Jorge Maestre Vidal

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/4373967/publications.pdf

Version: 2024-02-01

		759055	794469
37 papers	387 citations	12 h-index	19 g-index

38 all docs	38 docs citations	38 times ranked	322 citing authors

#	Article	IF	Citations
1	Measuring the Impact of Tactical Denial of Sustainability. Lecture Notes in Computer Science, 2022, , 537-556.	1.0	0
2	Framework Proposal toÂMeasure theÂStress asÂAdversarial Factor onÂCyber Decision Making. Lecture Notes in Computer Science, 2022, , 517-536.	1.0	1
3	Introducing the CYSAS-S3 Dataset for Operationalizing a Mission-Oriented Cyber Situational Awareness. Sensors, 2022, 22, 5104.	2.1	1
4	Battling against cyberattacks: towards pre-standardization of countermeasures. Cluster Computing, 2021, 24, 57-81.	3.5	11
5	A Bio-Inspired Reaction Against Cyberattacks: AIS-Powered Optimal Countermeasures Selection. IEEE Access, 2021, 9, 60971-60996.	2.6	12
6	Understanding the Ethical and Regulatory boundaries of the Military Actuation on the Cyberspace. , 2021, , .		1
7	Adaptive Mitigation of Tactical Denial of Sustainability. , 2021, , .		1
8	The Stress as Adversarial Factor for Cyber Decision Making. , 2021, , .		2
9	Conceptualization and cases of study on cyber operations against the sustainability of the tactical edge. Future Generation Computer Systems, 2021, 125, 869-890.	4.9	5
10	EsPADA: Enhanced Payload Analyzer for malware Detection robust against Adversarial threats. Future Generation Computer Systems, 2020, 104, 159-173.	4.9	18
11	Benchmark-Based Reference Model for Evaluating Botnet Detection Tools Driven by Traffic-Flow Analytics. Sensors, 2020, 20, 4501.	2.1	24
12	Obfuscation of Malicious Behaviors for Thwarting Masquerade Detection Systems Based on Locality Features. Sensors, 2020, 20, 2084.	2.1	10
13	Denial of sustainability on military tactical clouds. , 2020, , .		5
14	Anomaly-Based Intrusion Detection. Advances in Information Security, Privacy, and Ethics Book Series, 2020, , 195-218.	0.4	3
15	Detection of economic denial of sustainability (EDoS) threats in self-organizing networks. Computer Communications, 2019, 145, 284-308.	3.1	26
16	Framework for Anticipatory Self-Protective 5G Environments. , 2019, , .		5
17	Adversarial Communication Networks Modeling for Intrusion Detection Strengthened against Mimicry. , 2019, , .		0
18	Traffic-flow analysis for source-side DDoS recognition on 5G environments. Journal of Network and Computer Applications, 2019, 136, 114-131.	5.8	30

#	ARTICLE	IF	CITATIONS
19	A novel pattern recognition system for detecting Android malware by analyzing suspicious boot sequences. Knowledge-Based Systems, 2018, 150, 198-217.	4.0	30
20	Adaptive artificial immune networks for mitigating DoS flooding attacks. Swarm and Evolutionary Computation, 2018, 38, 94-108.	4.5	69
21	Orchestration of use-case driven analytics in 5G scenarios. Journal of Ambient Intelligence and Humanized Computing, 2018, 9, 1097-1117.	3.3	6
22	Detecting Workload-based and Instantiation-based Economic Denial of Sustainability on 5G environments. , 2018, , .		4
23	Source-side DDoS Detection on IoT-enabled 5G Environments. , 2018, , .		2
24	A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation. , 2018, , .		7
25	Alert correlation framework for malware detection by anomaly-based packet payload analysis. Journal of Network and Computer Applications, 2017, 97, 11-22.	5.8	17
26	Advanced Payload Analyzer Preprocessor. Future Generation Computer Systems, 2017, 76, 474-485.	4.9	8
27	Entropy-Based Economic Denial of Sustainability Detection. Entropy, 2017, 19, 649.	1.1	15
28	Reasoning and Knowledge Acquisition Framework for 5G Network Analytics. Sensors, 2017, 17, 2405.	2.1	11
29	An Approach to Data Analysis in 5G Networks. Entropy, 2017, 19, 74.	1.1	10
30	Towards Incidence Management in 5G Based on Situational Awareness. Future Internet, 2017, 9, 3.	2.4	17
31	Online masquerade detection resistant to mimicry. Expert Systems With Applications, 2016, 61, 162-180.	4.4	18
32	Quantitative Criteria for Alert Correlation of Anomalies-based NIDS. IEEE Latin America Transactions, 2015, 13, 3461-3466.	1.2	2
33	Malware Detection System by Payload Analysis of Network Traffic. IEEE Latin America Transactions, 2015, 13, 850-855.	1.2	15
34	Network Intrusion Detection Systems in Data Centers. , 2015, , 1185-1207.		0
35	Concurrency Optimization for NIDS (Poster Abstract). Lecture Notes in Computer Science, 2012, , 395-396.	1.0	1
36	COBRA: Cibermaniobras adaptativas y personalizables de simulaciÃ³n hiperrealista de APTs y entrenamiento en ciberdefensa usando gamificaciÃ³n. ColecciÃ³n Jornadas Y Congresos, 0, , .	0.0	0

#	Article	IF	Citations
37	Marco para el AnÃ¡lisis e Inferencia de Conocimiento en Redes 5G. , 0, , .		0