1

Introduction

1.1 Introduction

Networking systems have been experiencing rapid advancement in recent years, due to the fast development of 5G (Cheng et al., 2018, 2020b, Wu et al., 2021b), Internet of Things (IoT) (Wu et al., 2021c, Wu, 2021), Cloud/Edge Computing (Zhang et al., 2020, Wu, 2020), and Industry 4.0 (Wu et al., 2021a, Turner et al., 2021). On the one hand, many advanced networking techniques have been developed, such as software-defined networking (SDN) (Miao et al., 2016, Wang et al., 2018, Yang et al., 2020), network functions virtualization (NFV) (Miao et al., 2019, Cheng et al., 2020b), and network slicing (Wang et al., 2019, 2020) to facilitate network and service deployment and management. On the other hand, cybersecurity is a major concern for networking systems due to the increase in system exposure to the Internet (Wu et al., 2021a, Garg et al., 2020, Culot et al., 2019). Many security mechanisms, e.g. intrusion detection, traffic classification, and anomaly detection, have been developed to facilitate the security management of networking systems (Huang et al., 2017, 2018, Zuo et al., 2020, Sun et al., 2020).

Telecommunication networks such as 5G have received significant attention in the past few years because of their capabilities of accommodating diverse vertical industry applications (Wang et al., 2019, 2020). Along with the diversified services as well as their changing and/or stringent service requirements, 5G networks have become a complex system that requires advanced artificial intelligence (AI) and machine-learning (ML) techniques to manage and maintain high-standard services to users (Yan et al., 2020). From the perspective of network operators, it is important to maximize the resource utilization of 5G infrastructure, while minimizing the violation of service-level agreement (SLA) (Wang et al., 2019). The research of next-generation telecommunication networks, the so-called 6G (Wu et al., 2021d), has been initiated by many countries, such as United Kingdom, USA, China, Finland, just to name a few. "AI Everywhere" is an important component for 6G to ensure an automatic, healthy, and secure networking system.

AI and Machine Learning for Network and Security Management, First Edition.
Yulei Wu, Jingguo Ge, and Tong Li.

The fast advancement of IoT and Industrial Internet of Things (IIoT) is transforming many traditional industries (many of them are critical infrastructures), such as energy, healthcare, factory, and transportation, toward the goal of Industry 4.0 (Wu et al., 2021a). Such a complex networking system, connecting tens of billions of devices to the Internet, is collecting a huge amount of data every day. AI and ML techniques can leverage the knowledge learned from the data to automate many tasks for these industries (Lin et al., 2021), resulting in the so-called "smart energy, smart factory, smart transportation," to name a few. Such an automation remarkably increases the efficiency of system operation of industries. However, since traditional form of these industries is much more isolated, the exposure of these industries to the Internet as a result of the transformation, calls for significant security management to ensure the safety of these critical infrastructures (Culot et al., 2019, Wu et al., 2021a).

In order to properly apply AI and ML technologies into the field of network and security management, many real-world conditions and challenges need to be considered. For example, network intent is a key piece of information to enable autonomous network management (Lin et al., 2021). How to gain accurate network intent from network big data and how to ensure that the learned network intent can be readily used across different network environments is nontrivial. Reinforcement learning (RL) is a useful tool for autonomous network management (Yan et al., 2020). Successfully applying RL in various network management tasks is challenging. In many real-world conditions, such as IoT/IIoT, lightweight learning models are required (Cheng et al., 2020a). How to devise such models while maintaining the model performance is still worth to investigate for the field of network and security management. In addition, learning from encrypted data, e.g. encrypted traffic, is crucial, due to the increase in the volume of such traffic enforced by data regulations like the general data protection regulation (GDPR) (Liu et al., 2020). Further, because of the changing condition of real-world networking systems, network data are not ideal in many cases. They are usually evolving, changing, and imbalanced, and new data that have not been seen before may present from time to time. Besides, network data are usually hard to label, resulting in few-shot issues. How to effectively learn useful information from such "noisy" data is of paramount importance to ensure the success of AI-enabled network and security management (Sun et al., 2020).

