An SDN-Enabled Pseudo-Honeypot Strategy for Distrib Industrial Internet of Things

IEEE Transactions on Industrial Informatics

16, 648-657

DOI: 10.1109/tii.2019.2917912

Citation Report

#	Article	IF	Citations
1	A Lightweight Encryption Algorithm for Edge Networks in Software-Defined Industrial Internet of Things. , 2019, , .		11
2	Perimeter Network Security Solutions: A Survey. , 2019, , .		2
3	Anti-reconnaissance Model of Host Fingerprint Based on Virtual Node. Journal of Physics: Conference Series, 2020, 1584, 012033.	0.4	0
4	Game Theoretic Honeypot Deployment in Smart Grid. Sensors, 2020, 20, 4199.	3.8	13
5	Two-Stage Checkpoint Based Security Monitoring and Fault Recovery Architecture for Embedded Processor. Electronics (Switzerland), 2020, 9, 1165.	3.1	6
6	Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks. IEEE Access, 2020, 8, 169944-169956.	4.2	37
7	Spacechain: A Three-Dimensional Blockchain Architecture for IoT Security. IEEE Wireless Communications, 2020, 27, 38-45.	9.0	33
8	Prospect Theoretic Study of Honeypot Defense Against Advanced Persistent Threats in Power Grid. IEEE Access, 2020, 8, 64075-64085.	4.2	22
9	Fiden: Intelligent Fingerprint Learning for Attacker Identification in the Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2021, 17, 882-890.	11.3	9
10	Cyber Security and Privacy Issues in Industrial Internet of Things. Computer Systems Science and Engineering, 2021, 37, 361-380.	2.4	30
11	Potential Identity Resolution Systems for the Industrial Internet of Things: A Survey. IEEE Communications Surveys and Tutorials, 2021, 23, 391-430.	39.4	27
12	FLEAM: A Federated Learning Empowered Architecture to Mitigate DDoS in Industrial IoT. IEEE Transactions on Industrial Informatics, 2022, 18, 4059-4068.	11.3	54
13	Honeypot Detection Strategy Against Advanced Persistent Threats in Industrial Internet of Things: A Prospect Theoretic Game. IEEE Internet of Things Journal, 2021, 8, 17372-17381.	8.7	24
14	Route manipulation aware Software-Defined Networks for effective routing in SDN controlled MANET by Disney Routing Protocol. Microprocessors and Microsystems, 2021, 80, 103401.	2.8	10
15	SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT. Electronics (Switzerland), 2021, 10, 918.	3.1	55
16	Research on Optimization of Array Honeypot Defense Strategies Based on Evolutionary Game Theory. Mathematics, 2021, 9, 805.	2.2	14
17	A Bayesian Q-Learning Game for Dependable Task Offloading Against DDoS Attacks in Sensor Edge Cloud. IEEE Internet of Things Journal, 2021, 8, 7546-7561.	8.7	42
18	Real Time Remote Monitoring, Control and Reporting Dashboard System to Avoid Industrial Disasters Using Industrial IOT. Advances in Science and Technology, 0, , .	0.2	0

#	Article	IF	Citations
19	A Hybrid Deep Learning-Driven SDN Enabled Mechanism for Secure Communication in Internet of Things (IoT). Sensors, 2021, 21, 4884.	3.8	42
20	Contract-Based Incentive Mechanisms for Honeypot Defense in Advanced Metering Infrastructure. IEEE Transactions on Smart Grid, 2021, 12, 4259-4268.	9.0	5
21	Deep Learning-Based Autonomous Driving Systems: A Survey of Attacks and Defenses. IEEE Transactions on Industrial Informatics, 2021, 17, 7897-7912.	11.3	62
22	Identity Authentication with Association Behavior Sequence in Machine-to-Machine Mobile Terminals. Mobile Networks and Applications, 2022, 27, 96-108.	3.3	1
23	A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems. IEEE Communications Surveys and Tutorials, 2021, 23, 2351-2383.	39.4	87
24	Centralized and Distributed Intrusion Detection for Resource-Constrained Wireless SDN Networks. IEEE Internet of Things Journal, 2022, 9, 7746-7758.	8.7	15
25	A Time-Efficient Approach Toward DDoS Attack Detection in IoT Network Using SDN. IEEE Internet of Things Journal, 2022, 9, 3612-3630.	8.7	36
26	A Honeypot-based Attack Detection Method for Networked Inverted Pendulum System. , 2021, , .		0
27	nstrumental Equipment for Cyberattack Prevention. Information & Security an International Journal, 2020, 47, 285-299.	0.4	1
28	Deep Reinforcement Learning for Securing Software-Defined Industrial Networks With Distributed Control Plane. IEEE Transactions on Industrial Informatics, 2022, 18, 4275-4285.	11.3	6
29	A Deep One-Class Intrusion Detection Scheme in Software-Defined Industrial Networks. IEEE Transactions on Industrial Informatics, 2022, 18, 4286-4296.	11.3	5
30	Deep Learning for Securing Software-Defined Industrial Internet of Things: Attacks and Countermeasures. IEEE Internet of Things Journal, 2022, 9, 11179-11189.	8.7	6
31	An SDN-Enabled Proactive Defense Framework for DDoS Mitigation in IoT Networks. IEEE Transactions on Information Forensics and Security, 2021, 16, 5366-5380.	6.9	32
32	Countermeasure Based on Smart Contracts and AI against DoS/DDoS Attack in 5G Circumstances. IEEE Network, 2020, 34, 54-61.	6.9	14
33	DDoS Defense Method in Software-Defined Space-Air-Ground Network from Dynamic Bayesian Game Perspective. Security and Communication Networks, 2022, 2022, 1-13.	1.5	2
34	An Exploration Into Secure IoT Networks Using Deep Learning Methodologies. , 2022, , .		1
35	A Hybrid Intelligent Framework to Combat Sophisticated Threats in Secure Industries. Sensors, 2022, 22, 1582.	3.8	26
36	A multi-factor integration-based semi-supervised learning for address resolution protocol attack detection in SDIIoT. International Journal of Distributed Sensor Networks, 2021, 17, 155014772110599.	2.2	0

