Deep Science Publishing
https://doi.org/10.70593/978-93-49307-75-9_12

DeepScience
Open Access Books

Chapter 12: Envisioning the convergence of intelligent technologies to shape the future landscape of secure and scalable communications

12.1. Introduction

The advent of intelligent technologies is transforming various aspects of modern communications. Innovations in connectivity, as well as artificial intelligence, are redefining the scope and scale of communications in terms of massive devices, density, and mobility. Both static and dynamic spectra are being added to the system to cater to future needs, mitigating spectrum contention and reducing interference, thus enhancing throughput significantly. The Fourth Industrial Revolution technologies, such as the Internet of Things and cyber-physical and heterogeneous systems, hold a significant place in revolutionizing nearly every sector in the coming years. It is anticipated that a massive and heterogeneous network of billions of IoT-based devices and sensors deployed through untrusted environments will gather, process, and exchange data, enabling a new era of real-time and remote systems across various verticals.

The advanced communication systems, which ensure high spectral and energy efficiencies, resilient operations, fast response times, and scalability to meet the growing power requirements, require system-level security by design. While there have been rapid technological advancements in the domains of wireless connectivity and AI, there has been no scientific investigation into the potential benefits of converging smart communication techniques with intelligence, security, resilience, and trust. There have been various research-related works addressing security and privacy challenges in the context of different communication technologies that may not provide end-to-end secure and scalable solutions. Through this, we invite researchers to explore the potential.

12.1.1. Overview of the Transformation in Communication Technologies

Over the years, the communication technology domain has undergone a paradigm shift at several milestones. The journey began with the use of manually operated switches, which were later replaced by Strowger switches. After completing their lifespan, these switches were replaced by stored and forward digital switches. As of 2020, the public switched telephone network (PSTN) comprised 83% of digital communication systems. Digital communication systems have completely transformed the way communication takes place compared to traditional analog systems. While digital communication technology with applications like fiber optics, microwave, satellite, and encryption techniques has enhanced connectivity, the emergence of mobile communications and cloud computing has revolutionized the way we communicate and are interconnected. Today, 7.7 billion mobile subscribers worldwide make phone calls, share text and multimedia messages, browse the internet, and send emails. These subscribers also avail of cloud-based services with several benefits including cost-effectiveness, flexibility, resource pooling, easy accessibility, rapid elasticity, enhanced security, and rapid deployment of computing services.

The transformation in mobile phone technology for over a decade involved the use of 3G, 4G, and LTE for video telephony, video on demand, video chats, surveillance, and internet gaming. Worldwide deployment of 5G as another major transformative communication technology aims to provide more powerful connections to connect more devices and to keep the internet performing better. In addition, the communication technology domain has reached a stage where the world has become a global village with the internet spreading predominantly for data communication through optical fiber cables without geographical boundaries. Nevertheless, the advancement in communication technology has also posed challenges in dealing with terror attacks and cybercrimes. Overall, any transformative communication technology must be capable of addressing the current challenges and future trends in digital networking. At present, research avenues are involved in emerging digital communication systems, resources of cloud computing, and security. All these aspects help scholars and industry researchers to collectively learn the ongoing research trends of sustainable digital communication.

12.2. The Rise of Intelligent Technologies

The inception of the 21st century witnessed the proliferation of "intelligence" in various technologies across diverse application domains. Intelligence, in this context, primarily refers to a set of embedded capacities concerning learning, reasoning, perceiving, and decision-making. In general, technology is considered to be intelligent if it possesses

some or all of the following: autonomy, contextual awareness, adaptability, and resourcefulness. Once conceived as almost fantastical technologies, various forms of intelligent systems, including artificial intelligence, machine learning, connected environments, predictive analytics, and blockchain, have been significantly maturing over the past decade. These advancements are transforming communication infrastructure, bringing about the features of pervasive, ubiquitous, autonomous, self-organizing, secure, and reliable communication functionalities.

