Qiben Yan

List of Publications by Year
in descending order

63	1,666	623734	454955
papers	citations	14 h-index	30 g-index

66	66	66	1439
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	URadio: Wideband Ultrasound Communication for Smart Home Applications. IEEE Internet of Things Journal, 2022, 9, 13113-13125.	8.7	2
2	AuthIoT: A Transferable Wireless Authentication Scheme for IoT Devices without Input Interface. IEEE Internet of Things Journal, 2022, , 1-1.	8.7	1
3	Effective detection of mobile malware behavior based on explainable deep neural network. Neurocomputing, 2021, 453, 482-492.	5.9	17
4	SoundFence: Securing Ultrasonic Sensors in Vehicles Using Physical-Layer Defense. , 2021, , .		3
5	JammingBird: Jamming-Resilient Communications for Vehicular Ad Hoc Networks. , 2021, , .		5
6	Blockumulus: A Scalable Framework for Smart Contracts on the Cloud. , 2021, , .		5
7	SpecView: Malware Spectrum Visualization Framework With Singular Spectrum Transformation. IEEE Transactions on Information Forensics and Security, 2021, 16, 5093-5107.	6.9	10
8	EthClipper: A Clipboard Meddling Attack on Hardware Wallets with Address Verification Evasion. , 2021, , .		5
9	A Practical Downlink NOMA Scheme for Wireless LANs. IEEE Transactions on Communications, 2020, 68, 2236-2250.	7.8	12
10	Deep and broad URL feature mining for android malware detection. Information Sciences, 2020, 513, 600-613.	6.9	40
11	Jamsa: A Utility Optimal Contextual Online Learning Framework for Anti-Jamming Wireless Scheduling Under Reactive Jamming Attack. IEEE Transactions on Network Science and Engineering, 2020, 7, 1862-1878.	6.4	11
12	Tree decomposition based anomalous connected subgraph scanning for detecting and forecasting events in attributed social media networks. Neurocomputing, 2020, 407, 83-93.	5.9	4
13	TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Computers and Security, 2020, 95, 101867.	6.0	55
14	Multi-attributed heterogeneous graph convolutional network for bot detection. Information Sciences, 2020, 537, 380-393.	6.9	54
15	DINA: Detecting Hidden Android Inter-App Communication in Dynamic Loaded Code. IEEE Transactions on Information Forensics and Security, 2020, 15, 2782-2797.	6.9	16
16	Structured Sparsity Model Based Trajectory Tracking Using Private Location Data Release. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.	5.4	4
17	DART: Detecting Unseen Malware Variants using Adaptation Regularization Transfer Learning. , 2019, , .		9
18	Characterizing Location-based Mobile Tracking in Mobile Ad Networks. , 2019, , .		5

#	Article	IF	Citations
19	On User Selective Eavesdropping Attacks in MU-MIMO: CSI Forgery and Countermeasure. , 2019, , .		7
20	Detecting Vulnerable Android Inter-App Communication in Dynamically Loaded Code. , 2019, , .		6
21	Privacy-Preserving and Residential Context-Aware Online Learning for IoT-Enabled Energy Saving With Big Data Support in Smart Home Environment. IEEE Internet of Things Journal, 2019, 6, 7450-7468.	8.7	9
22	Tail Amplification in n-Tier Systems: A Study of Transient Cross-Resource Contention Attacks. , 2019, , .		5
23	Demystifying Application Performance Management Libraries for Android. , 2019, , .		6
24	A mobile malware detection method using behavior features in network traffic. Journal of Network and Computer Applications, 2019, 133, 15-25.	9.1	80
25	Obfusifier: Obfuscation-Resistant Android Malware Detection System. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2019, , 214-234.	0.3	9
26	Detecting Android Malware Leveraging Text Semantics of Network Flows. IEEE Transactions on Information Forensics and Security, 2018, 13, 1096-1109.	6.9	106
27	Significant Permission Identification for Machine-Learning-Based Android Malware Detection. IEEE Transactions on Industrial Informatics, 2018, 14, 3216-3225.	11.3	413
28	Machine learning based mobile malware detection using highly imbalanced network traffic. Information Sciences, 2018, 433-434, 346-364.	6.9	114
29	Deep and Broad Learning Based Detection of Android Malware via Network Traffic. , 2018, , .		16
30	Efficient Signature Generation for Classifying Cross-Architecture IoT Malware. , 2018, , .		44
31	Towards best secure coding practice for implementing SSL/TLS. , 2018, , .		2
32	Tracking location privacy leakage of mobile ad networks at scale. , 2018, , .		3
33	Uplink MU-MIMO in Asynchronous Wireless LANs. , 2018, , .		5
34	High-bandwidth ultrasonic communication using graphene-based acoustic devices. , 2018, , .		1
35	PSCluster: Differentially Private Spatial Cluster Detection for Mobile Crowdsourcing Applications. , 2018, , .		0
36	Lexical Mining of Malicious URLs for Classifying Android Malware. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2018, , 248-263.	0.3	3

