future internet

Review

A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas

Paul Scalise [1], Matthew Boeding [1], Michael Hempel [1,*], Hamid Sharif [1], Joseph Delloiacovo [2] and John Reed [2]

[1] Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, Lincoln, NE 68588, USA; pscalise2@huskers.unl.edu (P.S.); mboeding@huskers.unl.edu (M.B.); hsharif@unl.edu (H.S.)
[2] Belcan Government Solutions (BGS), Bellevue, NE 68123, USA; jdelloiacovo@belcangov.com (J.D.); jareed@belcangov.com (J.R.)
* Correspondence: mhempel@unl.edu

Abstract: With the rapid rollout and growing adoption of 3GPP 5thGeneration (5G) cellular services, including in critical infrastructure sectors, it is important to review security mechanisms, risks, and potential vulnerabilities within this vital technology. Numerous security capabilities need to work together to ensure and maintain a sufficiently secure 5G environment that places user privacy and security at the forefront. Confidentiality, integrity, and availability are all pillars of a privacy and security framework that define major aspects of 5G operations. They are incorporated and considered in the design of the 5G standard by the 3rd Generation Partnership Project (3GPP) with the goal of providing a highly reliable network operation for all. Through a comprehensive review, we aim to analyze the ever-evolving landscape of 5G, including any potential attack vectors and proposed measures to mitigate or prevent these threats. This paper presents a comprehensive survey of the state-of-the-art research that has been conducted in recent years regarding 5G systems, focusing on the main components in a systematic approach: the Core Network (CN), Radio Access Network (RAN), and User Equipment (UE). Additionally, we investigate the utilization of 5G in time-dependent, ultra-confidential, and private communications built around a Zero Trust approach. In today's world, where everything is more connected than ever, Zero Trust policies and architectures can be highly valuable in operations containing sensitive data. Realizing a Zero Trust Architecture entails continuous verification of all devices, users, and requests, regardless of their location within the network, and grants permission only to authorized entities. Finally, developments and proposed methods of new 5G and future 6G security approaches, such as Blockchain technology, post-quantum cryptography (PQC), and Artificial Intelligence (AI) schemes, are also discussed to understand better the full landscape of current and future research within this telecommunications domain.

Keywords: 5G; security; survey; Zero Trust architecture; confidentiality; integrity; availability; blockchain; post-quantum cryptography

check for updates

Citation: Scalise, P.; Boeding, M.; Hempel, M.; Sharif, H.; Delloiacovo, J.; Reed, J. A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas. *Future Internet* **2024**, *16*, 67. https://doi.org/10.3390/fi16030067

Academic Editors: Mario Di Mauro, Francesco Pascale and Marco Tambasco

Received: 19 January 2024
Revised: 17 February 2024
Accepted: 17 February 2024
Published: 20 February 2024

1. Introduction

The expansion of 5G technologies has ushered in a new era of communications with promises for high-speed mobile broadband communications, ultra-low latency applications, massive device connectivity, Internet of Things (IoT) support, and more. As 5G usage and coverage continue to increase in the near future for industries and consumers alike, it also brings with it a new range of security challenges and considerations. In order to uphold the promises of this technology, the confidentiality, integrity, and availability of the network are of utmost importance during its ongoing integration with critical infrastructure, government operations, and medical operations. This survey paper compiles a comprehensive review of academic and industry literature on current and future 5G security mechanisms in a systematic approach with a particular focus on the necessities and proposed methods for integrating Zero Trust Architecture (ZTA). Our paper aims to facilitate knowledge and research that is applicable not only to academia but also to industry and government users.

The challenges in 5G security are numerous and complicated. Researchers and standards organizations, like 3GPP, have outlined security structures and provisions that encompass the entirety of 5G. Even with such extensive considerations, there will always be security concerns post-design, whether inherent in the operations, due to misconfigurations by a vendor, or because of other factors outside of the control of the architect or operator. In 4G LTE (Long-Term Evolution), the predecessor to this current generation of cellular networks, security vulnerabilities were identified where a user's identity could become exposed whenever network authentication was requested [1]. This fault in LTE leads to a decrease in user identity protection and a lack of forward secrecy. For 5G to continue being a backbone of our technological society, all avenues of security need to be challenged and reviewed, and systems need to be fully compliant with established standards. Implementing robust security measures in 5G is not just a significant technical challenge but also vital for building trust with service users.

Scope and Contributions

This paper makes multiple significant contributions to the realm of 5G security research by providing a comprehensive survey of its current state and potential future directions. In this 5G survey, we seek to understand and showcase the research work that has taken place and new contributions in the realm of privacy and security of 5G networks. Security is of utmost importance when users all over the world are accessing these networks for their personal, business, or government use. We look into the vast amount of work that has been published in academia and industry regarding 5G security standards and compare and contrast relevant topics. The motivation for this survey is to bring to light the advantage of viewing 5G security through the lens of the Confidentiality, Integrity, and Availability model for highly sensitive information. As this survey represents a systematic review, it encompasses all major components of any 5G network: UE, the RAN and its gNodeB (gNB), and the Core Network. These three distinct aspects are further dissected into their constituent foundational considerations or features. For example, the Core Network portion goes in depth on authentication and network access along with Software-Defined Networking (SDN), Network Function Virtualization (NFV), Mobile Edge Computing (MEC, also known as Multi-access Edge Computing), and more.

The survey looks into the current methods of security and then compares and contrasts innovative new security mechanisms, like post-quantum cryptography for 5G. Finally, the aspect of Zero Trust networks is explored, expressing yet another future implementation of 5G security with considerations for highly secure communications. A high-level breakdown of what is covered in this survey can be found in Figure 1. Gathering new and trusted methods for security mechanisms in 5G will allow for the recognition of areas where improvements are already available or where additional research is still needed in order to continue working toward a more secure and confidential system architecture.

The remainder of the paper is organized as follows. In Section 2, we present a comprehensive review of related works. Section 3 presents the systematic approach taken by 5G in providing security mechanisms across its architecture, while the focus in Section 4 is specifically on Zero Trust Architecture considerations, and in Section 5, we review several suggested future security enhancements for 5G and beyond. Finally, in Section 6, we present our conclusions.

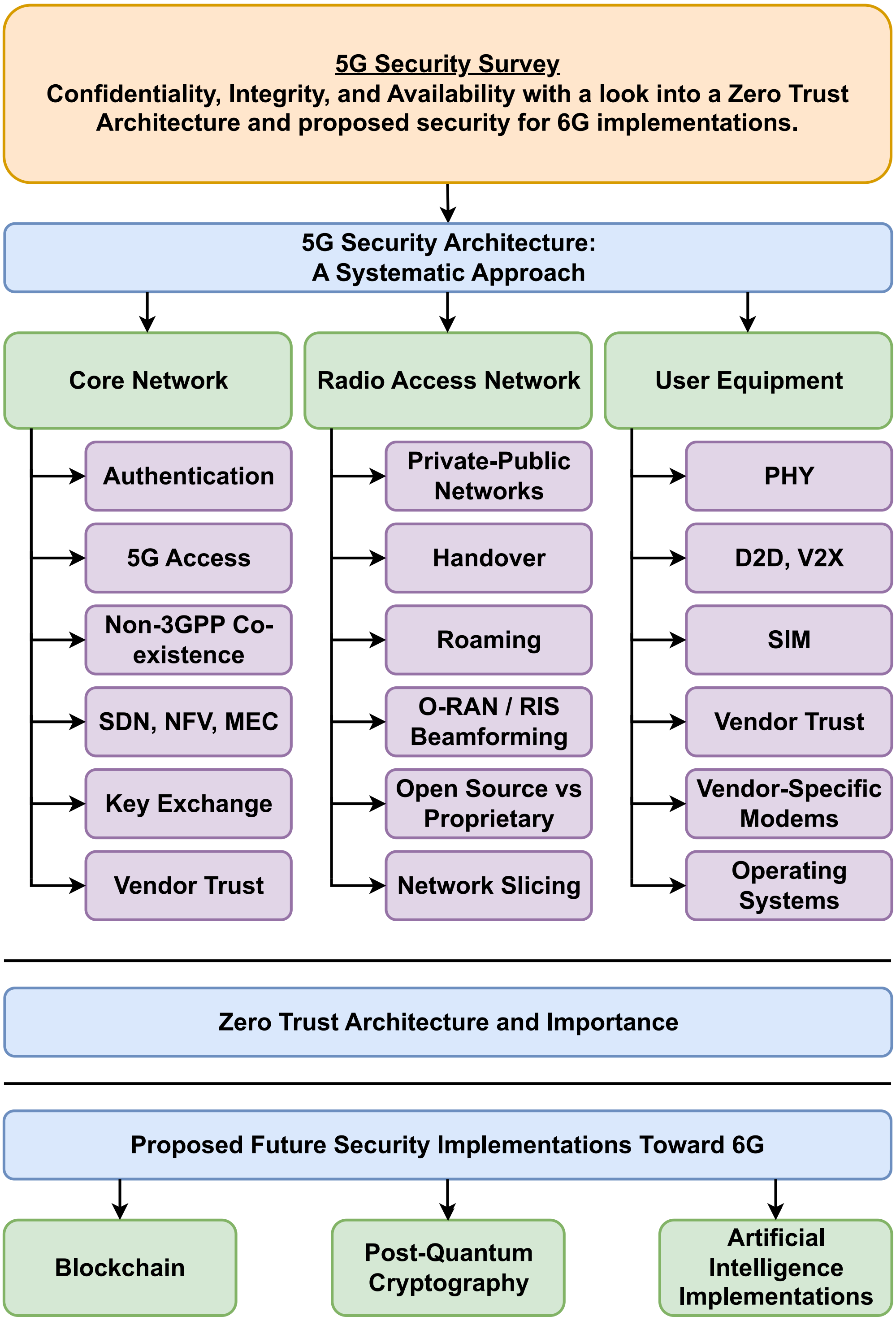
5G Security Survey
Confidentiality, Integrity, and Availability with a look into a Zero Trust Architecture and proposed security for 6G implementations.
5G Security Architecture: A Systematic Approach
Core Network
Radio Access Network
User Equipment
Authentication
5G Access
Non-3GPP Co-existence
SDN, NFV, MEC
Key Exchange
Vendor Trust
Private-Public Networks
Handover
Roaming
O-RAN / RIS Beamforming
Open Source vs Proprietary
Network Slicing
PHY
D2D, V2X
SIM
Vendor Trust
Vendor-Specific Modems
Operating Systems
Zero Trust Architecture and Importance
Proposed Future Security Implementations Toward 6G
Blockchain
Post-Quantum Cryptography
Artificial Intelligence Implementations

Figure 1. High-level scope and structure of our 5G security survey.

2. Related Works

2.1. Security Focuses in 5G

To enhance the security of 5G cellular networks, 3GPP released an updated Technical Standard (TS) 33.501 [2] for security architecture and procedures. This document outlines the security architecture through three different strata and six separate security domains, as shown in Figure 2. These security domains and the sections of this paper that discuss their respective research areas are listed below:

(1) Network Access Security focuses on UE authentication and secure network services access with a particular focus on attacks against the physical/radio interface. This domain includes both 3GPP and trusted non-3GPP access and the access security between the Serving Network (SN) and Access Network (AN). In the context of this paper, sections covering authentication, 5G access, RAN, and UE physical layer security will review the current state of research in each of these areas. These sections will outline current research enhancements, vulnerabilities, and future research directions to align with the TS 33.501 standard.

(2) Network Domain Security encompasses security for network nodes that enables the secure exchange of signaling data and user plane data. Sections covering the topics of non-3GPP co-existence, SDN, NFV, and MEC will discuss research in this domain later in this paper.

(3) User Domain Security contains the security features that secure the user's access to mobile equipment. Discussed later are general resources and security measures listed by the National Institute of Science and Technology (NIST) on identifying areas of concern for user security at the device end.

(4) Application Domain Security entails security for the user domain to the application provider domain in order to be able to exchange messages securely. Application domain security is not within the scope of TS 33.501, but this paper will discuss blockchain technology and post-quantum cryptography for applications specific to 5G networks.

(5) Service-Based Architecture (SBA) Domain Security is the set of security features that enables network functions to securely communicate within the serving network domain and with other network domains. Such features include network function registration, discovery, and authorization security aspects as well as the protection for the service-based interfaces. SBA domain security is a new security feature compared to TS 33.401 [3]. These security features will be discussed in the SBA section with specific subsections corresponding to the various network functions in a 5G system.

(6) Visibility and Configurability of Security spans the set of features that inform the user whether a security feature is in operation. Visibility and configurability are mentioned within this survey in the sections discussing the user equipment, the Core Network, and O-RAN (Open-RAN).

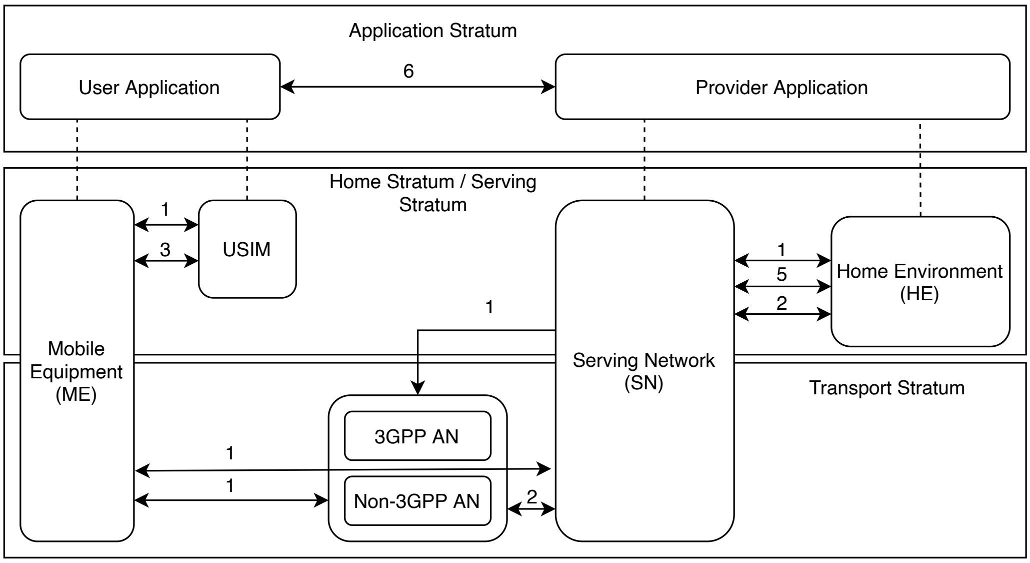

Figure 2. 3GPP security domains defined in TS 33.501. The interfaces are relative to the list 1–6 above.

2.2. 5G Security Research

As 5G expands its presence worldwide, the scientific literature evaluating the security aspects of 5G has grown, especially regarding surveys into specific areas of 5G's implementation. For example, in [4], the current research and challenges of security for different aspects of cloud services, RAN, MEC, and network slicing are investigated. The insights presented in this paper are focused on the need to deploy future 5G networks while taking great care of the vast security aspects. Understanding that these networks will serve applications to a wide range of consumers, they need to provide adaptability, resilience, and flexibility, embodied and provided by Software-Defined Networking (SDN) and Network Function Virtualization (NFV), in order to be able to provide and enforce comprehensive security measures. The authors of [5] focus their security research on access, handover, IoT, D2D, V2X, and 5G network slicing, whereas in [6], the focus is on architecture and design, attacks on 5G, physical security, and V2X. Both of these publications showcase potential vulnerabilities to the security mechanisms within architecture, specifically for authentication and network slicing, and thereby emphasize the need for more fine-grained security control in the network. A comparative analysis of 5G security mechanisms is discussed in [7,8], which includes a wide survey into the overall 5G security framework, Core Network, Radio Access Network, cloud infrastructure, and the Internet of Things. IoT protocols for 5G are reviewed in [9]. An overview of the threats to, and vulnerabilities of, both 5G and 6G, is presented in [10] with a specific focus on SDN, NFV, and MEC in 5G networks. The security issues of network coexistence are investigated in [11] with a focus on 5G/6G coexistence with WiFi 6. Application-specific attacks are outlined in [12] with a focus on cyber–physical systems, fog computing, and SDNs. The contributions from these primary surveys showcase the need for continued research and a strong focus on improving the adoption and implementation of security mechanisms. For confidential communication and heightened network monitoring and security, a Zero Trust Architecture (ZTA) is recommended, particularly in a 5G setting. ZTA opens the door for operations in which the assumption is that the attacker is always one step ahead of the fix or patch to a network issue.

2.3. Zero Trust Importance

ZTA focuses on a shift in security perspective from perimeter defense to defending each transaction within a network [13]. It is built around the assumption that the attacker may already have penetrated into the network and established a foothold. In ZTA environments, therefore, each transaction is individually scrutinized to ensure the integrity of every communication attempt and enforce strict policy compliance. This shift in network security is vitally important to 5G networks that inherently operate in an untrusted environment [14]. The added security of a ZTA can be used for a variety of applications, including military applications shown in [14,15]. Table 1 lists and describes the tenets of ZTA provided by the National Institute of Science and Technology (NIST), including backbone considerations for the deployment of a ZTA system.

