Mahmoud Nazzal

Ph.D. Candidate in Computer Engineering Specializing in AI Security and Applications

Personal Website : https://mahmoudkanazzal.github.io
Email : mn69[at]njit[dot]edu
LinkedIn : mahmoud-nazzal
GitHub : https://github.com/mahmoudkanazzal
Google Scholar : https://scholar.google.com/citations?user=ygjUJnYAAAAJ
Address : 410B-FMH, NJIT, Newark, NJ 07102, USA

Research Interests

Currently : Security, robustness, and applicability of Graph Neural Networks (GNNs) and Large Language Models (LLMs)

- Adversarial robustness of GNNs and LLMs in novel areas
- Prompt optimization and engineering
- Real-world applications of LLMs and GNNs in :
  - Secure and functional source code generation
  - Hardware design automation
  - Transportation system analytics
  - Internet security
  - Deepfake detection

Past interests : Machine learning (ML) for communications (Physical layer security, Channel estimation, and spectrum sensing)

Professional Experience

Present – 2021 | **Research Assistant/Teaching Assistant, New Jersey Institute of Technology, Newark, NJ, USA**
- Conduct research on LLM and GNN security and applications
- Collaborate with an industry partner (TelAI) on industry-focused legal document analysis
- Lecture undergraduate courses in computer engineering

2021 – 2019 | **Lecturer, Abu Dhabi Vocational Education and Training Institute, Abu Dhabi, UAE**
- Taught undergraduate courses in electrical engineering
- Supervised student projects and provided mentorship

2019 – 2017 | **Researcher, Istanbul Medipol University, Istanbul, Turkey**
- Conducted research on machine learning for wireless communication technologies

2017 – 2016 | **Lecturer, Izmir University of Economics, Izmir, Turkey**
- Taught courses in electrical engineering
- Supervised graduation projects

2016 – 2009 | **Research and Teaching Assistant, Eastern Mediterranean University, Famagusta, Cyprus**
- Supervised laboratory sessions for undergraduate students
- Taught courses in electrical and electronic engineering

Education

2025 – 2021 | **Ph.D. in Computer Engineering, New Jersey Institute of Technology, Newark, NJ, USA**
- GPA : 4.00/4.00
- Dissertation : *Adversarial Robustness in Advanced Sequential and Relational Machine Learning Models Integrating Graph Neural Networks and Large Language Models*
- Supervisors : Prof. Abdallah Khreishah and Dr. Issa Khalil

2010 – 2009 | **M.Sc. in Electrical and Electronic Engineering, Eastern Mediterranean University, Cyprus**
- GPA : 3.77/4.00
- Thesis : *Color Demosaicing for Digital Camera Images*

2009 – 2004 | **B.Sc. in Electrical Engineering, Birzeit University, Ramallah, West Bank**
- Final-year project : *Power Factor Correction Using a Three-Phase Converter*

Research Contribution Summary

- Over 12 journal papers and 20 conference papers
- 1 book chapter
- 7 US and EU patents
- 380+ Citations

Selected Awards and Honors

Oct. 2024	ACM Conference on Computer and Communications Security (CCS 2024), Salt Lake City, Utah, USA **Student Travel Grant** to attend the conference
Jun. 2023	33rd Great Lakes Symposium on VLSI (GLSVLSI), Knoxville, TN, USA **Best Paper Award (2nd place)**. *See award details here*
Nov. 2022	ECE PhD Stories Contest, NJIT, Newark, NJ, USA 3rd Prize
2021 - 2022	New Jersey Institute of Technology, Newark, NJ, USA Ross Fellowship
2022 - 2024	New Jersey Institute of Technology, Newark, NJ, USA Teaching Assistantship and Research Assistantship
Jun. 2021	Signal Processing and Communications Applications Conference (SIU 2021), Istanbul, Turkey **Best Paper Award (3rd place)**. *See award details here*
Oct. 2020	Turkish Patent and Trademark Office, Ankara, Turkey **5th Place**, *Second University Patent Competition*
2017 - 2019	The Scientific and Technological Research Council of Turkey (TUBITAK), Ankara, Turkey TUBITAK 2221 Fellowship
2009-2010	Eastern Mediterranean University, Famagusta, Cyprus Research Assistantship
2008 - 2009	Jerusalem District Electricity Company (JDECO), Ramallah, West Bank B.Sc. Graduation Project Fund, Amount $2,000