#	Article	IF	Citations
37	GranDroid: Graph-Based Detection of Malicious Network Behaviors in Android Applications. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2018, , 264-280.	0.3	4
38	Very Short Intermittent DDoS Attacks inÂan Unsaturated System. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2018, , 45-66.	0.3	8
39	Identity management using blockchain for cognitive cellular networks. , 2017, , .		33
40	TextDroid: Semantics-based detection of mobile malware using network flows. , 2017, , .		13
41	Security analysis of Internet-of-Things: A case study of august smart lock. , 2017, , .		26
42	Enabling jamming-resistant communications in wireless MIMO networks. , 2017, , .		15
43	SPRIDE: Scalable and private continual geo-distance evaluation for precision agriculture. , 2017, , .		3
44	Design and analysis of elastic handoff in cognitive cellular networks. , 2017, , .		4
45	Black penguin: On the feasibility of detecting intrusion with homogeneous memory. , 2017, , .		0
46	Enabling Technologies towards 5G Mobile Networks. Mobile Information Systems, 2017, 2017, 1-2.	0.6	0
47	DroidClassifier: Efficient Adaptive Mining of Application-Layer Header for Classifying Android Malware. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2017, , 597-616.	0.3	20
48	DroidCollector: A High Performance Framework for High Quality Android Traffic Collection. , 2016, , .		8
49	SigPID: significant permission identification for android malware detection. , 2016, , .		42
50	TrafficAV: An effective and explainable detection of mobile malware behavior using network traffic. , 2016, , .		14
51	Achieving 5As in Cloud Centric Cognitive Cellular Networks. , 2016, , .		2
52	Jamming Resilient Communication Using MIMO Interference Cancellation. IEEE Transactions on Information Forensics and Security, 2016, 11, 1486-1499.	6.9	84
53	A First Look at Android Malware Traffic in First Few Minutes. , 2015, , .		19
54	A Real-time Android Malware Detection System Based on Network Traffic Analysis. Lecture Notes in Computer Science, 2015, , 504-516.	1.3	7

#	Article	IF	Citations
55	PeerClean: Unveiling peer-to-peer botnets through dynamic group behavior analysis. , 2015, , .		18
56	MIMO-based jamming resilient communication in wireless networks. , 2014, , .		42
57	SpecMonitor: Toward Efficient Passive Traffic Monitoring for Cognitive Radio Networks. IEEE Transactions on Wireless Communications, 2014, 13, 5893-5905.	9.2	7
58	Proximity-Based Security Techniques for Mobile Users in Wireless Networks. IEEE Transactions on Information Forensics and Security, 2013, 8, 2089-2100.	6.9	75
59	Proximity-based security using ambient radio signals. , 2013, , .		6
60	Non-parametric passive traffic monitoring in cognitive radio networks. , 2013, , .		11
61	Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks. , 2012, , .		32
62	On the Limitation of Embedding Cryptographic Signature for Primary Transmitter Authentication. IEEE Wireless Communications Letters, 2012, 1, 324-327.	5.0	15
63	Throughput Analysis of Cooperative Mobile Content Distribution in Vehicular Network using Symbol Level Network Coding. IEEE Journal on Selected Areas in Communications, 2012, 30, 484-492.	14.0	59