Zero Trust and the development of similar security principles have circulated within the research community ever since the term was coined in 1994 by Stephen Paul Marsh [16]. Since then, the idea of limiting the trust shown to users of a network or networked resource to zero has gained popularity, especially over the past few years. Figure 3 shows the rapid increase in publications that mention the term ‘Zero Trust’ per year, giving weight to ZTA and the exploration of its feasibility in real-world deployments across different network and application implementations. This search was conducted using Google Scholar with the search phrase of “network, security, “zero trust” -game -health -mechanical”. The negated words are used to exclude publications that are not within this domain of literature. Topics akin to the excluded keywords initially showed up in the study but were excluded after their relevance was seen to be outside of this search domain. We then looked at the incorporation of both ZTA and 5G/6G in publications and see a similar growth in interest in the past few years. Figure 4 illustrates the increasing amount of publications including ZTA and 5G/6G, providing more weight to the importance of ZTA and the discovery of applications in a 5G or 6G network environment with each category growing in popularity at a rate that is nearly doubling year-over-year. This search was similarly conducted using

Google Scholar with the search phrase of "network, security, 5G OR 6G, 'zero trust' -game -health -mechanical".

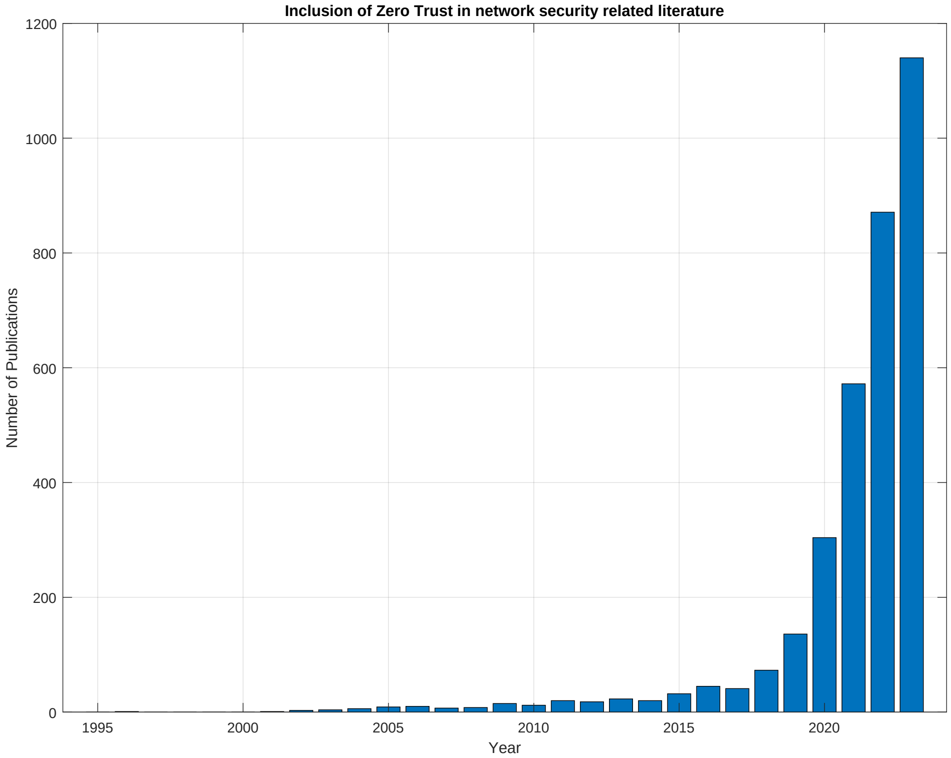

Figure 3. Mentions of the term 'Zero Trust' in network security oriented research publications starting from the year 1994.

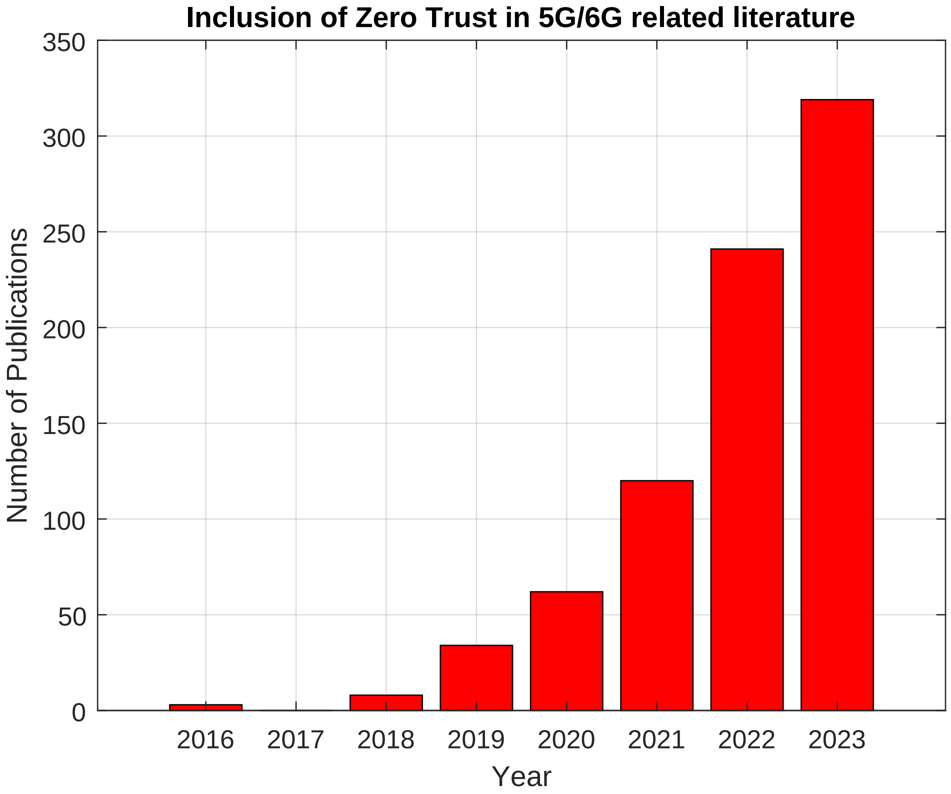

Figure 4. Mentions of the term 'Zero Trust' in conjunction with either 5G or 6G in network security-oriented research publications, starting from the year 2016.

Table 1. ZTA tenets.

Zero Trust Architecture Tenets from NIST [13]	
Tenet	**Explanation**
(1) "All data sources and computing services are considered resources".	A network can comprise different classes of devices, which can have different footprints and functions. A personal device can also be seen as a resource if it can access the enterprise-owned network.
(2) "All communication is secured regardless of network location".	Any equipment attempting to obtain access to a network, whether on-site or remote, must be authenticated. Network location alone does not imply trust. Confidentiality and integrity need to be protected.
(3) "Access to individual enterprise resources is granted on a per-session basis".	Prior to accessing an asset, the user will be identified and verified. Only the minimum resources should be given in order to complete a task. Successful authentication and access to one resource does not grant access to other resources on the network without further permissions.
(4) "Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes".	It is necessary for an organization to protect resources by defining what resources it has, who its members are, and what access to resources those members need. Requesting asset state can include device characteristics such as software versions installed, network location, time/date of request, previously observed behavior, and installed credentials. Resource access and action permission policies can vary based on the sensitivity of the resource/data.
(5) "The enterprise monitors and measures the integrity and security posture of all owned and associated assets".	No access within the network or remote can be inherently trusted. Devices should be monitored using continuous diagnostics and mitigation (CDM), and patches/fixes should be applied when necessary. Devices that do not match this criteria can be completely rejected from making any connections with the network.
(6) "All resource authentication and authorization are dynamic and strictly enforced before access is allowed".	A ZTA needs to be adaptive and continually reevaluate trust with devices and their open sessions. Identity, Credential, and Access Management (ICAM) and asset management systems are an expectation of the ZTA. Continual monitoring with possible reauthentication and reauthorization occurs throughout user transactions, as defined and enforced by policy (e.g., time-based, new resource requested, resource modification, anomalous subject activity detected) that strives to achieve a balance of security, availability, usability, and cost-efficiency.
(7) "The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture".	Any data on the network that can be captured should be. This allows for the improvement of the policy creation and enforcement.

3. 5G Security Architecture: A Systematic Approach

5G as a whole is a vast and complex protocol with a rich history that has evolved from previous cellular generations, such as 2G, 3G, and 4G LTE. Security has, over time, become one of the highest priorities for these networks and is of paramount importance in today's information society. This section presents a breakdown of security mechanisms currently in place, some of which are defined by 3GPP and others introduced in the literature. The survey of current security protocols and any necessary security considerations are separated into three subsections, focusing on the Core Network, Radio Access Network, and User Equipment, which are the main three pillars of a 5G connected system, as depicted in Figure 5.

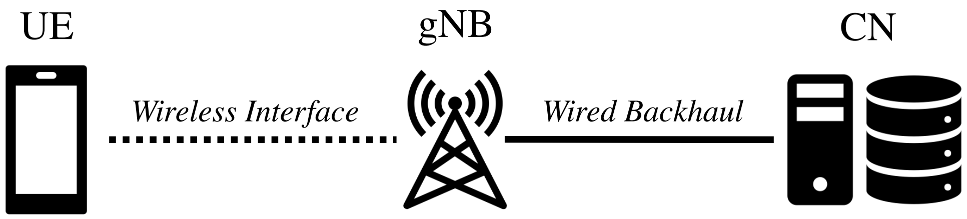

Figure 5. Basic 5G architecture based off of Figure 1 in 3GPP article “5G System Architecture” [17].

3.1. Core Network

3.1.1. Authentication

In any network, authentication is necessary in order to ensure the user attempting to gain access has the right to do so. This can be seen as the first line of defense when connecting a device to a network. Protocols used for authentication need to be robust to allow for seamless use for an authorized client but also have mechanisms in place to reject access by illegitimate users. Authentication mechanisms have grown over the years, adapting to the ever-changing communications landscape. The 3rd Generation Partnership Project (3GPP) has specified two main sectors of security in 5G authentication: primary and secondary authentication. Primary authentication is used for device and network mutual authentication in both 4G and 5G [18]. The purpose of secondary authentication is for a UE to be able to connect outside of its mobile network operator (MNO) domain [19]. Respectively, there are two protocols that handle the two different authentication methods in 5G: 5G-AKA (Authentication and Key Agreement) used in primary authentication when a device first connects or attaches to the network, and a suite of Extensible Authentication Protocols (EAPs) used in secondary authentication, usually when a device is connecting to a service on the internet using the 5G network [20]. The 5G-AKA protocol is outlined in 3GPP specification number 33.501 [21] and is used to verify authenticity when a user device connects to a home or serving network. 5G-AKA has been stated to be more secure than its predecessors in 3G and 4G LTE with privacy and integrity goals listed by 3GPP in [21] and summarized below from [22].

- Mutual authentication (implicit) between UE and SN, and UE and HN.
- SN is authorized by HN.
- Confidentiality for K_{SEAF} (Key [from] Security Anchor Function) even if the attacker learns session keys established in other sessions (previous or consequent).
- Anonymity: SUPI (Subscription Permanent Identifier) and SQN (Sequence Number) shall remain secret in the presence of a passive attacker in order to guarantee activity privacy.
- Unlinkability (user location confidentiality and user untraceability) against passive adversaries. An attacker cannot deduce the presence of a subscriber in a certain area or whether different services are delivered to the same user by eavesdropping on the radio access link.

The author of [22] points out that there have been integrity vulnerabilities of the 5G-AKA protocol detailed in the literature [23–25]. 5G-AKA security is affected when an attacker eavesdrops on a suspected target UE and intercepts a failed authentication challenge, either being a MAC_Failure or Sync_Failure. The attacker then has the ability to reply to the UE with another authentication message and will wait for either a Sync or MAC failure. If a Sync_Failure is returned, the adversary then knows that the target UE is the one being communicated with. This fault is a breach of user privacy, as it allows for potential user traceability and knowledge of their subscription location. One solution to this issue is to encrypt both messages, making them look indistinguishable to the attacker. The work in [26] addresses the formal verification of 5G-AKA and its findings. In the paper, the authors share that the UE’s data privacy is at risk if the USIM (Universal Subscriber

Identity Module) is compromised, as the master key K_{SEAF} can be found by using the K in the USIM and one of the initial messages sent to the UE in plain text containing the random number. The authors also state that Perfect Forward Security (PFS) is possible if a Diffie–Hellman (DH) key exchange is utilized.

3.1.2. Key Exchange

As discussed in the previous subsection on authentication, 5G key exchanges are performed via two primary protocols: 5G-AKA and EAP-AKA. During an initial connection to the network, the UE uses its secret key stored in the USIM and the same key stored in the CN, specifically in the UDM (Unified Data Management) function, as a shared secret. Unlike previous methods in 3G and 4G LTE, the UE will send its (SUPI) concealed and encrypted by way of the SUCI (Subscriber Concealed Identifier) to offer heightened security. Once the device is admitted to the network, the device is secured via derived keys, ultimately generating a master root session key KAUSF (Key [from] Authentication Server Function) [27].

One concern with key generation is the duration and updating of keys in order to maintain confidentiality. 3GPP TS 33.501 [2] defines the following events when keys are updated:

1. The UE establishes a new PDU session or modifies an existing session.
2. The UE is handed over to a new base station or RAN cell.
3. The UE moves to a different serving network.
4. The UE performs a registration or de-registration from the network.
5. The UE requests a key change, or the network requests a key change, put in place by the operator's policy.

If a UE is solely connected to one base station without disconnection or handover for a prolonged amount of time, TS 33.501 specifies that the network shall request a key change every 24 h. It is also stated that the amount of time can be reduced at the discretion of the network operator.

3.1.3. SDN, NFV, MEC

Software-Defined Networks (SDNs) and Network Function Virtualization (NFV) are the two dominant factors contributing to the successful rollout of 5G. SDN and NFV have allowed for the use of off-the-shelf networking equipment compared to previous generations of cellular communications needing to be supported with specific hardware. However, with this drastic change in the architecture, there are bound to be security concerns. 5G back-end networks are easier to operate and more centralized now than in the past, which greatly eases the burden on operators and system administrators. It also reduces the number of possible attack vectors. One concern, however, resulting from increased integration and reliance on software-controlled systems is discussed in [28]. The author states that Denial-of-Service (DOS) attacks may be more potent due to this centralized infrastructure. In some cases, if the system is overloaded, this could cause entire network components to fail.

It is also mentioned that the integration of NFV into 5G raises some of its own concerns: NFV opens the door for failures in provisioning and securing the host systems of the virtualized network functions, thereby potentially exposing the utilized hypervisors to an attacker. If the hypervisor is left vulnerable due to a misconfiguration, the entire core network is at a very high risk of being compromised. Proper configuration of the NFV platform is also important to guard against cross-contamination of shared resources [29]. The author also shares that if there is a vulnerability in a virtualized core network function, malware could be used to gain access to information from other network users and potentially allow for unauthorized API calls. Unwarranted connections to a core network can be denied if a ZTA is utilized with mutual authentication and constant network monitoring.

Software-Defined Networks have rapidly grown in popularity over the years, since they allow administrators to dynamically adapt their networks through intelligent software controls. This can be seen with most all of the papers presented in Table 2 substantially cover SDN, whereas blockchain and ZTA are less mentioned, as they are newer concepts. SDN further eases the burden of implementing security models for different applications within the network's control plane. This software-centric and programmatic approach to networking differs drastically from the historical—more physical and static—view of a network, as it incorporates many operations of an administrator's workflow into one central control system, thereby creating a cohesive network management interface. In SDN, the network comprises three layers: Application, Control, and Data. With this architecture, 5G operators are able to segment their network into different priorities, creating a market for providing different services to consumers. As SDN is a newer concept, the security of this system architecture may not be as robust as other more established systems. A survey conducted on SDN security [30] shares a few security analyses of Software-Defined Networks. One analysis shows that the popular OpenFlow protocol used in SDN can be susceptible to information disclosure and DoS attacks [31]. It is mentioned in the survey that methods to prevent these attacks may exist but are not proven in the text in a wide array of tests. The OpenFlow documentation advised the use of TLS with mutual authentication for devices on the network but did not specify the use of a specific version of TLS. The authors of the survey text also point out that different vendors' equipment may not support this security, causing more concern and the need for a more cohesive and standard approach to SDN. The paper mentions the need for more proposals in the advancements in the design of SDNs. One holistic approach presented is FRESCO [32], which allows for more rapid development of security modules that can be implemented as Open Flow modules. This method incorporates automatic rule checking for arising conflicts in the network and can act automatically and accept or decline actions based on security measures and risk tolerances. SDN is and will continue to make a growing impact in 5G networks, making it even more important for up-to-date security measures to be in place along with routine network audits.

Table 2. Comparison of literature on 5G security aspects with a focus on the Core Network.

Citation	SDN	NFV	MEC	Network Slicing	User Auth.	Encrypt.	Attack Vectors	HetNets	Vendor/ Trust Models	Blockchain	ZTA
[33]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	X
[28]	✓	✓	✓	✓	X	X	✓	X	X	X	X
[34]	✓	✓	✓	✓	✓	✓	✓	X	X	✓	X
[12]	✓	✓	✓	✓	✓	✓	✓	X	X	✓	X
[4]	✓	✓	✓	✓	✓	X	✓	X	✓	X	X
[18]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	X
[15]	✓	✓	✓	X	✓	✓	✓	✓	X	X	X
[35]	✓	✓	X	✓	✓	✓	✓	✓	✓	X	X
[36]	✓	X	X	✓	X	✓	✓	X	X	X	X
[37]	✓	X	X	X	✓	✓	✓	✓	✓	X	X
[14]	✓	✓	✓	X	✓	X	✓	✓	✓	X	✓
[38]	✓	✓	X	X	✓	✓	✓	X	✓	X	✓
[39]	X	X	X	X	X	X	✓	X	✓	✓	✓

✓ indicates the paper has a substantive discussion on the topic; X indicates little or no information on the topic.

