Zhihong Tian

List of Publications by Year in Descending Order

111 papers	2,195 citations	23 h-index	44 g-index
128 ext. papers	3,376 ext. citations	4.4 avg, IF	6.09 L-index

#	Paper	IF	Citations
111	Dynamic Prototype Network based on Sample Adaptation for Few-Shot Malware Detection. *IEEE Transactions on Knowledge and Data Engineering*, **2022**, 1-1	4.2	4
110	Epidemic Risk Assessment by a Novel Communication Station Based Method.. *IEEE Transactions on Network Science and Engineering*, **2022**, 9, 332-344	4.9	15
109	PANNER: POS-Aware Nested Named Entity Recognition Through Heterogeneous Graph Neural Network. *IEEE Transactions on Computational Social Systems*, **2022**, 1-9	4.5	1
108	An Anonymity Vulnerability in Tor. *IEEE/ACM Transactions on Networking*, **2022**, 1-14	3.8	2
107	Preventing Price Manipulation Attack by Front-Running. *Communications in Computer and Information Science*, **2022**, 309-322	0.3	
106	Proof of Learning (PoLe): Empowering neural network training with consensus building on blockchains. *Computer Networks*, **2021**, 201, 108594	5.4	1
105	An Aerial-Computing-Assisted Architecture for Large-Scale Sensor Networks. *IEEE Wireless Communications*, **2021**, 28, 43-49	13.4	1
104	A VMD and LSTM based hybrid model of load forecasting for power grid security. *IEEE Transactions on Industrial Informatics*, **2021**, 1-1	11.9	10
103	Federated Adaptive Asynchronous Clustering Algorithm for Wireless Mesh Networks. *IEEE Transactions on Knowledge and Data Engineering*, **2021**, 1-1	4.2	4
102	Classifying encrypted traffic using adaptive fingerprints with multi-level attributes. *World Wide Web*, **2021**, 24, 2071	2.9	0
101	Multi-party transaction framework for drone services based on alliance blockchain in smart cities. *Journal of Information Security and Applications*, **2021**, 58, 102792	3.5	3
100	IoT root union: A decentralized name resolving system for IoT based on blockchain. *Information Processing and Management*, **2021**, 58, 102553	6.3	1
99	Power Grid-Oriented Cascading Failure Vulnerability Identifying Method Based on Wireless Sensors. *Journal of Sensors*, **2021**, 2021, 1-12	2	1
98	Deep-Green: A Dispersed Energy-Efficiency Computing Paradigm for Green Industrial IoT. *IEEE Transactions on Green Communications and Networking*, **2021**, 5, 750-764	4	9
97	CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques. *IEEE Internet of Things Journal*, **2021**, 8, 3242-3254	10.7	114
96	A method of chained recommendation for charging piles in internet of vehicles. *Computing (Vienna/New York)*, **2021**, 103, 231-249	2.2	1
95	. *IEEE Network*, **2021**, 35, 215-221	11.4	12

