Towards dependable 6G networks

Felipe Rodriguez, Ijaz Ahmad, Jyrki Huusko, Kari Seppänen
VTT Technical Research Center of Finland, Espoo, Finland
Email: [firstname.lastname]@vtt.fi,

***Abstract*—6G communication networks must be highly dependable due to the huge number applications, services, and public infrastructures that will be dependant on it. However, the integration of vast number of technologies, ranging from physical layer up to the application layer, and diverse services ranging from entertainment to mission critical public services need investigation of the infrastructure from dependability point of view. We take four dependability concepts such as reliability, availability, safety and security, and discuss the dependability of 6G networks. Since intelligence and distribution of control functions and elements make the core of future networks, specific diligence is given federated learning and edge intelligence. This article, in summary, provides interesting insights into existing challenges and advocates future research through highlighting the most important research directions to make 6G dependable.**

***Index Terms*—6G networks; AI; Edge; Dependability; Mission-critical applications; Security**

I. Introduction

Mission-critical applications (MCAs) are software essential to a certain business that need to continuously function in order to succeed. They have stringent QoS (Quality of Service) requirements in terms of bandwidth, reliability, and latency, that existing 5G networks will have challenges to provide. Future 6G networks are expected to revolutionize communications networks by offering extreme network capabilities that satisfy the demands of a wide variety of use cases, among them those of MCAs. The evolution of 6G will focus on a new set of requirements like Further enhanced Mobile Broadband (FeMBB), ultra-massive Machine Type Communications (umMTC), and massive Low-Latency Machine Type Communications (mLLMT). These requirements are supported by the use of technologies such as Federated Learning (FL) [1], edge AI [2], Distributed Ledger Technologies (DLT) [3], and 3D networking, among others [4]. The highly distributed architecture of AI-based 6G networks pose a challenging scenario for dependability, since AI applications are usually not easy to test and conventional methodologies do not always apply. Furthermore, as AI applications become ubiquitous in communication networks, their complexity increases as well, escalating the importance of dependability on AI software aiming at 6G networks. From the systems engineering perspective, dependability is a measure associated with four well-known concepts: reliability, availability, security, safety [5], [6].

Reliability is the probability of a system working correctly for a certain period of time. As 6G networks will be highly distributed, the main concern regarding reliability is effectively coordinating the computing nodes. In order to achieve this, successful communication protocols between those computing nodes are needed, as well as a reliable underlying network [7]. ***Availability*** refers to the probability of a system working properly at any given time. Distributed AI solutions for 6G networks are an attractive option for improving learning time while reducing resource consumption, thus improving availability of AI-based systems and services. ***Security*** refers to capacity of a system for protecting itself, the services deployed on the systems and data exchanged among the components and users of the system. In the case of 6G network services, distributed AI algorithms are needed to train models locally, in order to preserve the end user information. Finally, ***safety*** refers to the ability of a system to avoid harming human life, the environment, or even properties. Since 6G networks will leverage use cases such as autonomous driving, it is in our interest to analyze the role of AI in such a situation.

In this work we study the dependability of 6G networks from the four dimension, i.e., reliability, availability, safety, and security. We also analyze how the distributed nature of 6G networks negatively affect their dependability. Furthermore, we dive into the role of distributed AI techniques and distributed mission-critical applications that are currently used in the intelligentization of the network. 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 briefly discusses the concept of dependability. Section 3 discusses dependability in 6G networks. Section 4 briefly introduces the AI techniques expected to be deployed in 6G edge, as well as their effect on dependability. Section 5 provides interesting insights into the relation between dependability of MCAs in 6G. Interesting future research directions are summarized in Section 6 and the article is concluded in Section 7.

II. Dependability

Dependability is the ability of a system to deliver a service that can justifiably be trusted, in other words, avoiding frequent and severe service failures [8]. Though crucial in importance, dependability is often down-looked 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 [9], [10]. Moreover, there are many of facets of dependability, for instance, also including confidentiality and integrity [11].

However, some of the concepts converge into the four aspects discussed throughout this article. Therefore, for brevity we keep the discussion under the topics of reliability, availability, safety and security, as described below.

A. Reliability

The complexity of distributed Edge networks means that achieving reliability in such an environment is not an easy task. With the increasing amount of mission-critical applications solutions in 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, fault tolerance, to mention some. In [5], the authors briefly explore reliability issues in Edge AI systems, as well as propose an architecture that meet latency and reliability requirements for many mission-critical applications. It is identified that computation on edge systems occur in three different layers: bottom (end devices), middle (servers), and top layer (centralized cloud). In order to achieve a good communication and fast response, all three layers must be properly synchronized, the same as the storing and data access for processing [12].

B. Availability

Availability is realized once reliability has been achieved, since reliability is the probability of the system 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 [13]. 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 even capable of performing the offloading based on network statistics and the edge servers computation capabilities. Other 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 cause 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 varying degree of each.

C. 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 [14], 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 single fault condition. However, this definition can be broadened to cover non-medical domains, thus including faulty conditions such as wrong lane selection in autonomous driving, or task offloading failure affecting the information given to the end user an 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 [15]. In [16], and [17], telesurgery safety considerations from the medical point of view are given, it also mentions their experience with different surgical robots and elaborate some comparisons.

D. Security

Security in one of the main issues in communication networks, as both nodes and the whole network are targeted by threats [18], [19]. The distributed and data driven 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 machine learning in communications networks are increasing at higher pace due to apparent reasons [20], however, AI and machine learning also bring its own security challenges in communications networks, as elaborated in [21], [22]. The most important part is to identify the required level of security for a certain use case, and adopt the principles of security-by-design approach. These concepts are quite important due to the diverse nature of 6G mission-critical applications. Furthermore, the rise in the number of capable attackers targeting communication networks call for stringent security requirements. In [23], the authors explore the application of Blockchain (BC) technology alongside ML in order to protect vehicular networks from cyber attacks. Similarly, in [24] the authors use 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.