3.1.4. Vendor Trust

5G has allowed for the incorporation of new technologies like NFV and SDN, which are a design departure compared to past cellular network architectures. Previously, cellular operators needed to design their deployments in a more hardware-driven paradigm, as some components required specific hardware solutions that could only be established with often proprietary purpose-built equipment. This made it more difficult for operators to deviate from what was available on the market and for new players to enter that market, which passively ensured a sense of security due to very limited vendor flux in the solutions landscape. In the current 5G era, however, vendor diversity and interoperability are key features, as the networks are more flexible than ever, allowing the core to be run using off-the-shelf server hardware instead of requiring specific purpose-built hardware. As off-the-shelf solutions are now commonplace in 5G and constitute a significant part of the rollout and promise of 5G, additional questions are raised on whether all operators and equipment vendors are following security guidelines and whether they can be trusted. These concerns in recent years have entered mainstream media through increased geopolitical tensions amid a global marketplace for 5G technology vendors.

Security for 5G core and backhaul networks is required to gain its users' trust and maintain confidentiality, integrity, and availability of the communications and the data both in flight and at rest. An example illustration of a possible untrusted network path is presented in Figure 6. Various standards have been created in the pursuit of realizing a secure system for all operators to implement [40]. The authors of [37] outline the major high-level security pillars for a backhaul network listed in Table 3.

Table 3. 5G backhaul network security requirements and considerations.

Backhaul Network Security Considerations [37]	
Security Consideration	**Explanation**
Confidentiality and Integrity	Confidentiality and integrity are two of the most basic security considerations for any public network. Data integrity is vital to maintaining a trusted connection between two users. If the data are altered in any way or cannot be verified, trust is broken and the network can no longer be considered safe. Figure 6 is a good example of a potential decrease in confidentiality and data integrity with information being passed to an untrusted network link.
Mutual Authentication	One way to verify that all components within a network are legitimate is to utilize Mutual Authentication (MA). One example of MA is the 5G-AKA protocol, which authenticates the UE with the CN and vice versa in a quick and efficient manner. Node authentication is discussed in [41], which allows for the verification of different network components. This ensures all devices in the backhaul are authorized and will deny access to rogue actors.
Access Control	In order for a user to securely connect to a 5G network, there need to be methods in place to only allow access to legitimate users. This is standard practice for any network, but protecting against illegitimate user access is always a 'cat and mouse game' between researchers and hackers.
Availability	In any 5G network, availability is paramount, especially for the URLLC slice of 5G, guaranteeing an ultra-reliable and low-latency Quality of Service (QoS). User authentication has a direct impact on the availability of a network. If a large number of illegitimate users are able to gain access to a network, they would not only degrade network integrity but also severely deteriorate availability by consuming resources that are then no longer available to legitimate users of the network. Availability is not only dependent on the resources of the network but also how usable, effective, and efficient the network can be [42]. This can range from how the user accesses the network to provisioned authentication and connection methods and more.
Perfect Forward Secrecy	These methods of keeping user data private are crucial when storing information within a core network. The author suggests the use of session keys to allow for future recovery if a private key is exposed.

Table 3. *Cont.*

Backhaul Network Security Considerations [37]	
Security Consideration	**Explanation**
Light-Weight Cryptography Operations	Cryptography is a necessity in 5G networks to allow for more confidentiality and integrity in communications. Network availability can be affected negatively if these algorithms are not efficient and lightweight, however. The use of ASICs (Application-Specific Integrated Circuits) for these algorithms can improve the reliability and availability of the network [43]. Two principal concerns with using an ASIC are forward compatibility and equipment cost. Thus, FPGAs (Field-Programmable Gate Arrays) have emerged as a preferred intermediate solution for hardware-specific designs, since they can be reprogrammed when future standard updates are released.
Tamper Resistance	The inner workings of a network need to be tamper-proof and protected against leaking of sensitive information. This requires that no backdoors are incorporated into the network architecture during its design or implementation and that any devices storing secret keys are well guarded and cannot be easily accessed.
Defend Against Replay Attacks	The network must be able to reject forged requests to prevent illegitimate users from gaining access. Security Mode Control (SMC) and Radio Resource Control (RRC) replay attacks are common replay attacks that accomplish this. In SMC attacks, a NAS-SMC packet is replayed to impersonate a UE and reduce the security of a UE's security context [44]. RRC replay attacks utilize a false base station, which receives UE RRC packets, informs the core network of a successful connection, and subsequently disconnects the UE, forcing it to attempt to re-acquire the RRC connection continually. If implemented successfully, this can deny the UE access to the 5G network [45]. For these attacks, the 5G Core needs to be able to identify and prevent these attacks to mitigate false users.
Physical Unclonable Function (PUF)	A PUF is a physical identifier hardware algorithm built inside of a semiconductor material [46]. PUFs output a non-reversible random key that can be used for cryptography algorithms, authentication, and signatures. [47]

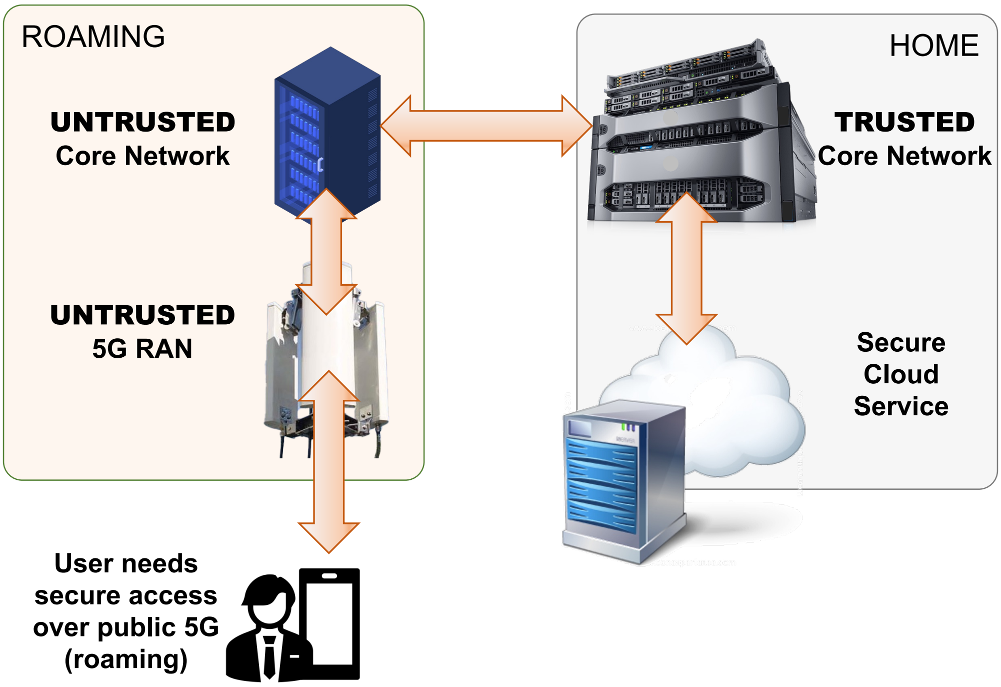

Figure 6. Network path through untrusted core.

3.2. Radio Access Network

3.2.1. Non-Public Networks

Non-Public Networks (NPNs), which are sometimes also referred to as private networks or public–private networks, are instances of an architecture that allows operators to partition their network infrastructure for the use of an exclusive party. Access to the network can be limited to a special network slice that has specific QoS, access controls, authentication requirements, and more. A Non-Public Network can also be solely owned by the exclusive party to achieve even higher data integrity and privacy. An article published by 3GPP [48] shares that in some instances, an organization may want to house and control all data passed through a network and restrict everything to within the bounds of the organization. In this specific case, the operators of the network achieve heightened security as they are in control of the architecture and its users and employ their own hardware for the Core and RAN. This provides three main advantages: optimized coverage, lower latency, and reduced network uncertainty by optimizing confidentiality, integrity, and availability. 3GPP outlines more information on NPNs in TS 22.261 [49]. The authors in [50,51] review the outlined security measures for NPNs along with potential use cases and considerations. Use cases for NPNs are also discussed in [52], which include emergency critical communications, smart city video surveillance, and services with Time-Sensitive Networking (TSN).

Each use case in this paper provides a unique infrastructure challenge, which helps to further define the challenges of building a robust private 5G network for multiple use cases. For emergency communications, for example, the network is proposed to serve as a "pop-up" network, which would require a set coverage area of the private 5G network. The smart city surveillance use case requires significant computing power at the edge, as streaming the video content from all surveillance cameras is impractical. In this case, micro-cells for higher-quality coverage and computer vision for emergency identification at the edge of the network would be required. TSN services, including autonomous mobile robots and factory process automation, were also outlined, focusing on the need for clear communication in a service area without re-cabling every device.

3.2.2. Handover

5G networks are designed to be highly flexible and heterogeneous with many different interfaces being supported. For instance, 5G allows several different technologies to interface with its network architecture besides its own New Radio (NR), some of which are Long-Term Evolution (LTE), IoT, Vehicular Ad Hoc Network (VANET), Wireless Local Area Networks (WLANs), and several types of Wi-Fi [53]. This Heterogeneous Network (HetNet) architecture is crucial for the evolution of 5G, as more and more devices connect to the network, highlighting the importance of available and reliable radio access methods. 3GPP outlines two main forms of handover within 3GPP networks in 5G: intra-handover and inter-handover.

Inter-handover is necessary for keeping LTE compatibility within the network, as there are still around 5.2 billion LTE subscribers around the world [54]. Inter-handover allows for communication between the gNB and eNB within 4G networks along with the 5G CN and LTE ePC (Evolved Packet Core).

Intra-system handover is a simpler operation as it does not involve communication with legacy systems. Intra-system handover takes place when a 5G UE is disconnected from one RAN and connected to another RAN. 3GPP outlines this within TS 23.502 [55].

As stated earlier, 5G comprises many different supplementary radio access networks, creating a HetNet. These technologies are not all defined by 3GPP standards and have been considered since 3G technologies. When 3G was the main technology, 3GPP interfaced with the Universal Mobile Telecommunications System (UMTS) and non-3GPP networks to devise services that are robust in order to support user mobility [56,57]. Support for more technologies grew over the years with the usage of 4G LTE and the introduction of 5G NR (New Radio). As these non-3GPP standards grew and matured, researchers have looked into the handover process from a security and performance perspective [58]. This survey outlines the current research and finds that no comprehensive approach exists that handles all use cases of the 5G handover and that the trade-off between performance and security creates several open research areas.

3.2.3. Roaming

In cellular networks, roaming allows a UE to move outside of its home network environment and connect to a visiting network to retain access to communications. This allows subscribers to maintain connectivity and services even if they are moving between different geographical areas where their own service provider has no coverage, and instead, they have to rely on other provider networks. Mobile service providers have agreements in place to allow users access, even if the equipment they are connecting to may not be from their home network. The main security consideration here is the ability to trust the visiting vendors they may connect to for services. This is discussed further in Section 3.1.4.

3.2.4. Reconfigurable Intelligent Surfaces (RIS) and RIS-Aided Beamforming

Reconfigurable Intelligent Surfaces (RISs) are surface structures that are programmable in order to aid RF signal propagation in specific areas. Broadly, they can be categorized into RIS that use metamaterial structures comprised of individual elements typically much smaller than the wavelength of the signal they are aiding. These metasurfaces are highly complex and provide significant capabilities. A far simpler and cost-effective approach to RIS instead utilizes surface-attached antenna arrays to provide RIS-aided beamforming to enable efficient data repeating/reflection. These devices are intended for high-frequency applications for 5G and especially for 6G deployments, as they aid in directing highly directional signals and can do so with high energy efficiency [59]. Figure 7 illustrates the main systematic differences between an architecture with the aid of RIS and without. Principally, there are two main security implications when implementing RIS: passive eavesdroppers and authentication of the RIS equipment. Presented in [60], the authors showcase an approach of utilizing a multiplicative random process at the RIS to mitigate the effectiveness of a passive eavesdropper. This is accomplished by degrading the quality of the reflected signals along with a one-time pad system at the RIS. The authors claim that this method outperforms conventional additive randomness methods in terms of power efficiency, as there is no artificial interference being transmitted. Results from both [61,62] share their claims on how RIS can heighten the security of the wireless communications in 5G and 6G applications at the physical layer.

One major security challenge with 6G communications and RIS is the deployment of an Illegal RIS (IRIS) into a network, which provides for extensive research opportunities in this domain, some of which are described in the RIS 6G review [63]. The authors of this paper state that preventing IRIS attacks requires powerful and effective countermeasures to defend against passive jamming attacks [64], as well as interference and leakage attacks, both of which are affecting the physical layer security (PLS) of the system. It will therefore be important for network operators to enforce strict authentication methods for their RIS systems and to continuously monitor the radio conditions at the edge of the deployment, which may be feasible also through the use of AI/ML.

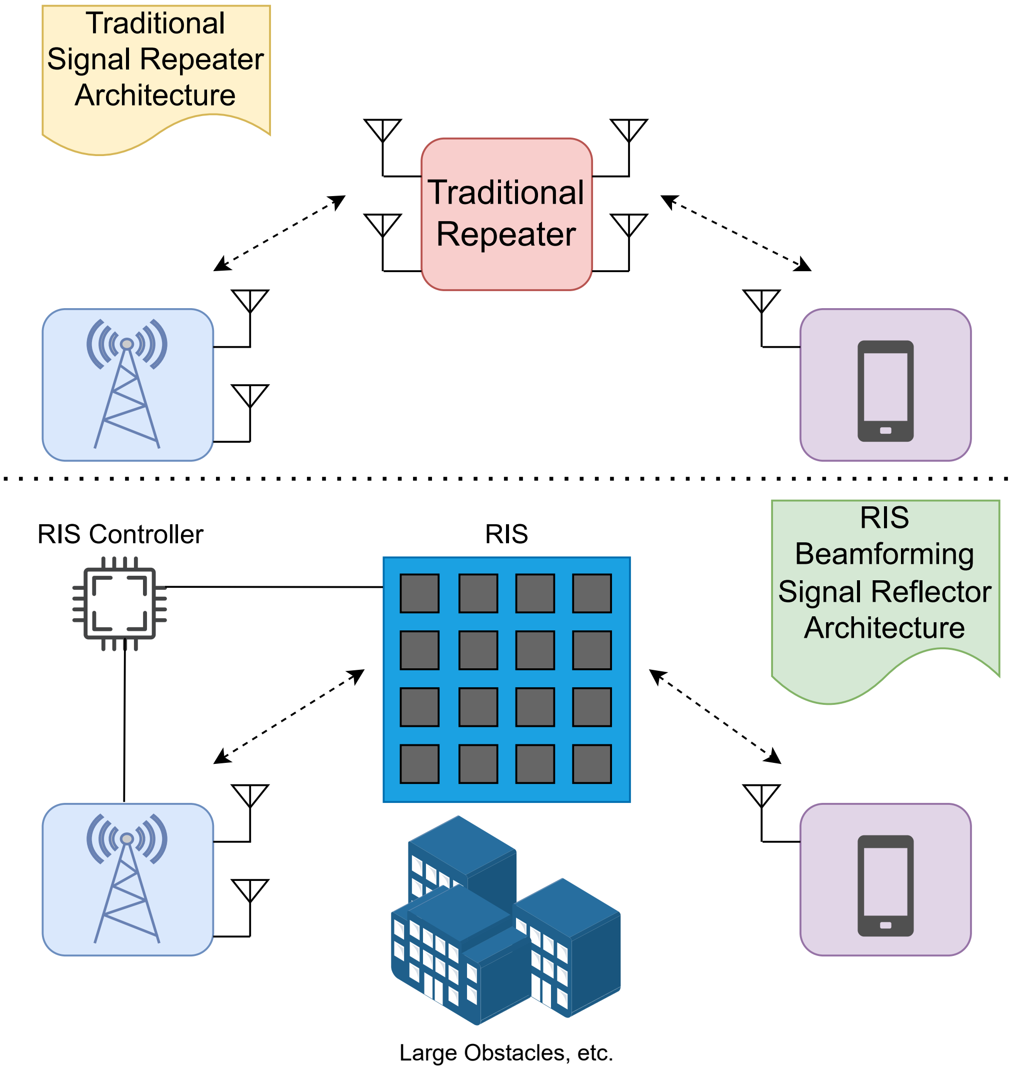
Traditional Signal Repeater Architecture
Traditional Repeater
RIS Controller
RIS
RIS Beamforming Signal Reflector Architecture
Large Obstacles, etc.

Figure 7. Traditional repeater architecture in comparison with RIS-aided repeating/reflection architecture.

3.2.5. O-RAN

Open Radio Access Network (O-RAN) is a coalition in a new approach to creating a more open, modular, and configurable RAN in cellular networks. Historically, RANs were proprietary monolithic solutions that tied service providers down into choosing equipment from a limited amount of vendors, thus causing concern for constraints in options that are available to address the various demands of a wide variety of networks. These proprietary solutions resulted in a lack of interoperability, which sometimes severely impacted the network's cost, quality, and efficiency for service providers, as deployments of these solutions could be seen as vendor-locked solutions. Such vendor lock diminished the service providers' ability to respond to the network's different requirements at different geological areas due to varying customer usages and applications. Monolithic RANs also limited the amount of centralized control a service provider could exercise on network edge operations, and many control functions were encapsulated within the RAN components. O-RAN seeks to overcome the proprietary nature of the RAN, as well as the lack of central management, by dividing the RAN functionality into different functional elements with well-defined interfaces, thereby enabling the use of interoperable sub-units regardless of the original vendor. Furthermore, many of the functional components can now be realized as software elements and moved further away from the edge for a more centralized and agile RAN operation. Illustrated in Figure 8 are the components of an O-RAN compared to a traditional RAN setup based on a figure presented in [65]. It can be seen that O-RAN has introduced modular components in the RAN and also virtualization features that are referred to as O-vRAN (Open Virtualized RAN).

