河南科技学院

2022 届本科毕业论文（设计）

英文文献及翻译

On the Dependability of 6G Networks

学生姓名： 胡超

所在院系： 信息工程学院

所学专业： 通信工程

评阅意见： _____ **导师签名:** _____

On the Dependability of 6G Networks

ABSTRACT

Sixth-generation communication networks must be highly dependable due to the foreseen connectivity of critical infrastructures through them. Dependability is a compound metric of four well-known concepts—reliability, availability, safety, and security. Each of these concepts have unique consequences for the success of 6G technologies and applications. Using these concepts, we explore the dependability of 6G networks in this article. Due to the vital role of machine learning in 6G, the dependability of federated learning, as a distributed machine learning technique, has been studied. Since mission-critical applications (MCAs) are highly sensitive in nature, needing highly dependable connectivity, the dependability of MCAs in 6G is explored. Henceforth, this article provides important research directions to promote further research in strengthening the dependability of 6G networks.

Keywords:6G; Dependability; Security; Reliability; Availability; Safety; Communication networks

1 Introduction

Fifth-generation wireless networks brought innovative technological concepts into the wireless domain that closed the gap between traditional IT domains and communication networks. For example, cloudification and softwarization of networking technologies enabled deploying new use cases and applications in wireless networks. Technologies from the physical layer, such as massive multi-input multi-output (MIMO), to the application layer, such as machine learning (ML) technologies, have increased networks' capacities and capabilities. However, 5G cannot meet the requirements of emerging services such as the Internet of Everything (IoE), due to the inherent limitations of 5G systems [1]. Sixthgeneration communications networks will take a huge leap beyond 5G in order to meet the needs of future services and societies, which will be centered around data centric, intelligent, and automated processes [2]. Novel disruptive technologies in the domains of terahertz and optical communications, cell-less coverage through integrated terrestrialsatellite access technologies [3], distributed end-user terminal-based artificial intelligence (AI) [4,5], and distributed ledger technologies (DLTs) [6], to name a few, will converge to fulfill the needs of emerging applications and use cases [7].

Furthermore, 6G is expected to ignite a human transformation, thanks to improved context-aware devices with new human–machine interfaces provided by end-devices that are no longer mere data collectors, but multiple synchronized entities working in unison. This will dramatically improve the way we interact with both the physical and digital worlds. Such services will have have stringent quality of service (QoS) requirements in terms of bandwidth, reliability, and latency that will be challenging for existing 5G networks to provide. For example, ubiquitous and universal computing with resources distributed locally and in the cloud, knowledge systems that store and convert data into actions, and efficient sensing for controlling the physical world cannot be provided in 5G, and thus, focus is put on 6G research. Sixth-generation networks are also envisioned to provide massive-scale connectivity, 3D networking, real-time immersion through extended reality (XR), and haptic applications [8].

In this work, we study the dependability of 6G networks in four dimensions, i.e., reliability, availability, safety, and security. We also analyze how the distributed nature of 6G networks negatively affects their dependability. Furthermore, we dive

into the roles of distributed AI techniques and distributed mission-critical applications (MCAs) that are currently used in the intelligentization of the networks. We bring forth important challenges with potential solutions and shed light on interesting future research directions. Henceforth, this article is organized as follows: Section 2 highlights the related work and contributions of this article. Section 3 briefly discusses the concept of dependability. Section 4 discusses dependability in 6G networks. Section 5 briefly introduces the AI techniques expected to be deployed on 6G edges, and their effects on dependability. Section 6 provides insights into the relation between dependability of MCAs in 6G. Interesting future research directions are summarized in Section 7, and the article is concluded in Section 8.

2 Related Work and Our Contributions

In this section, we describe the related work and our contributions.

2.1 Related Work

Dependability is extremely important for future 6G communications, mainly due to the integration of critical infrastructures through wireless networks. There exists research that focus on each individual topic, such as reliability, availability, safety, and security. However, dependability as whole has received little research attention. There also exist research on specific topics, such as dependability of industrial IoT [14], where the focus is on real-time and reliability requirements of industrial IoT networks. Similarly, the authors of [15] discuss the dependability of software-defined networks. The article argues the need for secure and dependable SDNs by-design by first highlighting the threat vectors that can be used by adversaries. Then, the article sketches the design of a secure and dependable network architecture, mainly focusing on the control platform.A survey on heterogeneous dependable wireless networks, focusing on industry, is presented in [16]. The article elaborates on the heterogeneous nature of the next generation factories, where diverse technologies are interconnected through a diverse set of wired and wireless connectivity technologies. However, the main focus is on industrial systems, where dependability in terms of availability and latency of existing technologies is critically discussed.

The main lesson learned from the existing research is that most articles are focused on a specific dimensions of dependability.

2.2 Contributions of the Paper

The main contributions of this article revolve around:

(1) We analyze the role of dependability in 6G networks from a system-wide point of view, studying each of the four components of dependability separately.

(2) We analyze how the omnipresence and distributed nature of AI/ML affects the dependability of 6G systems.

(3) We study the importance of dependability in MCAs, analyzing every aspect of dependability separately.

(4) We identify future research directions that are summarized in Table 1 and will help to increase the dependability of future 6G networks.

For smooth readability, the most important acronyms are defined in Abbreviations.In the following section, we discuss the background and principles of dependability.

Table 1. Existing challenges and potential future research directions.

Dependability	Challenge	Potential Future Research Directions
Reliability	Distributed control and management will increase the complexity of the overall system which can lead to reliability challenges.	Dependable 6G would require a hierarchical architecture that provide logical centralized view of the overall network including the architecture and infrastructure elements, and loosely coupled distributed control elements, all synchronized through a global view can simplify the overall system.
Availability	Due to the distributed control, availability can be increased in principle, however, availability can be compromised through weaknesses in security, reliability and safety.	The architecture should be modular and distributed as it is, and designed such that the effects of cascading failures are avoided, where availability of one module or component does not compromise the availability of another.
Safety	Safety is a rarely researched topic from technical perspectives and is intertwined with security.	The main work needed in increasing safety of future communications networks is defining safety in technical terms and aligning safety research with the rest, similar to security-by-design, safety-by-design must be brought into discussions and research.
Security	Security in 6G is extremely complicated in terms of new technologies, modular distributed design, and the increasingly vanishing physical-cyber borders leading to highly complex network architectures.	First, it will be important to know early whether to build 6G security on top of the 5G standards or rethink according to the new disruptive technologies from application to physical layers. How to design security systems for the loosely coupled, highly distributed, and inter-dependent systems that are synchronized on one hand and avoid the risks related to cascading failures on the other hand, will be extremely important. Furthermore, AI related risks and challenges including its sustainability will exacerbate in 6G and will require serious research efforts.

