Dr.-Ing. Kassem Kallas

Personal Information

Address:	5 Brighton Dr, Gaithersburg MD, 20877, USA
Email:	k_kallas@hotmail.com, kassem.kallas@nist.gov
Skype:	KassemKallas
Date of Birth:	27/08/1988
Place of Birth:	Saida, Lebanon
Nationality:	Lebanese
Date:	February 7, 2022

Biography

Dr. Kassem Kallas received his M.Sc. degree in Computer and Communication Engineering from Lebanese International University with a thesis in the field of radio channel coding. In 2013, he obtained a masters (advanced master II) in Wireless Systems and Related Technologies from Politecnico di Torino, Torino-Italy. He received his Ph.D. in Information Engineering and Mathematical Sciences in April 2017, working at the Visual Information Processing and Protection (VIPP) Lab under supervision of Professor Mauro Barni. His Ph.D thesis was in cybersecurity and focused on a Game-Theoretic approach for adversarial information fusion in distributed sensor networks. During his Ph.D he won two research scholarships one with the European Project AMULET (A MUlti-cLuE approach To image forensics) from the European Office of Aerospace Research and Development (EOARD); and from May 2017 till February 2018, he was a Chief Research Officer (CRO) at ViDiTrust srl. (Siena-Italy). At ViDiTrust, he worked on developing and improving an image analysis and pattern recognition system for anti-counterfeiting and security applications. From March 2018 till February 2020, he was a Postdoctoral Research Associate at the department of Information Engineering and Mathematics at University of Siena working on the use of machine learning and artificial neural networks for information security, and in particular, for adversarial signal processing. During his Postdoc, he published several papers (some of them were partially supported by a research sponsored by DARPA and Air Force Research Laboratory (AFRL) of the U.S. government and the Italian Ministry of University and Research (MUR)) in the fields of adversarial signal processing, and adversarial deep learning. Currently, he is a Research Scientist at the National Institute of Standards and Technology of the Department of Commerce, USA, where he is working on applying deep learning to wireless communication systems. Moreover, he is co-authored a book to published in Springer Signals and Communication Technology Book Series upon their invitation. Finally, he was a Lab-teaching assistant of Professor Abhir Bhalerao in his Ph.D. course "Interpretation and Analysis of Medical Images using Computational and Machine Learning techniques".

Research

My Ph.D research was mainly in cybersecurity and focused on the application side of Adversarial Signal Processing (Adv-SP). Briefly, Adv-SP is an emerging discipline that studies signal processing techniques explicitly to withstand intentional attacks of one or more adversaries. The aim is to model the interplay between a Defender, wishing to carry out a certain processing task, and an Attacker, with the aim at impeding it. A natural framework to model this interplay relies on Game-Theory since it provides a powerful mathematical model of conflict and cooperation between rational decision-makers. This framework helps to overcome the so called "cat & mouse" game in which researchers and system designers are continuously developing new attacks and countermeasures and also, helps us to understand who might be the winner. The

published results won the best paper at The Ninth International Conference on Advances in Multimedia, MMEDIA'17 and my Ph.D thesis was nominated by the University of Siena Ph.D board for the Springer "best-of-the-best" Ph.D thesis Award. During my Postdoc at University of Siena, I was working on adversarial signal processing and adversarial deep learning fields and I published several papers. Currently, I am looking on the application of deep learning on wireless communication systems.

Industrial Experience

After my Ph.D, I was a R & D scientist at ViDiTrust srl., a leading Italian company that is making a significant contribution to fighting counterfeiting. At ViDiTrust, I worked on developing and improving a cloud system capable of applying many image processing techniques and performing pattern recognition for anti-counterfeiting. By developing the system, I have gained a lot of experience in software engineering as I have to work on the back-end of the system. In addition, I have worked on developing a multimedia retrieval system for e-learning purposes. Furthermore, I applied and learned techniques on performing research with an industrial scope which is different from academic research. Moreover, I have widened my understanding of the business industry, especially because I was working and reporting to the CEO on a daily basis concerning the research side, and attending meetings and discussions with other companies on the technical and business sides. Currently, during my postdoctoral period, I am still collaborating with ViDiTrust. In this collaboration, I achieved the following:

- The development of CNN-based OCR system
- Development of different CNNs based anti-counterfeiting systems
- Developing a Generative Adversarial Network (GAN) based on DCGAN to generate synthetic images in an anti-counterfeiting context
- Contributing in writing projects
- Developing a real-time parking detection system using object recognition, based on ResNet101, and Yolo
- Setting up a first version of a system capable of performing live facial expressions detection and classification

