Digital Communications and Networks 6 (2020) 281–291

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Security and privacy in 6G networks: New areas and new challenges

Minghao Wang [a], Tianqing Zhu [a,*], Tao Zhang [a], Jun Zhang [b], Shui Yu [a], Wanlei Zhou [a]

[a] School of Computer Science, University of Technology Sydney, Ultimo, 2007, Australia
[b] School of Software and Electrical Engineering, Swinburne University of Technology, Australia

ARTICLE INFO

Keywords:
6G
Cyber security
Privacy preservation
Communication

ABSTRACT

With the deployment of more and more 5g networks, the limitations of 5g networks have been found, which undoubtedly promotes the exploratory research of 6G networks as the next generation solutions. These investigations include the fundamental security and privacy problems associated with 6G technologies. Therefore, in order to consolidate and solidify this foundational research as a basis for future investigations, we have prepared a survey on the status quo of 6G security and privacy. The survey begins with a historical review of previous networking technologies and how they have informed the current trends in 6G networking. We then discuss four key aspects of 6G networks – real-time intelligent edge computing, distributed artificial intelligence, intelligent radio, and 3D intercoms – and some promising emerging technologies in each area, along with the relevant security and privacy issues. The survey concludes with a report on the potential use of 6G. Some of the references used in this paper along and further details of several points raised can be found at: security-privacyin5g-6g.github.io.

1. Introduction

Even though the era of the 5G network has not yet fully arrived, the limitations of 5G technology mean we must begin with researching 6G networks now. In fact, in March 2019, the world's first 6G summit was held in Finland, where the world's top communications experts drafted together with the first-ever 6G white paper. With this act, 6G networking as a field of research was unofficially born. Since then, more and more governments and organizations have announced the introduction of their research projects into the 6G network. For example, the UK government has announced its intention to invest in techniques and technologies with potential uses in 6G networks [1], while the Academy of Finland has announced the launch of a research project named "6 Genesis", which focuses on foundational research.

But what is a 6G network? And how will it differ from 5G networks? So far, the 6G network has no standard functions or specifications, just many possibilities. Some people contend that 6G networks should be more than just a faster version of a 5G network, but rather the improvement of the 5G technology in all aspects. For example, coverage should not be limited to the ground level, as is the case with the 5G network. Instead, it should provide full space undersea surface coverage. The 6G network should also have much higher Artificial Intelligence (AI) capabilities. In fact, in the view of many researchers, the 6G network should be an "AI-empowered" network, meaning AI is both its driver and most prominent feature [2]. It should not merely use AI in its architecture as the 5G network does. The 6G network should be a deep integration of currently emerging AI tools and networking functions. Moreover, as issues on the security and privacy of networks have become increasingly important in recent years, risk mitigation should be an integral component of the architecture [3]. Therefore, in this paper, we will discuss the possible additions to the 5G network that could come together to make up the 6G network, along with the security and privacy challenges associated with each key technology and potential applications for 6G networks going forward. The topics discussed in this survey and how they relate to each other are illustrated in Fig. 1.

The circles in Fig. 1 indicate the four key components of a 6G network, which include real-time intelligent edge, distributed AI, intelligent radio, and 3D intercoms. We chose these four areas as our focus because they cover the most powerful part of the 6G study that is being conducted so far. They are also subject to the most security and privacy concerns. The technologies involved in the present research include the AI-based software, the molecular communications, the quantum communications, the blockchain, the TeraHertz (THz) technology, and the Visible Light Communication (VLC) technology. As denoted in squares in

* Corresponding author.
E-mail addresses: minghao.wang@student.uts.edu.au (M. Wang), tianqing.zhu@uts.edu.au (T. Zhu), tao.zhang-3@student.uts.edu.au (T. Zhang), Junzhang@swin.edu.au (J. Zhang), shui.yu@uts.edu.au (S. Yu), wanlei.zhou@uts.edu.au (W. Zhou).

https://doi.org/10.1016/j.dcan.2020.07.003
Received 15 April 2020; Received in revised form 7 July 2020; Accepted 8 July 2020
Available online 15 July 2020

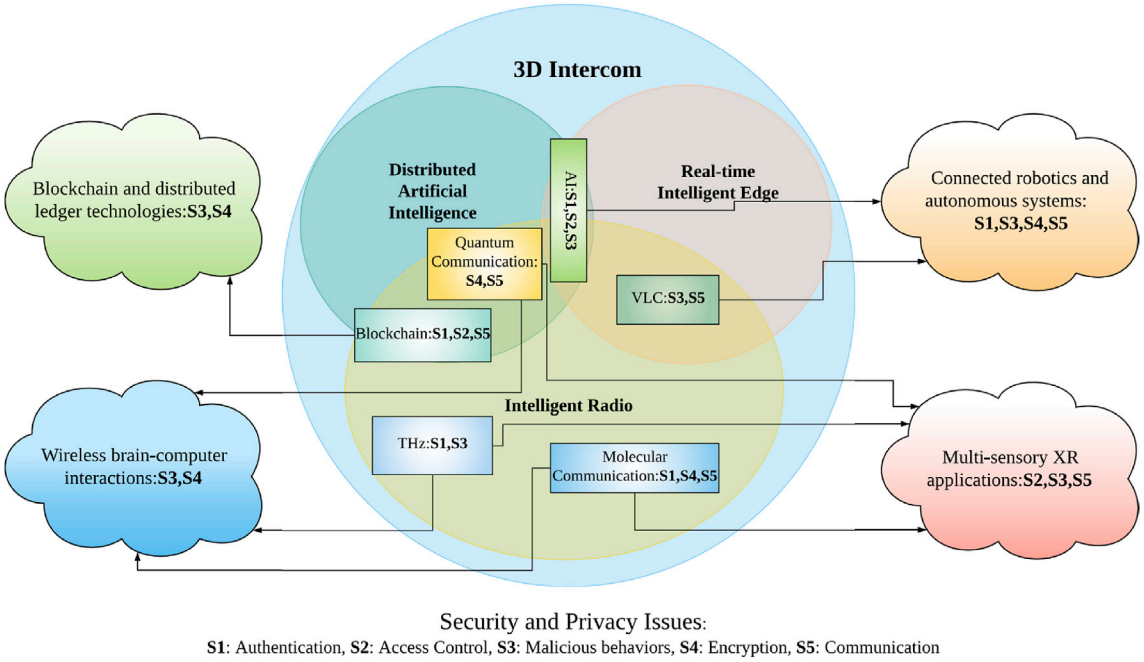

Fig. 1. Security and privacy issues in the 6G network.

Fig. 1, all these technologies hold great promise for use in various 6G network applications, such as multi-sensory X Reality (multi-sensory XR) applications, connected robotics and autonomous systems, wireless brain-computer interactions, and blockchain and distributed ledger technologies. These are shown as clouds in Fig. 1.

The first three areas, namely, the distributed AI area, the real-time intelligent edge area and the intelligent radio area, contain intersecting technologies. Moreover, AI exists at the intersection of all three areas because we assume that 6G networks will be AI-empowered.

The five main security and privacy issues are listed below the diagram. Most components of this diagram are vulnerable to authentication, access control, and malicious behavior. However, some technologies are particularly sensitive to certain issues. For example, the VLC, together with both real-time intelligent edge and intelligent radio, is particularly weak against malicious behavior and data transmission process. The molecular communication and the THz technology both support intelligent radio. The molecular communication technology is associated with security and privacy issues concerning authentication, encryption and communication, while the THz technology especially suffers from authentication security and malicious behavior. The blockchain technology and the quantum communication overlap with distributed artificial intelligence and intelligent radio. The main security and privacy concerns here relate to authentication, access control, data transmission and encryption.

6G applications also have specific vulnerabilities. The connected robotics and autonomous systems typically rely on the AI and the VLC technology where malicious behavior, encryption and data transmission can be problematic. The multi-sensory XR applications use the molecular communication technology, the THz technology and the quantum communication technology, which means they are susceptible to access control attacks, malicious behavior, and data transmission exposure. Wireless brain-computer interactions use the same techniques as the multi-sensory XR application, but have their own unique security and privacy issues. Malicious behavior and encryption are the main weaknesses. As the last applications of the 6G network, the blockchain and distributed ledger technologies (mainly based on blockchain) are relatively safe, but they may still be the target of malicious behaviors.

