

Kai Zeng

List of Publications by Year in Descending Order

Source: <https://exaly.com/author-pdf/8750428/kai-zeng-publications-by-year.pdf>

Version: 2024-04-28

This document has been generated based on the publications and citations recorded by exaly.com. For the latest version of this publication list, visit the link given above.

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

76
papers

1,329
citations

19
h-index

34
g-index

85
ext. papers

1,725
ext. citations

6.9
avg, IF

5.28
L-index

#	Paper	IF	Citations
76	Sharing Secrets via Wireless Broadcasting: A New Efficient Physical Layer Group Secret Key Generation for Multiple IoT Devices. <i>IEEE Internet of Things Journal</i> , 2022 , 1-1	10.7	1
75	Multuser Scheduling in Centralized Cognitive Radio Networks: A Multi-Armed Bandit Approach. <i>IEEE Transactions on Cognitive Communications and Networking</i> , 2022 , 1-1	6.6	1
74	Resource Allocation Optimization for Secure Multi-device Wirelessly Powered Backscatter Communication with Artificial Noise. <i>IEEE Transactions on Wireless Communications</i> , 2022 , 1-1	9.6	1
73	Orientation and Channel Independent RF Fingerprinting for 5G IEEE 802.11ad Devices. <i>IEEE Internet of Things Journal</i> , 2021 , 1-1	10.7	
72	Exploiting Beam Features for Spoofing Attack Detection in mmWave 60-GHz IEEE 802.11ad Networks. <i>IEEE Transactions on Wireless Communications</i> , 2021 , 20, 3321-3335	9.6	1
71	Machine Learning-Assisted Wireless PHY Key Generation with Reconfigurable Intelligent Surfaces 2021 ,		2
70	Manipulative Attack Against Physical Layer Key Agreement and Countermeasure. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2021 , 18, 475-489	3.9	5
69	Pilot Contamination Attack Detection for 5G MmWave Grant-Free IoT Networks. <i>IEEE Transactions on Information Forensics and Security</i> , 2021 , 16, 658-670	8	14
68	Physical Layer Secure MIMO Communications Against Eavesdroppers With Arbitrary Number of Antennas. <i>IEEE Transactions on Information Forensics and Security</i> , 2021 , 16, 466-481	8	9
67	Online-Learning-Based Defense Against Jamming Attacks in Multichannel Wireless CPS. <i>IEEE Internet of Things Journal</i> , 2021 , 8, 13278-13290	10.7	1
66	. <i>IEEE Access</i> , 2021 , 9, 60419-60432	3.5	4
65	Communication-Aware Secret Share Placement in Hierarchical Edge Computing. <i>IEEE Internet of Things Journal</i> , 2021 , 1-1	10.7	0
64	Enabling Efficient Blockage-Aware Handover in RIS-Assisted mmWave Cellular Networks. <i>IEEE Transactions on Wireless Communications</i> , 2021 , 1-1	9.6	2
63	Impact of Jamming Attacks on Vehicular Cooperative Adaptive Cruise Control Systems. <i>IEEE Transactions on Vehicular Technology</i> , 2020 , 69, 12679-12693	6.8	9
62	Compressed-Sensing-Based Pilot Contamination Attack Detection for NOMA-IoT Communications. <i>IEEE Internet of Things Journal</i> , 2020 , 7, 7764-7772	10.7	3
61	Physical Layer Authentication for 5G Communications: Opportunities and Road Ahead. <i>IEEE Network</i> , 2020 , 34, 198-204	11.4	10
60	Pilot Contamination Attack Detection for NOMA in 5G mm-Wave Massive MIMO Networks. <i>IEEE Transactions on Information Forensics and Security</i> , 2020 , 15, 1363-1378	8	15