In this book, we provide our insights and potential solutions to the above issues and challenges and consider various applications to network and security management including autonomous networks, resource allocation, traffic processing, traffic classification, anomaly detection, anomaly classification, and zero trust networks (ZTNs). In Section 1.2, we will explain the rationale under which the chapters in this book are organized.

1.2 Organization of the Book

There are two strands in this book. The first strand is in Chapter 2, where we provide a comprehensive review of potential AI and ML techniques for network and security management, the existing industry products, standards, projects, and proof-of-concepts. The second strand is across Chapters 3–9, where we elaborate the application of AI and ML techniques in various network and security management tasks. In Chapter 10, we elaborate an intelligent network management and operation system and discuss the deployment of the proposed solutions in this book. In Chapter 11, we conclude this book and provide potential research challenges and open issues that will be useful for future research in this area. Figure 1.1 shows the chapter organization of this book. In what follows, we briefly introduce each chapter to facilitate readers understand the content of this book.

Chapter 2. This chapter discusses the status and limitations of current network and security management and proposes an architecture for ML-empowered network and security management. Well-known AI and ML techniques that are useful for network and security management are reviewed and discussed. We also investigate existing industry products, standards, and proof-of-concepts for network and security management.

Chapter 3. The realization of network autonomy requires network knowledge to manage the network. The abstract intent of network management tasks

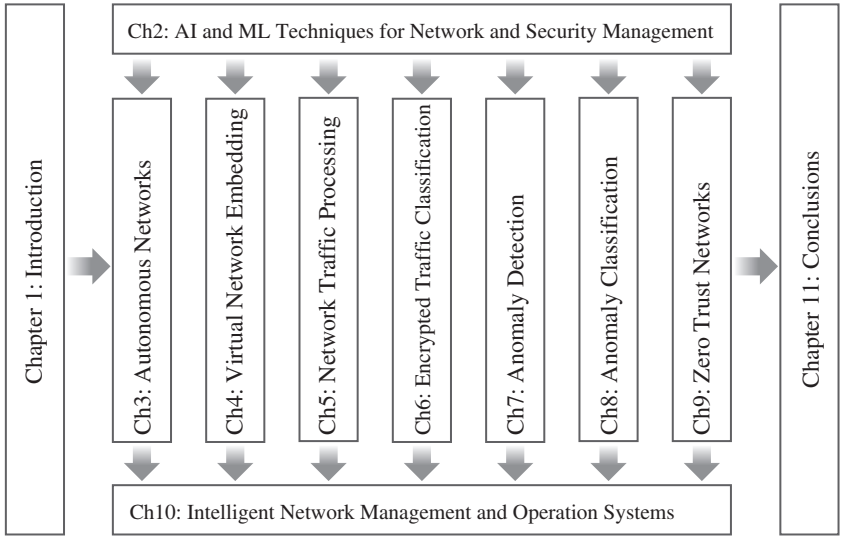

Figure 1.1 The chapter organization of this book.

can be considered as part of network knowledge. In this chapter, we treat abstract intents of network management tasks as a composite structure of symbols. Each symbol expresses the intention of the network management task in a certain aspect. The combinations of symbols, representing a network management task, should be able to be transferred and implemented across different networks. In this regard, we design a reference mechanism for learning intention symbols and their structures from network data. Taking path selection as an example, we describe in detail how to implement this mechanism to obtain the intent structure of the path selection task. It has been proved by experiments that the knowledge learnt by the proposed solution can be transferred and effectively leveraged in different network environments.

Chapter 4. Due to the outstanding performance of automatic exploration and quick development, RL methods have been applied to the virtual network embedding (VNE) problem. In this chapter, we find that a proactive VNE algorithm can benefit from hierarchical reinforcement learning (HRL). In this algorithm, a two-level agent is responsible for executing the VNE task, considering both the long-term impact and short-term impact. At the high level, the agent selects a feasible request from a batch, which aims to maximize the long-term revenue. At the low level, the agent manages to embed the selected request with the minimum cost.

