CURRICULUM VITAE

Name:	**Leon REZNIK**
Current Position:	**Professor**
Primary affiliation:	**Department of Computer Science**
Secondary affiliation:	**ESL Global Cybersecurity Institute**
@:	**Rochester Institute of Technology**
Address:	**102 Lomb Memorial Drive, Rochester NY 14623**
Phone:	**585-475-7210**
Email:	**leon** dot **reznik** at **rit** dot **edu**
WWW Home page:	**http:\\www.cs.rit.edu\~lr**

SUMMARY:

Qualifications:

PhD in Information and Measurement Systems, 1983, St. Petersburg State Polytechnic University
ME/BS in Computer Control Systems, 1978, St. Petersburg University of Airspace Instrumentation
Graduate Certificate in Tertiary Education, 2002, Victoria University, Melbourne

Teaching accomplishments:

31 years full time (USA, Australia) and 6 years part time experience of university teaching and training at different levels: undergraduate and postgraduate students, professionals, in-person and on-line. Experience in research development and supervision, mentoring of students and faculty.

Current courses (taught at least once over last five years):

CSCI-532 Introduction to Intelligent Security Systems - Undergraduate course for CS and CSec students
CSCI-630 Foundations of Artificial Intelligence - Graduate course for CS students
CSCI-735 Foundations of Intelligent Security Systems - Graduate course for CS and CSec students
CSCI-736 Foundations of Neural Networks and Machine Learning - Graduate course for CS students
CSCI-788 Master's Project supervision

New textbook

L. Reznik, Intelligent security systems: How artificial intelligence, machine learning and data science work for and against computer security, Wiley - IEEE Press, ISBN-10: 1119771536, 384 pp., 2022

Research results (over last five years):

Research areas:

Federated Learning, Machine learning; Artificial neural networks; Data quality; Cybersecurity; Sensor systems and networks

Current grants:

PI: 2023-26: Collaborative research: IDEAS lab: ETAUS: Smarter Microbial Observatories for Realtime ExperimentS (SMORES) (NSF award # 2321652)

Co-PI: 2024-26: IMPRESS-U: Exploratory Research in Robust Machine Learning for Object Detection and Classification (NSF award # 2415299)

Recently completed grants (as a PI)

PI: 2020-22: Self-learning capabilities for a mission oriented data quality and security assurance in military IoT systems (US Military Academy/DoD award # W911NF2010337)

PI: 2021-22: Security evaluation and improvement of the personal infrastructure with new tools and education development (CRDF Global/DoState award # G-202102-67515)

PI: 2016-21: CICI: Data Provenance: Data quality and security evaluation framework for mobile devices platform (NSF award # ACI-1547301)

PI: 2017-18: Intelligent security systems (Course development) (NSA award # H98230-I7-l-0200)

Software and data products

Six Android security and data quality apps, 2018-22 – available on Google Play

Data collections of electronic sensors incorporated into mobile devices available on the market with their quality evaluations – available at http://www.dataqualitylabs.com/dataView

Patents pending:

L. Reznik and S. Chuprov, "Federated Learning with A Compromised Unit Exclusion from Receiving Global Model Updates". *Application No. 63/439,995 filed on January 19, 2023, converted Jan. 2024*

L. Reznik and S. Chuprov, "Network Adjustment based on Machine Learning End System Performance Monitoring Feedback". *Application No. 63/406,514 filed on September 14, 2022, converted in Sep. 2023*

Summary of products developed:

	1992-2001	2002-11	2012-23
Books	2	3	2
Chapters in books	5	7	7
Refereed journal articles	7	7	7
Refereed conference papers	44	32	41
Apps developed	-	-	6
Data collections	-	-	2
Patent applications	-	-	2

Table of Contents

I. QUALIFICATIONS AND EXPERIENCE

1983	**PhD Degree in Engineering specializing in Information and Measurement Systems** St.Petersburg Polytechnic University, St.Petersburg, Russia
1978	**ME/BS Degree in Electrical Engineering/Computer Science (5.5 years course)** St.Petersburg University of Airspace Instrumentation, St.Petersburg, Russia
2001	**Graduate Certificate in Tertiary Education** Victoria University, Melbourne, Australia

ACADEMIC TITLE GRANTED

1987	**Academic title of Senior Research Fellow in Information and Measurement Systems** High Academic Certifying Commission, USSR Council of Ministers, Moscow, Russia

ADDITIONAL COURSES

2002	**Information Assurance – Capacity Building Program** Carnegie-Mellon University, Pittsburgh, USA
1998	**College Course in Cooperative Learning** University of Minnesota, USA
1990	**UNIX & C Programmer** Training Course, ANIRAL UTEC, Paris, France

EMPLOYMENT HISTORY

since Dec. 2002	**Professor (tenured since 2005)** Computer Science Department**,** Rochester Institute of Technology, NY
Jan.-Dec.2002	**Visiting Professor – Associate Professor** Computer Science Department, University of Texas at El Paso
Jul.1992- Dec. 2001	**Lecturer, Senior Lecturer (tenured since 1998)** School of Communications and Informatics, Victoria University, Melbourne, Australia
1988 - 91	**Leading Scientist** Joint Venture "Interquadro" (Russia-France-Italy), St.Petersburg, Russia
1987 - 88	**Leading Scientist** Central Research Institute of Shipbuilding Technology, St. Petersburg, Russia
1978 - 87	**Engineer, Programmer, Junior Scientist, Senior Scientist** Research Institute of Electromeasuring Instruments, St.Petersburg, Russia

VISITING POSITIONS

1998	**Honorary Academic Visitor** Department of Electrical and Computer Systems, Monash University, Melbourne, Australia
1998	**Visiting Fellow** Computer Science Department, University of Texas at El Paso, USA

II. Teaching Portfolio

Summary:

31 years full time (USA, Australia) and 6 years part time experience of university teaching and training at different levels: undergraduate and postgraduate students, professional engineers

Experience in teaching of both big classes and small groups as well as online delivery

Experience in research thesis and project supervision

Experience in developing new courses and programs and their accreditation

Mentoring and assisting other faculty in their research and teaching skills development

Formal education in tertiary teaching

Teaching areas: Computer Security, Intelligent Systems and Machine Learning

Current courses *(taught at least once over last five years):*

CSCI-532 Introduction to Intelligent Security Systems - Undergraduate course for CS and CSec students (taught in both online and in-class modes)

CSCI-630 Foundations of Intelligent Systems - Graduate course for CS students (taught in both online and in-class modes)

CSCI-735 Foundations of Intelligent Security Systems - Graduate course for CS and CSec students (taught in both online and in-class modes)

CSCI-736 Foundations of Neural Networks and Machine Learning - Graduate course for CS students

CSCI-788 MS Project supervision (taught in both online and in-class modes)

Courses taught recently*:*

Data Communications and Networks I - Undergraduate/graduate course for CS students

Artificial Intelligence/Introduction to Artificial Intelligence - Undergraduate/graduate course for CS students

Security Measurement and Testing - Undergraduate/graduate course for CS and CSec students

Intelligent Security Systems - Undergraduate/graduate course for CS and CSec students

Computer Science 1 - Introductory course for CS/SE/CE students

Computer Science 2 - Introductory course for CS/SE/CE students

Theory of Computer Algorithms - Graduate course for CS students

Neural Networks and Machine Learning - Graduate course for CS students

Research Seminar II and III– PhD courses

Introduction to Research – PhD course

Textbooks published:

[1] **L. Reznik** *Intelligent security systems: How artificial intelligence, machine learning and data science work for and against computer security*. IEEE Press-Wiley&Sons, 384 pp, ISBN-13: 978-1119771531, ISBN-10: 1119771536, 2022

[2] **L.Reznik** *Fuzzy Controllers: How they work? How to design them?* Elsevier-Newnes, Oxford-Boston, 1997, ISBN 0-7506-3429-4, 287 pp.

Research Supervision:

PhD Research Students (principal supervisor):

Rochester Institute of Technology:
R. Zatsarenko – PhD full time: started in Jan. 2024
S. Chuprov – PhD full time: started in 2021, completed 2024
I. Khokhlov – PhD full time: started in 2016, completed in 2020
Victoria University, Melbourne, Australia
O. Ghanayem - PhD full time - started in March 1994, completed in March 1997
A. Little - PhD full time - started in February 1996, completed June 2001
A. Stojcevski – Master’s full time – started in August 1998, completed February 2000
H. Nguyen - Master’s full time – started in March 2001, completed 2003
M. Zilevski - PhD part time – started in July 2001, stopped supervision in 2003
Monash University, Melbourne, Australia
G. Michalik – co-supervisor PhD, started in 1997, completed 2000
Central Research Institute of Shipbuilding Technology, St.Petersburg, Russia
N.Baskin – PhD part time, started 1988, stopped supervision in 1991

MS Capstone Project supervision

Supervised 113 MS Capstone project/theses over last 10 years, all students have successfully completed their degrees

completed over last 5 years

2023-24 – 7 projects

Shweta Sandip Sharma	Analyzing Effects of Adversarial Attacks on Classifier Performance
Vedika Vishwanath Painjane	Analyze the Effect of Data Poisoning on Semantic Segmentation Using Federated Learning
Harshil Pravintab Patel	Improving Federated Learning Security with Trust Evaluation to Detect Adversarial Attacks
Gaurav Raju Thakur	Resilience of Federated Learning Models in Image Classification Under Data Degradation
Sridhar Shenoy	Benchmarking Federated Learning Algorithms with FLAIR
Abhik Roy	Exploring the Robustness of Federated Learning for Image Classification
Anirudh Ramesh Narayanan	Soccer Highlight Generator

2022- 23 – 7 projects

Shivam Mahajan	Assessing Classifier Performance Following Adversarial Attacks on Transmission Networks carrying Video Packets
Chirayu Anil Marathe	Analyzing Network Degradation in Video Classifiers
Moinuddin Memon	Knowledge-Based Client Filtering Algorithm For Federated Learning
Michael Bashta	Extracting Information from a Model
Arjun Nair	Federated Learning: Defense against Global Model Poisoning Attacks
Rahul Babu Ganesh|	Analyzing attack effects on machine learning models
Bhushan Patil	Analyzing the Effects of Image Compression on Deep Learning Models

2021-22 – 7 projects

Kartavia Manojbhai Bhatt	Evaluating Robustness of Federated Learning towards Data Corruption
Akshaya Satam	Studying the Influence of Degrading Network Conditions on Medical Image Recognition Systems

Jaineel Vyas	Evaluating Robustness of Object Detectors using White-Box Attacks
Ankit Bapat	Smart and Secure Web Application Design
Antoun Obied	Effect of Network Infrastructure on ML-Based Speech Recognition
Venkata Karteek Paladugu	Performance Metrics of Transfer Learning on Image Classifier
Santosh Kumar Nunna	Multiclass Traffic Sign Classification Using CNN

2020-21 – 8 projects

Ashwin Yogesh	Integration of Data Quality in COSMOS and POWDER Testbeds
Ameya Deepak Nagnur	Optimal Sensor Selection using Evolutionary Computing
Adam Spindler	Evaluating Robustness of Cloud Based Object Detectors against adversarial attacks
Soham Dongargaonkar	Investigating Network Data Quality Metrics in POWDER Test Beds
Srujan Shetty	Performance Analysis of Classifiers on Images Transferred over POWDER Testbed
Zizhun Guo	Explore Object Detection Performances in Relation to Input Image Deterioration
Aseem Mehta	Analysis of pre-trained classifiers with audio files transferred over POWDER platform
Mouna Reddy Kallu	Enhancing Android System Security Data Quality and Processing Time

2019-20 – 9 projects

Sahil Ajmera	Data Collection and Data Quality Assessment of Mobile Sensors Using Machine Learning Techniques
Ninad Ligade	Improvements in colluded android application detection techniques using better data preprocessing techniques and a computationally efficient machine learning model
Mansha Malik	Security Evaluation Metrics for Android Device
Kunal Mulwani	Security Evaluation Tool for Windows OS
Rohit Ravishankar	Machine Learning in Anomaly Detection: Colluded Applications Attack in Android Devices
Shashank Rudroju	Thesis: Root failure analysis in meshed three networks
Sudhish Surendran Thazhakasseril	Road Pothole Classification and Reporting with Data Quality Estimates
Abhishek Patil	A User-Friendly Smartphone Application for Pothole Reporting and Recognition
Suyash Sorte	Data Quality Database Design and Implementation

2018-19 – 12 projects

Parinitha Nagaraja	Security evaluation for Android systems
Akshay Pudage	Finding best data sources using genetic algorithms
Saurabh Revaskar	Data quality evaluation integrating system functionality indicators
Arpit Vora	Colluded applications investigation with neural networks
Samir Saurav	Android System Security Evaluation
Utsav Dixit	Improving air traffic monitoring with OpenSky
Renzil Anthony Dourado	Malicious App Detector Based On Permission Analysis
Joe Tomb Job	Data collection and analysis to detect Inter Application Collusions in Android
Sanjay Haresh Khatwani	MeetCI - A Computational Intelligence software design framework modification
Qiaoran Li	Expert system implementation on Android devices through machine learning
Rohit Anbalagan Mudaliar	Colluded Applications detection in Android devices
Sandhya Murali	Detection of Android malware based on Permission History and Analysis

2017-18 – 13 projects

Akhil Killawala	Framework for Automatic Generation of Questions from Text
Akshay Renavikar	Colluded applications: vulnerability detection in Android devices
Milan Bhaskar	Finding vulnerable applications in Android

Pooja Kumari	Face Recognition Using Percentage Matching
Praful Konduru	Gait Analysis using Sensor Data and Machine Learning Techniques
Rohit Bhaskar	Impact of Mounting Positions on Data Quality and Human Activity Recognition for Wearable Sensors
Shashank Gangadhara	Feature Set Analysis for Activity Classification and Impact of Data Quality on Classifier Accuracy
Supriya Kharade	Network Configurator and Controller for Routing in the Internet
Vanessa Fernandes	Learning made Easy-Automatic Tech Quiz Question Generator
Atir Petkar	Semi Supervised Classification of Images Using Generative Adversarial Networks (GAN)
Ajinkya Kolhe	Security Analysis of Android Applications using Machine Learning
Saurabh Anant Wani	Android System Security Evaluation Manager
Jinesh J. Shah	Dynamic Classifier for Human Activity Recognition using Sensor Data and the Impact of Data Quality

Staff members:
In 1994 organized and had been leading until 2001 a collaborative research group in fuzzy technology. As the research mentor of this group I was developing the research skills of the group members in the new research area of neuro-fuzzy technology.