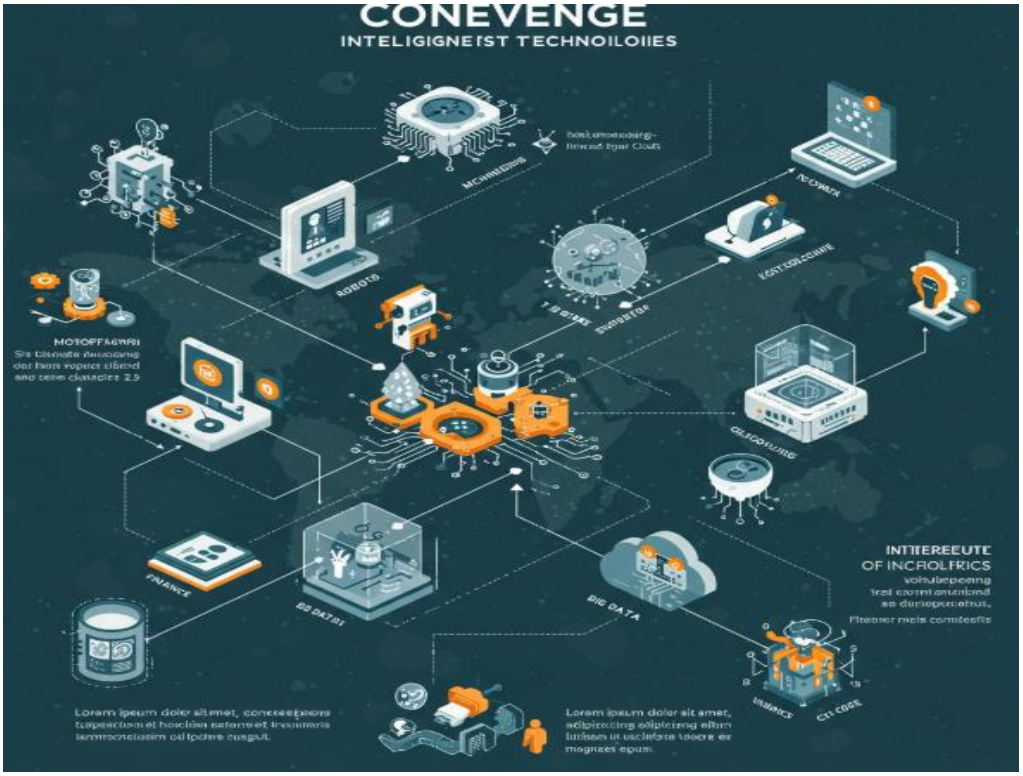

Fig 12 . 1 : Convergence of Intelligent Technologies in the 21st Century

Each of the aforementioned technologies has, to varying degrees, enhanced the capabilities of existing systems, and they all revolve around the core principles of intelligent systems design. The Internet of Things focuses on re-envisioning the Internet architecture by enabling smart objects to talk to each other in the first mile, in turn communicating with centralized or pseudo-distributed architectures at the core. This segment gradually converges with blockchain technologies. These applications can be useful in managing the inelastic, complex interdomain operations. Artificial intelligence, machine learning, and predictive analysis, at the other end of the spectrum, can be used as enabling functions for maximizing operational efficiencies and enhancing capacities to reduce threats and vulnerabilities. These technologies, often intertwined to a large

extent, can be used to support future intelligent and decentralized communications at a segment of the core-to-core network of networks. At present, a few challenges confront the universe of intelligent communications, including the paradigms' implausibility and complex operation in insecure regions. However, such outcomes may be a necessity in a highly disruptive era.

12.2.1. Artificial Intelligence and Machine Learning

Currently, we observe a fast-growing trend of various technologies providing the means to make the Internet a key enabler for social networks in cyberspace and consequently driving the evolution of digital communication. The capability of AI and machine learning techniques to autonomously adapt behavior provides the ability of a machine to process large amounts of data effectively and detect patterns that may be impossible for humans. When AI gains more experience, it can optimize its communication processes and provide better quality and easier data communication and analysis for human users. Therefore, these different technologies, together, can precipitate a new phase in innovative communication systems and infrastructure as they converge to provide new services and benefits for the daily activities of people and businesses (Zhang et al., 2019; Raza et al., 2020; Wang & Zhang, 2021;). This chapter outlines technological challenges that are currently being addressed to reach the vision outlined in this figure.

Often, artificial intelligence is associated with a broader concept: machine learning. In communication-related topics, machine learning provides AI with the ability to learn from the data we provide it. One of the advantages of machine learning is the capability to process and classify large amounts of structured data. Many data communication-based applications, considered in several domains and industries where smart communication takes place, use different types of machine learning techniques to facilitate operations. For example, patterns in large-scale communication system trace data can be used to create digital twin analytical models for communication performance in systems that accommodate future weather data to aid in real-time response and gain future operational insights that can be used as an evidence-based approach to predict when an event may occur, providing better decision-making.

12.2.2. Internet of Things (IoT)

The Internet of Things (IoT) is a mega-trend that is being considered the next revolution in human society after the industrial and information revolutions. It refers to the interconnectivity, interoperability, and integration of everyday objects, devices, systems,

and services to collect and exchange data as well as to extract value for the efficacy of various operations. The main idea behind it is to foster communication between objects and to automate decisions and tasks. This dynamic intercommunication facilitates enhanced user experience and operational efficiency. For instance, smart homes have already allowed homeowners extensive control over energy, appliances, and security systems, while in e-health it has resulted in remote patient monitoring and enabled real-time health data reporting and record-keeping. Meanwhile, industries have started implementing IoT for advanced assembly-line monitoring and control, as well as automation in discrete manufacturing and process handling for a variety of medical, automotive, and human augmentation sectors to amplify productivity and safety. The unified goal behind these implementations is to enable low-latency, scalable, and secure machines and systems for real-time industrial and consumer decision-making support.

Motivated by these developments, IoT has also been envisaged as part of the broader 5G and beyond-5G communication frameworks, including edge IoT in security, energy, blockchain, and applications that use massive sensor data. Consequently, various lightweight technologies have been combined with radio access technologies to enable the scalable inclusion of IoT nodes in future communication infrastructure. In particular, 5G and beyond-5G deployments are expected to facilitate secure interplay between IoT devices, edge computing, radio spectrum, network infrastructure, and the cloud to ensure extensive scalability and operational efficiency in the upcoming scenarios. For instance, by enabling the integration of low-latency network services and advanced mobile network solutions, IoT integration with communication frameworks will offer applications such as remote incident monitoring, environment monitoring, precision agriculture, supply chain optimization, critical asset monitoring, and the Internet of Soldiers.