Overall, these new areas are prone to five main types of security and privacy issues: authentication, access control, malicious behavior, encryption and data transmission, which are hereafter denoted as S1, S2, S3, S4 and S5, respectively. More details on how these issues affect the various aspects of the 6G network, as well as measures to mitigate the risks, are presented in Sections III, IV and V, respectively.

Hence, the key contributions of this survey can be summarized as follows:

1) The security and privacy issues in the key areas of the 6G network are identified and presented.
2) Promising key technologies to support 6G networks are outlined, along with a detailed explanation of the security and privacy issues relating to these technologies.
3) An overview of new security and privacy issues particular to 6G networks is provided and discussed.

The remainder of this paper is structured as follows: Section II presents a brief overview of the technological milestones from 1G to 5G to illustrate the historical development of these networks. Then, in Section III, we describe the four main areas of the 6G network. The key technologies of the 6G network are discussed in Section IV, and, in Section V, we present several 6G applications. Sections III, IV and V also contain a breakdown of the security and privacy issues associated with each of the topics covered. Finally, the paper concludes in Section VI.

2. Overview: 1G to 5G

In this section, we provide a high-level overview of the evolution of security and privacy in wireless networks from first-generation technology standard for cellular networks (1G) to fifth-generation technology standard for cellular networks (5G), as shown in Fig. 2.

2.1. 1G

The 1G network was introduced in the 1980s and designed for voice services. It relies on analog signals to transmit information and has no established wireless standard. This leads to many disadvantages, including hard handovers, a lack of security and privacy guarantees, and

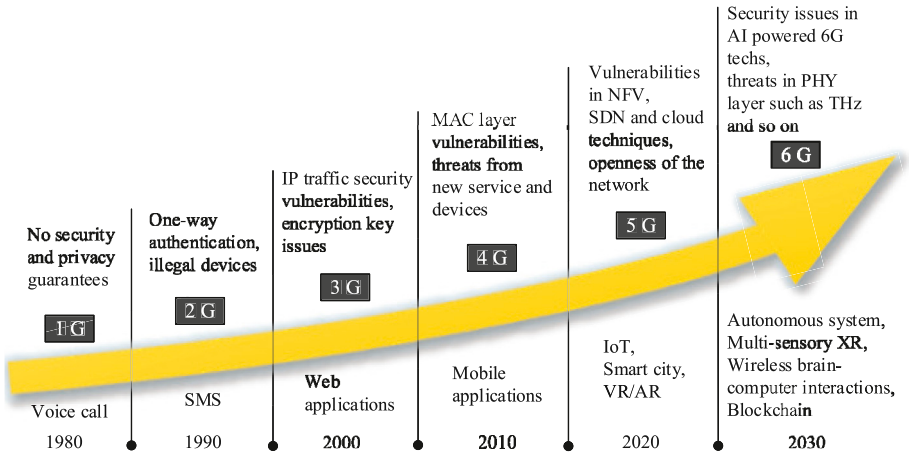

Fig. 2. Evolution of security and privacy issues in wireless systems.

low transmission efficiency. Phone services are not encrypted, meaning that data transmissions and phone conversations can neither be secure nor private. As a result, the entire network and its users face significant security and privacy challenges, including cloning, eavesdropping, and illegal access [4–6].

2.2. 2G

The 2G network is based on digital modulation techniques, such as Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA), which can support both voice and short message services. The most important and widely used mobile communication standard in 2G is GSM (Global System for Mobile Communications) [7].

The purpose of the GSM is to make the system as secure as a Public Switched Telephone Network (PSTN). Its security and privacy services include: 1) anonymity, 2) authentication, 3) signaling protection, and 4) user data protection [8]. Anonymity is achieved through the use of temporary identifiers, which make it difficult to track the user's real identity. However, the real identity must be used when the device is first switched on, after which a temporary identifier is issued. Authentication is mostly used by network operators to identify users. The authentication mechanism is an encryption-based approach referred to as "challenge and response". Signaling and user data protection are also implemented using encryption, and the Subscriber Identity Module (SIM) plays an important role in the encryption keys. There are two main methods for preserving privacy for users: the first is radio path encryption, and the second is Temporary Mobile Subscriber Identity (TMSI) [9].

However, despite the great improvements in security and privacy over 1G, 2G still suffers from many weaknesses. One important security issue is that the authentication is one-way; the network authenticates the user, but users cannot authenticate the network, which results in security holes. Illegal devices, such as base stations, can disguise themselves as legitimate network members, deceiving users and stealing their information [10]. Moreover, the encryption is not end-to-end. Only part of the wireless channel is encrypted, and there is also no encryption in the fixed network, which provides adversaries with an opportunity for attack [11]. In terms of privacy, the radio path encryption and TMSI have some limitations and are exposed to various types of attacks, such as eavesdropping.

2.3. 3G

The 3G network emerged in 2000 to provide "high-speed" data transmission and access to the internet, which means at least 2 Mbps. However, this speed could support advanced services that are not possible in the 1G and 2G networks, including web browsing, TV streaming, and video services [12].

The security of the 3G system is based on the 2G technologies. That is to say, GSM and other elements incorporated in 2G proved to be necessary, while additional robust security elements also needed to be adopted. The 3G also reduces some of the security weaknesses of the 2G and introduces the Authentication and Key Agreement (AKA) as well as two-way authentication. Moreover, the 3rd Generation Partnership Project (3GPP) provides a complete security system governing access that comprises two parts: air interface security, which is mainly used to protect users and the signaling information transmitted by wireless links; and the provision of user network authentication to ensure the physical reliability of users and both sides of the network. In terms of privacy, 3GPP incorporates some subscriber privacy requirements for 3G users, such as confidentiality of user identity, location and traceability.

However, the 3G networks are still vulnerable to threats associated with the Internet Protocol (IP) traffic and encryption keys. Further, the radio interface between the terminal equipment and the service network also provides opportunities for a set of attacks. Threats related to wireless interface attacks fall into the following categories: 1) unauthorized access to data; 2) threats to integrity; 3) Denial of Service (DOS); 4) unauthorized access to services [13]. Privacy issues are mostly related to certain types of attacks, such as AKA error messages, designed to destroy user identities and confidential or sensitive information.

2.4. 4G

The 4G of Long-Term Evolution (LTE) networks were introduced in 2009, providing the data rate of up to 1 Gbit/s on the downlink and up to 500 Mbits/s on the uplink. These networks provide better spectrum efficiency and reduced latency, which means they can meet the requirements of advanced applications, such as Digital Video Broadcasting (DVB), High Definition Television (HD TV) content and video chat. The LTE integrates a mix of existing and new technologies, such as Coordinated Multi-Point Transmission and Reception (CoMR), Multiple Input Multiple Output (MIMO) and Orthogonal Frequency Division Multiplexing (OFDM) [14].

Examples of 4G systems include IP backbone networks, wireless core networks, wireless access networks, and smart mobile terminals. Therefore, the relevant security threats mainly come from these areas: wireless link security issues, eavesdropping, tampering, insertion, or deletion of data, and network entity authentication issues, both wireless and hard-wired among others [15].

The 4G network is more vulnerable to security and privacy threats than the previous networks because users interact more closely with mobile terminals. As participants of all wireless protocols and executors of various wireless applications, interactions via 4G become more complex, and threats become more widespread. Moreover, due to

improvements of computing and storage capabilities of mobile terminals, an increasing number of malicious programs can be executed, which may cause more damage. Typical examples include viruses, tampering with hardware platforms, operating system vulnerabilities, etc. In addition, due to defects in key management protocols, the Worldwide Interoperability for Microwave Access (WiMAX) standards have some MAC layer vulnerabilities, such as DoS, eavesdropping, and replay attacks. The LTE networks are also vulnerable to DoS attacks, data integrity attacks, illegal use of users and mobile devices, and Medium Access Control (MAC) layer location tracking [16].

2.5. 5G

As we stand on the brink of the 5G network, we can look forward to faster speeds, more complete systems, and more secure architectures [6]. The main advancement of 5G networks is to facilitate the connection of an increasing number of devices and provide high-quality services for all devices simultaneously. Moreover, the supported devices will not be limited to smartphones; other devices like IoT equipment can also connect to the network [17,18].

The security and privacy issues in 5G networks can perhaps best be divided by network architecture and, more specifically, into three tiers of the architecture: the access networks, the backhaul networks, and the core network. In access networks, the diversity of nodes and access mechanisms give rise to some new security challenges as handovers between different access technologies increase the risk of attack.