Curriculum and educational programs development

2002-17	BS in Computer Science accreditation UTEP and RIT
2009-10	BS and MS in Computer Science – major re-development
2011-12	New BS and MS in Computer Security and Information Assurance
2010-11	New PhD in Computing and Information Sciences

PI on NSA grant "Intelligent security systems: course curriculum development" - funded by NSA (award # H98230-I7-l-0200), 2017-18, budget: $118,926.

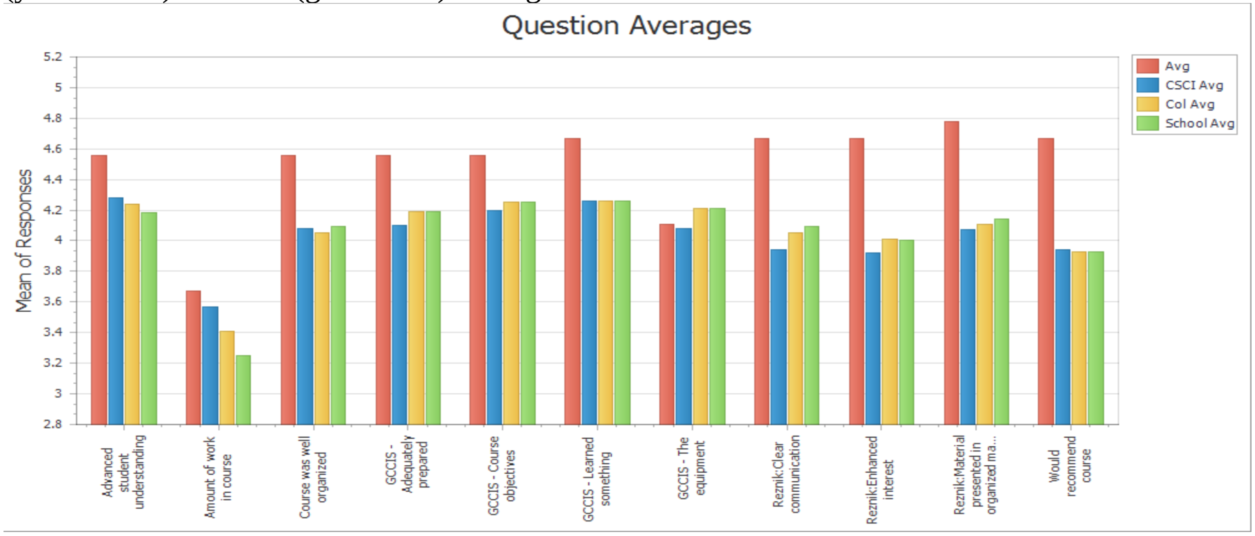
The project designed a curriculum, developed course materials, tested and evaluated them in real college classroom settings, prepared and submitted them for dissemination of a college level course on Intelligent Security Systems.

In order to facilitate interconnections with other courses and its inclusion into the national Cybersecurity curricula, the course is composed of nine separate modules. Five modules cover the specialized topics including: a review of the modern state of the cybersecurity and the current problems and approaches; firewall design; intrusion detection systems; anti-malware methods and tools; hacking activity and attack recognition and prevention. Other modules provide additional support to assist in course teaching preparation, such as test and exam questions, course project and research assignment specifications, and tool presentation descriptions. Each module is further subdivided into micromodules. Altogether, the modules provide an instructor with a comprehensive set to initiate the course.

This course merges together various knowledge areas as diverse as artificial intelligence and machine learning techniques with computer security systems and applications. The course will allow to instill into students a unique knowledge in the very intense domain and will lead students towards getting much better prepared to their practical work ahead. It combines theoretical knowledge and practical skills development. Also, it advances students research, communication and presentation skills.

High quality teaching as evidenced by student and other faculty evaluations.

I have excellent student and other faculty evaluations of my teaching. In the figure below I am reproducing an example of the recent student evaluations of my teaching of the Capstone project class. Evaluation is out of 5 with red bars (the most left) representing my teaching against the Computer Science program (blue bars) average, College of Computing and Information Sciences (yellow bars) and RIT (green bars) averages.



I was nominated for the Eisenhart Outstanding Teaching Award 6 times
This award is the RIT's most visible recognition of outstanding teaching.

Samples of teaching materials

(available upon the request)

- Textbook for the course of Intelligent Security Systems (L. Reznik Intelligent security systems: How artificial intelligence, machine learning and data science work for and against computer security. IEEE Press-Wiley&Sons, ISBN-13: 978-1119771531, ISBN-10: 1119771536, 2022)
  - just published by Wiley – IEEE Press
- Curriculum materials for the course of Intelligent Security Systems – developed in the project funded by NSA
- Textbook "Fuzzy Controllers" (Newnes-Butterworth-Heinemann, Oxford-Boston, 1997, ISBN 0-7506-3429-4, 287 pp.) – focused on undergraduate students
- Computer educational kit in Fuzzy Systems (upper level and graduate courses)

Over last five years

- Course materials including lecture notes, assignments, student projects in all courses I taught at RIT

Supportive evaluation evidence

Publications based on my teaching experience:

Books

[1] **L. Reznik** Intelligent security systems: How artificial intelligence, machine learning and data science work for and against computer security. IEEE Press-Wiley&Sons, ISBN-13: 978-1119771531, ISBN-10: 1119771536, 2022

[2] **L.Reznik** *Fuzzy Controllers* Elsevier-Newnes, Oxford-Boston, 1997, ISBN 0-7506-3429-4, 287 pp.

Chapters in Books

[3] **L. Reznik**, "Computer Security with Artificial Intelligence, Machine Learning, and Data Science Combination," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.1-56, doi: 10.1002/9781119771579.ch1.

[4] **L. Reznik**, "Firewall Design and Implementation," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.57-108, doi: 10.1002/9781119771579.ch2.

[5] **L. Reznik**, "Intrusion Detection Systems," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.109-176, doi: 10.1002/9781119771579.ch3.

[6] **L. Reznik**, "Malware and Vulnerabilities Detection and Protection," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.177-246, doi: 10.1002/9781119771579.ch4.

[7] **L. Reznik**, "Hackers versus Normal Users," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.247-313, doi: 10.1002/9781119771579.ch5.

[8] **L. Reznik**, "Adversarial Machine Learning," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.315-335, doi: 10.1002/9781119771579.ch6.

[9] **L. Reznik**, "Front Matter," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.i-xxvi, doi: 10.1002/9781119771579.fmatter.

Conference Papers (peer reviewed)

[10] Killawala A., Khokhlov, I., Reznik L., “Computational Intelligence Framework for Automatic Quiz Question Generation”. In IEEE World Congress on Computational Intelligence, Rio de Janeiro, Brazil, 2018. (pp. 76-83). IEEE

[11] **V.Kreinovich, E. Johnson-Holubec, L.Reznik, and M. Koshelev** *Cooperative Learning is Better: Explanation Using Dynamical Systems, Fuzzy Logic, and Geometric Symmetries* , Vietnam-Japan Bilateral Symposium on Fuzzy Systems and Applications, Halong Bay, Vietnam, 30 September – 2 October, 1998, Proceedings/Eds. H.-P. Nguyen and O.Ario, Ha Noi, 1998, p.154 – 160

[12] **L.Reznik** *How To Teach Fuzzy Technology?* Proceedings of the First International Discourse on Fuzzy Logic and the Management of Complexity, January 15-18, 1996, Sydney, Australia, vol.1, p. 87 – 91

[13] **L. Reznik** *Fuzzy Technology Teaching: Some Experience,* presented to the Pacific Region Conference on Electrical Engineering Education, February 23 - 24, 1995, Marysville and published in the Conference Proceedings “Advancing Electrical Engineering Curricula To Reflect Current And Future Technologies” pp. 119 – 122

III. RESEARCH AND ITS SCHOLARLY APPLICATION

A. Research administration

Current activities:

Professional and academic committees:

1. Identity Ecosystem Standards Coordination Standing Committee (IESCSC) – voting member since August 2012, member of the Research and Development subcommittee
2. IEEE working group of the P1451.001(Recommended Practice for Signal Treatment Applied to Smart Transducers) – member since November 2012
3. Member of the International Biography Centre Advisory Committee – IBC, Cambridge, UK – since 1998
4. QS World University Rankings Expert – since 2015

Associate Editor
ACM Journal of Data and Information Quality

Member of the Editorial Board:

International Journal On Advances in Systems and Measurements,
International Journal On Advances in Internet Technology,
International Journal On Advances in Telecommunications

Member of International Program Committee (IPC): numerous including**:**
Program Committee Chair - ICWMC 2008, The Fourth International Conference on Wireless and Mobile Communications , July 27 - August 1, 2008 - Athens, Greece
Member:

AP2PS 2012,The Fourth International Conference on Advances in P2P Systems, September 23 – 28 Barcelona, Spain,

The international Conference on Mobile Communications and Pervasive Computing (MCPC 2009), Leipzig (Germany), 23-25 March 2009,

2008 International Conference on Networking, Internet and Mobile Communications (NIMC 2008), Glasgow, UK, 22-24 July 2008,

2009 Sensor Networks, Embedded Systems, and Pervasive Computing (SEP) track in the 20th IEEE International Conference on Computer Communications and Networks (ICCCN 2011), Maui, Hawaii, August 2011

The 1st International Conference on Pervasive Networked Services and Internet of Things, UK, August 2011

Reviewer: multiple journals and conferences including:

International Journal of Computational Intelligence Systems
IEEE Trans. On Instrumentation and Measurement
IEEE Trans. On Parallel and Distributed Computing
IEEE Sensors Journal
Sensors Journal
Journal of Parallel and Distributed Computing
Journal of Neural Networks
International Journal on Advances in Systems and Measurements,
International Journal on Advances in Internet Technology,
International Journal on Advances in Telecommunications
ICSNC 2012

2013 IEEE Conference on Instrumentation and Measurement technology
2013 International IEEE Joint Conference on Neural Networks

Research promotion:

Initiated and led an organization of the 1st GCCIS Conference on Computing and Information Sciences

Although the conference became the first college-wide research conference, it did not concentrate on presenting research results only. In line with the GCCIS policy, it presented the current state of scholarship, which covered research, pedagogy and professional development issues. The conference was organized as a multi-track event with presentations and discussions covering different issues from pure and academic research to teaching methodologies debates and professional presentations.

Was invited and delivered key research presentation at other Universities, Industry and Research meetings, e.g.

- Key presentation "What is hot in computer science (hints: Cybersecurity, AI and ML, Big Data) and what we can do therein (hints: Data quality and security, Intelligent security systems)" – see recordings at https://www.youtube.com/watch?v=GWK3Y2Ziqio) to the Colgate University Technology Immersion week 2022- see https://colgatecoders.github.io/cccPage/ for more information.
- Key presentation with my former student Dmitri Yudanov Heterogeneous Implementation of Neural Network Algorithms to the AMD Developer Summit, San Jose, November 11-13, 2013
- Key address From Big Data to Quality Data: What is the emerging sensor and network technology going to deliver next? to NetWare 2014 , an umbrella event incorporating a few international conferences on November 20, 2014 in Lisbon, Portugal

Was invited to participate in special meetings and workshops – by invitation only
e.g. over last year of 2023:
DARPA's AI Forward initiative (strategy development for AI for National Security)– Boston, MA, in August 2023
NSF Workshop on Directions for SaTC EDU Program at The University of Texas at Dallas in November 2023
ARO workshop on Metacognitive Prediction of AI Behavior – at ASU, Phoenix AZ – in November 2023

B. Research Projects and Directions (a sample)

Patent applications:
L. Reznik and S. Chuprov, "Federated Learning with A Compromised Unit Exclusion from Receiving Global Model Updates". *Provisional application No. 63/439,995 filed on January 19, 2023*
L. Reznik and S. Chuprov, "Network Adjustment based on Machine Learning End System Performance Monitoring Feedback". *Application No. 63/406,514 filed on September 14, 2022, converted in Sep. 2023*

Current projects:
PI on the project "Collaborative research: IDEAS lab: ETAUS: Smarter Microbial Observatories for Realtime ExperimentS (SMORES)"- funded by NSF (award # 2321652), Sep. 2023 – Aug. 2026, budget: total: $1.5M, my part: $323,419
This is a joint project to be performed in collaboration between Harvard University, Rochester Institute of Technology, Florida International University and University of Georgia.
The project will study marine sediments, which play a critical role in natural carbon sequestration. They harbor a diverse community of microbes and animals that govern both carbon sequestration and remobilization. Many of these taxa are sensitive to oxygen (oxygen is typically absent below a few centimeters), yet physical processes such as tidal pumping can drive oxygen deeper into some coastal and

deep ocean sediments (especially sandy or fractured sediments). To date we know little about how these oxygen dynamics affect carbon sequestration/remobilization and related biogeochemical processes. Here we propose to develop a novel seafloor sensor/sampler array to better understand how tidal pumping and subsurface currents influence seafloor oxygenation and sedimentary carbon cycling (e.g. microbial carbon degradation, the extent of animal grazing on microbes, etc).

I am responsible for developing “smarter” control systems that use machine-learning models (MLM) to make intelligent predictions about when and where to best sense/sample based on the historical and real-time data. This is a marked advance over existing approaches, and the development of MLM-based controllers will enhance the efficacy of any unattended remote deployment, minimizing excess power consumption and the collection of sub-optimal samples.

Recent projects:

PI on the project “Self-learning capabilities for a mission oriented data quality and security assurance in military IoT systems” – funded by USMA/DoD (award # W911NF2010337), 2020-22, budget $85,935.