III. 6G and Dependability

The fast development of multimedia applications for use cases such as high-fidelity holograms, tactile Internet, and the support of mission-critical applications require a higher bandwidth than that offered by the current 5G communication networks [25]. 6G networks are bound to be large-scale, heterogeneous, complex, and dynamic; with heavily-distributed storage and computation capabilities available from the cloud, edge servers, and end devices [26]. For the transition from 5G to 6G, changes are not only required in bandwidth, but also from physical layer (PHY) to the higher layers to meet the new requirements of emerging services, for instance in the Internet of Everything (IoE). Furthermore, 6G networks are expected to achieve data rates in the range of terabits per second (Tbps), thanks to the developments in terahertz communications, improvements in massive MIMO and beamforming, and novel coding schemes. A successful combination of these next-generation wireless networks with cloud/edge platforms is vital, where increased network intelligence can be realized leveraging on bringing cloud platforms closer to the sources of data. Edge intelligence, thus opens new horizons in achieving and exploiting the full potential 6G networks.

Since the first generation (1G), communication networks have increased their complexity while expanding both horizontally and vertically, thus rendering them difficult to manage. Furthermore, along with the complexity the security threat landscape has also increased constantly [19]. Edge computing can play an important role in addressing both of these challenges, i.e., complexity and security. By devolving control into multiple control units, compared to centralized ones, security through redundancy increases as a general phenomenon. For instance, the chance of single points of failure, and a single target for denial of service (DoS) and resource exhaustion attacks become highly complicated. Furthermore, edge computing plays a vital role in 6G communication networks as it provides the computing resources necessary for carrying out management and analysis close to end-user devices [27].

Fast and focused data processing through edge computing is the cornerstone of applications in 6G, for example in V2X communications [28], whereas in-depth data analysis could be carried out by the centralized cloud at the expense of delays [29]. Fig. 1 shows a sample architecture of an AI-based 6G network, which is hierarchically divided into three layers: intelligence, data analytics, and sensing. In the top layer, or intelligence layer, functions like parameter optimization, resource management, and task scheduling are carried out. In the data analytics layer some of the tasks performed are data filtering, knowledge discovery, and feature extraction. Finally, the sensing layer is where 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 on a primary analysis, prior to passing it 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 [30], transforming it into a AI-based platform capable of offering intelligent services [31]. In order to achieve this, research have departed from the centralized cloud-based approach, sparkling an interest in distributed, low-latency, and reliable AI at the edge [32], [33].

Moreover, EdgeAI is drawing an increasing attention and its development is closely aligned with that of reliability in communications and end device constraints, allowing for the deployment of a network whose operation resembles that of a distributed computer being 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.

A. Dependability in 6G networks

In this part we analyze the dependability of future 6G networks from the perspective of their distributed and data-driven nature. Concepts like EdgeAI help reduce latency between the end devices and edge servers, but at the same time, they might be a point of failure and security attacks if the weaknesses are not conceived properly before deployment. Below we discuss the dependability of 6G networks from the four dimensions, i.e., reliability, availability, safety and security from the perspectives of EdgeAI.

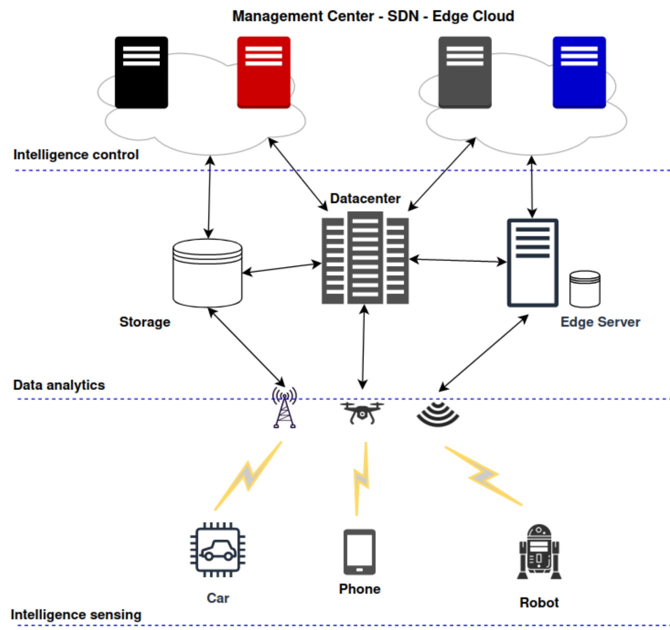

Fig. 1. Architecture of a AI-enabled 6G network.

1) Reliability: 6G networks are expected to offer extremely high reliability and EdgeAI supports the vision of 6G through offering more computational power near users or services while reducing overall latency. Reliability requires checking the necessary assumptions instead of assuming that these are fulfilled and constantly monitoring the network [34]. Although in terms of performance EdgeAI supposes a step forward, its distributed nature combined with the high number of servers required, might as well introduce other issues. First we have asynchronism, as the number of edge server 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 necessary. Another issue is the heterogeneity of software and hardware at the nodes, although it brings benefits in the long run, the adoption of heterogeneous solutions might as well pose challenges. As an example, heterogeneous EdgeAI servers might have different power consumption and performance due to non-identical CPU architectures. In the same manner, distinct feature support could hinder synchronism. Scalability could as well be a problem for networks as it increases complexity of management, and it might as well create issues with synchronism. As 6G networks will be highly scalable, fault tolerance is also important in order to ensure reliability. As a system scales to be hundreds of nodes in size, a fault tolerant system will enable the operations or services to continue at a reduced level, not stopping completely.