Chapter 5. Although network traffic classification algorithms based on machine learning can alleviate the limitations imposed by traditional techniques, most of them are carried out by learning an underlying concept (i.e. data distribution) from a static dataset. Due to the exponential increase in the available network data, considerable attention has been received on processing network data as a stream. In this scenario, due to unforeseen circumstances in the network, the phenomenon of concept drift will degrade the performance of the classifier. In this chapter, after measuring the impact of concept drift on network traffic classifiers, we present a concept drift detector based on conditional variational autoencoders (CVAEs) under the semisupervised learning. In addition, we deploy the detector in a real-world environment, and experimental results show that this algorithm plays a great role in stabilizing the performance of a classifier.

Chapter 6. The surge in the volume of encrypted traffic and the nontransparency of encrypted traffic leads to high computational overheads in efficient network management. In this chapter, we introduce a lightweight and online approach for traffic classification, which adopts the multihead attention mechanism and the convolutional networks. Due to the one-step interaction of all packets and the parallel computing, the multihead attention mechanism can significantly reduce the number of model parameters and the running time. In addition,

the effectiveness and efficiency of convolutional networks are proved in traffic classification.

Chapter 7. As the scale of networking systems expands, a fast-growing number of logs are produced. This chapter proposes a robust context-aware method for log anomaly detection. It combines word embedding with region embedding to conduct log vectorization. Such rich semantic information enables the proposed method to deal with unseen log data and understand imbalanced log data better and deeper. The proposed method combines semisupervised learning to make full use of labeled data and unlabeled data.

Chapter 8. ML-based log anomaly classification methods have been widely studied to ensure the stability and reliability of large-scale systems. This chapter briefly introduces the feature extraction in log analysis and the few-shot problem by examples. Then, we propose OpenLog, an anomaly classification method based on meta-learning. OpenLog uses a two-layer semantic encoder to simplify the complex feature engineering. It adopts the meta-learning strategy to train the models using sufficient auxiliary datasets to enhance its performance. OpenLog transforms the multiclassification task into a binary-classification task, and it can classify unseen anomalies without retraining.

Chapter 9. In recent years, many advanced persistent attacks (APTs) have occurred on corporate internal networks. Traditional perimeter-based security defense techniques such as firewalls, which assume that users and devices inside a network are safe and trustworthy, can no longer provide sufficient security protection. The concept of ZTN was therefore proposed. In ZTN, every request, whether it comes from an internal network or an external network, must be authenticated and authorized before accessing resources. In this chapter, we provide a brief introduction of ZTN, including its concept, its architecture, and its current implementation schemes such as access proxy-based, software-defined perimeter (SDP)-based, microsegmentation-based solutions, to name a few. Since ZTN needs to authenticate and authorize requests, it is necessary to consider as many devices, users, and environmental information as possible to make decisions. As there are a large number of services, traffic, and equipment logs in the corporate intranet, ML-based information fusion and decision-making methods may improve authentication and authorization performance. Therefore, in this chapter, we evaluate the possibility of using ML in ZTN.

Chapter 10. Although various intelligent operation and management technologies based on deep learning are being developed, how to efficiently apply them to real-world products is one of the core challenges faced by deep learning. In this chapter, we introduce various open source tools, frameworks, and characteristics in the field of operations management and security. Furthermore,

we analyze existing security operations and management systems based on deep learning. Finally, we propose a security framework for intelligent operation and management based on network big data and describe the core functions and interfaces in the framework.

Chapter 11. This chapter provides a brief summary of this book, followed by a list of important research challenges and open issues that can be used for further research on AI and ML for network and security management.

1.3 Conclusion

This chapter provided a brief introduction of this book, emphasizing the motivation of writing this book and the chapter organization of the book. In addition, a brief review of each chapter is also provided, facilitating readers understand the content of this book.

