**河南科技学院**

**2022届本科毕业论文（设计）**

**英文文献及翻译**

**Perspective—6G and IoT for Intelligent Healthcare: Challenges and Future Research Directions**

**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:**

**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:

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.

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

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

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. |

**Table 1.** *Cont*.

|  |  |  |
| --- | --- | --- |
| **Dependability** | **Challenge** | **Potential Future Research Directions** |
| 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

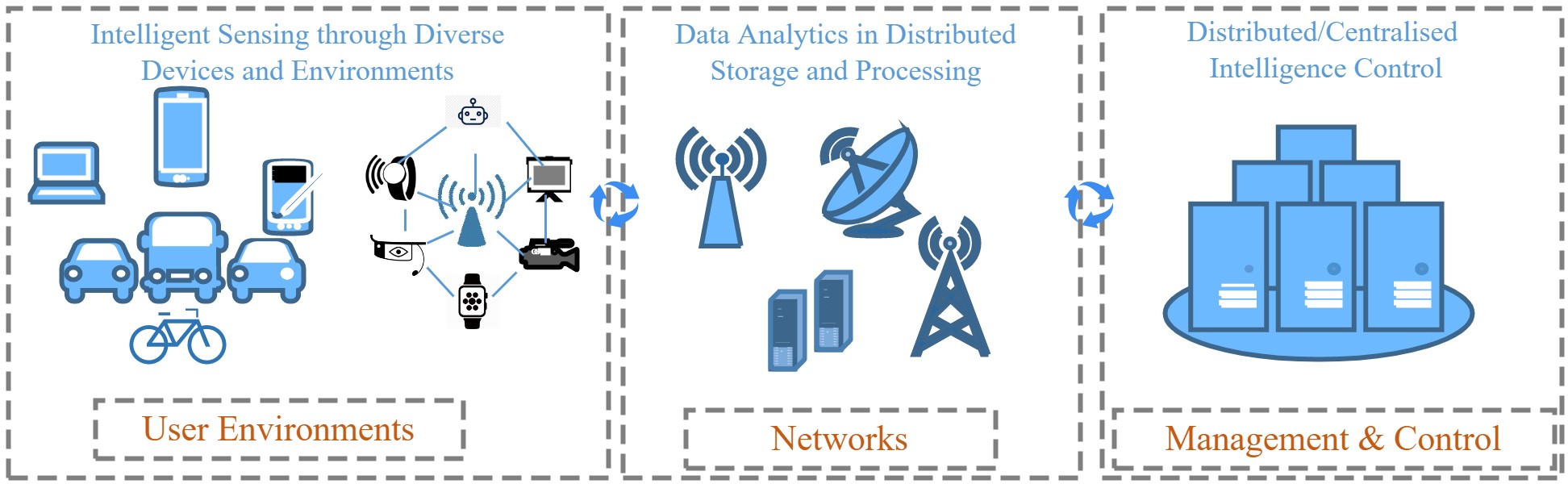
Security is one of the main issues in communication networks, as both nodes and the whole network are attacked by malicious users [22,33]. The distributed and datadriven nature of future 6G communication networks and its use cases mean more data, and of course, a wider attack surface. The applications 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]:

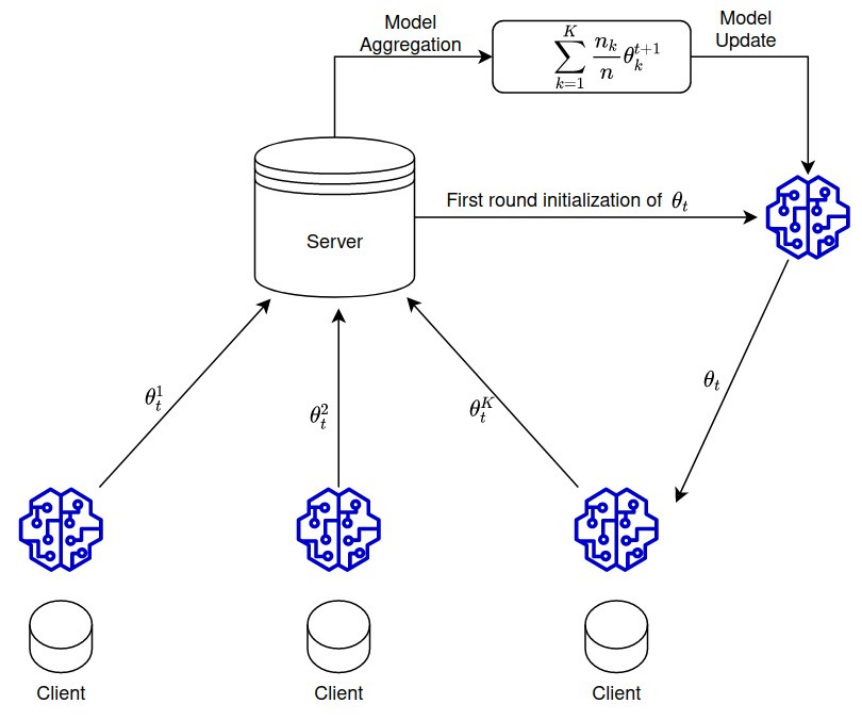
A number of clients is selected by the server based on certain conditions, such as being idle or its bandwidth limitation, to download the model parameters and use them to initialize their local model.

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.