



9th International Conference on

CONTROL AND OPTIMIZATION

WITH INDUSTRIAL APPLICATIONS

Editors

Aliev Fikret (Azerbaijan)

Akdemir Ahmet Ocak (Türkiye)

Deputy Editors-in-Chief

Safarova Nargiz (Azerbaijan)

Dokuyucu Mustafa Ali (Türkiye)

ISBN 978 - 625 - 97879 - 3 - 0



MINISTRY OF DIGITAL DEVELOPMENT
AND TRANSPORT
OF THE REPUBLIC OF AZERBAIJAN



Uluslararası Kalkınma Toplum ve Düşünce Derneği



PROCEEDINGS

of the

9th International Conference on

CONTROL AND OPTIMIZATION

WITH INDUSTRIAL

APPLICATIONS

27-29 August, 2024
Istanbul, Türkiye

CONTENTS

Metaheuristic Algorithms and their Applications to Fuzzy Control, Fuzzy Modeling and Learning-Based Control	<i>R.-E. Precup</i>	1
Adaptive Optimization of Industrial Network Flow Problems in Gas and District Heating Networks	<i>H. Danschel, V. Mehrmann, M. Roland, M. Schmidt</i>	4
Compartmental Systems: From SIDARTHE to Max-Entropic Markov Chains	<i>P. Colaneri</i>	7
Artificial Intelligence-Driven Design: Reasoning, Learning, and Control	<i>T. Kumbasar</i>	14
Piecewise Linear Optimization Model for Supervised Classification Problems in Imbalanced Data	<i>A. Bagirov, Md Moniruzzaman, I. Gondal</i>	18
Decision Support System Related to Risk Management in the Medical Device Development	<i>M. Kirişçi</i>	30
Some New Fractional Integral for η -Convex Functions	<i>B. Çelik, E. Set, A.O. Akdemir</i>	36
Maclaurin-Type Inequalities for Functions of Bounded Variation via Conformable Fractional Integrals	<i>E. Set, H. Budak, N. Uzun</i>	40
Dances in a Simple One-Dimensional Crystal Lattice	<i>V. Hacıyeva</i>	44
The Joukowski Function: Advancements in Aerodynamics and Mathematical Modeling	<i>Sh. Guliyev, M. Eminov</i>	49
Methodology and Algorithm for Calculating the Modes of Power Systems with Renewable Energy Sources with Phase Coordinates	<i>F. Ibrahimov, H.B. Guliyev, N. Huseynov</i>	55

Cointegration Relationship between Income, Expenditure Investment and GDP: Case Study Azerbaijan	<i>U. Karimova, L. Rustamova, H. Efendiyeva</i>	60
ARC Overvoltage Regression Model	<i>N. Orujov, H. Guliyev, S. Alimammadova</i>	64
Construction of a Gas Drying Model Based on Mining Studies	<i>I. Sardarova</i>	68
Mathematical Modeling of Spatial Structure of the Livagen Molecule	<i>L. Agayeva, L. Ismailova, N. Akhmedov</i>	72
The Inverse Problem of Displacement of the 6R Manipulator with a Sequential Structure by Means of Double Quaternions	<i>F. Mammadov, B. Ahmedov</i>	76
Hypothesis About the Vortex Effect of Ranque and Initial Considerations for its Mathematical Modeling	<i>A. Akhundov, E. Akhundova</i>	81
On Complex Rays and Caustics	<i>E. Hasanoğlu</i>	85
Technique for Fuzzy Multi-Criteria Evaluation of Clinics' Activity Based on Information in Medical Social Media Resources	<i>M. Mammadova, Z. Jabrayilova, N. Shikhaliyeva</i>	89
The Atmosphere Parameters of the Star <i>HD148743(A7Ib)</i>	<i>Z. Samedov, A. Hasanova, U. Rustem, A. Khalilov</i>	93
Solution of the Problem of Structural Conversion of a Finite Automata into the Appropriate Type of Petri Net	<i>Sh. Huseynzade, K. Aliyeva</i>	98
Computer Modeling of $C_{15}H_{11}Cl_2N_3O_2$ Molecule Using Density Functional Theory Method	<i>S. Demukhamedova, I. Aliyeva, U. Askerova, A. Maharramov, N. Shikhaliyev</i>	102
Prognosing Hepatocellular Carcinoma Based on a National Database Using Machine Learning Algorithms	<i>M. Mammadova, N. Bayramov, Z. Jabrayilova, L. Garayeva, M. Huseynova</i>	108
Modeling the Process of Gas Condensate Development Reserves in Accounting for the Thermodynamic Nonequilibrium	<i>M. Khalilov</i>	114
Fuzzy Control Algorithm for One Class of Technological Complexes	<i>I. Sardarova, T. Maharramova, E. Melikov</i>	119

On Behavior of Solutions to Quasilinear Elliptic Equations in Unbounded Domains	<i>S. Huseynov, S. Aliev, J. Guliyev</i>	123
On Iterative Processes and Spectral Problems of Generalized Difference Operator-Matrices	<i>A. Akhmedov</i>	127
Returned Sequences with Applications	<i>A. Akhmedov, S. Baghirov</i>	131
Modeling of Ultra-High Voltage Power Transmission Lines by Equations in Hyperbolic form with Distributed Nonlinear Conductivity	<i>A. Balametov, T. Isayeva</i>	135
An Innovative Approximate Solution Method of the Integer Knapsack Problem	<i>K. Mammadov, R. Niyazova</i>	139
On the Solution of One Problem for a Fourth Order Equation by the Finite Difference Method	<i>Z. Khankishiyev</i>	143
Derivation of the Precise Flow Rate Equation of a Hydrodynamic Incomplete Operation Well According to the Degree of Formation Opening	<i>G. Mammadova</i>	148
Fuzzy Computer Modeling of Liver Disease Diagnosis Based on Biochemical Blood Analysis	<i>G. Abbasova, Sh. Huseynzade, A. Tagiyeva</i>	151
Evaluating the Effectiveness of Geological and Technical Measures Using Evolutionary Modeling	<i>S. Abbasova</i>	155
About Some Approaches to Analyzing Economic Diversification	<i>Sh. Abbasova, F. Mirzayev, T. Orujova, M. Orujova</i>	159
The Influence of the Initial Flow Velocity and the Flow Direction of the Fluid on the Dispersion of the Quasi-Scholte Waves Propagating in the Orthotropic Plate in Contact with This Fluid	<i>R. Akbarli</i>	163
Some Properties of Triebel-Lizorkin-Lorentz Spaces	<i>A. Akbulut, S. Girginol</i>	167
The New Properties of the Support Function and Difference Compact Sets	<i>H. Akhundov</i>	171
The Implementation of a Commit Messages Filter for Software Version Control Systems	<i>S. Pogorilyy, B. Semonov</i>	175