Notable Publications

Conference Papers (C)

[C20] **M. Nazzal**, I. Khalil, A. Khreishah, and N.H. Phan, "**PromSec** : Prompt Optimization for Secure Generation of Functional Source Code with Large Language Models (LLMs)", *31st ACM Conference on Computer and Communications Security* **(CCS 2024)**, *Salt Lake City, U.S.A, UT, Oct. 2024*, [Covered by a US Provisional Patent.]

[C19] **M. Nazzal**, I. Khalil, A. Khreishah, N.H. Phan, and Y. Ma, "Multi-Instance Adversarial Attack on GNN-Based Malicious Domain Detection", *45th IEEE Symposium on Security and Privacy* **(IEEE S&P 2024)**, *San Francisco, CA, USA, May 2024.* [Presentation Video]

[C18] **D. Vungarala*, M. Nazzal***, M. Morsali, C. Zhang, A. Ghosh, A. Khreishah, and S. Angizi, "SA-DS : A Dataset for Large Language Model-Driven AI Accelerator Design Generation, " Accepted to appear in *58th IEEE International Symposium on Circuits and Systems (IEEE ISCAS)*, London, UK, May 2025 (*Equal contribution)

[C17] T.K. Ton, N. Nguyen, **M. Nazzal**, A. Khreishah, C. Borcea, N.H. Phan, R. Jin, I. Khalil, and Y. Shen, "Demo : **SGCode** : A Flexible Prompt-Optimizing System for Secure Generation of Code", *31st ACM Conference on Computer and Communications Security* **(CCS 2024)**, *Salt Lake City, UT, U.S.A, Oct. 2024*.

[C16] M. Morsali, **M. Nazzal**, A. Khreishah, and S. Angizi, "IMA-GNN : In-Memory Acceleration of Centralized and Decentralized Graph Neural Networks at the Edge", *33rd edition of Great Lakes Symposium on VLSI (GLSVLSI)*, Knoxville, TN, USA, Jun. 2023. [Best Paper Award]

Journal Papers (J)

[J12] **M. Nazzal**, A. Khreishah, J. Lee, S. Angizi, A. Al-Fuqaha, and M. Guizani, "Semi-decentralized Inference in Heterogeneous Graph Neural Networks for Traffic Demand Forecasting : An Edge-Computing Approach", *IEEE Transactions on Vehicular Technology*, Jan. 2024.

Patents (P)

[P7] **M. Nazzal**, I. Khalil, A. Khreishah, and N.H. Phan, "Method and System for Prompt Optimization for Secure Generation of Functional Source Code with Large Language Models", *US Patent*, Patent Application No. : US63/561,573, Washington, D.C., USA, Filing date : Mar. 5, 2024.

Book Chapters (BC)

[BC1] **M. Nazzal**, M. A. Aygul, and H. Arslan, *Channel Modeling for 5G and Beyond*, In : H. Arslan, E. Basar, *Flexible and Cognitive Radio Access Technologies for 5G and Beyond*, Telecommunications Series, Institution of Engineering and Technology, ISBN-13 : 978-1-83953-079-1, p. 342, 2020.

Recent Journal Papers (ML Security)

[J11] I. Alsmadi, K. Ahmad, **M. Nazzal**, F. Alam, A. Al-Fuqaha, A. Khreishah, and A. Algosaibi. "Adversarial NLP for social network applications : Attacks, defenses, and research directions". *IEEE Transactions on Computational Social Systems*, vol. 10, no. 6, pp. 3089-3108, Nov. 2022.