3 Dependability

Dependability is the ability of a system to deliver a service that can justifiably be trusted; in other words, it should avoid frequent and severe service failures [24]. Though crucial in importance, dependability is often overlooked in favor of other research directions. Priority has been given to coordinating computing activities between distributed nodes in order to achieve higher performance, or security mechanisms that help in protecting users and their data. As previously mentioned, dependability is a compound metric and can be discussed through four important indicators: reliability, availability, safety, and security. Although performance and security are important, and as such most of the works focus on them, the other three requirements of dependable systems should not be underestimated [25,26]. Moreover, there are many facets of dependability, for instance, confidentiality and integrity [27]. However, some of the concepts converge into the four aspects discussed throughout this article. Therefore, for brevity we limit the discussion to the topics of reliability, availability, safety, and security, as described below.

3.1 Reliability

The complexity of distributed edge networks means that achieving reliability in such an environment is not an easy task. With the increasing number of MCAs solutions on the market, requirements for reliable systems are indispensable, and furthermore, still a challenge to achieve. Rapid changes in computing environments also bring challenges to reliability, for example, asynchronism, heterogeneity of software/hardware, scalability, and fault tolerance, to mention some. In [28], the authors briefly explored reliability issues in edge AI systems and proposed an architecture that meet latency and reliability requirements for many MCAs. It is identified that computation on edge systems occur in three different layers: bottom (end devices), middle (servers), and top (centralized cloud). In order to achieve good communication and a fast response, all three layers must be properly synchronized, like the storing and data access for processing [13].

3.2 Availability

Availability is realized once reliability has been achieved. Reliability is the probability that the system is working, and availability is the probability of it working at a given time. Availability ensures that no denial of authorized access to the system occurs [29]. The advantage of distributed systems is that additional nodes and communication paths help hiding any failure that might exists. Current research

trends in edge computing aim at improving system availability by carefully planning task and data offloading from end devices towards edge servers with frameworks that are even capable of performing the offloading based on network statistics and the edge servers' computation capabilities. Another characteristic helping availability is the reassignment of tasks from failing nodes, although common node failures are still a problem, since a task that crashes a node can be moved to another node and causes the same type of crash. Since availability and reliability work together, it is important to notice they can also work at cross purposes; with this in mind, both concepts must be weighted against one another, as different systems might require a different degree of each.

3.3 Safety

Safety is critical for MCAs, especially in use cases where human lives are at danger, such as autonomous driving and telesurgery. The IEC 60601 [29]. which is a technical standard for the safety and performance of the medical electrical equipment, defines safety as the avoidance of any hazards due to the operation of a device under normal or singlefault conditions. However, this definition can be broadened to cover non-medical domains, thereby including faulty conditions such as wrong lane selection in autonomous driving, or task offloading failure affecting the information given to the end user, or creating distractions in an augmented reality application. The current trend in communication networks is to simplify safety through the development of bug-free software or through an AI-based optimization problem. It is necessary to study the interaction between the composing cyberphysical systems (CPS) and the environment of each use case [30]. In [31,32], telesurgery safety considerations from the medical point of view are given. It also mentions their experience with different surgical robots and elaborates on some comparisons.

3.4 Security

Security is one of the main issues in communication networks, as both nodes and the whole network are attacked by malicious users [22,33]. The distributed and datadriven nature of future 6G communication networks and its use cases mean more data, and of course, a wider attack surface. The applications of AI or ML in communications networks are increasing at a higher pace due to apparent reasons [34]; however, AI and ML also bring their own security challenges in communications networks, as elaborated in [35,36]. The most important part is to identify the required

level of security for a certain use case and adopt the principles of the security-by-design approach. These concepts are quite important due to the diverse nature of 6G MCAs. Furthermore, the rise in the number of capable attackers targeting communication networks call for stringent security requirements. In [37], the authors explore the application of blockchain technology alongside ML in order to protect vehicular networks from cyber attacks. Similarly, in [38], the authors used a smart contract architecture in heterogeneous vehicular networks for collaboratively performing tasks between moving vehicles and parked vehicles. The smart transactions consider the characteristics of both the network and the attack models for improving security. Furthermore, physical-layer security techniques can be used to provide security with drastic changes to the network architecture [23,39].

4 6G and Dependability

4.1 Brief Introduction to 6G Networks

The rapid development of multimedia applications for use cases such as high-fidelity holograms, tactile Internet, and the support of MCAs require a higher bandwidth, lower latency, and higher reliability than that offered by the current 5G communication networks [40,41]. Therefore, 6G aims to fulfill these requirements through base-station densification (mmWave and terahertz tiny cells, temporary hotspots) with other means for distribution of network functions, such as extended edge computing, and exploration of higher frequencies above 300 GHz, as discussed in [1]. The resulting 6G networks, thus, will be expected to provide more than just communications, i.e., to interconnect communication, computing, and sensing technologies with the physical, biological, and cyber worlds, thereby acting as distributed neural networks that will enable intelligence of everything. Sixth-generation networks will transform the way we communicate, from connected people and devices to connected intelligence. This means bringing intelligence closer to every person, home, or business, for example, in the form of edge intelligence. Therefore, 6G networks are bound to be large-scale, use heterogeneous access with cell-free or cell-less coverage, and dynamic with heavily-distributed storage and computation capabilities [42].

Fast and focused data processing through edge computing is the cornerstone of applications in 6G, for example, in vehicle-to-everything communications [46]. In-depth data analysis could be carried out by the centralized cloud at the expense of delays [47]. Figure 1 shows a simplified architecture of an AI-based 6G network, which is divided into three parts: user environment, networks, and management and control. In the management and control, functions such as parameter optimization, resource management, and task scheduling are carried out. In the network part, some of the tasks performed are data filtering, knowledge discovery, and feature extraction for data analytics, besides the usual network layers' work. Finally, in the user's environment, all the sensing, monitoring, and data collection occurs. The increase in data volumes being processed at the edge of the network represents a difficulty in properly identifying useful data for a primary analysis, prior to passing them to the centralized cloud. These requirements have paved the way to the intelligentization of the edge computing, referred to now as edge intelligence or EdgeAI [48], transforming it into a AI-based platform capable of offering intelligent services [49]. In order to achieve this, research hs departed from the centralized cloudbased approach, sparkling an interest in distributed, low-latency, and reliable AI at the edge [50,51].

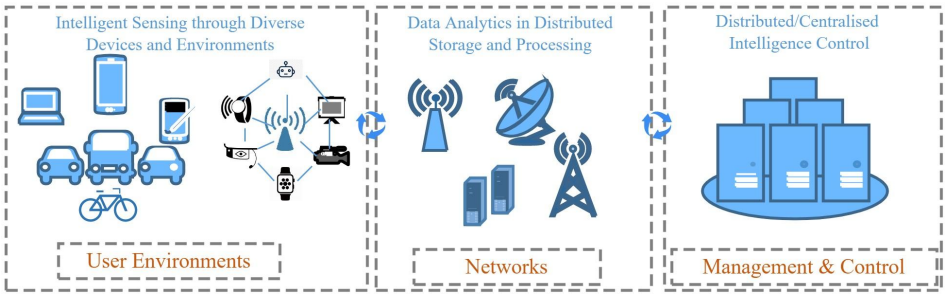

Figure 1. An abstract representation of enabling intelligence in 6G networks.

