Modeling the Propagation of Worms in Networks: A Sur

IEEE Communications Surveys and Tutorials
16, 942-960
DOI: 10.1109/surv.2013.100913.00195

Citation Report

#	Article	IF	Citations
1	Keynote Speech VI. , 2014, , .		0
2	Healing Wireless Sensor Networks from Malicious Epidemic Diffusion. , 2014, , .		5
3	Differential Game-Based Strategies for Preventing Malware Propagation in Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security, 2014, 9, 1962-1973.	6.9	75
4	Modeling and analyzing of botnet formation based on scale-free network. , 2015, , .		1
6	Mobility Increases the Risk of Malware Propagations in Wireless Networks. , 2015, , .		2
7	Macroscopic Malware Propagation Dynamics for Complex Networks With Churn. IEEE Communications Letters, 2015, 19, 577-580.	4.1	17
8	A Game Theoretical Method for Cost-Benefit Analysis of Malware Dissemination Prevention. Information Security Journal, 2015, 24, 164-176.	1.9	8
9	K-Center: An Approach on the Multi-Source Identification of Information Diffusion. IEEE Transactions on Information Forensics and Security, 2015, 10, 2616-2626.	6.9	57
11	Reliability Evaluation for Clustered WSNs under Malware Propagation. Sensors, 2016, 16, 855.	3.8	26
12	A stochastic model for the size of worm origin. Security and Communication Networks, 2016, 9, 1103-1118.	1.5	5
13	A time-dependent SIS-model for long-term computer worm evolution. , 2016, , .		3
14	Probability of infectious nodes in backward time. , 2016, , .		0
15	A bio-inspired method for locating the diffusion source with limited observers. , 2016, , .		1
16	On the Race of Worms and Patches: Modeling the Spread of Information in Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security, 2016, 11, 2854-2865.	6.9	52
17	MeDrone: On the use of a medical drone to heal a sensor network infected by a malicious epidemic. Ad Hoc Networks, 2016, 50, 115-127.	5.5	21
18	Detection of Superpoints Using a Vector Bloom Filter. IEEE Transactions on Information Forensics and Security, 2016, 11, 514-527.	6.9	40
19	NADTW: new approach for detecting TCP worm. Neural Computing and Applications, 2017, 28, 525-538.	5.6	4
20	Rumor restraining based on propagation prediction with limited observations in large-scale social networks. , 2017, , .		7

#	Article	IF	Citations
21	Network Moving Target Defense Technique Based on Self-Adaptive End-Point Hopping. Arabian Journal for Science and Engineering, 2017, 42, 3249-3262.	3.0	6
22	A theoretical method for assessing disruptive computer viruses. Physica A: Statistical Mechanics and Its Applications, 2017, 482, 325-336.	2.6	7
23	A non-cooperative non-zero-sum game-based dependability assessment of heterogeneous WSNs with malware diffusion. Journal of Network and Computer Applications, 2017, 91, 26-35.	9.1	37
24	Network moving target defense technique based on collaborative mutation. Computers and Security, 2017, 70, 51-71.	6.0	30
25	Behavioral Service Graphs: A formal data-driven approach for prompt investigation of enterprise and internet-wide infections. Digital Investigation, 2017, 20, S47-S55.	3.2	7
26	Epidemic Protection Over Heterogeneous Networks Using Evolutionary Poisson Games. IEEE Transactions on Information Forensics and Security, 2017, 12, 1786-1800.	6.9	38
27	The impact of patch forwarding on the prevalence of computer virus: A theoretical assessment approach. Applied Mathematical Modelling, 2017, 43, 110-125.	4.2	78
28	Identifying Propagation Sources in Networks: State-of-the-Art and Comparative Studies. IEEE Communications Surveys and Tutorials, 2017, 19, 465-481.	39.4	148
29	Modeling the Spread of Influence for Independent Cascade Diffusion Process in Social Networks. , 2017, , .		14
30	Catch Me If You Can: Detecting Compromised Users Through Partial Observation on Networks. , 2017, , .		2
31	Detecting Stealthy Botnets in a Resource-Constrained Environment using Reinforcement Learning. , 2017, , .		20
32	Using epidemic betweenness to measure the influence of users in complex networks. Journal of Network and Computer Applications, 2017, 78, 288-299.	9.1	32
33	Worm infectious probability distribution with backâ€toâ€origin model. IET Communications, 2017, 11, 2101-2109.	2.2	3
34	On the Optimal Dynamic Control Strategy of Disruptive Computer Virus. Discrete Dynamics in Nature and Society, 2017, 2017, 1-14.	0.9	17
35	A cloud-assisted malware detection and suppression framework for wireless multimedia system in IoT based on dynamic differential game. China Communications, 2018, 15, 209-223.	3.2	22
36	Detection of transmissible service failure in distributed service-based systems. Journal of Parallel and Distributed Computing, 2018, 119, 36-49.	4.1	1
37	Interplay between SIR-based disease spreading and awareness diffusion on multiplex networks. Journal of Parallel and Distributed Computing, 2018, 115, 20-28.	4.1	104
38	Inferring infection rate based on observations in complex networks. Chaos, Solitons and Fractals, 2018, 107, 170-176.	5.1	3