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 [35]. As mentioned in section II, 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 neighbor server. This is where synchronism plays a major role and in order to achieve this, servers must be aware of the each other status. Furthermore, predictive analysis of available resources in neighbouring edge nodes for performing certain tasks to ensure that the available resources are capable to perform the intended task, as discussed in [22] will be important. 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 availability of critical resources [36]. Although highly related, it must be noted that a system with high availability is not necessarily reliable, thus achieving the expected high reliability of 6G networks does not guarantee meeting the availability criteria.

3) Safety: Safety and security, looking intertwined, are highly complicated in terms of defining its role in communications networks. Safety, also defined similarly in [37], is a system's characteristic that can prevent 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 including also related to security, which are discussed in the following security part. Besides 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, play 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 edge, as discussed in [38], 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 [39], [40] 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 proximities, as well as security vulnerabilities and attacks which is discussed below.

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 [41]. Quantum communications are also expected to make significant contribution in 6G networks, mainly from the perspectives of communications security, such as quantum and post quantum cryptography [42]. 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 [43]. Visible light communication (VLC) can improve wireless communications as it offers high bandwidth and is immune to electromagnetic interference. Moreover, VLC faces threats coming from attackers that are capable of positioning themselves within line-of-sight of the target. Physical security is also important as the nodes of a highly distributed network can be easily targeted by malicious users and damaged as part of a cyberattack [38]. EdgeAI can help provide timely monitoring and response procedures, such as intrusion detection and prevention systems (IDS/IPS), deployed in the vicinity where the threat originates [19]. Moreover, machine learning techniques [20] such as federated learning that enable the applications of AI in a distributed manner, as in the case of EdgeAI, can enable predict and deploy security procedures before a security attack or incident happens. Therefore, in the following section we discuss the application of federated learning in 6G networks.

IV. Machine Learning, Dependability, and 6G

AI and its major branch, ML, will shape 6G networks [20], [26]. Thanks to its tight Quality of Service (QoS) requirements, future 6G networks will posses such a complex architecture that performing legacy network operations will be deemed as unsound. Because of this, ML techniques are emerging as a response to achieve truly intelligent orchestration and network management [44]. The dynamic nature of communication networks provide data for ML-enabled spectrum management and channel estimation, which are the basis of ultra-broadband techniques. Also, ML is being used to improve security, resource allocation, mobility management, and low latency services in MCAs [20]. Distributed ML will be highly important in 6G due to the emerging needs of distributed processing at the edges of the network [45]. Federated learning is currently among the most used distributed ML techniques in communication networks [46], and highly important for 6G due to its capability to be used in distributed manner, much like the the foreseen distributed control nature of 6G networks.

A. Background in Brief

Federated learning (FL) [47] was conceived by Google researchers back in 2016. Since then, it has experienced a 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, aiming at building a privacy-preserving ML framework by keeping all raw data on devices and aggregating local model updates, while also reducing communications overhead. FL process is conformed by several communication rounds between a server and the clients, performed in the following fashion [1], [48]:

- 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 (SGD), a determined number of mini-batch steps and several epochs are performed in order to increase the update quality and reduce communications cost.
- When the training is done, clients send their updates towards the server. It is important noticing that some clients might drop out due to connectivity issues or lack of processing power, etc. Nevertheless, the round continues with the received updates. In case there are too many dropped out clients, the current round is abandoned.
- The server receives the updates, weights them based on their training set size, and finally aggregates them. A new model is built at the server, and the next round begins.

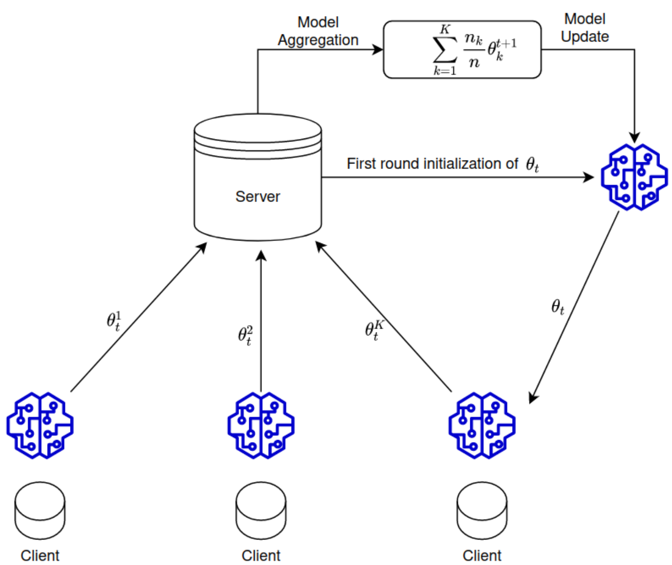

Fig. 2. Simplified Federated learning flowchart

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

B. Dependability of Federated Learning

As one of the most popular ML techniques, FL has been used and its processes are adopted to a wide range of use cases ranging from resource optimization to task offloading, and physical layer to the application layer. In this subsection we analyze the dependability of FL with regard to its process, focusing on its algorithm rather than its applications in certain use cases.

1) Reliability: ML techniques rely heavily on data, its quality is fundamental for achieving a high accuracy during the learning task. Client selection is a critical issue in FL, as clients are the one 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 on a random manner, or either based on resource conditions, this of course might affect the global performance as untrustable nodes are selected. Moreover, the complexity of conceiving client selection in a communications network due to its dynamic nature also hinders their reliability, and even further, as it is difficult for the centralized entity that performs the selection to actually monitor a large-scale behavior, the selected untrustable clients are unlikely to be removed. Also, since the FL process consists of several rounds, previously selected untrustable clients might as well be selected for future rounds, further damaging the learning accuracy. Similarly, security vulnerabilities and lapses can also affect reliability.