EdgeAI is drawing an increasing attention, and its development is closely aligned with that of reliability in communications and end-device constraints. This allows the deployment of a network whose operation resembles that of a distributed computer, which is deployed between the centralized cloud and end users. This distributed nature of EdgeAI can have huge impacts on dependability of 6G networks, as discussed below.

4.2 Dependability in 6G Networks

Sixth-generation networks are expected to offer extremely high reliability. EdgeAI supports the vision of 6G through offering more computational power near

users or services while reducing overall latency. Reliability requires checking the necessary requirements instead of assuming that these are fulfilled and constantly monitoring the network [52]. Although in terms of performance, EdgeAI supposes a step forward, its distributed nature, combined with the high number of servers required, might well introduce other issues. First, we have asynchronism. As the number of edge servers rises, they are also expected to be capable of working in unison; this means being synchronized. Synchronization is improved when servers are aware of the status of neighboring servers; in other words, the exchange of information, such as available memory or processing power, is shared in a timely manner.

4.2.1 Reliability

Sixth-generation networks are expected to offer extremely high reliability. EdgeAI supports the vision of 6G through offering more computational power near users or services while reducing overall latency. Reliability requires checking the necessary requirements instead of assuming that these are fulfilled and constantly monitoring the network [52]. Although in terms of performance, EdgeAI supposes a step forward, its distributed nature, combined with the high number of servers required, might well introduce other issues. First, we have asynchronism. As the number of edge servers rises, they are also expected to be capable of working in unison; this means being synchronized. Synchronization is improved when servers are aware of the status of neighboring servers; in other words, the exchange of information, such as available memory or processing power, is shared in a timely manner.

4.2.2 Availability

Availability is the assurance of access to services and resources by legitimate users, or the quality of being ready or present for immediate use [53]. As mentioned in Section 2, reliability and availability are both intertwined. As a combination of highly distributed systems, 6G networks will be capable of dissimulating failures at the edge servers by rapidly offloading the assigned processes towards a nearby server that possesses the required resources. In the context of EdgeAI, if an edge server fails, then its tasks are offloaded towards a neighboring edge. This is where synchronism plays a major role, and in order to achieve this, servers must be aware of the status of each other. Furthermore, predictive analysis of available resources in neighboring

edge nodes will be important. Such analysis will enable performing normal routine tasks, along with the system being able to offload tasks to neighboring nodes in cases of failures, as discussed in [36]. This process will be time consuming, but the system is perceived by the user as still functioning, even with the increase in delay that task offloading represents. Similarly, load-balancing techniques that can effectively distribute tasks among available resources can also increase the availability of critical resources [54]. Although highly related, it must be noted that a system with high availability is not necessarily reliable, thereby ensuring the expected high reliability of 6G networks does not guarantee meeting the availability criteria.

4.2.3 Safety

Safety and security, looking intertwined, are highly complicated in terms of defining their roles in communications networks. Safety, also defined similarly in [55], is a system's characteristic of preventing losses due to unintentional actions by normal, non-harmful actors. Security, on the other hand, relates to deliberate actions (mostly harmful) by deliberate actors. Safety in 6G communications networks can be achieved by taking several measures that are also related to security, which are discussed in the following security part. Aside from foolproof security, safety can be achieved by improving monitoring and response systems, increasing multiplicity or redundancy, and distributing important control functions throughout the network. EdgeAI thus plays a very important role in providing opportunity for redundant resources and distributing important network control functions. The concept of devolving control functions, with the help of miniaturizing edge to the extreme, as discussed in [56], can improve safety in terms of minimizing the impact of failures and delimiting the consequences. The same is true for communications links, using multiple access technologies to avoid blackout due to failure in one. Satellite communications [57,58] present interesting solutions to be coupled with terrestrial networks for enabling safe operation in times of failures, as a redundant communication infrastructure. The key point in improving safety in 6G is enabling the system to function in the wake of uncertainty, failures in different perimeters and surroundings, and security vulnerabilities and attacks, which are discussed below.

4.2.4 Security

As one of the main concerns regarding modern networks, security in 6G is of paramount importance. Novel technologies in 6G networks will also introduce new

security concerns. In this regard, we could mention teraHertz (THz) technology, which is believed to hinder the ability of malicious users to perform eavesdropping; however, recent research has shown it is still possible, although difficult, to intercept the signals, even when transmitted with narrow beams [59]. Quantum communications are also expected to make a significant contribution in 6G networks, mainly from the perspectives of communications security, such as quantum and post quantum cryptography [60]. Nevertheless, the technology is still at its infancy, and although many advances have been made in the quantum cryptography field, there are still issues regarding operation errors in long distance communications. Furthermore, quantum computing can raise significant challenges to existing cryptographic security protocols [61].

5 Machine Learning, Dependability, and 6G

AI and its major branch, ML, will shape 6G networks [34,42]. Due to its tight QoS requirements, future 6G networks will posses such a complex architecture that performing legacy network operations will be deemed unsound. For this, ML techniques are emerging as a response to achieve truly intelligent orchestration and network management [62]. The dynamic nature of communication networks provides data for ML-enabled spectrum management and channel estimation, which are the basis of ultra-broadband techniques. Additionally, ML is being used to improve security, resource allocation, mobility management, and low-latency services in MCAs [34]. In particular, ML techniques such as deep learning have proved to be extremely efficient in preventing serious security attacks, such as distributed DoS attacks [63]. Distributed ML will be highly important in 6G due to the emerging needs of distributed processing at the edges of the network [64]. FL is currently among the most used distributed ML techniques in communication networks [44,65] and is highly important for 6G due to its ability to be used in a distributed manner, much like the foreseen distributed control nature of 6G networks.

5.1 Background in Brief

FL [66] was conceived by Google researchers back in 2016. Since then, it has experienced wide adoption in both industry and academia. The idea behind FL is to move the training towards the end devices while federating local models and learning, to build a privacy-preserving ML framework by keeping all raw data on devices and

aggregating local model updates, while also reducing the communications overhead. The FL process is conformed by several communication rounds between a server and the clients, performed in the following fashion [4,67]:

A number of clients is selected by the server based on certain conditions, such as being idle or its bandwidth limitation, to download the model parameters and use them to initialize their local model.

Using their local data, each device trains and optimizes the downloaded model. This is done by using stochastic gradient descent, a determined number of minibatch steps, and several epochs in order to increase the update quality and reduce the communications cost.

When the training is done, clients send their updates towards the server. It is important to notice that some clients might drop out due to connectivity issues, lack of processing power, etc. Nevertheless, the round continues with the received updates. If there are too many dropped out clients, the current round is abandoned.