As far as the backhaul network is concerned, backhaul communication occurs between the base station and the core network, which can be realized through wireless channels, microwaves and sometimes satellite links, as well as wired lines [19]. In the absence of connections between devices, these networks encounter fewer security and privacy threats than access networks. The vulnerabilities they do have come from adjusted elements of the access network, such as EUTRAN Node B (eNB) or the Mobility Management Entity (MME) in the core network, although the GPRS Tunnel Protocol (GTP) can provide some additional security guarantees. Moreover, the backhaul network is shifted into the data plane using Network Functions Virtualization (NFV) and Software-Defined Networking (SDN) techniques, so that security threats are also transmitted to the core network [20].

In 5G networks, the core network consists of functions [21]. NFV, SDN and cloud techniques make the networks more dynamic than before, which, again, gives rise to a greater suite of vulnerabilities. For example, a massive number of devices and services can overwhelm the signaling load, which leads to the increased possibility of a DoS or resource attack [22]. So far, two methods have been developed to address signaling overloads [23]. The first is to use lightweight authentication and key agreement protocols to support communication for a huge number of devices. The second involves using protocols that allow the devices to be grouped together through various group-based AKA protocols.

In terms of security, the new techniques used to improve the performance of the 5G network also create security holes [24]. For example, massive MIMOs help to disguise passive and active eavesdroppings. OpenFlow implementation of SDN increases threats from malicious applications or activities. Moreover, NFV raises security issues while a service or function is being migrated from one resource to another [25].

There are also new privacy issues to contend with due to the diversity of business types and application scenarios in 5G networks. The openness of the platform can mean that a user's sensitive information can easily and frequently change from a closed state to an open state. Accordingly, the contact state changes from offline to online, greatly increasing the risk of leaks. Therefore, the privacy issues we will inevitably face with 5G will become a problem that must be faced and solved in the next few years. Fortunately, advancements in data mining and machine learning technologies mean that privacy protection methods have been well trained and will only become more powerful in the future.

3. Key areas in 6G networks

Some components of the 5G network have already been considered, and some components have already deployed AI as their backbone, e.g., channel coding and estimation in the physical layer, multiple access in the MAC layer, and various applications in the network layer [26]. However, AI applications are not common, and the, the support for AI-driven technologies in 5G networks is limited by the constraints of the traditional architecture that was available in the early stages of its conception. Accordingly, there is no support for the distributed AI or the intelligent radio, as these two areas are fully AI-based. Moreover, although the real-time intelligent edge, such as vehicle networks, have already been implemented for 5G networks, emergency conditions cannot be handled in "real-time" due to latency issues. However, 6G networks can. For example, the radio latency of 6G networks is 0.1 ms, which is one-tenth of that of 5G networks [27]. Moreover, 5G coverage is still only at the ground level; space and underwater communications at some levels of 3D intercoms are not possible. Accordingly, in the following, we will describe how these four areas might advance in 6G networks. Of course, we also discuss the likely security and privacy issues we expect to face in these areas. A summary of the section is presented in Table 1.

3.1. Real-time intelligent edge

Vehicle and Unmanned Aerial Vehicle (UAV) networks cannot be implemented, even in the 5G network, because controlling the whole network requires extremely low network latency and real-time intelligence, and our current technology is limited. This is particularly true for vehicle networks. Although the 5G network already allows for the possibility of autonomous driving, and some are even already in use by AI-based cloud services, network entities with self-awareness, self-adaptation or prediction cannot be supported [28]. Accordingly, a new network that can handle these functions is required. A 6G network should be able to support such interactive AI-powered services. In vehicle networks, in particular, real-time intelligent edge could allow an autonomous driving response to an unfamiliar environment in real time [26]. Moreover, some new technologies, such as VLC, will be particularly useful in vehicle-to-vehicle communications [29]. When artificial intelligence

Table 1
Summary of key areas.

Key Areas	Summary	Characteristic	Relation to 6G
Real-time intelligent edge	Real-time intelligent edge could facilitate autonomous driving response to unfamiliar environments in real-time	Real-time response	Capability of control
Distributed artificial intelligence	The distributed artificial intelligence should be a sizeable decentralized system capable of making an intelligent decision at different levels	Make intelligent decision	Decision-making capacity
Intelligent radio	In an intelligent radio framework, transceiver algorithms could dynamically configure and update themselves based on hardware information	Self-adaptive	Be responsible for communication
3D intercoms	3D intercoms could provide services based on where and when they are needed. Coverage is not only at the ground level, but also at the space and undersea levels	Full 3D-cover	Be responsible for coverage

(more specifically machine learning) is deployed in vehicle networks, this technology will advance some basic security algorithms beyond machine learning. But it will also present some new security challenges. Tang et al. [30] mention that a vehicle network should consider not only the network environment, but also the physical environment because, to some extent, this may curtail the threat of malicious vehicles. Group behavior in clustered vehicles should also be considered. It is worth mentioning that a production-scale system for real-time AI to supplement a vehicle network is already in development.

3.2. Distributed AI

Whereas 5G networks are IoT-compliant, 6G networks will need to be IoE-compliant, i.e., the Internet of Everything (IoE). By nature, this means the 6G network will almost certainly be a sizeable decentralized system capable of making intelligent decisions at different levels [26]. Further, because absolutely everything in IoE is connected to the internet, distributed artificial intelligence will be needed that should satisfy multiple requirements. 1) The training data-set should be distributed unevenly over most of the edge devices, while every edge device should have the ability to access and control part of the data. The edge device should also be able to compute and store data independently. Also, it should be able to reduce dimensionality, clean data, and abstract data [31]. In this way, the shared data acts as a training set beyond its treatment as personal information. If this approach can be implemented correctly, it can even improve the security and privacy of the network.

Some security issues associated with distributed AI have already been identified. For example, a malicious user can update a poisoned model to taint the entire training model. There are also some security issues at the device level [32]. In addition, machine learning models should be improved to ensure data integrity [33], and the end-to-end security of communications and control would benefit from improvements [31]. Blockchain-like mechanisms are expected to solve some authentication issues for distributed ledger technologies [34], but more work is needed to help machine-learning models predict incoming attacks [35].

3.3. Intelligent radio

In previous generations of network, the devices and transceiver algorithms were designed together. As such, the networks' hardware capabilities, such as decoder computation, the number of antennas, etc. have remained quasi-static [2]. However, with recent developments in circuits and antennas, it has become possible to separate the hardware from the transceiver algorithms, which means intelligent radio could operate as a unified framework. Under this paradigm, the transceiver algorithms could dynamically configure and update themselves based on the hardware information [26].

Yang et al. [1] note that software-defined radio and networking techniques could be combined to leverage multiple high-frequency bands and dynamically utilize different frequencies, making support for intelligent radio possible. Huang et al. [2] have presented an operating system and interface language based on hardware information and AI methods in which the transceiver algorithms are configurable. It has also been argued that intelligent radio support should satisfy several requirements. For example, the frequency band should adapt to the environment and hardware; the spectrum sharing should be AI-enabled; hardware capabilities should be estimated online, and so on. Further, Jiang et al. [36] find evidence for some wideband interference and signal-jamming issues in the data transmission process that could threaten data security, while Tariq et al. [29] recommend that suspicious activities by malicious nodes should be able to be predicted during communication processes.

3.4. 3D intercoms

In 6G networks, network analysis, planning and optimization capabilities will need to be increased over previous network generations from two dimensions to three [37]. Accordingly, 6G networks must be able to support communications in 3D space to accommodate satellites, UAVs, and undersea communications. A 3D intercom could provide this service according to the location and time needed [34]. For example, when an emergency occurs in a remote area, deployment and response of UAV networks are more cost-effective than using 4G or 5G networks because the fixed infrastructure associated with these generations cannot be relocated. Adding the dimensions of altitude and associated degrees of freedom requires new network optimization to achieve mobility management, routing, and resource management in the 3D-intercom context [38].

At the space level, THz bands are currently being investigated and trialed, since satellites need to use regulated frequency bands [39]. Moreover, some new technologies, such as molecular communication and quantum communication, could be applied here due to their suitability for long-distance communication [29]. However, Wei et al. [40] caution that there are some security issues with the authentication process when using the Beidou navigation system. Yao et al. [41] propose a technology called Space-Terrestrial Integrated Network (STIN), which is a convergence of satellite communications, the internet, and mobile wireless networking. However, this approach is impacted by some unicast and multicast communication problems with key management.