2) Availability: A lack, or improper criteria when selecting the clients for local training does not only affects reliability, but availability as well. Untrusted clients using low quality data for training hinder the whole learning process, with the possibility of severely affecting prediction. In this manner, a FL framework whose accuracy is not as desired, cannot be deployed nor services can trust it, thus 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 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 numeral 4.

3) Safety: Damage done by the selection of untrusted clients go 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, which according to the use case might pose danger to users involved. 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 decision of other vehicles, putting at risk the passengers lives. The problem only exacerbates considering the centralization issue raised in the previous subsection, where weak aggregation algorithms do not help discriminating good from bad trained models.

4) Security: Security is an important challenge in ML [21]. 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. Also, a malicious client could as well launch attacks alongside other malicious users aimed at increasing miss-classification. 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. Communications channel vulnerability also affects FL frameworks, as the learning process consists of several rounds, a unencrypted channel will render the locally trained model vulnerable for attackers to perform reconstruction attacks.

V. Dependability for Mission-critical Applications in 6G

One of the primary focus of 6G networks will be MCAs. These applications usually require dependable services in terms of latency and error rates, and due to their nature, this must be equivalent to wired networks. MACs requirements are closely related to those of Ultra-Reliable Low-Latency Communications (URLLC) with a target latency of 0.1ms and a Block Error Rate (BLER) of 10^{-9}. Although these KPI values are not applicable to all use cases, they do have practical relevance in a couple of them, we could mention autonomous driving, remote surgery, and augmented reality [49]. Needless to say, mission critical applications also mandate high security communications, and resource efficiency. Current 5G networks approaches for meeting the requirements of MCAs based on tweaking the system design is not scalable nor efficient, future 6G network need to make use of application-domain information in order to predict actual resource requirements. Furthermore, 6G networks need to introduce new parameters that will not only help characterizing resource needs, but will as well ease dependability analysis [50].

Due to its performance, edge computing is gaining terrain as a viable solution for meeting the requirements of MCAs. The drivers behind the adoption of edge computing in MCAs use cases are the amount of data being transferred between end devices and edge servers, and time of data processing at the edge server. Due to the proximity of the edge server to the source of data, the network requirements mentioned at the beginning of this subsection could be met, even in the scenario of a massive amount of data. Furthermore, edge intelligentization eases meeting these requirements as it is capable of offering micro-interaction with end devices, bringing management much closer to them thus reducing communications overhead due to data fetching, and controlling [20].

A. Mission-critical applications use cases

This section will focus on briefly introducing and surveying three specific use cases that are in high demand for automated solutions: telesurgery, autonomous driving, and augmented reality. Considered an emergent surgical system, telesurgery is the use of wireless networking and robotics that allow surgeons to operate patients located distantly. Among its benefits we can mention the capacity to offer surgery on unserved locations, and enabling collaboration between surgeons from different medical centers. The most important requirement for telesurgery systems is latency, in [51], Wirz et. al. determined the ideal latency for telesurgery systems to be 100 milisenconds or less, while presenting feasibility study for trans-sphenoidal resection of a pituitary tumor where a latency of 10 miliseconds was achieved. The work in [52] presents a drone-assisted telesurgery system that makes use of blockchain and 6G networks to become trusted, and ultra-responsive. The authors favoured an analysis on performance for the AI techniques used to classified diseases, and a cost analysis for the blockchain, dependability is not studied in this case. In [53], the authors introduced a 6G, blockchain-based scheme for telesurgery that aims at being intelligent, and efficient from the latency, throughput, and storage point of view. Although dependability is not directly mentioned, the authors do study the security, and safety of the framework, as well as the reliability of the underlying 6G network, no availability analysis was performed. The importance of security, a dimension of dependability, in remote healthcare enabled by existing and future communication networks, such as 5G and future 6G, is thoroughly studied in [54]. The authors conclude that without proper security in place, remote healthcare will be rather detrimental than beneficial. This makes dependability of communications networks highly important for such critical use case. Dependability must not be considered as an add-on, but used as a benchmark from the basic initial design stage, which should be revisited during the working stages and must be continuously improved.

Autonomous driving technology refers to self-driving cars which are capable of sensing the environment and safely move without human intervention. Self-driving cars set up is quite complex, usually comprising cameras, laser scanners, radars, laser beams, and a inertial measurement unit. Furthermore, autonomous driving represent the convergence of intelligent wireless sensing, communication, computing and caching [28], [55]. In this work we will focus on EdgeAI, which represents the computation and communication part of this use case as it allows self-driving cars to accurately sense their surroundings and timely react thanks to data offloading from the vehicles to the edge servers. In [56], the authors introduce a framework for EdgeAI-powered autonomous driving that achieves near-real-time task offloading while preserving privacy, and reducing communication delay. Also, reliability is explored as the inference accuracy, security is enhanced through local training, and safety is analyzed as a crucial element that depends on the offloading and inferring time window as well as feasible sensing. The work in [57], satisfies the QoS requirements of future vehicular networks through the use of idle resources from parked cars. The authors also successfully simulated user density as way to predict resources availability, and demonstrated a reduction in deployment costs. However, the paper does not discuss dependability or any of its components. The works in [58], [59], [60], and [61] investigate the improvement of dependability in vehicular networks, however none of them clearly defines nor exposes all the factors that affect dependability.