59	A Practical Downlink NOMA Scheme for Wireless LANs. <i>IEEE Transactions on Communications</i> , 2020 , 68, 2236-2250	6.9	9
58	Machine Learning-Based Delay-Aware UAV Detection and Operation Mode Identification Over Encrypted Wi-Fi Traffic. <i>IEEE Transactions on Information Forensics and Security</i> , 2020 , 15, 2346-2360	8	17
57	Secure MIMO-SVD Communications Against Eavesdroppers With Any Number of Antennas. <i>IEEE Transactions on Vehicular Technology</i> , 2020 , 69, 11077-11089	6.8	2
56	Machine Learning-based Spoofing Attack Detection in MmWave 60GHz IEEE 802.11ad Networks 2020 ,		3
55	Privacy Protection and Efficient Incumbent Detection in Spectrum Sharing Based on Federated Learning 2020 ,		2
54	Identity-Based Attack Detection and Classification Utilizing Reciprocal RSS Variations in Mobile Wireless Networks. <i>IEEE Transactions on Mobile Computing</i> , 2020 , 1-1	4.6	1
53	Message Integrity Protection Over Wireless Channel: Countering Signal Cancellation via Channel Randomization. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2020 , 17, 106-120	3.9	7
52	Redundant Sniffer Deployment for Multi-Channel Wireless Network Forensics With Unreliable Conditions. <i>IEEE Transactions on Cognitive Communications and Networking</i> , 2020 , 6, 394-407	6.6	1
51	Light-Weight Physical Layer Enhanced Security Schemes for 5G Wireless Networks. <i>IEEE Network</i> , 2019 , 33, 126-133	11.4	23
50	Spoofing Attack Detection in Mm-Wave and Massive MIMO 5G Communication 2019 ,		2
49	A Reassessment on Friendly Jamming Efficiency. <i>IEEE Transactions on Mobile Computing</i> , 2019 , 1-1	4.6	2
48	Pairwise Markov Chain: A Task Scheduling Strategy for Privacy-Preserving SIFT on Edge 2019 ,		7
47	Optimal Resource Allocation for Secure Multi-User Wireless Powered Backscatter Communication with Artificial Noise 2019 ,		10
46	Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. <i>IEEE Internet of Things Journal</i> , 2019 , 6, 8169-8181	10.7	104
45	Physical Layer Key Generation in 5G Wireless Networks. <i>IEEE Wireless Communications</i> , 2019 , 26, 48-54	13.4	22
44	Large-scale Cost-Aware Classification Using Feature Computational Dependency Graph. <i>IEEE Transactions on Knowledge and Data Engineering</i> , 2019 , 1-1	4.2	2
43	Robust Spectrum Monitoring in Cognitive Radio Networks With Uncertain Traffic Information. <i>IEEE Access</i> , 2018 , 6, 34696-34706	3.5	1
42	Guest Editorial Special Issue on Trust, Security, and Privacy in Crowdsourcing. <i>IEEE Internet of Things Journal</i> , 2018 , 5, 2880-2883	10.7	1

