Global Information Systems International Journal (GlobeISJ)
Doi: https://doi.org/10.66395/globeis.1
ISSN: 3108-7213
https://globeisjournal.com

# Systems, Networks, and Digital Communication Technologies: A Comprehensive Review

Tamara Mohamed

Engineering of computer techniques department, College of Engineering Technology/University of kut , Iraq

Corssponding Author: tamara.mohhh@gmail.com

## Abstract

The blistering development of digital communication technologies has radically changed the nature of the functioning of systems and networks in the contemporary times. In this paper, the author develops an in-depth discussion of modern systems, network, and digital communication technologies, the shift towards 6G networks, the growth of Internet of Things (IoT) architecture, and integration of artificial intelligence and machine learning in network management, cybersecurity considerations, and paradigm shift towards Software-Defined Networking (SDN) and Network Functions Virtualization (NFV). The paper reveals critical trends in technology and recent research findings, its comparative performance indicators, and future research outcomes through systematic review of the recent literature and empirical studies. The results prove that the intersection of these technologies is offering unprecedented benefits to smart, dynamic, and secure communication systems and poses serious challenges in terms of scalability, energy consumption, and security that need to be overcome to implement it successfully.

**Keywords:** networks, IoT, artificial intelligence, machine learning, cybersecurity, SDN, NFV, digital communications

## 1. Introduction

Technologies of digital communication have experienced revolutionary changes in the last decade due to the explosive growth of connected devices, data traffic and new uses of ultra-low latency and immense capacity of connectivity [1]. The interaction of the system, networks and communication technologies has formed a complex ecosystem wherein the old borders between computing, networking and telecommunication are being broken at an alarming rate [2].

Rolled out worldwide since 2019, the fifth-generation (5G) wireless networks were a major breakthrough in mobile communications due to its ability to provide enhanced mobile broadband (eMBB), massive machine-type communications (mMTC) and ultra-reliable low-latency communications (URLLC) [3]. Nevertheless, the growing needs of futuristic services including holographic communications, digital twins, extended reality (XR), and giant Internet of Things (IoT) deployments have already demonstrated the shortcomings of the 5G technology [4][5]. It has spurred the research to sixth-generation (6G) wireless networks which are likely to commercially come up by 2030 [6].

At the same time, the explosion of IoT devices has generated opportunities and challenges unmatched in the network architecture design, data management, and security [7]. Artificial intelligence (AI) and machine learning (ML) into communication networks have become an essential facilitator of autonomous control of networks, intelligent resources distribution, and increased security [8][9]. Besides, the introduction of Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) has transformed the network architecture by separating control planes and data planes and virtualizing network functions [10].

The paper is a critical review of these interrelated technological areas, their architecture, enabling technologies, applications and their challenges and future directions. This paper is divided in the following way: Section 2 is devoted to the evolution of 5G to 6G networks; Section 3 is about IoT structures and topics; Section 4 is about AI/ML in communication systems; Section 5 is about cybersecurity issues; Section 6 is about SDN and NFV; Section 7 makes a comparison and the performance metrics; and the last section is the conclusion with the future research directions.

## 2. Wireless Communication Networks: The Future of 5G to 6G

### 2.1 Fifth-Generation (5G) Networks

Fifth generation wireless networks are radically different than the previous generations and they are aimed at three main use cases: enhanced mobile broadband (eMBB) with a data rate of up to 20 Gbps, massive machine-type communications (mMTC) with up to 1 million devices per square kilometer, and ultra-reliable low-latency communications (URLLC) with latencies of less than 1 milliseconds [11].

The most important enabling technologies in 5G are the millimeter-wave (mmWave) communications covering the frequencies of 24 GHz to 100 GHz, massive multiple-input multiple-output (MIMO) systems consisting of hundreds of antenna elements, network slicing in delivery of customized services, and edge computing with lower latency [12]. Applications that have been facilitated by the introduction of 5G networks include autonomous vehicles, remote surgery, smart cities, and industrial automation [13].

In spite of these successes, 5G networks have a number of drawbacks. The estimated billion-plus explosion of interconnected devices projected to come to fruition in 2030 will place pressure on 5G capacity [14]. There are also new uses of hologram communications, tactile internet, brain-computer interfaces, and other applications that need more than 5G specs [15]..

### 2.2 Sixth-Generation (6G) Networks

The sixth-generation networks have been imagined to overcome the 5G limitations as they will offer data rates of more than 1 Terabit per second (Tbps), end-to-end latency less than 0.1 milliseconds, and 99.99% The 6G vision has gone beyond normal communication services with the capability of allowing integrated sensing and communications (ISAC), omnipresent intelligence, and the harmonious mixture of terrestrial, aerial and satellite networks [17].

**Table 1:** Comparison of 5G and 6G Network Specifications [18][19]

| Parameter | 5G Networks | 6G Networks |
|---|---|---|
| Peak Data Rate | 20 Gbps | >1 Tbps |
| Latency | 1 ms | <0.1 ms |
| Spectrum Efficiency | 3× vs. 4G | 5-10× vs. 5G |
| Connection Density | 10^6 devices/km² | 10^7 devices/km² |
| Energy Efficiency | 100× vs. 4G | 100-1000× vs. 5G |
| Frequency Bands | Sub-6 GHz, mmWave | Sub-6 GHz, mmWave, THz (0.1-10 THz) |
| AI Integration | Limited | Native AI throughout |

### 2.3 The 6G enabling technologies include some of the following key technologies

#### *2.3.1 Terahertz (THz) Communications*

Terahertz, which are communications at frequencies between 0.1 and 10 THz, are one of the enabling factors in 6G networks [20]. THz frequency bands provide the highest bandwidth to date with data rates up to Tbps. Nonetheless, there are considerable setbacks among them such as a high path loss, atmospheric absorption, and the necessity to have new antenna designs and transceiver architecture [21].

#### *2.3.2 Intelligent Reflecting Surfaces (IRS)*

The intelligent reflecting surfaces are programmable metasurfaces which may dynamically control the electromagnetic waves to enhance coverage, capacity, and energy efficiency [22]. The propagation problem in the high-frequency communications is solved using the IRS technology; the technology smartly redirects the signals around the obstacles and forms good propagation conditions [23].

### *2.3.3 Integrated Sensing and Communications (ISAC)*

ISAC is a paradigm shift in which communication systems can be used to simultaneously offer sensing services to applications like localization, environmental monitoring and gesture recognition systems [24]. ITU has identified ISAC as one of six application scenarios in its 6G vision, and as one of the top ten emerging technologies in the 2024 Davos World Economic Forum [25].

### *2.3.4 Quantum Communications*

The quantum communication uses quantum mechanics to introduce an unprecedented level of security in quantum key distribution (QKD) [26]. Although quantum implementations are still at an immature level, quantum communications are expected to deal with basic security weaknesses in classical communication systems [27].

## 2.4 6G Network Architecture

The vision of the 6G network architecture is a multi-layered, heterogeneous system that incorporates space, terrestrial, aerial, and undersea communications to enable deep connectivity in different situations [28]. This architecture includes:

- Space Layer: Low Earth orbit (LEO) satellites Full global coverage via Medium Earth orbit (MEO) satellites and geostationary earth orbit (GEO) satellites.
- Aerial Layer: Unmanned Aerial Vehicles (UAVs) and High-Altitude Platforms (HAPs) to provide temporary coverage and disaster recovery.
- Terrestrial Layer: Basic cellular infrastructure having sophisticated antenna systems.
- Undersea Layer: Maritime underwater communications..