94	Secure Data Sharing Framework via Hierarchical Greedy Embedding in Darknets. *Mobile Networks and Applications*, **2021**, 26, 940-948	2.9	1
93	. *IEEE Transactions on Computational Social Systems*, **2021**, 8, 191-200	4.5	2
92	An Energy-Efficient In-Network Computing Paradigm for 6G. *IEEE Transactions on Green Communications and Networking*, **2021**, 1-1	4	12
91	IEPSBP: A Cost-efficient Image Encryption Algorithm based on Parallel Chaotic System for Green IoT. *IEEE Transactions on Green Communications and Networking*, **2021**, 1-1	4	12
90	DeepAutoD: Research on Distributed Machine Learning Oriented Scalable Mobile Communication Security Unpacking System. *IEEE Transactions on Network Science and Engineering*, **2021**, 1-1	4.9	2
89	Honeypot Identification in Softwarized Industrial Cyber-Physical Systems. *IEEE Transactions on Industrial Informatics*, **2021**, 17, 5542-5551	11.9	12
88	A Novel Web Attack Detection System for Internet of Things via Ensemble Classification. *IEEE Transactions on Industrial Informatics*, **2021**, 17, 5810-5818	11.9	28
87	Contract and Lyapunov Optimization-Based Load Scheduling and Energy Management for UAV Charging Stations. *IEEE Transactions on Green Communications and Networking*, **2021**, 5, 1381-1394	4	6
86	StFuzzer: Contribution-Aware Coverage-Guided Fuzzing for Smart Devices. *Security and Communication Networks*, **2021**, 2021, 1-15	1.9	2
85	Attribution Classification Method of APT Malware in IoT Using Machine Learning Techniques. *Security and Communication Networks*, **2021**, 2021, 1-12	1.9	8
84	Multi-Candidate Voting Model Based on Blockchain. *IEEE/CAA Journal of Automatica Sinica*, **2021**, 8, 1891-1900	7	6
83	Malicious mining code detection based on ensemble learning in cloud computing environment. *Simulation Modelling Practice and Theory*, **2021**, 113, 102391	3.9	11
82	A multiple-kernel clustering based intrusion detection scheme for 5G and IoT networks. *International Journal of Machine Learning and Cybernetics*, **2021**, 12, 3129	3.8	7
81	Detection of False Data Injection Attacks in Smart Grid Based on Machine Learning. *Communications in Computer and Information Science*, **2021**, 191-203	0.3	
80	Applying artificial bee colony algorithm to the multidepot vehicle routing problem. *Software - Practice and Experience*, **2020**,	2.5	5
79	IoT malicious traffic identification using wrapper-based feature selection mechanisms. *Computers and Security*, **2020**, 94, 101863	4.9	75
78	A survey of game theory as applied to social networks. *Tsinghua Science and Technology*, **2020**, 25, 734-742	3.4	8
77	Deep learning based emotion analysis of microblog texts. *Information Fusion*, **2020**, 64, 1-11	16.7	33

76	A Reputation Management Scheme for Efficient Malicious Vehicle Identification over 5G Networks. *IEEE Wireless Communications*, **2020**, 27, 46-52	13.4	26
75	LocJury: An IBN-Based Location Privacy Preserving Scheme for IoCV. *IEEE Transactions on Intelligent Transportation Systems*, **2020**, 1-10	6.1	10
74	Location Privacy Challenges in Mobile Edge Computing: Classification and Exploration. *IEEE Network*, **2020**, 34, 52-56	11.4	19
73	Hierarchically defining Internet of Things security: From CIA to CACA. *International Journal of Distributed Sensor Networks*, **2020**, 16, 155014771989937	1.7	4
72	A consistency-guaranteed approach for Internet of Things software refactoring. *International Journal of Distributed Sensor Networks*, **2020**, 16, 155014772090168	1.7	0
71	Research on android infiltration technology based on the silent installation of an accessibility service. *International Journal of Distributed Sensor Networks*, **2020**, 16, 155014772090362	1.7	1
70	A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment. *IEEE Access*, **2020**, 8, 67192-67204	3.5	17
69	Topic representation model based on microblogging behavior analysis. *World Wide Web*, **2020**, 23, 3083-3097	2.7	1
68	A Quantitative Method for the DNS Isolation Management Risk Estimation. *Electronics (Switzerland)*, **2020**, 9, 922	2.6	0
67	A Survey on Access Control in the Age of Internet of Things. *IEEE Internet of Things Journal*, **2020**, 7, 4682-4696	10.7	120
66	A Public Psychological Pressure Index for Social Networks. *IEEE Access*, **2020**, 8, 23457-23469	3.5	3
65	Restricted Region Based Iterative Gradient Method for Non-Targeted Attack. *IEEE Access*, **2020**, 8, 25262-25271	3.5	1
64	System Log Detection Model Based on Conformal Prediction. *Electronics (Switzerland)*, **2020**, 9, 232	2.6	5
63	Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. *Future Generation Computer Systems*, **2020**, 107, 433-442	7.5	111
62	Deep Reinforcement Learning for Partially Observable Data Poisoning Attack in Crowdsensing Systems. *IEEE Internet of Things Journal*, **2020**, 7, 6266-6278	10.7	46
61	Research on Intelligent Detection of Command Level Stack Pollution for Binary Program Analysis. *Mobile Networks and Applications*, **2020**, 1	2.9	3
60	A Low-Latency and Energy-Efficient Neighbor Discovery Algorithm for Wireless Sensor Networks. *Sensors*, **2020**, 20,	3.8	3
59	A novel routing verification approach based on blockchain for inter-domain routing in smart metropolitan area networks. *Journal of Parallel and Distributed Computing*, **2020**, 142, 77-89	4.4	1