12.2.3. Blockchain Technology

Blockchain is a technology that became widely popular due to digital currency, which uses blockchain to secure and transparently transfer value from one digital address to another. As with cryptocurrency, the blockchain is a distributed technology operated by a large network of computers that duplicate every single transaction in a public ledger or a public block. The design of the blockchain, being decentralized and public, with algorithms as its protocols, makes it the most secure framework for communicating with others. This has made blockchain important in secure messaging and communication technologies related to transactions. Regarding digital messaging and trust, there is a need for effective identification of the message being communicated. Regardless of the system of communication and the contents being conveyed, trust in the system is central

to trusting any transaction made. Thus, the required background to utilize technologies such as blockchain is trust, and trust needs transparency. This includes a communication framework and mechanism that is transparent.

Though the blockchain offers secure communications and mechanisms with full transparency, the question becomes: how will we implement it in a manner that is also scalable and energy-efficient? The traditional blockchain system is relatively energy-wasting in the confirmation mechanism, especially the proof of work. While slow in the confirmation of transactions, it is also a competitor in energy consumption. Despite the energy waste and scalability drawbacks being criticized, early blockchain adopters have been able to revolutionize several industries, especially in making secure transactions, including cryptocurrencies. As a grand vision of the future, which we may state is under experimentation, if it is to run successfully, we will expect a fully secured digitally agreed system. In real-life scenarios, this might be the key to enabling an efficient, secure communication, digital identity, and metadata protection system. It can be directly imagined in the banking system; if a bank can allow another trusted bank to perform work on its behalf without any changes being made to any element of the transaction, like value or time, then inter-bank transactions, normally involving many stakeholders, have been made easy.

12.3. Current Landscape of Communication Technologies

The prevalent low-cost and reliable communication infrastructures have facilitated peer-to-peer collaboration models over a digital medium, such as email, messaging applications, and collaborative tools. Traditional communication systems follow strict regulatory and protocol standards to ensure information exchange. With increasing demand and changing user preferences due to the digital era's proliferation, there is a need for faster, more secure, inexpensive, and reliable communication technologies. Several concepts and protocols are available that could potentially open new frontiers in communication systems. These include wireless communication technologies, free-space laser communication, submarine cables, satellites, long-reach passive optical networks, machine-to-machine devices, and Internet of Things devices.

Devising and implementing such convergent technological infrastructures is vital to leveraging the potential of these technologies. Several research efforts are available to implement these next-generation technologies, specifically over software-defined networking, cloud computing, fog/edge computing, and other augmentations to the existing Internet architecture. In addition to these, there exists an even more recent strand of research that focuses on converging interconnected yet marginalized discipline-

specific domains, each representing a specific technology-building block, such as efficient spectrum usage, blockchain, acoustic and optical wireless communication technologies, delay-tolerant networking, network coding, software-defined networking, and cyber-physical systems, for extending the functionality and utility of existing communication technologies and addressing the ubiquitous inter-node handoff challenge effectively and efficiently.

The deployment of new digital era technologies will help to solve current communication system challenges and limitations, but they need to address the traditional security challenges. Further, integration of new technologies involves the modification of already deployed systems to accommodate the newly proposed technologies; in the case of machine-to-machine and Internet of Things, it involves merging digital-era technologies into already deployed physical systems. Understanding the current communication technologies landscape provides insights into evolving needs, limitations, and challenges that need to be addressed to develop new communication systems following the digital era.

12.3.1. Traditional Communication Systems

Communication is a fundamental human activity, and traditional communication systems have played a crucial role in shaping society in the 20th century. These systems include classic services such as radio and subscription television networks, complex applications such as telephony over the public switched telephone network or conferencing tools, as well as transmissions connected with the so-called information society, including data and multimedia transmission complemented with services such as custom ICAP and security protocols, among others. The radio and television signals can be received and consumed by almost everyone. Subscriber telephones were and still are used by people to do the widely spread Metropolitan Area Network – a one- to two-digit kilometers long form of communication – provided by a commercial network. They are traditional channels serving more than 100 years in the form as we know it today. They are successful because of their reliability and ubiquitous service, serving people at home, at work, and on the road (Zeng et al., 2020; Zhang & Wu, 2021).

However, although a wide range of solutions appeared within different segments of classical communication models, these solutions are restricted in terms of offered bandwidth, and the requirements for the available bandwidth significantly exceed the genuine capabilities of these systems. Therefore, it is predictable that these communication systems will become obsolete in the future. Nowadays, television, telephony, and radio communication systems are transitioning to digital systems. This

process, initiated many years ago, is still in progress. However, this does not mean that the traditional systems are discarded easily. On the other hand, traditional organizations are upgrading their systems to make them provisional with actual conditions. However, this digital evolution should respect the past organizational strategy, priorities, and management more or less, because many people know how the organization works.

12.3.2. Emerging Communication Protocols

A variety of communication protocols have had a significant impact on the connectivity of the physical world to the digital universe. They enable effective transmission, collection, and facilitation of large quantities of data through technologies such as the fifth generation. It was officially standardized in 2017 and is commercially available worldwide. The technology promises a high-speed peak and nominal data rate, in addition to ubiquitous, energy-efficient, and low-latency solutions. In addition to 5G, systems such as Wi-Fi 6, ultra-wideband, and eSHF are also available. They provide wireless data transfer rates that are several times faster than those of previous generations. In addition to a stronger communication system, the use of AI and IoT to optimize cognition, recognition, reasoning, and security aspects is a fast-growing field.

