieved through the location of the closed-loop poles. However, the final choice of these poles becomes a trial-and-error strategy. In contrast with pole-placement, in the LQR method, the desired performance objectives are directly and globally addressed by minimizing a quadratic function of the state and control input.

U. E. Kocamaz, Y. Uyaroğlu. Non-Identical Synchronization, Anti-Synchronization and Control of Single-Machine Infinite-Bus Power System via Active Control. *Information Technology and Control, Kaunas, Technologija,* 2014, Vol. 43, No. 2, 166–174.

Since the idea of synchronizing two identical chaotic systems under different initial conditions was first introduced by Pecora and Carroll, the synchronization of chaotic systems has attracted much attention, and the synchronization of non-identical chaotic systems has also been investigated. Single-Machine Infinite-Bus (SMIB) power system has nonlinear behaviour. On account of avoiding undesirable behaviours in power systems such as voltage collapse, the synchronization and control of SMIB power system have considerable importance. This paper presents chaos synchronization and anti-synchronization of SMIB power system to Duffing oscillator by means of active control method. The sum of synchronization and anti-synchronization signals converge asymptotically to zero and achieve the control of SMIB power system. Numerical simulations are used to demonstrate the validity of proposed active control method on the non-identical synchronization, anti-synchronization and control of SMIB power system.

Y. Wang, P. Zhou, Q. Wang, D. Duan. Reliable Robust Sampled-Data H_∞ Output Tracking Control with Application to Flight Control. *Information Technology and Control, Kaunas, Technologija*, 2014, Vol. 43, No. 2, 175–182.

This paper is concerned with the problem of robust H_∞ output tracking control for uncertain sampled-data systems with probabilistic actuator failures. By assuming that each actuator fault takes values randomly in a finite set, a new actuator-failure-mode is proposed. Lyapunov-Krasovskii functional combined with the input delay approach as well as the free-weighting matrix approach are employed to establish the H_∞ performance, and the controller design is cast into a convex optimization problem with linear matrix inequality (LMI) constraints. The designed reliable controller can guarantee that the output of the closed-loop sampled-data system tracks the reference signal without steady-state error. An airship model is considered in this paper and its simulation results are given.

C.-P. Chu, C.-Y. Yeh, S.-H. Hwang. An Efficient Search Strategy for ACELP Algebraic Codebook by Means of Reduced Candidate Mechanism and Iteration-Free Pulse Replacement. *Information Technology and Control, Kaunas, Technologija*, 2014, Vol. 43, No. 2, 183–187.

This work aims to present a combined version of reduced candidate mechanism (RCM) and iteration-free pulse replacement (IFPR) as a novel and efficient way to enhance the performance of algebraic codebook search in an algebraic code-excited linear-prediction (ACELP) speech coder. As the first step, individual pulse contribution in each track is given by RCM, and the number N of candidate pulses is then specified. Subsequently, the replacement of a pulse is performed through the search over the sorted top N pulses by IFPR, and those of 2 to 4 pulses are carried out by a standard IFPR. Implemented on a G.729A speech codec, this proposal requires as few as 24 searches, a search load tantamount to 7.5% of G.729A, 37.5% of the global pulse replacement method (iteration=2), 50% of IFPR, but still provides a comparable speech quality in any case. The aim of significant search performance improvement is hence achieved in this work.

A. Azarfar, H. T. Shandiz, M. Shafiee. Adaptive Control for Nonlinear Singular Systems. *Information Technology and Control, Kaunas, Technologija*, 2014, Vol. 43, No. 2, 188–198.

Nonlinear singular systems present a general mathematical framework for the modeling and controlling of complicated systems, however the complex nature of this type of systems causes many difficulties in control strategy. In this paper, a model reference control approach is addressed for nonlinear affine singular systems. First, a basic control system is proposed based on the Lyapunov stability theorem so that nonlinear singular system can asymptotically track the desired linear reference model. After that, in the second design, it has been considered that systems' parameters are unknown and two adaptive approaches are investigated. For better illustration, simulation has been done and the results show the tracking performance for both presented control systems.

N. Tiwari, S. Padhye, D. He. Provably Secure Proxy Multi-Signature Scheme Based on ECC. *Information Technology and Control, Kaunas, Technologija*, 2014, Vol. 43, No. 2, 199–204.