References

Xiangle Cheng, Yulei Wu, Geyong Min, and Albert Y. Zomaya. Network function virtualization in dynamic networks: A stochastic perspective. *IEEE Journal on Selected Areas in Communications*, 36(10):2218–2232, 2018. doi: 10.1109/JSAC.2018.2869958.

Jin Cheng, Runkang He, E Yuepeng, Yulei Wu, Junling You, and Tong Li. Real-time encrypted traffic classification via lightweight neural networks. In *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pages 1–6, 2020a. doi: 10.1109/GLOBECOM42002.2020.9322309.

Xiangle Cheng, Yulei Wu, Geyong Min, Albert Y. Zomaya, and Xuming Fang. Safeguard network slicing in 5G: A learning augmented optimization approach. *IEEE Journal on Selected Areas in Communications*, 38(7):1600–1613, 2020b. doi: 10.1109/JSAC.2020.2999696.

Giovanna Culot, Fabio Fattori, Matteo Podrecca, and Marco Sartor. Addressing industry 4.0 cybersecurity challenges. *IEEE Engineering Management Review*, 47(3):79–86, 2019. doi: 10.1109/EMR.2019.2927559.

Sahil Garg, Kuljeet Kaur, Georges Kaddoum, and Kim-Kwang Raymond Choo. Toward secure and provable authentication for internet of things: Realizing industry 4.0. *IEEE Internet of Things Journal*, 7(5):4598–4606, 2020. doi: 10.1109/JIOT.2019.2942271.

Chengqiang Huang, Geyong Min, Yulei Wu, Yiming Ying, Ke Pei, and Zuochang Xiang. Time series anomaly detection for trustworthy services in cloud computing systems. *IEEE Transactions on Big Data*, 1, 2017. doi: 10.1109/TBDATA.2017.2711039.

Chengqiang Huang, Yulei Wu, Yuan Zuo, Ke Pei, and Geyong Min. Towards experienced anomaly detector through reinforcement learning. *Proceedings of the AAAI Conference on Artificial Intelligence*, 32(1), 2018. URL https://ojs.aaai.org/index.php/AAAI/article/view/12130.

Guozhi Lin, Jingguo Ge, Yulei Wu, Hui Li, Tong Li, Wei Mi, and E Yuepeng. Network automation for path selection: A new knowledge transfer approach. In *2021 IFIP Networking Conference*, 2021.

Xun Liu, Junling You, Yulei Wu, Tong Li, Liangxiong Li, Zheyuan Zhang, and Jingguo Ge. Attention-based bidirectional GRU networks for efficient https traffic classification. *Information Sciences*, 541:297–315, 2020. ISSN 0020-0255. doi: 10.1016/j.ins.2020.05.035. URL https://www.sciencedirect.com/science/article/pii/S002002552030445X.

Wang Miao, Geyong Min, Yulei Wu, Haozhe Wang, and Jia Hu. Performance modelling and analysis of software-defined networking under bursty multimedia traffic. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 12(5s):2016. ISSN 1551-6857. doi: 10.1145/2983637. URL https://doi.org/10.1145/2983637.

Wang Miao, Geyong Min, Yulei Wu, Haojun Huang, Zhiwei Zhao, Haozhe Wang, and Chunbo Luo. Stochastic performance analysis of network function virtualization in future internet. *IEEE Journal on Selected Areas in Communications*, 37(3):613–626, 2019. doi: 10.1109/JSAC.2019.2894304.

Peijie Sun, E Yuepeng, Tong Li, Yulei Wu, Jingguo Ge, Junling You, and Bingzhen Wu. Context-aware learning for anomaly detection with imbalanced log data. In *2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pages 449–456, 2020. doi: 10.1109/HPCC-SmartCity-DSS50907.2020.00055.

Christopher J. Turner, John Oyekan, Lampros Stergioulas, and David Griffin. Utilizing industry 4.0 on the construction site: Challenges and opportunities. *IEEE Transactions on Industrial Informatics*, 17(2):746–756, 2021. doi: 10.1109/TII.2020.3002197.