These intelligent systems need an adaptive communication infrastructure that can send and receive data from anywhere at any time. It can be observed that existing communication systems are reaching their limits in terms of their capacity to handle the rapidly increasing volume of data. 5G, Wi-Fi 6, and other communication systems are not openly discussed in academia, industry, or society as potential universal communication systems with supporting mechanisms. Although research on these systems is still ongoing, they hold great promise for the future. These standards may require new control systems from the ground up. In addition, each standard may necessitate investment in new technologies if it is autonomous or required by all forthcoming technical systems. Lastly, and just as a caution, the introduction of new communication standards might have unexpected effects on existing systems and societies.

12.4. Security Challenges in Communication

Modern communication technologies face multiple security challenges, both in the digital world and the physical domain. With the ever-increasing use of digital, online, and wireless communication in everyday life, these challenges are becoming starker day by day. Cybercriminals often take advantage of vulnerabilities to gain unauthorized

access, overwhelm system capability to deny access to valid users, breach and manipulate data, or unethically capture and intercept sensitive information. As technology systems evolve, communication security and privacy have emerged as some of the biggest concerns because they are used to store, manipulate, and send large volumes of critical and personal information. A wide range of devices are getting interconnected through the Internet, so cloud security, the Internet of Things, Big Data, and other similar areas also come under threat. In some cases, software-embedded systems regulate the use of communication channels and services through a virtual infrastructure. Laws like the General Data Protection Regulation, the Health Insurance Portability and Accountability Act, and other similar laws in different countries have also been introduced recently to control the cyber communications environment specifically and network communications in general.

The current scenario involves several complex problems in communication security, which include technological advancements in communications, the existing communication infrastructure, system vulnerabilities, uncertain system behaviors, time-varying environments, and encrypted data communications, especially in dynamic environments. Its impact can range from data manipulation, false data generation, or unauthorized access to denial of service, eavesdropping, data theft, information warfare, and other similar attacks. A sudden attack in the communication network may not only affect the communication users, but also attacks on networks used by other domains, such as banking, aviation, healthcare, military, nuclear power, and election systems. Furthermore, any unforeseen attack on the national-scale critical communication network infrastructure may bring a country to its knees, with a potentially catastrophic impact on the economy, society, and national security. Various researchers, teams, and companies joining academics and industrial practitioners have worked to protect the communication network systems in different forums through mathematical formulations and defense mechanisms. The research community is also coming up with security architectures, trust management, secure routing, big data analytic systems, and hardware simulations to analyze security concerns ahead of time.

12.4.1. Data Privacy Concerns

As the amount of personal information being transmitted via the data service expands, there is a rising interest in privacy issues. Personal information, also known as personal data, includes any information relating to an identified or identifiable living individual and includes various kinds of identifiers. In recent years, privacy values, in practice, have revolved around data protection. As a result, we are focusing on technical solutions for safeguarding personal data communicated in networks. We believe that if data privacy

is incorporated into system-level design, it will lay the groundwork for building the convergent intelligent technologies used in secure and scalable communication from the ground up.

Data privacy is increasingly becoming a matter of concern, with regulators focusing their attention on safeguarding data. To address the privacy concerns, a stringent set of rules for managing data privacy and providing guidelines for organizations to comply with the new rules has been established. The rules apply not only to organizations located within certain regions but also to those located outside as well if they provide services within those regions. There are strict penalties and fines for organizations that do not comply with the rules. To address such privacy issues, penalties of up to 4% of the organization's global annual turnover for non-compliance with the rules may be imposed. Hence, organizations must comply with the rules to safeguard individuals' privacy and avoid penalties. To address these issues, it is essential to communicate to individuals the data usage and its implications through a privacy notice and terms of service.

In distributed systems, individuals can protect their privacy by becoming aware of the data lifecycle and the processing services. The data sender has several responsibilities. To gain trust, the entities are required to digitally sign the terms of service and the transaction key. Hash-chaining is applied to the input before it is sent into the system. The hash pointers chain the data to record the next hash value. Once it is hashed, the information is automatically uploaded and follows secure and transparent communication in the processing services. Both hashing and encryption can protect individually identifiable information, which is used for protecting the integrity and confidentiality of an individual's data. A sender creates a privacy notice for the dissemination of data processing history. Hash pointers are suitable for communication systems. They show different types of distributed families with and without input. The input data can be easily uploaded by an individual through secure communication.

12.4.2. Cybersecurity Threats

A wide range of cybersecurity threats confront communication services, including, among others, HAPS. These threats come with a steadily rising rate of modernization and increased sophistication and affect both public and private sectors. There is an ever-increasing number of cyber-strategic novelties aimed at further undermining global cyber infrastructures and resiliency in cyberspace. The list of escalated threats that shall be faced by HAPS-based networks in the future is vast. Some of the primary objectives of such cyber-related concerns include disruption of communication infrastructures, stealing data and information, fraud in the context of financial benefits, and even

targeting of physical destruction. These threats are growing both in volume and sophistication, encompassing a plethora of threat classes, which can be frightening unless addressed adequately.