Diagnosing the Technical Condition of the Traffic Management System	<i>H. Ahmadov, Q. Akhundov</i>	180
On Some New Inequalities for η -Convex Functions with the Help of AB-Fractional Integral Operators	<i>E. Set, A. Karaoğlan, A. Ekinici</i>	184
Numerical Solution of Second-Order IVPs Using a New P-stable Method	<i>A. Shokri, M. Mehdizadeh Khalsaraei</i>	188
Constructing Optimal Regulator for Discrete Linear Quadratic Optimization Problem with Constraints on Control Action	<i>F. Aliev, N. Hajiyeva, N. Velieva, M. Mutallimov, R. Tagiyev</i>	193
On the Structure of the Numerical Range of a Two-Parameter Problem under the Left Definiteness Condition	<i>E. Mammadov</i>	197
Features and Directions of the Use of New Technologies in the Field of Legal Assistance	<i>A. Baghirov</i>	200
The Optimization of Nusa Penida Island Power System for Emission Reduction and Cost Minimization Using Evolutionary Computation Artificial Intelligence	<i>D.H. Antoni, M.E. Andaswara, K.Y. Chan, D. Kim</i>	205
Bondage and Strong-Weak Bondage Number for Shadow Distance Graphs of the Path	<i>B. Atay</i>	211
Academic Concerns of Artificial Intelligence	<i>Z. Jafarov, A. Namazov, J. Abbasli</i>	215
Role of Decision Trees in Improving Intrusion Detection Systems (NIDS)	<i>A. Namazov, J. Abbasli, K. Gambarli</i>	219
A Comprehensive Analysis of the Fractal-Fractional 3D Hopfield Neural Network Model via Newton Interpolation Polynomials	<i>İ. Avci</i>	223
Technical-Economic Issues of Rational Placement of Reactive Power Compensation Devices in Electrical Networks	<i>A. Babayeva</i>	229
Positive Solutions to a Class of p-Laplacian Boundary Value Problem with Atangana-Baleanu Fractional Derivative	<i>A. Ahmadkhanlu</i>	233
Fuzzy Linear Programming Problems and Application of Neural Network to its Solution	<i>J. Zeynalov, K. Mammadova, S. Rzayeva, G. Bagirova, Sh. Babayev, A. Alakbarov</i>	240

A General Type 2 Fuzzy Clustering-Based Fuzzy Regression Function	<i>M.B. Başkır</i>	244
Fuzzy-Based Synchronization of Time-Varying Fractional-Order Networks in the Presence of Disturbance	<i>R. Behinfaraz</i>	248
Grüss Inequality for Right Quantum Integrals	<i>H. Budak, F. Hezenci</i>	252
Solving Non-Homogeneous Non-Linear Difference Equations by Using Additive and Multiplicative Discrete Derivatives	<i>M. Jahanshahi, N. Aliyev, H. Dehghani</i>	256
Optimization of PID Controller with Signature Method	<i>H.M. Durukan, B.Y. Durukan</i>	259
Qualitative Properties and Stability Analysis of the Mathematical Model for a DC-DC Electric Circuit	<i>E. Chistyakova, D. Sidorov, A. Domyshev, V. Chistyakov</i>	263
Civil Society and New Technologies:Formation of E-Civil Society	<i>E. Mirzayeva</i>	268
Ensuring the Security of Personal Data in Virtual Space	<i>E. Humbatov</i>	273
Autonomous Robotic Arm Grasping Objects with Reinforcement Learning	<i>N.U.A. Mushtaq, B. Mehmood, N. Jabbar, S. Narejo, F.A. Korai, S. Jatoi</i>	278
Calculation of Kinetic Energy of Electrons and Interaction Energy Between Electrons and Nuclei in Molecules with Open Electron Shell in a Basis of Slater Function	<i>F. Pashaev, T. Aliyeva, E. Demirtash</i>	284
Econometric Study of Factors Influencing Legal Violations Among Minors and Young Adults	<i>L. Huseynova, F. Mirzayev, R. Isgandarov, Z. Cavanshirova</i>	289
On One Problem of Synthesis One Class of Binary 4D - Multidimensional Modular Dynamic Systems	<i>F. Feyziyev, G. Mammadova, M. Mekhtiyeva</i>	293
The Numerical Method for Approximation of Hilbert Hypersingular Integral and its Justification with the Numerical Example	<i>Ch. Gadjieva</i>	298
New Inequalities Including Riemann Liouville Fractional Integral for Convex Functions	<i>B.G. Özdemir, S. Erden</i>	302
Method and Algorithm of Intelligent Control of Reactive Power Sources in Renewable Energy Source Electric Networkssion Model	<i>H. Guliyev</i>	307