The elliptic curve cryptosystem (ECC) achieves the security level equivalent to that of digital signature algorithm (DSA), but has a lower computational cost and a smaller key size than the DSA. Till now so many proxy multi-signature schemes based on ECC without pairings have been proposed. To the best of our knowledge, none of them are provable secure. Having motivated, we first define a formal security model and then propose a provable secure proxy multi-signature scheme based on ECC without pairings. Our proposed scheme can play a crucial role in application to distributed systems, grid computing, mobile agent environment etc.

SANTRAUKOS

L. Savulioniene, L. Sakalauskas. Tikimybinis susietumo taisyklių paieškos algoritmas. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2014, T. 43, Nr. 2, 121-132.

Duomenų tyryba – tai nežinomų, netrivialių, praktiškai naudingų ir lengvai interpretuojamų žinių aptikimas chaotiškuose duomenyse. Informacija, kuri randama taikant duomenų tyrybos metodus, iš anksto nėra žinoma. Žinias aprašo nauji savybių ryšiai, nusakantys vienų požymių reikšmes pagal kitus nustatytus požymius. Nustatytos naujos žinios turi būti taikomos ir naujai tam tikro patikimumo informacijai. Daugelis susietumo taisyklių paieškos algoritmų duomenų bazę skenuoja keletą kartų, o tai lemia dideles laiko sąnaudas. Straipsnyje pateikiamas tikimybinis susietumo taisyklių paieškos algoritmas. Pasiūlytas algoritmas duomenų bazę skenuoja vieną kartą, o tai lemia mažesnes laiko sąnaudas. Šis algoritmas leidžia suderinti du svarbius kriterijus: laiką ir tikslumą. Eksperimente naudota pirkimų transakcijų duomenų bazė. Pasiūlytas algoritmas efektyviai iš nustatytų dažnų posekių formuoja susietumo taisykles.

H. Pranevicius, M. Pranevicius, O. Pranevicius, M. Snipas, N. Paulauskas, F. Bukauskas. Ląstelių plyšinių jungčių kanalų laidumo modeliavimas tolydaus laiko Markovo grandinėmis. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2014, T. 43, Nr. 2, 133-142.

Straipsnio tikslas - sukurti tolydaus laiko Markovo grandinių (TLMG) modelius ląstelių plyšinių jungčių kanalų laidumui skaičiuoti. Plyšinėms jungtims aprašyti ir modeliui transformuoti į Markovo procesą buvo panaudotas atkarpomis tiesinių agregatų formalizmas. Taikant šią metodiką, Markovo grandinės perėjimo intensyvumų matrica sudaroma automatiškai iš formaliosios agregatinės specifikacijos. Sukurti Markovo modeliai buvo panaudoti plyšinių jungčių kanalų laidumo priklausomybei nuo įtampos apskaičiuoti. Straipsnyje pristatoma metodika buvo pritaikyta plyšinėms jungtims, turinčioms 4 kanalus ir 12 kanalų. TLMG modeliavimo rezultatai buvo palyginti su analogiškais rezultatais, gautais taikant diskretaus laiko Markovo modelius (DLMG). Rezultatai parodė, kad TLMG modeliavimo laiko sąnaudos yra gerokai mažesnės negu naudojant DLMG modelius.

M. S. Farash, M. A. Attari. Išplėstas ir saugus trišalis slaptažodžiu grindžiamas raktų apsikeitimo protokolas, nenaudojantis serverio viešųjų raktų ir simetrinių kriptosistemų. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2014, T. 43, Nr. 2, 143-150.

Slaptažodžiu grindžiamas autentifikuotas raktų apsikeitimo protokolas yra vienas iš autentifikuotų raktų apsikeitimo protokolų, leidžiančių dviem ar daugiau vienetams, turintiems bendrus silpnus, mažos entropijos ir lengvai įsimenamus slaptažodžius, autentifikuoti vienam kitą ir sukurti aukštos entropijos uždaros sesijos raktą. Siekiant pašalinti *Huang* schemos trūkumus, 2012 m. Tallapally pasiūlė išplėstą trišalį slaptažodžiu grindžiamą raktų apsikeitimo protokolą. Straipsnyje pateikiama, kad Tallapally schema yra nepajėgi apsisaugoti nuo sunkiai aptinkamų tiesioginių ir netiesioginių atakų, per kurias siekiama atspėti slaptažodį. Dėl šios priežasties siūloma saugesnė ir efektyvesnė schema, kuri pašalintų saugumo spragas.

W.-C. Kuo, H.-J. Wei, J.-C. Cheng. Išplėsta saugi anoniminė atpažinimo schema tarptinkliniam ryšiui mobiliuosiuose tinkluose. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2014, T. 43, Nr. 2, 151-156.