#	Article	IF	Citations
37	Pandora: An IOT based Intrusion Detection Honeypot with Real-time Monitoring. , 2021, , .		1
38	A Honeypot-enabled SDN-based Selector for Industrial Device Access Control. , 2021, , .		0
39	A Quantitative Risk Assessment Model for Distribution Cyber-Physical System Under Cyberattack. IEEE Transactions on Industrial Informatics, 2023, 19, 2899-2908.	11.3	9
40	Security of digitalized process systems. Methods in Chemical Process Safety, 2022, , 479-523.	1.0	6
42	Behavioral Study of Software-Defined Network Parameters Using Exploratory Data Analysis and Regression-Based Sensitivity Analysis. Mathematics, 2022, 10, 2536.	2.2	3
43	An Efficient Hybrid-DNN for DDoS Detection and Classification in Software-Defined IIoT Networks. IEEE Internet of Things Journal, 2023, 10, 8491-8504.	8.7	25
44	An AI-Driven Hybrid Framework for Intrusion Detection in IoT-Enabled E-Health. Computational Intelligence and Neuroscience, 2022, 2022, 1-11.	1.7	14
45	Cross-Plane DDoS Attack Defense Architecture Based on Flow Table Features in SDN. Security and Communication Networks, 2022, 2022, 1-16.	1.5	2
46	Review of game theory approaches for DDoS mitigation by SDN. Proceedings of the Indian National Science Academy, 0, , .	1.4	0
47	Mitigation strategies for distributed denial of service (DDoS) in SDN: A survey and taxonomy. Information Security Journal, 2023, 32, 444-468.	1.9	3
48	An Efficient Authenticated Group Key Agreement Protocol withÂDynamic Batch Verification forÂSecure Distributed Networks. Lecture Notes in Computer Science, 2022, , 305-318.	1.3	0
49	EA-POT: An Explainable AI Assisted Blockchain Framework for HoneyPot IP Predictions. Acta Cybernetica, 0, , .	0.6	0
50	Deep learning based energy efficient optimal RMC-CNN model for secured data transmission and anomaly detection in industrial IOT. Sustainable Energy Technologies and Assessments, 2023, 56, 102983.	2.7	5
51	S-Pot: A Smart Honeypot Framework with Dynamic Rule Configuration for SDN. , 2022, , .		1
52	Analysis of safety and security challenges and opportunities related to cyber-physical systems. Chemical Engineering Research and Design, 2023, 173, 384-413.	5.6	13
53	HoneyTrack: An improved honeypot. , 2023, , .		1
54	Hybrid cyber defense strategies using Honey-X: A survey. Computer Networks, 2023, 230, 109776.	5.1	4
55	Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. Engineering Applications of Artificial Intelligence, 2023, 123, 106432.	8.1	30

#	Article	IF	Citations
56	Strategic Cyber Camouflage. Advances in Information Security, 2023, , 183-201.	1.2	0
58	Software-Defined Networking approaches for intrusion response in Industrial Control Systems: A survey. International Journal of Critical Infrastructure Protection, 2023, 42, 100615.	4.6	2
59	Secure and efficient authenticated group key agreement protocol for AI-based automation systems. ISA Transactions, 2023, 141, 1-9.	5.7	2
60	Information centric wireless communication for variation detection and Mitigation Model in industrial internet of Things. Computer Communications, 2023, 211, 1-10.	5.1	0
61	DDoS attacks in Industrial IoT: A survey. Computer Networks, 2023, 236, 110015.	5.1	5
62	SDN-Based Cyber Deception Deployment forÂProactive Defense Strategy Using Honey ofÂThings andÂCyber Threat Intelligence. Lecture Notes on Data Engineering and Communications Technologies, 2023, , 269-278.	0.7	1
63	An Efficient Multiplex Network Model for Effective Honeypot Roaming Against DDoS Attacks. IEEE Transactions on Network Science and Engineering, 2024, 11, 1909-1921.	6.4	0
64	Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception. Computers and Security, 2024, 139, 103685.	6.0	1
65	A Comprehensive Analysis of Exploring SDN-Enabled Honeypots for IoT Security. , 2023, , .		0
66	Federated learning for green and sustainable 6G IIoT applications. Internet of Things (Netherlands), 2024, 25, 101061.	7.7	0
67	A HMM-Based ICS Adaptive Deception Defense Framework. , 2023, , .		0
68	AMINet: An Industrial Honeynet for AMI Systems. , 2023, , .		0
69	A Comprehensive Survey of Distributed Denial of Service Detection and Mitigation Technologies in Software-Defined Network. Electronics (Switzerland), 2024, 13, 807.	3.1	0
70	Modern Real-World Applications Using Data Analytics and Machine Learning. Studies in Big Data, 2024, , 215-235.	1.1	0