#	Article	IF	Citations
39	Supporting user authorization queries in RBAC systems by roleâ€“permission reassignment. Future Generation Computer Systems, 2018, 88, 707-717.	7.5	9
40	A hybrid strategy for network immunization. Chaos, Solitons and Fractals, 2018, 106, 214-219.	5.1	26
41	Hopf bifurcation analysis for an epidemic model over the Internet with two delays. Advances in Difference Equations, 2018, 2018, .	3.5	7
42	Modeling and analysis of epidemic spreading on community networks with heterogeneity. Journal of Parallel and Distributed Computing, 2018, 119, 136-145.	4.1	16
43	Malware Propagations in Wireless Ad Hoc Networks. IEEE Transactions on Dependable and Secure Computing, 2018, 15, 1016-1026.	5.4	25
44	Intersection Traffic Prediction Using Decision Tree Models. Symmetry, 2018, 10, 386.	2.2	48
45	Attacking Internet Border Routers â€“ A Graph-Based Analysis of Strategies. SSRN Electronic Journal, 2018, , .	0.4	1
46	SIRA Computer Viruses Propagation Model: Mortality and Robustness. International Journal of Applied and Computational Mathematics, 2018, 4, 1.	1.6	7
47	Malware Propagation Modelling in Peer-to-Peer Networks: A Review. , 2018, , .		4
48	Geolocating a WeChat user based on the relation between reported and actual distance. International Journal of Distributed Sensor Networks, 2018, 14, 155014771877446.	2.2	5
49	Designing Anomaly Detection System for Cloud Servers by Frequency Domain Features of System Call Identifiers and Machine Learning. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2018, , 137-149.	0.3	1
50	Evaluating model checking for cyber threats code obfuscation identification. Journal of Parallel and Distributed Computing, 2018, 119, 203-218.	4.1	23
51	State-Based Switching for Optimal Control of Computer Virus Propagation with External Device Blocking. Security and Communication Networks, 2018, 2018, 1-10.	1.5	3
52	An Efficient Anonymous Authentication Scheme for Internet of Vehicles. , 2018, , .		32
53	A two layer model of malware propagation in a search engine context. , 2018, , .		4
54	Thwarting Worm Spread in Heterogeneous Networks With Diverse Variant Placement. IEEE Communications Letters, 2018, 22, 1346-1349.	4.1	5
55	Every word is valuable: Studied influence of negative words that spread during election period in social media. Concurrency Computation Practice and Experience, 2019, 31, e4525.	2.2	1
56	Verifiable Chebyshev mapsâ€based chaotic encryption schemes with outsourcing computations in the cloud/fog scenarios. Concurrency Computation Practice and Experience, 2019, 31, e4523.	2.2	13