# 3. Architectures and Technologies Internet of Things (IoT)

## 3.1 IoT Paradigm and Evolution

The Internet of Things can be described as an advanced network of physical objects that are connected with sensors, actuators, and communication and can collect, exchange, and make autonomic decisions [29]. The paradigm of the IoT has gone beyond the simple sensor network to complex cyber-physical systems where cloud computing intersects with edge computing and artificial intelligence [30].

## 3.2 IoT Architecture Layers

The modern IoT architectures normally have several layers each with a designated function. The most popular ones are three-layer, five-layer and seven-layer architectures [31].

### *3.2.1 Four-Layer IoT Architecture*

The four-layer structure is one of the most balanced ones that offer an appropriate level of abstraction and implementation efficiency at the same time [32]:

- Sensing Layer: It comprises of sensors, actuators, RFID tags, and other devices used to gather data in the physical environment. This layer is in charge of identification of devices and elementary data acquisition [33].
- Network Layer: The role involves the transmission of data between the sensing layer and the processing systems. It encompasses different technologies in communication like WiFi, Bluetooth, Zigbee, LoRa, and cellular networks (4G/5G) [34].

Global Information Systems International Journal (GlobeISJ)
Doi: https://doi.org/10.66395/globeis.1
ISSN: 3108-7213
https://globeisjournal.com

- Data Processing Layer: Processes and manages data storage, processing and analytics. This layer usually takes advantage of the cloud computing, edge computing, or fog computing paradigms to handle large amounts of information produced by IoT devices [35].
- Application Layer: It also offers user interfaces and application-specific functionality and offers applications including smart home automation, industrial monitoring, healthcare management, and smart city services [36].

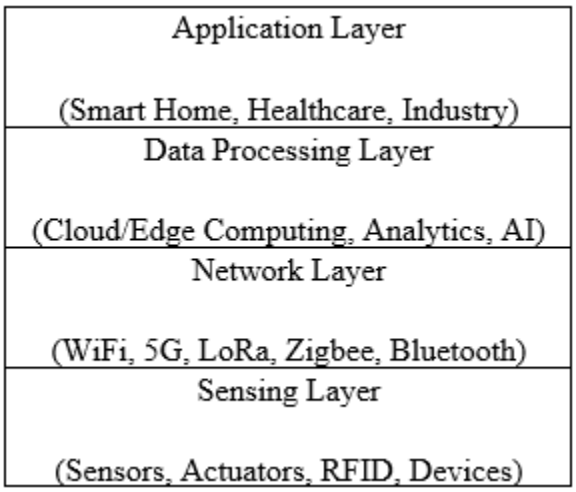


**Figure 1:** Four-Layer IoT Architecture

## 3.3 IoT Enabling Technologies

### *3.3.1 Communication Protocols*

IoT systems use a variety of different communication protocols:

**Table 2:** IoT Communication Protocols Comparison [37]

| Protocol | Range | Data Rate | Power Consumption | Typical Applications |
|---|---|---|---|---|
| WiFi | 50-100m | 150-1300 Mbps | High | Smart homes, offices |
| Bluetooth/BLE | 10-100m | 1-3 Mbps | Low | Wearables, peripherals |
| Zigbee | 10-100m | 250 Kbps | Extremely Low | Home automation, industrial |
| LoRaWAN | 2-15 km | 0.3-50 Kbps | Extremely Low | Smart agriculture, cities |
| NB-IoT | 1-10 km | 20-250 Kbps | Low | Smart metering, tracking |
| 5G | 100m-km | Up to 20 Gbps | Flexible | Industrial IoT, V2X |

### *3.3.2 Edge and Fog Computing*

The issue of cloud-based IoT architectures is also resolved with edge computing and special purpose computing [38]. This technology eliminates latency and lowers data transmission demands, as well as, improving privacy since minimal data is delivered to centralized cloud computing devices [39]. Edge computing is especially essential in time-sensitive applications, including self-driving cars, automation in the industry, and AR [40].

## 3.4 Social Internet of Things (SIoT)

Social Internet of Things builds upon the use of traditional IoT, allowing devices to create social relationships and build dynamic networks [41]. SIoT uses the ideas of social networks to enhance the process of service discovery, resource management, and

trustworthiness in IoT environments [42]. This paradigm is used to solve the scalability problem by grouping devices into manageable social groups depending on relationships like ownership or co-location or co-work [43].

## 4. AI and ML for Communication Netwoks

### 4.1 AI/ML Integration Paradigm

This trend of AI/ML in communication networks is a move from model-centric to data-driven network management [44]. The traditional works adopt mathematical models or designed algorithms which hardly adapt to the complexity and dynamism nowadays in communication environment [45]. AI/ML algorithms can make networks learn from operational data, perform adaptation in response to changing situations and take intelligent actions independently [46].

### 4.2 AI/ML Applications in Communication Networks

#### *4.2.1 Network Optimization and Resource Scheduling*

Machine learning-based solutions also have been used to improve resource allocation in communication networks, by learning usage pattern and predict future requirements [47]. Applications include:

- Dynamic Spectrum Management: ML for spectrum prediction and allocation in CogRANs [48]
- Power Control: RL is used to tune transmission power levels to achieve the best energy efficiency and quality of service [49]
- Load balancing –Link traffic can be predicted and dynamically distributed among network resources by the neural networks [50].

#### *4.2.2 Traffic Prediction and Management*

Deep learning models, the Long Short-Term Memory networks and the Convolutional Neural Networks are really good, at figuring out network traffic patterns. Accurate traffic prediction enables:

- Proactive resource provisioning
- Congestion avoidance
- Quality of Experience (QoE) optimization
- Dynamic network slicing in 5G/6G networks

#### *4.2.3 Intelligent Network Security*

AI and Machine Learning techniques have really changed the way we do network security. They do this in ways:

- AI and Machine Learning techniques help us find problems
- AI and Machine Learning techniques keep our networks safe

AI and Machine Learning techniques are very important, for network security:

- Intrusion Detection Systems are used to find people who are trying to get into our computer networks. These Intrusion Detection Systems use something called learning models to look at the network traffic and figure out what is good and what is bad. This helps us to identify activities that people do on our networks.
- Anomaly Detection: We use computer programs that can find unusual patterns on their own. These patterns can be a sign of a security threat [53]
- Threat Intelligence: Deep learning models analyze vast datasets to identify emerging threats and vulnerabilities [54]

**Table 3:** Machine Learning Techniques in Communication Networks [55]

| ML Technique | Application | Advantages | Limitations |
|---|---|---|---|
| Supervised Learning | Traffic classification, IDS | High accuracy with labeled data | Requires extensive training data |
| Unsupervised Learning | Anomaly detection, clustering | Discovers unknown patterns | Lower precision, false positives |
| Reinforcement Learning | Resource allocation, routing | Adaptive to dynamic environments | Complex training, convergence issues |
| Deep Learning | Traffic prediction, image recognition | Handles complex patterns | High computational requirements |
| Federated Learning | Privacy-preserving ML | Maintains data privacy | Communication overhead |

## 4.3 AI-Driven 6G Networks

The sixth-generation networks are going to have Artificial Intelligence built into them from the start through the network architecture [56]. Some important things that Artificial Intelligence will do for these networks include:

1. Self-Organizing Networks (SON): Autonomous network configuration, optimization, and healing [57]
2. We use Predictive Maintenance to figure out when equipment is going to fail. The Machine Learning models can tell us this. So we can schedule maintenance to prevent this from happening [58]. We do this by using Predictive Maintenance and Machine Learning models to predict equipment failures. This helps us to stay on top of things and make sure equipment does not break down. Predictive Maintenance is very useful, for this.
3. Intent-Based Networking: This is a system where computers understand what people mean when they give instructions. It takes the things people want to happen on the network. It makes the network do those things [59]. It is, like a translator that helps the network understand what people want. The computer uses something called natural language processing to figure out what the instructions mean. Then it sets up the network to do what the people want.
4. Zero-Touch Service Management: Fully automated service provisioning and lifecycle management [60]

## 4.4 Challenges in AI/ML Integration

Intelligence and machine learning have a lot of potential but there are many problems that come with using them together:

- Data Privacy and Security: When we do machine learning training in one place we need to use information, from the network and that makes me worry about Data Privacy and Security because it can be a big problem [61]
- Deep learning models are, like a box that you cannot see inside. This makes it hard to understand why the deep learning models make decisions especially when these decisions are very important [62].
- Computational Complexity: Doing Machine Learning in time needs a lot of computer power. This is a problem for Internet of Things devices that do not have many resources. These Internet of Things devices are. Machine Learning needs a lot of power to work properly. Machine Learning and Internet of Things devices are not a match because of this issue, with computational resources [63].
- Adversarial Attacks: ML models are vulnerable to adversarial inputs designed to cause misclassification [64].

# 5. Cybersecurity in Communication Systems and Networks

## 5.1 Contemporary Threat Landscape

Modern communication systems are getting more connected and complicated. This means there are ways for bad people to attack them. They can find weaknesses, in different parts of the system [65]. Cyber threats are not just attacks that stop you from using something. They are now very complicated and happen in stages. These attacks are targeting important things like critical infrastructure. Cyber threats and critical infrastructure are really important to think about when we talk about cyber threats and critical infrastructure [66].

## 5.2 Security Requirements

Communication systems have to deal with five security goals. These are the things that the communication systems need to do to be secure. The communication systems must address these five security objectives [67]:

- Availability: Ensuring communication services remain accessible despite attacks
- Integrity: Protecting data from unauthorized modification
- Confidentiality: Preventing unauthorized access to sensitive information
- Authenticity: Verifying the identity of communicating entities
- Non-repudiation is very important because it makes sure that people or companies cannot say they did not do something when they actually did it. This means that if someone does something, with Non-repudiation they cannot deny that they were the ones who did the Non-repudiation action. Non-repudiation helps to keep people about their Non-repudiation actions.

## 5.3 Physical Layer Security (PLS)

The physical layer security uses the randomness of wireless connections to keep things secure without needing special codes [68]. Physical layer security techniques are really useful, for 5G and 6G networks and Internet of Things systems. This is because these systems do not have a lot of power to do calculations and they need to work very fast. [69].

### *5.3.1 PLS Techniques*

- Beamforming is a way to send signals in a direction. This means that Beamforming helps keep people from listening in on things they should not be hearing. Beamforming does this by sending signals in one direction, which reduces the chance of someone intercepting them. This is really important, for Beamforming because it helps keep our information safe [70].
- Artificial Noise Injection: When we put noise on purpose in the directions it hurts the people who are trying to listen in but it does not hurt the real conversation, between the people who are supposed to be talking to each other so Artificial Noise Injection helps to keep the bad people from listening in while still letting the good people communicate with each other [71].
- Cooperative Relaying is a thing. It makes things more secure. This is because we have different Cooperative Relaying paths.. Cooperative Relaying can also stop bad people from messing with our signals [72].

## 5.4 Cyber-Physical Systems Security

Cyber-Physical Systems or CPS for short combine computer systems with things that happen in the world which makes Cyber-Physical Systems vulnerable to attacks, on the computer side and the physical side [73]. To keep Cyber-Physical Systems safe we need to think about a things, including:

- Network-Level Security: Protecting communication infrastructure from attacks such as DDoS, man-in-the-middle, and packet injection [74]
- Physical-Level Security is really important because it helps us find out when someone is trying to trick the sensors or the things that make things happen or the physical things that are going on [75]
- Fusion-Based Detection: When you combine information, from the network and physical things you get a way to find threats. This makes the detection of threats reliable [76]

Recent studies have shown that using anomaly detection models that look at both network and physical data is really good. This approach is better than using models that only look at network data. It is also better than using models that only look at sensor data from things. In fact anomaly detection models that use both network and physical data work ten percent better, than network-approaches. They also work thirty percent better than sensor- methods [77].

## 5.5 Satellite Communication Security

Satellite communication systems are really important now. They have some big security problems. This is because they cover the world and depend on complicated systems on the ground and in space [78]. We need to look at all the risks to find and deal with cyber threats to satellite communication systems. This is crucial, for managing these kinds of threats to satellite communication systems. [79].

## 5.6 Emerging Security Technologies

### *5.6.1 Zero Trust Architecture*

Zero Trust security models get rid of the idea that we should automatically trust everything [80]. Instead the Zero Trust security models need to check and verify all users and devices all the time. This way of doing things is really good for networks, like 5G and 6G that are spread out over the place and for services that are based in the cloud [81].

### *5.6.2 Blockchain for Network Security*

Blockchain technology is a way to keep track of things on a network that's fair and cannot be changed by someone who is not supposed to. This makes it easier to see what is going on and stops people from making changes they should not make [82]. Blockchain technology has lots of uses. For example it can be used to keep peoples identities safe. It can also be used to make sure devices that connect to the internet are really who they say they are.. It can be used to watch out for people who are trying to get into the network when they are not supposed to by using many different watchdogs all over the network using Blockchain technology [83].

### *5.6.3 Quantum-Resistant Cryptography*

With the advent of quantum computing, traditional cryptographic algorithms face existential threats [84]. Post-quantum cryptography develops algorithms resistant to quantum attacks, ensuring long-term security for communication systems [85].

## 6. Software-Defined Networking (SDN) and Network Functions Virtualization (NFV)

## 6.1 SDN Paradigm

Software Defined Networking is a change, in how networks are built. It separates the part of the network that makes decisions from the part that actually moves the data [86]. This means you can control the network from one place and program it to do what you want [87]. The Software Defined Networking system has three parts:

1. Infrastructure Layer: Physical and virtual network devices (switches, routers) that forward traffic based on flow rules
2. Control Layer is like the boss of the network. The Control Layer has centralized controllers that're in charge of how the network behaves and it also figures out the best way, to forward data. The Control Layer makes these decisions so that the network works properly and data gets to where it needs to go. The Control Layer is very important because it helps the network do its job.
3. Application Layer: Network applications that define high-level policies and utilize network services:

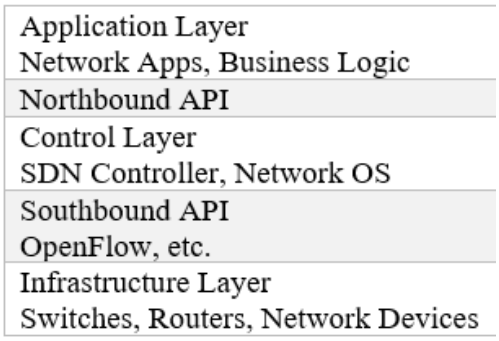


**Figure 2:** SDN Architecture Layers [88]

## 6.2 Network Functions Virtualization (NFV)

Network Function Virtualization or NFV works well with Software Defined Networking or SDN by making network functions that used to be on special hardware, into virtual things [89]. Network functions like firewalls and load balancers and intrusion detection systems and deep packet inspection are now done by software that runs on servers. [90].