58	Delving Deeper in Drone-Based Person Re-Id by Employing Deep Decision Forest and Attributes Fusion. *ACM Transactions on Multimedia Computing, Communications and Applications*, **2020**, 16, 1-15	3.4	3
57	Summary of Research on Information Security Protection of Smart Grid. *Lecture Notes in Computer Science*, **2020**, 365-379	0.9	
56	Resnet-Based Slide Puzzle Captcha Automatic Response System. *Communications in Computer and Information Science*, **2020**, 140-153	0.3	
55	Research on Automated Vulnerability Mining of Embedded System Firmware. *Communications in Computer and Information Science*, **2020**, 105-117	0.3	
54	Research on Intrusion Detection Technology of Industrial Control Systems. *Communications in Computer and Information Science*, **2020**, 129-139	0.3	
53	Data mining and machine learning methods for sustainable smart cities traffic classification: A survey. *Sustainable Cities and Society*, **2020**, 60, 102177	10.1	73
52	Vcash: A Novel Reputation Framework for Identifying Denial of Traffic Service in Internet of Connected Vehicles. *IEEE Internet of Things Journal*, **2020**, 7, 3901-3909	10.7	65
51	XWM: a high-speed matching algorithm for large-scale URL rules in wireless surveillance applications. *Multimedia Tools and Applications*, **2020**, 79, 16245-16263	2.5	
50	Nei-TTE: Intelligent Traffic Time Estimation Based on Fine-Grained Time Derivation of Road Segments for Smart City. *IEEE Transactions on Industrial Informatics*, **2020**, 16, 2659-2666	11.9	57
49	An Automated Refactoring Approach to Improve IoT Software Quality. *Applied Sciences (Switzerland)*, **2020**, 10, 413	2.6	1
48	Automatic Concept Extraction Based on Semantic Graphs From Big Data in Smart City. *IEEE Transactions on Computational Social Systems*, **2020**, 7, 225-233	4.5	16
47	Deep Learning and Dempster-Shafer Theory Based Insider Threat Detection. *Mobile Networks and Applications*, **2020**, 1	2.9	3
46	SoftSystem: Smart Edge Computing Device Selection Method for IoT Based on Soft Set Technique. *Wireless Communications and Mobile Computing*, **2020**, 2020, 1-10	1.9	5
45	The QoS and privacy trade-off of adversarial deep learning: An evolutionary game approach. *Computers and Security*, **2020**, 96, 101876	4.9	8
44	Improved Dota2 lineup recommendation model based on a bidirectional LSTM. *Tsinghua Science and Technology*, **2020**, 25, 712-720	3.4	30
43	. *IEEE Vehicular Technology Magazine*, **2020**, 15, 95-100	9.9	6
42	Security of Mobile Multimedia Data:The Adversarial Examples for Spatio-temporal Data. *Computer Networks*, **2020**, 181, 107432	5.4	0
41	AFLPro: Direction sensitive fuzzing. *Journal of Information Security and Applications*, **2020**, 54, 102497	3.5	0

40	Deep Learning Based Multi-Channel Intelligent Attack Detection for Data Security. *IEEE Transactions on Sustainable Computing*, **2020**, 5, 204-212	3.5	91
39	Obstructive sleep apnea detection using ecg-sensor with convolutional neural networks. *Multimedia Tools and Applications*, **2020**, 79, 15813-15827	2.5	14
38	Functional immunization of networks based on message passing. *Applied Mathematics and Computation*, **2020**, 366, 124728	2.7	18
37	A Distributed Deep Learning System for Web Attack Detection on Edge Devices. *IEEE Transactions on Industrial Informatics*, **2020**, 16, 1963-1971	11.9	117
36	Advanced persistent threat organization identification based on software gene of malware. *Transactions on Emerging Telecommunications Technologies*, **2020**, 31, e3884	1.9	3
35	Automated Vulnerability Discovery and Exploitation in the Internet of Things. *Sensors*, **2019**, 19,	3.8	4
34	Preserving Location Privacy in Mobile Edge Computing **2019**,		7
33	. *IEEE Access*, **2019**, 7, 134293-134300	3.5	6
32	A Practical Neighbor Discovery Framework for Wireless Sensor Networks. *Sensors*, **2019**, 19,	3.8	2
31	Timescale diversity facilitates the emergence of cooperation-extortion alliances in networked systems. *Neurocomputing*, **2019**, 350, 195-201	5.4	13
30	A Correlation-Change Based Feature Selection Method for IoT Equipment Anomaly Detection. *Applied Sciences (Switzerland)*, **2019**, 9, 437	2.6	22
29	Lightweight Anonymous Geometric Routing for Internet of Things. *IEEE Access*, **2019**, 7, 29754-29762	3.5	6
28	Block-DEF: A secure digital evidence framework using blockchain. *Information Sciences*, **2019**, 491, 151-165	7.7	131
27	Real-Time Lateral Movement Detection Based on Evidence Reasoning Network for Edge Computing Environment. *IEEE Transactions on Industrial Informatics*, **2019**, 15, 4285-4294	11.9	127
26	Trust architecture and reputation evaluation for internet of things. *Journal of Ambient Intelligence and Humanized Computing*, **2019**, 10, 3099-3107	3.7	44
25	Toward a Comprehensive Insight Into the Eclipse Attacks of Tor Hidden Services. *IEEE Internet of Things Journal*, **2019**, 6, 1584-1593	10.7	83
24	A Survey of Privacy-Preserving Techniques for Blockchain. *Lecture Notes in Computer Science*, **2019**, 225-234	0.4	3
23	Low-Power Distributed Data Flow Anomaly-Monitoring Technology for Industrial Internet of Things. *Sensors*, **2019**, 19,	3.8	4

