

Sheng Wen

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/7494581/publications.pdf>

Version: 2024-02-01

91
papers

3,490
citations

218677

26
h-index

175258

52
g-index

94
all docs

94
docs citations

94
times ranked

3095
citing authors

#	ARTICLE	IF	CITATIONS
1	The Fog Computing Paradigm: Scenarios and Security Issues. , 0, , .		632
2	An overview of Fog computing and its security issues. Concurrency Computation Practice and Experience, 2016, 28, 2991-3005.	2.2	291
3	Software Vulnerability Detection Using Deep Neural Networks: A Survey. Proceedings of the IEEE, 2020, 108, 1825-1848.	21.3	214
4	Android HIV: A Study of Repackaging Malware for Evading Machine-Learning Detection. IEEE Transactions on Information Forensics and Security, 2020, 15, 987-1001.	6.9	182
5	Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey. IEEE/CAA Journal of Automatica Sinica, 2022, 9, 377-391.	13.1	150
6	Identifying Propagation Sources in Networks: State-of-the-Art and Comparative Studies. IEEE Communications Surveys and Tutorials, 2017, 19, 465-481.	39.4	148
7	A Sword with Two Edges: Propagation Studies on Both Positive and Negative Information in Online Social Networks. IEEE Transactions on Computers, 2015, 64, 640-653.	3.4	142
8	Modeling the Propagation of Worms in Networks: A Survey. IEEE Communications Surveys and Tutorials, 2014, 16, 942-960.	39.4	135
9	Twitter spam detection: Survey of new approaches and comparative study. Computers and Security, 2018, 76, 265-284.	6.0	116
10	To Shut Them Up or to Clarify: Restraining the Spread of Rumors in Online Social Networks. IEEE Transactions on Parallel and Distributed Systems, 2014, 25, 3306-3316.	5.6	99
11	Detection and defense of application-layer DDoS attacks in backbone web traffic. Future Generation Computer Systems, 2014, 38, 36-46.	7.5	93
12	Modeling Propagation Dynamics of Social Network Worms. IEEE Transactions on Parallel and Distributed Systems, 2013, 24, 1633-1643.	5.6	87
13	Rumor Source Identification in Social Networks with Time-Varying Topology. IEEE Transactions on Dependable and Secure Computing, 2018, 15, 166-179.	5.4	74
14	Fuzzing: A Survey for Roadmap. ACM Computing Surveys, 2022, 54, 1-36.	23.0	61
15	Modeling and Analysis on the Propagation Dynamics of Modern Email Malware. IEEE Transactions on Dependable and Secure Computing, 2014, 11, 361-374.	5.4	58
16	K-Center: An Approach on the Multi-Source Identification of Information Diffusion. IEEE Transactions on Information Forensics and Security, 2015, 10, 2616-2626.	6.9	57
17	On the Race of Worms and Patches: Modeling the Spread of Information in Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security, 2016, 11, 2854-2865.	6.9	52
18	Bandwidth-aware energy efficient flow scheduling with SDN in data center networks. Future Generation Computer Systems, 2017, 68, 163-174.	7.5	51

#	ARTICLE	IF	CITATIONS
19	TouchWB : Touch behavioral user authentication based on web browsing on smartphones. Journal of Network and Computer Applications, 2018, 117, 1-9.	9.1	51
20	DeepBalance: Deep-Learning and Fuzzy Oversampling for Vulnerability Detection. IEEE Transactions on Fuzzy Systems, 2019, , 1-1.	9.8	50
21	Intersection Traffic Prediction Using Decision Tree Models. Symmetry, 2018, 10, 386.	2.2	48
22	Propagation Modeling and Defending of a Mobile Sensor Worm in Wireless Sensor and Actuator Networks. Sensors, 2017, 17, 139.	3.8	46
23	Following Targets for Mobile Tracking in Wireless Sensor Networks. ACM Transactions on Sensor Networks, 2016, 12, 1-24.	3.6	39
24	Efficient and secure attribute-based signature for monotone predicates. Acta Informatica, 2017, 54, 521-541.	0.5	38
25	Investigating the deceptive information in Twitter spam. Future Generation Computer Systems, 2017, 72, 319-326.	7.5	38
26	Using epidemic betweenness to measure the influence of users in complex networks. Journal of Network and Computer Applications, 2017, 78, 288-299.	9.1	32
27	On the Security of Networked Control Systems in Smart Vehicle and Its Adaptive Cruise Control. IEEE Transactions on Intelligent Transportation Systems, 2021, 22, 3824-3831.	8.0	28
28	Publicly verifiable database scheme with efficient keyword search. Information Sciences, 2019, 475, 18-28.	6.9	26
29	Detecting spamming activities in twitter based on deep learning technique. Concurrency Computation Practice and Experience, 2017, 29, e4209.	2.2	25
30	Malware Propagations in Wireless Ad Hoc Networks. IEEE Transactions on Dependable and Secure Computing, 2018, 15, 1016-1026.	5.4	25
31	CALD: Surviving Various Application-Layer DDoS Attacks That Mimic Flash Crowd. , 2010, , .		24
32	Daedalus: Breaking Nonmaximum Suppression in Object Detection via Adversarial Examples. IEEE Transactions on Cybernetics, 2022, 52, 7427-7440.	9.5	24
33	Covert Attacks Through Adversarial Learning: Study of Lane Keeping Attacks on the Safety of Autonomous Vehicles. IEEE/ASME Transactions on Mechatronics, 2021, 26, 1350-1357.	5.8	21
34	A Man-in-the-Middle Attack on 3G-WLAN Interworking. , 2010, , .		20
35	Locating Defense Positions for Thwarting the Propagation of Topological Worms. IEEE Communications Letters, 2012, 16, 560-563.	4.1	19
36	Traceable Identity-Based Group Signature. RAIRO - Theoretical Informatics and Applications, 2016, 50, 193-226.	0.5	19

