

# Qiben Yan

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/609095/publications.pdf>

Version: 2024-02-01

63  
papers

1,666  
citations

623734

14  
h-index

454955

30  
g-index

66  
all docs

66  
docs citations

66  
times ranked

1439  
citing authors

| #  | ARTICLE   | IF   | CITATIONS |
|----|---|------|-----------|
| 1  | Significant Permission Identification for Machine-Learning-Based Android Malware Detection. IEEE Transactions on Industrial Informatics, 2018, 14, 3216-3225.   | 11.3 | 413       |
| 2  | Machine learning based mobile malware detection using highly imbalanced network traffic. Information Sciences, 2018, 433-434, 346-364.  | 6.9  | 114       |
| 3  | Detecting Android Malware Leveraging Text Semantics of Network Flows. IEEE Transactions on Information Forensics and Security, 2018, 13, 1096-1109.   | 6.9  | 106       |
| 4  | Jamming Resilient Communication Using MIMO Interference Cancellation. IEEE Transactions on Information Forensics and Security, 2016, 11, 1486-1499.   | 6.9  | 84        |
| 5  | A mobile malware detection method using behavior features in network traffic. Journal of Network and Computer Applications, 2019, 133, 15-25.   | 9.1  | 80        |
| 6  | Proximity-Based Security Techniques for Mobile Users in Wireless Networks. IEEE Transactions on Information Forensics and Security, 2013, 8, 2089-2100.   | 6.9  | 75        |
| 7  | 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        |
| 8  | TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Computers and Security, 2020, 95, 101867.   | 6.0  | 55        |
| 9  | Multi-attributed heterogeneous graph convolutional network for bot detection. Information Sciences, 2020, 537, 380-393.   | 6.9  | 54        |
| 10 | Efficient Signature Generation for Classifying Cross-Architecture IoT Malware. , 2018, , .  |      | 44        |
| 11 | MIMO-based jamming resilient communication in wireless networks. , 2014, , .  |      | 42        |
| 12 | SigPID: significant permission identification for android malware detection. , 2016, , .  |      | 42        |
| 13 | Deep and broad URL feature mining for android malware detection. Information Sciences, 2020, 513, 600-613.  | 6.9  | 40        |
| 14 | Identity management using blockchain for cognitive cellular networks. , 2017, , .   |      | 33        |
| 15 | Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks. , 2012, , .  |      | 32        |
| 16 | Security analysis of Internet-of-Things: A case study of august smart lock. , 2017, , .   |      | 26        |
| 17 | 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        |
| 18 | A First Look at Android Malware Traffic in First Few Minutes. , 2015, , .   |      | 19        |

| #  | ARTICLE   | IF  | CITATIONS |
|----|---|-----|-----------|
| 19 | PeerClean: Unveiling peer-to-peer botnets through dynamic group behavior analysis. , 2015, , .  |     | 18        |
| 20 | Effective detection of mobile malware behavior based on explainable deep neural network. Neurocomputing, 2021, 453, 482-492.  | 5.9 | 17        |
| 21 | Deep and Broad Learning Based Detection of Android Malware via Network Traffic. , 2018, , .   |     | 16        |
| 22 | 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        |
| 23 | On the Limitation of Embedding Cryptographic Signature for Primary Transmitter Authentication. IEEE Wireless Communications Letters, 2012, 1, 324-327.  | 5.0 | 15        |
| 24 | Enabling jamming-resistant communications in wireless MIMO networks. , 2017, , .  |     | 15        |
| 25 | TrafficAV: An effective and explainable detection of mobile malware behavior using network traffic. , 2016, , .   |     | 14        |
| 26 | TextDroid: Semantics-based detection of mobile malware using network flows. , 2017, , .   |     | 13        |
| 27 | A Practical Downlink NOMA Scheme for Wireless LANs. IEEE Transactions on Communications, 2020, 68, 2236-2250.   | 7.8 | 12        |
| 28 | Non-parametric passive traffic monitoring in cognitive radio networks. , 2013, , .  |     | 11        |
| 29 | 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        |
| 30 | SpecView: Malware Spectrum Visualization Framework With Singular Spectrum Transformation. IEEE Transactions on Information Forensics and Security, 2021, 16, 5093-5107.                                     | 6.9 | 10        |
| 31 | DART: Detecting Unseen Malware Variants using Adaptation Regularization Transfer Learning. , 2019, , .  |     | 9         |
| 32 | 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         |
| 33 | 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         |
| 34 | DroidCollector: A High Performance Framework for High Quality Android Traffic Collection. , 2016, , .   |     | 8         |
| 35 | Very Short Intermittent DDoS Attacks in An Unsaturated System. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2018, , 45-66.                  | 0.3 | 8         |
| 36 | SpecMonitor: Toward Efficient Passive Traffic Monitoring for Cognitive Radio Networks. IEEE Transactions on Wireless Communications, 2014, 13, 5893-5905.   | 9.2 | 7         |