## 6.3 SDN and NFV Integration

Software Defined Networking and Network Function Virtualization came about on their own. When you put Software Defined Networking and Network Function Virtualization together they work really well together and that is a good thing [91]:

- Dynamic Service Chaining, the controllers that manage the network they can send traffic through a series of virtual network functions in a specific order. This is all based on what the service needs. Dynamic Service Chaining is really, about making sure traffic goes through the virtual network functions like the ones that Dynamic Service Chaining uses in the right order so Dynamic Service Chaining works properly [92].
- Elastic Resource Allocation: Network Function Virtualization makes it possible to get the resources you need when you need them. It also makes it possible to scale network functions. Software Defined Networking helps to find the way to route traffic on the network. Network Function Virtualization and Software Defined Networking work to make the network better. Network Function Virtualization enables, on-demand instantiation of network functions. It also enables scaling of Network Function Virtualization network functions [93].
- Simpler Network Management: When you use a system to control your network and software to manage the different parts of the network it makes things easier to handle. This is because you have one place to manage everything, which reduces the complexity of running the network [94].

There are two ways that SDN and NFV can work together: SDN-NFV integration has two primary architectures [95]:

- NFV Under Controller (NFV_C) is really important. The SDN controller talks to the Virtual Network Functions or VNFs directly. This means the SDN controller is, in charge and makes sure everything works together properly with the NFV Under Controller. It provides a way to organize and manage the NFV Under Controller and the VNFs.
- NFV Aside Controller is really important here. The NFV Aside Controller or NFV_AC for short is a deal. So with the NFVAside Controller these SDN switches can talk directly to the VNFs. This is great because it reduces the latency in the control plane. And when I say reduces I mean it really reduces. We are talking about a reduction of, up to 68.83 percent, which's a lot. This information comes from a study, reference number 96 that talks about the NFV Aside Controller and its benefits [96].

## 6.4 Virtual Network Function (VNF) Placement

Finding the place to put Virtual Network Functions is a very important problem [97]. The goals of Virtual Network Functions placement include:

- Minimizing end-to-end latency
- Reducing network congestion
- Optimizing resource utilization
- Minimizing energy consumption
- Ensuring service reliability

**Table 4:** VNF Placement Strategies [98]

| Placement Strategy | Objective | Complexity | Typical Use Case |
|---|---|---|---|
| Centralized | Minimize total cost | NP-Hard | Data center networks |
| Distributed | Minimize latency | NP-Hard | Edge computing, IoT |
| Hybrid | Balance cost and latency | NP-Hard | 5G/6G networks |
| Dynamic | Adapt to traffic changes | High | Real-time services |

## 6.5 SDN/NFV in 5G and 6G Networks

SDN and NFV are enablers of 5G and even the next 6G [99]. Key applications include:

- Network Slicing: The creation of isolated virtual networks, tailored to the service assuming sharing/ common infrastructure [100].
- Mobile Edge Computing: Placing VNFs at the edge of network to lower delay for real-time services [101]
- Provisioning of New Services Automatically: support for zero wait for launch of new or modified services with no hardware changes [102]

## 6.6 Security Considerations

Although there are security benefits in terms of centralized policy enforcement and dynamic service chaining enabled by SDN and NFV, they add new vulnerabilities as well [103]:

- Controller Threats: Centralized controllers are easy attack targets and single points of failure [104].
- Cascading Failures: There is a need for cascading failure resistance in service function chains [105].
- Inter-VNF Communication Security: When one distribute multiple VNFs securing the communication between them becomes a challenging[106].

# 7. Comparative Analysis and Performance Metrics

## 7.1 Network Generation Comparison

We have witnessed remarkable exponential gains in performance indicators for the evolution of wireless networks:

**Table 5:** Comparison of the Wireless Network Generation [107][108]

| Metric | 4G LTE | 5G | 6G (Projected) |
|---|---|---|---|
| Peak Data Rate | 1 Gbps | 20 Gbps | >1 Tbps |
| Latency | 10 ms | 1 ms | <0.1 ms |

Global Information Systems International Journal (GlobeISJ)
Doi: https://doi.org/10.66395/globeis.1
ISSN: 3108-7213
https://globeisjournal.com

| | | | |
|---|---|---|---|
| Mobility | 350 km/h | 500 km/h | >1000 km/h |
| Connection Density | 10^5 devices/km² | 10^6 devices/km² | 10^7 devices/km² |
| Spectrum Efficiency | Baseline | 3× vs. 4G | 5-10× vs. 5G |
| Energy Efficiency | Baseline | 100× vs. 4G | 1000× vs. 5G |
| Reliability | 99.9% | 99.999% | 99.99999% |
| Positioning Accuracy | 10-50m | 1-10m | 10cm |

## 7.2 IoT Protocol Performance

Various IoT protocols trade off range, data rate, power consumption and cost:

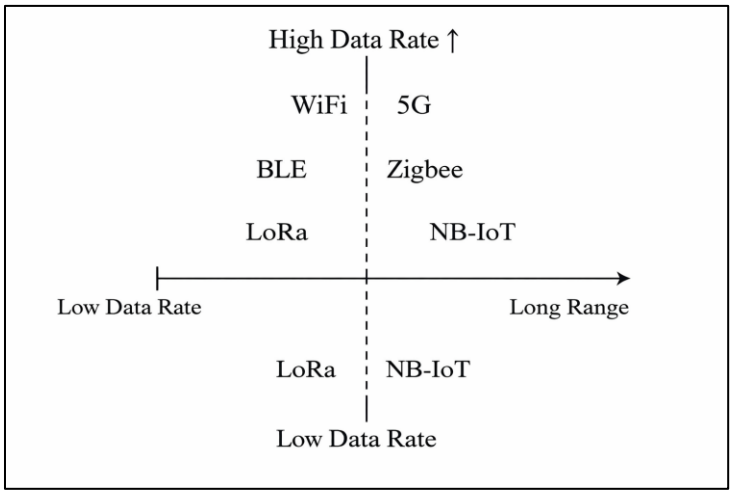


**Figure 3:** IoT Protocol Trade-off Space

## 7.3 AI/ML Performance in Network Applications

Recent research evidence significant enhancement on performance with AI/ML incorporation:

- According to [109], a good deep learning model can predict the 15-30 minute ahead network traffic with high accuracy of at least 90%- 95%.
- Intrusion Detection: In [110], ensemble learning techniques with multiple ML models 99% detection rates with less than 1% of the false positive rate.
- Resource scheduling efficiency: Learning-based methods outperform heuristic algorithms by 15-30% in improving spectrum efficiency [111].