Work and Academic Experience

Current date	*Research Fellow*, National Institute of Standards and Technology, Department of Commerce, Gaithersburg MD, USA
Feb. 2020	Application of deep learning on wireless communication systems.
Feb. 2020	*Postdoctoral Research Associate*, Department of Information Engineering and Mathematics, University of Siena, Siena, Italy
March 2018	Adversarial machine learning and artificial neural networks, pattern recognition, anti-counterfeiting,video processing for object recognition using deep learning, and adversarial signal processing.
February 2018	*R&D Scientist* at ViDiTrust s.r.l, Siena, Italy
May 2017	Digital image processing, analysis, and classification for anti-counterfeiting and security applications, multimedia retrieval.
Sep. 2013	*Research Internship* at Telecommucation Networks Group (TNG) Lab., Politecnico di Torino, Turin, Italy
June 2013	*Research Project:* Design and implementation of energy efficient rate adaptation technique for TCP protocol using Markov chain models. *Supervisor:* Professor Marco Ajmone Marsan and Professor Michela Meo.

Education

April 2017	Ph.D in Information Engineering and Mathematical Sciences - Research Line: Telecommunications and Telematics Technologies
Dec. 2013	University of Siena, Siena, Italy
	Thesis Title: A Game-Theoretic Approach for Adversarial Information Fusion in Distributed Sensor Networks
	Supervisor: Professor Mauro Barni
	Thesis Reviewers and Examination Committee: Prof. Vincenzo Matta, Prof. Vito Fragnelli and Prof. Andrea Garzelli.
	A full copy of the Ph.D. Dissertation can be found on one of the following links:
	- EURASIP Library of Ph.D. Theses: http://theses.eurasip.org/theses/718/a-game-theoretic-approach-for-adversarial/
	- VIPP research group website: http://clem.dii.unisi.it/ vipp/files/tesi/PhD_thesis_KassemKallas.pdf
	- ResearchGate: https://www.researchgate.net/publication/316621244_A_Game-Theoretic_Approach_for_Adversarial_Information_Fusion_in_Distributed_Sensor_Networks
Sep. 2013	Second Level Master in Wireless Systems and Related Technologies.
Sep. 2012	Politecnico di Torino, Turin, Italy
Jul. 2012	Master of Science (M.Sc.) in Computer and Communications Engineering
	Thesis Title: Simulation of bit-interleaved Low Density Parity Check code (LDPC) with iterative decoding system.
Oct. 2010	Lebanese International University, Beirut, Lebanon
Feb. 2010	Bachelor of Science (B.Sc.) in Telecommunications Engineering
Oct. 2006	Lebanese International University, Beirut, Lebanon

Professional Activities

- **Invited Speaker:** "Adversarial and Backdoor Attacks in Machine Learning", University of Warwick, December 2019, Coventry-United Kingdom.
- **Session Chair:** ICN 5: NGN and Network Management, IARIA MMEDIA 2017, Venice-Italy.
- **Technincal committee, PC member:** The 51^{st} International Carnahan Conference on Security Technology ICCST 2017.
- **Conference Reviewer:** IEEE WCNC'2016, IRACON-WS 2017, Inscrypt 2019, iSES 2019.
- **Journal Reviewer:** IEEE Transactions on Information Forensics and Security (TIFS), IEEE Transactions on Signal Processing, EURASIP Journal on Information Security, NIST internal reviewer.

PhD courses, Seminars and Schools

Please refer to the corresponding appendix.

Professional Membership

- IEEE Student and Young Professionals Member
- IEEE Signal Processing Society Member
- European Association for Signal Processing (EURASIP) Member
- Asia-Pacific Signal and Information Processing Association (APSIPA) Member
- Visual Information Processing and Protection (VIPP) Research Group Member

Technical Skills

- **Programming Languages:** Matlab, Python, C#, Java, Bash, SQL.
- **Deep Learning Frameworks:** Keras, Tensorflow, PyTorch.
- **Operating Systems:** Windows, Linux (Ubuntu, Backtrack).
- **Web Development:** HMTL, ASP.Net, MySQL, Posgres.
- **Application Software:** MATLAB/Simulink, MS. Office and Visual Studio, Netbeans, Eclipse, LaTeX, Pgadmin, WinSCP, pycharm, anaconda.

Languages

- **Arabic**: Native Speaker
- **English**: Fluent
- **Italian**: Fluent
- **French**: Basic

Certificates and Training

- *Generative Adversarial Networks (GANs) Specialization*, online specialization on Coursera, License Number: ZLPZRM2V2K9R, November 2020, *certification link*.
- *Deep Learning Specialization*, online specialization on Coursera by Prof. Andrew Ng, License Number: UED8HR9BGU2H, June 2018, *certification link*.
- IBM cognitiveclass.ai certificates: *Deep Learning*, *Applied Data Science with Python - Level II,*,*BlockChain*, 2018.
- *Machine Learning by Stanford University*, online course on Coursera by Prof. Andrew Ng, License Number: XBXMRK65QBZX, January 2017, *certification link*.
- *Internship on Microwave design for urban areas* at Ogero Telecom, Beirut, Lebanon Aug. 2011.