A variety of threats like phishing, man-in-the-middle, denial of service and distributed denial of service, eavesdropping, spoofing, replay attacks, and more mental attack attacks might exploit security vulnerabilities to disrupt communications. Denial of service and distributed denial of service attacks may drain system resources and sabotage service. Phishing attacks are fraudulent schemes that utilize emails and fake websites to mask official communications and commercial transactions. Phished emails may be used to steal sensitive information. This hampers the scalability of the network's operating structure, ensuring that prior precautions against such threats are in place. As the dependency on the IoT network and communication networks escalates, the concerns of cyber-related attacks are also intensifying. Mitigating these challenges requires an intense and comprehensive cybersecurity approach to assess threats and conduct robust risk management assessments to secure critical infrastructure. Early monitoring of weaknesses or vulnerabilities must be addressed and rectified by proactive measures. Organizational immune defense mechanisms entail primarily detection of the threat, risk-informed choices based on objectives, avoiding cross-disciplinary silos, formal risk and semi-formal calculation, and systematic incident reporting to enable real-time hazard control. In the event of an incident or real-time threat detection, a pragmatic governance scheme is crucial to promoting situational awareness. It focuses on developing the capacities to predict, prevent, and address one's state of insecurity and weakness. Attempts to pool and collaborate resources and data across functions, departments, and cultures have proven to be limited or inefficient. While difficulties in consent to share inadequacies or lapses in situational management approach exist, some resources to prioritize and invest in cybersecurity can be combined in this way, especially where the core capabilities of different organizations fit. Conclusively, the future attacks are unknown; however, cyber vigilance is an ongoing endeavor. Ongoing malware developments with millions of new viruses annually show that internet systems are invariably vulnerable. Every application layer in the network will face some degree of peril, be it from human factors or technical factors.

12.5. Scalability Issues in Communication Networks

Scalability, by definition, is the ability to evolve without disrupting established operations and significantly increasing overheads. In future communication environments, this type of evolution will be important if our networks are to continue to operate efficiently. Efficiency is pivotal for best accommodating rapidly growing traffic

demands. However, regardless of the value in increased scalability, many current networks are candidates for being overwhelmed by sheer numbers of users attempting to access services, heavy amounts of aggregated traffic, economically driven high congestion levels, and outdated, inefficient technology that still pervades many areas of communication infrastructure. Despite technological evolution, several types of problems inherent in older systems are difficult or impossible to correctly address. Therefore, many technological and political challenges related to scalability lie ahead. A great deal of the generalization treatments in the remainder of this text assumes the Internet as a case study since, to date, it is one of the most scalable worldwide systems currently in existence.

Currently, network congestion problems can be addressed by numerous means, such as re-routing traffic to bypass network areas, slowing down data delivery rates, or overprovisioning hardware. Ideally, it is preferable to proactively address congestion before it becomes an acute problem. Some of the most effective general techniques appear at the resource allocation level. Resource allocation techniques distribute network assets for the common good and maximize some form of benefit, for example, network welfare. Generally speaking, service providers can only control network assets in terms of network resources, such as bandwidth and processing power; hence, allocation of network assets involves network resource allocation. In current wide area packet-switched systems such as the Internet, packets are scheduled for available resources in both space and time at each router. Interestingly, future communication systems are expected to consist of a complex combination of both the current packet-based model and other data and circuit-switched models. Given that, the challenges for control are multi-fold. It is anticipated that these networks will evolve in a piecemeal fashion, incrementally adding support for newer, more revolutionary technologies that lean toward packet-like models.

12.5.1. Infrastructure Limitations

Infrastructure limitations can hinder future communication systems, trustworthiness, as well as scalability as communication networks continue to grow. Often, poor architectural designs and lack of foresight are more significant design trade-offs than security concerns, which can be solved using cryptographic methods. Upgrading home routers running software might be infeasible because providers are no longer active, do not guarantee long-term support, or risk vulnerabilities on systems that are not supposed to be decrypted. Consequently, many systems will keep older operating systems and their vulnerabilities, which will indirectly impact the work of security and obstacle emergence. If we are not agile enough to swiftly replace systems to adapt to future

shortcuts, the scalability and performance of the system would be impacted, and the lifetime of these devices has to be in the order of the infrastructure's growth behavior. The I-35 bridge collapse in the US happened due to an outdated infrastructure.

Potentially, there are numerous infrastructure bottlenecks because of limited scalability that could impact a nationwide economy or infrastructure, such as power requirements, growing traffic, spectrum availability, and software and hardware limits. Planning for medium-term communications would thus also need to involve strategically upgrading the infrastructure to prevent or bypass limitations, such as focusing on training ethereal AI on silicon, and moving networks away from their off-the-shelf Ethernet. In the transport industry, providing flexible solutions and minimizing risks for the critical layers of the infrastructure have therefore become a great concern for new technology adoption, cozy with legacy systems.