At the aerial level, Zeng et al. [42] have discussed a "ghost control" scenario in which unauthorized agents control UAVs via spoofed controls or navigation signals. Gupta et al. [6] have discovered that one of the security mechanisms of the protocol used in the UAV handover scenario is too weak. In addition, Chen et al. [43] outlined an Android-based attack method that could be used to compromise any UAV running the Android system.

When it comes to coverage, the question of whether 6G networks could operate underwater remains controversial due to the complex nature of the undersea environment. However, Grimmett [44] is pioneering a discussion on some security issues associated with the transmission processes in undersea wireless acoustic communication networks. Thus, if it is confirmed that an undersea network will become part of the 6G network, more security issues will inevitably emerge in the future.

4. 6G technologies: security and privacy issues

As mentioned in the previous section, some key technologies are already proving useful in crucial areas of the 6G network. They are giving 6G networks high reliability, low latency, and secure and efficient transmission services. However, as also mentioned in the previous section, most of these technologies come at the cost of new security and privacy concerns. This is what we discuss in this section. An overview of the security and privacy issues associated with key 6G technologies is presented in Table 2.

4.1. AI

Compared with all other technologies expected to be used in 6G networks, AI is widely considered to be one of the key parts of the future network infrastructure. It is an understatement to say that artificial intelligence has attracted a lot of attention in the field of network. And with that attention, an increasing number of new security and privacy issues are emerging [59]. Although AI in the 5G network is ostensibly operated in isolated areas where massive amounts of training data and powerful but private computing hubs are available, AI will become more of a core component of the 6G network [29]. Once again, AI technologies can be divided into the architectural layers they serve [60]: the physical layers, which includes devices such as data links and network infrastructure; and the computing layers, which include software-defined networks, network function virtualization and cloud/edge/fog computing, etc. We discuss each in turn below.

Table 2
Overview of the main security and privacy issues in key 6G technologies.

Key technology	Ref	Security and privacy issues	Key technology contribution
AI	[33]	Access control	Fine-grained control processes
	[37]	Malicious behavior	Detect network anomalies and provide early warnings
	[45]	Authentication	An unsupervised learning method that could be used in the authentication process to enhance the security of the physical layers
	[46]	Communication	An antenna design based on machine learning that could be used in PHY layer communication to prevent information leaks
	[47]	Encryption	Machine learning and quantum encryption schemes
Molecular communication	[48]	Malicious behavior	An adversary disrupting molecular communication or its processes
	[49]	Encryption	A coding scheme that could enhance the security of data transmission
	[50]	Authentication	Provides direction for developing new authentication mechanisms
Quantum communication	[47]	Encryption	Mechanisms for protecting quantum encryption keys
	[51]	Communication	Different modes of quantum communication
Blockchain	[52]	Authentication	A new conceptual architecture for mobile service authorization
	[53]	Access control	A method that improves access protocols
	[54]	Communication	Using hashing power to validate transactions
THz	[55]	Authentication	Electromagnetic signatures as a method of authentication
	[56]	Malicious behavior	Even when a signal is transmitted via a narrow beam, it can still be intercepted by an eavesdropper
VLC	[57]	Communication	A secure protocol that can be used in the communication process
	[58]	Malicious behavior	Cooperating eavesdroppers can reduce security

4.1.1. Physical layers

Zhang et al. [60] presented several AI-based technologies, including deep neural networks, K-Means, and supervised/unsupervised learning, which could be used in different physical layers. Not only can these techniques improve the performance of physical layers by optimizing connectivity, but they also have the ability to predict traffic and enhance security. Sattiraju et al. [45] proposed an unsupervised learning method that could be used in the authentication process to enhance the security of the physical layer. Hong et al. [46] presented a machine learning-based antenna design that could be implemented in the physical layer communication to prevent information leaks. Also, Nawaz et al. [47] noted that machine learning and quantum encryption schemes could be used to protect the security of communication links in 6G networks.

4.1.2. Network architecture

In the aspect of network architecture, Loven et al. [33] propose that AI might improve edge security via security systems and fine-grained controls. Zhou et al. [61] also discuss AI technologies, claiming that more specific deep learning might be used to detect threats in edge computing. However, this notion requires further exploration.

4.1.3. Other functions

In addition to the physical layers and network architecture, AI is also useful in other respects, such as big data analysis, distributed AI, resource management, and network optimization. Dang et al. [37] contend that AI could help detect network anomalies and provide early warning mechanisms to improve the security of 6G networks. Tomkos et al. [31] further note that by using distributed and federated AI in a 6G network, the edge devices do not need to exchange data, which further enhances network security. Moreover, Zhang et al. [62] mention that the impact of data correlation in some machine learning algorithms might lead to an increase in privacy leaks, and Zhu et al. [63] discuss some algorithms based on differential privacy that could be suitable for solving some of 6G's privacy issues.

4.2. Molecular communication

Molecular communication is a natural phenomenon observed among living entities with nanoscale structures [64]. Due to the development of nanotechnology, bioengineering, and synthetic biology in the past decade, microscale and nanoscale devices are becoming a reality [48]. Moreover, the energy consumption associated with the generation and propagation of a molecular communication signal is very low. Although this phenomenon has been studied in biology for many years, it has only been a research topic in the field of communication for perhaps the last decade. The molecular communication technology is a very promising technology for 6G communications. However, it is an interdisciplinary technique and one that is still in its early stages. The key idea of molecular communication is to use biochemical signals to transmit information. Nakano et al. [65] presented a mobile molecular communication process that enables the sender, the receiver and the associated nodes to communicate while they are moving.

However, several security and privacy issues related to the communication, authentication and encryption process have already been found. Farsad et al. [48] argued that this type of communication channel could be disrupted by an adversary and that only a few studies have even considered the safety of molecular communication links. Lu et al. [49] presented a coding scheme capable of enhancing the security of the transmitted data. Moreover, Loscri et al. [50] proposed some potentially effective key directions for molecular communication that would promote the development of new authentication mechanisms to protect data security and privacy. These authors also discuss several attack methods at different levels of molecular communication, such as flooding attacks, jamming, and desynchronization. Yet, while it is clear that more time is required to develop practicable molecular communication mechanisms for the 6G network, this technology is expected to achieve what traditional communication methods cannot.

4.3. Quantum communication

Quantum communication is another communication technology with great application potential in 6G networks. One of its main benefits is that it can significantly enhance the security and reliability of data transmission. If an adversary eavesdrops on, measures or replicates anything in quantum communication, the quantum state will be affected. Therefore, it is not possible for the recipient to be unaware of the interference [60]. In theory, quantum communication could provide absolute security and, with the right breakthroughs, it should be highly suitable for long-distance communication. It offers many new solutions and elevates communications to a level that traditional communications systems are unable to reach [66].

However, quantum communication is not currently a panacea for all security and privacy issues. Although significant progress has been made in developing quantum cryptography for quantum communication, fiber attenuation and operation errors are making long-distance quantum communication a serious challenge. Hu et al. [51] conjecture that several different modes of quantum encryption and other techniques may be

required to ensure completely secure quantum communications, such as quantum key distribution, quantum secret sharing, quantum secure direct communication, quantum teleportation, and quantum dense coding. Moreover, Zhang et al. [67] present further information regarding the security of quantum secure direct communication, which can transmit secret messages directly via a quantum channel without using a private key. Nawaz et al. [47] have also discussed some of the quantum mechanisms that use quantum key distribution models to protect key security.

4.4. Blockchain

The Blockchain technology has many potential uses in a 6G network. Examples include network decentralization, distributed ledger technologies, and spectrum sharing. As Dang et al. [37] observe, network decentralization based on the blockchain technology could simplify network management and improve network performance. The same is true for the use of the blockchain in distributed ledger technologies, which would significantly enhance the security of authentication [34]. In fact, the blockchain may turn out to be one of the most disruptive Internet of Everything technologies [38]. Moreover, by deploying the blockchain technology in a spectrum sharing system, the problems of low spectrum utilization and spectrum monopoly could be overcome [60], while securing spectrum utilization at the same time.

