Raheem Beyah

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/11082403/publications.pdf

Version: 2024-02-01

63	1,086	516710 16	501196 28
papers	citations	h-index	g-index

64	64	64	973
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 1826-1840.	5.4	17
2	Towards Certifying the Asymmetric Robustness for Neural Networks: Quantification and Applications. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 3987-4001.	5.4	1
3	A Practical Side-Channel Based Intrusion Detection System for Additive Manufacturing Systems. , 2021, , .		1
4	OB-WSPES: A Uniform Evaluation System for Obfuscation-based Web Search Privacy. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.	5.4	2
5	Text Captcha Is Dead? A Large Scale Deployment and Empirical Study. , 2020, , .		14
6	A privacyâ€preserving multifactor authentication system. Security and Privacy, 2019, 2, e88.	2.7	9
7	Towards understanding the security of modern image captchas and underground captcha-solving services. Big Data Mining and Analytics, 2019, 2, 118-144.	8.9	21
8	Enabling a Decentralized Smart Grid Using Autonomous Edge Control Devices. IEEE Internet of Things Journal, 2019, 6, 7406-7419.	8.7	35
9	A secure routing protocol with regional partitioned clustering and Beta trust management in smart home. Wireless Networks, 2019, 25, 3805-3823.	3.0	6
10	Attacker Location Evaluation-Based Fake Source Scheduling for Source Location Privacy in Cyber-Physical Systems. IEEE Transactions on Information Forensics and Security, 2019, 14, 1337-1350.	6.9	26
11	HoneyBot: A Honeypot for Robotic Systems. Proceedings of the IEEE, 2018, 106, 61-70.	21.3	21
12	DPPG: A Dynamic Password Policy Generation System. IEEE Transactions on Information Forensics and Security, 2018, 13, 545-558.	6.9	11
13	SOTA: Secure Over-the-Air Programming of IoT Devices. , 2018, , .		8
14	Quantifying Graph Anonymity, Utility, and De-anonymity. , 2018, , .		5
15	Emerging Technologies for Connected and Smart Vehicles. IEEE Communications Magazine, 2018, 56, 20-21.	6.1	5
16	Zero-Sum Password Cracking Game: A Large-Scale Empirical Study on the Crackability, Correlation, and Security of Passwords. IEEE Transactions on Dependable and Secure Computing, 2017, 14, 550-564.	5.4	33
17	Graph Data Anonymization, De-Anonymization Attacks, and De-Anonymizability Quantification: A Survey. IEEE Communications Surveys and Tutorials, 2017, 19, 1305-1326.	39.4	79
18	Password correlation: Quantification, evaluation and application. , 2017, , .		4

#	Article	IF	Citations
19	Structural Data De-Anonymization: Theory and Practice. IEEE/ACM Transactions on Networking, 2016, 24, 3523-3536.	3.8	22
20	On the relative de-anonymizability of graph data: Quantification and evaluation. , 2016, , .		15
21	Rethinking the Honeypot for Cyber-Physical Systems. IEEE Internet Computing, 2016, 20, 9-17.	3.3	58
22	Seed-Based De-Anonymizability Quantification of Social Networks. IEEE Transactions on Information Forensics and Security, 2016, 11, 1398-1411.	6.9	27
23	Information Leakage in Encrypted IP Video Traffic. , 2015, , .		11
24	Primary social behavior aware routing and scheduling for Cognitive Radio Networks. , 2015, , .		9
25	Whitespace measurement and virtual backbone construction for Cognitive Radio Networks: From the social perspective. , 2015, , .		7
26	Attacking and securing beacon-enabled 802.15.4 networks. Wireless Networks, 2015, 21, 1517-1535.	3.0	1
27	Using Network Traffic to Infer Hardware State. Transactions on Embedded Computing Systems, 2015, 14, 1-22.	2.9	6
28	Constructing loadâ€balanced virtual backbones in probabilistic wireless sensor networks via multiâ€objective genetic algorithm. Transactions on Emerging Telecommunications Technologies, 2015, 26, 147-163.	3.9	13
29	GTID: A Technique for Physical Device <italic>and</italic> Device Type Fingerprinting. IEEE Transactions on Dependable and Secure Computing, 2015, 12, 519-532.	5.4	138
30	Broadcast Scheduling with Latency and Redundancy Analysis for Cognitive Radio Networks. IEEE Transactions on Vehicular Technology, 2014, , 1-1.	6.3	3
31	Active deception model for securing cloud infrastructure. , 2014, , .		8
32	Snapshot and Continuous Data Collection in Probabilistic Wireless Sensor Networks. IEEE Transactions on Mobile Computing, 2014, 13, 626-637.	5.8	41
33	MACA: A privacy-preserving multi-factor cloud authentication system utilizing big data. , 2014, , .		27
34	Information Leakage in Encrypted IP Video Traffic. , 2014, , .		1
35	Cell-based snapshot and continuous data collection in wireless sensor networks. ACM Transactions on Sensor Networks, 2013, 9, 1-29.	3.6	14
36	Semi-Structure Routing and Performance Analysis for Cognitive Radio Networks. , 2013, , .		4