The goal of this project is to include intelligent self-learning capabilities into a proof-of-the-concept design prototype of the IoT data collection and security evaluation framework, that would enable structural and procedural autonomic re-adjustments of the data sources, data streams communication and fusion in order to assure the required DQS for a particular mission at the data point of use. Unlike conventional IoT data collection systems, the developed procedures deliver data quality and security level estimates that would significantly simplify further data analysis on the battlefield. To make the procedures operational in real time and in a dynamic environment we developed and employed artificial intelligence and machine learning novel models andtechniques.

One book and five papers were published. Two PhD students were supported.

PI on the project “Security evaluation and improvement of the personal cyberinfrastructure with new tools and education development” –funded by US Civilian Research and Development Foundation -CRDF Global (award # G-202102-67515), 2021-22, budget total: $149,867, my part: $74,995.

With the international economy and the whole society getting increasingly computerized and mobile, endpoint security as well as a human factor are frequently overlooked in cybersecurity research and education. The project merged together research and educational activities addressing those issues in order to dramatically improve cybersecurity of the common infrastructure and the overall life of general population. Unlike other projects, this one focuses on improving security of the cyberinfrastructure first mile that resides in the ordinary people’s homes and hands.

The project was performed by the international diverse team, which included researchers, educators and students. The team was based at the Global Cybersecurity Institute and College of Computing and Information Sciences at RIT, New York, USA and KPI University, Kyiv, Ukraine and collaborated with other universities.

This project concentrated on an integration of various approaches, methodologies and tools in improving the cyberinfrastructure security, considering both technological and organizational factors. It not only produced research and development results in security improvement but also made efforts to develop the taskforce to promote and implement those results into the real life. By fusing research and education, the project grows strong on both sides. Technical report on old oscilloscope data analysis was produced. The new research results were analyzed and prepared to the IEEE International Conference on Computer Communications (INFOCOM’22), 2-5 May 2022, London UK. Four more papers were published. Five Android application new versions were updated and submitted to Google Play. Curriculum materials (course descriptions, lecture slides and notes) were delivered to the Ukrainian team. The structure of a course was formed and discussed, Syllabus was adapted to the Ukrainian side.

PI on NSF grant ”CICI: Data Provenance: Data Quality and Security Evaluation Framework for Mobile Devices Platform” (award ACI-1547301), 2016-21, budget: total: $499, 235, my part: $250,052

Intellectual Merit: We proposed and investigated a novel data management scheme that integrates data quality and security evaluation into data collection and communication processes, demonstrated significant variations between the DQS indicator values in different devices of the same model, demonstrated that DQS monitoring could be employed not only for detecting anomalies in measurements, but also for identifying sensors and devices that are not functioning properly, tested a method of sensor- originated data security evaluation for Android-based devices that evaluates the possibility of various data manipulation attacks and takes into account already discovered system vulnerabilities, as well as possible methods of data falsification and manipulation (see the Webinar recordings and the publications for more results). We have developed the knowledge base of smartphone sensors that includes data about sensors embedded in mobile devices. The current version contains the processed data and is available at dataqualitylabs.com.
Broader Impacts: Four new Android apps have been developed and released on Google Play and 23 papers were published in various conferences and journals. One PhD and 26 Master’s Capstone projects and a few Independent Study Master’s projects on topics directly related to this project have also been successfully completed and defended at RIT. PI Reznik used this project results in the preparation of the Intelligent Security Systems course. That project was funded by the NSA (award H98230-17-1-0200). Also, the project results were included into the textbook authored by PI Reznik that was published this year by Wiley-IEEE Press.

PI on NSA grant “Intelligent security systems: course curriculum development” - funded by NSA (award # H98230-I7-l-0200), 2017-18, budget: $118,926.
The project designed a curriculum, developed course materials, tested and evaluated them in real college classroom settings, prepared and submitted them for dissemination of a college level course on Intelligent Security Systems.
In order to facilitate interconnections with other courses and its inclusion into the national Cybersecurity curricula, the course is composed of nine separate modules. Five modules cover the specialized topics including: a review of the modern state of the cybersecurity and the current problems and approaches; firewall design; intrusion detection systems; anti-malware methods and tools; hacking activity and attack recognition and prevention. Other modules provide additional support to assist in course teaching preparation, such as test and exam questions, course project and research assignment specifications, and tool presentation descriptions. Each module is further subdivided into micromodules. Altogether, the modules provide an instructor with a comprehensive set to initiate the course.
This course merges together various knowledge areas as diverse as artificial intelligence and machine learning techniques with computer security systems and applications. The course will allow to instill into students a unique knowledge in the very intense domain and will lead students towards getting much better prepared to their practical work ahead. It combines theoretical knowledge and practical skills development. Also, it advances students research, communication and presentation skills.

Previous research projects:

Fundamental research

Feasibility study of applying new emerging intelligent methods such as expert systems, fuzzy logic, neural networks and interval analysis for expression and evaluation of the measurement uncertainty. Fuzzy and interval theory models are examined for describing some uncertainty components. Research towards the creation of a general theory of perception, measurement and quality evaluation.

The evaluation of uncertainty of measurement is a central concern in all quantitative fields of measurements. The International Standards Organization (ISO) “Guide to the Expression of Uncertainty in Measurement” establishes a consistent and widely agreed upon methodology based on probability and statistical theories. Since the early 90’s and in particular since publication of the ISO Guide, there has been a widening recognition that uncertainty of measurement is no less critical than the value of the measurement result itself. In parallel with this the development of more rigorous, systematic and sophisticated approaches to its evaluation, based on the ISO Guide, have led to an increase in the complexity of its application. The rationale for intelligent technologies applications in the modern metrology environment is driven by:

- increasingly higher resolution and higher sensitivity measurements, which require more sophisticated physical models for their description,
- extensive pre- and post-processing of measurement data so that the final measurement result is many steps removed from the initial measurands, and
- more sophisticated mathematical treatment of measurement uncertainty, currently based on the ISO Guide and probability framework.

I believe that a measurement has to be considered as a particular type of information collection procedure that involves an application of certain instruments and as such should be modeled as a special case of information perception and presentation. Furthermore, a neuro-fuzzy approach can produce models better fit to describe measurement and more generally perception uncertainty for both qualitative and quantitative measurements with applications ranging from engineering to the social sciences. This research will lead to generalizing existing intelligent models and methods into a general theory of perception that will be applicable across all the fields and disciplines. It will facilitate the development of artificial intelligence methods aiming at building human-computer synergetic systems.

Results achieved so far
uncertainty sources are classified in regard to the feasibility of intelligent model application,
fuzzy and neural models are proposed for description of some uncertainty components,
fuzzy methods are investigated for processing uncertainty and measurement results.

Development of novel model based security enhancement and sensor network protocols
Sensor networks is a novel technology providing an improved avenue of an effective and efficient collecting, communicating and processing more information about the monitored objects and/or environment. This information wealth could be applied for the advancement of the technology itself. This research aims at enhancing accuracy, reliability and security in sensor networks based on a development and an application of monitored objects and environment models. The models should be made available from external sources or generated during the sensor network operation, and sensor results Accuracy improvement is achieved based on the fusion of the measurements with the models. Reliability and security enhancement is achieved by detecting maliciously altered results or malfunctioning channels by comparison of the current measurement results against the model information. Both conventional and intelligent methods are used for building multilevel models and their multilayer realization. In this research potential solutions are investigated and their characteristics are studied.

Feasibility study of measurement methodology for computer security evaluation
Rationale for research
Information assurance and computer security has become one of the most important aspects of information technology and the hottest research field. However, we still have not developed the procedures on how to measure and /or evaluate security and its attributes. Designers often apply information assurance or security technology to systems without the ability to evaluate the impact of those mechanisms to the overall system. And as usual our inability to measure definitely acts as a main constraint to our ability to improve.
Computer and network system security is recognized as a complex issue with no clear definition, with the research domain having no sharp boundaries. Over recent years one could see substantial changes in the security problems pattern and their significance on a national and international scenes. This area will serve as a major application of the previous research with fuzzy and neural networks models being investigated for applications in measurement and evaluation of computer security properties.

Theoretical research

Security and reliability enhancement in sensor networks based on signal anomaly and change detection

The project is devoted to the development of novel multilayer sensor networks protocols and utilities enhancing reliability and security based on detection of anomalies in sensor signals, which is due to malfunctioning or malicious actions. The system utilizes a time based multi-layer perceptron neural network methodology to predict sensor outputs in order to determine if the sensor outputs are novel. In addition to the anomaly detection system, a modification to a standard neural network function predictor is proposed that allows the anomaly detection system to quickly learn to accurately predict next sensor outputs. The parameter choice and the relationship between the threshold values and false alarm and missing attack rates are studied and the recommendations are provided.

Neural networks for cognitive sensor networks

Cognition, or an ability of perception, reasoning and judgment is a fundamental feature of natural intelligence, which a modern technology has not been able to reproduce in full capacity. Wireless sensor networks provide a new technological support for an increase in an amount and quality of information that might be collected and communicated in complex adaptive systems. Their application may significantly increase the level of intelligence in system design and implementation. One might get an opportunity to move up the overall intelligence into the levels where effects of cognition will start kicking in and producing marvelous results of global system functions optimization comparable with ones observed in natural intelligence. This goal can be approached through an advancement of modern artificial intelligence methodologies toward making them more effective in terms of their performance in applications and efficient in relation to resource consumption. The project puts forward a concept of cognitive sensor networks, which should be able to perform self-organizing and self-reconfiguring depending on the given goal. It investigates a feasibility of artificial neural networks application for its realization through the design of novel hierarchical configurations imitating the structural topology of brain-like architectures. They are composed from artificial neural networks distributed over network platforms with limited resources. The project examines a cognition idea based on its implementation through the signal change detection. The novel multilevel neural networks architectures are designed and tested in sensor networks built from Crossbow Inc. sensor kits. The results are compared against conventional multilayer perceptron structures in terms of both functional efficiency and resource consumption.

Model learning for signal change detection in sensor networks

Wireless Sensor Networks (WSN) collect and make available a huge amount of information that could be used to build up the models of monitored objects and environment. The models could be supplied a priori or generated during the WSN operation. The model's application in network protocols design may significantly improve WSN power consumption and deployment time, reliability and security. The paper investigates the development of multilayer intelligent protocols capable of learning and self-modification based on the models created during their operation. In particular, it focuses on the development and implementation of the intelligent utility for signal change. Its realization could be adjusted to the resources available and may range from a simple comparison against predetermined thresholds to checking up rules and employing machine learning techniques based on artificial neural networks. In order to reduce resource consumption, the novel neural network topology allowing for its distribution over the sensor network platform is introduced and investigated. Different design options are compared through computer simulation.

Design methodology of embedded intelligent systems

Rationale for research

Current competition on the embedded computer market and product development limitations have resulted in new combinations of design constraints, such as very good performance at very low power and very low cost. Technically, this often translates into fast specialized processors using very small memories. There is a strong need in a design methodology providing tools for the fast capture of the designer's expertise on the one hand and for quick low cost design implementation on embedded microprocessors on the other hand.

The proposed design way includes a formulation of design ideas with the help of fuzzy rules initially and their consequent optimization with neural networks and evolutionary programming for specified implementation constraints. This methodology allows for combining the fuzzy system capability of capturing and expressing a knowledge frame with the neural network learning and optimization abilities. It should develop a practical, goal-oriented approach with comprehensive consideration of all problems involved in reaching the results from an initial design knowledge formulation to the implementation.

Results achieved so far:

recommendations on fuzzy system design

fuzzy system implementation on general purpose and specialized microprocessors

approximation of fuzzy system with neural networks (see below)

Investigation of a neural network (NN) application for a fuzzy system (FS) implementation after its formulation by an expert with fuzzy rules.

Rationale for research

This research studies NN capabilities of a practical, cost-effective FS implementation and aims at eventual development of a comprehensive methodology, covering all aspects from an initial FS design through to its microprocessor implementation. This approach allows for complementing the convenience of a fuzzy rules design frame with NN flexibility. In order to develop such a methodology different NN types and FS structures have to be analyzed and compared. The main problems, which are addressed are:

what type of NN should be chosen for a FS approximation,

how the NN parameters influence an approximation and implementation quality,

which FS structures are the most suitable for this approach.

Results achieved so far:

radial basis network and multilayer perceptron are investigated for their feasibility of application in a FS approximation,

the choice of some NN parameters (spreading factor, basis functions) has been studied,

modification of some parameters is proposed to simplify implementation

Development of a practical user-friendly methodology of a fuzzy controller (FC) design

Rationale for Research

Attempts to develop systematic FC design procedures date back to the earliest years of the theory and different approaches have been proposed. Until now, the design process has been mainly conducted in an intuitive, ad-hoc manner. FC design is still more an art than a technology, the area where a designer's experience plays the main role. There is a strong need to develop a unifying methodology covering all FC design aspects from its initial formulation with fuzzy rules by an expert, through to an implementation on a low cost, general purpose microprocessor.

Results so far:

FC design methodologies have been researched and classified,

practical recommendations on the choice of FC structure and parameters have been developed,

an initial choice of parameters (membership functions, scaling factors) has been researched,

some similarity between the choice and tuning of FC parameters and PID-coefficients have been discovered and proposed to employ in FC design.

Applications

Evaluation of mobile device security

This project develops a framework to evaluate the trustworthiness of the individual components in a mobile system, as well as the security of the entire system. The major components under investigation are installed applications, devices and networks of devices. Given this diversity and multiple levels of a real mobile system, we aim at designing a hierarchical evaluation methodology, which enables the combination of various metrics and allows to verify the particular metric for each component based on the metrics for others.

The project first will develop this idea for individual applications and Android-based smartphones. The methodology involves two stages: initial evaluation and verification. In the first stage, an expert rule system is used to evaluate the metrics at the lowest level of the hierarchy. In the second stage, the metrics are verified by comparing data from components and an evaluation is produced for the combined system.