[J10] N. Aljaafari, **M. Nazzal**, A. Sawalmeh, A. Khreishah, M. Anan, A. Algosaibi, M. Alnaeem, A. Aldalbahi, A. Alhumam, and C. P. Vizcarra, "Investigating the Factors Impacting Adversarial Attack and Defense Performances in Federated Learning", *IEEE Transactions on Engineering Management*, vol. 71, pp. 12542-12555, May 2022.

[J9] I. Alsmadi, N. Aljaafari, **M. Nazzal**, S. Alhamed, A. Sawalmeh, C. P. Vizcarra, A. Khreishah, M. Anan, A. Algosaibi, M. Alnaeem, A. Aldalbahi, and A. Alhumam, "Adversarial Machine Learning in Text Processing : A Literature Survey", *IEEE Access*, vol. 10, pp. 17043-17077, Jan. 2022.

[J8] H. M. Furqan, M. A. Aygül, **M. Nazzal**, and H. Arslan, "Primary User Emulation and Jamming Attack Detection in Cognitive Radio via Sparse Coding", *EURASIP Journal on Wireless Communications and Networking*, no. 1, pp. 1-9, Apr. 2020.

Journal Papers (ML and Signal Processing)

[J7] M. Aygül, **M. Nazzal**, and H. Arslan, "Sparsifying dictionary learning for beamspace channel representation and estimation in millimeter-wave massive MIMO", *IEEE Access*, vol. 11, pp. 98436-98451, Sep. 2023.

[J6] S. Shao, **M. Nazzal**, A. Khreishah, and M. Ayyash, "Self-optimizing Data Offloading in Mobile Heterogeneous Radio-Optical Networks : A Deep Reinforcement Learning Approach", *IEEE Network Magazine*, vol. 36, no. 2, pp. 100-106, May 2022.

[J5] A. Alenezi, **M. Nazzal**, A. Sawalmeh, A. Khreishah, S. Shao, and M. Almutiry, "Machine Learning Regression-based RETRO-VLP for Real-time and Stabilized Indoor Positioning", *Cluster Computing*, Vol. 27, pp. 299–311, Dec. 2022.

[J4] M. A. Aygül, **M. Nazzal**, and H. Arslan, "Using OMP and SD Algorithms Together in mm-Wave mMIMO Channel Estimation", *Signal, Image and Video Processing, Springer*, vol. 16, pp. 1205–1213, Jan. 2022.

[J3] M. A. Aygül, **M. Nazzal**, M. İ. Sağlam, D. B. da Costa, H. F. Ates, and H. Arslan, "Efficient Spectrum Occupancy Prediction Exploiting Multidimensional Correlations through Composite 2D-LSTM Models", *Sensors-Special Issue AI-Enabled Cognitive Radio Networks*, vol. 21, no. 1, pp. 135-153, Dec. 2020

[J2] **M. Nazzal**, A. R. Ekti, A. Gorcin, and H. Arslan, "Exploiting sparsity recovery for compressive spectrum sensing : A machine learning approach", *IEEE Access*, vol. 7, pp. 126098-126110, Apr. 2019.

[J1] **M. Nazzal**, F. Yeganli, and H. Ozkaramanli, "A strategy for residual component-based multiple structured dictionary learning", *IEEE Signal Processing Letters*, vol. 22, no. 11, pp. 2059-2063, Nov. 2015.

Conference Papers (Security, ML, Signal Processing)

[C15] **M. Nazzal**, N. Aljaafari, A. Sawalmeh, A. Khreishah, M. Anan, A. Algosaibi, M. Alnaeem, A. Aldalbahi, A. Alhumam, C. P. Vizcarra, and S. Alhamed, "Genetic Algorithm-Based Dynamic Backdoor Attack on Federated Learning-Based Network Traffic Classification", *8th International Conference on Fog and Mobile Edge Computing (FMEC 2023)*, Tartu, Estonia, Sep. 18-20, 2023.