Finally, we have augmented reality, which is the enhancement of object thanks to computer-generated information. Augmented reality applications are fast becoming attractive in mobile or smart wereable devices, especially because of their ability to enhance the visualization of the environment. The authors in [62] researched task offloading in mobile augmented reality applications, and used 6G network characteristics on their simulations. Due to latency being of the major concerns in augmented reality applications, the authors focus on transmission and application latency during their experimental analysis, dependability nor any of its components was taken into account. In [63], a metrology-oriented, automatic system based on augmented reality reality was designed in order to help surgeons during operations. The authors aimed at achieving transmission dependability, which was verified based on the accuracy and latency of the system. Nevertheless, no description of dependability or its components was provided, also, the work focuses mainly on reliability. The work in [64] aims at increasing the reliability of augmented reality applications by lowering the probability of communication and computation errors, as well as timeouts. Latency and accuracy are balanced thanks to an optimization problem that minimizes failure probability, the other concepts associated to dependability are not explored. Other works such as [65], and [66] also explore certain aspects of dependability.

B. *Dependability analysis of 6G Mission-critical Applications*

Based on the information from the previous section, MCAs are expected to be extremely dependable. Not only due to their stringent network requirements but also because of their use cases. A lack of dependability in a MCA could badly harm operations at a production factory, or potentially place human lives at risk.

1) Reliability: Reliability of a MCA is directly related to how well it complies with the stringent requirements in terms of latency and errors, from one point of view these requirements are met with the help of capable underlying networks. However, reliability is also affected by the architecture chosen for a given MCA, since it will determine the overall behavior and qualities if such an application. From the 6G perspective, the importance given to software architecture is nowhere near that of the underlying network, of course a capable network greatly benefits an application performance, but a proper architecture further improves these benefits. Focus should also be given to use case-specific hardware, as an MCA will depend on their quality and trustability as many use cases revolve around their use, such as telesurgery.

2) Availability: Bad architecture and low quality hardware can as well affect the availability of a MCA. As many use cases such as telesurgery or autonomous driving depend on external hardware (like sensors, or CPS components) it is important to ensure that these are trustable and will not hinder the execution of the MCA. Moreover, a proper architecture, in the form of resource localization, would ensure the MCA is capable of deploying high capacity node replacements, thus offering an adequate scalability. Depending on the use case, some MCAs might use EdgeAI approaches for improving their bandwidth and latency requirements, proper resource and task allocation are needed in order to take advantage of these scenarios.

3) Safety: Reliability and availability of MCAs have a direct relationship with safety, especially in use cases that involve direct human contact. Since MCAs are usually the backbones of their respective use cases, if failing then the consequences can go from vast economical losses to putting human lives at danger. As an example, in an autonomous driving scenario, if the vehicle is not capable of properly perform computations that help it determine whether or not to change lanes, the risk of an accident and as extension human losses are high. In this aspect, MCAs need to re-focus, becoming more autonomous, so human operators are less involved, and thus less prone to be affected in case of faulty behavior. Also, a distributed architecture would benefit MCAs since it increases their availability and reliability, making it easier to update or make changes to the application.

4) Security: MCAs are constantly targeted by malicious attackers either due to the importance of the data they handle, or because of their key role in some industrial or medical use cases. If not properly secured, attackers targeting a remote surgery system could execute commands that hinder the performance of the controlled devices, severely threatening human lives. Moreover, other scenarios such as autonomous driving are also susceptible to malicious attacks that could hinder many of the systems running on the vehicle, from communication devices, to sensors and other integral parts of its systems. Although security aspects rely mostly on the underlying communication network, it is also worth noting that MCAs could provide some security aspects such as controlling inter-element communications, or defining which element can access what information in the system.

VI. Future Research Directions

6G networks will be highly distributed in nature. Network control will be shifted to far edge nodes, such as micro-edge [38], which may arise with new terminologies and technologies. Since centralized control will not be suitable for latency critical services, distribution of network management and control functions will be inevitable. However, such distribution will complicate the dependability of future networks. The challenges to dependability will be from many dimensions. For example, reliable network function or service transfer from a centralized cloud infrastructure to far edge or user node will be challenging and require more research in terms of resource discovery alongside reliable function or service transfer. The distributed control, apparently, can can increase the availability. However, such control functions can also be targeted by security attacks such as denial of service (DoS) attacks and resource exhaustion attacks to block access to legitimate users. The success of such attacks usually depend on availability of resources at the receiving ends of the attack. Hence, distributed network control functions into small units may decrease the overall dependability.

The resilience of the networks also must increase, which requires proper resilience strategies. Network resilience means that a network operates in the presence of difference challenges such as security attacks, operational mistakes, configuration errors or equipment failures [67]. This will require network mechanisms that are capable to protect the network from failures through flexible means of configurations, cooperative techniques that enable network devices and segments to provide alternative routes, and efficient anomaly detection and

TABLE I
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.

traffic shaping techniques. The notion of network abstraction and simplicity of control put forward by the concepts of Software Defined Networking (SDN) [68] can really help in this direction, for instance in run-time mobility of traffic [69], traffic management [70], or load-balancing among congested nodes [71]. Whether the technologies of SDN will prevail in 6G or not, research will show, however, the concepts and philosophy of SDN can surely help in increasing dependability of 6G networks, and thus, must be researched further.

Safety and security are highly intertwined. For example, if an equipment is not physically safe, it cannot be considered as secure. Similarly, if a device can be compromised through cyber attacks, its physical security can be meaningless in most use-cases. Safety must be research from the technical perspectives to have key performance indicators for safety much like security. We do have security-by-design but safety-by-design is rarely discussed. The security in 6G is highly complicated. New technologies are emerging and it is possible that security requirements of different technology do not match, for instance in the debate of privacy vs accountability. Furthermore, the more the network control becomes distributed and modular, the more the security of the whole eco-system comprising of diverse services, users and even network functions, will become complicated. Dependability, therefore, will be highly complicated to comprehend and must be researched from this perspective. One of the key questions in this regard will be to take an evolutionary incremental approach, based on existing 5G standards or a revolutionary approach and start thinking of redesigning from scratch.