Resources aware intrusion detection design based on neural networks
High learning and adaptation ability of intelligent agents based on artificial neural networks (ANN) has made them a popular tool in design and implementation of intrusion detection systems (IDS). However, ANN might consume significant resources during their retraining because of network changes. This requirement becomes crucial when intensive attacks occur and the resources availability drops down. The project investigates the design of ANN structures that may reduce the resource consumption without a substantial performance degradation. It conducts empirical studies examining a variety of design solutions, such as the choice of the ANN architecture and its parameters, the choice of an ANN fully connected topology versus a partial connectivity, the IDS design in a form of a hierarchical system of heterogeneous ANN-based agents. While a wide set of parameters are investigated, the particular attention is paid to the choice of ones responsible for the resource consumption such as the training set size and the training time in an ANN application, the number of generations in genetic algorithms, the number of agents in a multiagent systems. The results are analyzed and design recommendations are provided. The fully connected ANN structure optimized with genetic algorithms has been found to achieve the best performance, while partial connectivity might save resources without a significant sacrifice of possible accomplishments. At the same time, the parameters of genetic algorithms could be chosen based on the resources (time and memory) availability.

Design of a distributed framework for sensor networks anomaly detection.
The project aims at facilitating design and implementation of the sensor networks anomaly detection system, which would allow the integration of sensor data streams from a number of aggregate nodes with data collection components, data display components and anomaly detection components. Components will be added and removed from the system during runtime, and components can be upgraded to a newer version on the fly. The architecture is scalable, allowing components to be spread across multiple computing devices. The project focuses on developing a system of distributed components that can be managed from a central (or several) administrative consoles. User will be able to create components locally or remotely, connect and configure them, replace them, upgrade them, move them from one node to another. Classes will be transferred to the remote nodes as needed.

Design of the Sensor Network Anomaly Detection System (SNADS).
SNADS is designed as an implementation platform for contents based security enhancement protocols in sensor networks. SNADS system is aimed to be modular, extensible, robust, and scalable. By providing a generic sensor abstraction and sensor-definable configuration mechanisms, SNADS allows for simple, secure management of arbitrary sensor networks. By supporting network nodes with different hardware and software configurations, SNADS will be a versatile cross platform tool. Modularity is achieved via a central signaling system, which allows components to work together. This setup allows for simple runtime reconfiguration of the SNADS system and minimizes the damage, which a malfunctioning component can cause.

Modified time-based multilayer perceptron structure for various applications
The project develops applications of a modified time-based multilayer perceptron (MTBMLP), which is a complex structure composed from a few time-based multilayer perceptrons with a reduced connectivity. This structure is one of intelligent agents developed for SNADS and included therein. The modification reduces connections, isolates information for each function and produces knowledge about the system of functions as a whole. This neural network is applied for novelty and change detection in signals delivered by sensor networks and for edge detection in image processing. In both applications a MTBMLP is utilized for function predictions and, after a further structure development is implemented, for an error prediction

also. In sensor network applications, a number of experiments with Crossbow sensor kits and the MTBMLP acting as a function predictor have been conducted and analyzed for detecting a significant change in signals of various shapes and nature. A series of experiments with Lena image have been conducted for edge detection applications. The results demonstrate that MTBMLP is more efficient and reliable than other methodologies in sensor network change detection and that its application in change detection is more effective than in edge detection.

Intelligent real-time environment adaptation for power efficient sensor networks
The project develops an intelligent, dynamic power conservation scheme for sensor networks, in which the sensor network operation is adaptive to both changes in the objects under measurement and the network itself. The conservation scheme switches sensor nodes between a sleep and an active mode in a manner such that the nodes can maximize the time they spend in a power-efficient sleep state, which corresponds to a non-measuring and/or non-transmitting mode, while not missing important events. A switching decision is made based on changes (or their absence) in the signals sensed from the environment by an intelligent agent that has been trained to determine whether or not a special event has occurred. This intelligent agent is based on a novel neural network topology that allows for a significant reduction in the resource consumption required for its training and operation without compromising its change detection performance. The scheme was implemented to control a sensor network built from a number of Telos rev. B motes currently available on the market. Power consumption measurements taken in a laboratory environment confirm that use of the designed system results in a significant extension of sensor network lifetime (versus “always on” systems) from a few days to a few years.

Fuzzy controller design for industrial applications
A universal adaptive fuzzy controller structure allowing for on-line tuning of the scaling factors (both input and output) has been developed and tested by computer simulation and in real control of a synchronous power generator. The structure of this FC is system independent. Its on-line operation supports the overall control loop robustness under various operating conditions. The structure’s application in different projects is expected.

Expert system shell development for computer security evaluation applications
The project develops the universal fuzzy Basic Expert System Shell (BESS). The goal of the Bess system is to provide a fuzzy expert system development framework that is not only language independent, but is not attached to a specific expert system shell either. An expert system that is written in Bess may be written exactly once dependless on how many implementations and modifications will be developed; the only changes required in the system are the additions of new data, or the modifications of existing data. This arrangement completely separates the knowledge and data bases in an expert system. Bess is built on top of a simple, easy to use XML compliant language for describing expert systems in terms that are commonly used for this purpose. This software is used for developing an expert system for computer security evaluation.

Fuzzy logic applications in mobile communications and computing
The method of fuzzy logic application for mobile locating and positioning has been proposed. Different implementations have been simulated. Simulation results prove the advantage of the method over the conventional ones. Fuzzy handover method is researched. Further development based on an application of extra information available is anticipated.

Intelligent techniques for electrical power transformer state monitoring and prediction.
In order to predict the additional load that may be placed on a transformer it is necessary to know the temperature regime of different winding parts. The research examines the possibility of neuro-fuzzy models application in an identification of the transformer temperature behavior patterns. The derived models describe the relationship between the spotted temperatures and external factors such as load and ambient conditions. These models are derived as a neuro-fuzzy system, initially formulated as a fuzzy rules frame

based on conventional knowledge. Later the models are tuned using measurement results applied to neural networks. The proposed algorithm has been tested by computer simulation and verified by practical experiments with real transformers.

AI techniques application in electrical energy contracting in the competitive electricity market.
Neuro-fuzzy techniques are applied in the development of an effective tool allowing market participants to estimate spot prices and to reduce the risk of electricity contracting. Two methodologies are to be investigated. One is based on the application of fuzzy logic techniques to incorporate human attitudes to a market risk analysis and imprecision of linguistic modeling. Another one is based on a combination of fuzzy systems and neural networks and an application of ANFIS systems for modeling the dependence of the spot price upon the predicted demand. The case is tested with real data from the Victorian electricity market.

Development and implementation of the industrial fuzzy logic controller for a power generator.
The fuzzy logic controller was designed and implemented in the excitation control of a synchronous generator connected to an infinite bus through a transmission line. The adaptive fuzzy excitation control system replaces both the automatic voltage regulator and the power system stabilizer. It has been achieved through an introduction of the pre-control stage where a single parameter representing the rotor angle and the terminal voltage was introduced. The control system is implemented on a DSP processor and applied to control a laboratory prototype generator. The reported test results demonstrate both efficiency and robustness of the structure developed.

Development and implementation of the industrial fuzzy logic controller for a multi-zone domestic HVAC embedded system.
The control system has been designed to facilitate the commercial viability, while also achieving robustness in multi-zone control. The system allows for a distributed control, whereby the fuzzy controllers operation can be disseminated to prevent a large number of zones overloading the master controller. Each fuzzy controller has similar implementation requirements, simplifying software and communication.

IV. LIST OF PRODUCTS

Summary:

	1992-2001	2002-11	2012-23
Books	2	3	2
Chapters in books	5	7	7
Refereed journal articles	7	7	7
Refereed conference papers	44	32	41
Apps developed	-	-	6
Data collections	-	-	2
Patent applications	-	-	2

Products:

Applications developed

[1] **Igor Khokhlov, Leon Reznik** Sensor Selector- available at Google Play – see https://play.google.com/store/apps/details?id=edu.rit.dataqualitylab.sensorselector, ver. June 3, 2022

[2] **Igor Khokhlov, Leon Reznik** System Security Evaluation application - available at Google Play – see https://play.google.com/store/apps/details?id=com.igorkh.trustcheck.securitycheck , ver. 1.5, February 16, 2021

[3] **Sahil Ajimera, Igor Khokhlov, Leon Reznik** Sensor Quality Assessment - available at Google Play – see available at Google Play – see https://play.google.com/store/apps/details?id=com.dataqualitylab.sensorquality, ver. 1.1, January 20, 2020

[4] **Igor Khokhlov, Leon Reznik** Road pothole reporter, - available at Google Play – see https://play.google.com/store/apps/details?id=sdh.application.reportthepotholes, ver. Jan. 9, 2020

[5] **Igor Khokhlov, Leon Reznik** Smartphone Data Collection Tool, - available at Google Play – see https://play.google.com/store/apps/details?id=com.dataqualitylab.collectinfo.collectinfo, ver. 1.11, December 7, 2018

[6] **Igor Khokhlov, Leon Reznik** System Security Evaluation: Cloud version - available at Google Play – see https://play.google.com/store/apps/details?id=com.igorkh.trustcheck.securitycheckcloud, ver. 1, November 1, 2018

[7] **Igor Khokhlov, Milan Bhaskar, Leon Reznik** Detector of Unverified Apps - available at Google Play – see https://play.google.com/store/apps/details?id=dataqualitylab.rit.ver_app_finder, updated March 12, 2018

[8] **Milan Bhaskar, Igor Khokhlov, Leon Reznik** Unverified App Finder - available at Google Play – see https://play.google.com/store/apps/details?id=project.afinal.rit.capstone_milans_app, updated March 2, 2018

Data collections

[9] Sensors incorporated in mobile devices, their characteristics and quality evaluation, 2018 - 21 – available at http://www.dataqualitylabs.com/downloadDataFor/Sensor%20Info

[10] Personal smartphones security evaluation, 2018-20 – available at http://www.dataqualitylabs.com/downloadDataFor/Security%20Info

Patent pending applications:

[1] **L. Reznik, S. Chuprov**, **R. Zatsarenko** `` Federated Learning with A Compromised Unit Exclusion from Receiving Global Model Updates". *Application No. 63/439,995 filed on January 19, 2023, transferred to non-provisional in Jan. 2024- pending*
[2] **L. Reznik and S. Chuprov**, ``Network Adjustment based on Machine Learning End System Performance Monitoring Feedback". *Application No. 63/406,514 filed on September 14, 2022- transferred to non-provisional in Sep. 2023- pending*

Publications:

Books

[1] **L. Reznik** Intelligent security systems: How artificial intelligence, machine learning and data science work for and against computer security. IEEE Press-Wiley&Sons, ISBN-13: 978-1119771531, ISBN-10: 1119771536, 2022

[2] **L. Reznik and Popescu M./Eds.** Proceedings of 4th International conference on wireless and mobile communications 2008 (ICWMC 2008), 27 July - 1 August 2008, Athens, Greece, IEEE 2008, ISBN CD:978-0-7695-3274-5, doi: 10.1109/ICWMC.2008.

[3] **L.Reznik/Ed**. *Advancing Computing and Information Sciences*. RIT Cary Graphic Arts Press, 2005, ISBN 1-933360-05-4

[4] **L.Reznik, V.Kreinovich/Eds**. *Soft Computing in Measurement and Information Acquisition*, Springer Verlag, Heidelberg-New York, 2003, ISBN 3-540-00246-4, 284 pp.

[5] **L.Reznik, V.Dimitrov, J.Kacprzyk/Eds**. *Fuzzy System Design: Social and Engineering Applications,* Physica Verlag, Heidelberg-New York, 1998, ISBN 3-7908-1118-1, 334 pp.

[6] **L.Reznik** *Fuzzy Controllers* Elsevier-Newnes, Oxford-Boston, 1997, ISBN 0-7506-3429-4, 287 pp.

Chapters in Books

[7] **L. Reznik**, "Computer Security with Artificial Intelligence, Machine Learning, and Data Science Combination," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.1-56, doi: 10.1002/9781119771579.ch1.

[8] **L. Reznik**, "Firewall Design and Implementation," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.57-108, doi: 10.1002/9781119771579.ch2.

[9] **L. Reznik**, "Intrusion Detection Systems," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.109-176, doi: 10.1002/9781119771579.ch3.

[10] **L. Reznik**, "Malware and Vulnerabilities Detection and Protection," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.177-246, doi: 10.1002/9781119771579.ch4.

[11] **L. Reznik**, "Hackers versus Normal Users," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.247-313, doi: 10.1002/9781119771579.ch5.

[12] **L. Reznik**, "Adversarial Machine Learning," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.315-335, doi: 10.1002/9781119771579.ch6.

[13] **L. Reznik**, "Front Matter," in *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security* , IEEE, 2022, pp.i-xxvi, doi: 10.1002/9781119771579.fmatter.