[C14] M. A. Aygül, **M. Nazzal**, and H. Arslan, "Estimating Multi-Dimensional Sparsity Level for Spectrum Sensing", *2023 IEEE Wireless Communications and Networking Conference (WCNC 2023)*, Glasgow, Scotland, UK, Mar. 2023.

[C13] M. A. Aygül, H. M. Furqan, **M. Nazzal**, and H. Arslan, "Deep Learning-Assisted Detection of PUEA and Jamming Attacks in Cognitive Radio Systems", *2020 IEEE 92nd Vehicular Technology Conference : VTC2020-Fall*, Victoria, BC, Canada, Oct. 2020.

[C12] **M. Nazzal**, A. Sawalmeh, S. Shao, M. Anan, A. Khreishah, and A. Alanazi, "Retro-VLP : Towards Single Light Source-based Real-time Indoor Positioning", *International Conference on Information and Communication Systems (ICICS 2022)*, Irbid-Jordan, Jun. 2022.

[C11] **M. Nazzal**, M. A. Aygül, and H. Arslan, "Estimation and Exploitation of Multidimensional Sparsity for MIMO-OFDM Channel Estimation", *2022 IEEE Wireless Communications and Networking Conference (WCNC 2022)*, Austin, TX, USA, Apr. 2022.

[C10] M. A. Aygül, **M. Nazzal**, and H. Arslan, "Deep RL-Based Spectrum Occupancy Prediction Exploiting Time and Frequency Correlations", *2022 IEEE Wireless Communications and Networking Conference (WCNC 2022)*, Austin, TX, USA, Apr. 2022.

[C9] **M. Nazzal**, M. A. Aygül, and H. Arslan, "Sparse Coding with Enhanced Atom Selection for FDD Massive MIMO Channel Estimation", *2021 IEEE 94th Vehicular Technology Conference : VTC2021-Fall*, Norman, OK, USA, Sep. 2021.

[C8] M. A. Aygül, **M. Nazzal**, and H. Arslan, "Using OMP and SD Algorithms Together in Millimeter Wave Massive MIMO Channel Estimation", *Signal Processing and Communications Applications Conference (SIU 2021)*, Istanbul, Turkey, Jun. 2021. **[Best Paper Award]**

[C7] M. A. Aygül, **M. Nazzal**, and H. Arslan, "Deep Learning-Based Optimal RIS Interaction Exploiting Previously Sampled Channel Correlations", *2021 IEEE Wireless Communications and Networking Conference (WCNC 2021)*, Nanjing, China, Mar. 2021.

[C6] M. A. Aygül, **M. Nazzal**, A. R. Ekti, A. Gorcin, D. B. da Costa, H. F. Ates, and H. Arslan, "Spectrum Occupancy Prediction Exploiting Time and Frequency Correlations Through 2D-LSTM", *2020 IEEE 91st Vehicular Technology Conference : VTC2020-Spring*, Antwerp, Belgium, May 2020.

[C5] **M. Nazzal**, O. Hasekioğlu, A. R. Ekti, A. Gorcin, and H. Arslan, "Compressed spectrum sensing using sparse recovery convergence patterns through machine learning classification", *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2019)*, Istanbul, Turkey, Sep. 2019.

[C4] **M. Nazzal**, M. A. Aygül, A. Görçin, and H. Arslan, "Dictionary learning-based beamspace channel estimation in millimeter-wave massive MIMO systems with a lens antenna array", *the International Wireless Communications & Mobile Computing Conference (IWCMC 2019)*, Tangier, Morocco, Jun. 2019.

[C3] **M. Nazzal**, M. A. Aygül, A. Görçin, and H. Arslan, "Sparse Coding for transform domain-based sparse OFDM channel estimation", *Signal Processing and Communications Applications Conference (SIU 2019)*, Sivas, Turkey, Apr. 2019.

[C2] **M. Nazzal**, H. M. Furqan, and H. Arslan, "FDD massive MIMO channel estimation by sparse coding over AoA/AoD cluster dictionaries", *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2018)*, Bologna, Italy, Sep. 2018.