Guodong Wang, Yanxiao Zhao, Jun Huang, and Yulei Wu. An effective approach to controller placement in software defined wide area networks. *IEEE Transactions on Network and Service Management*, 15(1):344–355, 2018. doi: 10.1109/TNSM.2017.2785660.

Haozhe Wang, Yulei Wu, Geyong Min, Jie Xu, and Pengcheng Tang. Data-driven dynamic resource scheduling for network slicing: A deep reinforcement learning approach. *Information Sciences*, 498:106–116, 2019. ISSN 0020-0255. doi: 10.1016/j.ins.2019.05.012. https://www.sciencedirect.com/science/article/pii/S0020025519303986.

Haozhe Wang, Yulei Wu, Geyong Min, and Wang Miao. A graph neural network-based digital twin for network slicing management. *IEEE Transactions on Industrial Informatics*, 1, 2020. doi: 10.1109/TII.2020.3047843.

Yulei Wu. Cloud-edge orchestration for the internet-of-things: Architecture and AI-powered data processing. *IEEE Internet of Things Journal*, 1, 2020. doi: 10.1109/JIOT.2020.3014845.

Yulei Wu. Robust learning-enabled intelligence for the internet of things: A survey from the perspectives of noisy data and adversarial examples. *IEEE Internet of Things Journal*, 8(12):9568–9579, 2021. doi: 10.1109/JIOT.2020.3018691.

Yulei Wu, Hong-Ning Dai, and Hao Wang. Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. *IEEE Internet of Things Journal*, 8(4):2300–2317, 2021a. doi: 10.1109/JIOT.2020.3025916.

Yulei Wu, Hong-Ning Dai, Hao Wang, and Kim-Kwang Raymond Choo. Blockchain-based privacy preservation for 5G-enabled drone communications. *IEEE Network*, 35(1):50–56, 2021b. doi: 10.1109/MNET.011.2000166.

Yulei Wu, Zehua Wang, Yuxiang Ma, and Victor C.M. Leung. Deep reinforcement learning for blockchain in industrial IoT: A survey. *Computer Networks*, 191:108004, 2021c. ISSN 1389-1286. doi: 10.1016/j.comnet.2021.108004. URL https://www.sciencedirect.com/science/article/pii/S1389128621001213.

Y. Wu, S. Singh, T. Taleb, A. Roy, H.S. Dhillon, M.R. Kanagarathinam, and A. De. *6G Mobile Wireless Networks*. Springer, 2021d).

Zhongxia Yan, Jingguo Ge, Yulei Wu, Liangxiong Li, and Tong Li. Automatic virtual network embedding: A deep reinforcement learning approach with graph convolutional networks. *IEEE Journal on Selected Areas in Communications*, 38(6):1040–1057, 2020. doi: 10.1109/JSAC.2020.2986662.

Shu Yang, Laizhong Cui, Xinhao Deng, Qi Li, Yulei Wu, Mingwei Xu, Dan Wang, and Jianping Wu. FISE: A forwarding table structure for enterprise networks. *IEEE Transactions on Network and Service Management*, 17(2):1181–1196, 2020. doi: 10.1109/TNSM.2019.2951426.

Juan Zhang, Yulei Wu, Geyong Min, Fei Hao, and Laizhong Cui. Balancing energy consumption and reputation gain of UAV scheduling in edge computing. *IEEE Transactions on Cognitive Communications and Networking*, 6(4):1204–1217, 2020. doi: 10.1109/TCCN.2020.3004592.

Yuan Zuo, Yulei Wu, Geyong Min, Chengqiang Huang, and Ke Pei. An intelligent anomaly detection scheme for micro-services architectures with temporal and spatial data analysis. *IEEE Transactions on Cognitive Communications and Networking*, 6(2):548–561, 2020. doi: 10.1109/TCCN.2020.2966615.