[14] **L. Reznik** *Measurement Theory and Uncertainty in Measurements: Application of Interval Analysis and Fuzzy Sets Methods* In: Handbook of Granular Computing /Ed: W. Pedrycz, A.Skowron and V.Kreinovich , Wiley and Sons , Chichester, England, 2008, ISBN 978-0-470-03554-2, pp.517-532

[15] **Von Pless G., Al Karim T., and Reznik L.** *Modified Time-Based Multilayer Perceptron for Sensor Networks and Image Processing Applications.* In *Advancing Computing and Information Sciences*. Reznik L. /Eds. RIT Cary Graphic Arts Press, pp. 27-33, 2005, ISBN 1-933360-05-4

[16] **Yampolskiy R., Novikov D., and Reznik L.** *Performance of MLP and RBF in Character Recognition Utilizing Fuzzy Zoning Feature*. In *Advancing Computing and Information Sciences*. Reznik L. /Eds. RIT Cary Graphic Arts Press, 2005, pp. 34-41, ISBN 1-933360-05-4

[17] **Samant A., Reznik L., Carithers W.** *Using System Call Analysis to Stop Evasion Attacks*. In *Advancing Computing and Information Sciences*. Reznik L. /Eds. RIT Cary Graphic Arts Press, 2005, ISBN 1-933360-05-4

[18] **L.Mari and L.Reznik** *Uncertainty in Measurement: Some Thoughts about its Expressing and Processing* In L.Reznik and V.Kreinovich/Eds. *Soft Computing in Measurement and Information Acquisition*, Springer, Berlin-Heidelberg-New York, 2003, ISBN 3-540-00246- 4, pp. 1-9

[19] **L.Reznik** *General Principles and Purposes of Computational Intelligence* in *Systems Science and Cybernetics*, [Ed. F. Parra-Luna], In: Encyclopedia of Life Support Systems, Developed under the Auspices of the UNESCO, EOLSS Publishers, Oxford, UK, 2003 (available on-line at http://www.eolss.net/)

[20] **L.Reznik** *Neuro-Fuzzy Control Applications: Looking for New Areas and Techniques?* In:Fuzzy Logic: A Framework for the New Millennium Korotkich V. and V.Dimitrov/Eds. Physica Verlag, Heidelberg – New York, 2002, ISBN 3-7908-1425-3, p.337 - 351

[21] **G. Solopchenko, V.Kreinovich, L.Reznik** *Development of Mathematical Structure of the Modern Measurement Science* In: Measurement Science - a Discussion, K.Kariya and L. Finkelstein /Eds. Ohmsha Ltd. and IOS Press, Amsterdam, Oxford, Tokyo, Washington, 2000, ISBN 4-274-90398-2 and 1-58603-088-4, p.23-36

[22] **L. Reznik** *What Is Intelligent Measurement*? In*:* Computing with Words in Information /Intelligent Systems, L.A. Zadeh and J.Kacprzyk/Eds. Physica Verlag, Heidelberg – New York, 1999, ISBN 3-7908-1217-X, p.78 - 89

[23] **L.Reznik** *Fuzzy Controller Design for Different Applications: Evolution, Methods, and Practical Recommendations* In: *Fuzzy System Design: Social and Engineering Applications*, L. Reznik, V.Dimitrov, J.Kacprzyk/Eds. Physica Verlag, Heidelberg- New York, 1998, p.185-201

[24] **O.Ghanayem and L. Reznik** *A Universal Approach to Adaptive Fuzzy Logic Controller Design With an Application to a Power Generator Excitation Control* In: *Fuzzy System Design: Social and Engineering Applications*, L. Reznik, V.Dimitrov, J.Kacprzyk/Eds. Physica Verlag, Heidelberg – New York, 1998, p. 287-308

[25] **L.Reznik** *Intelligent Measurement: How to Achieve?* In: Gorodetsky A.E. and Kurbanov V.G./Eds. *Physical Metrology: Theory and Application Aspects*, St.Petersburg, KN Publishers, 1996, pp.86 - 106 (in English and Russian)

Journal articles (refereed)

[26] **Sergei Chuprov, Raman Zatsarenko, Leon Reznik, and Igor Khokhlov** (2024). Data Quality Based Intelligent Instrument Selection with Security Integration. ACM Journal of Data and Information Quality Vol. 16, Iss. 3, Article 15 (September 2024), 24 pages, doi: 10.1145/3695770

[27] **Chuprov, S.; Belyaev, P.; Gataullin, R.; Reznik, L.; Neverov, E.; Viksnin, I**. Robust Autonomous Vehicle Computer-Vision-Based Localization in Challenging Environmental Conditions. *Appl. Sci*. 2023, *13*, 5735. Doi: 10.3390/app13095735I.

[28] **I. Khokhlov, L. Reznik and S. Chuprov, "**Framework for Integral Data Quality and Security Evaluation in Smartphones", IEEE Systems Journal, June 2021, vol. 15, iss. 2, pp. 2058-2065, doi: 10.1109/JSYST.2020.2985343,

[29] **I. Khokhlov, L. Reznik and S. Ajmera**, "Sensors in Mobile Devices Knowledge Base," in *IEEE Sensors Letters*, vol. 4, no. 3, pp. 1-4, March 2020, Art no. 5500404. doi: 10.1109/LSENS.2020.2975161

[30] **Alrubaye H. , Mkaouer M., Khokhlov, I., Reznik L., Ouni A., Mcgoff J**. Learning to recommend third-party library migration opportunities at the API level, Applied Soft Computing, vol. 90, pp.106-140, 2020

[31] **A. Heyman, L.Reznik, M.Negnevitsky, A. Hoffman** Fuzzy System Design for Security and Environment Control Applications, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 23, Suppl. 1 (December 2015), pp. 43-56

[32] **K. K. Semenov, L. Reznik, and G. N. Solopchenko** Fuzzy Intervals Application for Software Metrological Certification in Measurement and Information Systems, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 23, Suppl. 1 (December 2015), pp. 95−104

[33] **L. Reznik, S.E. Lyshevski** Data Quality Indicators Composition and Calculus: Engineering and Information Systems Approaches, Sensors & Transducers, Vol. 185, Issue 2, February 2015, pp. 140-148 (also available online at http://www.sensorsportal.com/HTML/DIGEST/february_2015/Vol_185/P_2612.pdf)

[34] **G.P. Timms, P.A. de Souza, Jr., L. Reznik and D. V. Smith** Automated Data Quality Assessment of Marine Sensors, Sensors 2011, 11(10), p.9589-9602

[35] **L. Reznik, Von Pless, G.; Al Karim, T**. *Distributed Neural Networks for Signal Change Detection: On the Way to Cognition in Sensor Networks*, IEEE Sensors Journal, Volume 11 , Issue 3, March 2011, pp. 791-798

[36] **L. Reznik, M. J. Adams, and B. Woodard** *Intelligent Intrusion Detection Based on Genetically Tuned Artificial Neural Networks*, Journal of Advanced Computational Intelligence and Intelligent Informatics, Vol.14, No.6 pp. 708-713, 2010

[37] G.**N.Solopchenko, K.K. Semenov, V.Kreinovich and L.Reznik** *Measurement's Result and its Error as Fuzzy Variables: Background and Perspectives*, Key Engineering Materials, vol. 437, May 2010, pp 487-491

[38] **J. Podpora, L.Reznik , and G. Von Pless**, *Intelligent Real Time Adaptation for Power Efficiency in Sensor Networks*, IEEE Sensors Journal, vol.8, issue 12, December 2008, pp.2066 – 2073

[39] **L.Reznik and V.Kreinovich** *Fuzzy Models in Measurement*, IEEE Transactions on Fuzzy Systems, vol. 16, No.4, August 2008, pp. 851-862

[40] **D. Novikov, R. V. Yampolskiy, L. Reznik**. *Traffic Analysis Based Identification of Attacks*. International Journal of Computer Science & Applications (IJCSA), vol. 5, Issue 2, 2008, pp.69-88

[41] **L.Reznik and K.P.Dabke** *Measurement Models: Application of Intelligent Methods,* Measurement, 2004, vol. 35, pp. 47-58

[42] **L.Reznik and S. Spiteri** *Embedded Smart Controller for an Industrial Reefer Refrigeration*, Australian Journal of Intelligent Information Processing Systems, vol.7, No.1/2, 2001, pp. 52-57

[43] **A.Little and L.Reznik** *Improving the Approximation Smoothness of Radial Basis Neural Networks* Journal of Advanced Computational Intelligence, vol. 4, No. 6, 2000, pp.417-420

[44] **L.Reznik, O. Gnanayem and A. Bourmistrov** *PID plus Fuzzy Controller Structures as a Design Base for Industrial Applications*, Engineering Applications of Artificial Intelligence, 2000, vol. 13, No.4, p. 419-430

[45] **A.T. Popov, H. Nguyen, L.Reznik** *An Application of Fuzzy Mathematical Morphology to Interval-Valued Knowledge Representation: A Remark* Reliable Computing, 1998, No. 3, p. 283-290 - 20%

[46] **L.Reznik** *Controller Design: The Combination of Techniques***,** Neural Network World, 1996, vol. 6, No. 4, pp. 691 - 699

[47] **L.Reznik and A.Little** *Fuzzy Controller Design From A Practitioner's Point Of View - The Review of Methodologies*, Australian Journal of Intelligent Information Processing Systems, 1995, vol.2, No.4, pp.1- 9

[48] **L.Reznik and J.Shi.** *Fuzzy Controller Design From A Practitioner's Point Of View - Membership Fuction Choice* , Australian Journal of Intelligent Information Processing Systems, 1995, vol.2, No.2, pp.38 - 46

[49] **L. Reznik, G. Britov** *On Dynamics of Fuzzy Discrete Systems*. AUTOMATION AND REMOTE CONTROL, 1987, v. 48, 8, p.185-188

[50] **L. Reznik** *Fuzzy Models of a priori Information in the Measurements' Results Processing* AMSE REVIEW, 1987, v.4, 2, p.1-12

[51] **L. Reznik, G. Solopchenko** *The USSR Patent: Method of Complexing of Measurements*, BULLETIN OF PATENTS, 1986, No. 47

[52] **L. Reznik, G. Solopchenko** *Use of a priori Information on Functional Relations between Measured Quantities for Improving Accuracy of Measurement*. MEASUREMENT, 1986, v.3, 2, p.61-69

[53] **G.Britov and L. Reznik** *Optimal Control on the Linear Fuzzy Systems*. AUTOMATION AND REMOTE CONTROL, 1981, v.42, 4, p. 462-465

Conference Papers (peer reviewed)

[54] Zatsarenko, R., Chuprov, S., Korobeinikov, D., & **Reznik, L.** (2024). ``Trust-Based Anomaly Detection in Federated Edge Learning" in the Proceedings of the 2024 5th Annual IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 29-31th May 2024, Eds.: R. Paul, A. Kundu, R. Bhattacharyya, pp. 273-279, doi: 10.1109/AIIoT61789.2024.10578967 – **won the BEST PRESENTER award**

[55] Chuprov, S., Zatsarenko, R., Korobeinikov, D., & **Reznik, L**. (2024). ``Robust Training on the Edge: Federated vs. Transfer Learning for Computer Vision in Intelligent Transportation Systems" in the Proceedings of the 2024 5th Annual IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 29-31th May 2024, Eds.: R. Paul, A. Kundu, R. Bhattacharyya, pp. 172-178, doi: 10.1109/AIIoT61789.2024.10578970

[56] Harshil Patel, Sergei Chuprov, Dmitrii Korobeinikov, Raman Zatsarenko and **Leon Reznik** "Improving Federated Learning Security with Trust Evaluation to Detect Adversarial Attacks" in of 19th Annual Symposium on Information Assurance (ASIA' 24) , June 4-5, 2024, Albany, NY /Eds. S. Goel

[57] Dmitrii Korobeinikov, Sergei Chuprov, Raman Zatsarenko, and **Leon Reznik** "Federated Learning Robustness on Real World Data in Intelligent Transportation Systems" in Proceedings of 19th Annual Symposium on Information Assurance (ASIA' 24) , June 4-5, 2024, Albany, NY / Eds. S. Goel

[58] **S. Chuprov, K. M. Bhatt and L. Reznik**, "Federated Learning for Robust Computer Vision in Intelligent Transportation Systems," 2023 IEEE Conference on Artificial Intelligence (CAI), Santa Clara, CA, USA, 2023, pp. 26-27, doi: 10.1109/CAI54212.2023.00019.

[59] **S. Chuprov, M. Memon and L. Reznik**, "Federated Learning with Trust Evaluation for Industrial Applications," 2023 IEEE Conference on Artificial Intelligence (CAI), Santa Clara, CA, USA, 2023, pp. 347-348, doi: 10.1109/CAI54212.2023.00153.

[60] **S. Chuprov, Mahajan, S., Zatsarenko, R., Reznik, L., & Ruchkan, A.** (2023). ``Are Industrial ML Image Classifiers Robust to Withstand Adversarial Attacks on Videos?" in 2023 IEEE Western New York Image and Signal Processing Workshop (WNYISPW), 2023, pp. 1-4, doi: 10.1109/WNYISPW60588.2023.10349595. URL

[61] **R. Zatsarenko, Marathe, C.A., Chuprov S, Hyland, M., & Reznik, L.** (2023). ``Are Industrial ML Image Classifiers Robust to Data Affected by Network QoS Degradation?" in 2023 IEEE Western New York Image and Signal Processing Workshop (WNYISPW), 2023, pp. 1-4, doi: 10.1109/WNYISPW60588.2023.10349560. URL

[62] **Chuprov, S., Reznik, L., & Grigoryan, G.** (2023). ``Study on Network Importance for ML End Application Robustness" in ICC 2023 - IEEE International Conference on Communications, 2023, pp. 6627-6632, doi: 10.1109/ICC45041.2023.10279698. URL

[63] **S. Chuprov, L. Reznik, I. Khokhlov and K. Manghi,** "Multi-Modal Sensor Selection with Genetic Algorithms," *2022 IEEE Sensors*, Dallas, TX, USA, 2022, pp. 1-4. doi: 10.1109/SENSORS52175.2022.9967296

[64] **I. Khokhlov, S. Chuprov and L. Reznik,** "Integrating Security with Accuracy Evaluation in Sensors Fusion," *2022 IEEE Sensors*, Dallas, TX, USA, 2022, pp. 1-4. doi: 10.1109/SENSORS52175.2022.9967235

[65] **S. Chuprov, A. N. Satam and L. Reznik,** "Are ML Image Classifiers Robust to Medical Image Quality Degradation?," *2022 IEEE Western New York Image and Signal Processing Workshop (WNYISPW)*, Rochester, NY, USA, 2022, pp. 1-4.doi: 10.1109/WNYISPW57858.2022.9983488

[66] **S. Chuprov, I. Khokhlov, L. Reznik and S. Shetty,** "Influence of Transfer Learning on Machine Learning Systems Robustness to Data Quality Degradation," *2022 International Joint Conference on Neural Networks (IJCNN)*, Padua, Italy, 2022, pp. 1-8. doi: 10.1109/IJCNN55064.2022.9892247

[67] **S. Chuprov, L. Reznik, A. Obeid and S. Shetty**, "How Degrading Network Conditions Influence Machine Learning End Systems Performance?," *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, May 2022, London, UK, pp. 1-6, doi: 10.1109/INFOCOMWKSHPS54753.2022.9798388.