[C1] H. M. Furqan, **M. Nazzal**, and H. Arslan, "Iterative tap pursuit for channel shortening equalizer design", *7th International Conference on Computer and Communication Engineering (ICCCE 2018)*, pp. 416-420, Kuala Lumpur, Malaysia, Sep. 2018.

Patent Disclosures

[P7] **M. Nazzal**, I. Khalil, A. Khreishah, and N.H. Phan, "Method and System for Prompt Optimization for Secure Generation of Functional Source Code with Large Language Models", *US Patent*, Patent Application No. : US63/561,573, Washington, D.C., USA, Filing date : Mar. 5, 2024.

[P6] M. A. Aygül, **M. Nazzal**, and H. Arslan, "Learning-Based Spectrum Occupancy Prediction Exploiting Multi-Dimensional Correlation", *US Patent*, Patent No. : US20230388809A1, Washington, D.C., USA, Publication date : Nov. 30, 2023.

[P5] M. A. Aygül, H. M. Furqan, **M. Nazzal**, and H. Arslan, "Primary User Emulation / Signal Jamming Attack Detection Method", *US Patent*, Patent No. : US20230025147A1, Washington, D.C., USA, Publication date : Jan. 26, 2023.

[P4] M. A. Aygül, H. M. Furqan, **M. Nazzal**, and H. Arslan, "Primary User Emulation / Signal Jamming Attack Detection Method", *Patent Cooperation Treaty (PCT)*, Patent No. : EP4082135A1, Munich, Germany, Publication date : Nov. 2, 2022.

[P3] M. A. Aygül, **M. Nazzal**, and H. Arslan, "Learning-Based Spectrum Occupancy Prediction Exploiting Multi-Dimensional Correlation", *Patent Cooperation Treaty (PCT)*, Patent No. : EP3989626A1, Munich, Germany, Publication date : Apr. 27, 2022.

[P2] M. A. Aygül, **M. Nazzal**, and H. Arslan, "Learning-Based Spectrum Occupancy Prediction Exploiting Multi-Dimensional Correlation", *European Patent Office (EPO) Patent Pending*, Patent No. : WO2022084096A1, Munich, Germany, Publication date : Apr. 28, 2022.

[P1] M. A. Aygül, H. M. Furqan, **M. Nazzal**, and H. Arslan, "Primary User Emulation / Signal Jamming Attack Detection Method", *World Intellectual Property Organization (WIPO)*, Patent No. : WO2021133312A1, Geneva, Switzerland, Publication date : Jul. 1, 2021.

Technical Skills

AI Programming Environments	**Pytorch**, **TensorFlow**, **Scikit-learn**, **PyG**, **DGL**
LLM-Related Skills	Retrieval-Augmented Generation (RAG), Vector Databases, Semantic Search
Programming Languages	**MATLAB**, **Python**, **C/C++**, **Java**
Cluster Computing Infrastructure	High-performance computing (HPC) utilizing **Slurm Wulver** for CPU/GPU nodes and parallel storage management, **Hadoop**, **Apache Spark** for data processing and analytics
Embedded Systems	**Micro-controllers**, **Arduino**
Technical Software	**Simulink**, **OrCAD**, **AutoCAD**, **LabVIEW**
Scientific and Professional Skills	Professional and Scientific Reporting, Grant Proposal Writing, Class Management in International English-Speaking Environments
Computer Literacy	**MS Windows**, **MS Office**, **Linux**, LaTeX

Seminars and Presentations

[S4] **M. Nazzal**, I. Khalil, A. Khreishah, and N.H. Phan, "PromSec : Prompt Optimization for Secure Generation of Functional Source Code with Large Language Models (LLMs)," 31st ACM Conference on Computer and Communications Security **(CCS 2024)**, Salt Lake City, U.S.A, USA, UT, Oct. 2024. *Covered by a US Provisional Patent*. (In person)