| #  | ARTICLE  | IF  | CITATIONS |
|----|--|-----|-----------|
| 37 | A Real-time Android Malware Detection System Based on Network Traffic Analysis. Lecture Notes in Computer Science, 2015, , 504-516.  | 1.3 | 7         |
| 38 | On User Selective Eavesdropping Attacks in MU-MIMO: CSI Forgery and Countermeasure. , 2019, , .  |     | 7         |
| 39 | Proximity-based security using ambient radio signals. , 2013, , .  |     | 6         |
| 40 | Detecting Vulnerable Android Inter-App Communication in Dynamically Loaded Code. , 2019, , .   |     | 6         |
| 41 | Demystifying Application Performance Management Libraries for Android. , 2019, , .   |     | 6         |
| 42 | Uplink MU-MIMO in Asynchronous Wireless LANs. , 2018, , .  |     | 5         |
| 43 | Characterizing Location-based Mobile Tracking in Mobile Ad Networks. , 2019, , .   |     | 5         |
| 44 | Tail Amplification in n-Tier Systems: A Study of Transient Cross-Resource Contention Attacks. , 2019, , .  |     | 5         |
| 45 | JammingBird: Jamming-Resilient Communications for Vehicular Ad Hoc Networks. , 2021, , .   |     | 5         |
| 46 | Blockumulus: A Scalable Framework for Smart Contracts on the Cloud. , 2021, , .  |     | 5         |
| 47 | EthClipper: A Clipboard Meddling Attack on Hardware Wallets with Address Verification Evasion. , 2021, , .   |     | 5         |
| 48 | Design and analysis of elastic handoff in cognitive cellular networks. , 2017, , .   |     | 4         |
| 49 | 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         |
| 50 | Structured Sparsity Model Based Trajectory Tracking Using Private Location Data Release. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.  | 5.4 | 4         |
| 51 | 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         |
| 52 | SPRIDE: Scalable and private continual geo-distance evaluation for precision agriculture. , 2017, , .  |     | 3         |
| 53 | Tracking location privacy leakage of mobile ad networks at scale. , 2018, , .  |     | 3         |
| 54 | SoundFence: Securing Ultrasonic Sensors in Vehicles Using Physical-Layer Defense. , 2021, , .  |     | 3         |

| #  | ARTICLE   | IF  | CITATIONS |
|----|---|-----|-----------|
| 55 | 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         |
| 56 | Achieving 5As in Cloud Centric Cognitive Cellular Networks. , 2016, , .   |     | 2         |
| 57 | Towards best secure coding practice for implementing SSL/TLS. , 2018, , .   |     | 2         |
| 58 | URadio: Wideband Ultrasound Communication for Smart Home Applications. IEEE Internet of Things Journal, 2022, 9, 13113-13125.   | 8.7 | 2         |
| 59 | High-bandwidth ultrasonic communication using graphene-based acoustic devices. , 2018, , .  |     | 1         |
| 60 | AuthIoT: A Transferable Wireless Authentication Scheme for IoT Devices without Input Interface. IEEE Internet of Things Journal, 2022, , 1-1.   | 8.7 | 1         |
| 61 | Black penguin: On the feasibility of detecting intrusion with homogeneous memory. , 2017, , .   |     | 0         |
| 62 | Enabling Technologies towards 5G Mobile Networks. Mobile Information Systems, 2017, 2017, 1-2.  | 0.6 | 0         |
| 63 | PSCluster: Differentially Private Spatial Cluster Detection for Mobile Crowdsourcing Applications. , 2018, , .  |     | 0         |