[68] **S. Chuprov, I. Viksnin, I. Kim, T.Melnikov, L. Reznik, I. Khokhlov** Improving Knowledge Based Detection of Soft Attacks Against Autonomous Vehicles with Reputation, Trust and Data Quality Service Models, IEEE World Congress on Services, Sep. 5-11, 2021, Chicago, IL, USA 2021 IEEE International Conference on Smart Data Services (SMDS), 2021, pp. 115-120, doi: 10.1109/SMDS53860.2021.00025

[69] **L. Reznik, I. Khokhlov** *From Extensive Data Collection to Intensive Quality Knowledge Production* , NSF Workshop on Overcoming Measurement Barriers to Internet Research (WOMBIR 2021), Jan. 11-12, 2021, accessed at https://www.caida.org/workshops/wombir/slides/wombir2021-paper12.pdf on Jan. 11, 2021

[70] **Khokhlov I., Ligade N., Reznik L**., "Recurrent Neural Networks for Colluded Applications Attack Detection in Android OS Devices", IEEE World Congress on Computational Intelligence (WCCI) 2020, Glasgow, UK, July 2020. doi: 10.1109/IJCNN48605.2020.9207339.

[71] **Khokhlov I., Reznik L**., "What is the Value of Data Value in Practical Security Applications", IEEE/NDIA/INCOSE Systems Security Symposium 2020, Crystal City, Virginia, USA, July 2020 doi: 10.1109/SSS47320.2020.9174457.

[72] **Chuprov S., Viksnin I., Kim I., Reznik L., Khokhlov I.,** "Reputation and Trust Models with Data Quality Metrics for Improving Autonomous Vehicles Traffic Security and Safety", IEEE/NDIA/INCOSE Systems Security Symposium 2020, Crystal City, Virginia, USA, July 2020 doi: 10.1109/SSS47320.2020.9174269.

[73] **Khokhlov I., Reznik L**., "Knowledge Graph in Data Quality Evaluation for IoT Applications", 2020 IEEE World Forum on Internet of Things, New Orleans, Louisiana, USA, June 2020. doi: 10.1109/WF-IoT48130.2020.9221091

[74] **Chuprov S., Marinenkov E., Viksnin I., Reznik L., Khokhlov I.,** "Image Processing in Autonomous Vehicle Model Positioning and Movement Control", 2020 IEEE World Forum on Internet of Things, New Orleans, Louisiana, USA, June 2020. doi: 10.1109/WF-IoT48130.2020.9221258.

[75] **I. Khokhlov, L. Reznik and S. E. Lyshevski**, "Adaptive Data Fusion in Inertial Sensors and Data Quality Analysis of Sensor Networks," *2020 IEEE 40th International Conference on Electronics and Nanotechnology (ELNANO)*, Kyiv, Ukraine, 2020, pp. 430-435. doi: 10.1109/ELNANO50318.2020.9088859

[76] **L.Reznik and I.Khokhlov.** From Data Communication to Delivery of Quality Data, Large Scale Networking (LSN) Workshop on Huge Data: A Computing, Networking and Distributed Systems Perspective, *Sponsored by the National Science Foundation (NSF),* Chicago, IL, April 13 -- 14, 2020 available online at https://drive.google.com/drive/folders/1_rzzcVMv0jBGtZ8kvaelrXSZhOk4xgIz accessed on Dec. 11, 2020

[77] **I. Khokhlov, M. Perez and L. Reznik**, "Machine Learning in Anomaly Detection: Example of Colluded Applications Attack in Android Devices," *2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA),* Boca Raton, FL, USA, 2019, pp. 1328-1333, doi: 10.1109/ICMLA.2019.00216

[78] **I. Khokhlov, L. Reznik and R. Bhaskar,** "The Machine Learning Models for Activity Recognition Applications with Wearable Sensors," *2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA)*, Boca Raton, FL, USA, 2019, pp. 387-391, doi: 10.1109/ICMLA.2019.00072

[79] **I. Khokhlov, A. Pudage and L. Reznik**, "Sensor Selection Optimization with Genetic Algorithms," *2019 IEEE SENSORS*, Montreal, QC, Canada, 2019, pp. 1-4, doi: 10.1109/SENSORS43011.2019.8956579

[80] **I. Khokhlov, M. Perez and L. Reznik**, "System Signals Monitoring and Processing for Colluded Application Attacks Detection in Android OS," *2019 IEEE Western New York Image and Signal Processing Workshop (WNYISPW)*, Rochester, NY, USA, 2019, pp. 1-5, doi: 10.1109/WNYIPW.2019.8923113

[81] **I.Khokhlov, Q. Li, L.Reznik** D.I.F.E.N.S.E.: Distributed Intelligent Framework for Expendable Android Security Evaluation In the Proceedings of ASIA '19: 14th Annual Symposium on Information Assurance (ASIA '19), June 4-6, 2019, Empire State Plaza, Albany, NY.

[82] **Khokhlov, I., Jain C., Miller-Jacobson B., Heyman A., Reznik L., St.Jacques R.,** “MeetCI: A Computational Intelligence Software Design Automation Framework”. In IEEE World Congress on Computational Intelligence, Rio de Janeiro, Brazil, July 2018. (pp. 1499-1506). IEEE

[83] **Killawala A., Khokhlov, I., Reznik L.,** “Computational Intelligence Framework for Automatic Quiz Question Generation”. In IEEE World Congress on Computational Intelligence, Rio de Janeiro, Brazil, 2018. (pp. 76-83). IEEE.

[84] **I. Khokhlov, L. Reznik, J. Cappos and R. Bhaskar**, "Design of activity recognition systems with wearable sensors," 2018 IEEE Sensors Applications Symposium (SAS), Seoul, Korea (South), 2018, pp. 1-6. doi: 10.1109/SAS.2018.8336752

[85] **I. Khokhlov and L. Reznik**, "Android system security evaluation," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2018, pp. 1-2.

[86] **I. Khokhlov, L. Reznik, S. B. Jothilingam and R. Bhaskar**, "What can data analysis recommend on design of wearable sensors?," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2018, pp. 1-2.

[87] **A. Vora, L. Reznik and I. Khokhlov,** "Mobile road pothole classification and reporting with data quality estimates," 2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, 2018, pp. 1-6.

[88] **I. Khokhlov and L. Reznik,** "Colluded Applications Vulnerabilities in Android Devices," 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Orlando, FL, USA, 2017, pp. 462-469. doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.89

[89] **M. Potter, L. Reznik and S. Radziszowski**, "Neural networks and the search for a quadratic residue detector," *2017 International Joint Conference on Neural Networks (IJCNN)*, Anchorage, AK, May 2017, pp. 1887-1894.

[90] **L. Herlihy, E. Golen, L. Reznik and S. E. Lyshevski**, "Secure communication and signal processing in inertial navigation systems," *2017 IEEE 37th International Conference on Electronics and Nanotechnology (ELNANO)*, Kiev, 2017, pp. 414-419.

[91] **I. Khokhlov, L. Reznik, A. Kumar, A. Mookherjee, R. Dalvi** Data Security and Quality Evaluation Framework: Implementation Empirical Study on Android Devices, 2017 20th IEEE Conference of Open Innovations Association and Seminar on Information Security and Protection of Information Technology (FRUCT-ISPIT), St.Petersburg, April 3-7, 2017, ISSN 2305-7254 , pp. 161-168

[92] **I. Khokhlov, L. Reznik** Data Security Evaluation for Mobile Android Devices, 2017 20th IEEE Conference of Open Innovations Association and Seminar on Information Security and Protection of Information Technology (FRUCT-ISPIT), St.Petersburg, April 3-7, 2017, ISSN 2305-7254, pp. 154-160

[93] **R. Weiss, L. Reznik, Y. Zhuang, A. Hoffman, D. Pollard , A. Rafetseder, T. Li and J. Cappos** Trust Evaluation in Mobile Devices: An Empirical Study, The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15), Helsinki, Finland, 20-22 August, 2015, vol.1, pp. 25-32

[94] **S.E. Lyshevski, L. Reznik, Smith, T.C. ; Beisenbi, M.A. ; Jarasovna, J.Y. ; Mukataev, N.S. ; Omarov, A.N.** Estimates and measures of data communication and processing in nanoscaled classical and quantum physical systems 2014 IEEE 14th International Conference on Nanotechnology (IEEE-NANO), Toronto, 2014 , pp.1044 – 1047

[95] **L. Reznik, S. Lyshevski** Data Quality and Security Evaluation Tool for Nanoscale Sensors, SECURWARE 2014, The Eighth International Conference on Emerging Security Information, Systems and Technologies, Lisbon, November 16-21, 2014 in NetWare 2014, ISBN: 978-1-61208-047-5

[96] **S.E.Lyshevsky and L.Reznik** Information-theoretic estimates of communication and processing in nanoscale and quantum optoelectronic systems, 2013 IEEE XXXIII International Scientific Conference on Electronics and Nanotechnology (ELNANO), 16-19 April 2013, pp. 33-37

[97] **J.Bacaj and L.Reznik** Signal Anomaly Based Attack Detection in Wireless Sensor Networks, CCS '13: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, Berlin, November 2013

[98] **L.Reznik and E.Bertino** Data Quality Evaluation: Integrating Security and Accuracy, CCS '13: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, Berlin, November 2013

[99] **D. Yudanov and L. Reznik**. Scalable multi-precision simulation of spiking neural networks on GPU with OpenCL The 2012 International Joint Conference on Neural Networks (IJCNN), 2012 , pp: 1 – 8

[100] **V. Kreinovich, L. Reznik, K. K. Semenov, G. N. Solopchenko** Metrological Self-Assurance Of Data Processing Software, XX IMEKO World Congress: Metrology for Green Growth, Busan, Korea; September 2012

[101] **L. Reznik, A. Christian, A. Patel, B. Treich, and M. Alromaih** The Current State of Ordinary User Security, ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE & SECURE KNOWLEDGE MANAGEMENT, JUNE 5-6, 2012, ALBANY, NY, pp.62-67

[102] **S.Lyshevski and L.Reznik** Processing of Extremely-Large-Data and High Performance Computing Proceedings of International conference on High Performance Computing 2012 Kyiv, Ukraine, October 8-11, 2012, pp. 41-43, available also online at **http://www.hpc-ua.org/2012/proceedings**

[103] **L.Reznik** Integral Instrumentation Data Quality Evaluation: the Way to Enhance Safety, Security, and Environment Impact," 2012 IEEE International Instrumentation and Measurement Technology Conference, Graz, Austria, May 13-16, 2012, IEEE, 2012, pp. 2138 - 2143

[104] **L. Reznik, V.J. Buccigrossi , J. Lewis, A. Dipon, S. Milstead, N. LaFontaine, K.Beck, H. Silvia** Security of Computer Use Practice :The case of ordinary users survey, 6th Annual Symposium on Information Assurance (ASIA '11) ,Albany, NY, June 7-8, 2011, pp.18-25

[105] **L.Reznik and M.Becker** Future of Instrumentation? Accuracy! Reliability! Performance! Security? IEEE International Future of Instrumentation Workshop, November 7-8, 2011, Oak Ridge, TN

[106] **G.P. Timms, P.A. de Souza, L. Reznik** Automated assessment of data quality in marine sensor networks, IEEE International Conference OCEANS 2010 IEEE – Sydney, Australia, 24-27 May 2010, pp.1-5

[107] **D. Yudanov, M. Shaaban, R. Melton and L. Reznik** GPU-Based Simulation of Spiking Neural Networks with Real-Time Performance and High Accuracy, WCCI 2010, World Congress on Computational Intelligence, Barcelona, Spain, July 18 – 23, 2010

[108] **L.Reznik and K.Nathan.** *A Framework for Measurement Anomaly Detection in Sensor Networks*, IEEE Sensors 2009 Conference, Christchurch, New Zealand, 25-29 October 2009, IEEE, pp.597-600, ISBN: 978-1-4244-5335-1

[109] **L.Reznik, B.K. Bitemirov, M.Negnevitsky**. *Intrusion Detection in Sensor Networks Based on Measurements*, IEEE Sensors 2009 Conference, Christchurch, New Zealand, 25-29 October 2009, IEEE, pp.1026-1029, ISBN: 978-1-4244-5335-1

[110] **L. Reznik, R. Yampolskiy, J. Harlow, D. Novikov.** *When the Resource Consumption Does Matter: Artificial Neural Network Structure Choice for Intrusion Detection*, AISAT 2009, THE THIRD INTERNATIONAL WORKSHOP ON ARTIFICIAl INTELLIGENCE IN SCIENCE AND TECHNOLOGY, Proceedings/Ed.: M.Negnevitsky, 23- 24 November 2009, Hobart, Tasmania, Australia

[111] **L. Reznik, M. Adams, B. Woodard**, *When the Resource Consumption Does Matter: Artificial Neural Network Optimization for Intrusion Detection*, AISAT 2009, THE THIRD INTERNATIONAL WORKSHOP ON ARTIFICIAl INTELLIGENCE IN SCIENCE AND TECHNOLOGY, Proceedings/Ed.: M.Negnevitsky, 23- 24 November 2009, Hobart, Tasmania, Australia

[112] **G.N.Solopchenko, K.S.Semenov, V.Kreinovich, L.Reznik** "Measurement's result and its error as fuzzy variables: background and perspectives" Proceedings of ISMTII 2009, The 9th International Symposium on Measurement Technology and Intelligent Instrumentation, St.Petersburg, Russia, 28th June – 2nd July, 2009, pp. 4-132 - 4-136.