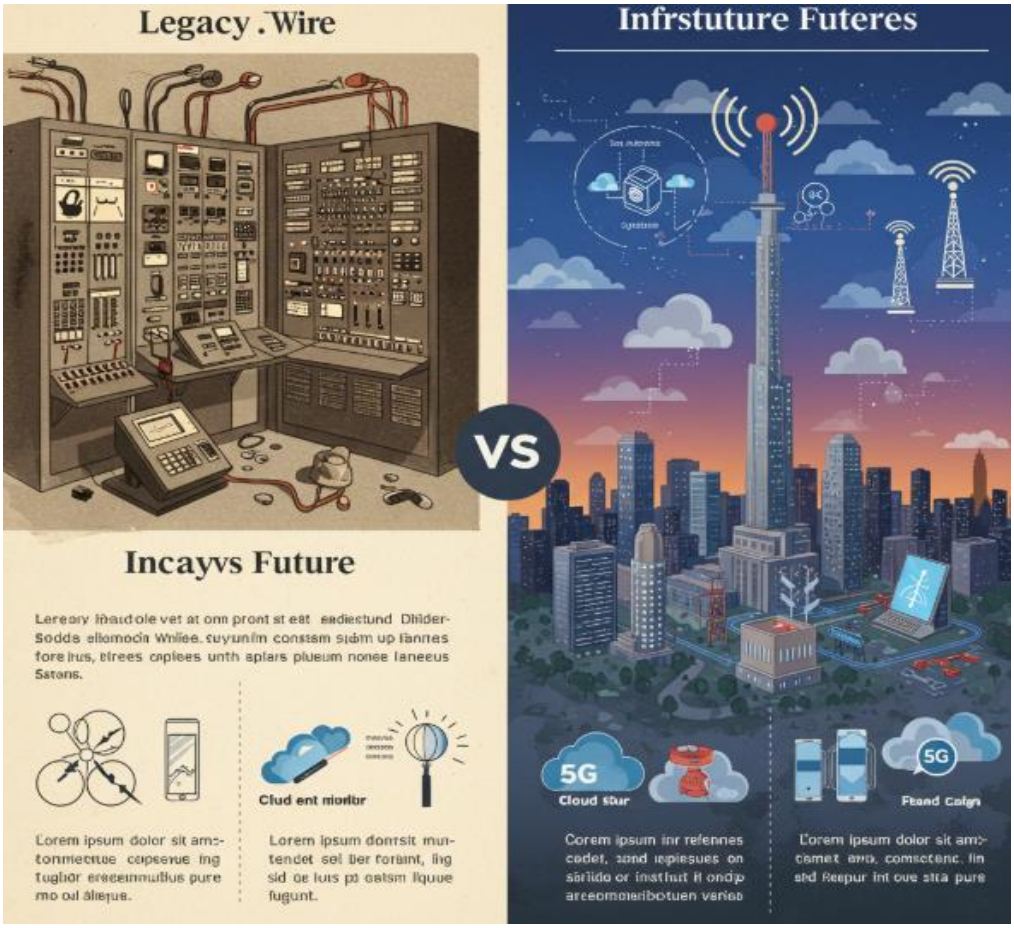

Fig 12 . 2 : Legacy vs. Future: Infrastructure Challenges in Evolving Communication Systems

12.5.2. Network Congestion and Latency

Network congestion is one of the serious challenges in the design of communication networks. On the one hand, it results in poor quality of service and users' quality of experience, and on the other hand, congestion hampers the performance of the systems at the service provider's side. When the data traffic exceeds the network's capacity, it results in slow data throughput or throughput deterioration, which is also known as network congestion. The increasing number of devices with internet connectivity and multimedia traffic advances in communication networks are responsible for high data traffic. They are responsible for a disproportionate amount of network communications; hence, they multiply the number of packet flows in a network. As a result, a common outcome of heavy traffic conditions is network congestion. It is believed that a significant portion of network traffic is due to cloud-based services. Cloud services access or utilize network resources to provide support to users with no inherent mobility. Also, when various cloud services are utilized by users, these service requests from multiple clients and servers lead to network congestion. Network congestion can be minimized using traffic management techniques such as optimized routing, traffic control, resource allocation, and traffic load balancing.

The performance of a network can be affected, particularly for applications requiring a minimum delay, such as video streaming, voice-over IP, telesurgery, and real-time networks. The recommended delay for real-time communications is 100 ms or less. Above this delay, communication is perceived as poor quality. The time traffic takes from source to destination is referred to as latency. It is used in various fields of communication networks to specify the time taken, such as request replication time by the cache system and storage latency. For communication networks, in general, it can be referred to as the total time taken to receive acknowledgment back after sending the request. Latency is a key network performance metric that defines the performance of an application or an end-to-end network. Managing the problem of network congestion, latency, etc., is challenging with the growth of network communication technologies, and novel solutions are also needed. Due to the features mentioned in this section, there is a need to mitigate these large-scale and real-time issues to envision unhindered communication among numerous SDN-enabled IoT and set the user-embraced future Internet of Intelligent Things for ensuring scalable communication.

12.6. Convergence of Intelligent Technologies

Today we live in a world that is always connected, be it people connected to the internet, to devices, even devices directly connected to other devices, etc. However, each

technology in most cases is optimized to perform specific functions. Convergence in communication systems is the mechanism through which distinct technologies can integrate into the same system, allowing for more efficient and effective communication. The goal of all human civilization and evolution has been to combine all fields and develop advanced solutions to ensure the utilization of maximum output with minimum resources in a cost-effective way. The developments in deep learning and artificial intelligence in particular mean that we are now better poised than ever to introduce robust AIs to a broad range of application domains. This would provide a mechanism for a fundamental reworking of the way we think about technology from the ground up, and would be particularly significant in domains that exhibit an element of dynamic consideration. For the point of this paper, we are taking three underlying technologies: AI, Internet of Things, and Blockchain, and assessing how they could come together in a strategy for addressing two main issues within the control plane area of next-generation communication systems, namely in the areas of security and scalability. Technologies converge primarily in a synergistic manner; when integrated, they provide more output than the mere combination of outputs obtained by applying these technologies independently. These technologies, in combination with shared value, security identity, and enterprise cloud—either public or private—have been successfully implemented in various studies. However, several legal and moral implications must be addressed, as well as some required legal and regulatory aspects. While there is a combination of hardware, software, and network virtualization capabilities, such an overlay of intelligent technologies is always based on customization and alignment in close collaboration between technologists and lawmakers in the true sense and context. This will open the way to commercialize the basic and jointly collaborative technologies as a convergence for future generations, thus predicting the world from the Internet of Things, data, knowledge, wisdom, and the will of human interaction converged in the true sense. This gives a complete multimedia immersive environment picturing the world of the future where every gadget would be different, but technology as a whole would be the same and accessible over long distances reliably.