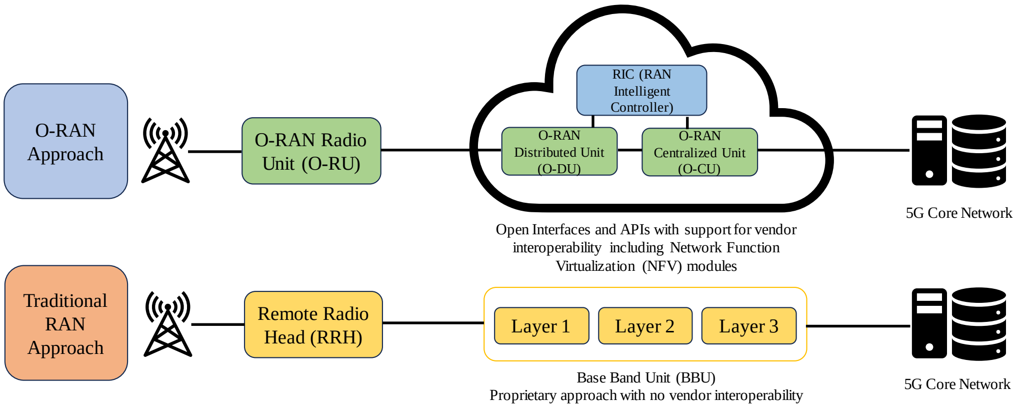
O-RAN Approach
O-RAN Radio Unit (O-RU)
RIC (RAN Intelligent Controller)
O-RAN Distributed Unit (O-DU)
O-RAN Centralized Unit (O-CU)
5G Core Network
Open Interfaces and APIs with support for vendor interoperability including Network Function Virtualization (NFV) modules
Traditional RAN Approach
Remote Radio Head (RRH)
Layer 1
Layer 2
Layer 3
Base Band Unit (BBU)
Proprietary approach with no vendor interoperability
5G Core Network

Figure 8. Traditional RAN compared to O-RAN architecture.

In a white paper on the security benefits of O-RAN, the author shares how security is improved with an O-RAN architecture compared to traditional methods [66]. The author further reports on an incident in 2018 where major service provider networks were brought to a halt due to a specific vendor's proprietary software that utilized an expired certificate. With O-RAN, and its greater insight into the functional elements and its software-centric approach, it is likely that the issue would have been caught before a critical service outage occurred. The report concludes that O-RAN provides operators with more fine-grained control over the security of their networks and drastically reduces potential attack vectors that could result in the loss of service for the entire network by limiting its potential impact on parts of the network. While incidents such as this are rarely published, researchers at Nokia found that in 2022, at least 1/3 of surveyed cybersecurity professionals report eight or more breaches in a single category, including loss of funds, regulatory liability, theft of service, or service outage [67] related to 5G operations. This is further elevated as an area of concern given the fact that 5G services essentially rely on cloud services for many aspects of virtualized network functions. This means that there is a heightened risk of exposure to attacks from the web, which in 2018 accounted for 25% of all cyber incidents [68]. Configuration issues also compound the problem, as research has shown that 160,000 UPF interfaces were exposed to the web in 2023 [69].

As O-RAN allows for interoperability between software and hardware, there is a significant possibility that open-source software is employed for some of these functionalities. There has always been a discussion on whether open-source software is beneficial or detrimental to security efforts. Some corporations believe that releasing their code to the public increases the chance for malicious supply chain attacks, leading to the rise in demand for a Software Bill of Materials and illustrating the need for extensive code review and verification processes. Other corporations turn away from open-source releases due to the perceived loss in market presence, competitiveness, and intellectual property. In order for any open-source project to succeed and remain relevant, it therefore needs to provide high-quality, strong support and responsiveness to user demands, and low cost [70]. In a case where open-source code is used in an O-RAN deployment, a closed-loop security management system is introduced in [71]. It is presented as a solution to find Common Vulnerabilities and Exposures (CVEs) risks in open-source projects while aiding in providing timely alerts for potential future security threats. The authors also state that it guarantees that systems and applications adhere to relevant security standards and regulations, offering compelling proof to partners of their dedication to maintaining information security.

3.2.6. Network Slicing

As 5G has the ability to handle many different use cases for the end user, it becomes necessary for it to provide a mechanism to control and track these different usage requirements in order to maintain fairness and QoS on the network. This strategy is called network slicing. Physical network resources are partitioned into multiple logically isolated networks, such that each 'slice' can provide specific services corresponding to the usage requirements of the users' application [72]. A network slice is an independent virtual network that isolates resources, data flows, security features, network structure, and a clear and established QoS standard. These slices are segregated from one another and offer services to subscribers based on their specific requirements [73,74].

An important concept of network slicing is its method of isolating and allocating resources for all users. The authors of [75] point out three vital pillars of network slicing, in terms of isolation, which are summarized below.

1. Performance: Every slice is designed to meet specific service requirements. In order to protect the performance of one slice compared to other concerns on the network, there must be mechanisms in place to ensure that requirements are met as best as possible under changing network conditions while ensuring that security is not sacrificed in the process and without impeding the operations of other slices.
2. Security and Privacy: Faults or attacks impacting one slice must not impact another slice. Every slice must, therefore, provide its own independent security functions that prohibit unauthorized read or write access to configuration/management/accounting information.
3. Management: Each slice is seen as a separate network, and to achieve isolation, consistent policies and mechanisms need to be defined at the virtualization layer. The policies describe how different manageable entities must be separated from each other while the mechanisms within the system execute the protocols and enforce the defined policies. The author states that the interplay of both virtualization and orchestration is necessary.

Network slicing security is of great importance. In an article published by 3GPP [76], and referencing 3GPP TS 33.501 [2], the author offers a helpful perspective on the importance of creating, updating, and deleting network slices securely, which is summarized below.

1. Mutual authentication
    - Implemented between the management service consumer (the entity using or consuming the management services) and the management service producer (the entity providing the management services).
    - Transport Layer Security (TLS) is used to secure the communications
    - Designed to prevent unauthorized actions at the exposed management interfaces
2. Protection of management
    - Interactions between the management service consumer and producer are secured via TLS.
    - TLS includes protections such as:
        - Confidentiality Protection: Keeping the message exchanges confidential and encrypted;
        - Integrity Protection: Awareness that the data have not been changed or tampered with;
        - Replay Protection: Preventing the unauthorized replaying of previously captured messages to commit unauthorized actions.
3. Authorization of management
    - Management service consumers are authorized by the management service producer by way of an OAuth (Open Authorization) [77] mechanism.
    - Operators' local policies are taken into account during authorization.
    - Only specific authorized services are granted to the consumer.

UE access to a network slice is also covered in the article. A secure handshake needs to occur as a UE needs to communicate which slice to operate on with the Core Network. This happens by way of the Non-Access-Stratum (NAS) Signaling and Access-Stratum (AS) Signaling. Any information is always sent over NAS regarding a network slice after NAS security is established.

Network slicing has changed the way the telecommunication industry views network operations. Network slicing changed the landscape for operators from a network-as-an-infrastructure to a network-as-a-service paradigm. It has also reduced the need for a multitude of necessities within a network [78]. However, this switch brings new challenges and considerations related to network security. The authors of [74] created an in-depth survey of 5G network slicing with a focus on AI and ML. Their work states that AI is another potential weakness in a 5G network due to the rise of adversarial machine learning attacks. Adversaries attempt to fool the ML model by adding data samples with disrupting factors to force the appearance of otherwise hard-to-find vulnerabilities. To combat this, models can be trained with adversarial methods in mind, eventually developing a secure environment using adversarial machine learning [79].

Other discussions in [80] share the implementation of a network slice for military and government use. The authors share that key services of the slice would facilitate push-to-talk, fixed mobile convergence, prioritized access in case of disaster or war, autonomous edge, coverage on demand, satellite backhaul, many-to-many communication service, and the use of the RAN to sense and detect drones and perform jamming and anti-jamming operations.

3.2.7. Massive MIMO

Multiple Input, Multiple Output (MIMO) is a technology where multiple antennas are simultaneously utilized in both the transmitter and receiver to enable concurrent communication across multiple independent propagation paths. This can be leveraged to increase overall throughput for a single user, to concurrently communicate with multiple users, or to perform beamforming to more tightly control propagation aspects. MIMO technology falls within the realm of smart antenna technology. 5G technology can employ a vast array of antennas at base stations, allowing them to simultaneously serve multiple users on the same radio module or radio bearer (RB). Compared to traditional communication methods, massive MIMO enhances spectrum efficiency, minimizes user interference, and boosts energy efficiency, resulting in higher system throughput [53,81–85]. The author that presents the previous claim in [86] also shares a more in-depth analysis of how the usage of MIMO in 5G opens another vector of security requirements. Namely, MIMO security algorithms produce a large amount of noise if spatial redundancy is not sufficient, eavesdroppers can obtain information through users with poor connection, and theoretical reception indicators for MIMO security algorithms do not currently match measurable indicators. The author completed a survey of the literature on MIMO security and conducted a quantitative assessment of MIMO security posture within a 5G network. Simulations in the paper evaluated and predicted the situational level of active attack and passive eavesdropping via a dynamic and real-time prediction. Since the proposed evidence-based algorithm performs well in predicting the security situation of devices in a MIMO system, the results can be used to adapt security measures to specific security situations. Active eavesdropping detection and avoidance are furthermore discussed in [87] with promising findings in derivations of achievable secrecy rates and the probabilistic detection of eavesdroppers on a network. The findings show that with a higher number of base station antennas, there is a higher probability of detecting an eavesdropper. The detection of active attacks on MIMO channels is discussed in [88], and the use of NOMA (Non-Orthogonal Multiple Access) with a hierarchical security model is discussed in [89].

3.3. User Equipment

3.3.1. PHY Security

The physical layer (PHY) of any network is the lowest layer of a typical protocol stack and is responsible for generating and interpreting electrical signals to provide a foundation for communication. This layer of the communication scheme needs to be standardized just like the layers above it in order to maintain the expected level of user experience. The 5G physical layer offers the latest technology within 5G modems to bring the best experience to consumers compared to previous cellular generations. As 5G promises higher data rates, lower latency, and more connection density, these devices need to be specialized more than ever. Security is also a top priority when considering the PHY layer. For example, PLS leverages special channel coding and random characteristics of the wireless channel to protect the confidentiality of the information exchanged between two partners [90] over what is inherently a broadcast medium. Coding acts as a form of data protection, rather than encryption, to allow for bit error recovery. In the scenario of an eavesdropper, which represents an illegitimate passive listener observing a communication channel, attempts are made to intercept and record or decode the physical signals. Depending on how close the eavesdropper is to the signal's origin, it may be possible for the eavesdropper to succeed in their efforts, opening the door to potential data exfiltration. Three ways to combat this scenario at the physical layer are listed in [90]: power control, beamforming, and clustering. For each of these methods, the authors assume that the presence of an eavesdropper is known to the communicating parties.

Power control comes into play if an eavesdropper is identified in the region near a legitimate communication channel of a UE and the base station. Power control is a proposed method of heightening the confidentiality of 5G communications: when an eavesdropper is identified, the gNB and UE will reduce the power used in the radio link to lower the chances of the attacker being able to observe the signal. As stated in [90], this is a novel approach to solving this concern, and there has not been much development in making it become a reality. Beamforming is another tactic that can be used to circumvent unwanted listeners in a channel. Beamforming uses an antenna array and phase control of each constituent antenna's signal transmission in order to form a composite signal that, through phase alignment, is strong only in a specific and narrow direction while weak in all other directions [91]. Such highly directional transmissions make it very difficult for an eavesdropper to observe signals outside of a very narrow region, thereby protecting the communication and providing higher confidentiality. Beamforming also improves overall communication reliability by providing a better signal-to-noise ratio (SNR) for the legitimate channel. Physical layer security for 5G and beyond is also extensively covered in [92], where three 5G PLS solutions are presented: (1) a constellation rotation-based signal design for enhanced secrecy in D2D communications [93], (2) fine-grained security level characterization and statistical security guarantees for delay-sensitive services [94], and (3) Fountain Coding-aided security enhancements for IoT applications [95]. In the rotation-based scheme, the constellation of symbols is rotated to provide more protection from interference and also, in turn, improve the security of the D2D communications. The authors state that with the optimization of the constellation angle, an error floor can be created for the detection of non-intended messages while further improving transmission secrecy. The authors' proposed second method is meant to mitigate the success probability of eavesdropping in delay-sensitive operations. The authors introduce a new architecture for secure transmissions in 5G with fine-grained QoS requirements and integrated requirements on security, delay, sustainable traffic load, and reliability. Their last method mentioned further aims to hinder the abilities of an eavesdropper by way of Fountain Coding [96], which is a method used to encode packets in a stream of continuous data without re-transmissions. Their implementation utilizes an adaptive power allocation policy that varies SNR, thereby creating an even more difficult scenario for an eavesdropper to capture meaningful information. Physical layer security thus can benefit all three sectors of the security paradigm: confidentiality, integrity, and availability. This makes PLS so important for 5G and beyond and warrants continued research and exploration.

3.3.2. D2D, V2X

5G opens the possibilities for non-traditional communication methods, such as device-to-device (D2D) and vehicle-to-everything (V2X) methods. These two communication methods stem from the promises of 5G, allowing for even lower latency communication, larger device densities, and smarter transportation infrastructure. However, this brings with it new security considerations and challenges. The discussions in this section will focus on the considerations of D2D with V2X operations sharing many of these same requirements and concerns.

The correct authentication of connections of IoT and D2D communications is of high importance for maintaining private and secure operations. The authors of [97] present a lightweight crypto algorithm to securely connect 5G IoT devices to each other over D2D all while not being vulnerable to security exploits or attacks. They also present four major factors when considering security for D2D, which are summarized in the list below:

1. Authentication: Securing D2D communication requires authentication as one of the main aspects when connecting to the 5G IoT network. All networks need to have mechanisms in place to identify and verify users.
2. Data Confidentiality and Integrity: The use of hash functions and message authentication algorithms along with encrypted messages are vital to the confidentiality and integrity of the network. Prevalent concerns over these aspects stem from the number of eavesdropping, replay, and modification attacks that can occur if data are not secured.
3. Anonymity: The aspect of anonymity in a network is necessary so the identity of users is concealed and unknown to attackers. Anonymity prevents attackers from targeting specific users on the network. In the case of V2X, anonymity is paramount because when this principle is violated, an attacker could pinpoint a specific car, track its movement, and cause harm to an individual or a group of people.
4. Efficiency: As IoT devices have limited resources, it is important that they can request and obtain information on demand and without delay, as they are resource-constrained. The economical and efficient operation of communication systems is vital to the swift operations necessary in an IoT environment.

Further discussions in [4] present potential privacy concerns of D2D communications. In [98], the authors propose Cross-Physical-Application-Layer Security for D2D links, which introduces channel conditions alongside cryptographic keys to authenticate connections between devices. This approach utilizes physical security methods, such as channel-based key agreements and channel-based entity authentication, and applies them to public key cryptography and symmetric encryption at the application layer. Other surveys and studies of D2D 5G networks are presented in [99–101]. In [99], the challenges and research opportunities in D2D cellular interference and physical security are outlined. Sun et al. [100] propose a robust and efficient mutual authentication and key exchange method. The authors of [101] propose the use of biometric keys for stronger D2D link security.

3.3.3. SIM, Modems, Operating Systems

The security of a system is only as strong as its weakest link, and the user equipment has many attack vector opportunities for a threat actor. In this context, it is critically important to always use trusted hardware components and trusted operating systems on these devices to prevent unnecessary data leakage or unauthorized network access. NIST has composed a guide for enterprises on what should be considered essential when dealing with people using their personal devices for work activities. NIST speaks to reducing risk, improving the security of mobile devices, and enhancing visibility into the mobile device all while utilizing industry best practices. Within their guide, they provide resources for multiple different operations and scenarios that are summarized below [102]:

1. Identify and defend against network-based attacks, phishing scams, and mobile malware installation.
2. Force users to implement a password on devices.
3. Enable the selective device wipe feature for corporate data and applications to safeguard sensitive data.
4. Safeguard organizational data integrity by limiting an employee's capability to copy and paste, take screen captures, or save corporate data in unauthorized locations.
5. Understand the potential hazards associated with the Bring-Your-Own-Device (BYOD) strategies and take corrective measures to address threats, such as risks resulting from rooted or jailbroken devices.
6. Grant users the ability to reach secured business assets, such as knowledge bases, internal wikis, and application data.
7. Ensure executing code is genuine while maintaining the integrity of the runtime state and safeguarding the confidentiality of persistent memory data.
8. Secure data from eavesdropping during its transmission across a network.
9. Evaluate and verify the security of mobile applications utilized for work-related tasks.
10. Facilitate quick deployment and evaluation of BYOD solutions by providing detailed how-to guides covering initial setup and configuration for each component in the system.

Based on the above list, it becomes apparent that it is vitally important for any corporation or organization to practice information security to safeguard their data and their users' privacy and security. Time and time again, data leaks or hacks have made their way into the news with some being attributed to the actions of ill-informed employees falling victim to social engineering tactics like phishing attacks or as a consequence of a fault in the company's security architecture.

4. Zero Trust Architecture (ZTA)

Traditional network security focuses on perimeter defense, aiming to protect a network by preventing external access to network resources. However, this approach becomes ineffective once external actors gain a foothold within the network. Once this occurs, assets and resources within the network may no longer be protected. Zero Trust is the concept of transitioning from this perimeter-based static security toward a focus on securing individual assets, resources, and interactions within a network. With a Zero Trust Architecture, even after gaining access to a network, a malicious actor will still have to gain individual access to any resource within a network. The authors of [13] establish the following four pillars for ZTA:

Trust Evaluation: Access requests are considered untrusted. Trust analysis and risk reviews are conducted in an ongoing manner, and reviews may have changing requirements depending on a network's status.