[113] **L.Reznik and G. Von Pless** *Neural Networks for Cognitive Sensor Networks*, World Congress on Computational Intelligence, Hong Kong, 1-6 June 2008, IEEE, 2008, pp.1236-1242

[114] **L.Reznik and C.Hoffman** *Development of the Intelligent Sensor Network Anomaly Detection System: Problems and Solutions*, Proceedings of the 2008 Workshop on Building Computational Intelligence and Machine Learning Virtual Organizations, October 24, 2008, Fairfax, VA, pp.21 – 27

[115] **L. Reznik, G. Von Pless, T. Al Karim** Application Testing of Novel Neural Network Structures, Proceedings of the 2008 Workshop on Building Computational Intelligence and Machine Learning Virtual Organizations, October 24, 2008, Fairfax, VA, pp.28 - 33

[116] **Podpora J. and L.Reznik** *An Environmentally Aware, Intelligently Controlled System for Power Efficient Wireless Sensor Networks*, The Sixth IEEE Conference on Sensors, Atlanta, USA, October 28-31, 2007 , pp.147-150

[117] **L.Reznik and K.A. Kluever** Improving Measurement Accuracy in Sensor Networks by an Object Model Generation and Application, The Sixth IEEE Conference on Sensors, Atlanta, USA, October 28-31, 2007, pp.371-374

[118] **Reznik L. and St. Jacques R**. ***Fuzzy Expert System Shell Development with Computer Security Assessment Application*** FUZZ-IEEE 2007. IEEE International Fuzzy Systems Conference, 2007, London, UK, 23-26 July 2007, pp.253-258

[119] **Nguyen H., G. W. Baxter and L. Reznik** *Soft Computing Techniques to Model the Top Oil Temperature of Power Transformers,* ISAP 2007 The 14th International Conference on Intelligent System Applications to Power Systems, November 4 - 8, 2007, Kaohsiung, Taiwan, pp.200-205

[120] **Novikov D., Yampolskiy R.V. and Reznik L. *Artificial Intelligence Approaches for Intrusion Detection* ,** 2006. LISAT 2006. IEEE Long Island Systems, Applications and Technology Conference, 5 May 2006, pp:1 – 8, New York, 2006

[121] **King, J.L.and Reznik, L “*Topology Selection for Signal Change Detection in Sensor Networks: RBF vs MLP***”, IJCNN '06. International Joint Conference on Neural Networks, 16-21 July 2006, pp.:2529 - 2535

[122] **Novikov, D.; Yampolskiy, R.V.; Reznik, L. “*Anomaly Detection Based Intrusion Detection”*** Third International Conference on Information Technology: New Generations, 2006, ITNG 2006, 10-12 April 2006, pp: 420 - 425

[123] **Von Pless, G.; T. Al Karim, T.; Reznik, L “*Modified time-based multilayer perceptron for sensor networks and image processing applications***”, Proceedings of the 2005 IEEE International Joint Conference on Neural Networks, 2005. IJCNN '05. Vol. 4, 31 July-4 Aug. 2005, pp:2201 – 2206, vol. 4

[124] **L. Reznik, G. Von Pless, T. Al Karim**, “*Embedding Intelligent Sensor Signal Change Detection into Sensor Network Protocols”*, 2005 Second Annual IEEE Communications Society Conference on Sensor and AdHoc Communications and Networks, Santa Clara, 26-29 September 2005, IEEE, pp. 207-217, ISBN 0-7803-9012-1

[125] L**. Reznik, G. Von Pless, T. Al Karim**, “*Intelligent Protocols Based on Sensor Signal Change Detection”,* 2005 Systems Communications Conference, 14-17 August 2005, Montreal, IEEE, pp 443-448, ISBN 0-7695-2422-2

[126] **L. Reznik, G. Von Pless and T. Al Karim** *Signal Change Detection in Sensor Networks with Artificial Neural Network Structure* CIHSPS2005 - IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, Orlando, FL, USA, 31 March - 1 April 2005, p.44-51

[127] **M. Negnevitsky, M.J-H. Lim, J.Hartnett, L.Reznik** *Email Communications Analysis: How to Use Computational Intelligence Methods and Tols?* CIHSPS2005 - IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, Orlando, FL, USA, 31 March - 1 April 2005, p.16 - 23

[128] **G. Von Pless, T.Karim and L.Reznik** *Time-Based Multi-Layer Perceptron for Novelty Detection in Sensor Networks*, 2004 IEEE/ACM International Conference on Machine Learning and Applications (ICMLA'04), 16-18 December 2004 -Louisville, KY, USA, pp.156-163

[129] **L.Reznik, M.Negnevitsky, C.Hoffman** *Contents Based Security Enhancement in Sensor Networks Protocols,* CIHSPS2004 - IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, Venice, Italy, 21-22 July 2004, pp.87-91

[130] **L.Reznik, V.Kreinovich** *Fuzzy and Probabilistic Models of Association Information in Sensor Networks*, Proceedings of the FUZZ '04, The 13th IEEE International Conference on Fuzzy Systems, Budapest, Hungary, July 25-30, 2004, vol. 1, pp.185 - 189

[131] **L.Reznik, V.Kreinovich and S.A.Starks** *Use of fuzzy expert's information in measurement and what we can gain from its application in geophysics* Proceedings of the FUZZ '03, The 12th IEEE International Conference on Fuzzy Systems, St.Louis, May 25- 28, 2003, IEEE, vol. 2, pp. 1026- 1031

[132] **M. Negnevitsky and L.Reznik** *Application of Neuro-Fuzzy Systems for Recognition and Reduction of Power Disturbances*, Proceedings of the Sixth IASTED International Conference on Software Engineering and Applications, M. H. Hamza, ed., Cambridge, USA, November 4-6, 2002, pp. 57-62

[133] **L.Reznik** *Fuzzy System Implementation through its Approximation with Simplified Radial Basis Networks* Proceedings of the 2002 IEEE International Conference on Fuzzy Systems FUZZ-IEEE’02 May 12 – 17, 2002 Hilton Hawaiian Village Hotel Honolulu, Hawaii, IEEE and NNS, vol. 2, pp. 1186-1191

[134] **H.H. Nguyen,J. Shi, and L. Reznik**, *A Neural Fuzzy Approach to Modeling the Top Oil Temperature of Power Transformer.* In: MS'02 : Proceedings of the Fourth International Conference on Modelling and Simulation : 11-13 November, 2002, Melbourne, Australia. Zayegh, Aladin, ed. Victoria University, Melbourne, pp. 27-31. ISBN 1862726175

[135] **L. Reznik and M. Negnevitsky** *A Neuro-Fuzzy Method of Power Disturbances Recognition and Reduction* Proceedings of the 2002 IEEE International Conference on Fuzzy Systems FUZZ-IEEE’02 May 12 – 17, 2002 Hilton Hawaiian Village Hotel Honolulu, Hawaii, IEEE and NNS, vol. 2, pp. 1517-1522

[136] **L.Reznik and B.Pham** *Fuzzy Models in Evaluation of Information Uncertainty in Engineering and Technology Applications*, The 10th IEEE International Conference on Fuzzy Systems, December 2-5, 2001, Melbourne, Australia, ISBN 0-7803-7294-X

[137] **S.Spiteri, L.Reznik, P. Vilas-Boah** *Embedded Fuzzy Control for Reefer Refrigeration Systems***,** The 10th IEEE International Conference on Fuzzy Systems, December 2-5, 2001, Melbourne, Australia, ISBN 0-7803-7294-X

[138] **L.Reznik and A.Little** *Choice of the Radial Basis Function Approximation in Neural Networks Used for Fuzzy System Implementation* Joint 9th IFSA World Congress and 20th NAFIPS International Conference, July 25-28, 2001, Vancouver, Canada, Proceedings IEEE, p.3032-37

[139] **A. Little, L. Reznik** *Implementation of Fuzzy Controllers with Radial Basis Neural Networks* The Ninth IEEE International Conference on Fuzzy Systems, FUZZ IEEE 2000 San Antonio, USA, 7-10 May 2000 Proceedings IEEE vol.2 p.581 - 586

[140] **L. Reznik** *What Is the Right Place for Fuzzy Control in Industry?* In Proceedings of AISAT'2000 International Conference on Artificial Intelligence in Science and Technology, Hobart, Australia, 17-20 December 2000, The University of Tasmania, Australia, 2000, pp. 157-162

[141] **H.T. Nguyen, V.Kreinovich, and L.Reznik** *Integrating Domain Knowledge with Data: From Crisp to Probabilistic and Fuzzy Knowledge*, Workshop on Fusion of Domain Knowledge with Data for Decision Support, Stanford University, Stanford CA, USA, June 30, 2000

[142] **L. Reznik, K.P. Dabke** *Evaluation of Uncertainty in Measurement: A Proposal for Application of Intelligent Methods* in H. Imai/Ed. Measurement to Improve Quality of Life in the 21st Century, IMEKO –XV World Congress, June 13-18, 1999, Osaka, Japan, vol. II, p.93 – 100

[143] **L. Reznik, A. Stojcevski, V.Kreinovich** *Modelling of Human Measurement Functions as a Way of Intelligent Sensor Design* in H. Imai/Ed. Measurement to Improve Quality of Life in the 21st Century, IMEKO –XV World Congress, June 13-18, 1999, Osaka, Japan, vol. XI, p. 75 - 82

[144] **G. Solopchenko, V.Kreinovich, L.Reznik** *Development of Mathematical Structure of the Modern Measurement Science* in Proceedings of International Workshop on Advances of Measurement Science, June 20-21, 1999, Kyoto, Japan, p.35 – 47

[145] **L. Reznik** *Fuzzy + Neural + PID Combination as a Way to Design New Industrial Information and Control Systems* in ICEX’99 Instrumentation and Control Exhibition, Symposium, Workshops, Melbourne, May 25-28, 1999

[146] **L.Reznik** *Measurement Result Uncertainty Evaluation: New Soft Approaches?* SCM’99 International Conference on Soft Computing and Measurements, St. Petersburg, Russia, May 25-28, 1999

[147] **A.Little and L.Reznik** *Implementation of Fuzzy Logic Controllers Using Neural* networks SCIRF'99 Collaborative Research Forum Proceedings, 18 November 1999, Melbourne, Victoria University, p.52-57

[148] **A.Stojcevski, L.Reznik, M.Faulkner** Trends in Cellular Position Location Techniques - an Overview SCIRF'99 Collaborative Research Forum Proceedings, 18 November 1999, Melbourne, Victoria University, p.69 - 73

[149] **V.Kreinovich, E. Johnson-Holubec, L.Reznik, and M. Koshelev** *Cooperative Learning is Better: Explanation Using Dynamical Systems, Fuzzy Logic, and Geometric Symmetries* , Vietnam-Japan Bilateral Symposium on Fuzzy Systems and Applications, Halong Bay, Vietnam, 30 September – 2 October, 1998, Proceedings/Eds. H.-P. Nguyen and O.Ario, Ha Noi, 1998, p.154 – 160

[150] **L.Reznik** *Intelligent Sensor: An attempt to Define* 1998 Second International Conference on Knowledge-Based Intelligent Electronic Systems, Adelaide, South Australia, 21-23 April 1998, Eds.: L.C.Jain and R.K.Jain, IEEE, p.603-608

[151] **L. Reznik** *Fuzzy Controller Design: Recommendations to the User* 1998 Second International Conference on Knowledge-Based Intelligent Electronic Systems, Adelaide, Australia, 21-23 April 1998, Eds.: L.C.Jain and R.K.Jain, IEEE, p.609-616

[152] **L. Reznik** *How to Design a New Intelligent Controller for Industrial Applications?* Control-97 International Conference Proceedings, October 20-22, 1997, Sydney, The Institution of Engineers, p.281-286

[153] **M.Selesnew and L.Reznik** *Development of a Hydraulic Dynamometer Engine Test System for High Speed Inertia Simulation* Control-97 International Conference Proceedings, October 20-22, 1997, Sydney, The Institution of Engineers, p. 61-66

[154] **L. Reznik** *Evolution of Fuzzy Controller Design* Proceedings of the 6th IEEE International Conference on Fuzzy Systems, July 1-5, 1997, Barcelona, Spain, IEEE Neural Networks Council, vol. 1, pp.503 - 508

[155] **O. Gnanayem and L.Reznik** *Excitation Control of a Synchronous Generator Using an On-Line Adaptive Fuzzy Logic Controller Structure* Proceedings of the 6th IEEE International Conference on Fuzzy Systems, July 1-5, 1997, Barcelona, Spain, IEEE Neural Networks Council, vol. 3, pp.1493 - 1498

[156] **L.Reznik** *Fuzzy Controller Design: Methods Classification and Parameters Choice*, 7th International Fuzzy Systems Association World Congress, June 25-29, 1997, Prague, Czech Republic, Proceedings, vol. 3, pp. 398 - 403, Academia, Prague, 1997

[157] **O. Gnanayem and L.Reznik** *A Fuzzy Logic Structure for On-Line Parameter Tuning with the Application to Power System Excitation Control***,** 7th International Fuzzy Systems Association World Congress, June 25-29, 1997, Prague, Czech Republic, Proceedings, vol. 3, pp. 488 - 493, Academia, Prague, 1997

[158] **O. Gnanayem and L.Reznik** *A Universal Adaptation Procedure for Fuzzy Controller Design with the Application to Power System Stability Control*, 35th IEEE Conference on Decision and Control, pp.1141 - 1146, Kobe, Japan, December 11- 13, 1996

[159] **A. Little and L. Reznik** *A Speech Detection Method Analysis and Intelligent Structure Development*, 1996 Australian and New Zealand Conference on Intelligent Information Systems, pp. 203 - 206, Adelaide, November 18 - 20, IEEE, 1996

[160] **O. Gnanayem and L.Reznik** *A Novel Excitation Control Scheme: Design and Implementation*, 1996 Australian and New Zealand Conference on Intelligent Information Systems, pp. 212 - 215 , Adelaide, November 18 - 20, IEEE, 1996

[161] **L.Reznik** *Intelligent Measurement: How To Achieve?* The 2nd International Conference on Problems of Physical Metrology (FISMET'96) June 17-23, 1996, St.Petersburg, Russia, p.80-81

[162] **L.Reznik** *How To Teach Fuzzy Technology?* Proceedings of the First International Discourse on Fuzzy Logic and the Management of Complexity, January 15-18, 1996, Sydney, Australia, vol.1, p. 87 - 91