Development of a Mathematical Model of Natural Gas Drying	<i>A. Gurbanov</i>	311
Mathematical Model of Transportation of Natural Gases with Complex Shaped Pipelines	<i>A. Gurbanov, S. Alekberli</i>	315
Product Model of Control of Mechatronic Devices Operating Under Conditions of Uncertainty	<i>V. Mustafaeu, R. Ruffullaeva, S. Gurbanova</i>	319
Optimization of Lagrange Problem with State Constraints	<i>G. Çiçek, E. Mahmudov</i>	323
Sweep Method for Defining of Discrete Linear Quadratic Optimization Problem with Constraint in the Form of Equalities on Control	<i>N. Hajiyeua</i>	327
Optimal Regulators for Multipoint Problems of Dynamic Systems	<i>F. Aliev, M. Mutallimov, N. Hajiyeua, N. Velieua, A. Abbasov, N.A. Ismayilov</i>	331
Design of Adaptive Fuzzy PID Controller for Quadcopter System	<i>H. Benariba, A. Boumediene</i>	336
Fractional Milne-Type Inequalities for Functions of Bounded Variation	<i>F. Hezenci, H. Budak</i>	343
Optimal Control of Discrete Inclusions with Delay	<i>H. Mirzayeua, A. Sadygov</i>	347
Properties of Uniform Separability of Nonlocal Differential Operator Equations Depending on Parameters	<i>H. Musaev, A. Nabieua</i>	351
An Analytic Approach to Predict Transient Streaming Potential Considering Changes in Surface Potential by Piezoelectricity	<i>H. Kim, S. Min, J. Kim, S. Jung, Y. Lee, H. Song, J.H. Kim, S.H. Kim, J. Hong</i>	356
Research Interference Immunity Multiservice Corporate Communication Networks	<i>B. Ibrahimov, A. Nabieua</i>	360
The Lawfulness Gas-Hydrodynamic of the Drainage Zone of Pumping Wells	<i>R. Gurbanov, T. Ibrahimlii, I. Karimova</i>	364
Method of Optimization in the Question on the Number of Lattice Points in the Circles	<i>I. Jabbarov, G. Hasanova, J. Abdullayev</i>	369

Mathematical Modeling of Logistics Problems on Water, Land and Air Modes of Transport in the East-West Transport Corridor	<i>I. Mamedov, A. Abdullayeva</i>	372
Detection of UAVs by Automatically Operating Electro-Optical Device	<i>R. Maharramov, I. Maharramov, Kh. Mammadova</i>	377
Study of the Influence of Water Injection and Fluid Withdrawal Rates on the Oil Recovery Process	<i>J. Wang</i>	381
Cauchy Problems for Variable-Order Fractional Derivative with Exponential Kernel . . .	<i>I. Koca</i>	385
Development of Algorithms for Solving the Optimization Problem of Oscillatory Systems with Liquid Dampers	<i>I. Aliyeva, A. Rasulzade, Y. Sevdimaliyev</i>	389
On Solvability of an Inverse Boundary Value Problem for the Linearized Equation of Longitudinal Waves in Rods with Periodic and Integral Condition	<i>Y. Mehraliyev, R. Iskenderov</i>	393
Digital Transformation and Economic Growth	<i>V. Ismayilov</i>	398
Hermite–Hadamard Type Inequalities for LR-Convex Interval-Valued Functions via Fractional Conformable Integrals	<i>H. Kara, H. Budak, F. Hezenci</i>	402
Air Pollution Emission Control	<i>G. Darkhooshi, K. Ivaz</i>	408
Application of Fictitious Domain Method with Conjugate Optimization for the Burgers Equation	<i>A. Temirbekov, S. Kasenov</i>	411
Parametrical Nonlinear Three Wave Interaction in Metamaterials at Constant Intensity Approximation	<i>N. Karimli, G. Safarova</i>	416
Optimal Control Problem for an Inhomogeneous Equation of Vibrations of a Three-Layer Plate	<i>H. Kuliyeu, Kh. Seyfullayeva</i>	420
Using of Ellipsoid Method for Fitting Convex or Concave Quadratic Function	<i>P. Stetsyuk, M. Korablov</i>	424
Digitization of Cultural Heritage: A Complex Legal Analysis	<i>A. Aliyev, L. Hashimova</i>	428
L-Stable Algorithm for Quasilinear Integral-Algebraic Equations	<i>L. Solovarova</i>	433

Communication in the Digital Information Society as a Right to Decent Mental Health	<i>M. Rahimova</i>	437
Removable of a Compact Sets of the Solution of Nonlinear Parabolic Equations	<i>K. Mammadova</i>	441
Comprehensive Assessment of the Activities of University Teachers Using Fuzzy Decision-Making Methods	<i>M. Mardanov, E. Aliyev, R. Rzayev, A. Rahmanov</i>	445
Algorithm of the Calculation of the Effect on an Oil Reservoir by the Streamline Method	<i>N. Bayramova, N. Safarova</i>	450
A Non-Local Problem with Integral Boundary Conditions	<i>M. Mardanov, Y. Sharifov</i>	455
On the Existence of a Solution to a Mixed Problem for One Non-Traditional Class of Equations	<i>V. Mastaliev, S. Aleskerova</i>	459
Refinements Associated to the Hermite-Hadamard Inequality for Fractional Integrals	<i>M.Z. Sarıkaya</i>	462
Modeling of a Fibrous Composite Reinforced with Unidirectional Orthotropic Fibers, Weakened by Double-Periodic Adhesion by Arched Cracks under Longitudinal Shear	<i>R.K. Mehtiyev, Y.A. Tanriverdiyev, V.F. Gakhramanov</i>	467
On the Bounds Associated to the Hermite-Hadamard-Fejer Inequality for Convex Mappings	<i>M. Yıldırım, M.Z. Sarıkaya</i>	472
Application the Nearest Neighbor Algorithm to the Recognition of Authors	<i>L. Hasanova, M. Orujova, N. Huseynova</i>	478
DCP Write Protection on PROFINET	<i>H. Mutlu, L. Altın, İ.G. Önel, Ç. Özçetin, E. Türkay</i>	483
A Method for Estimating the Pressure Gradient Required to Stimulate the Reservoir in Order to Control Its Leak-Off Capacity	<i>I. Huseynov, N. Huseynova, G. Asadova</i>	487
Mathematical Modeling and Analysis of the Solution of Vibrations of Rods with Rheological Features	<i>N. Kurbanov, V. Babajanova, U. Aliyeva, K. Agamaliyeva</i>	491
Mathematical Models of Parameters of Dispersion Patterns of Service Life of a Batch of Mechanical Engineering Products	<i>U. Nadirov, N. Rasulov</i>	495