The server receives the updates, weights them based on their training set sizes, and finally, aggregates them. A new model is built on the server, and the next round begins.

Figure 2 shows a simplified flowchart of the previously explained FL process. θ represents the global model parameters, nk corresponds to the data size of the client k, K is the total number of clients, and t is the communication round.

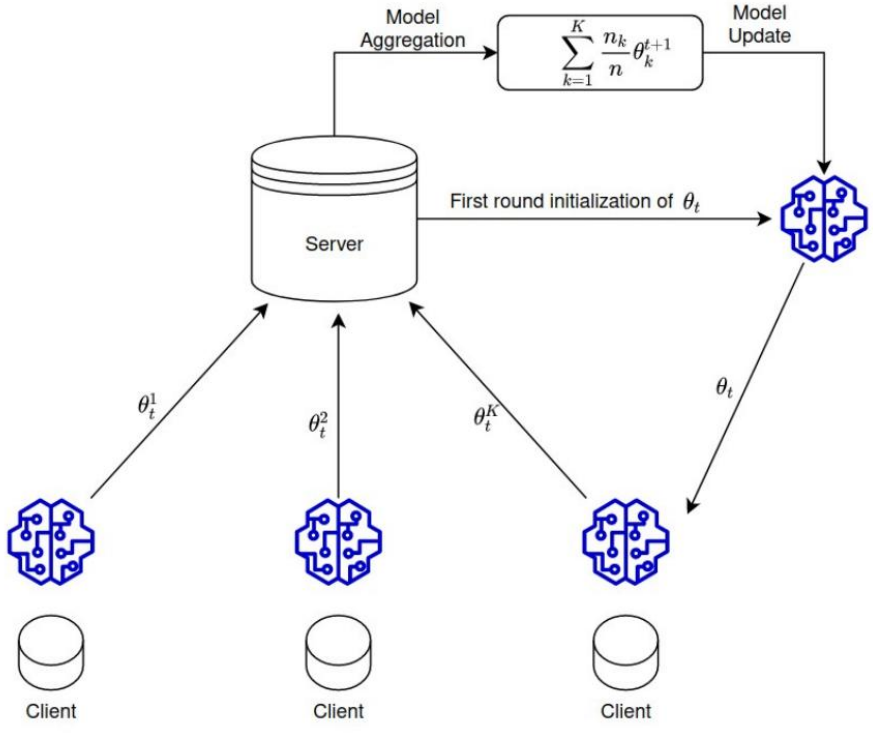

Figure 2. Simplified FL model presentation.

5.2 Dependability of Federated Learning

5.2.1 Reliability

ML techniques rely heavily on data. Data quality is fundamental for achieving high accuracy during the learning task. Client selection is a critical issue in FL, as clients are the ones updating the local models previous to the global aggregation, it is fundamental to properly select the clients that train the models using the highest quality of data. Most of the FL systems select their clients in a random manner, or based on resource conditions. Such selection of course might affect the global performance, as non-trustable nodes can also be selected. Moreover, the complexity of conceiving client selection in a communications network due to its dynamic nature also hinders their reliability. Even further, as it is difficult for the centralized entity that performs the selection to actually monitor a largescale behavior, the selected untrustable clients are unlikely to be removed. Moreover, since the FL process consists of several rounds, previously selected untrusted clients might also be selected for future rounds. This can further damage the learning accuracy. Similarly, security vulnerabilities and lapses can also affect reliability.

5.2.2 Availability

A lack of, or improper, criteria when selecting the clients for local training does not only affect reliability, but availability also. Untrusted clients using low quality data for training hinders the whole learning process and may severely affect predictions. In this manner, a FL framework whose accuracy is not as desired cannot be deployed, nor can services trust it, thereby rendering it unavailable. Availability in FL systems is complex to achieve due to the distributed nature of the model training, and the centralization of global model aggregation; in other words, it is not possible to hide a “faulty” or badly trained model when several untrusted clients have performed training with corrupted data. Moreover, this centralization of the aggregation process renders a FL framework vulnerable to weak aggregation algorithms, which are incapable of discerning high-quality trained models from those coming from suspicious clients. Availability is also hindered by security issues discussed in Section 4.

5.2.3 Safety

Damage done by the selection of untrusted clients goes further than that of a

faulty or badly trained model. Since learning is crucial for many use cases, untrusted clients might hinder the prediction capacity of a system. This can cause safety-related issues for users. We can consider an autonomous vehicle with an positioning model based on FL, which is trained collectively with other autonomous vehicles. If a malicious vehicle is allowed to send its trained model for aggregation, this could affect the driving decisions of other vehicles, putting the passengers' lives at risk. The problem is only exacerbated by the centralization issue raised in the previous subsection, where weak aggregation algorithms do not help discriminating good from bad trained models.

5.2.4. Security

Security is an important challenge in ML [35]. Even when FL improves user data privacy, security is still a main concern. An untrusted client that is selected to participate in a FL round could perform attacks, such as maliciously using unreliable data or injecting false data. Additionally, a malicious client could also launch attacks alongside other malicious users aimed at increasing misclassification. False-data injection refers to clients purposely adding wrong data to the training sets. On the other hand, workers might unintentionally provide low-quality raw data due to constraints in energy or high-speed mobility. Another security threat is related to the centralized model aggregation and the server where this function is located. In case a malicious user gains access to it, then the whole learning process will be hindered in the best case. In the worst case scenario, availability would be severely compromised. A communications channel vulnerability also affects FL frameworks, as the learning process consists of several rounds. An unencrypted channel will render the locally trained model vulnerable for attackers to perform reconstruction attacks.

6 Conclusions

Sixth-generation communication networks will connect critical infrastructures. Therefore, the dependability of 6G communication networks is extremely important. Since 6G exacerbates the merging of the physical and digital worlds beyond the current traditional cyber-physical systems, dependability in terms of reliability, availability, safety, and security needed a thorough investigation. Therefore, in this article we have shed light on the dependability of 6G networks, first to highlight its importance and relevance in 6G, and then to bring forward existing challenges and

potential solutions. The main challenges that persist in all dimensions of dependability arise from the distributed nature of 6G. The solutions, thus, must also be targeted at distributed network architectures. Therefore, edge computing, FL, and movable softwarized network functions, to name a few directions, related to reliability, availability, safety, and security, need to be researched. In summary, this article opens up interesting research questions and highlights research gaps to improve the dependability of 6G networks and systems.