#	Article	IF	Citations
57	Theoretic derivations of scan detection operating on darknet traffic. Computer Communications, 2019, 147, 111-121.	5.1	9
58	On Modeling Malware Propagation in Interest-Based Overlapping Communities. , 2019, , .		3
59	A four-step method for investigating network worm propagation. , 2019, , .		3
60	On Modeling Malware Propagation in Interest-Based Overlapping Communities. IEEE Access, 2019, 7, 121374-121387.	4.2	0
61	HSIRD: A model for characterizing dynamics of malware diffusion in heterogeneous WSNs. Journal of Network and Computer Applications, 2019, 146, 102420.	9.1	29
62	A propagation model with defensive measures for PLC-PC worms in industrial networks. Applied Mathematical Modelling, 2019, 69, 696-713.	4.2	19
63	A Lightweight Assisted Vulnerability Discovery Method Using Deep Neural Networks. IEEE Access, 2019, 7, 80079-80092.	4.2	18
64	Rumor Source Detection in Networks Based on the SEIR Model. IEEE Access, 2019, 7, 45240-45258.	4.2	21
65	Countermeasures against Worm Spreading. ACM Computing Surveys, 2020, 52, 1-25.	23.0	17
66	PJC: A Multi-source Method for Identifying Information Dissemination in Networks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2019, , 268-281.	0.3	0
67	Modelling and Detection of Worm Propagation for Web Vehicular Ad Hoc Network (WVANET). Wireless Personal Communications, 2019, 109, 223-241.	2.7	3
68	An attack-defense game based reliability analysis approach for wireless sensor networks. International Journal of Distributed Sensor Networks, 2019, 15, 155014771984129.	2.2	7
69	Improving wireless sensor networks performance through epidemic model. International Journal of Electronics, 2019, 106, 862-879.	1.4	22
70	CC²: Defending Hybrid Worm on Mobile Networks with Two-Dimensional Circulation Control. Complexity, 2019, 2019, 1-19.	1.6	2
71	Preventing Malware Propagation in D2D Offloading Networks with Strategic Mobile Users. , 2019, , .		1
72	Modeling Worm Propagation and Insider Threat in Air-Gapped Network using Modified SEIQV Model. , 2019, , .		2
73	A Novel Permutational Sampling Technique for Cooperative Network Scanning. , 2019, , .		1
74	MalPro. , 2019, , .		2

#	Article	IF	Citations
76	Bayesian inference of private social network links using prior information and propagated data. Journal of Parallel and Distributed Computing, 2019, 125, 72-80.	4.1	8
77	Universal behavior of the linear threshold model on weighted networks. Journal of Parallel and Distributed Computing, 2019, 123, 223-229.	4.1	7
78	Video denoising for security and privacy in fog computing. Concurrency Computation Practice and Experience, 2019, 31, e4763.	2.2	1
79	SeShare: Secure cloud data sharing based on blockchain and public auditing. Concurrency Computation Practice and Experience, 2019, 31, e4359.	2.2	25
80	Practical privacyâ€preserving deep packet inspection outsourcing. Concurrency Computation Practice and Experience, 2019, 31, e4435.	2.2	1
81	A survey on security issues in services communication of Microservicesâ€enabled fog applications. Concurrency Computation Practice and Experience, 2019, 31, e4436.	2.2	66
82	FingerAuth: 3D magnetic finger motion pattern based implicit authentication for mobile devices. Future Generation Computer Systems, 2020, 108, 1324-1337.	7.5	9
83	Secure and efficient outsourcing differential privacy data release scheme in Cyberâ€“physical system. Future Generation Computer Systems, 2020, 108, 1314-1323.	7.5	16
84	Logarithmic encryption scheme for cyberâ€“physical systems employing Fibonacci Q-matrix. Future Generation Computer Systems, 2020, 108, 1307-1313.	7.5	28
85	A probability distribution function for investigating node infection and removal times. Transactions on Emerging Telecommunications Technologies, 2020, 31, e3753.	3.9	0
86	Statistical modeling of computer malware propagation dynamics in cyberspace. Journal of Applied Statistics, 2022, 49, 858-883.	1.3	1
87	Threat-Event Detection for Distributed Networks Based on Spatiotemporal Markov Random Field. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 1735-1752.	5.4	1
88	Modeling and analyzing malware diffusion in wireless sensor networks based on cellular automaton. International Journal of Distributed Sensor Networks, 2020, 16, 155014772097294.	2.2	16
89	Analysis of Malware-Induced Cyber Attacks in Cyber-Physical Power Systems. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 67, 3482-3486.	3.0	19
90	Locating the propagation source in complex networks with a direction-induced search based Gaussian estimator. Knowledge-Based Systems, 2020, 195, 105674.	7.1	17
91	Differential Security Game in Heterogeneous Device-to-Device Offloading Network Under Epidemic Risks. IEEE Transactions on Network Science and Engineering, 2020, 7, 1852-1861.	6.4	14
92	Improved Model for the Stability Analysis of Wireless Sensor Network Against Malware Attacks. Wireless Personal Communications, 2021, 116, 2525-2548.	2.7	34
93	Riccati equation as topology-based model of computer worms and discrete SIR model with constant infectious period. Physica A: Statistical Mechanics and Its Applications, 2021, 566, 125606.	2.6	4

