

1. Record Nr.	UNINA9910623986003321
Autore	Ge Jingguo
Titolo	AI and Machine Learning for Network and Security Management
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2022 ©2022
ISBN	1-119-83590-9 1-119-83589-5 1-119-83588-7
Descrizione fisica	1 online resource (338 pages)
Collana	IEEE Press Series on Networks and Service Management Ser.
Altri autori (Persone)	LiTong WuYulei
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Table of Contents -- Title Page -- Copyright -- Author Biographies -- Preface -- Acknowledgments -- Acronyms -- 1 Introduction -- 1.1 Introduction -- 1.2 Organization of the Book -- 1.3 Conclusion -- References -- 2 When Network and Security Management Meets AI and Machine Learning -- 2.1 Introduction -- 2.2 Architecture of Machine LearningEmpowered Network and Security Management -- 2.3 Supervised Learning -- 2.4 Semisupervised and Unsupervised Learning -- 2.5 Reinforcement Learning -- 2.6 Industry Products on Network and Security Management -- 2.7 Standards on Network and Security Management -- 2.8 Projects on Network and Security Management -- 2.9 ProofofConcepts on Network and Security Management -- 2.10 Conclusion -- References -- Notes -- 3 Learning Network Intents for Autonomous Network Management* -- 3.1 Introduction -- 3.2 Motivation -- 3.3 The Hierarchical Representation and Learning Framework for Intention Symbols Inference -- 3.4 Experiments -- 3.5 Conclusion -- References -- Notes -- 4 Virtual Network Embedding via Hierarchical Reinforcement Learning1 -- 4.1 Introduction -- 4.2 Motivation -- 4.3 Preliminaries and Notations -- 4.4 The Framework of VNEHRL -- 4.5 Case Study -- 4.6 Related Work -- 4.7 Conclusion -- References -- Note -- 5 Concept Drift Detection

for Network Traffic Classification -- 5.1 Related Concepts of Machine Learning in Data Stream Processing -- 5.2 Using an Active Approach to Solve Concept Drift in the Intrusion Detection Field -- 5.3 Concept Drift Detector Based on CVAE -- 5.4 Deployment and Experiment in Real Networks -- 5.5 Future Research Challenges and Open Issues -- 5.6 Conclusion -- References -- Note -- 6 Online Encrypted Traffic Classification Based on Lightweight Neural Networks* -- 6.1 Introduction -- 6.2 Motivation -- 6.3 Preliminaries -- 6.4 The Proposed Lightweight Model. 6.5 Case Study -- 6.6 Related Work -- 6.7 Conclusion -- References -- Notes -- 7 ContextAware Learning for Robust Anomaly Detection* -- 7.1 Introduction -- 7.2 Pronouns -- 7.3 The Proposed Method-AllRobust -- 7.4 Experiments -- 7.5 Discussion -- 7.6 Conclusion -- References -- Note -- 8 Anomaly Classification with Unknown, Imbalanced and Few Labeled Log Data -- 8.1 Introduction -- 8.2 Examples -- 8.3 Methodology -- 8.4 Experimental Results and Analysis -- 8.5 Discussion -- 8.6 Conclusion -- References -- Notes -- 9 Zero Trust Networks -- 9.1 Introduction to ZeroTrust Networks -- 9.2 Zero Trust Network Solutions -- 9.3 Machine Learning Powered Zero Trust Networks -- 9.4 Conclusion -- References -- 10 Intelligent Network Management and Operation Systems -- 10.1 Introduction -- 10.2 Traditional Operation and Maintenance Systems -- 10.3 Security Operation and Maintenance -- 10.4 AIOps -- 10.5 Machine Learning Based Network Security Monitoring and Management Systems -- 10.6 Conclusion -- References -- 11 Conclusions, and Research Challenges and Open Issues -- 11.1 Conclusions -- 11.2 Research Challenges and Open Issues -- References -- Index -- End User License Agreement.