关于 6G 网络的可靠性

摘要

第六代通信网络必须高度可靠，因为可以预见关键基础设施将通过它们连接。可靠性是四个众所周知的概念的复合指标——可靠性、可用性、安全性和保密性。这些概念中的每一个都对 6G 技术和应用的成功产生了独特的影响。使用这些概念，我们在本文中探讨了 6G 网络的可靠性。由于机器学习在 6G 中的重要作用，联邦学习作为一种分布式机器学习技术的可靠性得到了研究。由于关键任务应用程序 (MCA) 本质上是高度敏感的，需要高度可靠的连接，因此探索了 6G 中 MCA 的可靠性。今后，本文提供了重要的研究方向，以促进进一步研究加强 6G 网络的可靠性。

关键词：6G；可靠性；安全性；可靠度；可用性；安全；通讯网络

1 绪论

第五代无线网络将创新的技术概念带入无线领域，缩小了传统 IT 领域与通信网络之间的差距。例如，网络技术的云化和软件化使得能够在无线网络中部署新的用例和应用程序。从物理层（例如大规模多输入多输出 (MIMO)）到应用层（例如机器学习 (ML) 技术)的技术提高了网络的容量和能力。然而，由于 5G 系统的固有局限性，5G 无法满足万物互联 (Internet of Everything, IoE) 等新兴服务的需求 [1]。第六代通信网络将超越 5G 实现巨大飞跃，以满足未来服务和社会的需求，这些需求将围绕以数据为中心的智能和自动化流程 [2]。太赫兹和光通信领域的新型颠覆性技术、通过集成地面卫星接入技术实现的无小区覆盖 [3]、基于分布式终端用户终端的人工智能 (AI) [4,5] 以及分布式账本技术 (DLT) [6]，仅举几例，将融合以满足新兴应用程序和用例的需求 [7]。

此外，6G 有望引发人类变革，这要归功于改进的情境感知设备以及由终端设备提供的新人机界面，这些终端设备不再仅仅是数据收集器，而是多个同步实体协同工作。这将极大地改善我们与物理世界和数字世界互动的方式。此类服务在带宽、可靠性和延迟方面将具有严格的服务质量 (QoS) 要求，这对于现有 5G 网络来说将是一项挑战。例如，资源分布在本地和云端的普适通用计算、存储数据并将数据转化为行动的知识系统、控制物理世界的高效感知等，5G 都无法提供，因此 6G 研究成为重点。第六代网络还设想提供大规模连接、3D 网络、通过扩展现实 (XR) 实现的实时沉浸和触觉应用 [8]。

在这项工作中，我们从可靠性、可用性、安全性和保密性四个维度研究了 6G 网络的可靠性。我们还分析了 6G 网络的分布式特性如何对其可靠性产生负面影响。此外，我们深入探讨了当前用于网络智能化的分布式人工智能技术和分布式关键任务应用程序 (MCA) 的作用。我们带来了重要的挑战 具有潜在的解决方案，并阐明有趣的未来研究方向。此后，本文组织如下：第 2 节重点介绍了本文的相关工作和贡献。第 3 节简要讨论可靠性的概念。第 4 节讨论 6G 网络中的可靠性。第 5 节简要介绍了有望部署在 6G 边缘的 AI 技术及其对可靠性的影响。第 6 节提供了对 6G 中 MCA 可靠性之间关系的见解。第 7 节总结了未来有趣的研究方向，第 8 节总结了本文。

2 相关工作和我们的贡献

在本节中，我们描述了相关工作和我们的贡献。

2.1 相关工作

可靠性对于未来的 6G 通信极为重要，这主要是由于通过无线网络集成了关键基础设施。存在着重于每个单独主题的研究，例如可靠性、可用性、安全性和安全性。然而，作为一个整体的可靠性很少受到研究关注。也有针对特定主题的研究，例如工业物联网的可靠性 [14]，重点是工业物联网网络的实时性和可靠性要求。同样，[15] 的作者讨论了软件定义网络的可靠性。这篇文章通过首先强调对手可以使用的威胁向量来论证安全可靠的 SDN 设计的必要性。然后，本文概述了安全可靠的网络架构的设计，主要侧重于控制平台。[16] 中介绍了针对工业的异构可靠无线网络的调查。这篇文章详细阐述了下一代工厂的异构性质，其中各种技术通过各种有线和无线连接技术相互连接。然而，主要关注点是工业系统，其中批判性地讨论了现有技术的可用性和延迟方面的可靠性。

从现有研究中吸取的主要教训是，大多数文章都侧重于可靠性的特定维度。

2.2 论文的贡献

本文的主要贡献围绕：

（1）我们从系统范围的角度分析可靠性在 6G 网络中的作用，分别研究可靠性的四个组成部分。

（2）我们分析了 AI/ML 的无处不在和分布式特性如何影响 6G 系统的可靠性。

（3）我们研究可靠性在 MCA 中的重要性，分别分析可靠性的各个方面。

（4）我们确定了表 1 中总结的未来研究方向，这将有助于提高未来 6G 网络的可靠性。

为了便于阅读，最重要的首字母缩略词在缩写中进行了定义。在下一节中，我们将讨论可靠性的背景和原则。

表 1 现有挑战和潜在的未来研究方向

可靠性	挑战	潜在的未来研究方向
可靠性	分布式控制和管理将增加整个系统的复杂性可能导致可靠性挑战。	可靠的 6G 需要一个分层架构，提供整个网络的逻辑集中视图，包括架构和基础设施元素，以及松散耦合的分布式控制元素，所有这些元素都通过全局视图同步，可以简化整个系统。

可用性	由于分布式控制，可用性可以提高原则上，但是，可用性可以通过妥协、安全性、可靠性和安全性方面的弱点。	该体系结构应该是模块化的和分布式的，并且设计为避免级联故障的影响，其中一个模块或组件的可用性不会损害另一个的可用性。
安全	安全是一个很少从技术角度研究的话题，并且与安全交织在一起。	提高未来通信网络安全性所需的主要工作是用技术术语定义安全性，并将安全研究与其他研究相结合，类似于设计安全性，必须将设计安全性纳入讨论和研究。
安全性	6G 的安全性在新的方面极其复杂技术，模块化分布式设计，以及越来越消失的物理网络边界导致高度复杂的网络架构。	首先，重要的是要及早知道是在 5G 标准之上构建 6G 安全还是根据 新的颠覆性标准重新思考从应用层到物理层的技术。如何为松耦合、高度分布式、相互依赖的安全系统设计一方面同步，另一方面避免与级联故障相关的风险的系统将极其重要。 此外，AI 相关的风险和挑战（包括其可持续性）将在 6G 中加剧， 需要认真的研究工作。

3 可靠性

可靠性是系统提供可以合理信任的服务的能力；换句话说，它应该避免频繁和严重的服务故障 [24]。尽管重要性至关重要，但可靠性往往被其他研究方向所忽视。优先考虑协调分布式节点之间的计算活动，以实现更高的性能，或帮助保护用户及其数据的安全机制。如前所述，可靠性是一个复合指标，可以通过四个重要指标进行讨论：可靠性、可用性、安全性和安全性。尽管性能和安全性很重要，因此大多数工作都集中在它们上，但不应低估可靠系统的其他三个要求 [25,26]。此外，可靠性还有很多方面，例如机密性和完整性 [27]。但是，一些概念汇集到本文中讨论的四个方面。因此，为简洁起见，我们将讨论限制在可靠性、可用性、安全性和保障性主题上，如下所述。