Least Privilege: If a request is granted access after trust evaluation, the grant only encompasses the lowest level of permissions required to complete the specific requested task within the network. To ensure the security of other network resources, permission should only be granted to the required resources and no other resources.

Dynamic Policy: A network's access policy and trust evaluation should be changed depending on the network's behavior and security status.

Integrity Monitoring: Individual devices' security status and network asset activity patterns should be thoroughly evaluated by the architecture. Previously trusted activity should not be assumed safe for all network operations.

While these additional security measures can improve a network's response to malicious activity, there are trade-offs in network complexity and latency. To increase the speed of trust evaluation, the authors of [14] propose an intelligent ZTA (i-ZTA) to enhance the real-time processing of big data that will be present in 5G/6G networks. For military-specific applications, additional security metrics for trust evaluation were proposed in [103] to support the needs of tactical edge networks. The authors of [38] present a virtual evolved packet core and virtual software-defined perimeter for the 5G core using machine learning. This method proved effective for trust evaluation in detecting denial of service attacks.

AI was also leveraged to create a Self-Driving Network (SelfDN) in [39] to evaluate network performance with telemetry data. In a large-scale deployment, a framework for federated learning was proposed to monitor network performance as a whole. To aid with the computational complexity of a ZTA, the authors of [104] propose dividing the concepts of Zero Trust into modules that can distribute the computational load throughout the network.

4.1. Zero Trust Applications in 5G

IoT: While Zero Trust is desirable for IoT, there are technical challenges that will potentially result in several issues [105]. Network scalability is a major concern with the millions of devices expected to connect through IoT. The sheer number of devices complicates the implementation of policy enforcement. The devices included in IoT infrastructure are simple and resource-constrained and are not appropriate for integrating a robust and secure system. Therefore, this creates an attack vector in the exploitation of inherent weaknesses of the IoT devices [106]. The authors of [105] propose that a policy engine and policy administrator be external to the 5G network and IoT devices, as shown in Figure 9. Through this architecture, no device is implicitly trusted, and all activities and network access must first be reviewed and approved through the Policy Enforcement Point (PEP).

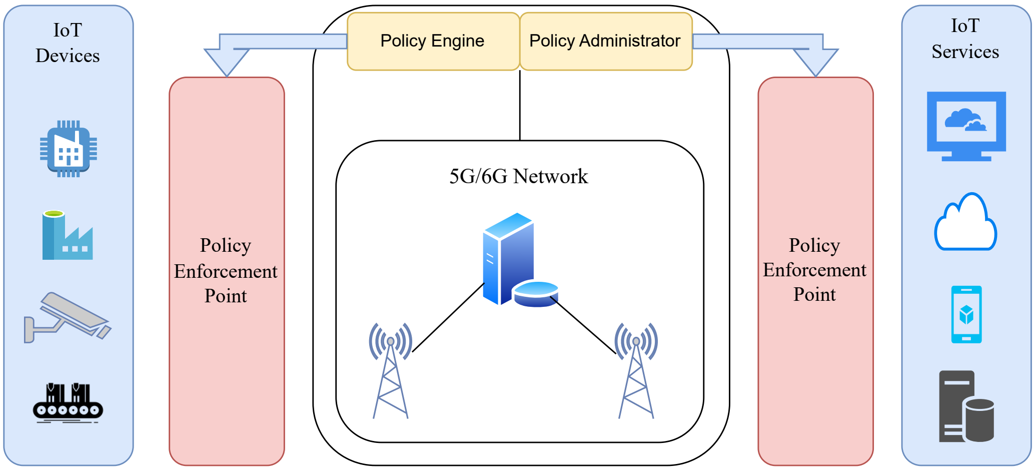

Figure 9. ZTA overview for IoT.

Smart Grid: Another approach to expanding 5G connectivity is on the power grid. Creating a more connected grid would allow for better maintenance, customer satisfaction, data and analytics, and more. One problem with creating a virtually layered smart grid is the question of reliability and security. A novel approach to connecting power grid devices over 5G using a ZTA is discussed in [107], listing the pros and cons of the proposed Zero Trust method. The author describes the necessity for the network to be under a Zero Trust Architecture due to the mission-critical nature of the smart grid and all of its components.

MEC: Multi-access Edge Computing provides an opportunity to reduce the overall load on cloud services and latency experienced by the end users by allowing applications to be deployed at the edge of a 5G network. With less computational offloading to cloud services, edge computing would foster better resource efficiency, requiring less bandwidth for each edge device and thereby supporting a larger number of users or end devices. The authors in [108] describe the general security threats to MEC in 5G: infrastructure security, MEC platform (MEP) security, edge UPF (User Plane Function) security, communication security with the 5G core, networking security and MEC application security. Of these listed security threats, MEP, UPF, and MEC application security are particularly important. The approach described in [108] to address this need is a dual-layer ZTA to enforce ongoing authentication with the UE and the CN, along with reinforcement authentication with the edge network, which in the paper's use case scenario is an industrial environment. Through this dual ZTA architecture, a user's derived 'trust value' can be continuously monitored and acted upon, for example, by forcibly de-authenticating the user or device if necessary. Given the vast applications of MEC, additional investigation should be placed on methods that secure the various traffic these devices would produce.

This concept is expanded with an example architecture for Intelligent ZTA, as described in [14], where the authors introduce an additional Network Exposure Function to the Core Network. This function acts as an intermediary between MEC hosts and the MEC management function, as shown in Figure 10. In this proposed architecture, the MEC host performs internal security scanning through the "Intelligent Platform Portal", which is used by the MEC management system's trust evaluation.

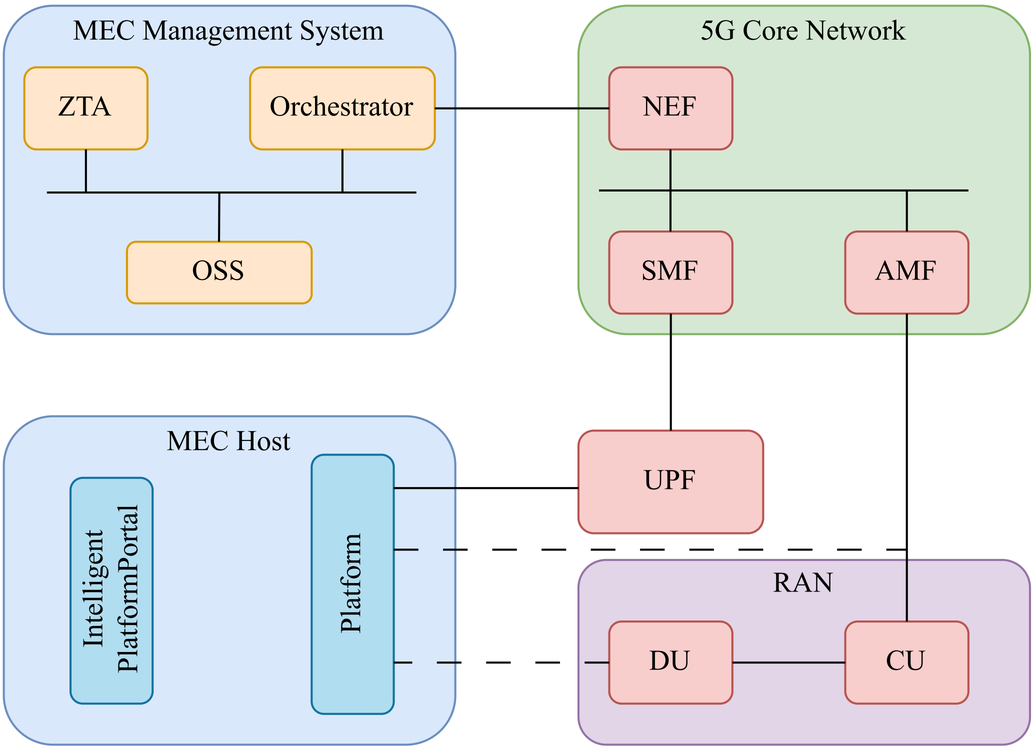

Figure 10. Proposed Intelligent ZTA for MEC.

4.2. Risks and Limitations of ZTA

While ZTAs show great promise for improving security in computer networks, the scientific literature does outline limitations with the currently proposed approaches. One such limitation is the lack of universal authentication methods for all devices in ZTAs. The authors of [109] outline continuous authentication methods commonly proposed with ZTA, but many of these authentication methods are device-specific and cannot be accomplished on IOT or other resource-constrained devices. This is explained further in [110], as access control, identity authentication, and trust assessment still require significant research. In [111], the authors argue that the lack of quantitative analysis of zero trust's benefits and drawbacks are not adequately considered–as are the ramifications of user-related network interactions.

5. Proposed Future Security Mechanisms

5.1. Blockchain

Blockchain technology has brought a new perspective into the security landscape due to its ability to be decentralized and flexibly leveraged by different applications. The core tenet of blockchain is that it protects and upholds the integrity of the data stored within, as it operates as a chain-linked data structure with a decentralized, unfalsifiable, and highly protected ledger framework. This architecture could be used as an alternative to 5G security systems in place now, as described in the following subsections.

5.1.1. Blockchain for Ultra-Dense Networks

One area of 5G where blockchain can positively influence the integrity of a network is in UDNs (Ultra-Dense Networks). UDNs play a big part in 5G as they play a significant role in meeting the requirements of high reliability and usability for highly populated areas. This means that in a highly dense area, there will be many base station nodes that a UE may interact with over time. A security concern is that there could be false base stations in this dense region, which aim to maliciously gain access to information on the users, thereby impacting confidentiality on the network. A new method of verification is presented in [112], where the UE is authenticated more efficiently to a known group of nodes via the blockchain. The proposed method incorporates all of the known legitimate APs (access points) in the network and passes this information to the UE to allow for seamless operation. The authors also claim that this operation is more efficient in utilizing the radio frequency bands, as it does not require as much radio access compared to regular AP to UE authentication.

5.1.2. Blockchain for Mobile Edge Computing

Another use case for blockchain in 5G is in the MEC space, which was introduced earlier. MEC enables more efficient usage of network resources but also provides for a better end-user experience. However, there are significant challenges for reliability, data privacy, and security with MEC. The authors of [113] outline the risk of attacks on edge nodes disrupting an entire system and consequently showing potential issues that can severely degrade MEC reliability. The incorporation of blockchain with MEC—both being architecturally decentralized systems—can address many of the safety and security issues within such a system, as the survey in [113] shows. For example, blockchain technology can help alleviate the challenge in MECs of ensuring the secure exchange of configuration information during MEC service scaling, migration, and adaptation. During those changes to the edge deployments of MEC services, configuration and authentication information needs to be exchanged between the orchestrator and the edge deployments, posing a significant risk of intercepts, falsification, and more. By using distributed ledgers, this information can be securely provided and accessed, and risks to their authenticity can be greatly reduced. Another significant benefit is to the data integrity, using data compute operations at the mobile edge. Here, ledgers can be used to ensure the immutability of the data—an inherent property of blockchain technology [113].

Additionally, multiple works have been completed on improving MEC's reliability through blockchain technology. These works include the dynamic offloading of individual transactions and computational tasks [114–116]. For data privacy, the authors of [117] use smart contracts to complete and register distributed authentications without a central authority.

Meanwhile, the authors of [118] speak to the fact that typically, the privacy of most MEC systems only prioritizes user security at the expense of network topology privacy. Keeping the network's inner workings hidden from the user landscape increases the confidentiality of the network and thereby makes it more difficult for a threat actor to identify potentially viable attack vectors. Having a trusted MEC system enables the system to provide more reliable services and achieve lower latency in certain applications. The authors propose a method of using blockchain technology in order to verify different routes in cross-domain MEC architectures using different known ledgers. Their findings show that it is a feasible solution, as their simulation results demonstrate similar or better latency compared to normal routing algorithms.

5.1.3. Blockchain Uses in 6G

6G will bring many opportunities for the integration of blockchain technology. There are many different areas within 6G that can benefit from the use of blockchain technology. In a survey of opportunities and challenges of blockchain application in 6G, many security-related cases are presented, which are listed below [119].

- Intelligent Resource Management;
- Elevated Security Features;
- Industrial Applications;
- Smart Healthcare;
- Decentralized 6G Communications ;
- Authentication, Availability, Integrity.

The authors share how blockchain technology can be a candidate to improve these aspects due to its major fundamental properties and add further trust to a network. If implemented correctly, most apparent properties include but are not limited to the following: decentralization, transparency with anonymity, provenance and non-repudiation of transactions, immutability and tamper-proof of distributed ledgers, and elimination of single points of failure.

Another proposed area for integration into 6G is the use of blockchain technologies to ensure the authenticity of training data from edge devices used by machine learning models. Data are usually stored and processed on centralized servers, owned or rented by network operators, where the source cannot always be guaranteed to be authentic. One method could be to encrypt the data, but the authors in [120] claim it can be more efficient and verifiable if the data-sharing technique is decentralized without the use of a third party entity or intermediary. Further studies show that blockchain can also be used in federated learning architectures where local edge device learning model updates are exchanged and verified [121]. All training results from the edge devices are put through a validation process, meaning there is no need to specifically identify and isolate untrustworthy devices in the federation.

5.2. Post-Quantum Cryptography

As quantum computers become more of a reality over time, it is important to consider the implications of these machines and their capabilities. Quantum computers pose a significant risk to classical cryptography, as approaches such as Shor's algorithm make it feasible to effectively break current public key cryptography approaches given a quantum computer with a sufficiently high number of qubits. In 1994, Peter Shor created a quantum algorithm for factoring integers and solving discrete logarithmic problems, essentially breaking two commonly used encryption algorithms, Elliptic Curve Cryptography (ECC) and RSA. Currently, the US implements AES encryption as the standard approach, replacing its predecessor DES, which is now considered insecure. Fortunately, no current quantum computer is powerful enough for this task, as the number of available qubits in current quantum computers falls far short of the required amount to effectively apply Shor's algorithm [122]. However, if advances are not made in current encryption schemes in order to protect against quantum attacks, AES may eventually be vulnerable to quantum attacks. Understanding the theory behind these claims also sheds more light on whether or not quantum computers threaten 5G operations and or its safeguards for confidentiality, integrity, and availability. Current efforts also focus on a new generation of cryptographic algorithms that aim to be robust against such quantum attacks. These new algorithms are known as post-quantum ciphers or post-quantum cryptography (PQC).

5.2.1. Possible Post-Quantum Ciphers

As post-quantum ciphers do not have the traditional building blocks of a normal cipher, they do not have a direct 1:1 relationship [123]. The authors in [123] offer four post-quantum ciphers that would protect against confidentiality attacks when quantum devices are more relevant and powerful. These four algorithms are: Lattice-Based Cryptography, Hash-Based Cryptography, Code-Based Cryptography, and Supersingular Elliptic Curve Isogeny Cryptography. The Lattice-Based approach incorporates an NP-hard problem into cryptography. This method takes a normal vector lattice and seeks to find the shortest non-zero vector in the vector space spanned by the basis vectors. NTRU [124] is a commonly known Lattice-Based scheme, which has been tested and revised into two new standards; IEEE Standard 1363.1 and ANSI standard X9.98. Hash-Based Cryptography incorporates the eXtended Merkle Signature Scheme (XMSS), as blockchain technology has been studied more robustly. One code-based approach is the McEliece scheme, which was introduced in 1978. McEliece based his method on the implementation of computing random linear transformations of an error-correcting code's generator matrix. Only the private key holder would know the factors of the matrix. Oftentimes, this method is overlooked for PQC due to it needing extremely long keys [125].

NIST has made great strides over the recent decade in verifying and vetting quantum-resistant cryptographic algorithms from research groups around the world. NIST made a public call for submissions in December of 2016 and has narrowed the field of algorithms down to three as of the publication of this paper. Three drafts were published as part of the Federal Information Processing Standards (FIPS) in August of 2023, showcasing post-quantum algorithms resistant to quantum computer decryption methods. Each draft includes a complete description of each algorithm and its constituent functions. FIPS 203 [126], based on CRYSTALS (Cryptographic Suite for Algebraic Lattices)-Kyber [127], is also referred to as the Module-Lattice-based Key-Encapsulation Mechanism Standard that allows users to generate a shared secret key for communication over a public channel. FIPS 204 [128] is based on the CRYSTALS-Dilithium approach [129] and is also known as the Module Lattice-Based Digital Signature Standard. Originally published in the CRYSTALS-Dilithium paper, the authors share that their implementation operates in constant time and has a public key 2.5 times smaller than the previously most efficient lattice-based schemes. In FIPS 205 [130], the Stateless Hash-Based Digital Signature Standard, based on the SPHINCS+ [131] paper submission, is used to protect messages and to perform the verification and validation of digital signatures. As 5G progresses in its rollout and maturation in the near future, it is imperative that post-quantum cryptography is incorporated in areas where current classical algorithms are at risk in order to maintain the confidentiality and integrity of user data. This also applies to other standards on the internet, such as TLS. The best-case scenario for such standards would support PQC drop-in replacements. In order to make this a reality, associated Certification Authority (CA) infrastructure is necessary to issue, manage, and revoke these new PQC keys, however [123].