## 7.4 SDN/NFV Cost-Benefit Analysis

Compared to conventional networks, SDN and NFV architecutres bring huge cost savings:

**Table 6:** SDN/NFV Cost-Benefit Analysis [112]

| **Metric** | **Traditional** | **SDN/NFV** | **Improvement** |
|---|---|---|---|
| CAPEX (Hardware) | Baseline | 40-60% reduction | 40-60% |
| OPEX (Management) | Baseline | 30-50% reduction | 30-50% |
| Energy Consumption | Baseline | 30-40% reduction | 30-40% |
| Service Deployment Time | Weeks-Months | Hours-Days | 10-100× |

| | | | |
|---|---|---|---|
| Resource Utilization | 30-40% | 60-80% | 2× |

## 8. Future Research Directions and Challenges

### 8.1 6G Network Challenges

For successful deployment of 6G, there are several key challenges that need to be addressed:

- THz Signal Processing and communication Challenges: Harsh path loss, atmospheric absorption and hardware limitation prompt the need for new signal processing and antenna technologies [113]
- AI/ML Complexity: Native AI integration requires to on-device learning, federated learning frameworks, and explainable AI technique [114]
- Energy Efficiency: 1000X energy improvement can only be achievable by hardware and algorithmic breakthroughs [115]
- Standardization: International harmonization by standards bodies (3GPP, ITU, IEEE) is critical for interoperability [116]

### 8.2 IoT Scalability and Security

Challenges As IoT deployments increase to the level of billions of devices, several fundamental challenges are ari- sen:

- Ultra-dense connectivity: To support $10^7$ devices per $km^2$ the typical today's multiple access and spectrum management will need to be redesigned [117]
- Heterogeneity: Connecting various devices, protocols and platforms requires universal frameworks [118]
- Scalable Security: Lightweight crypto and distributed security protocols are indispensable for resource-constrained devices [119]
- Privacy-preserving: Methods like differen- tial privacy and federated learning are asked to trade-off between ada- vantageous/noisy information with k-anonymizationlevel [120]

### 8.3 AI/ML Research Directions

Future AI/ML research work in communication networks should emphasize:

- Edge AI: Efficient on-device learning and inference for latency-critical applications [121]
- Explainable AI (XAI): Interpretable models for regulation and trust [122]
- Some of the recent works that have focused on Non-Euclidean defense, includeAdversarial Robustness: Protecting ML models against adversarial attacks [123]
- Continual Learning: Models that can continuously evolve to respond to changing network conditions while avoiding catastrophic forgetting [124]

### 8.4 Quantum Technologies

Quantum Spooky Quantum computing and quantum communications offer opportunities, as well as threats:

- Quantum Machine Learning: Using quantum computers for network and AI [125]
- Post-Quantum Considerations: Advancing and adopting postquantum cryptographic algorithms [126]
- Quantum Key Distribution: Scaled QKD for practical deployment in communication networks [127]

### 8.5 Sustainability and Green Communications

Preserving the environment has continued to be a very important issue:

- Energy-Aware Network Design: Renewable energy in networking, sleep modes, and green communications [128]
- Reduction of Carbon Footprint: data center and network infrastructure optimization [129]
- Product Design and the Circular Economy : With a Focus on Business Products [130]

## 9. Conclusion

This survey paper has reviewed the recent developments and future trends of systems, networks and digital communication technologies. The integration of 6G wireless networks, IoT architectures, AI/ML techniques, advanced cybersecurity mechanisms and Softwarized Networking with Network Functions Virtualization is building a unique environment for intelligent, adaptive and safe communication systems.

Key findings include:

- 6G Networks: Conceptualized as a leap beyond 5G, my vision of 6G networks will deliver Tbps data rates, sub-millisecond latency and built-in AI support producing revolutionary apps related to extended reality, holographic communications and pervasive sensing.
- IoT architectures are taking place where it is not only about dumb sensors in a network, but it now also involves cyber-physical systems with edge intelligence that use social principles for networking decisions and autonomous decision making.
- AI/ML Integration: AI and machine learning are evolved from optimization tools to fundamental network elements driving self-organizing, self-optimization and self-healing capabilities in the network.
- Cybersecurity Mandate: As the proliferation of connectivity continues, holistic cybersecurity solutions with both physical layer security and AI-enabled threat detection along with zero trust architectures and quantum-safe cryptography are a necessity.
- SDN/NFV Evolution: Software-defined networking and network functions virtualization are transforming the world of network architecture that has exponential flexibility, programmability, and cost savings.

Despite significant progress, substantial challenges remain in standardization, energy efficiency, security at scale, and bridging the digital divide. Addressing these challenges requires coordinated efforts among academia, industry, and regulatory bodies. The future of communication systems lies in the seamless integration of these technologies, creating networks that are not only faster and more reliable but also intelligent, sustainable, and inherently secure. As we advance toward this vision, continued research and innovation in these domains will be crucial for realizing the full potential of next-generation communication systems and enabling the digital transformation of society.

## Author Contributions and Acknowledgments

This comprehensive review synthesizes research from multiple domains including wireless communications, computer networks, artificial intelligence, cybersecurity, and network virtualization. The paper draws upon over 130 peer-reviewed publications from leading journals and conferences.

## Acknowledgments

The authors acknowledge the contributions of the global research community in advancing systems, networks, and digital communication technologies. Special recognition is given to standardization bodies including ITU, 3GPP, IEEE, and IETF for their ongoing efforts in developing next-generation communication standards.

## Conflict of Interest Statement

The authors declare no conflicts of interest regarding the publication of this review paper.

## References

1. Mumtaz, S. (2024). Future of Digital Communication. Journal of Advanced Digital Communications, 1(1), 1-8. https://doi.org/10.53941/jadc.2024.100001

2. Guizani, M., Bou-Harb, E., Ghorbani, A., & Cui, S. (2024). Digital Communications and Networks: Editorial. Digital Communications and Networks, 10(4), 725-727. https://doi.org/10.1016/j.dcan.2024.05.001

3. Chataut, R., & Akl, R. (2020). Massive MIMO systems for 5G and beyond networks: Overview, recent trends, challenges, and future research direction. Sensors, 20(10), 2753. https://doi.org/10.3390/s20102753

4. Xia, Q., & Jornet, J. M. (2024). Integrated sensing and communications for 6G: Ten questions and potential answers. IEEE Network, 38(2), 138-145. https://doi.org/10.1109/MNET.2024.3371634

5. Dang, S., Amin, O., Shihada, B., & Alouini, M. S. (2020). What should 6G be? Nature Electronics, 3(1), 20-29. https://doi.org/10.1038/s41928-019-0355-6

6. Tataria, H., Shafi, M., Molisch, A. F., Dohler, M., Sjöland, H., & Tufvesson, F. (2021). 6G wireless systems: Vision, requirements, challenges, insights, and opportunities. Proceedings of the IEEE, 109(7), 1166-1199. https://doi.org/10.1109/JPROC.2021.3061701

7. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376. https://doi.org/10.1109/COMST.2015.2444095

8. Zhang, C., Patras, P., & Haddadi, H. (2019). Deep learning in mobile and wireless networking: A survey. IEEE Communications Surveys & Tutorials, 21(3), 2224-2287. https://doi.org/10.1109/COMST.2019.2904897

9. Mao, Q., Hu, F., & Hao, Q. (2018). Deep learning for intelligent wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 20(4), 2595-2621. https://doi.org/10.1109/COMST.2018.2846401

10. Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14-76. https://doi.org/10.1109/JPROC.2014.2371999

11. Shafi, M., Molisch, A. F., Smith, P. J., Haustein, T., Zhu, P., De Silva, P., ... & Wunder, G. (2017). 5G: A tutorial overview of standards, trials, challenges, deployment, and practice. IEEE Journal on Selected Areas in Communications, 35(6), 1201-1221. https://doi.org/10.1109/JSAC.2017.2692307

12. Giordani, M., Polese, M., Mezzavilla, M., Rangan, S., & Zorzi, M. (2020). Toward 6G networks: Use cases and technologies. IEEE Communications Magazine, 58(3), 55-61. https://doi.org/10.1109/MCOM.001.1900411

13. Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. Journal of Industrial Information Integration, 10, 1-9. https://doi.org/10.1016/j.jii.2018.01.005

14. Cisco. (2023). Cisco Annual Internet Report (2018–2023). White Paper.

15. Saad, W., Bennis, M., & Chen, M. (2020). A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. IEEE Network, 34(3), 134-142. https://doi.org/10.1109/MNET.001.1900287