3.1 可靠性

分布式边缘网络的复杂性意味着在这样的环境中实现可靠性并非易事。随着市场上 MCA 解决方案的数量不断增加，对可靠系统的要求必不可少，而且仍然是一个挑战。计算环境的快速变化也给可靠性带来了挑战，例如异步性、软硬件异构性、可扩展性和容错性等。在 [28] 中，作者简要探讨了边缘 AI 系统中的可靠性问题，并提出了一种满足许多 MCA 的延迟和可靠性要求的架构。确定边缘系统的计算发生在三个不同的层：底部（终端设备）、中间（服务器）和顶部（集中式云）。为了实现良好的通信和快速响应，所有三个层都必须正确同步，例如用于处理的存储和数据访问 [13]。

3.2 可用性

一旦实现了可靠性，就实现了可用性。可靠性是系统工作的概率，可用性是它在给定时间工作的概率。可用性确保不会拒绝对系统的授权访问 [29]。分布式系统的优点是额外的节点和通信路径 帮助隐藏可能存在的任何故障。边缘计算的当前研究趋势旨在通过仔细规划任务和数据从终端设备向边缘服务器的卸载来提高系统可用性，这些框架甚至能够根据网络统计数据和边缘服务器的计算能力执行卸载。另一个有助于可用性的特性是从故障节点重新分配任务，尽管常见的节点故障仍然是一个问题，因为使节点崩溃的任务可以移动到另一个节点并导致相同类型的崩溃。由于可用性和可靠性一起工作，重要的是要注意它们也可以交叉工作；考虑到这一点，这两个概念必须相互权衡，因为不同的系统可能需要不同的程度。

3.3 安全

安全对于 MCA 至关重要，尤其是在人类生命处于危险之中的用例中，例如自动驾驶和远程手术。 IEC 60601 [29]。它是医疗电气设备安全和性能的技术标准，将安全定义为避免因设备在正常或单一故障条件下运行而造成的任何危险。然而，这个定义可以扩大到涵盖非医学领域，从而包括故障情况，例如自动驾驶中的错误车道选择，或影响提供给最终用户的信息的任务卸载失败，或在增强现实应用程序中造成干扰。通信网络的当前趋势是通过开发无错误软件或通过基于 AI 的优化问题来简化安全性。有必要研究构成网络物理系统（CPS）与每个用例环境之间的相互作用 [30]。在 [31,32] 中，给出了从医学角度考虑的远程手术安全性。它还提到了他们使用不同手术机器人的经验，并详细说明了一些比较。

3.4 安全性

安全是通信网络中的主要问题之一，因为节点和整个网络都受到恶意用户的

攻击 [22,33]。未来 6G 通信网络及其用例的分布式和数据驱动特性意味着更多数据，当然还有更广泛的攻击面。由于显而易见的原因 [34]，人工智能或机器学习在通信网络中的应用正在以更快的速度增长；然而，AI 和 ML 也在通信网络中带来了自身的安全挑战，如 [35,36] 中所述。最重要的部分是确定特定用例所需的安全级别，并采用设计安全方法的原则。由于 6G MCA 的多样性，这些概念非常重要。此外，针对通信网络的有能力的攻击者数量的增加要求严格的安全要求。在 [37] 中，作者探索了区块链技术与 ML 的应用，以保护车辆网络免受网络攻击。同样，在 [38] 中，作者在异构车辆网络中使用智能合约架构，以在移动车辆和停放车辆之间协作执行任务。智能交易考虑了网络和攻击模型的特点，以提高安全性。此外，物理层安全技术可用于为网络架构的剧烈变化提供安全性 [23,39]。

4 6G 和可靠性

4.1 6G 网络简介

针对高保真全息图、触觉互联网和 MCA 支持等用例的多媒体应用程序的快速发展需要比当前 5G 通信网络提供的更高的带宽、更低的延迟和更高的可靠性 [40,41]。因此，6G 旨在通过基站致密化（毫米波和太赫兹微型蜂窝、临时热点）以及其他网络功能分配方式（例如扩展边缘计算和探索 300 GHz 以上的更高频率）来满足这些要求，如[1].因此，由此产生的 6G 网络将有望提供的不仅仅是通信，即将通信、计算和传感技术与物理、生物和网络世界互连，从而充当分布式神经网络，使万物智能.第六代网络将改变我们的沟通方式，从互联的人和设备转变为互联的智能。这意味着让智能更接近每个人、家庭或企业，例如，以边缘智能的形式。因此，6G 网络必然是大规模的，使用具有无小区或无小区覆盖的异构接入，以及具有高度分布式存储和计算能力的动态 [42]。

通过边缘计算进行快速且集中的数据处理是 6G 应用的基石，例如，车联网通信 [46]。集中式云可以以延迟为代价进行深入的数据分析 [47]。图 1 是基于 AI 的 6G 网络简化架构，分为用户环境、网络和管控三部分。在管控上，进行参数优化、资源管理、任务调度等功能。在网络部分，除了通常的网络层工作外，执行的一些任务是数据过滤、知识发现和数据分析的特征提取。最后，在用户环境中，所有的传感、监控和数据收集都会发生。在网络边缘处理的数据量的增加表明，在将有用数据传递到集中式云之前，很难正确识别用于主要分析的有用数据。这些要求为边缘计算的智能化铺平了道路，现在称为边缘智能或 EdgeAI [48]，将其转变为能够提供智能服务的基于 AI 的平台 [49]。为了实现这一目标，

研究人员脱离了基于云的集中式方法，激发了对边缘分布式、低延迟和可靠 AI 的兴趣 [50,51]。

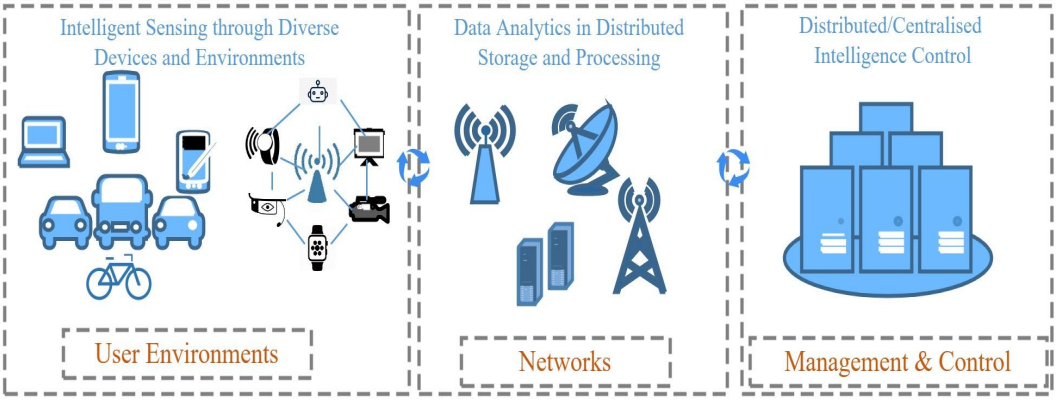

图 1. 在 6G 网络中实现智能的抽象表示。

EdgeAI 越来越受到关注，其发展与通信可靠性和终端设备约束密切相关。这允许部署其操作类似于分布式计算机的网络，该网络部署在集中式云和最终用户之间。如下所述，EdgeAI 的这种分布式特性会对 6G 网络的可靠性产生巨大影响。