Bound States of Klein-Gordon Equation for Double Ring-Shaped Hyperbolic Potential	<i>Sh. Nagiyev, V. Tarverdiyeva, R. Taghiyev</i>	499
Constructing the Observer for the Linear-Quadratic Optimal Control Problem in Continuous Case	<i>N. Velieva, N. Safarova, L. Amirova, R. Zulfuqarova</i>	504
Second Order Conditions in the Problem of the Calculus of Variations with a Quadratic Functional and Higher-Order Derivatives	<i>N. Gubatova</i>	508
Controllability of Fractional Linear Oscillating Systems with Damping Term . . .	<i>N.I. Mahmudov</i>	512
HR-YOLOv8: An Architecture for Mitosis Detection in Histopathology Images	<i>N. Nemati, R. Samet</i>	518
Projection of Solution of M-Sturm Liouville Problem Having Legendre Type Potential Function	<i>M. Karaoglan, E. Bas, E. Panakhov</i>	523
Probabilistic Perturbation Analysis of the Schur Decomposition . . .	<i>P. Petkov, M. Konstantinov</i>	529
Stress Distribution in the Areas of Interaction of Contact Pair Parts	<i>P. Akhundova</i>	533
Coreference Resolution in Ukrainian-Language Texts Using Llama 3 Large Language Model	<i>S. Pogorilyy, P. Biletskyi</i>	537
Calculation of the Coefficient of Hydraulic Resistance in the Main Gas Pipeline	<i>G. Gasimov</i>	542
Simulation of an Arch-Shaped Adhesion Crack in a Composite Reinforced with Unidirectional Fibers under Longitudinal Shear	<i>R. Mehtiyev, A. Musayev, G. Gasimov</i>	546
Assessment of the Impact of Production and Sales on Financial Stability in Industrial Enterprises	<i>R. Aliyev</i>	551
Optimization of Two-Directional Variable Wall Thickness Shells of Rotation by Methods of the Theory of Optimal Processes	<i>A. Dziuba, R. Iskenderov, V. Sirenko, L. Levitina</i>	556
On the Use of Differentiation of Boolean Functions in the Automatic Design of Digital Systems	<i>R. Amirova, G. Babanli, O. Hashimli</i>	562

Analog of the Euler Equation and Second Order Necessary Optimality Conditions for Rosser Type Continuous Stochastic Control Problem	<i>K. Mansimov, R. Mastaliyev</i>	566
Mathematical Evaluation of Crystallization of Composition Coated Casting in a Casting Mold	<i>F. Rasulov, A. Rasulzade</i>	570
Two Stage Multistep Methods for Integral Algebraic Equations	<i>M. Bulatov, O. Budnikova</i>	574
Mathematical Model of Casting Cooling Process and Formation in Contact Within Liquid Metal-Dispersed Metallic Surface of Mold	<i>F. Rasulov, A. Rasulzade, Q. Akhundov, A. Rasulzade</i>	578
$W^\pm$ and Z- Bosons Scatterings with Exchange of Higgs Particles	<i>L. Agamalieva, A. Gasimov, R. Jafarov, M. Mutallimov, R. Naghiyeva</i>	582
Accelerated Algebraic Multi-Subdomains Method and Application to Markov Chain Problem	<i>M. Laaraj, A. Radid, K. Rhofir</i>	587
State Regulation of the Purchasing Power of Industrial Products	<i>R. Aliyeva, A. Nabiyeu, V. Ramazanov, A. Hasanli</i>	592
On the Influence of Fluid Compressibility on the Frequency Response of the Interface Pressure in Axisymmetric Forced Vibrations of the Plate + Viscous Fluid Layer Systems	<i>R. Iskenderov, J. Imamaliyeva, Z. Kutug,</i>	596
On Some Boundary Problem for Operator-Differential Equations of the Fourth Order in Partial Derivatives	<i>S. Mirzoyev, S. Babayeva</i>	600
About a Stochastic Model of Production and Consumption	<i>S. Hamidov, N. Allahverdiyeva</i>	604
Model of Price Regulation of Firms Operating as Natural Monopoly	<i>I. Sadigov</i>	608
Extremal Problem for Differential Inclusions of a Special Form Goursat-Darboux Type	<i>M.A. Sadygov</i>	615
Riemann-Liouville Fractional Integral Inequalities Based on Convex Functions	<i>S. Erden</i>	620
Forecasting the Release of Products (Services) in the ICT Sector in the Republic of Azerbaijan Using a Fuzzy Model	<i>R. Shikhlinaskaya, N. Hajiyeu</i>	624

