Scanning the Issue

Point of View:
Choose Your Weapon: Survival Strategies for Depressed AI Academics
by J. Togelius and G. N. Yannakakis

A growing number of artificial intelligence (AI) academics can no longer find the means and resources to compete on a global scale. This is a somewhat recent phenomenon, but an accelerating one, with private actors investing enormous compute resources into cutting-edge AI research. In this month's feature article [A1], the authors discuss what AI researchers in academia can do to stay competitive given the structural and financial limitations of academic research. They propose several strategies for how to take advantage of the strengths of working in academia with small groups and constrained resources, including rapid pivoting, not having to ship software, and the ability to work on unusual or unpopular topics. The article also briefly discusses what universities, and the private sector could do to improve the situation if they are so inclined. While the list of proposed strategies is certainly not exhaustive, the authors hope to inspire further discussion about this important topic within the community.

This month's regular papers survey the topic of cloud-native computing and physical layer covert communications.

Cloud-Native Computing: A Survey From the Perspective of Services
by S. Deng, H. Zhao, B. Huang, C. Zhang, F. Chen, Y. Deng, J. Yin, S. Dustdar, and A. Y. Zomaya

Services are self-describing and technology-neutral computation entities that support rapid and low-cost composition of web applications in distributed network systems. Service-oriented architecture (SOA) is the principle to design the software systems by provisioning independent, reusable, and automated functions as reusable services and providing a robust and secure foundation for leveraging these services. In recent years, the most influential variant of SOA is the microservices architecture, which decouples a monolithic application into a collection of loosely coupled, fine-grained microservices, communicating through lightweight protocols. Over the last decade, the microservices architecture is more and more appealing, as it allows software organizations to be more productive to build systems with the support of DevOps through continuous integration and continuous delivery (CI/CD) pipelines.

Accompanied with the development of microservices, a new terminology, cloud-native, or cloud-native computing, is attracting increasing attention in academia. In accordance with the Cloud Native Computing Foundation (CNCF), the open-source vendor-neutral hub of cloud-native computing, cloud-native is the collection of technologies that break down applications into microservices and package them in lightweight containers to be deployed and orchestrated across a variety of servers. In addition to the microservices architecture, cloud-native is also characterized by terminologies such as containerization and orchestration. Containerization is a function isolation mechanism that leverages the Linux kernel to isolate resources, creating containers as different processes in the Host OS. Orchestration is the automated configuration, management, and coordination of the inter-related microservices to build the elastic and scalable functionalities.

In conclusion, a cloud-native application can be viewed as a distributed, elastic, and horizontal scalable system composed of inter-related microservices, which isolate states in a minimum of stateful components. Cloud-native can be regarded as cloud computing version 2.0. Specifically, cloud computing provides the infrastructure and backend services over the internet, while being cloud-native involves an application architecture and development approach that maximizes the benefits of cloud computing. Being cloud-native adopts practices including microservices, containerization, and orchestration to enable agility, scalability, and rapid development and deployment of applications.

Considering that cloud-native is better known in the industry, this article [A2] surveys the past and present of cloud-native applications with respect to the key problems during their lifecycle from a research perspective. It attempts to merge the industrial popularity,

Digital Object Identifier 10.1109/JPROC.2024.3367208

including the widely used open-source software and platforms, with trending research, either theoretical or systematic, from the perspective of services computing. Specifically, the article elaborates on the research domains by decoupling the lifecycle of cloud-native applications into four states: building, orchestration, operation, and maintenance. The fundamental necessities and key performance metrics that play critical roles during the development and management of cloud-native applications are discussed and summarized. The article highlights the key implications and limitations of existing works in each state and ends by discussing the challenges, future directions, and research opportunities in this area.

Physical Layer Covert Communication in B5G Wireless Networks—Its Research, Applications, and Challenges
by Y. Jiang, L. Wang, H.-H. Chen, and X. Shen

While 5G wireless communication networks are being implemented globally, it is anticipated that these networks will not be sufficient by 2030 and beyond. With new paradigm shifts such as integrated space–air–ground communication networks, full-spectrum exploration, extremely heterogeneous networks, and network security, beyond 5G (B5G) or the sixth generation (6G) will spearhead a comprehensive wave of digital revolution both economically and in society. To meet the need for ubiquitous and massive wireless connectivity, a large-scale heterogeneous network architecture that incorporates satellites, unmanned aerial vehicles, and other devices will have to be established. A broader spectrum range, encompassing sub-6 GHz, millimeter wave (mmWave), and terahertz (THz), will be explored in order to offer an ultrahigh data rate. Furthermore, B5G will stimulate creative smart applications powered by machine learning (ML) and AI.

At the same time, B5G will need robust or endogenous network security for both the physical and network layers in order to establish trust in a variety of services, like entertainment, telemedicine, and autonomous driving. While conventional cryptography can be employed to increase wireless communications security, adversaries with ever-increasing computing power remain a threat to its integrity. To counter this, traditional upper-layer security cryptography systems (such as application layer cryptography) can be supplemented by physical layer security. While traditional security techniques concentrate on safeguarding the information content that is delivered, they leave the transmission's existence vulnerable to detection by adversaries. This is where physical layer covert communication can make an impact, since its primary goal is to prevent eavesdroppers from hearing/deciphering the information that is received, with the help of natural characteristics of wireless channels, such as noise and interference. There are many instances where users try to communicate without being detected by others. For instance, in a dynamic spectrum access network, a secondary user attempting to communicate might want to do so without being detected by the primary user. Sending information in a way that makes it invisible to its enemies might therefore be the better course of action. Physical layer covert communications can make it possible for a transmitter to securely and covertly communicate with a recipient without being detected by adversaries.

Several recent studies have examined the application of physical layer covert communication in B5G networks given its promise to fulfill the ever-increasing requirement for robust security in B5G or 6G wireless. This article [A3] provides an extensive overview of the basic theories and several strategies in physical layer covert communications. In particular, it goes into great detail about the basic theories of physical layer covert communications, such as channel models, codes, secret keys, and covertness metrics, as well as various covert schemes in progressively more complicated scenarios, such as covert communications in single-antenna and multiantenna three-node systems and covert communications in jammer- and relay-aided systems. In addition, the article identifies the challenges and future directions for research on covert communications in B5G wireless networks. ■

APPENDIX: RELATED ARTICLES

[A1] J. Togelius and G. N. Yannakakis, "Choose your weapon: Survival strategies for depressed AI academics," *Proc. IEEE*, vol. 112, no. 1, pp. 4–11, Jan. 2024.

[A2] S. Deng et al., "Cloud-native computing: A survey from the perspective of services," *Proc. IEEE*, vol. 112, no. 1, pp. 12–46, Jan. 2024.

[A3] Y. Jiang, L. Wang, H.-H. Chen, and X. Shen, "Physical layer covert communication in B5G wireless networks—Its research, applications, and challenges," *Proc. IEEE*, vol. 112, no. 1, pp. 47–82, Jan. 2024.