4.2 6G 网络的可靠性

第六代网络有望提供极高的可靠性。 EdgeAI 通过在用户或服务附近提供更多计算能力同时减少整体延迟来支持 6G 的愿景。可靠性需要检查必要的要求，而不是假设这些要求得到满足并不断监控网络 [52]。尽管在性能方面，EdgeAI 应该向前迈进了一步，但它的分布式特性，加上所需的大量服务器，很可能会带来其他问题。首先，我们有异步性。随着边缘服务器数量的增加，它们也有望能够协同工作；这意味着同步。当服务器知道相邻服务器的状态时，同步得到改善；换句话说，可用内存或处理能力等信息的交换是及时共享的。

4.2.1 可靠性

第六代网络有望提供极高的可靠性。 EdgeAI 通过在用户或服务附近提供更多计算能力同时减少整体延迟来支持 6G 的愿景。可靠性需要检查必要的要求，而不是假设这些要求得到满足并不断监控网络 [52]。尽管在性能方面，EdgeAI 应该向前迈进了一步，但它的分布式特性，加上所需的大量服务器，很可能会带来其他问题。首先，我们有异步性。随着边缘服务器数量的增加，它们也有望能够协同工作；这意味着同步。当服务器知道相邻服务器的状态时，同步得到改善；换句话说，可用内存或处理能力等信息的交换是及时共享的。

4.2.2 可用性

可用性是合法用户访问服务和资源的保证，或者是准备好或立即使用的质量[53]。如第 2 节所述，可靠性和可用性是相互交织的。作为高度分布式系统的组合，6G 网络将能够通过将分配的进程快速卸载到拥有所需资源的附近服务器来模拟边缘服务器的故障。在 EdgeAI 的上下文中，如果边缘服务器发生故障，则其任务将卸载到相邻的边缘。这就是同步起主要作用的地方，为了实现这一点，服务器必须了解彼此的状态。此外，对相邻边缘节点中可用资源的预测分析也很重要。此类分析将能够执行正常的例行任务，并且系统能够在出现故障的情况下将任务卸载到相邻节点，如 [36] 中所述。此过程将非常耗时，但用户认为系统仍在运行，即使任务卸载所代表的延迟增加也是如此。同样，可以在可用资源之间有效分配任务的负载平衡技术也可以提高关键资源的可用性 [54]。尽管高度相关，但必须注意，具有高可用性的系统不一定可靠，因此确保 6G 网络预期的高可靠性并不能保证满足可用性标准。

4.2.3 安全

就定义其在通信网络中的角色而言，安全和安保看起来交织在一起，非常复杂。安全性，在[55]中也有类似的定义，是一种系统的特征，可以防止由于正常的、无害的行为者的无意行为而造成的损失。另一方面，安全与故意行为者的故意行为（主要是有害的）有关。 6G 通信网络的安全可以通过采取一些也与安全相关的措施来实现，这些措施将在以下安全部分进行讨论。除了万无一失的安全性之外，还可以通过改进监控和响应系统、增加多样性或冗余性以及在整个网络中分配重要的控制功能来实现安全性。因此，EdgeAI 在为冗余资源提供机会和分配重要的网络控制功能方面发挥着非常重要的作用。正如 [56] 中所讨论的那样，在将边缘微型化到极致的帮助下，下放控制功能的概念可以在最大限度地减少故障影响和界定后果方面提高安全性。通信链路也是如此，采用多种接入技术，避免因某一故障而中断。卫星通信 [57,58] 提出了与地面网络相结合的有趣解决方案，以作为冗余通信基础设施在发生故障时实现安全运行。提高 6G 安全性的关键点是使系统能够在不确定性、不同边界和环境中的故障以及安全漏洞和攻击之后正常运行，这些将在下面讨论。

4.2.4 安全性

作为现代网络的主要关注点之一，6G 的安全性至关重要。 6G 网络中的新技术也将带来新的安全问题。在这方面，我们可以提到太赫兹 (THz) 技术，该技术被认为可以阻止恶意用户执行窃听的能力；然而，最近的研究表明，即使在使用窄波束传输时，仍然有可能拦截信号，尽管很困难 [59]。量子通信也有望

在 6G 网络中做出重大贡献，主要是从通信安全的角度，如量子和后量子密码学 [60]。尽管如此，这项技术仍处于起步阶段，虽然量子密码领域取得了很多进展，但在远距离通信中仍然存在误操作的问题。此外，量子计算会对现有的密码安全协议提出重大挑战 [61]。

5 机器学习、可靠性和 6G

AI 及其主要分支 ML 将塑造 6G 网络 [34,42]。由于其严格的 QoS 要求，未来的 6G 网络将拥有如此复杂的架构，以至于执行传统网络操作将被认为是不可靠的。为此，ML 技术正在作为一种响应来实现真正的智能编排和网络管理 [62]。通信网络的动态特性为支持 ML 的频谱管理和信道估计提供了数据，这是超宽带技术的基础。此外，ML 还被用于提高 MCA 中的安全性、资源分配、移动性管理和低延迟服务 [34]。特别是，深度学习等 ML 技术已被证明在防止严重的安全攻击方面非常有效，例如分布式 DoS 攻击 [63]。由于网络边缘分布式处理的新兴需求，分布式 ML 在 6G 中将非常重要 [64]。 FL 目前是通信网络中使用最广泛的分布式 ML 技术之一 [44,65]，并且由于它能够以分布式方式使用，这与 6G 网络的可预见分布式控制性质非常相似，因此对于 6G 非常重要。

5.1 背景简介

FL [66] 由谷歌研究人员于 2016 年构想。从那时起，它在工业界和学术界得到了广泛采用。 FL 背后的想法是将训练转移到终端设备，同时联合本地模型和学习，通过将所有原始数据保存在设备上并聚合本地模型更新来构建一个保护隐私的 ML 框架，同时减少通信开销。 FL 过程由服务器和客户端之间的几轮通信组成，执行方式如下 [4,67]：

服务器根据某些条件（例如空闲或带宽限制）选择一些客户端来下载模型参数并使用它们来初始化其本地模型。

每个设备使用其本地数据训练和优化下载的模型。这是通过使用随机梯度下降、确定数量的小批量步骤和几个 epoch 来完成的，以提高更新质量并降低通信成本。

训练完成后，客户端将更新发送到服务器。重要的是要注意一些客户端可能会由于连接问题、处理能力不足等原因而退出。尽管如此，该回合仍会继续接收更新。如果退出的客户过多，则放弃本轮。

