5G: Agent for Further Digital Disruptive Transformations

Beng Chin Ooi, Gang Chen, Dumitrel Loghin, Wei Wang, Meihui Zhang
National University of Singapore, Zhejiang University, Beijing Institute of Technology

1 Introduction

The fifth-generation (5G) mobile communication technologies are on the way to be adopted as the next standard for mobile networking. It is therefore timely to analyze the impact of 5G on the landscape of computing, in particular, data management and data-driven technologies. With a predicted increase of 10-100× in bandwidth and 5-10× decrease in latency, 5G is expected to be the main enabler for edge computing which includes accessing cloud-like services, as well as conducting machine learning at the edge. In this paper, we examine the impact of 5G on both traditional and emerging technologies, and discuss research challenges and opportunities.

5G specifications are handled by the 3rd Generation Partnership Project (3GPP), while the actual implementation is done by big networking hardware players, such as Nokia, Ericsson, Huawei, Qualcomm, among others. Compared to the current 4G technologies which are widely-spread all over the world, 5G is supposed to have a higher bandwidth of up to 10 Gbps, lower latency of 1 ms and a higher device density of up to one million devices per square kilometer [1, 2]. 5G operates in a high-frequency band between 28 GHz and 95 GHz, also known as the millimeter wave spectrum (mmWave) [1, 2]. While this spectrum allows for larger bandwidths, 5G also employs massive multiple-input and multiple-output (MIMO) [1] technology to further increase the bandwidth. MIMO uses large antenna arrays in both the base station and the device to allow for parallel data streams and to direct the radio wave such that it avoids interference and achieves superior spectral efficiency [1]. Consequently, 5G is supposed to be more energy-efficient compared to current wireless technologies.

5G does not bring only improved communication speeds, but also a series of technologies that have the potential to change the computing landscape in a disruptive way. Among these technologies, we distinguish Software Defined Networking (SDN), Network Function Virtualization (NFV), Network Slicing (NS), and Device-to-Device communications (D2D) [3]. SDN represents methods to separate the data plane, which is responsible for handling and forwarding networking packets, and the control plane, which is responsible for establishing the route of the packets. NFV represents the usage of commodity hardware running virtualized services to replace custom networking hardware. For example, a commodity server could run firewall services instead of using a specialized physical firewall. Network Slicing enables several logical networks to share a single physical network infrastructure. D2D communication is a feature of 5G that allows devices to communicate directly, with minimum help from a central authority. For example, the base station may help only with device pairing and authentication, while subsequent steps, including data transfers, are performed without its involvement. In this paper, we group SDN, NFV, and NS into 5G virtualization, while D2D is a distinct feature.

2 Digital Disruptive Transformations

Among different domains that are going to be significantly impacted by the adoption of 5G [1], we discuss three key areas related to data management and data-driven technologies, as highlighted in Figure 1.

2.1 Distributed and Federated Data Processing

With the increasing number of data breaches and awareness of the General Data Protection Regulation (GDPR) and value of data, the demand for having full control of the data by the user is on the rise. For example, the healthcare records of a patient may be stored in the individual's mobile device instead of being fragmented and stored only in hospital databases. 5G has the potential to bring to reality the concept of millions of micro-databases with each being kept in an individual edge device, in the form of distributed and federated micro-databases, as shown in Figure 1. GDPR and federated data processing in dynamic networks due to node churning and joining