Blockchain security and privacy issues are related to the access control, authentication, and communications processes. Ling et al. [68] discuss a blockchain radio access network architecture that could secure and effectively manage network access and authentication among trustless network entities, while Kiyomoto et al. [52] present a new conceptual architecture for mobile service authorization based on the blockchain technology. Kotobi et al. [53] further proposed a method of using the blockchain to improve the security of media access protocols and cognitive radio in order to gain access to the unused licensed spectrums. Moreover, even though the decentralized architecture of the 6G network means it would only be possible to alter records if more than 51% of the nodes were under the hacker's control (which means it is secure enough), there is no trusted third party responsible for secure data storage and management when security breaches occur [69]. Also, Ferraro et al. [54] mention that the hash capability required to validate transactions in a blockchain-based network may adversely affect security.

4.5. TeraHertz technology (THz)

Although mm-wave bands have been widely used in 5G networks, these bands are inadequate in the 6G context owing to the demand for high transmission rates. In any case, the Radio Frequency (RF) band is almost full and cannot be used for future technology [70]. These factors have spurred the development of terahertz technology. Terahertz communication uses the 0.1–10 THz band, which has more abundant spectrum resources than the mm-wave band. In addition, it exploits both electromagnetic waves and light waves [60]. Huang et al. [26] highlight several benefits of using the THz band. First, the THz communication technology may be able to support the data rate of 100 Gbps or higher. Second, because of the narrow beam and short pulse duration used in THz communication, eavesdropping would be limited, resulting in higher communications security. Third, the attenuation of THz waves through certain materials is very small, which means they could be used in a variety of unique applications. Moreover, THz communication transmission can be highly directional, which can significantly reduce intercell impact [60]. Perhaps most importantly, two types of THz physical layers have already been specified in IEEE 802.15.3d. Strianti et al. [34] observe that the energy consumption of the THz communication is an obvious problem. The size of 6G cells needs to change from "small" to "tiny", meaning that more complex hardware and architectures need to be designed [38].

Like other technologies, THz has its own security and privacy issues. These mainly focus on authentication and malicious behaviors. For instance, Akyildiz et al. [55] mention concepts such as the electromagnetic signature of THz frequencies, which might be used for authentication processes of the physical layer. Also, although the THz communication is widely believed to make eavesdropping difficult, Ma et al. [56] argue that an eavesdropper could still intercept a signal when it is transmitted via narrow beams. They do, however, discuss a way to resist this kind of eavesdropping attack.

4.6. Visible light communication (VLC)

Visible light communication technology is a promising approach that could be used to solve the growing demands for wireless connectivity [71]. Far from being in its inception stages, VLC has been studied for a number of years and has already been deployed in many areas, such as indoor positioning systems and the Vehicular Ad Hoc Network (VANET) network. Luo et al. [72], for example, have published hundreds of papers related to VLC-based positioning technology.

Compared with RF which has interference and high latency, VLC has higher bandwidths and can resist electromagnetic interference [73]. The development of solid-state lighting has also helped to advance VLC technology. For example, since LEDs can switch to different light intensities at a very fast rate, some researchers have attempted to use LEDs for high-speed data transmission [74]. Chen et al. [75] devised a VLC system named LiFi that supports multiple access and could potentially provide a large number of connected mobile users with high-speed services. However, there are also some deficiencies that hinder the development of VLC technology. For example, the main usage scenarios for VLC should be indoors, because strong natural light will affect transmissions.

The security and privacy issues related to VLC include malicious behaviors and communication processes. Pathak et al. [74] noted that if an attacker wants to launch an attack on an ongoing VLC operation, they must be in line-of-sight of the victim. Clearly, this would make the attacker easier for attackers to be detected. Ucar et al. [57] presented a SecVLC protocol that could be used in a vehicle network to protect the security of transmission data. Mostafa et al. [76] proposed a precoding technique for VLC links to enhance the security of the physical layer. Moreover, Cho et al. [58] have verified that the cooperation of eavesdroppers may reduce security in VLC technologies.

5. 6G applications: future research challenges

Every new era of network technology brings new and different applications. Although some applications from previous network generations will still be applied to 6G networks, the future application of the technologies outlined in Section V is exciting. In this section, we will review these possible developments and challenges that researchers are currently working on. A summary of 6G applications is shown in Table 3.

5.1. Multi-sensory XR applications

The high bandwidth and low latency of 5G networks have already improved the VR/AR experience of 5G users. However, there are still many problems in the application of impeding VR in 5G networks, which need to be solved in the 6G network. For example, cloud VR/AR services can already bring some immersive experiences to users, but latency is a significant problem, and the resulting ambiguity leads to more problems. Deploying VR/AR through cloud services makes it more portable and easier to access, but with 5G bandwidths, images need to be compressed, so transmitting enormous quantities of lossless images or videos in real-time will need to wait for the 6G network.

In 6G networks, the immersive experience of VR/AR will be further improved. Multiple sensors will be used to collect sensory data and provide feedback to users. Thus, the XR in 6G networks is likely to

Table 3
Overview of security and privacy issues in 6G Applications.

Applications	Ref	Security and privacy issues	Key contribution
Multi-sensory XR applica-tions	[77]	Communication	Treats the dynamics of the network to improve the security of the communication process
	[78]	Malicious behavior	A new scheme that could defend against eavesdropping
	[79]	Access control	A DOMA multiple-access method for managing access
Connected robotics and autonomous systems	[80]	Malicious behavior	Prevents WiFi-based attacks in autonomous drone networks
	[81]	Malicious behavior	Explores eavesdropping attacks, hijacking attacks, spoofing attacks and DoS attacks in autonomous drone systems
	[82]	Malicious behavior	Presents several attack methods via wireless networks to assault autonomous vehicles
	[83]	Encryption	A novel mathematical framework that could enhance the security of autonomous drone networks
	[84]	Communication	A unique communications method that could prevent eavesdropping attacks
	[85]	Authentication	A self-driving vehicle protocol that could support two-factor authentication
Wireless brain-computer interactions	[86]	Malicious behavior	Discusses hacking applications that may access neuroscience results
	[87]	Encryption	A password method that could prevent reply attacks in braincomputer interaction applications
Blockchain and distributed ledger technologies	[88]	Malicious behavior	Presents three types of malicious behaviors that could occur in blockchain-based 6G applications
	[88]	Encryption	Presents several cryptographic algorithms that could be used to enhance the security and privacy of blockchain

combine traditional Ultra-Reliable Low Latency Communications (URLLC) with enhanced Mobile BroadBand (eMBB), which could be referred to as Mobile Broad Bandwidth and Low Latency (MBBLL) [35].

The outstanding security and privacy issues with URLLC and eMBB in multisensory XR applications include malicious behavior, access control, and internal communication. Chen et al. [89] argue that the security of an ultra-low latency network needs to be improved by addressing the dynamics of the network. Chen et al. [77] also note that in a few applications of URLLC, some attacks are still difficult to defend against, so it is still possible to leak critical and confidential information. However, Hamamreh et al. [78] have made progress in eavesdropping and proposed a technique to enhance the security against this type of attack on URLLC services. Moreover, Al et al. [79] have devised a new multiple-access method, called DOMA, that could be used in multisensory XR applications given the capacity for mass access to XR devices in the 6G network.

Yet Dang et al. [37] stress that the security, secrecy and privacy of eMBB should be given more attention. Likewise, Yamakami et al. [90] describe a 3-dimensional model of privacy threats in XR applications as a roadmap for the issues researchers should be addressing. And Pilz et al. [91] mention that multisensory XR applications could control the verticals themselves to protect internal security and privacy.

5.2. Connected robotics and autonomous systems

The second application of the 6G network is the connected robotics and autonomous systems. Autonomous driving is a key application in 5G networks. In 6G networks, however, autonomous driving alone is far from sufficient – a more comprehensive autonomous system is required. In addition to the driving mechanics, the autonomous system should contain a multi-dimensional network. Moreover, this system should embed not only intelligence across the whole network, but also the logic of AI into the network structure [26]. This would enable all internal components to be automatically controlled and connected via AI by us.

Strianti et al. [34] discuss “industry 4.0”, which refers to reducing human intervention in industrial processes through the use of automatic control systems. These authors also envisioned an automated factory capable of automatically handling the communications, computations, caching and resource control of an entire system. In this scenario, the automated factory contains not only mobile inspectors and actuators, but also UAV networks, databases and cloud services, making it a truly complete autonomous system.