22	Evaluating Reputation Management Schemes of Internet of Vehicles Based on Evolutionary Game Theory. *IEEE Transactions on Vehicular Technology*, **2019**, 68, 5971-5980	6.8	97
21	A Comparison of Machine Learning Algorithms for Detecting XSS Attacks. *Lecture Notes in Computer Science*, **2019**, 214-224	0.9	3
20	Research on Content Extraction of Rich Text Web Pages. *Lecture Notes in Computer Science*, **2019**, 279-287	0.9	1
19	Bitcoin Network Size Estimation Based on Coupon Collection Model. *Lecture Notes in Computer Science*, **2019**, 298-307	0.9	1
18	Crowdsourcing Approach for Developing Hands-On Experiments in Cybersecurity Education. *IEEE Access*, **2019**, 7, 169066-169072	3.5	2
17	Salaxy: Enabling USB Debugging Mode Automatically to Control Android Devices. *IEEE Access*, **2019**, 7, 178321-178330	3.5	2
16	A Fine-Grained Video Encryption Service Based on the Cloud-Fog-Local Architecture for Public and Private Videos. *Sensors*, **2019**, 19,	3.8	5
15	A data-driven method for future Internet route decision modeling. *Future Generation Computer Systems*, **2019**, 95, 212-220	7.5	92
14	Bidirectional self-adaptive resampling in internet of things big data learning. *Multimedia Tools and Applications*, **2019**, 78, 30111-30126	2.5	12
13	sEMG-Based Gesture Recognition with Convolution Neural Networks. *Sustainability*, **2018**, 10, 1865	3.6	43
12	Answering the Min-Cost Quality-Aware Query on Multi-Sources in Sensor-Cloud Systems. *Sensors*, **2018**, 18,	3.8	12
11	An efficient dynamic ID-based remote user authentication scheme using self-certified public keys for multi-server environments. *PLoS ONE*, **2018**, 13, e0202657	3.7	5
10	. *IEEE Access*, **2018**, 6, 74854-74864	3.5	28
9	Automatically Traceback RDP-Based Targeted Ransomware Attacks. *Wireless Communications and Mobile Computing*, **2018**, 2018, 1-13	1.9	14
8	A Privacy Preserving Scheme for Nearest Neighbor Query. *Sensors*, **2018**, 18,	3.8	21
7	A Data Leakage Prevention Method Based on the Reduction of Confidential and Context Terms for Smart Mobile Devices. *Wireless Communications and Mobile Computing*, **2018**, 2018, 1-11	1.9	16
6	A Real-Time Correlation of Host-Level Events in Cyber Range Service for Smart Campus. *IEEE Access* , **2018**, 6, 35355-35364	3.5	64
5	Succinct and practical greedy embedding for geometric routing. *Computer Communications*, **2017**, 114, 51-61	5.1	5

4	. *China Communications*, **2015**, 12, 167-176	3	6
3	Geometric Name Routing for ICN in dynamic world. *China Communications*, **2015**, 12, 47-59	3	3
2	A digital evidence fusion method in network forensics systems with Dempster-shafer theory. *China Communications*, **2014**, 11, 91-97	3	9
1	Reduction of false positives in intrusion detection via adaptive alert classifier **2008**,		1