2012 m. Kim ir Kwak pasiūlė mobiliesiems tinklams skirtą anoniminę atpažinimo schemą, kuri pagerina pakartojimo ir „tarpininko“ (angl. MITM) atakų trūkumus, nurodytus Mun ir kt. schemoje. Tačiau jų siūloma schema vis dar nėra pajėgi apsisaugoti nuo pakartojimo ir atsisakymo prižiūrėti atakas. Rimta jų schemos problema yra tai, kad negalima gauti seanso rakto K_{MF}. Norint pagerinti šiuos trūkumus, siūloma išplėsta saugi anoniminė atpažinimo schema. Schemos saugumo analizė rodo, kad ne tik užtikrinamas Mun ir kt. schemos saugumas, bet ir efektyviai pagerinami Kim ir Kwan schemos trūkumai.

P. Teppa-Garran, G. Garcia. ADRC reguliavimas taikant tiesinio kvadratinio būsenos reguliatoriaus metodą neapibrėžtų MIMO sistemų ryšiui nutraukti. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2014, T. 43, Nr. 2, 157-165.

ADRC reguliavimas, taikant tiesinio kvadratinio būsenos reguliatoriaus (LQR) metodą, nutraukia neapibrėžtus MIMO sistemų ryšius. Tai atliekama laikant sistemos kanalų jungčių ir trikdžių sąveikas pažeidimais. Naudojamas išplėstinis būsenos stebėtojas (ESO), kad jie būtų įvertinti realiu laiku, ir panaikinamas jo poveikis pritaikius skaičiavimą kaip valdymo signalo dalį. ADRC reguliavimas iš esmės yra vienalaikės būsenos grįžtamojo ryšio būdas. Norimas efektyvumas netiesiogiai pasiekiamas naudojant uždarojo ciklo būsenų vietą. Nepaisant to, galutinis šių būsenų pasirinkimas tampa bandymų ir klaidų strategija. Priešingai vienalaikės būsenos grįžtamojo ryšio metodui, taikant LRQ metodą, norimo pasiekti efektyvumo tikslai yra tiesiogiai ir bendrai detaliai nagrinėjami iki minimumo norint sumažinti būsenos ir valdymo pradinių duomenų kvadratinę funkciją.

U. E. Kocamaz, Y. Uyaroğlu. Vieno įrenginio begalinės magistralės (SMIB) sistemoje maitinimo sistemos neidentiška sinchronizacija, antisinchronizacija ir aktyvusis valdymas. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2014, T. 43, Nr. 2, 166-174.

Nuo to laiko, kai Pecora ir Carroll pasiūlė mintį sinchronizuoti dvi vienodas chaotiškas sistemas skirtingomis pradinėmis sąlygomis, chaotiškų sistemų suvienodinimui buvo skiriama daug dėmesio. Tačiau buvo nagrinėjamas ir neidentiškų chaotiškų sistemų sinchronizavimas. SMIB maitinimo sistema pasižymi netiesine elgsena. Norint išvengti elektros energijos sistemų veikimo klaidų, tokių kaip įtampos dingimas, labai reikšminga SMIB maitinimo sistemos sinchronizacija ir kontrolė. Straipsnyje nagrinėjama dinaminių sistemų sinchronizacija ir SMIB elektros energijos sistemų antisinchronizacija su Duffingo osciliatoriumi, taikant aktyvaus valdymo metodą. Sinchronizavimo ir antisinchronizavimo signalų suma nukreipta į asimptotę, lygią nuliui, ir perima SMIB elektros energijos sistemų valdymą. Skaitmeninis modeliavimas naudojamas tam, kad būtų parodytas siūlomo aktyvaus valdymo metodo, taikomo SMIB elektros energijos sistemoms nevienodai sinchronizuoti, antisinchronizuoti ir valdyti, svarumas.

Y. Wang, P. Zhou, Q. Wang, D. Duan. Patikimų veiksmingų atrinktųjų išvesties duomenų H_∞ stebėjimo kontrolė, pritaikant ją skrydžio kontrolei. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2014, T. 43, Nr. 2, 175-182.