Honors and Awards

- **Best paper** award at the MMEDIA'17 conference, Venice-Italy, June 2017.
- **Research Scholarship:** Compilation of an inventory of techniques for data fusion in distributed sensor networks in the presence of an adverarsy and the implementation and testing over simulated data of the most promising techniques, Univeristy of Siena-Italy, January 2017. This funding was a part of the European Project AMULET: A MUlti-cLuE approach To image forensics from the European Office of Aerospace Research and Development (EOARD).
- **Research Scholarship:** Study and development of Adversarial Signal Processing (AdvSP) techniques based on game theory with applications to cognitive radio systems, Univeristy of Siena-Italy,April 2014.

Volunteer Experience

Current	*IEEE Collabortec: Mentor*
July 2019	Help students in scientific problems and discussing ideas about career and research.
Sep. 2011	*Lebanese Red Cross - Youth Volunteer*, Lebanon
Nov. 2010	The general activities of the youth volunteers are to carry out several activities directed towards a large segment of Lebanese society. They are aimed at raising awareness of the youth and children on means to erase wrong practices that fragment society. The volunteers take advantage of several occasions, such as national and international days, to organize activities, celebrations, and school and university seminars and workshops on health, environment, and prevention methods, and visits to patients in hospitals and nursing homes, as well as other functions that include fundraising to support Youth programs and Lebanese Red Cross activities.

Publications

Thesis

T.1 **Kassem Kallas**, "A Game-Theoretic Approach for Adversarial Information Fusion in Distributed Sensor Networks", Ph.D Thesis, University of Siena, 2017.
Note: The thesis was nominated for the Springer "best-of-the-best" PhD thesis Award.

T.2 **Kassem Kallas**, "Design of Capacity control for TCP protocol", Master II Thesis, Polytechnic University of Turin, 2013.

T.3 **Kassem Kallas**, "Simulation of Bit-Interleaved Coded Modulation with Iterative Decoding System", Msc. Thesis, Lebanese Internation University, 2012.

Books

B.1 Andrea Abrardo, Mauro Barni, **Kassem Kallas**, and Benedetta Tondi, *"Information Fusion in Distributed Sensor Networks with Byzantines"*, Springer Signals and Communication Technology Book Series, upcoming 2019.

Journal papers

J.1 Andrea Abrardo, Mauro Barni, **Kassem Kallas**, and Benedetta Tondi, "A Message Passing Approach for Decision Fusion in Adversarial Multi-Sensor Networks," *Information Fusion*, Volume 40, March 2018, 101-111, ISSN 1566-2535. *(IF = 12.975)*

J.2 Andrea Abrardo, Mauro Barni, **Kassem Kallas**, and Benedetta Tondi, "A Game-Theoretic Framework for Optimum Decision Fusion in the Presence of Byzantines," *in IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1333-1345, June 2016. *(IF = 6.211)*

Conference papers

C.1 Thao T. Nguyen, Raied Caromi, **Kassem Kallas**, and Michael R. Souryal " Deep Learning for Path Loss Prediction in the 3.5 GHz CBRS Spectrum Band," *Accepted at the IEEE Wireless Communications and Networking Conference 2022*, Austin, TX, USA, April 2022.

C.2 Raied Caromi, Alex Lackpour, **Kassem Kallas**, Thao T. Nguyen and Michael R. Souryal "Deep Learning for Radar Signal Detection in the 3.5 GHz CBRS Band," *Accepted at IEEE International Symposium on Dynamic Spectrum Access Networks (DySpan) 2021* , December 2021.

C.3 Mauro Barni, **Kassem Kallas**, Ehsan Nowroozi, and Benedetta Tondi " CNN Detection of GAN-Generated Face Images based on Cross-Band Co-occurrences Analysis," *Accepted paper at the* 12^{th} *IEEE International Workshop on Information Forensics and Security (WIFS) 2020*, New York, USA, December 2020.

C.4 Abhir Bhalerao, **Kassem Kallas**, Benedetta Tondi, and Mauro Barni " Luminance-based video backdoor attack against anti-spoofing rebroadcast detection," *Accepted paper at the* 21^{st} *IEEE International Workshop on Multimedia Signal Processing (MMSP'19)*, Kuala Lumpur, Malaysia, September 2019.

C.5 Mauro Barni, **Kassem Kallas**, and Benedetta Tondi, " A New Backdoor Attack in CNNs by Training Set Corruption without Label Poisoning," *in the* 26^{th} *IEEE International Conference on Image Processing (ICIP'19)*, TAPEI, TAIWAN, September 2019.