#	ARTICLE	IF	CITATIONS
37	On-Street Car Parking Prediction in Smart City: A Multi-source Data Analysis in Sensor-Cloud Environment. Lecture Notes in Computer Science, 2017, , 641-652.	1.3	18
38	Are the popular users always important for information dissemination in online social networks?. IEEE Network, 2014, 28, 64-67.	6.9	14
39	Maximizing real-time streaming services based on a multi-servers networking framework. Computer Networks, 2015, 93, 199-212.	5.1	14
40	Reliable wireless connections for fast-moving rail users based on a chained fog structure. Information Sciences, 2017, 379, 160-176.	6.9	14
41	Backdoor Attack on Machine Learning Based Android Malware Detectors. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 3357-3370.	5.4	13
42	Traffic Flow Prediction for Road Intersection Safety. , 2018, , .		12
43	Crowdsensing From the Perspective of Behavioral Economics: An Incentive Mechanism Based on Mental Accounting. IEEE Internet of Things Journal, 2019, 6, 9123-9139.	8.7	12
44	The Microcosmic Model of Worm Propagation. Computer Journal, 2011, 54, 1700-1720.	2.4	11
45	The structure of communities in scale-free networks. Concurrency Computation Practice and Experience, 2017, 29, e4040.	2.2	11
46	Using AI to Attack VA: A Stealthy Spyware Against Voice Assistances in Smart Phones. IEEE Access, 2019, 7, 153542-153554.	4.2	11
47	SADI: A Novel Model to Study the Propagation of Social Worms in Hierarchical Networks. IEEE Transactions on Dependable and Secure Computing, 2019, 16, 142-155.	5.4	11
48	Addictive Incentive Mechanism in Crowdsensing From the Perspective of Behavioral Economics. IEEE Transactions on Parallel and Distributed Systems, 2022, 33, 1109-1127.	5.6	10
49	Eliminating Errors in Worm Propagation Models. IEEE Communications Letters, 2011, 15, 1022-1024.	4.1	9
50	Pokémon GO in Melbourne CBD: A case study of the cyber-physical symbiotic social networks. Journal of Computational Science, 2018, 26, 456-467.	2.9	9
51	Defending Against Adversarial Attack Towards Deep Neural Networks Via Collaborative Multi-Task Training. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 953-965.	5.4	9
52	Man-in-the-Middle Attacks Against Machine Learning Classifiers Via Malicious Generative Models. IEEE Transactions on Dependable and Secure Computing, 2021, 18, 2074-2087.	5.4	9
53	Faces are Protected as Privacy: An Automatic Tagging Framework Against Unpermitted Photo Sharing in Social Media. IEEE Access, 2019, 7, 75556-75567.	4.2	8
54	A Feature-Oriented Corpus for Understanding, Evaluating and Improving Fuzz Testing. , 2019, , .		8