On the Solution Method of the Dynamics of the Eccentric Hollow Cylinder Made of Transversely Isotropic Material with Homogeneous Initial Stresses . . .	<i>S. Akbarov, S. Farajova, Y. Sevdimaliyev</i>	628
Runge-Kutta-Adams-Moulton Methods for Fractional Equations and Application to Fractional Logistic Problem	<i>S. Buranay, N. Mahmudov</i>	633
Commutator of Fractional Maximal Operator Associated with Schrödinger Operator on Generalized Morrey Spaces	<i>A. Akbulut, S. Celik, M.N. Omarova</i>	638
Solving the Inverse Boundary Value Problem Using the Conjugate Gradient Method	<i>S. Kasenov, A. Tleulesova, A. Temirbekov</i>	644
The Solution of Roesser-Type Equations for the Gas-Lift Process Using Laplace Transform Method	<i>R. Tagiyev, O. Namazov</i>	649
Application of a Modified Splitting Scheme for Modeling Atmospheric Air Pollution	<i>D. Tamabay, B. Zhumagulov, M. Tanashova</i>	653
Forecasting the Development of Post-Conflict Territories of Azerbaijan by Using Simulation Models	<i>T. Yadigarov, D. Allahverdiyev</i>	658
The Method of Conjugate Equations for the Numerical Solution of the Problem of the Boundary Layer of the Atmosphere	<i>N. Temirbekov</i>	663
rAdam: An Escaping from Local Minima of Adam Method for Constrained Optimization Problems	<i>T.T. Tran</i>	667
On the Optimality Conditions of the Switched Optimal Control Problem: Disjunctive Programming Reformulation and Local Maximum Principle	<i>B.D. Tran, E. Kostina</i>	670
Fuzzy Control System for Wastewater Treatment System	<i>T. Mustafazade, F. Abilov</i>	676
Quantum Chemical Study of A Number of Dichlorovinylidiazenes Using Computer Modeling	<i>U. Askerova, S. Demukhamedova, I. Aliyeva, A. Maharramov, N. Shikhaliyev</i>	681
The Role of Income in Ensuring the Financial Stability of Industrial Enterprises	<i>A. Nabiyeu, I. Hasanov, G. Imamgulyeva, V. Bayramov, R. Aliyev</i>	687
Econometric Assessment of the Impact of the Use of Renewable Energy Sources on the Amount of Greenhouse Gases in Azerbaijan	<i>Y. Hasanli, A. Taghiyeva</i>	692

A Methodology for Comparative Analysis of the Economic Impact of Traffic Accidents on Government, Enterprises, and Households Using the Input-Output Model	<i>Y. Hasanli, A. Safarova</i>	696
Chinese Lantern-Type Stability Loss of Circular Solid Cylinder Made of FGM Under Axial Compression	<i>U.B. Yesil, F. Aylıkcı, N. Yahnioğlu</i>	700
Maximal Operator in the “Complementary” Generalized Weighted Morrey Space	<i>Z.V. Safarov</i>	705
Nonlinear Optimal Control Problem for Fuzzy Systems	<i>J. Zeynalov, M. Seyidova, M. Eliyev, H. Gasimov, H. Askerli</i>	709
Algorithm for Multi-Criteria Optimization of Geometric Parameters of Robots Using Machine Learning for Predicting Mappings	<i>D. Malyshev, D. Dyakonov, A. Pisarenko, G. Stas</i>	713
The Role of Artificial Intelligence in Cyber Resilience of Cyber Physical Systems	<i>R.Alakbarov, M. Hashimov</i>	721
About Sobolev-Morrey Estimates for Nondivergence Degenerate Operators with Drift on Homogeneous Groups	<i>V. Guliyev</i>	726
Maximal Function in Total Morrey Spaces for the Dunkl Operator on the Real Line	<i>Y. Mammadov, F. Muslumova</i>	731
Regularization of Necessary Conditions of Solvability a Nonlocal Boundary Value Problem for an Integral-Differential Equation of Elliptic Type in a Cube	<i>Y. Mustafayeva, N. Aliiev, A. Aliiev</i>	735
Exploring Fan Power Efficiency in Water Cooling Systems Through Regression Analysis of Wind Speed Effects	<i>F. Agayev, S. Aghamатов</i>	740
On the Family of First Passage Time of a Parabola by the Markov Perturbed Random Walk Described by an Autoregressive Process AR(1)	<i>F. Rahimov, R. Aliyev, A. Farhadova</i>	745
Development of a Regression Model with One Input Variable	<i>N. Suleymanov, Z. Mahmudova</i>	748
Nonlocal Quasilinear Elliptic Equations in Weighted Spaces	<i>H. Musaev</i>	752
Development of Algorithms for Increasing Measurement Accuracy and Conversion Functions on Information-Measuring Systems	<i>A. Mehdiyeva, A. Safarova, S. Bakhshaliyeva</i>	756

A Survey on Striction Curves	<i>A. Çakmak, S. Çakar</i>	762
Some Main Directions of Information Technologies in the Educational Management	<i>F. Aliev, N. Ismayilova</i>	767
On the ZGV Modes in the Dispersion of Axisymmetric Waves Propagating in a Cylinder with Inhomogeneous Pre-Stresses Immersed in a Compressible, Inviscid Fluid . . .	<i>E. Bagirov, S. Akbarov</i>	770

The Role of Artificial Intelligence in Cyber Resilience of Cyber Physical Systems

Rashid Alakbarov

Institute of Information Technology
Baku, Azerbaijan
t.direktor_muavini@iit.science.az

Mammad Hashimov

Institute of Information Technology
Baku, Azerbaijan
mamedhashimov@gmail.com

Abstract—Lately, artificial intelligence (AI) technology has been extensively applied in the struggle against cyber threats in CPS. AI may improve system security by providing tools to quickly detect cyberthreats and automatically resolve them. Digitization of critical infrastructures (energy distribution networks, smart systems, oil and gas industry, water infrastructure, etc.) has increased their efficient management and at the same time, the number of cyber attackers on sensors, actuators, network and control equipment has also increased. Cyber security of critical objects can be ensured through AI. This article explores the role of AI in enhancing the cyber resilience of CPS. The article analyzes the advantages and disadvantages of using AI technologies in the security of Cyber-Physical systems. Mechanisms for detecting cyber threats in cyber-physical systems with the help of AI, predicting and preventing security threats have been proposed.

Index Terms—artificial intelligence, cyber security, cyber physical systems.