The security and privacy issues related to these two applications are discussed separately below.

5.2.1. Autonomous drone systems

Although it has not been possible so far to fully deploy an autonomous drone system owing to the limitations of 5G networks, 6G networks could unlock the full potential of such systems. However, there are also some attacks against these systems. Li et al. [92] highlight that the SDN controllers used to manage and control UAV networks are easy targets. Hooper et al. [80] mention a WiFi-based attack, which could be used by a Tiro adversary. Fotouhi et al. [81] continue to note that eavesdropping attacks, hijacking attacks, spoofing attacks and DoS attacks can also occur in autonomous drone systems. Accordingly, corresponding security protection mechanisms are needed. Challita et al. [93] propose an artificial neural network-based scheme that could ensure secure real-time operations in autonomous drone systems. Sanjab et al. [83] present a novel mathematical framework that could be used to analyze and enhance the security of autonomous drone networks, while Sun et al. [84] present a unique communication method that could prevent eavesdropping attacks. Kim et al. [94] propose a privacy-preserving framework that could be used to manage permission issues in UAV networks.

5.2.2. Autonomous driving systems

The security and privacy issues in autonomous driving systems involve several different elements, for example, system-level privacy and security issues, location privacy, vulnerable energy consumption systems. Xu et al. [95] propose an Efficient and Privacy-preserving Truth Discovery (EPTD) approach for smart autonomous driving systems to protect users’ security and privacy. Ni et al. [85] mention a protocol for self-driving vehicles that could support two-factor authentication with mutual traceability for reducing the risk of vehicle theft and also preventing privacy leaks. Ding et al. [96] present a novel fuel-efficient path-planning framework that could solve energy consumption problems in autonomous driving systems. Wang et al. [82] warn that hackers could use wireless network attacks to assault autonomous vehicles using methods such as brute force cracks and packet capture. Moreover, Tang et al. [30] present a full-scale survey of various machine learning techniques.

5.3. Wireless brain-computer interactions

Wireless Brain-Computer Interaction (BCI) is not a new technology, but after two decades of development, it has matured. The key idea behind wireless BCI is to build a connection between the brain and a device. The device can be located inside the body (such as the visual cortex) or outside (such as an artificial limb). Typically, this involves four steps: signal acquisition, feature extraction, feature translation, and

feedback. Until recently, the main applications of wireless BCI were related to health, mainly focusing on helping disabled people control auxiliary equipment. However, in 2015, Chen et al. [97] presented a new approach to BCI designed to help speed up spelling via brain signals. With the coming of 6G networks, wireless BCI is anticipated to find more applications. Although somewhat similar to XR applications, wireless BCI applications are typically more sensitive to physical perceptions and need a guarantee of "Quality-of-Physical-Experience" (QoPE) [38].

The security and privacy issues raised by wireless BCI technology mostly concern malicious behavior and encryption. Mccullagh et al. [98] emphasize that data security is one of the main challenges in wireless BCI, while Ramadan et al. [86] suggest that some hacking applications could be developed to access highly-sensitive neurological information. Interestingly, Vsvogor et al. [87] proposed a password method that requires the user to enter a certain psychological state to prevent reply attacks. The protection method of Karthikeyan et al. [99] not only improves the already impressive features of wireless BCI, but also enhances security levels.

5.4. Blockchain and distributed ledger

Since the blockchain technology shares data with all involved stakeholders [24], it is likely to be used for spectrum and data sharing, thus significantly enhancing the security of 6G networks.

However, some of these issues remain particularly malicious. Nguyen et al. [88] mention three types of malicious behavior attacks: most vulnerability attack, transaction privacy leakage attacks, and double-spending attacks. They also propose several blockchain-based solutions to solve these issues in 6G networks, such as incentive strategies, cryptographic algorithms, and so on. Dai et al. [100] note that while some types of blockchains have low security, such as private blockchains, there are still some high-level security blockchains, such as consortium blockchains, which can be used for secure resource transactions. A comprehensive survey of the blockchain security can be found in Ref. [101], to which we recommend interested readers to refer.

6. Conclusion

With the 5G network research phase coming to an end and soon to be deployed, 6G networks have become the agenda of many researchers. The 6G network will undoubtedly bring network service to a higher level than those of previous generations. In this paper, we conducted a detailed investigation into the security and privacy issues related to 6G networks. First, we presented an overview of the milestones from 1G to 5G, laying a foundation for the development of the 6G network. We then examined four key areas of the 6G network to uncover the security issues related to tomorrow's technologies. The investigation concludes with a discussion of the potential applications that the 6G network will support. We hope that this discussion will stimulate people's interest and further research on 6G network security and privacy issues.

Acknowledgments

This work was supported by an ARC Linkage Project (LP180101150) from the Australian Research Council, Australia.