#	ARTICLE	IF	CITATIONS
55	Missing Value Filling Based on the Collaboration of Cloud and Edge in Artificial Intelligence of Things. IEEE Transactions on Industrial Informatics, 2022, 18, 5394-5402.	11.3	8
56	Secure fine-grained spatio-temporal Top- k queries in TMWSNs. Future Generation Computer Systems, 2018, 86, 174-184.	7.5	7
57	CSI-Fuzz: Full-speed Edge Tracing Using Coverage Sensitive Instrumentation. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.	5.4	6
58	Edge-based stochastic network model reveals structural complexity of edges. Future Generation Computer Systems, 2019, 100, 1073-1087.	7.5	5
59	First-Priority Relation Graph-Based Malicious Users Detection in Mobile Social Networks. Lecture Notes in Computer Science, 2015, , 459-466.	1.3	5
60	A Lightweight Intrusion Alert Fusion System. , 2010, , .		3
61	CAFS: a novel lightweight cache-based scheme for large-scale intrusion alert fusion. Concurrency Computation Practice and Experience, 2012, 24, 1137-1153.	2.2	3
62	Network Topology Inference Using Higher-Order Statistical Characteristics of End-to-End Measured Delays. IEEE Access, 2020, 8, 59960-59975.	4.2	3
63	Fuzzing With Optimized Grammar-Aware Mutation Strategies. IEEE Access, 2021, 9, 95061-95071.	4.2	3
64	Social Media Event Prediction using DNN with Feedback Mechanism. ACM Transactions on Management Information Systems, 2022, 13, 1-24.	2.8	3
65	Mobility Increases the Risk of Malware Propagations in Wireless Networks. , 2015, , .		2
66	Catch Me If You Can: Detecting Compromised Users Through Partial Observation on Networks. , 2017, , .		2
67	How Spam Features Change in Twitter and the Impact to Machine Learning Based Detection. Lecture Notes in Computer Science, 2017, , 898-904.	1.3	2
68	Hiding RFID in the Image Matching Based Access Control to a Smart Building. , 2018, , .		2
69	Who Spread to Whom? Inferring Online Social Networks with User Features. , 2018, , .		2
70	Catering to Your Concerns. ACM Transactions on Cyber-Physical Systems, 2019, 3, 1-21.	2.5	2
71	Malicious Attack Propagation and Source Identification. Advances in Information Security, 2019, , .	1.2	2
72	Vulnerability Detection in IoT Applications: A Fuzzing Method on their Binaries. IEEE Transactions on Network Science and Engineering, 2022, 9, 970-979.	6.4	2

#	ARTICLE	IF	CITATIONS
73	Characterizing Sensor Leaks in Android Apps. , 2021, , .		2
74	Modeling worms propagation on probability. , 2011, , .		1
75	Identifying Diffusion Sources in Large Networks: A Community Structure Based Approach. , 2015, , .		1
76	Analysis of the Spreading Influence Variations for Online Social Users under Attacks. , 2016, , .		1
77	My Face is Mine: Fighting Unpermitted Tagging on Personal/Group Photos in Social Media. Lecture Notes in Computer Science, 2017, , 528-539.	1.3	1
78	Every word is valuable: Studied influence of negative words that spread during election period in social media. Concurrency Computation Practice and Experience, 2019, 31, e4525.	2.2	1
79	Static Detection of File Access Control Vulnerabilities on Windows System. Concurrency Computation Practice and Experience, 2020, , e6004.	2.2	1
80	Synthesized Corpora to Evaluate Fuzzing for Green Internet of Things Programs. IEEE Transactions on Green Communications and Networking, 2021, 5, 1041-1050.	5.5	1
81	Real-Time Detection of COVID-19 Events From Twitter: A Spatial-Temporally Bursty-Aware Method. IEEE Transactions on Computational Social Systems, 2023, 10, 656-672.	4.4	1
82	An Analytical Model on the Propagation of Modern Email Worms. , 2012, , .		0
83	Detecting stepping stones by abnormal causality probability. Security and Communication Networks, 2015, 8, 1831-1844.	1.5	0
84	The Relation Between Local and Global Influence of Individuals in Scale-Free Networks. , 2015, , .		0
85	Forward to the special issue of the 9th International Symposium on Cyberspace Safety and Security (CSS 2017). Concurrency Computation Practice and Experience, 2019, 31, e5535.	2.2	0
86	Identifying Propagation Source in Large-Scale Networks. Advances in Information Security, 2019, , 159-178.	1.2	0
87	Identifying Multiple Propagation Sources. Advances in Information Security, 2019, , 139-157.	1.2	0
88	Detecting Stepping Stones by Abnormal Causality Probability. Lecture Notes in Computer Science, 2013, , 308-322.	1.3	0
89	Modeling and Analysis for Thwarting Worm Propagation in Email Networks. Lecture Notes in Computer Science, 2013, , 763-769.	1.3	0
90	Restrain Malicious Attack Propagation. Advances in Information Security, 2019, , 41-62.	1.2	0

#	ARTICLE	IF	CITATIONS
91	SAM: Multi-turn Response Selection Based on Semantic Awareness Matching. ACM Transactions on Internet Technology, 2023, 23, 1-18.	4.4	0