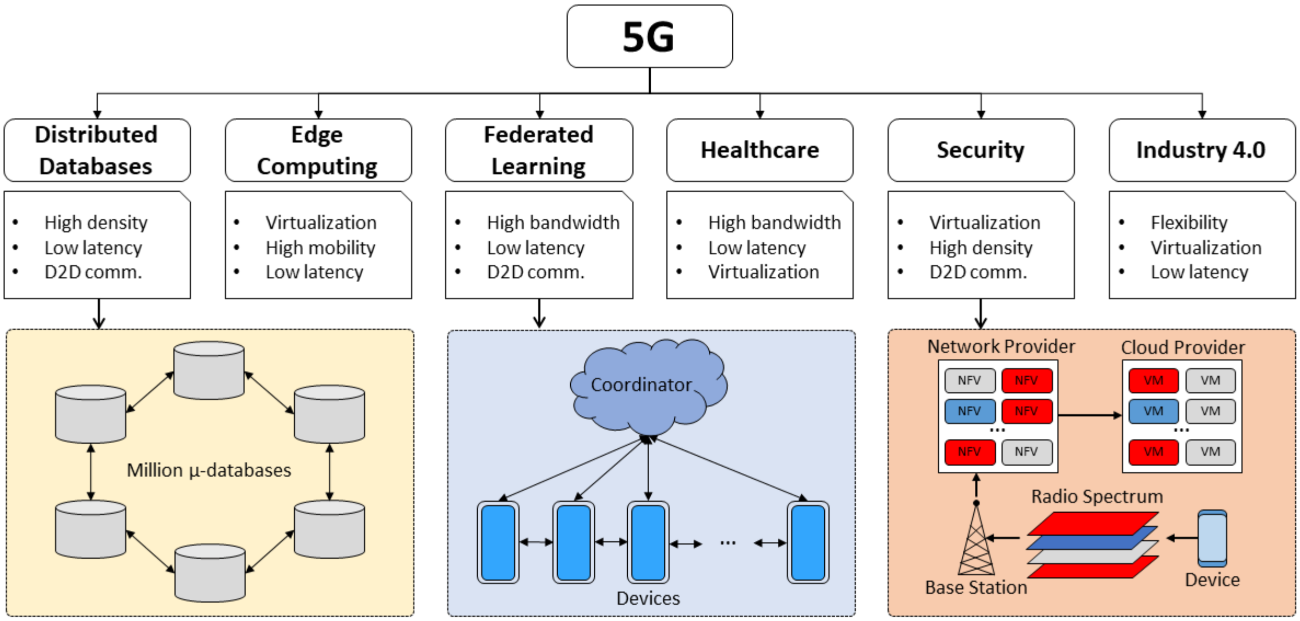

Figure 1: The impact of 5G on different domains. Some 5G features have higher impact on each domain.

introduce many new challenges such as accuracy, completeness, fairness, and representativeness, in addition to performance issues.

The key characteristics of 5G that could help with the implementation of federated micro-databases are high device density, low latency, energy efficiency, and D2D communications. For instance, a 5G deployment is expected to be able to support one million devices in a square kilometer [2]. With a few millions of interconnected devices, a smart city becomes the playground of federated micro-databases. Low latency and D2D communication allow nodes to communicate fast and directly, in a setup that may prove to be superior even to datacenters with Gigabit Ethernet links. Compared to these datacenters, a distributed 5G setup has a few advantages, such as improved networking, higher energy efficiency, and mobility.

First, D2D communication without direct base station involvement is reducing the risk of network partitioning due to faulty centralized infrastructure. In comparison, a datacenter that depends on a few switches and routers is more prone to partitioning. Second, 5G terminals are predicted to be more energy-efficient [2]. This, together with the low-power nature of smartphones and IoT devices, could help in reducing the energy consumption by up to 10× compared to a classic datacenter based on high-performance servers [1].

In the context of increased enthusiasm for blockchain technologies, we analyze the impact of 5G in this domain which is closely-connected with distributed databases [4]. A blockchain ledger represents a database distributed across thousands or millions of physical nodes, in a Byzantine environment where peers do not trust each other since some of them may be malicious. Currently, mobile networks are not involved in blockchains because the nodes are most likely connected via wired or optical links. At most, some clients interacting with blockchain peers may use mobile devices. But with the increasing scalability issue of the blockchain, and the adoption of solutions involving sharding [5] or second-tier, sub-blockchains [6], 5G has the potential to impact the performance of these systems [1]. Shards or second-tier blockchains may run at the edge of the network and include both fixed and mobile nodes and clients and peers may also run on the same physical node at the edge.

2.2 Federated Learning

The explosion of mobile and IoT devices at the edge requires a new approach towards efficient machine learning (ML). These devices act as both data consumers (e.g. actuators) and data producers (e.g. sensors). As data consumers, these devices run model inference on their own collected data. As data producers, these devices push data to higher network levels, where more powerful systems run ML model training [7]. But the explosion of edge devices exerts too much pressure on the networking connections to the cloud, and on cloud's computation and storage resources [1]. A solution to this problem is *federated learning*.

Federated learning [8] entails the building of a model on multiple devices that contribute their data to the training process. A coordinator gets the learned parameters from the devices to build an aggregated model, as shown in Figure 1. This approach is directly addressing the issue of isolated data islands, where data is found in different locations, under different organizations, and it cannot be merged or aggregated.