5.2.2. Post-Quantum Cryptography in 5G and 6G

The direction of computing is headed toward quantum processing, which will directly affect many current and widely used encryption methods. With access to a powerful enough machine, these traditional schemes will be rendered useless, as discussed earlier. The 5G authentication protocols are thus primed to fall victim to quantum decryption due to 5G-AKA and EAP-AKA both having a public key architecture. This realization has caused calls for the adoption of PQC into the 5G standard by NIST and other researchers. However, at present, 3GPP does not specify standards for PQC incorporation into 5G. An article covering the migration to PQC in mobile networks details that with the current pace of PQC standardization, it is presumed that PQC will be rolled out in 5G with 3GPP Release 19 or 20 [132] at the earliest. This will lead right into 3GPP Release 21, which will be the first 6G standard, to be issued around the year 2030.

Researchers have been investigating the use cases for PQC in 6G with the notion that 6G will incorporate more connected AI/ML, terahertz (THz) communications, automation, operations over Non-Terrestrial Networks (NTNs), and more. An important consideration of the use of PQC is the amount of computation required to encrypt and decrypt communications. This is a similar problem to what we currently face for resource-constrained devices, which then often leads to these devices resorting to more lightweight cryptographic algorithms. One aspect explored therefore is the usage of PQC algorithms for IoT applications that are more efficient both in terms of storage and computation. The authors of a recent 6G security survey share that lattice-based algorithms are best suited for IoT applications [133]. Since this approach uses smaller key types compared to other algorithms, it could be a candidate for use in a constrained 32-bit device. The authors do note that these are only considerations and have not yet been standardized specifically for IoT. Some performance analyses of popular PQC algorithms were conducted on a Raspberry Pi 4 to inspect the computational duration requirements for key generation, encapsulation, and decapsulation along with the signing and verification of messages [134]. Their results show that the Dilithium and Kyber algorithms, presented earlier, are the best all-around approaches for low-latency applications. With low delays, it is presumed that a resource-constrained device will have a better possibility of extended battery life while also ensuring that sufficient compute resources remain for other tasks. The authors' results have been visually recreated in Figures 11 and 12 from [134]. Computational resources will be a major consideration for the rollout and adoption of any 6G standards, as it aims to incorporate a higher volume of IoT devices along with a diverse set of personal, business, and medical devices. This will also be important for the continued expansion of NTNs targeted by 6G in order to maintain reasonable latency benchmarks when communicating with, or through, satellite constellations.

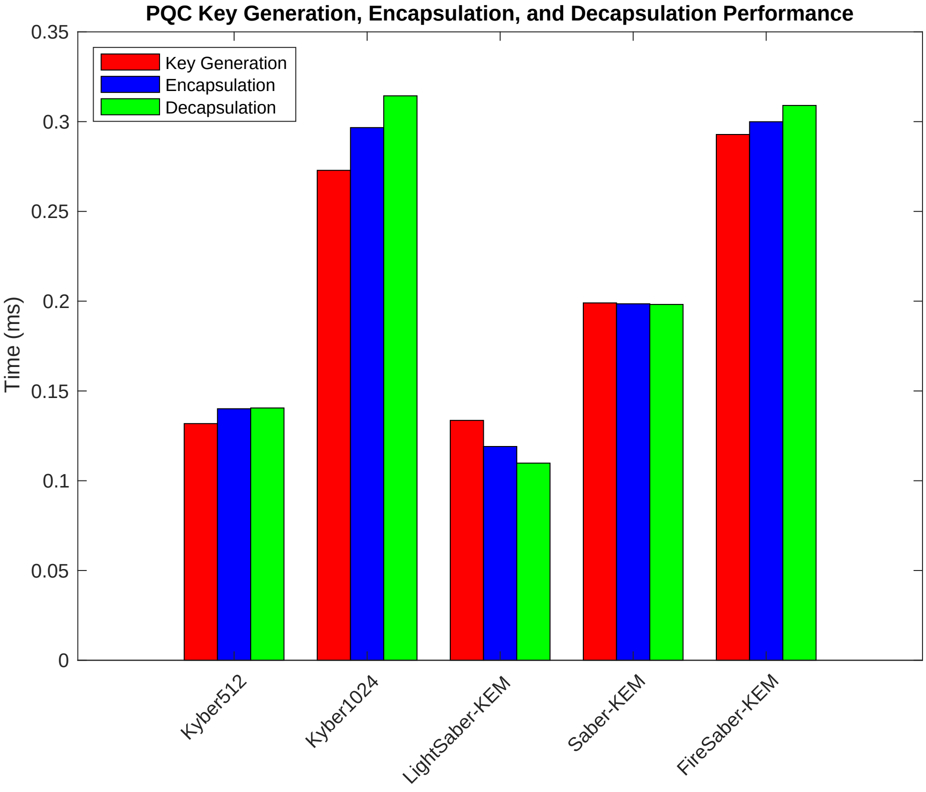

Figure 11. Results from [134] for popular PQC algorithms evaluating keypair signing and verification performance on a Raspberry Pi 4.

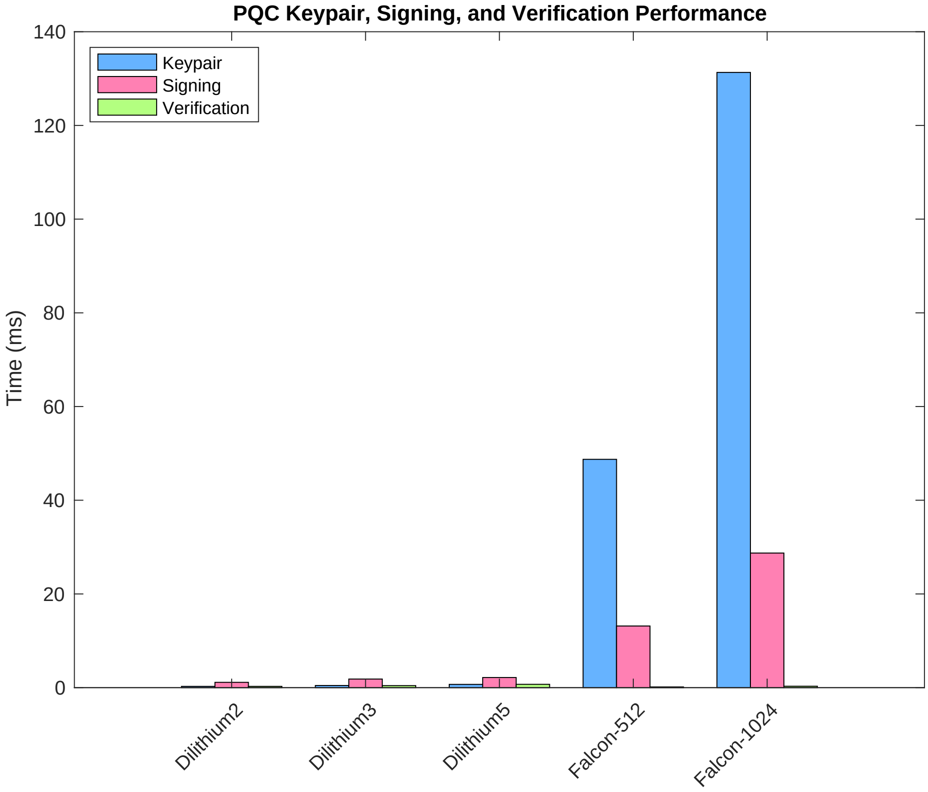

Figure 12. Results from [134] for popular PQC algorithms key generation, encapsulation, and decapsulation performance on a Raspberry Pi 4.

5.3. Artificial Intelligence for 6G

While 3GPP has not implemented any AI requirements into the current slate of 5G standard releases, advancements in connectivity nonetheless present significant opportunities for improving performance and security through AI implementations in 5G but more importantly present extensive opportunities for AI to become a key consideration in the standard development for 6G. Already, numerous options are taking shape for use cases of AI in the 5G RAN, such as for resource management, energy efficiency, load balancing, and mobility operations [135]. Similarly, there are extensive efforts and oferrings related to 5G cybersecurity aspects utilizing AI/ML integration, network provisioning and orchestration, and more.

Fulfilling requirements of 6G for applications such as Extended Reality (XR), connected robotics, autonomous systems, and eHealth through body area networks (BANs) requires a system reliability that meets or exceeds 99.99999% reliability (also known as "Seven Nines"), and a significant boost to throughput far beyond that of 5G, up to 1 Tb/s [136]. To enable these applications, AI is anticipated to assist with SDNs and resource allocation for both core and edge applications [137]. Some applications for which AI has been proposed are network slicing and RIS beamforming, which have been outlined in Section 3, as well as additional areas described below.

5.3.1. RAN Intelligent Controller

5G networks are incredibly complex from a protocol and software reliance perspective but even more so from a system management perspective. This is especially true for the complex, highly time-dependent and demanding task of radio resource management. To allow more responsive system operations, and to widen interoperability opportunities, O-RAN presents a significant change to the RAN organizational and operational structure. In addition, it created the opportunity to improve the monitoring and management of the RAN's most crucial tasks in the form of the RAN Intelligent Controller (RIC) defined by 3GPP. The RIC comes in two variants, Non-Real Time and Real Time. Both of these mechanisms are provided through virtualized network functions (VNFs) and serve to optimize RAN operations including improving radio unit efficiency, network slicing, high-bandwidth and low-latency provisioning, as well as for beamforming and radio resource management [138]. Researchers in [139] created their own ML workflow and executed the model on O-RAN compliant hardware. Through their study, they present suggestions on making the RIC more efficient by way of hardware accelerators, federated learning, and ML model packaging, to name a few. The RIC presents numerous opportunities for AI/ML-assisted 5G operations, which are expected to become central in the development of 6G as well.

5.3.2. Proposed Security Features

Security in 6G will need to address the existing vulnerabilities identified in 5G, as NFV and SDN will continue to be a central and pivotal aspect to 6G system design [140]. 6G will also further embrace the use of AI/ML for aspects such as QoS and Quality of Experience (QoE), which expose another attack surface to malicious actors that can directly impact the end user applications and user experience. To combat the threats of this expanded attack surface, predictive models for QoS and QoE have been proposed [141] as well as intrusion detection models [142] and anomaly detection models [143].

These methods take different approaches to attack identification and prevention. The predictive QoS models analyze current network information and predict QoS challenges through regular user traffic but also any malicious traffic that may occur on the network. Such predictive analysis methods aim to prevent an attack from even occurring, while intrusion and anomaly detection are used in response to an attack occurring. While intrusion and anomaly detection both analyze current network traffic to identify a possible attack, their methodology is slightly different. Intrusion detection focuses mainly on outside access to network operations that should not have been authorized during normal activities, while anomaly detection takes a holistic approach to network traffic and aims to detect any malicious traffic from new or existing connections.

5.3.3. Risks of AI in 6G Security

While AI can improve security through more agility and responsiveness, rather than by incorporating frequent updates and changes to monitoring capabilities in traditional security methods, it is expected that it can also be leveraged for malicious attacks against 6G. These attacks are often called adversarial model attacks [144] and often constitute injecting false data to change a security model's behavior or evading detection from models all together. Adversarial model attacks, like the attack outlined in [144], attempt to avoid known security models, such as intrusion detection systems. These attacks are also referred to as evasion attacks [145], which augment normal traffic on a network to gain information without being detected or deteriorate network performance as in a poisoning attack [146].

There are also inherent risks to implementing AI models that are not fully explainable. When models are implemented that are treated as "black boxes", there are considerable risks to deployment, since model performance cannot be anticipated for all input parameters. This has led to an increase in works for Explainable AI [147], ensuring that models are fully understood before deployment. This is expected to be a crucial component to the use of AI/ML models in 6G system operations, particular for cyber forensics aspects, troubleshooting and more. As can be seen, while AI and ML are expected to be pivotal to 6G operations, they are also expected to be a pivotal consideration as a source and method of cyber attacks and thus provide tremendous potential for additional research in order to ensure their reliability, trustworthiness, and effectiveness in future cellular network operations.

6. Conclusions

In this article, the current landscape of 5G security was assessed from a systematic vantage point along with an exploration of considerations toward a Zero Trust Architecture in a 5G setting. This work was motivated by furthering the understanding of the current important topics regarding 5G security for use within academia, industry, and government. The presented topics encompass all three primary 5G system components (Core Network, Radio Access Network, and the User Equipment) and further deep dives into their individual aspects. By scrutinizing these elements, both individually and with their interconnections in mind, we uncovered major security challenges, summarized in Table 4, that must be met with stringent security measures. Other 5G and 6G security considerations, such as the use of blockchain, post-quantum cryptography, and AI security were also discussed to continue working toward countering emerging threats and the pursuit of a more private, trustworthy, and secure system.

Table 4. A list of the most important security challenges and their proposed resolutions that have been uncovered in this survey.

Uncovered Security Challenges Presented in Our Survey	
Security Challenge	**Proposed Resolution**
5G-AKA user privacy and traceability exposure [22]	Encrypt the initial control messages during the 5G-AKA authentication procedure.
Compromised USIM leading to data privacy issues [26]	Utilize a Diffie–Hellman key exchange to enable PFS.
Key refresh for the UE and serving network	TS 33.501 [2] states that 24 h is the maximum time a key can be valid but does allow for operators to refresh keys on a more frequent basis.
Exposure of an NFV hypervisor due to misconfiguration and cross contamination of shared resources [28,29]	Provided clear and succinct steps for configuration of systems and implemented a ZTA with mutual authentication and constant network monitoring.
Potential loss of confidentiality when connected to an untrusted core network	Careful consideration of network usage in a roaming scenario, mutual authentication and adopting ZTA.
Securing backhaul networks in 5G [37]	The use of mutual authentication for devices on the network, ZTA, PFS, light-weight cryptography, and physical tamper resistance.
Network downtime due to specific vendor software problems	Usage of an O-RAN architecture that gives operators more fine-grained control over the security and operation of their network [66].
Verifying security robustness of open source software and O-RAN architecture	Usage of a closed-loop security management system outlined in [71].
Network slicing attacks using adversarial machine learning with the goal of forcing the appearance of a hard-to-find vulnerability [74]	Train AI/ML models with adversarial methods in mind [79].
Eavesdroppers on the physical channel in 5G communications	The usage of beamforming to create a more focused connection between the UE and gNB, achieving weak signal strength outside of the narrow beam region [91].
Passive eavesdroppers on a link with RIS-aided beamforming	Utilize multiplicative random process at the RIS to mitigate the effectiveness of a passive eavesdropper [60].
Illegal addition of RIS-aided beamforming equipment	Enforce strict authentication methods for RIS systems and continuously monitor the radio conditions at the edge of the deployment, possibly through the use of AI/ML.
Security measures for resource-constrained IoT devices	A lightweight crypto algorithm presented in [97] to securely connect 5G IoT devices over D2D.
Evaluation of trust in a ZTA	Trust evaluation schemes discussed in [103] to support the needs of tactical edge networks in a military setting.
Connection and authentication of critical infrastructure over 5G	A novel approach of connecting power grid devices over 5G in a ZTA is discussed in [107].
False base stations attack in ultra-dense networks	Using blockchain technology to verify a cluster of base stations in an ultra-dense network is presented in [112], claiming it is more efficient than normal authentication methods.
Maintaining confidentiality in a world with quantum computers	NIST has published three drafts [126,128,130] of post-quantum cryptographic algorithms that are currently not breakable by quantum computers.

This article serves as a comprehensive survey of understanding the diverse nature of 5G security, its limitations, risks, and potential solutions. It highlights valuable insights into the operational mechanisms of 5G security and the importance of robust security protocols for stakeholders across the 5G and 6G community. As 5G continues to evolve into 6G, the principles and findings outlined in this survey and the accompanying literature will be vital in shaping the security landscape around 6G and beyond.

Author Contributions: Investigation, P.S., M.B., M.H. and H.S.; writing—original draft preparation, P.S., M.B. and M.H.; writing—review and editing, P.S., M.B., M.H., H.S., J.D. and J.R.; supervision, H.S. and M.H.; project administration, H.S., M.H., J.D. and J.R.; funding acquisition, H.S. and M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been supported by the University of Nebraska-Lincoln's Advanced Telecommunications Engineering Laboratory (TEL) and Belcan Government Solutions (BGS) under grant #TEL-Belcan-5G23. Founded in 1958, Belcan is a global technology leader with over 10,000 professionals serving more than 900 customers from over 60 locations worldwide with advanced design, manufacturing, and engineering expertise. Belcan Government Solutions couples its mature commercial best practices to U.S. Department of Defense (DoD) and International Council on Systems Engineering (INCOSE) directives and guidelines to reduce risk, lower cost, and optimize efficiency for the rapid delivery of scalable solutions to its diverse clients. Belcan Government Solutions' Digital Foundry is strategically located in Bellevue, Nebraska, near UNL's TEL lab and Offutt Air Force Base.

Data Availability Statement: This study did not report any data.

