

# Wade Trappe

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/2699116/publications.pdf>

Version: 2024-02-01

55  
papers

2,333  
citations

331642

21  
h-index

243610

44  
g-index

56  
all docs

56  
docs citations

56  
times ranked

2054  
citing authors

#	ARTICLE	IF	CITATIONS
1	An eavesdropping and jamming dilemma with sophisticated players. <i>ICT Express</i> , 2023, 9, 691-696.	4.8	2
2	Drug-Resistant Cancer Treatment Strategies Based on the Dynamics of Clonal Evolution and PKPD Modeling of Drug Combinations. <i>IEEE/ACM Transactions on Computational Biology and Bioinformatics</i> , 2022, 19, 1603-1614.	3.0	2
3	Projecting the Pandemic Trajectory through Modeling the Transmission Dynamics of COVID-19. <i>International Journal of Environmental Research and Public Health</i> , 2022, 19, 4541.	2.6	2
4	Dosage strategies for delaying resistance emergence in heterogeneous tumors. <i>FEBS Open Bio</i> , 2021, 11, 1322-1331.	2.3	2
5	A Multi-Jammer Power Control Game. <i>IEEE Communications Letters</i> , 2021, 25, 3031-3035.	4.1	3
6	A Multi-Jammer Game With Latency as the User's Communication Utility. <i>IEEE Communications Letters</i> , 2020, 24, 1899-1903.	4.1	11
7	Distributed beamforming based wireless power transfer: Analysis and realization. <i>Tsinghua Science and Technology</i> , 2020, 25, 758-775.	6.1	4
8	A Dilemma in the Communication of a UAV with its Controller. <i>International Game Theory Review</i> , 2020, 22, 2040003.	0.5	2
9	A Jamming Game With Rival-Type Uncertainty. <i>IEEE Transactions on Wireless Communications</i> , 2020, 19, 5359-5372.	9.2	27
10	Journal of Cybersecurity and Privacy: A New Open Access Journal. <i>Journal of Cybersecurity and Privacy</i> , 2020, 1, 1-3.	3.9	0
11	Drug Combinations: Mathematical Modeling and Networking Methods. <i>Pharmaceutics</i> , 2019, 11, 208.	4.5	37
12	A bargaining approach for resolving the tradeoff between beneficial and harmful drug responses. <i>Journal of Mathematical Biology</i> , 2018, 77, 1059-1072.	1.9	0
13	Cybersecurity: A New Open Access Journal. <i>Journal of Cybersecurity and Privacy</i> , 2018, 1, 1.	3.9	3
14	No Need for Speed : More Signal Processing Innovation Is Required Before Adopting Automated Vehicles [In the Spotlight]. <i>IEEE Signal Processing Magazine</i> , 2017, 34, 124-122.	5.6	1
15	Bandwidth Scanning When Facing Interference Attacks Aimed at Reducing Spectrum Opportunities. <i>IEEE Transactions on Information Forensics and Security</i> , 2017, 12, 1916-1930.	6.9	15
16	Competitive Sharing of Spectrum: Reservation Obfuscation and Verification Strategies. <i>Entropy</i> , 2017, 19, 363.	2.2	0
17	A Security Framework for the Internet of Things in the Future Internet Architecture. <i>Future Internet</i> , 2017, 9, 27.	3.8	93
18	Data Treasure Hunters: Science Expanding to New Frontiers [In the Spotlight]. <i>IEEE Signal Processing Magazine</i> , 2017, 34, 116-115.	5.6	0