#	Article	IF	Citations
94	Source Identification of Asymptomatic Spread on Networks. IEEE Access, 2021, 9, 34142-34155.	4.2	2
95	Effect of Noise on Pandemic Structure for Proliferation of Malevolent Nodes in Remote Sensor Network. Wireless Personal Communications, 2021, 119, 567-584.	2.7	2
96	A Review Article on Wireless Sensor Networks in View of E-epidemic Models. Wireless Personal Communications, 2021, 120, 95-111.	2.7	4
97	Building epidemic models for living populations and computer networks. Science Progress, 2021, 104, 003685042110178.	1.9	3
98	EASBF: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles. Journal of Information Security and Applications, 2021, 59, 102802.	2.5	30
99	Malware propagation model for cluster-based wireless sensor networks using epidemiological theory. PeerJ Computer Science, 2021, 7, e728.	4.5	3
100	Modeling social worm propagation for advanced persistent threats. Computers and Security, 2021, 108, 102321.	6.0	8
102	Evolution algebras and dynamical systems of a worm propagation model. Linear and Multilinear Algebra, 2022, 70, 4097-4116.	1.0	1
103	Evaluation of Malware Spreading in Wireless Multihop Networks with Churn. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2014, , 63-74.	0.3	1
104	A Self-adaptive Hopping Approach of Moving Target Defense to thwart Scanning Attacks. Lecture Notes in Computer Science, 2016, , 39-53.	1.3	4
105	Resilient wireless sensor networks for cyber-physical systems. , 2016, , 239-267.		5
106	Malware propagation in Wireless Sensor Networks: global models vs Individual-based models. Advances in Distributed Computing and Artificial Intelligence Journal, 2017, 6, 5-15.	1.5	8
107	The Propagation Dynamics of Multiple Internet Worms. The Journal of the Korean Institute of Information and Communication Engineering, 2015, 19, 2858-2864.	0.1	0
108	A Survey on Malware Propagation Analysis and Prevention Model. International Journal of Computer Applications, 2015, 131, 23-27.	0.2	1
109	A New Biologically-Inspired Analytical Worm Propagation Model for Mobile Unstructured Peer-to-Peer Networks. Lecture Notes in Computer Science, 2016, , 251-263.	1.3	0
110	A Vaccination Game for Mitigation Active Worms Propagation in P2P Networks. Lecture Notes in Computer Science, 2019, , 267-274.	1.3	0
111	Adaptive Cyber Defenses for Botnet Detection and Mitigation. Lecture Notes in Computer Science, 2019, , 156-205.	1.3	3
112	Which Node Properties Identify the Propagation Source in Networks?. Lecture Notes in Computer Science, 2020, , 256-270.	1.3	0