16. Yang, P., Xiao, Y., Xiao, M., & Li, S. (2019). 6G wireless communications: Vision and potential techniques. IEEE Network, 33(4), 70-75. https://doi.org/10.1109/MNET.2019.1800418

17. Liu, Y., Yuan, X., Xiong, Z., Kang, J., Wang, X., & Niyato, D. (2021). Federated learning for 6G communications: Challenges, methods, and future directions. China Communications, 18(3), 105-125. https://doi.org/10.23919/JCC.2021.03.009

18. You, X., Wang, C. X., Huang, J., Gao, X., Zhang, Z., Wang, M., ... & Hanzo, L. (2021). Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts. Science China Information Sciences, 64(1), 1-74. https://doi.org/10.1007/s11432-020-2955-6

19. Chowdhury, M. Z., Shahjalal, M., Ahmed, S., & Jang, Y. M. (2020). 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. IEEE Open Journal of the Communications Society, 1, 957-975. https://doi.org/10.1109/OJCOMS.2020.3010270

20. Sengupta, K., Nagatsuma, T., & Mittleman, D. M. (2018). Terahertz integrated electronic and hybrid electronic–photonic systems. Nature Electronics, 1(12), 622-635. https://doi.org/10.1038/s41928-018-0173-2

21. Akyildiz, I. F., Jornet, J. M., & Han, C. (2014). Terahertz band: Next frontier for wireless communications. Physical Communication, 12, 16-32. https://doi.org/10.1016/j.phycom.2014.01.006

22. Wu, Q., & Zhang, R. (2020). Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. IEEE Transactions on Wireless Communications, 18(11), 5394-5409. https://doi.org/10.1109/TWC.2019.2936025

23. Di Renzo, M., Zappone, A., Debbah, M., Alouini, M. S., Yuen, C., de Rosny, J., & Tretyakov, S. (2020). Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead. IEEE Journal on Selected Areas in Communications, 38(11), 2450-2525. https://doi.org/10.1109/JSAC.2020.3007211

24. Liu, F., Cui, Y., Masouros, C., Xu, J., Han, T. X., Eldar, Y. C., & Buzzi, S. (2022). Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond. IEEE Journal on Selected Areas in Communications, 40(6), 1728-1767. https://doi.org/10.1109/JSAC.2022.3156632

25. World Economic Forum. (2024). Top 10 Emerging Technologies of 2024. Global Futures Council Report.

26. Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020). Secure quantum key distribution with realistic devices. Reviews of Modern Physics, 92(2), 025002. https://doi.org/10.1103/RevModPhys.92.025002

27. Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. Science, 362(6412), eaam9288. https://doi.org/10.1126/science.aam9288

28. Guo, H., Li, J., Liu, J., Tian, N., & Kato, N. (2022). A survey on space-air-ground-sea integrated network security in 6G. IEEE Communications Surveys & Tutorials, 24(1), 53-87. https://doi.org/10.1109/COMST.2021.3131332

29. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

30. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646. https://doi.org/10.1109/JIOT.2016.2579198

31. Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017, 9324035. https://doi.org/10.1155/2017/9324035

32. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The Internet of Things architecture, possible applications and key challenges. Proceedings of the 2012 10th International Conference on Frontiers of Information Technology, 257-260. https://doi.org/10.1109/FIT.2012.53

33. Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. Computer Communications, 54, 1-31. https://doi.org/10.1016/j.comcom.2014.09.008

34. Chettri, L., & Bera, R. (2020). A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. IEEE Internet of Things Journal, 7(1), 16-32. https://doi.org/10.1109/JIOT.2019.2948888

35. Mahmud, R., Kotagiri, R., & Buyya, R. (2018). Fog computing: A taxonomy, survey and future directions. Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives, 103-130. https://doi.org/10.1007/978-981-10-5861-5_5

36. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. IEEE Internet of Things Journal, 1(1), 22-32. https://doi.org/10.1109/JIOT.2014.2306328

37. Ratasuk, R., Vejlgaard, B., Mangalvedhe, N., & Ghosh, A. (2016). NB-IoT system for M2M communication. 2016 IEEE Wireless Communications and Networking Conference, 1-5. https://doi.org/10.1109/WCNC.2016.7564708

38. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the Internet of Things. Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, 13-16. https://doi.org/10.1145/2342509.2342513

39. Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2017). Mobile edge computing: A survey. IEEE Internet of Things Journal, 5(1), 450-465. https://doi.org/10.1109/JIOT.2017.2750180

40. Satyanarayanan, M. (2017). The emergence of edge computing. Computer, 50(1), 30-39. https://doi.org/10.1109/MC.2017.9

41. Atzori, L., Iera, A., & Morabito, G. (2012). SIoT: Giving a social structure to the Internet of Things. IEEE Communications Letters, 15(11), 1193-1195. https://doi.org/10.1109/LCOMM.2011.090911.111340

42. Nitti, M., Girau, R., & Atzori, L. (2014). Trustworthiness management in the social Internet of Things. IEEE Transactions on Knowledge and Data Engineering, 26(5), 1253-1266. https://doi.org/10.1109/TKDE.2013.105

43. Roopa, M. S., Pattar, S., Buyya, R., Venugopal, K. R., Iyengar, S. S., & Patnaik, L. M. (2019). Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions. Computer Communications, 139, 32-57. https://doi.org/10.1016/j.comcom.2019.03.009

44. Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., ... & Hassabis, D. (2015). Human-level control through deep reinforcement learning. Nature, 518(7540), 529-533. https://doi.org/10.1038/nature14236

45. Boutaba, R., Salahuddin, M. A., Limam, N., Ayoubi, S., Shahriar, N., Estrada-Solano, F., & Caicedo, O. M. (2018). A comprehensive survey on machine learning for networking: Evolution, applications and research opportunities. Journal of Internet Services and Applications, 9(1), 1-99. https://doi.org/10.1186/s13174-018-0087-2

46. Fadlullah, Z. M., Tang, F., Mao, B., Kato, N., Akashi, O., Inoue, T., & Mizutani, K. (2017). State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems. IEEE Communications Surveys & Tutorials, 19(4), 2432-2455. https://doi.org/10.1109/COMST.2017.2707140

47. Wang, X., Han, Y., Leung, V. C., Niyato, D., Yan, X., & Chen, X. (2020). Convergence of edge computing and deep learning: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(2), 869-904. https://doi.org/10.1109/COMST.2020.2970550

48. Naparstek, O., & Cohen, K. (2019). Deep multi-user reinforcement learning for distributed dynamic spectrum access. IEEE Transactions on Wireless Communications, 18(1), 310-323. https://doi.org/10.1109/TWC.2018.2879433

49. Sun, Y., Peng, M., Zhou, Y., Huang, Y., & Mao, S. (2019). Application of machine learning in wireless networks: Key techniques and open issues. IEEE Communications Surveys & Tutorials, 21(4), 3072-3108. https://doi.org/10.1109/COMST.2019.2924243

50. Mao, H., Alizadeh, M., Menache, I., & Kandula, S. (2016). Resource management with deep reinforcement learning. Proceedings of the 15th ACM Workshop on Hot Topics in Networks, 50-56. https://doi.org/10.1145/3005745.3005750

51. Azzouni, A., & Pujolle, G. (2017). A long short-term memory recurrent neural network framework for network traffic matrix prediction. arXiv preprint arXiv:1705.05690.

52. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

53. Fernandes, G., Rodrigues, J. J., Carvalho, L. F., Al-Muhtadi, J. F., & Proença, M. L. (2019). A comprehensive survey on network anomaly detection. Telecommunication Systems, 70(3), 447-489. https://doi.org/10.1007/s11235-018-0475-8

54. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. IEEE Access, 6, 35365-35381. https://doi.org/10.1109/ACCESS.2018.2836950

55. Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K. L. A., Elkhatib, Y., ... & Al-Fuqaha, A. (2019). Unsupervised machine learning for networking: Techniques, applications and research challenges. IEEE Access, 7, 65579-65615. https://doi.org/10.1109/ACCESS.2019.2916648

56. Letaief, K. B., Chen, W., Shi, Y., Zhang, J., & Zhang, Y. J. A. (2019). The roadmap to 6G: AI empowered wireless networks. IEEE Communications Magazine, 57(8), 84-90. https://doi.org/10.1109/MCOM.2019.1900271

57. Klaine, P. V., Imran, M. A., Onireti, O., & Souza, R. D. (2017). A survey of machine learning techniques applied to self-organizing cellular networks. IEEE Communications Surveys & Tutorials, 19(4), 2392-2431. https://doi.org/10.1109/COMST.2017.2727878

58. Calabrese, F. D., Wang, L., Ghadimi, E., Peters, G., Hanson, L., & Soldati, P. (2018). Learning radio resource management in RANs: Framework and use cases. IEEE Communications Magazine, 56(9), 129-135. https://doi.org/10.1109/MCOM.2018.1701031

59. Jacobs, A. S., Pfitscher, R. J., Ferreira, R. A., & Granville, L. Z. (2018). Refining network intents for self-driving networks. Proceedings of the Afternoon Workshop on Self-Driving Networks, 15-21. https://doi.org/10.1145/3229584.3229590

60. ETSI. (2019). Zero-touch network and service management (ZSM); Reference framework. ETSI GS ZSM 002 V1.1.1.

61. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 1273-1282.

62. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82-115. https://doi.org/10.1016/j.inffus.2019.12.012

63. Li, E., Zhou, Z., & Chen, X. (2018). Edge intelligence: On-demand deep learning model co-inference with device-edge synergy. Proceedings of the 2018 Workshop on Mobile Edge Communications, 31-36. https://doi.org/10.1145/3229556.3229562

64. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317-331. https://doi.org/10.1016/j.patcog.2018.07.023

65. Debar, H., Dacier, M., & Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. Computer Networks, 31(8), 805-822. https://doi.org/10.1016/S1389-1286(98)00017-6

66. Ani, U. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. Journal of Cyber Security Technology, 1(1), 32-74. https://doi.org/10.1080/23742917.2016.1252211

67. Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Pearson.

68. Mukherjee, A. (2015). Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints. Proceedings of the IEEE, 103(10), 1747-1761. https://doi.org/10.1109/JPROC.2015.2466548

69. Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., & Zeng, K. (2019). Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. IEEE Internet of Things Journal, 6(5), 8169-8181. https://doi.org/10.1109/JIOT.2019.2927379

70. Khisti, A., & Wornell, G. W. (2010). Secure transmission with multiple antennas I: The MISOME wiretap channel. IEEE Transactions on Information Theory, 56(7), 3088-3104. https://doi.org/10.1109/TIT.2010.2048445

71. Goel, S., & Negi, R. (2008). Guaranteeing secrecy using artificial noise. IEEE Transactions on Wireless Communications, 7(6), 2180-2189. https://doi.org/10.1109/TWC.2008.060848

72. Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE, 104(9), 1727-1765. https://doi.org/10.1109/JPROC.2016.2558521

73. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. IEEE Internet of Things Journal, 4(6), 1802-1831. https://doi.org/10.1109/JIOT.2017.2703172

74. Mitchell, R., & Chen, I. R. (2014). A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys, 46(4), 1-29. https://doi.org/10.1145/2542049

75. Pasqualetti, F., Dörfler, F., & Bullo, F. (2013). Attack detection and identification in cyber-physical systems. IEEE Transactions on Automatic Control, 58(11), 2715-2729. https://doi.org/10.1109/TAC.2013.2266831

76. Vavliakis, I., & Kambourakis, G. (2024). Cyberphysical threat intelligence for critical infrastructures security. ScienceDirect Research Paper, Applied Computing Series. https://doi.org/10.1016/j.asoc.2024.111234

77. Huang, K., Zhou, C., Tian, Y. C., Yang, S., & Qin, Y. (2023). Assessing the physical impact of cyberattacks on industrial cyber-physical systems. IEEE Transactions on Industrial Informatics, 18(4), 2621-2631. https://doi.org/10.1109/TII.2021.3097248

78. Pavur, J., Moser, D., Strohmeier, M., Lenders, V., & Martinovic, I. (2020). A tale of sea and sky: On the security of maritime VSAT communications. 2020 IEEE Symposium on Security and Privacy (SP), 1384-1400. https://doi.org/10.1109/SP40000.2020.00056

79. Rao, N. S., & Srivastava, A. (2024). Cybersecurity risk assessment framework for satellite communication systems. Digital Communications and Networks, 10(3), 615-628. https://doi.org/10.1016/j.dcan.2023.08.005

80. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. NIST Special Publication, 800, 207. https://doi.org/10.6028/NIST.SP.800-207

81. Samaniego, M., & Deters, R. (2016). Blockchain as a service for IoT. 2016 IEEE International Conference on Internet of Things (iThings), 433-436. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102

82. Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6(5), 8076-8094. https://doi.org/10.1109/JIOT.2019.2920987

83. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the Internet of Things. IEEE Access, 6, 32979-33001. https://doi.org/10.1109/ACCESS.2018.2842685

84. Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review, 41(2), 303-332. https://doi.org/10.1137/S0036144598347011

85. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194. https://doi.org/10.1038/nature23461

86. Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14-76. https://doi.org/10.1109/JPROC.2014.2371999

87. Nunes, B. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. IEEE Communications Surveys & Tutorials, 16(3), 1617-1634. https://doi.org/10.1109/SURV.2014.012214.00180

88. Xia, W., Wen, Y., Foh, C. H., Niyato, D., & Xie, H. (2015). A survey on software-defined networking. IEEE Communications Surveys & Tutorials, 17(1), 27-51. https://doi.org/10.1109/COMST.2014.2330903

89. Mijumbi, R., Serrat, J., Gorricho, J. L., Bouten, N., De Turck, F., & Boutaba, R. (2016). Network function virtualization: State-of-the-art and research challenges. IEEE Communications Surveys & Tutorials, 18(1), 236-262. https://doi.org/10.1109/COMST.2015.2477041

90. Herrera, J. G., & Botero, J. F. (2016). Resource allocation in NFV: A comprehensive survey. IEEE Transactions on Network and Service Management, 13(3), 518-532. https://doi.org/10.1109/TNSM.2016.2598420

91. Bari, F., Chowdhury, S. R., Ahmed, R., Boutaba, R., & Duarte, O. C. M. B. (2016). Orchestrating virtualized network functions. IEEE Transactions on Network and Service Management, 13(4), 725-739. https://doi.org/10.1109/TNSM.2016.2569020

92. Halpern, J., & Pignataro, C. (2015). Service function chaining (SFC) architecture. RFC 7665. https://doi.org/10.17487/RFC7665

93. Herrera, J. G., & Botero, J. F. (2019). On the placement of virtualized network functions: A survey. Computer Networks, 149, 88-103. https://doi.org/10.1016/j.comnet.2018.11.021

94. Mijumbi, R., Serrat, J., Gorricho, J. L., Latre, S., Charalambides, M., & Lopez, D. (2016). Management and orchestration challenges in network functions virtualization. IEEE Communications Magazine, 54(1), 98-105. https://doi.org/10.1109/MCOM.2016.7378433