Straipsnyje aptariama veiksmingo H_∞ išvedimo stebėjimo kontrolės, taikomos neapibrėžtoms atrinktųjų duomenų sistemoms, pasižyminčioms tikimybiniais pavaros mechanizmo gedimais, problema. Darant prielaidą, kad kiekvieno pavaros mechanizmo gedimo vertės baigtiniame rinkinyje yra atsitiktinės, pasiūlomas naujas pavaros mechanizmo gedimo režimas. Lyapunovo ir Krasovskii funkcinis metodas ir įvesties duomenų bei laisvos apkrovos matricos metodai yra taikomi H_∞ veikti, o valdiklio modelis tampa iškiliosios funkcijos optimizavimo problema, turinčia tiesinių matricų nelygybių (LMI) ryšių. Sumodeliuotas patikimas valdiklis gali užtikrinti, kad uždarojo ciklo atrinktųjų duomenų sistemos išvesties duomenys suseka standartinį signalą be nuolatinės būsenos klaidos. Straipsnyje aptariamas orlaivio modelis ir pateikiami jo modeliavimo rezultatai.

C.-P. Chu, C.-Y. Yeh, S.-H. Hwang. Efektyvi paieškos strategija algoritmo ACELP algebriniam kodų vykdymo protokolui, naudojant redukuoto kandidato mechanizmą (RCM) ir nuo iteracijos nepriklausantį impulso pakeitimą (IFPR). *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2014, T. 43, Nr. 2, 183-187.

Straipsnyje aptariamas RCM ir IFPR junginys kaip nauja ir efektyvi priemonė, norint pagerinti ACELP kalbos koderio algebrinį kodų vykdymo protokolą. Visų pirma RCM parodo individualų impulso įnašą kiekviename takelyje, tada nurodomas galimų impulsų N skaičius. Paskui impulsas yra pakeičiamas per IFPR ieškant išrūšiuotų aukščiausių N impulsų. Nuo 2 iki 4 impulsų apdoroja IFPR. Pritaikius G.729A kalbos kodekus, šiam siūlymui įgyvendinti reikia 24 paieškų. Paieškos apkrovos tolygios iki 7,5 proc. G.729A, 37,5 proc. pritaikomas bendrojo impulso pakeitimo metodas (iteracija=2), 50 proc. – IFPR. Tačiau gaunama kalbos kokybė bet kuriuo atveju yra panaši. Taigi straipsnio tikslas – reikšmingai pagerinti paieškos įvykdymą – yra pasiekiamas.

A. Azarfar, H. T. Shandiz, M. Shafiee. Netiesinių algebrinių-diferencialinių sistemų adaptyvusis valdymas. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2014, T. 43, Nr. 2, 188-198.

Netiesinės algebrinės-diferencialinės sistemos sudaro bendrąjį matematinį modeliavimo ir sudėtingų sistemų valdymo pagrindą, tačiau dėl sudėtingo šio tipo sistemų pobūdžio kyla daug valdymo strategijos sunkumų. Straipsnyje aptariamas netiesinėms sutampančioms algebrinėms-diferencialinėms sistemoms taikomas modelio informacijos valdymo būdas. Visų pirma pagrindinė valdymo sistema yra grindžiama Liapunovo teorema, kad netiesinė algebrinė-diferencialinė sistema gali asimptotiškai stebėti siektiną tiesinį informacijos modelį. Paskui antrajame modelyje svarstoma, kad sistemų parametrai yra nežinomi, ir tiriami du adaptyvieji metodai. Kad būtų aiškiau, buvo atliktas modeliavimas, kurio rezultatai rodo stebimą abiejų pristatytų valdymo sistemų našumą.

N. Tiwari, S. Padhye, D. He. Daugybinio parašo, grindžiamo elipsinės kreivės kriptosistema (ECC), schema, kurios saugumą galima įrodyti. *Informacinės technologijos ir valdymas, Kaunas, Technologija*, 2014, T. 43, Nr. 2, 199-204.

Elipsinės kreivės kriptosistemos (ECC) ir skaitmeninio parašo algoritmo (DSA) saugumo lygiai yra vienodi, tačiau ECC pasižymi mažesnėmis skaičiuojamosiomis sąnaudomis ir mažesniu nei DSA raktu. Iki šiol buvo pasiūlyta daugybė įgaliotojo serverio daugybinio parašo schemų, pagrįstų nesugrupuotų į poras ECC. Žinoma, kad nė vienos iš jų saugumas nėra absoliutus. Straipsnyje visų pirma motyvuotai pristatomas formalusis saugumo modelis ir tuomet pasiūloma kiek įmanoma saugi įgaliotojo asmens daugybinio parašo schema, pagrįsta ne iš porų sudaryta ECC. Siūloma schema gali būti itin svarbi naudojant paskirstytąsias sistemas, mobiliojo agento aplinką, atliekant tinklo skaičiavimus ir t. t.