I. INTRODUCTION

Cyber-physical systems (CPS) connect digital and analogous devices, interfaces, networks, computer systems with the physical world. CPS is based on a computer system that processes information in the automotive, aviation, energy and other industries. These computer systems are used to perform specific tasks. CPS incorporates sensors, actuators and similar embedded systems that interact with the real world, as well as sophisticated software. CPS refers to the close interactions and relationships between cyber components such as sensor systems and physical components that form the origin of the Internet of Things [1], [2]. The main areas covered by CPS are shown below [2], [3]:

- In smart cities: Smart traffic management systems, Smart buildings and infrastructure, environmental monitoring and waste management, etc.
- In energy management: Supervisory Control And Data Acquisition (SCADA) systems, smart grid, production and distribution of electricity, and adaptation and optimization of its consumption;
- In the environment: monitoring of the environment in wide and diverse geographical areas (forests, rivers and mountains), early detection of natural disasters (forest fires);
- In intelligent transport management: operational management of complex traffic flow through real-time data sharing, accident prevention;

- In agriculture: precise farming, smart irrigation and more efficient distribution of nutrients (fertilization, nitrogen), improvement of crop production capabilities;
- In health care: real-time monitoring of patients' health and providing notification, telemedicine systems for remote delivery of medical services;

The interaction of the aforementioned areas with digital infrastructures exposes CPS to cyber threats and makes cyber resilience an important aspect of them. Increasingly sophisticated cyber threats, along with traditional system vulnerabilities, posing significant challenges to CPS resilience [4].

II. DIFFERENT TYPES OF ATTACKS, THREATS AND VULNERABILITIES IN CYBER-PHYSICAL SYSTEMS

Below are some of the different types of attacks, threats, and vulnerabilities that compromise CPS [5]–[7]:

- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. DoS attacks aim to disrupt CPS availability at the expense of multiple system resources, whereas DDoS attacks use multiple compromised systems to intensify this effect. These attacks can cause significant interruptions to critical infrastructure, such as shutting down production lines or disordering power grids.
- Mal ware attacks. Mal ware, including viruses, worms, trojans, and ransom ware, can intrude CPS to steal data, disrupt operations, or control system functions. Mal ware can cause data corruption, loss of control over physical processes, and significant financial and reputational damage.
- Man-in-the-Middle (MitM) Attacks. In MitM attacks, attackers intercept and manipulate CPS components or connections between CPS and external networks. These attacks can result in data theft, unauthorized control of system operations, and injection of false information, compromising the integrity and reliability of the CPS.
- Advanced Persistent Threats (APTs). APTs are long-term and targeted attacks where cyber criminals intrude a system and collect data over a long period of time and compromise the integrity of the system. APTs can cause significant data exfiltration, disruption of critical services, and long-term damage to system integrity and reliability.

- **Insider Threats.** Insider threats include malicious actions by individuals with access to CPS within the organization. These threats can lead to data breaches, sabotage of system operations, and unauthorized access to vulnerable information.
- **Zero Day Exploits.** Zero-day exploits target unknown vulnerabilities in software or hardware and leave the system vulnerable until a patch is developed and deployed. Because these threats exploit unpatched vulnerabilities, they can lead to significant damage and potentially cause widespread disruption and data corruption.
- **Phishing and Social Engineering.** Phishing and social engineering attacks trick individuals into revealing confidential information or taking actions that compromise CPS security. These attacks can lead to unauthorized access, data corruption, and the introduction of malware into the CPS.
- **Software vulnerabilities.** Bugs, flaws, or vulnerabilities in software code can be used by attackers to gain unauthorized access, disrupt operations, or steal data. Software vulnerabilities can compromise the integrity, availability, and confidentiality of CPS.
- **Hardware Vulnerabilities.** Deficiencies or weaknesses in the physical components of the CPS can be exploited to disrupt operations or gain control over system functions. Hardware vulnerabilities can lead to physical damage, disruption of operations, and unauthorized control of CPS.
- **Communication Protocol Vulnerabilities.** Secure communication protocols can be used to capture, modify, or insert data into CPS communication streams. These vulnerabilities can compromise data integrity, allow unauthorized access, and disrupt system operations.

Given the various types of attacks, threats and vulnerabilities mentioned above, cyber security is a critical concern in current digital age, with cyber-attacks posing significant risks to individuals, organizations and nations. Although traditional security methods are important, new countermeasures are needed to keep up with the dynamism of cyber threats. As cyber threats grow in complexity and frequency, traditional security measures often fail to provide adequate protection. AI offers advanced capabilities to detect and prevent cyber-attacks through sophisticated algorithms and real-time analysis. AI provides a promising solution by automating threat detection and response, increasing the accuracy and efficiency of cyber security systems. AI has emerged as a transformative force in enhancing the resilience of CPS. AI's ability to process large amounts of data, recognize patterns, and make autonomous decisions ensure new opportunities to protect these systems from cyber threats.

III. APPLYING ARTIFICIAL INTELLIGENCE TO DETECT AND PREVENT CYBER ATTACKS

Signature-based detection systems are mainly used to ensure the cyber security of traditional CPS. These systems work by comparing an incoming package (of software) against a

database of identified intimidations or malevolent code signatures. If any part of the code of the viewed program matches a known virus code (signature) in the database of antivirus programs, the antivirus program deletes the infected program, sends the program to "quarantine", or tries to restore the program by removing the virus itself from the program. This approach is actual against acknowledged intimidations, but insufficient against new and unidentified ones. Cyber criminals may effortlessly avoid signature-based detection systems by changing code in applications or creating new malware that is not available in the database. Analysis of cyber security issues for signature-based detection systems is mainly performed by engineers (security analysts). Security analysts manually used to review patterns or indicators of security breaches. This was time-consuming and also relied on the security analyst's expertise in identifying threats. Although signature-based detection systems are operative in specified circumstances, they are often inflexible and unable to recognize evolving threats. In order to solve the above mentioned problems, AI technologies have been used in recent times. Systems designed by people to facilitate the exchange of information, goods, and services have become an integral part of modern life, effectively forming a crucial infrastructure. These infrastructures encompass a range of networks, including transportation, communication, energy, and digital systems, which have evolved over centuries to meet the evolving needs of society. AI is a powerful intelligence tool that can effectively detect and prevent threats to the security of cyber-physical systems. Some of them are shown below [8]–[11]:

- **Threat detection.** AI has the ability to detect and automatically remediate cyber attacks on the network. If AI detects a threat in the system, it can take automatic actions such as blocking access to infected resources (hardware). AI can instantly access vast amounts of data and analyze specific data patterns to detect signs of an attack. It helps provide system defense mechanisms by automatically detecting threats in network traffic data.
- **Anomaly detection:** Anomaly detection embraces identifying deviations from established patterns of behavior. AI algorithms can analyze network traffic, user behavior and system logs to detect anomalies that could indicate a cyber-attack. For example, an AI system can detect unusual access attempts from unfamiliar locations or at unusual times and record them as potential security incidents.
- **Attack prediction:** AI is used to predict and prevent future attacks based on available data. It helps develop defense strategies against potential attacks based on analysis of past attack patterns and data. AI equipped with learning algorithms, can study data to identify new types of attacks and develop defense strategies against these attacks.
- **Automation of routine processes.** AI automates routine cyber threat detection processes. Systems can automatically update their defenses based on new threat information, allowing them to quickly respond to new

types of attacks. AI helps perform deep analysis and other defensive measures to defend against an attack, automatically applying security policies after detecting dangerous data.

- Incident Response: AI can automate the incident response process, reducing the time needed to mitigate the threat. AI-driven systems can generate alerts, prioritize them based on severity, and enable pre-defined response protocols.
- Behavioral Analysis: Behavioral analysis involves monitoring and analyzing the behavior of users and systems to detect suspicious activities. AI algorithms can determine baselines of normal behavior and detect deviations that could indicate a security breach. For example, an AI system can detect when a user is accessing sensitive information that they would not normally interact with and enable an alert for further investigation.
- Alert prioritization: Cyber security teams are often faced with a high volume of alerts, making it difficult to prioritize and respond to the most critical threats. AI algorithms can analyze alerts based on factors such as threat severity, potential impact on the organization, and historical data. This helps security teams focus on the most urgent and high-risk incidents.
- Mal ware detection. Machine learning algorithms are exploited by AI to identify both known and unknown mal ware threats and react to them. These algorithms examine huge volumes of data to distinguish patterns and irregularities that are hard for humans to identify. Analysis of mal ware behavior may determine new and unknown mal ware variations that cannot be detected through old-style antivirus software.
- Transaction monitoring: Financial institutions and e-commerce platforms use AI to detect fraudulent transactions. AI algorithms can monitor financial transactions in real-time to detect signs of fraud. By analyzing transaction patterns, such as the frequency and costs of transactions, AI systems can identify unusual activities that may indicate fraudulent behavior. For example, an AI system may detect that a user's spending behavior significantly deviates from their typical patterns and record the transaction for further investigation.
- Identity Verification: AI-powered identity verification involves the use of biometric data such as facial recognition and fingerprint scanning to verify the identity of users. This helps prevent identity theft and ensures that only authorized individuals can access sensitive information and conduct transactions.
- Vulnerability Assessment: AI algorithms can scan systems and applications for known vulnerabilities by comparing them to a database of known vulnerabilities, such as the Common Vulnerabilities and Exposures (CVE) database. AI can also identify potential vulnerabilities based on observed patterns in code or configuration.
- Detection of phishing attacks. Old-style approaches to phishing detection often rely on rule-based filtering or

blacklisting to detect and obstruct identified phishing emails. Since these approaches are only actual against recognized attacks and not against newly created ones, they have limitations. Using machine learning algorithms AI-powered phishing detection solutions analyze the emails' content and structure in order to detect possible phishing attacks. These algorithms can learn from huge volumes of data to identify patterns and irregularities showing a phishing attack.

- Predictive Analytics: AI-powered predictive analytics can identify potential vulnerabilities before they are exploited by analyzing trends and patterns in cyber security data. For example, AI algorithms can predict what types of vulnerabilities will be targeted by attackers based on historical data and emerging threat intelligence.
- Implementation of AI in access control and authentication systems. Access control and authentication systems play an important role in ensuring the security of information systems and data. They determine who has access to certain system resources and functions and verify that the user is the one who claims to be.

IV. ADVANTAGES AND DISADVANTAGES OF USING ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

Applying AI in cyber security of CPSs has several advantages. AI ensures real-time threat detection and response. Second, AI can learn from experience and improve its skills or abilities over time. A number of important advantages of using AI in the field of cyber security are shown below [12], [13]:

- High level of security. AI technologies allow to implement security measures faster and more effectively by analyzing data in real-time. This helps to make the systems more secure.
- Real-time Analysis: AI systems can analyze large amounts of data in real-time and identify threats as they happen. This immediacy enables faster response to potential breaches.
- Data processing efficiency. AI has the ability to process and analyze larger amounts of data than humans, allowing it to identify complex or hidden threats.
- Anomaly Detection: AI can determine baselines of normal behavior and detect anomalies that may indicate cyber threats. Machine learning algorithms can identify patterns that would be difficult for humans to recognize.
- Speeding up the threat detection process. AI is capable of analyzing huge volumes of data in real time, providing faster and more productive threat detection than traditional methods. AI can respond faster to security incidents and prevent attacks from spreading.
- Adaptability: AI systems can adapt to the evolving cyber security landscape by learning from new data and emerging threats to be up-to-date and effective.
- Development of protection strategies. Due to its capability to learn from past cyber attack data, AI can predict future threats and help develop defense strategies. AI,

equipped with learning algorithms, can learn from past threats and perform higher levels of data analysis to detect new or evolving threats.