[S3] **M. Nazzal**, I. Khalil, A. Khreishah, N.H. Phan, and Y. Ma, "Multi-Instance Adversarial Attack on GNN-Based Malicious Domain Detection," 45th IEEE Symposium on Security and Privacy **(IEEE S&P 2024)**, San Francisco, CA, USA, May 2024. [Presentation Video]. (In person)

[S2] **M. Nazzal**, N. Aljaafari, A. Sawalmeh, A. Khreishah, M. Anan, A. Algosaibi, M. Alnaeem, A. Aldalbahi, A. Alhumam, C. P. Vizcarra, and S. Alhamed, "Genetic Algorithm-Based Dynamic Backdoor Attack on Federated Learning-Based Network Traffic Classification," 8th International Conference on Fog and Mobile Edge Computing **(FMEC 2023)**, Tartu, Estonia, Sep. 18-20, 2023. (Online)

[S1] Presenter at the **IEEE 802.11™ Wireless Local Area Networks standard meetings**. Represented Istanbul Medipol University and Vestel Group, contributing to cognitive radio in Nov. 2020. (Online)

Teaching Experience

May 2024 – Sep. 2022 | **New Jersey Institute of Technology, Newark, NJ, USA**
Lecturer, Courses Taught :
- Microprocessors
  - *Course evaluation : 3.29/4.00*
- Computer Architecture and Organization
  - *Course evaluation : Fall 3.69/4.00, Spring 3.24/4.00*

Jul. 2021 – Aug. 2019 | **Institute of Applied Technology, Abu Dhabi, UAE**
Lecturer, Courses Taught :
- Robotics
- Circuit Analysis
- Engineering Communications
- Graduation Project

Jun. 2017 – Sep. 2016 | **Izmir University of Economics, Izmir, Turkey**
Lecturer, Courses Taught :
- Graduation Project
- Java Programming
- Electric Circuits
- Digital Electronics
- Computer Organization and Architecture

Jun. 2016 – Sep. 2015 | **Eastern Mediterranean University, Famagusta, Cyprus**
Lecturer, Courses Taught :
- Introduction to Logic Design
- Computer Architecture and Organization
- C/C++ Programming
- Electric Circuits

Sep. 2015 – Oct. 2009 | **Eastern Mediterranean University, Famagusta, Cyprus**
Teaching Assistant, supervised laboratory sessions and conducted tutorials for the courses :
- Digital Signal Processing
- Introduction to Logic Design
- Introduction to Programming
- Signals and Systems

Mentoring Experience

2023 – 2022 | **Faculty Advisor, NJIT Undergraduate Summer Research and Innovation Symposium (Provost URI Summer Research Fellowship), Newark, NJ, USA**
Mentored summer interns Youssef Kanani and Pulami Basu, whose works were published in the NJIT annual conference proceedings.

2022 – 2021 | **Faculty Advisor, NJIT Undergraduate Summer Research and Innovation Symposium (Provost URI Summer Research Fellowship), Newark, NJ, USA**
Mentored summer intern Oscar Mahecha-Benitez whose work was published in the NJIT annual conference proceedings.

Professional Development and Certificates

- **Participant**, Virtual Excite the Dream Program, Old Dominion University, Sep. 2024.
- **Faculty Certificate in Smart Learning**, A Certified Online Faculty from Hamdan Bin Mohammed Smart University, Abu Dhabi, United Arab Emirates, March 2020.

Professional Affiliations

- The Institute of Electrical and Electronics Engineers (IEEE)
- Association for Computing Machinery (ACM)

Editing and Referee Service

- *IEEE/ACM Transactions on Networking*
- *IEEE Transactions on Signal Processing*
- *IEEE Transactions on Wireless Communications*
- *IEEE Wireless Communications Letters*
- *IEEE Access*

Relevant Courses

- Deep Learning on Graphs
- Statistical Machine Learning and Pattern Recognition
- Optimization Theory
- Optimization for Communication Networks
- Neural Networks
- Computational Intelligence
- Probability Theory
- Digital Image Processing

Languages

- **Arabic :** Native proficiency
- **English :** Fluent
- **Turkish :** Intermediate proficiency