We envision that 5G is going to accelerate the adoption of federated learning. With high bandwidth and low latency, local model parameters and the aggregated model can be shared much faster between the devices and the coordinator. D2D communication could relieve some pressure from the device-coordinator connections by sharing intermediate parameters directly. However, this D2D communication introduces security risks in environments with malicious devices. On the other hand, network virtualization could help in solving the security and privacy issues by creating isolated slices for the task of federated learning.

2.3 Security

The adoption of 5G is going to create new security challenges. We analyze these challenges based on the 5G characteristics involved. First, we discuss the higher device density, higher bandwidth and lower latency that could create the ideal environment for launching massive distributed denial of service (DDoS) attacks [9]. It is well known that IoT devices are relatively easier to compromise compared to servers, due to factors such as low system performance that does not allow running complex anti-virus solutions on the device, software immaturity and bad security practices which are adopted to get faster time-to-market. With 5G allowing more IoT devices to be connected to the Internet, the attack surface is going to increase significantly. One of the biggest attacks to date was done using infected IoT devices with a botnet called Mirai [9] which targeted Dyn DNS servers and took down many websites, especially on the East side of the USA.

Secondly, we examine the impact of D2D communications on security. D2D is supposed to reduce the traffic to base stations, but will require strict security protocols to avoid privacy violations and device hijacking. For example, D2D communications may require an ad-hoc authentication step to determine the identity of the devices. Given the scale of 5G networks, a centralized solution is unfeasible. We envision an authentication service based on the decentralized blockchain to avoid data tempering. However, current blockchains suffer from low throughput and high latency, hence there is a need for developing novel blockchain platforms.

Thirdly, we analyze the impact of network slicing on security. As a generalization of virtualization, network slicing allows different applications to share the same physical network by operating across all layers of the networking stack. At the physical layer, the radio connection is multiplexed through spectrum sharing. At the networking layer, providers use SDN and NFV to multiplex the network. At the application level, computing resources are multiplexed using virtual machines (VM), either on the cloud or at the edge. This multitude of virtualized resources managed by different parties is a challenge for security. The threats could be present at all layers, as shown in Figure 1 where the honest user (blue) is attacked by malicious actors (red). Achieving the isolation of the entire slice across all layers poses a significant challenge because there is a need to apply a cross-layer coordinated security protocol.

3 Conclusions

In summary, the adoption of 5G is expected to accelerate the development of emerging technologies, such as IoT, edge computing, blockchain, and federated learning. In addition, 5G is going to give rise to new systems, such as millions of interconnected databases, and generate new use cases, such as remote work, immersive augmented reality, telemedicine and smart automotive, among others [1]. Security is one of the key challenges of end-to-end virtualization in 5G networks. It remains to be studied how to ensure security across systems managed by different entities and threatened by different security risks. Another key challenge is ensuring data privacy in the context of millions of interconnected databases and federated learning.

Acknowledgement: This research is supported by Singapore Ministry of Education Academic Research Fund Tier 3 under MOE's official grant number MOE2017-T3-1-007.

References

[1] D. Loghin, S. Cai, G. Chen, T. T. A. Dinh, F. Fan, Q. Lin, J. Ng, B. C. Ooi, X. Sun, Q.-T. Ta, W. Wang, X. Xiao, Y. Yang, M. Zhang, and Z. Zhang, "The Disruptions of 5G on Data-driven Technologies and Applications." CoRR, vol. abs/1909.08096, 2019.

[2] N. Al-Falahy and O. Y. Alani, "Technologies for 5G Networks: Challenges and Opportunities," *IT Professional*, vol. 19, no. 1, pp. 12–20, 2017.

[3] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," *IEEE Communications Surveys Tutorials*, vol. 19, no. 3, pp. 1657–1681, 2017.

[4] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[5] H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, and B. C. Ooi, "Towards Scaling Blockchain Systems via Sharding," in *Proc. of International Conference on Management of Data*, pp. 123–140, 2019.

[6] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments." https://lightning.network/lightning-network-paper.pdf, 2016.

[7] B. C. Ooi, K.-L. T. Tan, S. Wang, W. Wang, Q. Cai, G. Chen, J. Gao, Z. Luo, A. K. Tung, Y. Wang, Z. Xie, M. Zhang, and K. Zheng, "SINGA: A Distributed Deep Learning Platform," in *Proc. of the 23rd ACM International Conference on Multimedia*, pp. 685–688, 2015.

[8] H. B. McMahan, E. Moore, D. Ramage, and B. A. y Arcas, "Federated Learning of Deep Networks using Model Averaging," *CoRR*, vol. abs/1602.05629, 2016.

[9] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.