References

[1] P. Yang, Y. Xiao, M. Xiao, S. Li, 6g wireless communications: vision and potential techniques, IEEE Network 33 (4) (2019) 70–75.
[2] K.B. Letaief, W. Chen, Y. Shi, J. Zhang, Y.-J.A. Zhang, The roadmap to 6g: Ai empowered wireless networks, IEEE Commun. Mag. 57 (8) (2019) 84–90.
[3] T. Zhu, P. Xiong, G. Li, W. Zhou, S. Y. Philip, Differentially private model publishing in cyber physical systems, Future Generat. Comput. Syst..
[4] P. Chandra, D. Bensky, T. Bradley, C. Hurley, S.A. Rackley, J. Rittinghouse, J.F. Ransome, C. Cism, T. Stapko, G.L. Stefanek, et al., Wireless Security: Know it All, Newnes, 2011.
[5] I. Union, Imt traffic estimates for the years 2020 to 2030, Report ITU-R M. 2370–0, ITU-R Radiocommunication Sector of ITU.
[6] L. Gupta, R. Jain, G. Vaszkun, Survey of important issues in uav communication networks, IEEE Commun. Surv. Tutorials 18 (2) (2015) 1123–1152.
[7] G. Arunabha, J. Zhang, J. G. Andrews, R. Muhamed, Fundamentals of Lte, The Prentice Hall communications engineering and emerging technologies series.
[8] C. Brookson, Gsm security: a description of the reasons for security and the techniques, in: IEE Colloquium on Security and Cryptography Applications to Radio Systems, 1994, 2/1–2/4.
[9] S. Gindraux, From 2g to 3g: a guide to mobile security, in: Third International Conference on 3G Mobile Communication Technologies, IET, 2002, pp. 308–311.
[10] G. Cattaneo, G. De Maio, U.F. Petrillo, Security issues and attacks on the gsm standard: a review, J. UCS 19 (16) (2013) 2437–2452.
[11] M. Toorani, A. Beheshti, Solutions to the gsm security weaknesses, in: 2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies, IEEE, 2008, pp. 576–581.
[12] P. Sharma, Evolution of mobile wireless communication networks-1g to 5g as well as future prospective of next generation communication network, Int. J. Comput. Sci. Mobile Comput. 2 (8) (2013) 47–53.
[13] M. C. Chuah, Universal mobile telecommunications system (umts) quality of service (qos) supporting variable qos negotiation, uS Patent 7,668,176 (Feb. 23 2010)..
[14] U. Varshney, 4g wireless networks, IT Prof. 14 (5) (2012) 34–39.
[15] J. Cao, M. Ma, H. Li, Y. Zhang, Z. Luo, A survey on security aspects for lte and lte-a networks, IEEE Commun. Surv. Tutorials 16 (1) (2013) 283–302.
[16] N. Seddigh, B. Nandy, R. Makkar, J.-F. Beaumont, Security advances and challenges in 4g wireless networks, in: 2010 Eighth International Conference on Privacy, Security and Trust, IEEE, 2010, pp. 62–71.
[17] R.N. Mitra, D.P. Agrawal, 5g mobile technology: a survey, ICT Express 1 (3) (2015) 132–137.
[18] N. Panwar, S. Sharma, A.K. Singh, A survey on 5g: the next generation of mobile communication, Phys. Commun. 18 (2016) 64–84.
[19] M. Jaber, M.A. Imran, R. Tafazolli, A. Tukmanov, 5g backhaul challenges and emerging research directions: a survey, IEEE Access 4 (2016) 1743–1766.
[20] J. Prados-Garzon, O. Adamuz-Hinojosa, P. Ameigeiras, J.J. Ramos-Munoz, P. Andres-Maldonado, J.M. Lopez-Soler, Handover implementation in a 5g sdn-based mobile network architecture, in: 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE, 2016, pp. 1–6.
[21] J. Kim, D. Kim, S. Choi, 3gpp sa2 architecture and functions for 5g mobile communication system, ICT Express 3 (1) (2017) 1–8.
[22] N. Alliance, 5g security recommendations package, White paper.
[23] P. Bisson, J. Waryet, 5g Ppp Phase1 Security Landscape, 5G PPP Security Group White Paper.
[24] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, M. Ylianttila, Security for 5g and beyond, IEEE Commun. Surv. Tutorials 21 (4) (2019) 3682–3722.
[25] M. Pattaranantakul, R. He, Q. Song, Z. Zhang, A. Meddahi, Nfv security survey: from use case driven threat analysis to state-of-the-art countermeasures, IEEE Commun. Surv. Tutorials 20 (4) (2018) 3330–3368.
[26] T. Huang, W. Yang, J. Wu, J. Ma, X. Zhang, D. Zhang, A survey on green 6g network: architecture and technologies, IEEE Access 7 (2019) 175758–175768.
[27] M. Latva-aho, K. Leppanen, Key Drivers and Research Chal¨ Lenges for 6g Ubiquitous Wireless Intelligence (White Paper), 6G Flagship Research Program, University of Oulu, Finland.
[28] M.G. Kibria, K. Nguyen, G.P. Villardi, O. Zhao, K. Ishizu, F. Kojima, Big data analytics, machine learning, and artificial intelligence in next-generation wireless networks, IEEE Access 6 (2018) 32328–32338.
[29] F. Tariq, M. Khandaker, K.-K. Wong, M. Imran, M. Bennis, M. Debbah, A Speculative Study on 6g, arXiv Preprint arXiv:1902.06700.
[30] F. Tang, Y. Kawamoto, N. Kato, J. Liu, Future intelligent and secure vehicular network toward 6g: machine-learning approaches, Proc. IEEE.
[31] I. Tomkos, D. Klonidis, E. Pikasis, S. Theodoridis, Toward the 6g network era: opportunities and challenges, IT Prof. 22 (1) (2020) 34–38.
[32] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, et al., Communication-efficient learning of deep networks from decentralized data, arXiv Preprint arXiv: 1602.05629.
[33] L. Loven, T. Lepp´anen, E. Peltonen, J. Partala, E. Harjula, P. Porambage, M. Ylianttila, J. Riekki, Edge Ai: A vision for distributed, edge-native artificial intelligence in future 6g networks, The 1st 6G Wireless Summit, 2019, pp. 1–2.
[34] E. C. Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Ktenas, N. Cassiau, C. Dehos, 6g: the Next Frontier, arXiv´ Preprint arXiv:1901.03239.
[35] G. Gui, M. Liu, F. Tang, N. Kato, F. Adachi, 6g: opening new horizons for integration of comfort, security and intelligence, IEEE Wireless Commun..
[36] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, L. Hanzo, Machine learning paradigms for next-generation wireless networks, IEEE Wireless Commun. 24 (2) (2016) 98–105.
[37] S. Dang, O. Amin, B. Shihada, M.-S. Alouini, What should 6g be? Nat. Electron. 3 (1) (2020) 20–29.
[38] W. Saad, M. Bennis, M. Chen, A vision of 6g wireless systems: applications, trends, technologies, and open research problems, IEEE network.
[39] M. Katz, P. Pirinen, H. Posti, Towards 6g: getting ready for the next decade, in: 2019 16th International Symposium on Wireless Communication Systems (ISWCS), IEEE, 2019, pp. 714–718.