#	Article	IF	Citations
37	PROVIZ: An integrated visualization and programming framework for WSNs. , 2013, , .		2
38	A Multi-Objective Genetic Algorithm for constructing load-balanced virtual backbones in probabilistic Wireless Sensor Networks. , 2013, , .		2
39	Minimum-Latency Broadcast Scheduling for Cognitive Radio Networks. , 2013, , .		23
40	Practical unicast and convergecast scheduling schemes for cognitive radio networks. Journal of Combinatorial Optimization, 2013, 26, 161-177.	1.3	15
41	CLIP: Content labeling in IPv6, a layer 3 protocol for information centric networking. , 2013, , .		3
42	Broadcast Scheduling for Cognitive Radio Networks. , 2013, , .		0
43	Plugging the leaks without unplugging your network in the midst of Disaster. , 2012, , .		1
44	Snapshot/Continuous Data Collection capacity for large-scale probabilistic Wireless Sensor Networks. , 2012, , .		24
45	Guest editorial: Special issue on wireless computing and networking. Tsinghua Science and Technology, 2012, 17, 485-486.	6.1	0
46	SIMAGE: Secure and Link-Quality Cognizant Image Distribution for wireless sensor networks. , 2012, , .		5
47	An 802.11 MAC layer covert channel. Wireless Communications and Mobile Computing, 2012, 12, 393-405.	1.2	22
48	On the construction of k-connected m-dominating sets in wireless networks. Journal of Combinatorial Optimization, 2012, 23, 118-139.	1.3	38
49	Continuous Data Collection Capacity of Wireless Sensor Networks under Physical Interference Model. , 2011, , .		27
50	Covert DCF: A DCF-Based Covert Timing Channel in 802.11 Networks. , 2011, , .		24
51	Sensor scheduling for p-percent coverage in wireless sensor networks. Cluster Computing, 2011, 14, 27-40.	5.0	44
52	SMITE: A stochastic compressive data collection protocol for Mobile Wireless Sensor Networks. , 2011, , .		27
53	DSF - A Distributed Security Framework for heterogeneous wireless sensor networks. , 2010, , .		4
54	A Passive Solution to the Memory Resource Discovery Problem in Computational Clusters. IEEE Transactions on Network and Service Management, 2010, 7, 218-230.	4.9	7

#	Article	IF	Citations
55	Delay-Bounded and Energy-Efficient Composite Event Monitoring in Heterogeneous Wireless Sensor Networks. IEEE Transactions on Parallel and Distributed Systems, 2010, 21, 1373-1385.	5.6	29
56	Authentic delay bounded event detection in heterogeneous wireless sensor networks. Ad Hoc Networks, 2009, 7, 599-613.	5.5	7
57	Filtering Spam by Using Factors Hyperbolic Tree. , 2008, , .		0
58	Dynamic Energy-based Encoding and Filtering in Sensor Networks. , 2007, , .		11
59	A passive approach to rogue access point detection. , 2007, , .		30
60	Using Network Traffic to Passively Detect Under Utilized Resources in High Performance Cluster Grid Computing Environments. , 2007, , .		6
61	Securing Wireless Networks Using Device Type Identification. , 2007, , 191-221.		0
62	A Passive Approach to Wireless NIC Identification. , 2006, , .		28
63	D etect S ec : Evaluating the robustness of object detection models to adversarial attacks. International Journal of Intelligent Systems, 0, , .	5.7	0