- Machine learning: Machine learning algorithms learn from historical data and adapt to new threats. The more data they process, the more improves their ability to distinguish between malicious and malicious activity.
- Automation of the analysis process. AI can automate the process of analyzing big data, which can reduce the time and resources spent on information processing. This is especially important in an environment where the volume of data is constantly increasing. AI reduces the workload of implementing security measures and protecting systems by automatically managing large amounts of data.
- Speed and Efficiency: Automated systems can immediately react to threats, isolate affected systems, block malicious IP addresses, and initiate other defensive measures immediately. This reduces the attackers' opportunity and minimizes potential damage.

Despite the advantages of AI technologies, the issues related to the use of these methods for malicious purposes have caused argument. Applying AI in cyber security tools also has its limitations and challenges. First, the security AI itself can be attacked and manipulated by malicious hackers. Second, AI can fail and misinterpret data, which can lead to wrong things being done or real threats being missed. Despite the significant advantages, several problems related to the use of AI in cyber security. While there are many benefits of applying AI in cyber security, there are also possible risks to consider. Below are some of them [14], [15]:

- Misuse of AI by attackers. Just as security professionals can use AI to combat cyber threats, attackers can also take advantage of AI technology to generate new types of attacks. This may include everything from creating more convincing phishing attacks to automating the process of seeking vulnerabilities in network systems.
- Data Quality and Quantity: AI systems rely on large volumes of high-quality data for training and operation. Inadequate or biased information can undermine their effectiveness.
- Incomplete Information: Incomplete information can lead to inaccurate detection of threats and wrong conclusions. Providing comprehensive data sets is crucial for full AI performance.
- Privacy issues. The use of AI to analyze large volumes of data may increase privacy concerns, particularly those related to personal data.
- Dependence on AI. While AI automates many aspects of cyber security, human control remains essential. Relying solely on AI without human intervention can lead to non-avoided threats and inadequate responses.
- With the increased use of AI in cyber security, there is a risk of over-dependence on technology, which can lead to people losing control over it.
- Lack of qualified specialists. Implementing and main-

taining AI systems requires specialized knowledge and expertise, which can be a barrier for some organizations. Learning and working with AI requires high qualifications and specialized knowledge, which is currently in short supply in the labor market.

- Possibility of wrong decisions. AI can sometimes make wrong decisions, that is, it may consider normal user actions as security threats. This may cause the security system to be overloaded. AI can create new risks related to data security and protection. Algorithms are likely to make bad decisions, increasing the potential access by hackers to data and creating new threats to the protection of that data.
- Computing resources. AI requires powerful systems with large computing resources and memory resources to process and analyze huge volume of data. This can be problematic for organizations with limited funds.
- Integration with Existing Systems: Integrating AI with existing cyber security infrastructure can be complicated and requires a significant investment in time and resources.

V. CONCLUSIONS

This article examined the use of AI in cyber security tools of CPS. Proposals were made for the use of AI technologies in the identification and avoidance of cyber attacks. The advantages and disadvantages and problems of using AI in cyber security systems were highlighted. The purpose of this review article is to identify future research directions and to use machine learning, deep learning methods, neural networks, etc. to improve the efficiency, reliability and cyber resilience of cyber-physical systems. Future research work is to develop new methods and algorithms through AI tools.

ACKNOWLEDGMENT

This work supported by the Science Foundation of the State Oil Company of Azerbaijan Republic (SOCAR) (Contract No. 3LR-AMEA)

REFERENCES

- [1] T. Sanislav, and L. Miclea, "Cyber-physical systems - concept, challenges and research areas," *Control Engineering and Applied Informatics*, vol. 14, 2012, pp. 28–33.
- [2] R. G. Alakbarov, and M. A. Hashimov, "Fog computing technology application in cyber-physical systems and analysis of cybersecurity problems," *Problems of Information Society*, vol. 13, pp. 23–29, 2022.
- [3] C. Hong, "Applications of cyber-physical system: A literature review," *Journal of Industrial Integration and Management*, vol. 2, 2017, pp. 1–28.
- [4] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, 2018, pp. 212–223.
- [5] A. K. Tyagi, and N. Sreenath, "Cyber physical systems: Analyses, challenges and possible solutions," *Internet of Things and Cyber-Physical Systems*, vol. 1, 2021, pp. 22–33.
- [6] M. Sagar, and C. Vanmathi, "Attacks on cyber physical system: Comprehensive review and challenges," *I.J. Wireless and Microwave Technologies*, vol. 5, 2022, pp. 53–73.
- [7] J. A. Yaacouba, O. Salmanb, H. N. Nouraa, N. Kaanichec, A. Chehabb, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocessors and Microsystems*, vol. 77, 2020, pp. 103–201.

- [8] N. B. Dokur, "Artificial Intelligence (AI) Applications in Cyber Security,"
- [9] M. F. Rafy, "Artificial Intelligence in Cyber Security."
- [10] A. J. G. Azambuja, C. Plesker, K. Sch?tzer, R. Anderl, B. Schleich, and V. R. Almeida, "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0-A Survey", *Electronics*, vol. 12, 2023, pp. 1–18.
- [11] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, "Explainable artificial intelligence in cybersecurity: A Survey," *IEEE Access*, vol. 10, 2022, pp. 93575–93600.
- [12] R. Calderon, "The benefits of artificial intelligence in cybersecurity," *Economic Crime Forensics Capstones*, vol. 36, 2019, pp. 1–22.
- [13] L. Lazic, "Benefit From AI in Cybersecurity", *The 11th International Conference on Business Information Security (BISEC-2019)*, 18th October 2019, Belgrade, Serbia.
- [14] J. Wilkins, "Is artificial intelligence a help or hindrance," *Network Security*, vol. 2018, 2018, pp. 18–19.
- [15] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, "The impact and limitations of artificial intelligence in cybersecurity: A literature review," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 11, 2022, pp. 81–90.