Conflicts of Interest: The authors Joseph Delloiacovo and John Reed are from the company Belcan Government Solutions (BGS). Hamid Sharif has received a research grant from Belcan Government Solutions (BGS). The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

3GPP	3rd Generation Partnership Project
5G	5th Generation
CN	Core Network
RAN	Radio Access Network
UE	User Equipment
PQC	Post-Quantum Cryptography
IoT	Internet of Things
ZTA	Zero Trust Architecture
gNB	gNodeB
SDN	Software-Defined Network
NFV	Network Function Virtualization
MEC	Mobile Edge Computing
TS	Technical Standard
AKA	Authentication and Key Agreement
SN	Serving Network
AN	Access Network
AUSF	Authentication Server Function
SEAF	Security Anchor Function
NIST	National Institute of Science and Technology
SBA	Service Based Architecture
O-RAN	Open Radio Access Network
CDM	Continuous Diagnostics and Mitigation
ICAM	Identity, Credential, and Access Management
MNO	Mobile Network Operator
EAP	Extensible Authentication Protocols
PFS	Perfect Forward Security

DH	Diffie–Hellman
USIM	Universal Subscriber Identity Module
UDM	Unified Data Management
SUPI	Subscription Permanent Identifier
SUCI	Subscriber Concealed Identifier
DOS	Denial of Service
MA	Mutual Authentication
ASIC	Application-Specific Integrated Circuits
FPGA	Field-Programmable Gate Array
SMC	Security Mode Control
RRC	Radio Resource Control
PUF	Physical Unclonable Function
NPN	Non-Public Networks
TSN	Time-Sensitive Networking
NR	New Radio
LTE	Long-Term Evolution
VANET	Vehicular Ad Hoc Network
WLANs	Wireless Local Area Networks
HetNet	Heterogeneous Network
EPC	Evolved Packet Core
UMTS	Universal Mobile Telecommunications System
O-vRAN	Open Virtualized Radio Access Network
CVE	Common Vulnerabilities and Exposures
QoS	Quality of Service
TLS	Transport Layer Security
RIS	Reconfigurable Intelligent Surface
IRIS	Illegal Reconfigurable Intelligent Surface
OAuth	Open Authentication
NAS	Non-Access Stratum
AS	Access Stratum
MIMO	Multiple Input Multiple Output
RB	Radio Bearer
NOMA	Non-Orthogonal Multiple Access
PHY	Physical Layer
PLS	Physical Layer Security
SNR	Signal-to-Noise Ratio
D2D	Device to Device
V2X	Vehicle to Everything
BYOD	Bring Your Own Device
i-ZTA	Intelligent Zero Trust Architecture
SelfDN	Self-Driving Network
MEP	Mobile Edge Computing Platform
UPF	User Plane Function
UDN	Ultra Dense Network
AP	Access Point
ECC	Elliptic Curve Cryptography
XMSS	eXtended Merkle Signature Scheme
FIPS	Federal Information Processing Standards
CRYSTALS	Cryptographic Suite for Algebraic Lattices
CA	Certificate Authority
QoE	Quality of Experience
RIC	RAN Intelligent Controller
VNF	Virtualized Network Functions
THz	Terahertz
NTN	Non-Terrestrial Networks

References

1. Vintilă, C.E.; Patriciu, V.V.; Bica, I. Security analysis of LTE access network. In Proceedings of the 10th International Conference on Network, Valencia, Spain, 9–13 May 2011; pp. 29–34.
2. *TS 33.501*; Security Architecture and Procedures for 5G System. 3GPP: Valbonne, France, 2023. Available online: https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/ (accessed on 10 August 2023).
3. *TS 33.401* ; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evoltuion (SAE); Security Architecture, Release 17, V17.4.0. 3rd Generation Partnership Project: Valbonne, France, 2023.
4. Dutta, A.; Hammad, E. 5G Security Challenges and Opportunities: A System Approach. In Proceedings of the 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 10–12 September 2020; pp. 109–114. [CrossRef]
5. Cao, J.; Ma, M.; Li, H.; Ma, R.; Sun, Y.; Yu, P.; Xiong, L. A Survey on Security Aspects for 3GPP 5G Networks. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 170–195. [CrossRef]
6. de Castro Nunes Borges, V.O.; Rosa, R.L. General Aspects of Information Security in 5G Networks: Survey. Available online: https://infocomp.dcc.ufla.br/index.php/infocomp/article/view/3072 (accessed on 16 February 2024).
7. Sachdeva, T.; Kumar, S.; Diwakar, M.; Singh, P.; Pandey, N.K.; Choudhary, S. Comparative Analysis of 5G Security Mechanisms. In Proceedings of the 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 3–4 March 2023; pp. 1–4. [CrossRef]
8. Zhang, S.; Wang, Y.; Zhou, W. Towards secure 5G networks: A Survey. *Comput. Netw.* **2019**, *162*, 106871. [CrossRef]
9. Tashtoush, Y.; Darweesh, D.; Karajeh, O.; Darwish, O.; Maabreh, M.; Swedat, S.; Koraysh, R.; Almousa, O.; Alsaedi, N. Survey on authentication and security protocols and schemes over 5G networks. *Int. J. Distrib. Sens. Netw.* **2022**, *18*, 15501329221126609. [CrossRef]
10. Ounza, J.E. A taxonomical survey of 5G and 6G security and privacy issues. *Glob. J. Eng. Technol. Adv.* **2023**, *14*, 042–060. [CrossRef]
11. Ramezanpour, K.; Jagannath, J.; Jagannath, A. Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective. *Comput. Netw.* **2023**, *221*, 109515. [CrossRef]
12. Park, J.H.; Rathore, S.; Singh, S.K.; Salim, M.M.; Azzaoui, A.; Kim, T.W.; Pan, Y.; Park, J.H. A comprehensive survey on core technologies and services for 5G security: Taxonomies, issues, and solutions. *Hum.-Centric Comput. Inf. Sci.* **2021**, *11*.
13. Stafford, V. Zero trust architecture. *Nist Spec. Publ.* **2020**, *800*, 207.
14. Ramezanpour, K.; Jagannath, J. Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Comput. Netw.* **2022**, *217*, 109358. [CrossRef]
15. Bhardwaj, A. 5G for Military Communications. *Procedia Comput. Sci.* **2020**, *171*, 2665–2674. [CrossRef]
16. Marsh, S.P. Formalising Trust as a Computational Concept. Available online: https://www.cs.stir.ac.uk/~kjt/techreps/pdf/TR133.pdf (accessed on 16 February 2024).
17. Sultan, A. *5G System Overview*; 3GPP: Valbonne, France, 2022.
18. Khan, R.; Kumar, P.; Jayakody, D.N.K.; Liyanage, M. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 196–248. [CrossRef]
19. Prasad, A.R.; Zugenmaier, A.; Escott, A.; Soveri, M.C. *3GPP 5G Security*; 3GPP: Valbonne, France, 2018.
20. Ben Henda, N.; Wifvesson, M.; Jost, C. An Overview of the 3GPP 5G Security Standard-Ericsson. Available online: https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview (accessed on 16 February 2024).
21. *TS 33.501*; Technical Specification Group Services and System Aspects; Security Architecture and Procedures for 5G System Release 18, V18.2.0. 3rd Generation Partnership Project: Valbonne, France, 2023.
22. Munilla, J.; Burmester, M.; Barco, R. An enhanced symmetric-key based 5G-AKA protocol. *Comput. Netw.* **2021**, *198*, 108373. [CrossRef]
23. Koutsos, A. The 5G-AKA authentication protocol privacy. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 17–19 June 2019; pp. 464–479.
24. Basin, D.; Dreier, J.; Hirschi, L.; Radomirovic, S.; Sasse, R.; Stettler, V. A Formal Analysis of 5G Authentication. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security CCS '18, New York, NY, USA, 15–19 October 2018; pp. 1383–1396. [CrossRef]
25. Khan, H.; Martin, K.M. A survey of subscription privacy on the 5G radio interface-the past, present and future. *J. Inf. Secur. Appl.* **2020**, *53*, 102537. [CrossRef]
26. Edris, E.K.K.; Aiash, M.; Loo, J.K.K. Formal verification and analysis of primary authentication based on 5G-AKA protocol. In Proceedings of the 2020 Seventh International Conference on Software Defined Systems (SDS), Paris, France, 20–23 April 2020; pp. 256–261.
27. Nair, S. *Authentication and Key Management for Applications (AKMA) in 5G*; 3GPP: Valbonne, France, 2022.
28. Vidhani, S.M.; Vidhate, A.V. Security Challenges in 5G Network: A technical features survey and analysis. In Proceedings of the 2022 5th International Conference on Advances in Science and Technology (ICAST), Mumbai, India, 2–3 December 2022; pp. 592–597. [CrossRef]
29. Ji, X.; Huang, K.; Jin, L.; Tang, H.; Liu, C.; Zhong, Z.; You, W.; Xu, X.; Zhao, H.; Wu, J.; et al. Overview of 5G security technology. *Sci. China Inf. Sci.* **2018**, *61*, 081301. [CrossRef]

30. Scott-Hayward, S.; O'Callaghan, G.; Sezer, S. SDN security: A survey. In Proceedings of the 2013 IEEE SDN For Future Networks and Services (SDN4FNS), Trento, Italy, 11–13 November 2013; pp. 1–7.
31. Kloeti, R.; Kotronis, V.; Smith, P. OpenFlow: A Security Analysis. April 2013. In Proceedings of the 2013 21st IEEE International Conference on Network Protocols (ICNP), Goettingen, Germany, 7–10 October 2013.
32. Shin, S.W.; Porras, P.; Yegneswara, V.; Fong, M.; Gu, G.; Tyson, M. Fresco: Modular composable security services for software-defined networks. In Proceedings of the 20th Annual Network & Distributed System Security Symposium, San Diego, CA, USA, 24–27 February 2013.
33. Salahdine, F.; Han, T.; Zhang, N. Security in 5G and beyond recent advances and future challenges. *Secur. Priv.* **2023**, *6*, e271. [CrossRef]
34. Kazmi, S.H.A.; Qamar, F.; Hassan, R.; Nisar, K.; Chowdhry, B.S. Survey on Joint Paradigm of 5G and SDN Emerging Mobile Technologies: Architecture, Security, Challenges and Research Directions. *Wirel. Pers. Commun.* **2023**, *130*, 2753–2800. [CrossRef]
35. Tang, Q.; Ermis, O.; Nguyen, C.D.; Oliveira, A.D.; Hirtzig, A. A Systematic Analysis of 5G Networks with a Focus on 5G Core Security. *IEEE Access* **2022**, *10*, 18298–18319. [CrossRef]
36. Sahni, I.; Kaur, A. A Systematic Literature Review on 5G Security. *arXiv* **2022**, arXiv:2212.03299.
37. Choudhary, G.; Kim, J.; Sharma, V. Security of 5G-mobile backhaul networks: A survey. *arXiv* **2019**, arXiv:1906.11427.
38. Bello, Y.; Hussein, A.R.; Ulema, M.; Koilpillai, J. On Sustained Zero Trust Conceptualization Security for Mobile Core Networks in 5G and Beyond. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 1876–1889. [CrossRef]
39. Hireche, O.; Benzaïd, C.; Taleb, T. Deep data plane programming and AI for zero-trust self-driven networking in beyond 5G. *Comput. Netw.* **2022**, *203*, 108668. [CrossRef]
40. Fang, D.; Qian, Y.; Hu, R.Q. Security Requirement and Standards for 4G and 5G Wireless Systems. *Getmobile Mob. Comp. Comm.* **2018**, *22*, 15–20. [CrossRef]
41. Moreira, C.M.; Kaddoum, G.; Bou-Harb, E. Cross-layer authentication protocol design for ultra-dense 5G HetNets. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–7.
42. Samonas, S.; Coss, D. The CIA strikes back: Redefining confidentiality, integrity and availability in security. *J. Inf. Syst. Secur.* **2014**, *10*.
43. Kornaros, G.; Tomoutzoglou, O.; Coppola, M. Hardware-assisted security in electronic control units: Secure automotive communications by utilizing one-time-programmable network on chip and firewalls. *IEEE Micro* **2018**, *38*, 63–74. [CrossRef]
44. Salazar, Z.; Nguyen, H.N.; Mallouli, W.; Cavalli, A.R.; Montes de Oca, E. 5Greplay: A 5G Network Traffic Fuzzer-Application to Attack Injection. In Proceedings of the 16th International Conference on Availability, Reliability and Security, ARES '21, New York, NY, USA, 17–20 August 2021. [CrossRef]
45. Park, S.; You, I.; Park, H.; Kim, D. Analyzing RRC Replay Attack and Securing Base Station with Practical Method. In Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22, New York, NY, USA, 23–26 August 2022. [CrossRef]
46. Bordel Sánchez, B.; Alcarria Garrido, R.P. Physical Unclonable Functions based on silicon micro-ring resonators for secure signature delegation in Wireless Sensor Networks. *J. Internet Serv. Inf. Secur.* **2018**, *8*, 40–53.
47. Yousef Alshunaifi, S.; Mishra, S.; Alshehri, M. Cyber-Attack Detection and Mitigation Using SVM for 5G Network. *Intell. Autom. Soft Comput.* **2022**, *31*. [CrossRef]
48. Kim, D. *Non-Public Networks (NPN)*; 3GPP: Valbonne, France, 2022.
49. *TS 22.261*; Service Requirements for the 5G System, Release 19, V19.4.0. 3rd Generation Partnership Project: Valbonne, France, 2023.
50. Jerichow, A.; Covell, B.; Chandramouli, D.; Rezaki, A.; Lansisalmi, A.; Merkel, J. 3GPP non-public network security. *J. ICT Stand.* **2020** , 57–76. [CrossRef]
51. Prados-Garzon, J.; Ameigeiras, P.; Ordonez-Lucena, J.; Muñoz, P.; Adamuz-Hinojosa, O.; Camps-Mur, D. 5G non-public networks: Standardization, architectures and challenges. *IEEE Access* **2021**, *9*, 153893–153908. [CrossRef]
52. Trakadas, P.; Sarakis, L.; Giannopoulos, A.; Spantideas, S.; Capsalis, N.; Gkonis, P.; Karkazis, P.; Rigazzi, G.; Antonopoulos, A.; Cambeiro, M.A.; et al. A cost-efficient 5G non-public network architectural approach: Key concepts and enablers, building blocks and potential use cases. *Sensors* **2021**, *21*, 5578. [CrossRef]
53. Andrews, J.G.; Buzzi, S.; Choi, W.; Hanly, S.V.; Lozano, A.; Soong, A.C.; Zhang, J.C. What will 5G be? *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1065–1082. [CrossRef]
54. Ericsson. *Ericsson Mobility Report, Mobile Subscriptions Q2 2023*; Technical report; Ericsson: Stockholm, Sweden, 2023.
55. *TS 23.502*; Technical Specification Group Services and System Aspects; Procedures for the 5G System; Release 18, V18.2.0. 3rd Generation Partnership Project: Valbonne, France, 2023.
56. *TS 23.837*; Location Services (LCS) Architecture for 3GPP System-Wireless Local Area Network (WLAN) Interworking; Release 7. 3rd Generation Partnership Project: Valbonne, France, 2006.
57. *TS 38.300*; NR; NR and NG-RAN Overall Description; Stage-2 Release 17. 3rd Generation Partnership Project: Valbonne, France, 2023.
58. Zhao, D.; Yan, Z.; Wang, M.; Zhang, P.; Song, B. Is 5G Handover Secure and Private? A Survey. *IEEE Internet Things J.* **2021**, *8*, 12855–12879. [CrossRef]