Since AI will be used on much higher scale than 5G, the real threats that AI can pose will also become inevitable. Therefore, research is needed on sustainable AI-based security approaches for AI-based security threats in 6G. One way ahead in ensuring dependable 6G networks is to maintaining simplicity in design with global visibility of network resources and its use, and enabling programmable deployment of services, including security functions, in reliable, safe and secure manner. The main challenges that need further research in this direction are also summarized in Table I along with possible research directions.

VII. CONCLUSIONS

Dependability is an important feature of communications networks and has always been increasing in importance with the evolution of communications networks. The main reason behind this increasing importance is the step-by-step integration of digital technologies into important aspects of our lives through communication networks. V2X and digital healthcare services, for instance, will require a highly dependable network. Since 6G exacerbates the merger of the physical and digital worlds beyond the current traditional cyber-physical systems, dependability in terms of reliability, availability, safety and security will need a thorough investigation. Therefore, in this article we have shed light on dependability of 6G networks mainly to highlight its importance and relevance in 6G. Furthermore, we have highlighted important challenges to stir further debate and research in this direction.

REFERENCES

[1] S. AbdulRahman, H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi, and M. Guizani, "A survey on federated learning: The journey from centralized to distributed on-site learning and beyond," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5476–5497, 2021.

[2] E. Peltonen, M. Bennis, M. Capobianco, M. Debbah, A. Ding, F. Gil-Castiñeira, M. Jurmu, T. Karvonen, M. Kelanti, A. Kliks *et al.*, "6G white paper on edge intelligence," *arXiv preprint arXiv:2004.14850*, 2020.

[3] R. Sekaran, R. Patan, A. Raveendran, F. Al-Turjman, M. Ramachandran, and L. Mostarda, "Survival study on blockchain based 6G-enabled mobile edge computation for IoT automation," *IEEE Access*, vol. 8, pp. 143 453–143 463, 2020.

[4] S. J. Nawaz, S. K. Sharma, B. Mansoor, M. N. Patwary, and N. M. Khan, "Non-coherent and backscatter communications: Enabling ultra-massive connectivity in 6G wireless networks," *IEEE Access*, vol. 9, pp. 38 144–38 186, 2021.

[5] R. Gupta, D. Reebadiya, and S. Tanwar, "6g-enabled edge intelligence for ultra -reliable low latency applications: Vision and mission," *Computer Standards & Interfaces*, vol. 77, p. 103521, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0920548921000167

[6] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, "In-edge AI: Intelligentizing mobile edge computing, caching and communication by federated learning," *IEEE Network*, vol. 33, no. 5, pp. 156–165, 2019.

[7] W. Ahmed and Y. W. Wu, "A survey on reliability in distributed systems," *Journal of Computer and System Sciences*, vol. 79, no. 8, pp. 1243–1255, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0022000013000652

[8] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, 2004.

[9] D. I. Heimann, N. Mittal, and K. S. Trivedi, "Dependability modeling for computer systems," in *Annual Reliability and Maintainability Symposium. 1991 Proceedings*. IEEE, 1991, pp. 120–128.

[10] D. Chen, S. Garg, C. M. Kintala, and K. S. Trivedi, "Dependability enhancement for IEEE 802.11 wireless LAN with redundancy techniques." in *DSN*, 2003, pp. 521–528.

[11] J.-C. Laprie, "Dependable computing: Concepts, limits, challenges," in *Special issue of the 25th international symposium on fault-tolerant computing*. Citeseer, 1995, pp. 42–54.

[12] A. Waseem and W. W. Yong, "A survey on reliability in distributed systems," *Journal of Computer and System Sciences*, vol. 79, no. 8, pp. 1243–1255, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0022000013000652

[13] I. Ahmad and S. Namal and M. Ylianttila and A. Gurtov, "Security in Software Defined Networks: A Survey," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2317–2346, Fourthquarter 2015.

[14] Medical electrical equipment - part 1: General requirements for basic safety and essential performance. [Online]. Available: https://webstore.iec.ch/publication/2603

[15] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber–physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 283–299, 2012.

[16] R. J., Y. B., L. S., F. Y., and W. Lew, "Anesthetic implications of robotically assisted surgery with the Da Vinci Xi surgical robot," *Open Journal of Anesthesiology*, vol. 6, pp. 115–118, 2016.

[17] L. J. Rim, "Anesthetic considerations for robotic surgery," *Korean J Anesthesiol*, vol. 66, no. 1, pp. 3–11, 2014. [Online]. Available: http://ekja.org/journal/view.php?number=7850

[18] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[19] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and Beyond," *IEEE Communications Surveys Tutorials*, vol. 21, no. 4, pp. 3682–3722, Fourthquarter 2019.

[20] I. Ahmad, S. Shahabuddin, H. Malik, E. Harjula, T. Leppänen, L. Lovén, A. Anttonen, A. H. Sodhro, M. Mahtab Alam, M. Juntti, A. Ylä-Jääski, T. Sauter, A. Gurtov, M. Ylianttila, and J. Riekki, "Machine learning meets communication networks: Current trends and future challenges," *IEEE Access*, vol. 8, pp. 223 418–223 460, 2020.

[21] J. Suomalainen, A. Juhola, S. Shahabuddin, A. Mämmelä, and I. Ahmad, "Machine learning threatens 5G security," *IEEE Access*, vol. 8, pp. 190 822–190 842, 2020.

[22] I. Ahmad, S. Shahabuddin, T. Sauter, E. Harjula, T. Kumar, M. Meisel, M. Juntti, and M. Ylianttila, "The challenges of artificial intelligence in wireless networks for the internet of things: Exploring opportunities for growth," *IEEE Industrial Electronics Magazine*, vol. 15, no. 1, pp. 16–29, 2020.