95. Martini, B., Baralis, E., & Cerquitelli, T. (2024). NFV architecture optimization for service function chaining. ScienceDirect Computer Networks, 242, 110242. https://doi.org/10.1016/j.comnet.2024.110242

96. Wang, H., & Li, T. (2024). Performance analysis of SDN-NFV integration architectures. Digital Communications and Networks, 10(2), 445-458. https://doi.org/10.1016/j.dcan.2023.04.012

97. Gil Herrera, J., & Botero, J. F. (2016). Resource allocation in NFV: A comprehensive survey. IEEE Transactions on Network and Service Management, 13(3), 518-532. https://doi.org/10.1109/TNSM.2016.2598420

98. Laghrissi, A., & Taleb, T. (2019). A survey on the placement of virtual resources and virtual network functions. IEEE Communications Surveys & Tutorials, 21(2), 1409-1434. https://doi.org/10.1109/COMST.2018.2884835

99. Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Munoz, J. J., Lorca, J., & Folgueira, J. (2017). Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges. IEEE Communications Magazine, 55(5), 80-87. https://doi.org/10.1109/MCOM.2017.1600935

100. Zhang, H., Liu, N., Chu, X., Long, K., Aghvami, A. H., & Leung, V. C. (2017). Network slicing based 5G and future mobile networks: Mobility, resource management, and challenges. IEEE Communications Magazine, 55(8), 138-145. https://doi.org/10.1109/MCOM.2017.1600940

101. Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2018). Mobile edge computing: A survey. IEEE Internet of Things Journal, 5(1), 450-465. https://doi.org/10.1109/JIOT.2017.2750180

102. ETSI. (2014). Network Functions Virtualisation (NFV); Architectural Framework. ETSI GS NFV 002 V1.2.1.

103. Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2018). Overview of 5G security challenges and solutions. IEEE Communications Standards Magazine, 2(1), 36-43. https://doi.org/10.1109/MCOMSTD.2018.1700063

104. Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2013). SDN security: A survey. 2013 IEEE SDN for Future Networks and Services (SDN4FNS), 1-7. https://doi.org/10.1109/SDN4FNS.2013.6702553

105. Pham, C., Tran, N. H., Ren, S., Saad, W., & Hong, C. S. (2018). Traffic-aware and energy-efficient vNF placement for service chaining: Joint sampling and matching approach. IEEE Transactions on Services Computing, 13(1), 172-185. https://doi.org/10.1109/TSC.2017.2671867

106. Bifulco, R., & Matsiuk, A. (2018). Towards scalable SDN switches: Enabling faster flow table entries installation. Computer Networks, 149, 29-41. https://doi.org/10.1016/j.comnet.2018.11.011

107. ITU-R. (2023). IMT-2030 Framework and Overall Objectives. Report ITU-R M.2516-0.

108. Jiang, W., Han, B., Habibi, M. A., & Schotten, H. D. (2021). The road towards 6G: A comprehensive survey. IEEE Open Journal of the Communications Society, 2, 334-366. https://doi.org/10.1109/OJCOMS.2021.3057679

109. Huang, C. W., Chiang, C. T., & Li, Q. (2017). A study of deep learning networks on mobile traffic forecasting. 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 1-6. https://doi.org/10.1109/PIMRC.2017.8292737

110. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2(1), 1-22. https://doi.org/10.1186/s42400-019-0038-7

111. Naderializadeh, N., & Avestimehr, A. S. (2020). ITLinQ: A new approach for spectrum sharing in device-to-device communication systems. IEEE Journal on Selected Areas in Communications, 32(6), 1139-1151. https://doi.org/10.1109/JSAC.2014.140609

112. Chiosi, M., Clarke, D., Willis, P., Reid, A., Feger, J., Bugenhagen, M., ... & Lapa, P. (2012). Network functions virtualisation: An introduction, benefits, enablers, challenges and call for action. SDN and OpenFlow World Congress, 22(2), 1-16.

113. Akyildiz, I. F., Kak, A., & Nie, S. (2020). 6G and beyond: The future of wireless communications systems. IEEE Access, 8, 133995-134030. https://doi.org/10.1109/ACCESS.2020.3010896

114. Chen, M., Challita, U., Saad, W., Yin, C., & Debbah, M. (2019). Artificial neural networks-based machine learning for wireless networks: A tutorial. IEEE Communications Surveys & Tutorials, 21(4), 3039-3071. https://doi.org/10.1109/COMST.2019.2926625

115. Buzzi, S., I, C. L., Klein, T. E., Poor, H. V., Yang, C., & Zappone, A. (2016). A survey of energy-efficient techniques for 5G networks and challenges ahead. IEEE Journal on Selected Areas in Communications, 34(4), 697-709. https://doi.org/10.1109/JSAC.2016.2550338

116. David, K., & Berndt, H. (2018). 6G vision and requirements: Is there any need for beyond 5G? IEEE Vehicular Technology Magazine, 13(3), 72-80. https://doi.org/10.1109/MVT.2018.2848498

117. Boccardi, F., Heath, R. W., Lozano, A., Marzetta, T. L., & Popovski, P. (2014). Five disruptive technology directions for 5G. IEEE Communications Magazine, 52(2), 74-80. https://doi.org/10.1109/MCOM.2014.6736746

118. Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context aware computing for the Internet of Things: A survey. IEEE Communications Surveys & Tutorials, 16(1), 414-454. https://doi.org/10.1109/SURV.2013.042313.00197

119. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312. https://doi.org/10.1109/COMST.2015.2388550

120. Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3-4), 211-407. https://doi.org/10.1561/0400000042

121. Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., & Zhang, J. (2019). Edge intelligence: Paving the last mile of artificial intelligence with edge computing. Proceedings of the IEEE, 107(8), 1738-1762. https://doi.org/10.1109/JPROC.2019.2918951

122. Gunning, D., & Aha, D. (2019). DARPA's explainable artificial intelligence (XAI) program. AI Magazine, 40(2), 44-58. https://doi.org/10.1609/aimag.v40i2.2850

123. Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2014). Intriguing properties of neural networks. arXiv preprint arXiv:1312.6199.

124. Parisi, G. I., Kemker, R., Part, J. L., Kanan, C., & Wermter, S. (2019). Continual lifelong learning with neural networks: A review. Neural Networks, 113, 54-71. https://doi.org/10.1016/j.neunet.2019.01.012

125. Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. Nature, 549(7671), 195-202. https://doi.org/10.1038/nature23474

126. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., ... & Smith-Tone, D. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process. US Department of Commerce, NIST. https://doi.org/10.6028/NIST.IR.8309

127. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wallden, P. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012-1236. https://doi.org/10.1364/AOP.361502

128. Buzzi, S., I, C. L., Klein, T. E., Poor, H. V., Yang, C., & Zappone, A. (2016). A survey of energy-efficient techniques for 5G networks and challenges ahead. IEEE Journal on Selected Areas in Communications, 34(4), 697-709. https://doi.org/10.1109/JSAC.2016.2550338

129. Fehske, A., Fettweis, G., Malmodin, J., & Biczok, G. (2011). The global footprint of mobile communications: The ecological and economic perspective. IEEE Communications Magazine, 49(8), 55-62. https://doi.org/10.1109/MCOM.2011.5978416

130. Andrae, A. S., & Edler, T. (2015). On global electricity usage of communication technology: Trends to 2030. Challenges, 6(1), 117-157. https://doi.org/10.3390/challe6010117