C.6 Mauro Barni, **Kassem Kallas**, Ehsan Nowroozi, and Benedetta Tondi, "On the Transferability of Adversarial Examples Against CNN-Based Image Forensics," *in the* 44^{th} *International Conference on Acoustics, Speech, and Signal Processing (ICASSP'19)*, Brighton, UK, May 2019.

C.7 Andrea Abrardo, Mauro Barni, **Kassem Kallas**, and Benedetta Tondi, "Decision Fusion with Unbalanced Priors under Synchronized Byzantine Attacks: a Message-Passing Approach," in the *IEEE Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, Honolulu, Hawaii, November 2018.

C.8 Andrea Abrardo, Mauro Barni, **Kassem Kallas**, and Benedetta Tondi, "A Message Passing Approach for Decision Fusion of Hidden-Markov observations in the presence of Synchronized Attacks in Sensor Network, "in *MMEDIA 2017, The Ninth International Conferences on Advances in Multimedia*, Venice, Italy, April 2017.
Note: Best Paper Award.

C.9 **Kassem Kallas**, Benedetta Tondi, Riccardo Lazzeretti and Mauro Barni, "Consensus Algorithm with Censored Data for Distributed Detection with Corrupted Measurements: A Game-Theoretic Approach," *in the* 7^{th} *Conference on Decision and Game Theory for Security*, New York, NY, November 2016.

C.10 Andrea Abrardo, Mauro Barni, **Kassem Kallas**, and Benedetta Tondi, "Decision fusion with corrupted reports in multi-sensor networks: a game-theoretic approach," in *IEEE Conference on Decision and Control (CDC)*, Los Angeles, California, December 2014.

[1]Following the convention of the VIPP research group, in all the papers published with VIPP group, the authors are mentioned in alphabetical order. In some particular cases, exceptions could be applied.

Academic Contact References

NIST	Dr. Nada T. Golmie National Institute of Standards and Technology, 100 Bureau Drive Gaithersburg, MD 20899, USA. Phone number: +1 (301) 975-4190 nada.golmie@nist.gov Website Dr. Golmie
University of Siena	Professor Mauro Barni Department of Information Engineering, University of Siena, Via Roma, 56, 53100 – Siena, Italy. Phone number: +39 0577 234850 int. 1005 barni@unisi.it Website Prof. Barni
University of Siena	Professor Andrea Abrardo Department of Information Engineering, University of Siena, Via Roma, 56, 53100, Siena, Italy. Phone number: +39 0577 234850 int. 1002 abrardo@diism.unisi.it Website Prof. Abrardo
University of Warwick	Professor Abhir Bhalerao Department of Computer Science, University of Warwick, CV4 7AL , Coventry, UK. Phone number: +44 02476 524910 abhir.bhalerao@warwick.ac.uk Website Prof. Bhalerao

Industrial Contact References

Centrica srl ViDiTrust srl	Eng. Marco Cappellini, CEO, CFO, President Centrica srl, Piazza della Madonna della Neve, 5, 50122, Italy. Phone number: +39 0552 466802 m.cappellini@centrica.it Website Centrica srl
ViDiTrust srl	Dr. Giacomo Cancelli, CEO, CTO ViDitrust srl, Via Fontebranda, 69, 53100, Siena, Italy. Phone number: +39 0577 45945 g.cancelli@viditrust.eu Website ViDitrust srl

- **Elements of Modern Physics (Basics of Quantum Physics):** Prof. Giuseppe Bevilacqua, University of Siena.
- **Linear Functional Analysis:** Prof. Duccio Papini, University of Siena.
- **Deep Learning**: Prof. Yoshua Bengio, University of Montreal.
- **Reinforcement Learning**: Prof. Maurizio Parton, University of "G. D'annunzio" Chieti-Pescara.
- **Signal Processing over Graphs: distributed optimization and bio-inspired mechanisms**: Prof. Sergio Barbarossa, University of La Sapienza.
- **Information Theory and Statistics**: Prof. Mauro Barni, University of Siena.
- **Statistical Signal Processing For Multimedia Forensics and Security**: Prof. Fernando Peréz Gonzáles, University of Vigo.
- **Bioinformatics: Models of Computation Inspired by the Functioning of the Living Cell: Natural Computing Approach**: Prof. Grzegorz Rozenberg, University of Leiden.
- **Physical Layer Security**: Prof. Lorenzo Mucchi, University of Florence.
- **Summer School**: 2015/2016/2018 IEEE SPS Italy Chapter Summer School on Signal Processing.
- **Seminar on Modulated Metasurface Antennas for Space Applications**: Prof. M. Sabbadini - European Space Agency, Paris.
- **Seminar on Challenges in Securing Vehicular Networks**: Prof. Rajeev Shorey - IT Research Academy, MediaLab Asia, Dept of IT, Government of India.
- **2016 Annual Meeting National Telecommunications and Information Theory Group - GTTI**: held at University of Genova.