41	Physical Layer Key Generation Using Virtual AoA and AoD of mmWave Massive MIMO Channel 2018		17
40	A Survey on Security, Privacy, and Trust in Mobile Crowdsourcing. <i>IEEE Internet of Things Journal</i> , 2018 , 5, 2971-2992	10.7	68
39	Physical layer multi-user key generation in wireless networks. <i>Wireless Networks</i> , 2018 , 24, 1043-1054	2.5	3
38	Secret Beam: Robust Secret Key Agreement for mmWave Massive MIMO 5G Communication 2018 ,		8
37	Efficient Identity Spoofing Attack Detection for IoT in mm-Wave and Massive MIMO 5G Communication 2018 ,		8
36	Explore Recurrent Neural Network for PUE Attack Detection in Practical CRN Models 2018 ,		3
35	Prediction-time Efficient Classification Using Feature Computational Dependencies 2018 ,		12
34	Online Learning With Randomized Feedback Graphs for Optimal PUE Attacks in Cognitive Radio Networks. <i>IEEE/ACM Transactions on Networking</i> , 2018 , 26, 2268-2281	3.8	8
33	. <i>IEEE Transactions on Wireless Communications</i> , 2018 , 17, 7849-7864	9.6	35
32	Pilot Contamination Attack Detection for NOMA in Mm-Wave and Massive MIMO 5G Communication 2018 ,		8
31	Secure Inductive-Coupled Near Field Communication at Physical Layer. <i>IEEE Transactions on Information Forensics and Security</i> , 2018 , 13, 3078-3093	8	6
30	String Stability Analysis of Cooperative Adaptive Cruise Control under Jamming Attacks 2017 ,		29
29	Throughput optimization in multi-hop wireless networks with reconfigurable antennas 2017 ,		2
28	Achieving Unconditional Security for MIMO-BAN under Short Blocklength Wiretap Code 2017 ,		3
27	Delay Analysis of Physical-Layer Key Generation in Dynamic Roadside-to-Vehicle Networks. <i>IEEE Transactions on Vehicular Technology</i> , 2017 , 66, 2526-2535	6.8	19
26	Practical Secret Key Agreement for Full-Duplex Near Field Communications. <i>IEEE Transactions on Mobile Computing</i> , 2016 , 15, 938-951	4.6	15
25	MagPairing: Pairing Smartphones in Close Proximity Using Magnetometers. <i>IEEE Transactions on Information Forensics and Security</i> , 2016 , 11, 1306-1320	8	35
24	Intelligence Measure of Cognitive Radios with Learning Capabilities 2016 ,		3

23	Online learning-based optimal primary user emulation attacks in cognitive radio networks 2016 ,		7
22	A smartphone-based driver fatigue detection using fusion of multiple real-time facial features 2016 ,		19
21	Online learning for unreliable passive monitoring in multi-channel wireless networks 2015 ,		4
20	Live Video Forensics: Source Identification in Lossy Wireless Networks. <i>IEEE Transactions on Information Forensics and Security</i> , 2015 , 10, 28-39	8	17
19	Physical layer key generation in wireless networks: challenges and opportunities 2015 , 53, 33-39		124
18	Physical layer key agreement under signal injection attacks 2015 ,		2
17	MagPairing: Exploiting magnetometers for pairing smartphones in close proximity 2014 ,		4
16	PHY-CRAM: Physical Layer Challenge-Response Authentication Mechanism for Wireless Networks. <i>IEEE Journal on Selected Areas in Communications</i> , 2013 , 31, 1817-1827	14.2	57
15	Adaptive Wireless Channel Probing for Shared Key Generation Based on PID Controller. <i>IEEE Transactions on Mobile Computing</i> , 2013 , 12, 1842-1852	4.6	32
14	Video source identification in lossy wireless networks 2013 ,		7
13	Hearing Is Believing: Detecting Wireless Microphone Emulation Attacks in White Space. <i>IEEE Transactions on Mobile Computing</i> , 2013 , 12, 401-411	4.6	18
12	On energy efficiency of geographic opportunistic routing in lossy multihop wireless networks. <i>Wireless Networks</i> , 2012 , 18, 967-983	2.5	14
11	Edge-prioritized channel- and traffic-aware uplink Carrier Aggregation in LTE-advanced systems 2012 ,		13
10	Chaining for securing data provenance in distributed information networks 2012 ,		4
9	Hearing is believing: Detecting mobile primary user emulation attack in white space 2011 ,		19
8	Probability Density of the Received Power in Mobile Networks. <i>IEEE Transactions on Wireless Communications</i> , 2011 , 10, 3613-3619	9.6	53
7	Opportunistic spectrum scheduling for mobile cognitive radio networks in white space 2011 ,		12
6	Opportunistic Routing Security 2011 , 213-229		

5	Adaptive wireless channel probing for shared key generation 2011 ,	30
4	Identity-based attack detection in mobile wireless networks 2011 ,	19
3	Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks 2010 ,	115
2	Non-cryptographic authentication and identification in wireless networks [Security and Privacy in Emerging Wireless Networks]. <i>IEEE Wireless Communications</i> , 2010 , 17, 56-62	13.4 156
1	Metrics for Evaluating Video Streaming Quality in Lossy IEEE 802.11 Wireless Networks 2010 ,	26