[163] **L.Reznik** *Fuzzy Controller Design: Some Experience* Proceedings of the First International Discourse on Fuzzy Logic and the Management of Complexity, January 15-18, 1996, Sydney, Australia, vol.2, p. 109 - 114

[164] **M.Selesnew and L.Reznik** *Fuzzy Modelling and Control for an Engine Test System* Proceedings for the First International Discourse on Fuzzy Logic and the Management of Complexity, January 15-18, 1996, Sydney, Australia, vol.2, p. 140 - 144

[165] **A.Bourmistrov and L.Reznik** *Hybrid Guidance Control for a Self-Piloted Aircraft* Proceedings for the First International Discourse on Fuzzy Logic and the Management of Complexity, January 15-18, 1996, Sydney, Australia, vol.2, p. 155-159

[166] **V.Kreinovich and L.Reznik** *Fuzzy Information Improves Measurement (If This Information Is Correct)* Proceedings for the First International Discourse on Fuzzy Logic and the Management of Complexity, January 15-18, 1996, Sydney, Australia, vol.2, p. 206 - 210

[167] **O. Ghanayem and L. Reznik** *A Hybrid AVR-PSS Controller Based on Fuzzy Logic Technique,* presented to the International Conference "Control-95", Melbourne, 20 -24 October 1995 and published in the Conference Proceedings, The Institution of Engineers, Australia, 1995, vol. 2, pp. 347 - 351

[168] **M.Selesnew and L. Reznik** *Intelligent Control for Engines Testing: Which Model To Apply?,* presented to the International Conference "Control-95", Melbourne, 20 -24 October 1995 and published in the Conference Proceedings, The Institution of Engineers, Australia, 1995, vol. 2, pp.539 - 543

[169] **O. Ghanayem and L. Reznik** *A New Reasoning Approach and its Application in Power System Stability*, Proceedings of the Third European Congress on Intelligent Techniques and Soft Computing (EUFIT'95), August 29-September 1, 1995, Aachen, Germany, vol.3, pp.1527 - 1532

[170] **A.Stoica, L.Herron, M.Wingate, L.Reznik, O. Ghanayem** *Fuzzy Neural Networks as Distributed Fuzzy reasoning Systems* Proceedings of the Third European Congress on Intelligent Techniques and Soft Computing (EUFIT'95), August 29-September 1, 1995, Aachen, Germany, vol.1, pp.86 - 90

[171] **L. Reznik** *Fuzzy Technology Teaching: Some Experience*, presented to the Pacific Region Conference on Electrical Engineering Education, February 23 - 24, 1995, Marysville and published in the Conference Proceedings "Advancing Electrical Engineering Curricula To Reflect Current And Future Technologies" pp. 119 - 122

[172] **L. Reznik, G. Solopchenko, W. Carroll-Johnson** *Fuzzy Intervals as a Basis for Measurement Theory*, First international Joint Conference of the North American Fuzzy Information Processing Society Biannual Conference, the Industrial Fuzzy Control and Intelligent Systems Conference, and the NASA Joint Technology Workshop on Neural Networks and Fuzzy Logic, pp. 405 - 406, San Antonio, USA, December 18-21, NASA, 1994

[173] **L. Reznik and O. Ghanayem** *Hierarchical Versus Adaptive Fuzzy Logic Controllers: Design and Performance*, 2nd Australian and New Zealand Conference on Intelligent Information Systems, pp. 224 - 228 , Brisbane, November 29 - December 2, IEEE, 1994

[174] **A.Stoica and L. Reznik** *Mapping Alpha-Cut Borders: Classification and PID Realization*, 3rd IEEE International Conference on Fuzzy Systems, vol.3, pp.1604 - 1607, IEEE, Orlando, USA, June 26-29, 1994 - 40%

[175] **L. Reznik and J. Shi** *Simulation Study of the Choice of Membership Function Model for Control Applications*, Proceedings of Second International Conference on Modelling and Simulation, Melbourne, July, 1993, vol.1, p.209-217

[176] **L. Reznik and A. Stoica** *Some Tricks in Fuzzy Controller Design*, Australia and New Zealand conference on Intelligent Information Systems, (ANZIIS – 93) IEEE, Perth, Western Australia, November,1993, p. 60 - 64

[177] **V. Kreinovich, L. Reznik, et.al**. *What Non-Linearity to Choose? Mathematical Foundations of Fuzzy Control,* 1992 INTERNATIONAL FUZZY SYSTEMS AND INTELLIGENT CONTROL CONFERENCE, Louisville, KY, USA, 1992, p.349-412

[178] **V. Kreinovich , Quintana C**., **L. Reznik** *Gaussian Membership Functions Are Most Adequate in Representing Uncertainty in Measurements*, North American Fuzzy Information

Processing Society (NAFIPS'92) Conference in Puerto Vallarta, Mexico, Dec. 1992 and published in NASA Conference Publication 10112, vol. 11, p.618-624

[179] **V. Kreinovich, L. Reznik, et.al**. *Inverse Problems: Fuzzy Representation of Uncertainty Generates a Regularization*, North American Fuzzy Information Processing Society (NAFIPS'92) Conference in Puerto Vallarta, Mexico, Dec. 1992 and published in NASA Conference Publication 10112, vol. 11, p. 418-426

[180] **L. Reznik** *Problems of Expert Systems Using in Intelligent Measuring Instruments*, presented to MEASURE-90 International Conference, Moscow and published in the Conference Proceedings, Moscow, 1990, p.157-165

[181] **V. Kreinovich, L. Reznik** *Prospects for Using Expert Systems as a Part of Intelligent Measuring Instruments*, presented to INTERNATIONAL SCHOOL ON THE PROBLEMS OF INTELLIGENT MEASURING INSTRUMENTS, Dagomys, 1990 and published in the Proceedings Moscow, 1990, part 2, p.97-110

Non-Refereed Papers

[182] **H. P. Fernando, L.W. Turner and L.Reznik** *Forecasting Tourism to Japan: A Comparison of Neural Networks and Time Series Models*, The 20th International Symposium on Forecasting, Lisbon, Portugal, June 21-24, 2000

[183] **L.Reznik** *Towards Fuzzy Logic Application in Measurement Theory* 1st International Conference "Soft Computing and Measurement" (SCM'98), St.Petersburg, Russia, June 22-26, 1998

[184] **L. Reznik** *How to Design an Intelligent Sensor: A Few Ideas* Third international Conference on problems of Physical Metrology (FIZMET'98) Abstracts, June 15-19, 1998, St.Petersburg, Russia, p. 16-18

[185] **L. Reznik** *Intelligent Measurement: Some Trends and Problems*, presented to Symposium on Measurement and Quality Assessment, RMIT, Melbourne, Australia, 31 March 1994 and published in the Symposium abstracts, p.22

Multimedia presentations and publications available in non-registered publications or on-line only:

[186] **Chuprov, S., & Reznik, L**. (2023). "FLAME: Federated Learning against Malicious Engineering. Employing Trust and Reputation to Enhance Learning Security and Privacy" at Rochester Security Summit (RSS:2023), 25-26 October 2023, Rochester, NY, USA.

[187] **Chuprov, S., Reznik, L., & Zatsarenko, R.** (2023). "MLIN or How to Make Networks and ML Applications Work Together in Real Conditions?" at First IEEE Upstate New York Workshop on Secure and Sustainable Communications Networks (SSCN), 10 October 2023, Rochester Institute of Technology, Rochester, NY, USA.

[188] **Chuprov, S., Reznik, L., & Zatsarenko, R**. (2023). "FLAME: Federated Learning against Malicious Engineering. Employing Trust and Reputation to Enhance Learning Security and Privacy" at Eastern Great Lakes (EaGL) Theory Computation Workshop 2023, 30 September – 1 October 2023, University of Rochester, Rochester, NY, USA.

[189] **Chuprov, S., Reznik, L., & Memon, M.** (2023). "Enhancing Federated Learning Security with Reputation and Trust-Based Indicators" at UPSTAT 2023, 21–22 April 2023, , Rochester, NY, USA – ***Gold medal best paper award***

[190] **Chuprov, S., Reznik, L., Bhatt, K.M., & Memon, M**. (2023). "Discovering and Addressing Privacy and Robustness Flaws in Federated Learning" at the Great Lakes Security Day (GLSD) 2023, 21 April 2023, Rochester, NY, USA.

[191] **L.Reznik** What is hot in computer science (hints: Cybersecurity, AI and ML, Big Data) and what we can do therein (hints: Data quality and security, Intelligent security systems) – Invited Key Speech at Colgate University, New York on April 2, 2022 - see recordings at

https://www.youtube.com/watch?v=GWK3Y2Ziqio) to the Colgate University Technology Immersion week 2022- see https://colgatecoders.github.io/cccPage/ for more information.

[192] **Chuprov, S., & Reznik, L. (2021**). "Reputation and Trust Models with Data Quality Metrics for Improving Autonomous Vehicles Traffic Security and Safety" at Great Lakes Security Day (GLSD) 2021 Online, 12 November 2021, Rochester, NY, USA. – Poster session.

[193] **L.Reznik and I.Khokhlov** recordings of the **webinar** organized by TrustCI Center under auspices of NSF, on **March 26, 2018** , **Data Quality & Security Evaluation Framework Development with Leon Reznik & Igor Khokhlov** available on the YouTube channel *https://youtu.be/nkp0kvJvTWw*. Also, you can download the corresponding slides are available at https://www.ideals.illinois.edu/handle/2142/99558

[194] **I.Khokhlov and L.Reznik** What is the Android Colluded Applications Attack and How to Detect It at the 2018 Rochester Security Summit - https://www.rochestersecurity.org/schedule/owasp-track/#o1, Oct. 10, 2018

[195] **L.Reznik** Panel Discussion: Identifying and Supporting Science Drivers in the Campus Environment at the 2018 NSF Campus Cyberinfrastructure and Cybersecurity Innovation for Cyberinfrastructure PI Workshop, Sep. 29, 2018 Available at https://www.thequilt.net/wp-content/uploads/LReznik_RIT_DataQuality.pdf

[196] **L.Reznik** "From Big Data to Quality Data: What is the emerging and network technology is going to deliver next" - Keynote presentation to NetWare 2014, an umbrella event incorporating a few international conferences on November 20, 2014 in Lisbon, Portugal available online at http://www.iaria.org/conferences2014/filesSENSORCOMM14/LeonReznik_Keynote.pdf

[197] **L.Reznik** Panel on November 19 on the topic Information Privacy: Does it really matter? which is available at http://www.iaria.org/conferences2014/filesAFIN14/AFIN2014_EXPERT_PANEL.pdf

[198] **D.Yudanov and L.Reznik** Heterogeneous Implementation of Neural Network Algorithms, presentation to the AMD Developer Summit, San Jose, November 11-13, 2013 available at the Summit website at http://www.slideshare.net/DevCentralAMD/hc4016-heterogeneous-implementation-of-neural-network-algorithms-by-dmitri-yudanov-and-leon-reznik

[199] **L.Reznik** Use of Fuzzy Association Information for Uncertainty Evaluation in Heterogeneous Sensor Networks, 2nd IEEE Upstate New York Workshop on Sensor Networks, University Sheraton Hotel, Syracuse, NY, October 10, 2003 (available at http://comlab.ecs.syr.edu/workshop/)

[200] **R.Yampolskiy, L.Reznik** Feature mixing for reduction of computational requirements, 2004 IEEE Western New York Image Processing Workshop, RIT, Rochester, NY, September 24, 2004 (available at https://dspace.lib.rochester.edu/retrieve/2216/wnyipw2004Proceedings.pdf)

[201] **Gregory Von Pless, Tayeb Al Karim and Leon Reznik** Security and Reliability Enhancement in Sensor Networks Based on Change Detection, 3rd IEEE Upstate New York Workshop on Sensor Networks, University Sheraton Hotel, Syracuse, NY, October 15, 2004 (program is given at http://www.ece.rochester.edu/~wheinzel/sn04/)

[202] **W Carithers, L Reznik, A Samant** Using System Call Analysis to Stop Evasion Attacks 1st IEEE Upstate NY Workshop on Communications and Networking Proceedings, p.1-5, Rochester, NY, November 12, 2004 (program is given at http://www.ewh.ieee.org/r1/rochester/comm_aero/oral.html)

[203] **Gregory Von Pless, Tayeb Al Karim and Leon Reznik** Intelligent Novelty Detection in Sensor Networks with Time Based Multilayer Perceptron Neural Network, Computer Science Colloquium presentation, December 2, 2004, RIT

Webinars and external presentations recorded:

[204] **L.Reznik** What is hot in computer science (hints: Cybersecurity, AI and ML, Big Data) and what we can do therein (hints: Data quality and security, Intelligent security

systems), Colgate University Technology Immersion Week 2022 Invited lecture available at https://www.youtube.com/watch?v=GWK3Y2Ziqio

[205] **L. Reznik and I. Khokhlov Data Quality & Security Evaluation Framework Development** presented at the National Center for Supercomputing Applications at University of Illinois at Urbana-Champaign under auspices of NSF, on **March 26, 2018** , recordings available on the YouTube channel https://www.youtube.com/watch?v=nkp0kvJvTWw&feature=youtu.be. Also, you can download the corresponding slides are available at https://www.ideals.illinois.edu/handle/2142/99558

[206] **L.Reznik** Panel presentation “**Identifying and Supporting Science Drivers in the Campus Environment**” at 2018 NSF Campus Cyberinfrastructure and Cybersecurity Innovations for Cyberinfrastructure PI Workshop – available at https://www.thequilt.net/wp-content/uploads/LReznik_RIT_DataQuality.pdf

Reviews of my work

[1] **B. Bona** *Fuzzy Controllers by L.Reznik* AUTOMATICA, vol. 37, 2001, no.2 , p.319-320

[2] **Linkens D. A.** *Fuzzy Controllers. How to design them, How they work* Proc. of the Institute of Mechanical Engineers, vol. 212, 1998, part 1, p. 325