[23] M. Dibaei, X. Zheng, Y. Xia, X. Xu, A. Jolfaei, A. K. Bashir, U. Tariq, D. Yu, and A. V. Vasilakos, "Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–18, 2021.

[24] Y. Hui, N. Cheng, Z. Su, Y. Huang, P. Zhao, T. H. Luan, and C. Li, "Secure and personalized edge computing services in 6G heterogeneous vehicular networks," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[25] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, 2020.

[26] F. Tariq, M. R. A. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A Speculative Study on 6G," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 118–125, 2020.

[27] Q.-V. Pham, F. Fang, V. N. Ha, M. J. Piran, M. Le, L. B. Le, W.-J. Hwang, and Z. Ding, "A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art," *IEEE Access*, vol. 8, pp. 116 974–117 017, 2020.

[28] D. P. M. Osorio, I. Ahmad, J. D. V. Sánchez, A. Gurtov, J. Scholliers, M. Kutila, and P. Porambage, "Towards 6G-enabled Internet of Vehicles: Security and Privacy," *IEEE Open Journal of the Communications Society*, pp. 1–1, 2022.

[29] J. Okwuibe, J. Haavisto, I. Kovacevic, E. Harjula, I. Ahmad, J. Islam, and M. Ylianttila, "SDN-Enabled Resource Orchestration for Industrial IoT in Collaborative Edge-Cloud Networks," *IEEE Access*, vol. 9, pp. 115 839–115 854, 2021.

[30] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge intelligence: Paving the last mile of artificial intelligence with edge computing," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1738–1762, 2019.

[31] S. Deng, H. Zhao, W. Fang, J. Yin, S. Dustdar, and A. Y. Zomaya, "Edge intelligence: The confluence of edge computing and artificial intelligence," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7457–7469, 2020.

[32] C. Li, W. Guo, S. C. Sun, S. Al-Rubaye, and A. Tsourdos, "Trustworthy deep learning in 6G-enabled mass autonomy: From concept to quality-of-trust key performance indicators," *IEEE Vehicular Technology Magazine*, vol. 15, no. 4, pp. 112–121, 2020.

[33] E. Harjula, P. Karhula, J. Islam, T. Leppänen, A. Manzoor, M. Liyanage, J. Chauhan, T. Kumar, I. Ahmad, and M. Ylianttila, "Decentralized IoT edge nanoservice architecture for future gadget-free computing," *IEEE Access*, vol. 7, pp. 119 856–119 872, 2019.

[34] M. Herlich and C. Maier, "Measuring and monitoring reliability of wireless networks," *IEEE Communications Magazine*, vol. 59, no. 1, pp. 76–81, 2021.

[35] R. Bhagwan, S. Savage, and G. M. Voelker, "Understanding availability," in *International Workshop on Peer-to-Peer Systems*. Springer, 2003, pp. 256–267.

[36] I. Ahmad, S. N. Karunarathna, M. Ylianttila, and A. Gurtov, "Load balancing in software defined mobile networks," *Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture*, pp. 225–245, 2015.

[37] W. Young and N. G. Leveson, "An integrated approach to safety and security based on systems theory," *Communications of the ACM*, vol. 57, no. 2, pp. 31–35, 2014.

[38] I. Ahmad, S. Lembo, F. Rodriguez, S. Mehnert, and M. Vehkaperä, "Security of Micro MEC in 6G: A Brief Overviewing," in *2022 IEEE 19th Annual Consumer Communications Networking Conference (CCNC)*, 2022, pp. 332–337.

[39] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, J. Querol, L. Lei, T. X. Vu, and G. Goussetis, "Satellite communications in the new space era: A survey and future challenges," *IEEE Communications Surveys Tutorials*, vol. 23, no. 1, pp. 70–109, 2021.

[40] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6G," *IEEE Communications Surveys Tutorials*, vol. 24, no. 1, pp. 53–87, 2022.

[41] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, 2018.

[42] F. Song, "A note on quantum security for post-quantum cryptography," in *International Workshop on Post-Quantum Cryptography*. Springer, 2014, pp. 246–265.

[43] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, W. H. Alshoura, and H. Arshad, "The internet of things security: A survey encompassing unexplored areas and new insights," *Computers & Security*, vol. 112, p. 102494, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821003187

[44] L. U. Khan, S. R. Pandey, N. H. Tran, W. Saad, Z. Han, M. N. H. Nguyen, and C. S. Hong, "Federated learning for edge networks: Resource optimization and incentive mechanism," *IEEE Communications Magazine*, vol. 58, no. 10, pp. 88–93, 2020.

[45] C. Mwase, Y. Jin, T. Westerlund, H. Tenhunen, and Z. Zou, "Communication-efficient distributed AI strategies for the IoT edge," *Future Generation Computer Systems*, vol. 131, pp. 292–308, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X22000218

[46] Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang, and D. Niyato, "Federated learning for 6G communications: Challenges, methods, and future directions," *China Communications*, vol. 17, no. 9, pp. 105–118, 2020.

[47] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings *et al.*, "Advances and open problems in federated learning," *Foundations and Trends® in Machine Learning*, vol. 14, no. 1–2, pp. 1–210, 2021.

[48] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020.