12.6.1. Integrating AI with Communication Systems

Artificial intelligence plays a vital role in automating systems, resulting in improved process efficiency and responsiveness. The main advantage of AI is increasingly intuitive feedback via the utilization of developed user profiling and content feature estimation, helping to provide better-personalized services to users. AI has the potential to deal with users' affinity for specific content and help in predicting future trends by monitoring system operations with the flexibility and capacity obtained by learning specific user behavior. There are several fields of communication systems where AI

holds the ability to bring transformational change in terms of improving overall performance, such as in the areas of network management and optimization, resource allocation and adaptable communication strategies, intelligent caching, auto-tuning techniques, auto-reconfiguration, and recovery, improved quality of experience, user behavior visualization, and intelligent planning.

Another important field where AI possesses a significant and far-reaching impact for the future lies in the domain of communication security. AI is expected to be integrated with security services, not only to detect and mitigate attacks but also to enhance the robustness and reliability of systems against ever-growing threats and vulnerabilities. However, AI-based security has its own regulations and privacy concerns that should be met to avoid any misuse. Due to the rapid growth of AI usage in almost every field of communication systems, it has drawn keen interest in both academia and industry. However, AI-based systems are challenging. They raise various issues such as threats from AI-based attacks, privacy, and, more importantly, the collaboration of various independent networks, which play a vital role in future communication systems. The understanding and collaboration of multidisciplinary individuals will help shape AI-secured future communication systems. In this section, we highlighted the potential of AI-powered communication systems in the future communication landscape and its intersection across various research communities.

12.6.2. IoT and Smart Communication Solutions

While IoT holds a variety of definitions, the term broadly relies on a large network of interconnected things, devices, or machines that are equipped to directly communicate and respond to each other. Sometimes referred to as M2M communications, which is steadily optimized towards more sophisticated uses such as Smart City, among others. The technology, its services, and applications support a reduction of workload and process optimization for ideal communications. In the context of a Smart City, it enables people and devices to interact with other systems of a city appropriately.

In conjunction with the technological improvements in the communication world, IoT already provides a variety of significant advantages, such as remarkable data distribution from every nook. Furthermore, the sharing of valuable information minimizes operation costs by enhancing sufficient and secure access throughout the whole world. Moreover, it also supports network administrators to continually share up-to-date status of real-time monitoring systems. A huge amount of IoT applications can be seen in various fields such as healthcare, industry, urbanization, and many more. It is assumed to contain a wide range of modernized devices and gadgets that are designed for holding different

purposes for real-world applications. With the advanced features, IoT has capabilities that can effectively be implemented in numerous forms such as U-Health, U-Vehicle, U-City, U-Transport, and Ultra-Market Healthcare. Standardization and the creation of compatible algorithms between the makers and users constitute a significant challenge. It therefore can be pronounced as a globally distributed solution. One of the most remarkable approaches is U-Healthcare, an integration of healthcare and IoT that is administered in a home hospital which ideally focuses on sick and senior people. Interconnected massive amounts of collected data are exchanged for further process communication and adapted network infrastructures. Officially, IoT technology is considered one of the next thrillers for future communications solutions that can influence a revolutionary change in the behavior of human life. What more can assure a flabbergasting upward swing of the future communication world? Communication over IoT is rapidly advancing in several fields and draws substantial attention as a perspective for the upcoming modernized world.

12.6.3. Blockchain for Secure Transactions

Blockchain is a digital public ledger in which cryptography authenticates a list of transactions, making them permanent and unchangeable without a chain of new blocks. Major characteristics of blockchain include decentralization and immutability, which can ensure the authenticity of the data and enhance security in communication. In an insecure internet environment, blockchain is expected to create a trust mechanism and simplify trust in digital interactions, and it has been applied in automation processes and decentralized infrastructures for several real-world scenarios. Historically, blockchain technology was first used as an underlying data structure of Bitcoin, which has provided a range of motivations for a variety of transactions in cyberspace. However, the integration of blockchain in communication frameworks can be more complex. Transport protocols must be upgraded to use elliptically distributed cryptographic keys; routers must be able to process transactions by control and data planes; and edge networks and mobile devices must have the capability to host a public ledger.

Despite these apparent complexities, several researchers are trying to develop new blockchain systems by taking a key role in their enhancement. As blockchain technology has developed and its adoption has exploded, researchers are proposing multiple blockchain solutions for various purposes, from generic ones to those optimized for a specific class of applications. Such rapid development is assumed to continue in the future. In particular, systems that may enable scalable blockchain implementation are likely to be adopted in the coming years when the throughput deficiencies of the actual systems may lead to more regulation by reliable technologies. The most urgent

challenges that become research areas of their own are governance, coexistence among different distributed ledgers and/or DLTs, scaling data management, energy consumption, compliance by linking transactions with identities, and circular economy principles. An effective and efficient approach to implementing blockchain and a more systematic approach to designing a solution have yet to be established, offering opportunities for researchers to help communicate excellence. Nevertheless, there is a consensus that, in general, the successful application of a multiple-technology approach can enhance the assurance of security applications in a given domain and, therefore, that blockchain can be part of a secure end-to-end architecture for secure communications.