#	Article	IF	Citations
113	Socially and Biologically Inspired Computing for Self-organizing Communications Networks. Lecture Notes in Computer Science, 2020, , 461-484.	1.3	0
114	H2P: A Novel Model to Study the Propagation of Modern Hybrid Worm in Hierarchical Networks. Lecture Notes in Computer Science, 2020, , 251-269.	1.3	0
115	Modeling and Analysis of Malware Propagation for Cluster-based Wireless Sensor Networks. , 2020, , .		0
116	Revert Propagation: Who are responsible for a contagion initialization in a Diffusion Network?. , 2020, , .		1
117	Locating Multi-Sources in Social Networks With a Low Infection Rate. IEEE Transactions on Network Science and Engineering, 2022, 9, 1853-1865.	6.4	32
118	Steady-State Availability Evaluation for Heterogeneous Edge Computing-Enabled WSNs with Malware Infections. Mobile Information Systems, 2022, 2022, 1-16.	0.6	1
119	D-CEWS: DEVS-Based Cyber-Electronic Warfare M&S Framework for Enhanced Communication Effectiveness Analysis in Battlefield. Sensors, 2022, 22, 3147.	3.8	7
120	Dynamic analysis of the e-SITR model for remote wireless sensor networks with noise and Sokol-Howell functional response. Results in Physics, 2022, 38, 105643.	4.1	1
121	Capturing Dynamics of Information Diffusion in SNS: A Survey of Methodology and Techniques. ACM Computing Surveys, 2023, 55, 1-51.	23.0	5
122	Defect prediction using deep learning with Network Portrait Divergence for software evolution. Empirical Software Engineering, 2022, 27, .	3.9	1
123	Inferring spatial source of disease outbreaks using maximum entropy. Physical Review E, 2022, 106, .	2.1	2
124	A Quadratic Worm Propagation Model. Springer Proceedings in Mathematics and Statistics, 2022, , 369-376.	0.2	0
125	A Privacy-Preserving Approach to Identify COVID-19 Infection Origins via Volunteered Share of Health Data Records by Mobile Users. IEEE Sensors Journal, 2023, 23, 889-897.	4.7	0
126	Periodic orbit analysis for a delayed model of malicious signal transmission in wireless sensor networks with discontinuous control. Mathematical Methods in the Applied Sciences, 2023, 46, 5267-5285.	2.3	3
127	Global dynamics and control of malicious signal transmission in wireless sensor networks. Nonlinear Analysis: Hybrid Systems, 2023, 48, 101324.	3.5	9
128	Learning theÂPropagation ofÂWorms inÂWireless Sensor Networks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2023, , 102-115.	0.3	0
129	From the Dialectical Perspective: Modeling and Exploiting of Hybrid Worm Propagation. IEEE Transactions on Information Forensics and Security, 2023, 18, 1610-1624.	6.9	1
130	Locating the propagation source in complex networks with observers-based similarity measures and direction-induced search. Soft Computing, 2023, 27, 16059-16085.	3.6	2

#	Article	IF	Citations
131	Diffusion characteristics classification framework for identification of diffusion source in complex networks. PLoS ONE, 2023, 18, e0285563.	2.5	0
132	Defending IoT Devices against Bluetooth Worms with Bluetooth OBEX Proxy. Information (Switzerland), 2023, 14, 525.	2.9	0
133	Quantitative Analysis of Worm Transmission and Insider Risks in Air-Gapped Networking Using a Novel Machine Learning Approach. IEEE Access, 2023, 11, 111034-111052.	4.2	1
134	IoTSecSim: A framework for modelling and simulation of security in Internet of things. Computers and Security, 2024, 136, 103534.	6.0	1
135	Transient Modeling of Topology-based Worms in Networks with Link Interference. , 2023, , .		0