[49] N. H. Mahmood, S. Böcker, A. Munari, F. Clazzer, I. Moerman, K. Mikhaylov, O. L. A. López, O. Park, E. Mercier, H. Bartz, R. Jäntti, R. Pragada, Y. Ma, E. Annanperä, C. Wietfeld, M. Andraud, G. Liva, Y. Chen, E. Garro, F. Burkhardt, H. Alves, C. Liu, Y. Sadi, J. Dore, E. Kim, J. Shin, G. Y. Park, S. Kim, C. Yoon, K. Anwar, and P. Seppänen, "White paper on critical and massive machine

type communication towards 6G," *CoRR*, vol. abs/2004.14146, 2020. [Online]. Available: https://arxiv.org/abs/2004.14146

[50] C. She, R. Dong, Z. Gu, Z. Hou, Y. Li, W. Hardjawana, C. Yang, L. Song, and B. Vucetic, "Deep learning for ultra-reliable and low-latency communications in 6G networks," *IEEE Network*, vol. 34, no. 5, pp. 219–225, 2020.

[51] R. Wirz, L. G. Torres, P. J. Swaney, H. Gilbert, R. Alterovitz, R. J. Webster, K. D. Weaver, and P. T. Russell, "An experimental feasibility study on robotic endonasal telesurgery," *Neurosurgery*, no. 3, pp. 479 – 484, 2015.

[52] R. Gupta, A. Shukla, and S. Tanwar, "BATS: A blockchain and AI-empowered drone-assisted telesurgery system towards 6G," *IEEE Transactions on Network Science and Engineering*, pp. 1–1, 2020.

[53] R. Gupta, U. Thakker, S. Tanwar, M. S. Obaidat, and K.-F. Hsiao, "BITS: A blockchain-driven intelligent scheme for telesurgery system," in *2020 International Conference on Computer, Information and Telecommunication Systems (CITS)*, 2020, pp. 1–5.

[54] I. Ahmad, Z. Asghar, T. Kumar, G. Li, A. Manzoor, K. Mikhaylov, S. A. Shah, M. Höyhtyä, J. Reponen, J. Huusko, and E. Harjula, "Emerging technologies for next generation remote health care and assisted living," *IEEE Access*, vol. 10, pp. 56 094–56 132, 2022.

[55] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 957–975, 2020.

[56] B. Yang, X. Cao, K. Xiong, C. Yuen, Y. L. Guan, S. Leng, L. Qian, and Z. Han, "Edge intelligence for autonomous driving in 6G wireless system: Design challenges and solutions," *IEEE Wireless Communications*, vol. 28, no. 2, pp. 40–47, 2021.

[57] W. Qi, Q. Li, Q. Song, L. Guo, and A. Jamalipour, "Extensive edge intelligence for future vehicular networks in 6G," *IEEE Wireless Communications*, vol. 28, no. 4, pp. 128–135, 2021.

[58] J. Almeida, J. Rufino, M. Alam, and J. Ferreira, "A survey on fault tolerance techniques for wireless vehicular networks," *Electronics*, vol. 8, no. 11, 2019. [Online]. Available: https://www.mdpi.com/2079-9292/8/11/1358

[59] Z. Zhou, H. Yu, C. Xu, Y. Zhang, S. Mumtaz, and J. Rodriguez, "Dependable content distribution in d2d-based cooperative vehicular networks: A big data-integrated coalition game approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 3, pp. 953–964, 2018.

[60] A. Boukerche, B. Kantarci, and C. Kaptan, "Towards ensuring the reliability and dependability of vehicular crowd-sensing data in GPS-less location tracking," *Pervasive and Mobile Computing*, vol. 68, p. 101248, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574119220300973

[61] F. O. Olowononi, D. B. Rawat, and C. Liu, "Dependable adaptive mobility in vehicular networks for resilient mobile cyber physical systems," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2020, pp. 1–6.

[62] K. Chakrabarti, "Deep learning based offloading for mobile augmented reality application in 6G," *Computers & Electrical Engineering*, vol. 95, p. 107381, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790621003505

[63] P. Arpaia, E. De Benedetto, C. A. Dodaro, L. Duraccio, and G. Servillo, "Metrology-based design of a wearable augmented reality system for monitoring patient's vitals in real time," *IEEE Sensors Journal*, vol. 21, no. 9, pp. 11 176–11 183, 2021.

[64] J. Liu and Q. Zhang, "Code-partitioning offloading schemes in mobile edge computing for augmented reality," *IEEE Access*, vol. 7, pp. 11 222–11 236, 2019.

[65] X. Zhang, R. Slavin, X. Wang, and J. Niu, "Privacy assurance for android augmented reality apps," in *2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC)*, 2019, pp. 114–1141.

[66] S. S. Bahaei, B. Gallina, K. Laumann, and M. R. Skogstad, "Effect of augmented reality on faults leading to human failures in socio-technical systems¡sup¿*¡/sup¿," in *2019 4th International Conference on System Reliability and Safety (ICSRS)*, 2019, pp. 236–245.

[67] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[68] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," *IEEE Communications surveys & tutorials*, vol. 16, no. 3, pp. 1617–1634, 2014.

[69] S. Namal, I. Ahmad, A. Gurtov, and M. Ylianttila, "Enabling secure mobility with OpenFlow," in *2013 IEEE SDN for Future Networks and Services (SDN4FNS)*. IEEE, 2013, pp. 1–5.

[70] I. Ahmad, M. Liyanage, S. Namal, M. Ylianttila, A. Gurtov, M. Eckert, T. Bauschert, Z. Faigl, L. Bokor, E. Saygun *et al.*, "New concepts for traffic, resource and mobility management in software-defined mobile networks," in *2016 12th Annual conference on wireless on-demand network systems and services (WONS)*. IEEE, 2016, pp. 1–8.

[71] S. Namal, I. Ahmad, A. Gurtov, and M. Ylianttila, "SDN based inter-technology load balancing leveraged by flow admission control," in *2013 IEEE SDN for future networks and services (SDN4FNS)*. IEEE, 2013, pp. 1–5.