[40] Y. Wei, H. Liu, J. Ma, Y. Zhao, H. Lu, G. He, Global voice chat over short message service of beidou navigation system, in: 2019 14th IEEE Conference on Industrial Electronics and Applications (ICIEA), IEEE, 2019, pp. 1994–1997.
[41] H. Yao, L. Wang, X. Wang, Z. Lu, Y. Liu, The space-terrestrial integrated network: an overview, IEEE Commun. Mag. 56 (9) (2018) 178–185.
[42] Y. Zeng, R. Zhang, T.J. Lim, Wireless communications with unmanned aerial vehicles: opportunities and challenges, IEEE Commun. Mag. 54 (5) (2016) 36–42.
[43] X. Chen, C. Li, D. Wang, S. Wen, J. Zhang, S. Nepal, Y. Xiang, K. Ren, Android hiv: a study of repackaging malware for evading machine-learning detection, IEEE Trans. Inf. Forensics Secur. 15 (2019) 987–1001.
[44] D.J. Grimmett, Message routing criteria for undersea acoustic communication networks, in: OCEANS 2007-Europe, IEEE, 2007, pp. 1–6.
[45] R. Sattiraju, A. Weinand, H. D. Schotten, Ai-assisted Phy Technologies for 6g and beyond Wireless Networks, arXiv Preprint arXiv:1908.09523.
[46] T. Hong, C. Liu, M. Kadoch, Machine learning based antenna design for physical layer security in ambient backscatter communications, Wireless Commun. Mobile Comput. (2019).
[47] S.J. Nawaz, S.K. Sharma, S. Wyne, M.N. Patwary, M. Asaduzzaman, Quantum machine learning for 6g communication networks: state-of-the-art and vision for the fu-ture, IEEE Access 7 (2019) 46317–46350.
[48] N. Farsad, H.B. Yilmaz, A. Eckford, C.-B. Chae, W. Guo, A comprehensive survey of recent advancements in molecular communication, IEEE Commun. Surv. Tutorials 18 (3) (2016) 1887–1919.
[49] Y. Lu, M.D. Higgins, M.S. Leeson, Comparison of channel coding schemes for molecular communications systems, IEEE Trans. Commun. 63 (11) (2015) 3991–4001.
[50] V. Loscri, C. Marchal, N. Mitton, G. Fortino, A.V. Vasilakos, Security and privacy in molecular communication and networking: opportunities and challenges, IEEE Trans. NanoBioscience 13 (3) (2014) 198–207.
[51] J.-Y. Hu, B. Yu, M.-Y. Jing, L.-T. Xiao, S.-T. Jia, G.-Q. Qin, G.-L. Long, Experimental quantum secure direct communication with single photons, Light Sci. Appl. 5 (9) (2016), e16144.
[52] S. Kiyomoto, A. Basu, M.S. Rahman, S. Ruj, On blockchain-based authorization architecture for beyond-5g mobile services, in: 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, 2017, pp. 136–141.
[53] K. Kotobi, S.G. Bilen, Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networks enhances security and user access, IEEE Veh. Technol. Mag. 13 (1) (2018) 32–39.
[54] P. Ferraro, C. King, R. Shorten, Distributed ledger technology for smart cities, the sharing economy, and social compliance, IEEE Access 6 (2018) 62728–62746.
[55] I.F. Akyildiz, J.M. Jornet, C. Han, Terahertz band: next frontier for wireless communications, Phys. Commun. 12 (2014) 16–32.
[56] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J.M. Jornet, D.M. Mittleman, Security and eavesdropping in terahertz wireless links, Nature 563 (7729) (2018) 89–93.
[57] S. Ucar, S. Coleri Ergen, O. Ozkasap, D. Tsonev, H. Burchardt, Secvlc: secure visible light communication for military vehicular networks, in: Proceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access, 2016, pp. 123–129.
[58] S. Cho, G. Chen, J.P. Coon, Enhancement of physical layer security with simultaneous beamforming and jamming for visible light communication systems, IEEE Trans. Inf. Forensics Secur. 14 (10) (2019) 2633–2648.
[59] T. Zhu, S.Y. Philip, Applying differential privacy mechanism in artificial intelligence, in: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2019, pp. 1601–1609.
[60] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G.K. Karagiannidis, P. Fan, 6g wireless networks: vision, requirements, architecture, and key technologies, IEEE Veh. Technol. Mag. 14 (3) (2019) 28–41.
[61] Z. Zhou, H. Liao, B. Gu, K.M.S. Huq, S. Mumtaz, J. Rodriguez, Robust mobile crowd sensing: when deep learning meets edge computing, IEEE Network 32 (4) (2018) 54–60.
[62] T. Zhang, T. Zhu, P. Xiong, H. Huo, Z. Tari, W. Zhou, Correlated differential privacy: feature selection in machine learning, IEEE Trans. Ind. Inf..
[63] T. Zhu, G. Li, W. Zhou, S.Y. Philip, Differentially private data publishing and analysis: a survey, IEEE Trans. Knowl. Data Eng. 29 (8) (2017) 1619–1638.
[64] O.B. Akan, H. Ramezani, T. Khan, N.A. Abbasi, M. Kuscu, Fundamentals of molecular information and communication science, Proc. IEEE 105 (2) (2016) 306–318.
[65] T. Nakano, Y. Okaie, S. Kobayashi, T. Hara, Y. Hiraoka, T. Haraguchi, Methods and applications of mobile molecular communication, Proc. IEEE 107 (7) (2019) 1442–1456.
[66] L. Gyongyosi, S. Imre, H.V. Nguyen, A survey on quantum channel capacities, IEEE Commun. Surv. Tutorials 20 (2) (2018) 1149–1205.
[67] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, G.-C. Guo, Quantum secure direct communication with quantum memory, Phys. Rev. Lett. 118 (22) (2017), 220501.
[68] X. Ling, J. Wang, T. Bouchoucha, B.C. Levy, Z. Ding, Blockchain radio access network (b-ran): towards decentralized secure radio access paradigm, IEEE Access 7 (2019) 9714–9723.
[69] D. Puthal, N. Malik, S.P. Mohanty, E. Kougianos, C. Yang, The blockchain as a decentralized security framework [future directions], IEEE Consum. Electron. Mag. 7 (2) (2018) 18–21.
[70] S. Elmeadawy, R.M. Shubair, 6g wireless communications: future technologies and research challenges, in: 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA), IEEE, 2019, pp. 1–5.
[71] M.S. Islim, R.X. Ferreira, X. He, E. Xie, S. Videv, S. Viola, S. Watson, N. Bamiedakis, R.V. Penty, I.H. White, et al., Towards 10 gb/s orthogonal frequency division multiplexing-based visible light communication using a Gan violet micro-LED, Photon. Res. 5 (2) (2017) A35–A43.
[72] J. Luo, L. Fan, H. Li, Indoor positioning systems based on visible light communication: state of the art, IEEE Commun. Surv. Tutorials 19 (4) (2017) 2871–2893.
[73] L.U. Khan, Visible light communication: applications, architecture, standardization and research challenges, Digit. Commun. Network. 3 (2) (2017) 78–88.
[74] P.H. Pathak, X. Feng, P. Hu, P. Mohapatra, Visible light communication, networking, and sensing: a survey, potential and challenges, IEEE Commun. Surv. Tutorials 17 (4) (2015) 2047–2077.
[75] C. Chen, R. Bian, H. Haas, Omnidirectional transmitter and receiver design for wireless infrared uplink transmission in lifi, in: 2018 IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2018, pp. 1–6.
[76] A. Mostafa, L. Lampe, Physical-layer security for indoor visible light communications, in: 2014 IEEE International Conference on Communications (ICC), IEEE, 2014, pp. 3342–3347.
[77] R. Chen, C. Li, S. Yan, R. Malaney, J. Yuan, Physical layer security for ultra-reliable and low-latency communications, IEEE Wireless Commun. 26 (5) (2019) 6–11.
[78] J.M. Hamamreh, E. Basar, H. Arslan, OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services, IEEE Access 5 (2017) 25863–25875.
[79] Y. Al-Eryani, E. Hossain, The d-oma method for massive multiple access in 6g: performance, security, and challenges, IEEE Veh. Technol. Mag. 14 (3) (2019) 92–99.
[80] M. Hooper, Y. Tian, R. Zhou, B. Cao, A.P. Lauf, L. Watkins, W.H. Robinson, W. Alexis, Securing commercial wifi-based uavs from common security attacks, in: MILCOM 20162016 IEEE Military Communications Conference, IEEE, 2016, pp. 1213–1218.
[81] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L.G. Giordano, A. Garcia-Rodriguez, J. Yuan, Survey on uav cellular communications: practical aspects, standardization advancements, regulation, and security challenges, IEEE Commun. Surv. Tutorials 21 (4) (2019) 3417–3442.
[82] J. Wang, J. Liu, N. Kato, Networking and communications in autonomous driving: a survey, IEEE Commun. Surv. Tutorials 21 (2) (2018) 1243–1274.
[83] A. Sanjab, W. Saad, T. Bas,ar, Prospect theory for enhanced cyber-physical security of drone delivery systems: a network interdiction game, in: 2017 IEEE International Conference on Communications (ICC), IEEE, 2017, pp. 1–6.
[84] X. Sun, W. Yang, Y. Cai, R. Ma, L. Tao, Physical layer security in millimeter wave SWIPT UAV-based relay networks, IEEE Access 7 (2019) 35851–35862.
[85] J. Ni, X. Lin, X. Shen, Toward privacy-preserving valet parking in autonomous driving era, IEEE Trans. Veh. Technol. 68 (3) (2019) 2893–2905.
[86] R.A. Ramadan, A.V. Vasilakos, Brain computer interface: control signals review, Neurocomputing 223 (2017) 26–44.
[87] I. Svogor, T. Kĩ sasondi, Two factor authentication using eeg̃ augmented passwords, in: Proceedings of the ITI 2012 34th International Conference on Information Technology Interfaces, IEEE, 2012, pp. 373–378.
[88] T. Nguyen, N. Tran, L. Loven, J. Partala, M.-T. Kechadi, S. Pirttikangas, Privacy-aware blockchain innovation for 6g: challenges and opportunities, in: 2020 2nd 6G Wireless Summit (6G SUMMIT), IEEE, 2020, pp. 1–5.
[89] K.-C. Chen, T. Zhang, R.D. Gitlin, G. Fettweis, Ultra-low latency mobile networking, IEEE Network 33 (2) (2018) 181–187.
[90] T. Yamakami, A privacy threat model in xr applications, in: International Conference on Emerging Internetworking, Data & Web Technologies, Springer, 2020, pp. 384–394.
[91] J. Pilz, B. Holfeld, A. Schmidt, K. Septinus, Professional live audio production: a highly synchronized use case for 5g URLLC systems, IEEE Network 32 (2) (2018) 85–91.
[92] B. Li, Z. Fei, Y. Zhang, UAV communications for 5g and beyond: recent advances and future trends, IEEE Internet Things J. 6 (2) (2018) 2241–2263.
[93] U. Challita, A. Ferdowsi, M. Chen, W. Saad, Machine learning for wireless connectivity and security of cellular-connected UAVs, IEEE Wireless Commun. 26 (1) (2019) 28–35.
[94] H. Kim, J. Ben-Othman, L. Mokdad, Udipp: a framework for differential privacy preserving movements of unmanned aerial vehicles in smart cities, IEEE Trans. Veh. Technol. 68 (4) (2019) 3933–3943.
[95] G. Xu, H. Li, S. Liu, M. Wen, R. Lu, Efficient and privacy-preserving truth discovery in mobile crowd sensing systems, IEEE Trans. Veh. Technol. 68 (4) (2019) 3854–3865.
[96] Y. Ding, C. Chen, S. Zhang, B. Guo, Z. Yu, Y. Wang, Greenplanner: planning personalized fuel-efficient driving routes using multi-sourced urban data, in: 2017 IEEE International Conference on Pervasive Computing and Communications (PerCom), IEEE, 2017, pp. 207–216.
[97] X. Chen, Y. Wang, M. Nakanishi, X. Gao, T.-P. Jung, S. Gao, High-speed spelling with a noninvasive brain–computer interface, Proc. Natl. Acad. Sci. Unit. States Am. 112 (44) (2015) E6058–E6067.

[98] P. McCullagh, G. Lightbody, J. Zygierewicz, W.G. Kernohan, Ethical challenges associated with the development and deployment of brain computer interface technology, Neuroethics 7 (2) (2014) 109–122.
[99] D.T. Karthikeyan, B. Sabarigiri, Enhancement of multimodal biometric authentication based on iris and brain neuro image coding, Int. J. Biometric Bioinf. (IJBB) 5 (5) (2011) 249.
[100] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, Y. Zhang, Blockchain and deep reinforcement learning empowered intelligent 5g beyond, IEEE Network 33 (3) (2019) 10–17.
[101] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A Survey on the Security of Blockchain Systems, Future Generation Computer Systems.