服务器接收更新，根据训练集大小对它们进行加权，最后聚合它们。服务器上建立了一个新模型，下一轮开始。

图 2 显示了先前解释的 FL 过程的简化流程图。 θ表示全局模型参数，nk 对应客户端 k 的数据大小，K 为客户端总数，t 为通信轮次。

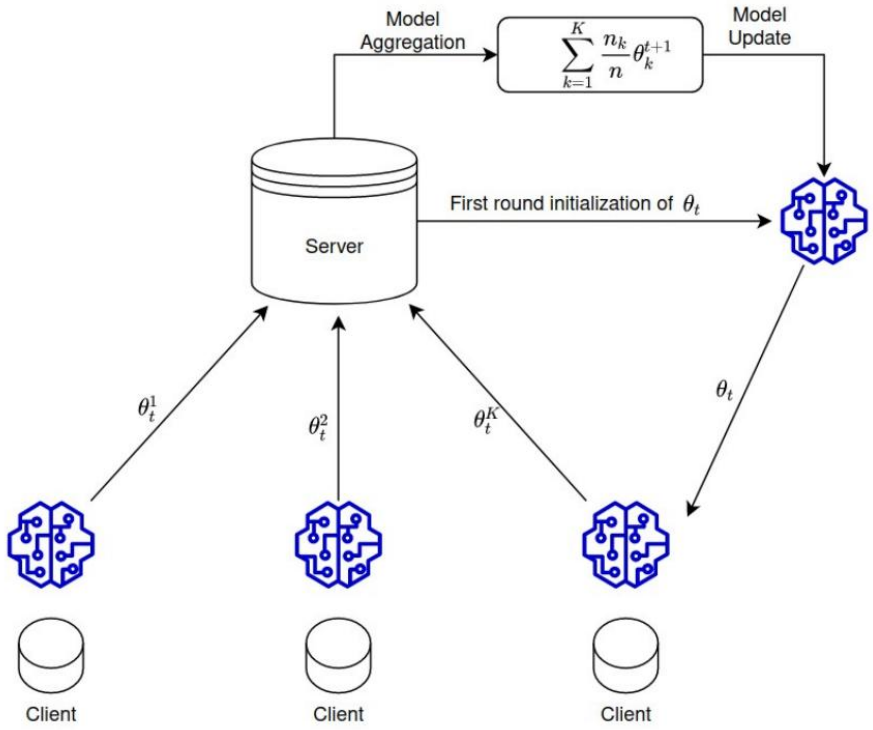

图 2. 简化的 FL 模型演示。

5.2 联邦学习的可靠性

5.2.1 可靠性

机器学习技术在很大程度上依赖于数据。数据质量是在学习任务中实现高精度的基础。客户端选择是 FL 中的一个关键问题，因为客户端是在全局聚合之前更新本地模型的客户端，因此正确选择使用最高质量数据训练模型的客户端至关重要。大多数 FL 系统以随机方式或基于资源条件选择它们的客户端。这样的选择当然可能会影响全局性能，因为也可以选择不可信任的节点。此外，由于通信网络的动态特性，在通信网络中构想客户端选择的复杂性也阻碍了它们的可靠性。更进一步，由于执行选择的中心化实体很难实际监控大规模行为，因此所选择的不可信客户端不太可能被删除。此外，由于 FL 过程由几轮组成，以前选择的不受信任的客户端也可能被选择用于未来的轮次。这会进一步损害学习的准确性。同样，安全漏洞和失误也会影响可靠性。

5.2.2 可用性

在为本地培训选择客户时缺乏标准或标准不当不仅会影响可靠性，还会影响可用性。使用低质量数据进行训练的不受信任的客户端会阻碍整个学习过程，并可能严重影响预测。这样一来，精度达不到要求的 FL 框架就无法部署，服务也

无法信任它，从而使其不可用。由于模型训练的分布式特性和全局模型聚合的集中化，FL 系统的可用性很难实现；换句话说，当多个不受信任的客户端使用损坏的数据进行训练时，不可能隐藏“错误”或训练有素的模型。此外，这种聚合过程的集中化使得 FL 框架容易受到弱聚合算法的影响，这些算法无法从来自可疑客户的模型中辨别出高质量的训练模型。可用性也受到第 4 节中讨论的安全问题的阻碍。

5.2.3 安全

选择不受信任的客户端所造成的损害比错误或训练有素的模型造成的损害更大。由于学习对于许多用例至关重要，因此不受信任的客户端可能会阻碍系统的预测能力。这可能会给用户带来安全相关的问题。我们可以考虑具有基于 FL 的定位模型的自动驾驶汽车，它与其他自动驾驶汽车一起训练。如果允许恶意车辆发送其经过训练的模型进行聚合，这可能会影响其他车辆的驾驶决策，从而危及乘客的生命安全。上一小节中提出的中心化问题只会加剧这个问题，其中弱聚合算法无助于区分好的和坏的训练模型。

5.2.4 安全性

安全性是 ML [35] 中的一个重要挑战。即使 FL 改善了用户数据隐私，安全仍然是主要问题。被选中参与 FL 回合的不受信任的客户端可能会执行攻击，例如恶意使用不可靠的数据或注入虚假数据。此外，恶意客户端还可以与其他恶意用户一起发起攻击，以增加错误分类。虚假数据注入是指客户故意向训练集中添加错误数据。另一方面，由于能源或高速移动的限制，工作人员可能会无意中提供低质量的原始数据。另一个安全威胁与中心化模型聚合和该功能所在的服务器有关。如果恶意用户获得访问权限，那么在最好的情况下整个学习过程都会受到阻碍。在最坏的情况下，可用性将受到严重影响。通信通道漏洞也会影响 FL 框架，因为学习过程由几轮组成。未加密的通道将使本地训练的模型容易受到攻击者执行重建攻击。

6 结论

第六代通信网络将连接关键基础设施。因此，6G 通信网络的可靠性极为重要。由于 6G 加速了物理世界和数字世界的融合，超越了当前传统的网络物理系统，因此需要对可靠性、可用性、安全性和保障性方面的可靠性进行彻底调查。因此，在本文中我们对 6G 网络的可靠性进行了阐述，首先强调其在 6G 中的重要性和相关性，然后提出存在的挑战和潜在的解决方案。在可靠性的各个方面持

续存在的主要挑战来自 6G 的分布式特性。因此，解决方案还必须针对分布式网络架构。因此，需要研究边缘计算、FL 和移动软件化网络功能等与可靠性、可用性、安全性和保密性相关的几个方向。总之，本文提出了有趣的研究问题并强调了研究差距，以提高 6G 网络和系统的可靠性。