The security of underlying blocks and transactions is provided in many ways, with the establishment of a cryptocurrency. Nonce, for providing proof-of-work of Monero, and mining calculation is a common practice for securing the blockchain. For the PoW nonce, the blockchain should be entropy-length, which can be optimized. As such, the PoW can reduce the duration of the chain and lead to the selection of blocks in nominal conditions. All participants, with less than a 10−2 probability of launching an attack, would have less than 9% of the total hash power. Therefore, the PoW has proved to be considerably robust, as long as the difficulty level is sufficiently high. Consequently, more proofs are added. Other methods such as title-based signing, deposit-based PoS, and proof-of-burn were also highlighted relative to the other blockchain theories. Those are all related to cryptocurrencies. In addition, PoW contributed effectively to the use of Bitcoin.

12.7. Conclusion

Concluding Remarks and Recommendations

The essays in this Forum bring to light some exciting new potentialities for the secure and scalable communication system of 2040 and beyond. The contributions underscore the importance of secure and scalable communications and the pivotal role such systems will play towards the ongoing Fourth Industrial Revolution and in effectively tackling yet undefined future challenges.

Fig 12 . 3 : Future Secure Communication Systems (2040 and beyond)

They also concur that new computational and networking capabilities are making it possible today to contemplate the development of a communication and information infrastructure that is highly adaptive, reconfigurable, autonomous, and thus promises to enhance flexibility, agility, dependability, and security. Several technological elements are identified as archetypal candidates for acting as concealed "master trendsetters": artificial intelligence, the integration of the Internet of Things with communication networks, and new networking paradigms including blockchain and quantum-inspired networks. However, the coming age of communication intelligence is not unambiguously rosy. The essays briefly discuss some technically, societally, and economically complex challenges that deserve much attention in the years leading up to 2040.

Even with the expected rapid progress in the field of intelligent technology, several key requirements and goals remain largely unsolved. This includes developing new methods of learning and communicating securely, addressing the locus of trust issues, coordinating AI strategies, and developing, where necessary, new encryption technologies. Therefore, some form of "Final Report" Forum activities in 2040 and beyond could potentially serve as fruition points of what are bound to be continuing

discussions, research, and innovative input that must be constantly reinvested into intelligent digital infrastructure to ensure that it continues to evolve commensurately with the times.

12.7.1. Final Thoughts on the Evolution of Communication Technologies

Final Thoughts

Looking at human history, one easily concludes that the only permanent thing is change. This is valid for communication technologies as well. The first efforts to connect people living in remote places go back to ancient times. After learning to use fire, sails, and horses, ancient Egyptians managed to communicate at a distance using mirrors with reflected sunlight. As we all know, progress has never stopped; with costs going down and performance going up, the capacity and reach of communication technologies are always experiencing progress. In times of the Internet, blockchain, 5G wireless, and Web3, the only useful belief is adaptability to fast technological changes. The co-evolution of innovation in terms of technologies and communication infrastructures provided by the computer and networking industries and the requirements of society, the economy, education, as well as industrial and service applications have been the driving forces for mutual success, and the same rationale and expectation should apply to these proposed research directions.

Certainly, we may experience a promising future in the area provided the proposed scenarios of the future and eye-catching hypotheses are right at the proper time. Neuro-symbolic reasoning, human-centered AI, research related to AI fairness, accountability, and transparency, functional intelligent materials, AI-augmented quantum mechanics, proteome prediction, in vivo microbial therapies, learning with less labeled data, meta-metalanguage reimaginings, or other breakthroughs in intelligent technologies can make such scenarios realistic. Thus, it is our belief in a successful future in communication if the corresponding concepts and technologies are seriously considered today. Instead of taking the stance that these breakthroughs are still far away and not worth worrying about or exciting the present, the proposed scenario for a wonderful world enabled by intelligent technologies should receive all of our interest. We should then align our path to get there. We should no longer hold a passive voice in the advancements of any technology, let alone communication. After all, in more than a few hundred years of advancement in communication, societies have seen both positive and negative shifts as exponential advancements minimize the time for society to reflect on the ethical implications of new technologies. Recognizing the societal changes that may occur with intelligent technologies will require interdisciplinary collaboration and teamwork,

sharing of best practices, and increased exposure to our research community and other non-technical domains such as humanities, arts, and social science.

References

Raza, U., & Hossain, E. (2020). *Intelligent Networks for Secure and Scalable Communications in 5G and Beyond: A Survey.* IEEE Access, 8, 171236–171254. https://doi.org/10.1109/ACCESS.2020.3025287

Wang, L., & Zhang, J. (2021). *Converging Intelligent Technologies for Securing and Scaling Future Communication Systems: From 5G to 6G.* Journal of Communications and Networks, 23(1), 1–15. https://doi.org/10.1109/JCN.2021.000013

Zhang, H., & Li, Z. (2019). *The Role of AI and Blockchain in Secure and Scalable Communication Networks: Prospects for the Future.* Future Generation Computer Systems, 97, 291–300. https://doi.org/10.1016/j.future.2019.03.048

Zeng, M., & Zhao, Z. (2020). *Artificial Intelligence and Cloud Computing for Secure Communication: Trends and Challenges in Next-Generation Networks.* Computer Networks, 175, 107258. https://doi.org/10.1016/j.comnet.2020.107258

Zhang, Y., & Wu, Y. (2021). *Intelligent Automation for Secure and Scalable Communications in the Era of 5G and Beyond.* IEEE Communications Magazine, 59(3), 92–98. https://doi.org/10.1109/MCOM.001.2000151