Tanja Zseby

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/4976941/publications.pdf

Version: 2024-02-01

45	713	759233	580821
papers	citations	12 h-index	25 g-index

47	47	47	718
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Analysis of network traffic features for anomaly detection. Machine Learning, 2015, 101, 59-84.	5.4	147
2	Botnet Communication Patterns. IEEE Communications Surveys and Tutorials, 2017, 19, 2768-2796.	39.4	99
3	Cyber attack models for smart grid environments. Sustainable Energy, Grids and Networks, 2017, 12, 10-29.	3.9	67
4	When YouTube Does not Workâ€"Analysis of QoE-Relevant Degradation in Google CDN Traffic. IEEE Transactions on Network and Service Management, 2014, 11, 441-457.	4.9	49
5	Resilience and Security: A Qualitative Survey of Urban Smart Grid Architectures. IEEE Access, 2016, 4, 839-848.	4.2	30
6	MDCGen: Multidimensional Dataset Generator for Clustering. Journal of Classification, 2019, 36, 599-618.	2.2	25
7	Absolute Cluster Validity. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2020, 42, 2096-2112.	13.9	22
8	Teaching Network Security With IP Darkspace Data. IEEE Transactions on Education, 2016, 59, 1-7.	2.4	20
9	Analysis of Lightweight Feature Vectors for Attack Detection in Network Traffic. Applied Sciences (Switzerland), 2018, 8, 2196.	2.5	20
10	Why are My Flows Different? A Tutorial on Flow Exporters. IEEE Communications Surveys and Tutorials, 2020, 22, 2064-2103.	39.4	18
11	A Network Steganography Lab on Detecting TCP/IP Covert Channels. IEEE Transactions on Education, 2016, 59, 224-232.	2.4	14
12	Cobot attack: a security assessment exemplified by a specific collaborative robot. Procedia Manufacturing, 2021, 54, 191-196.	1.9	14
13	Network-Based Secret Communication in Clouds: A Survey. IEEE Communications Surveys and Tutorials, 2017, 19, 1112-1144.	39.4	13
14	A Meta-Analysis Approach for Feature Selection in Network Traffic Research. , 2017, , .		13
15	Extreme Dimensionality Reduction for Network Attack Visualization with Autoencoders. , 2019, , .		13
16	Malware propagation in smart grid networks: metrics, simulation and comparison of three malware types. Journal of Computer Virology and Hacking Techniques, 2019, 15, 109-125.	2.2	12
17	Time-activity footprints in IP traffic. Computer Networks, 2016, 107, 64-75.	5.1	11
18	DAT detectors: uncovering TCP/IP covert channels by descriptive analytics. Security and Communication Networks, 2016, 9, 3011-3029.	1.5	11

#	Article	IF	Citations
19	Walling up Backdoors in Intrusion Detection Systems. , 2019, , .		10
20	Security Challenges for Wide Area Monitoring in Smart Grids. Elektrotechnik Und Informationstechnik, 2014, 131, 105-111.	1.1	9
21	Entropy-Based Characterization of Internet Background Radiation. Entropy, 2015, 17, 74-101.	2.2	9
22	Outlier Detection Based on Low Density Models. , 2018, , .		9
23	Impact of Asynchronous Renewable Generation Infeed on Grid Frequency: Analysis Based on Synchrophasor Measurements. Sustainability, 2018, 10, 1605.	3.2	8
24	Pattern Discovery in Internet Background Radiation. IEEE Transactions on Big Data, 2019, 5, 467-480.	6.1	7
25	Workshop report. Computer Communication Review, 2012, 42, 49-53.	1.8	6
26	Nightlights: Entropy-Based Metrics for Classifying Darkspace Traffic Patterns. Lecture Notes in Computer Science, 2014, , 275-277.	1.3	6
27	A measurement framework for inter-domain SLA validation. Computer Communications, 2006, 29, 703-716.	5.1	5
28	Is IPv6 Ready for the Smart Grid?. , 2012, , .		5
29	Modelling IP darkspace traffic by means of clustering techniques. , 2014, , .		4
30	The FUSE testbed: establishing a microgrid for smart grid security experiments. Elektrotechnik Und Informationstechnik, 2017, 134, 30-35.	1.1	4
31	Analytic Study of Features for the Detection of Covert Timing Channels in NetworkTraffic. Journal of Cyber Security and Mobility, 2017, 6, 225-270.	0.7	4
32	Malware propagation in smart grid monocultures. Elektrotechnik Und Informationstechnik, 2018, 135, 264-269.	1.1	4
33	MDCStream. , 2020, , .		4
34	Cross-Layer Profiling of Encrypted Network Data for Anomaly Detection. , 2020, , .		4
35	Fuzzy classification boundaries against adversarial network attacks. Fuzzy Sets and Systems, 2019, 368, 20-35.	2.7	3
36	NTARC: A Data Model for the Systematic Review of Network Traffic Analysis Research. Applied Sciences (Switzerland), 2020, 10, 4307.	2.5	3

#	Article	IF	Citations
37	The Day after Patch Tuesday: Effects Observable in IP Darkspace Traffic. Lecture Notes in Computer Science, 2013, , 273-275.	1.3	3
38	Are Network Attacks Outliers? A Study of Space Representations and Unsupervised Algorithms. Communications in Computer and Information Science, 2020, , 159-175.	0.5	3
39	Clustering refinement. International Journal of Data Science and Analytics, 2021, 12, 333-353.	4.1	2
40	Synchrophasor communication. Elektrotechnik Und Informationstechnik, 2014, 131, 8-13.	1.1	1
41	Interpretability and Refinement of Clustering. , 2020, , .		1
42	CCgen: Injecting Covert Channels into Network Traffic. Security and Communication Networks, 2022, 2022, 1-11.	1.5	1
43	A New Direction for Research on Data Origin Authentication in Group Communication. Lecture Notes in Computer Science, 2018, , 515-525.	1.3	0
44	Anomaly Detection for Mixed Packet Sequences. , 2020, , .		0
45	Modeling data with observers. Intelligent Data Analysis, 2022, 26, 785-803.	0.9	0