#	ARTICLE	IF	CITATIONS
19	Overlay tunneling as a policy tool for defending mobile ad hoc networks. Security and Communication Networks, 2016, 9, 4482-4494.	1.5	1
20	Connectivity jamming game for physical layer attack in peer to peer networks. Security and Communication Networks, 2016, 9, 6080-6093.	1.5	0
21	An Online Admission Control Algorithm for Dynamic Traffic in Underlay Coexistence Paradigm. IEEE Transactions on Cognitive Communications and Networking, 2016, 2, 411-426.	7.9	0
22	Optimum Co-Design for Spectrum Sharing between Matrix Completion Based MIMO Radars and a MIMO Communication System. IEEE Transactions on Signal Processing, 2016, 64, 4562-4575.	5.3	269
23	Bargaining over the Fair Trade-Off Between Secrecy and Throughput in OFDM Communications. IEEE Transactions on Information Forensics and Security, 2016, , 1-1.	6.9	9
24	A Feature Article Cluster on Brain Signal Analytics: Analytical Approaches to Enhanced Understanding of Brain Function From the Editors. IEEE Signal Processing Magazine, 2016, 33, 12-13.	5.6	0
25	A Bandwidth Monitoring Strategy Under Uncertainty of the Adversary's Activity. IEEE Transactions on Information Forensics and Security, 2016, 11, 837-849.	6.9	33
26	Anti-jamming Strategy Versus a Low-Power Jamming Attack When Intelligence of Adversary's Attack Type is Unknown. IEEE Transactions on Signal and Information Processing Over Networks, 2016, 2, 49-56.	2.8	35
27	Topology adaptation for robust ad hoc cyberphysical networks under puncture-style attacks. Tsinghua Science and Technology, 2015, 20, 364-375.	6.1	1
28	Low-Energy Security: Limits and Opportunities in the Internet of Things. IEEE Security and Privacy, 2015, 13, 14-21.	1.2	199
29	One-Time Spectrum Coexistence in Dynamic Spectrum Access When the Secondary User May Be Malicious. IEEE Transactions on Information Forensics and Security, 2015, 10, 1064-1075.	6.9	23
30	Introduction to the Issue on Signal and Information Processing for Privacy. IEEE Journal on Selected Topics in Signal Processing, 2015, 9, 1173-1175.	10.8	2
31	The Role of Signal Processing in Meeting Privacy Challenges: An Overview. IEEE Signal Processing Magazine, 2013, 30, 95-106.	5.6	13
32	Secure Name Resolution for Identifier-to-Locator Mappings in the Global Internet. , 2013, , .		5
33	Physical layer secret key generation for fiber-optical networks. Optics Express, 2013, 21, 23756.	3.4	64
34	Optimizing scanning strategies: Selecting scanning bandwidth in adversarial RF environments. , 2013, , .		20
35	Predicting MIMO Performance in Urban Microcells Using Ray Tracing to Characterize the Channel. IEEE Transactions on Wireless Communications, 2012, 11, 2402-2411.	9.2	8
36	Detecting anomalous spectrum usage in dynamic spectrum access networks. Ad Hoc Networks, 2012, 10, 831-844.	5.5	24

#	ARTICLE	IF	CITATIONS
37	BIT-TRAPS: Building Information-Theoretic Traffic Privacy Into Packet Streams. IEEE Transactions on Information Forensics and Security, 2011, 6, 752-762.	6.9	15
38	Guest Editorial Special Issue on Using the Physical Layer for Securing the Next Generation of Communication Systems. IEEE Transactions on Information Forensics and Security, 2011, 6, 521-522.	6.9	4
39	Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks. IEEE Transactions on Vehicular Technology, 2010, 59, 2418-2434.	6.3	170
40	Information-Theoretically Secret Key Generation for Fading Wireless Channels. IEEE Transactions on Information Forensics and Security, 2010, 5, 240-254.	6.9	325
41	Exploiting the physical layer for enhanced security [Security and Privacy in Emerging Wireless Networks. IEEE Wireless Communications, 2010, 17, 63-70.	9.0	68
42	Achieving Secret Communication for Fast Rayleigh Fading Channels. IEEE Transactions on Wireless Communications, 2010, 9, 2792-2799.	9.2	50
43	Inverting Systems of Embedded Sensors for Position Verification in Location-Aware Applications. IEEE Transactions on Parallel and Distributed Systems, 2010, 21, 722-736.	5.6	2
44	Channel-Based Detection of Sybil Attacks in Wireless Networks. IEEE Transactions on Information Forensics and Security, 2009, 4, 492-503.	6.9	106
45	SEAR: a secure efficient ad hoc on demand routing protocol for wireless networks. Security and Communication Networks, 2009, 2, 325-340.	1.5	16
46	An IBC and certificate based hybrid approach to WiMAX security. Journal of Communications and Networks, 2009, 11, 615-625.	2.6	0
47	Secure wireless networking. Journal of Communications and Networks, 2009, 11, 323-327.	2.6	1
48	Characterizing indoor wireless channels via ray tracing combined with stochastic modeling. IEEE Transactions on Wireless Communications, 2009, 8, 4165-4175.	9.2	53
49	Channel-based spoofing detection in frequency-selective rayleigh channels. IEEE Transactions on Wireless Communications, 2009, 8, 5948-5956.	9.2	113
50	Secure, pseudonymous, and auditable communication in vehicular ad hoc networks. Security and Communication Networks, 2008, 1, 233-244.	1.5	36
51	Evaluation of Localization Attacks on Power-Modulated Challenge-Response Systems. IEEE Transactions on Information Forensics and Security, 2008, 3, 259-272.	6.9	7
52	Using the physical layer for wireless authentication in time-variant channels. IEEE Transactions on Wireless Communications, 2008, 7, 2571-2579.	9.2	278
53	Exploiting environmental properties for wireless localization. Mobile Computing and Communications Review, 2008, 12, 49-51.	1.7	1
54	Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationships. IEEE Transactions on Information Forensics and Security, 2007, 2, 793-808.	6.9	36

#	ARTICLE	IF	CITATIONS
55	Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation. IEEE Transactions on Image Processing, 2005, 14, 804-821.	9.8	142