59. Reddy Chavva, A.K.; Rao, V.R.R. Reconfigurable Intelligent Surface (RIS) and Factors Influencing Its Role in Future Networks. Available online: https://research.samsung.com/blog/Reconfigurable-Intelligent-Surface-RIS-and-Factors-Influencing-it-s-Role-in-Future-Networks (accessed on 16 February 2024).
60. Luo, J.; Wang, F.; Wang, S.; Wang, H.; Wang, D. Reconfigurable intelligent surface: Reflection design against passive eavesdropping. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 3350–3364. [CrossRef]
61. Dong, L.; Wang, H.M.; Bai, J. Active Reconfigurable Intelligent Surface Aided Secure Transmission. *IEEE Trans. Veh. Technol.* **2022**, *71*, 2181–2186. [CrossRef]
62. Zhang, J.; Du, H.; Sun, Q.; Ai, B.; Ng, D.W.K. Physical Layer Security Enhancement with Reconfigurable Intelligent Surface-Aided Networks. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3480–3495. [CrossRef]
63. Naeem, F.; Ali, M.; Kaddoum, G.; Huang, C.; Yuen, C. Security and Privacy for Reconfigurable Intelligent Surface in 6G: A Review of Prospective Applications and Challenges. *IEEE Open J. Commun. Soc.* **2023**, *4*, 1196–1217. [CrossRef]
64. Lyu, B.; Hoang, D.T.; Gong, S.; Niyato, D.; Kim, D.I. IRS-based wireless jamming attacks: When jammers can attack without power. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 1663–1667. [CrossRef]
65. Networks, G. OpenRAN (O-ran) for 5G Explained . 2020. Available online: https://www.5g-networks.net/5g-technology/openran-o-ran-for-5g-explained/ (accessed on 27 December 2023).
66. Hanselman, E. Security Benefits of Open Virtualized RAN. 2020. Available online: https://www.cisco.com/c/dam/en/us/solutions/service-provider/pdfs/5g-network-architecture/white-paper-sp-open-vran-security-benefits.pdf (accessed on 27 December 2023).
67. Nokia. 5G Managed Security Survey 2022. 2023. Available online: https://onestore.nokia.com/asset/212741?_ga=2.218954462.611512529.1668533812-1895305122.1668533812 (accessed on 7 February 2024).
68. GSMA. 5G Security Issues. 2019. Available online: https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2019/11/5G-Research_A4.pdf (accessed on 7 February 2024).
69. TrendMicro. Attacks on 5G Infrastructure from User Devices. 2023. Available online: https://www.trendmicro.com/en_us/research/23/i/attacks-on-5g-infrastructure-from-users-devices.html (accessed on 7 February 2024).
70. Lawton, G. Open source security: Opportunity or oxymoron? *Computer* **2002**, *35*, 18–21. [CrossRef]
71. Tung, Y.C.; Liou, E.C.; Cheng, C.H.; Lin, T.H.; Chuang, S.M. Closed-Loop Security Management for Developing O-RAN Infrastructure and B5G RIC Applications. In Proceedings of the 2023 26th International Symposium on Wireless Personal Multimedia Communications (WPMC), Tampa, FL, USA, 19–22 November 2023; pp. 278–281.
72. Zhang, H.; Liu, N.; Chu, X.; Long, K.; Aghvami, A.H.; Leung, V.C.M. Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges. *IEEE Commun. Mag.* **2017**, *55*, 138–145. [CrossRef]
73. Campolo, C.; Molinaro, A.; Iera, A.; Menichella, F. 5G Network Slicing for Vehicle-to-Everything Services. *IEEE Wirel. Commun.* **2017**, *24*, 38–45. [CrossRef]
74. Dangi, R.; Jadhav, A.; Choudhary, G.; Dragoni, N.; Mishra, M.K.; Lalwani, P. ML-Based 5G Network Slicing Security: A Comprehensive Survey. *Future Internet* **2022**, *14*, 116. [CrossRef]
75. Ordonez-Lucena, J.; Ameigeiras, P.; Lopez, D.; Ramos-Munoz, J.J.; Lorca, J.; Folgueira, J. Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges. *IEEE Commun. Mag.* **2017**, *55*, 80–87. [CrossRef]
76. Cano, M. *Technologies*; 3GPP: Valbonne, France, 2023.
77. OAuth. OAuth 2.0, an Industry-Standard Protocol for Authorization, 2023. Available online: https://oauth.net/2/ (accessed on 16 February 2024).
78. Khan, L.U.; Yaqoob, I.; Tran, N.H.; Han, Z.; Hong, C.S. Network Slicing: Recent Advances, Taxonomy, Requirements, and Open Research Challenges. *IEEE Access* **2020**, *8*, 36009–36028. [CrossRef]
79. Adesina, D.; Hsieh, C.C.; Sagduyu, Y.E.; Qian, L. Adversarial machine learning in wireless communications using RF data: A review. *IEEE Commun. Surv. Tutor.* **2022**, *25*, 77–100. [CrossRef]
80. Grønsund, P.; Gonzalez, A.; Mahmood, K.; Nomeland, K.; Pitter, J.; Dimitriadis, A.; Berg, T.K.; Gelardi, S. 5g service and slice implementation for a military use case. In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
81. Osseiran, A.; Boccardi, F.; Braun, V.; Kusume, K.; Marsch, P.; Maternia, M.; Queseth, O.; Schellmann, M.; Schotten, H.; Taoka, H.; et al. Scenarios for 5G mobile and wireless communications: The vision of the METIS project. *IEEE Commun. Mag.* **2014**, *52*, 26–35. [CrossRef]
82. Boccardi, F.; Heath, R.W.; Lozano, A.; Marzetta, T.L.; Popovski, P. Five disruptive technology directions for 5G. *IEEE Commun. Mag.* **2014**, *52*, 74–80. [CrossRef]
83. Wang, C.X.; Haider, F.; Gao, X.; You, X.H.; Yang, Y.; Yuan, D.; Aggoune, H.M.; Haas, H.; Fletcher, S.; Hepsaydir, E. Cellular architecture and key technologies for 5G wireless communication networks. *IEEE Commun. Mag.* **2014**, *52*, 122–130. [CrossRef]
84. Chih-Lin, I.; Rowell, C.; Han, S.; Xu, Z.; Li, G.; Pan, Z. Toward green and soft: A 5G perspective. *IEEE Commun. Mag.* **2014**, *52*, 66–73.
85. Ge, X.; Cheng, H.; Guizani, M.; Han, T. 5G wireless backhaul networks: Challenges and research advances. *IEEE Netw.* **2014**, *28*, 6–11. [CrossRef]
86. Yang, S.; Yin, D.; Song, X.; Dong, X.; Manogaran, G.; Mastorakis, G.; Mavromoustakis, C.X.; Batalla, J.M. Security situation assessment for massive MIMO systems for 5G communications. *Future Gener. Comput. Syst.* **2019**, *98*, 25–34. [CrossRef]

87. Schaefer, R.F.; Amarasuriya, G.; Poor, H.V. Physical layer security in massive MIMO systems. In Proceedings of the 2017 51st Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, 29 October–1 November 2017; pp. 3–8.
88. Kapetanovic, D.; Zheng, G.; Rusek, F. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. *IEEE Commun. Mag.* **2015**, *53*, 21–27. [CrossRef]
89. Xiao, K.; Gong, L.; Kadoch, M. Opportunistic multicast NOMA with security concerns in a 5G massive MIMO system. *IEEE Commun. Mag.* **2018**, *56*, 91–95. [CrossRef]
90. Gao, Y.; Hu, S.; Tang, W.; Li, Y.; Sun, Y.; Huang, D.; Cheng, S.; Li, X. Physical Layer Security in 5G Based Large Scale Social Networks: Opportunities and Challenges. *IEEE Access* **2018**, *6*, 26350–26357. [CrossRef]
91. Ahmed, I.; Khammari, H.; Shahid, A.; Musa, A.; Kim, K.S.; De Poorter, E.; Moerman, I. A Survey on Hybrid Beamforming Techniques in 5G: Architecture and System Model Perspectives. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3060–3097. [CrossRef]
92. Sun, L.; Du, Q. Physical layer security with its applications in 5G networks: A review. *China Commun.* **2017**, *14*, 1–14. [CrossRef]
93. Sun, L.; Du, Q.; Ren, P.; Wang, Y. Two birds with one stone: Towards secure and interference-free D2D transmissions via constellation rotation. *IEEE Trans. Veh. Technol.* **2015**, *65*, 8767–8774. [CrossRef]
94. Du, Q.; Sun, L.; Ren, P.; Wang, Y. Statistical security model and power adaptation over wireless fading channels. In Proceedings of the 2015 International Conference on Wireless Communications & Signal Processing (WCSP), Nanjing, China, 15–17 October 2015; pp. 1–6.
95. Li, W.; Du, Q.; Sun, L.; Ren, P.; Wang, Y. Security enhanced via dynamic fountain code design for wireless delivery. In Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, Doha, Qatar, 3–6 April 2016.
96. MacKay, D.J. Fountain codes. *IEE Proc.-Commun.* **2005**, *152*, 1062–1068. [CrossRef]
97. Seok, B.; Sicato, J.C.S.; Erzhena, T.; Xuan, C.; Pan, Y.; Park, J.H. Secure D2D communication for 5G IoT network based on lightweight cryptography. *Appl. Sci.* **2019**, *10*, 217. [CrossRef]
98. Zhang, A.; Lin, X. Security-aware and privacy-preserving D2D communications in 5G. *IEEE Netw.* **2017**, *31*, 70–77. [CrossRef]
99. Wang, M.; Yan, Z. Security in D2D communications: A review. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Washington, DC, USA, 20–22 August 2015; Volume 1, pp. 1199–1204.
100. Sun, Y.; Cao, J.; Ma, M.; Li, H.; Niu, B.; Li, F. Privacy-preserving device discovery and authentication scheme for D2D communication in 3GPP 5G HetNet. In Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 18–21 February 2019; pp. 425–431.
101. Mars, A.; Abadleh, A.; Adi, W. Operator and manufacturer independent D2D private link for future 5G networks. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 29 April–2 May 2019; pp. 1–6.
102. Howell, G.; Boeckl, K.; Grayson, N.R.; Lefkovitz, N.; Ajmo, J.; Craft, R.E.; McGinnis, M.; Sandlin, K.; Slivina, O.; Snyder, J.; et al. *Mobile Device Security: Bring Your Own Device (BYOD)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023.
103. Kholidy, H.A.; Karam, A.; Sidoran, J.; Rahman, M.A.; Mahmoud, M.; Badr, M.; Mahmud, M.; Sayed, A.F. Toward Zero Trust Security IN 5G Open Architecture Network Slices. In Proceedings of the MILCOM 2022—2022 IEEE Military Communications Conference (MILCOM), Rockville, MD, USA, 28 November–2 December 2022; pp. 577–582. [CrossRef]
104. Manan, A.; Min, Z.; Mahmoudi, C.; Formicola, V. Extending 5G services with Zero Trust security pillars: A modular approach. In Proceedings of the 2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 5–8 December 2022; pp. 1–6. [CrossRef]
105. Li, S.; Iqbal, M.; Saxena, N. Future industry internet of things with zero-trust security. *Inf. Syst. Front.* **2022** , 1–14. [CrossRef]
106. Malik, A.; Parihar, V.; Bhushan, B.; Chaganti, R.; Bhatia, S.; Astya, P.N. Security Services for Wireless 5G Internet of Things (IoT) Systems. In *5G and Beyond*; Bhushan, B., Sharma, S.K., Kumar, R., Priyadarshini, I., Eds.; Springer Nature: Singapore, 2023; pp. 169–195. [CrossRef]
107. Alipour, M.A.; Ghasemshirazi, S.; Shirvani, G. Enabling a Zero Trust Architecture in a 5G-enabled Smart Grid. *arXiv* **2022**, arXiv:2210.01739.
108. Feng, Z.; Zhou, P.; Wang, Q.; Qi, W. A Dual-layer Zero Trust Architecture for 5G Industry MEC Applications Access Control. In Proceedings of the 2022 IEEE 5th International Conference on Electronic Information and Communication Technology (ICEICT), Hefei, China, 21–23 August 2022; pp. 100–105. [CrossRef]
109. Syed, N.F.; Shah, S.W.; Shaghaghi, A.; Anwar, A.; Baig, Z.; Doss, R. Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access* **2022**, *10*, 57143–57179. [CrossRef]
110. He, Y.; Huang, D.; Chen, L.; Ni, Y.; Ma, X. A survey on zero trust architecture: Challenges and future trends. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 6476274. [CrossRef]
111. Buck, C.; Olenberger, C.; Schweizer, A.; Völter, F.; Eymann, T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Comput. Secur.* **2021**, *110*, 102436. [CrossRef]
112. Chen, Z.; Chen, S.; Xu, H.; Hu, B. A Security Authentication Scheme of 5G Ultra-Dense Network Based on Block Chain. *IEEE Access* **2018**, *6*, 55372–55379. [CrossRef]
113. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. *J. Netw. Comput. Appl.* **2020**, *166*, 102693. [CrossRef]

114. Wu, H.; Wolter, K.; Jiao, P.; Deng, Y.; Zhao, Y.; Xu, M. EEDTO: An Energy-Efficient Dynamic Task Offloading Algorithm for Blockchain-Enabled IoT-Edge-Cloud Orchestrated Computing. *IEEE Internet Things J.* **2021**, *8*, 2163–2176. [CrossRef]
115. Xu, Y.; Zhang, H.; Ji, H.; Yang, L.; Li, X.; Leung, V.C.M. Transaction Throughput Optimization for Integrated Blockchain and MEC System in IoT. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 1022–1036. [CrossRef]
116. Chen, Y.; Zhang, N.; Zhang, Y.; Chen, X. Dynamic Computation Offloading in Edge Computing for Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 4242–4251. [CrossRef]
117. Guo, S.; Hu, X.; Guo, S.; Qiu, X.; Qi, F. Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System. *IEEE Trans. Ind. Inform.* **2020**, *16*, 1972–1983. [CrossRef]
118. Yang, H.; Liang, Y.; Yuan, J.; Yao, Q.; Yu, A.; Zhang, J. Distributed Blockchain-Based Trusted Multidomain Collaboration for Mobile Edge Computing in 5G and Beyond. *IEEE Trans. Ind. Inform.* **2020**, *16*, 7094–7104. [CrossRef]
119. Hewa, T.; Gür, G.; Kalla, A.; Ylianttila, M.; Bracken, A.; Liyanage, M. The role of blockchain in 6G: Challenges, opportunities and research directions. In Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 17–20 March 2020; pp. 1–5.
120. Li, W.; Su, Z.; Li, R.; Zhang, K.; Wang, Y. Blockchain-based data security for artificial intelligence applications in 6G networks. *IEEE Netw.* **2020**, *34*, 31–37. [CrossRef]
121. Kim, H.; Park, J.; Bennis, M.; Kim, S.L. Blockchained on-device federated learning. *IEEE Commun. Lett.* **2019**, *24*, 1279–1283. [CrossRef]
122. Aumasson, J.P. The impact of quantum computing on cryptography. *Comput. Fraud. Secur.* **2017**, *2017*, 8–11. [CrossRef]
123. Clancy, T.C.; McGwier, R.W.; Chen, L. Post-Quantum Cryptography and 5G Security: Tutorial. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '19, New York, NY, USA, 15–17 May 2019; p. 285. [CrossRef]
124. Hoffstein, J.; Pipher, J.; Silverman, J.H. NTRU: A ring-based public key cryptosystem. In *International Algorithmic Number Theory Symposium*; Buhler, J.P., Ed.; Springer: Berlin/Heidelberg, Germany, 1998; pp. 267–288.
125. Augot, D.; Batina, L.; Bernstein, D.J.; Bos, J.; Buchmann, J.; Castryck, W.; Dunkelman, O.; Güneysu, T.; Gueron, S.; Hülsing, A.; et al. Initial Recommendations of long-Term Secure Post-Quantum Systems (2015). Available online: https://pqcrypto.eu.org/docs/initial-recommendations.pdf (accessed on 12 August 2023).
126. National Institute of Standards and Technology. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023.
127. Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J.M.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 24–26 April 2018; pp. 353–367.
128. National Institute of Standards and Technology. Module-Lattice-Based Digital Signature Standard. 2023. Available online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.ipd.pdf (accessed on 30 December 2023).
129. Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schwabe, P.; Seiler, G.; Stehlé, D. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2018**, *2018*, 238–268. [CrossRef]
130. National Institute of Standards and Technology. *Stateless Hash-Based Digital Signature Standard*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023.
131. Bernstein, D.J.; Hülsing, A.; Kölbl, S.; Niederhagen, R.; Rijneveld, J.; Schwabe, P. The SPHINCS+ signature framework. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 2129–2146.
132. Preuss Mattsson, J.; Thormarker, E.; Smeets, B. Migration of quantum-resistant algorithms to mobile networks. *Ericsson Blog* **2023**. Available online: https://www.ericsson.com/en/blog/2023/2/quantum-resistant-algorithms-mobile-networks (accessed on 30 December 2023).
133. Porambage, P.; Gür, G.; Osorio, D.P.M.; Liyanage, M.; Gurtov, A.; Ylianttila, M. The roadmap to 6G security and privacy. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1094–1122. [CrossRef]
134. Sajimon, P.; Jain, K.; Krishnan, P. Analysis of post-quantum cryptography for internet of things. In Proceedings of the 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 25–27 May 2022; pp. 387–394.
135. 3GPP. *Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Study on Enhancement for Data Collection for NR and EN-DC (Release 17)*; 3GPP: Valbonne, France, 2022.
136. Alwis, C.D.; Kalla, A.; Pham, Q.V.; Kumar, P.; Dev, K.; Hwang, W.J.; Liyanage, M. Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research. *IEEE Open J. Commun. Soc.* **2021**, *2*, 836–886. [CrossRef]
137. Siriwardhana, Y.; Porambage, P.; Liyanage, M.; Ylianttila, M. AI and 6G Security: Opportunities and Challenges. In Proceedings of the 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 8–11 June 2021; pp. 616–621. [CrossRef]
138. Balasubramanian, B.; Daniels, E.S.; Hiltunen, M.; Jana, R.; Joshi, K.; Sivaraj, R.; Tran, T.X.; Wang, C. RIC: A RAN Intelligent Controller Platform for AI-Enabled Cellular Networks. *IEEE Internet Comput.* **2021**, *25*, 7–17. [CrossRef]
139. Lee, H.; Cha, J.; Kwon, D.; Jeong, M.; Park, I. Hosting AI/ML Workflows on O-RAN RIC Platform. In Proceedings of the 2020 IEEE Globecom Workshops (GC Wkshps), Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [CrossRef]
140. Yang, H.; Alphones, A.; Xiong, Z.; Niyato, D.; Zhao, J.; Wu, K. Artificial-Intelligence-Enabled Intelligent 6G Networks. *IEEE Netw.* **2020**, *34*, 272–280. [CrossRef]

141. Bárcena, J.L.C.; Ducange, P.; Marcelloni, F.; Nardini, G.; Noferi, A.; Renda, A.; Stea, G.; Virdis, A. Towards Trustworthy AI for QoE prediction in B5G/6G Networks. In Proceedings of the First Int'l Workshop on Artificial Intelligence in Beyond 5G and 6G Wireless Networks (AI6G 2022), Padua, Italy, 21 July 2022.
142. Kohli, P.; Sharma, S.; Matta, P. Intrusion Detection Techniques For Security and Privacy of 6G Applications. In Proceedings of the 2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 26–28 May 2023; pp. 560–565. [CrossRef]
143. Saeed, M.M.; Saeed, R.A.; Abdelhaq, M.; Alsaqour, R.; Hasan, M.K.; Mokhtar, R.A. Anomaly detection in 6G networks using machine learning methods. *Electronics* **2023**, *12*, 3300. [CrossRef]
144. Ayub, M.A.; Johnson, W.A.; Talbert, D.A.; Siraj, A. Model Evasion Attack on Intrusion Detection Systems using Adversarial Machine Learning. In Proceedings of the 2020 54th Annual Conference on Information Sciences and Systems (CISS), Princeton, NJ, USA, 18–20 March 2020; pp. 1–6. [CrossRef]
145. Wang, S.; Ko, R.K.L.; Bai, G.; Dong, N.; Choi, T.; Zhang, Y. Evasion Attack and Defense On Machine Learning Models in Cyber-Physical Systems: A Survey. *IEEE Commun. Surv. Tutor.* **2023**, 1–38. [CrossRef]
146. Khowaja, S.A.; Khuwaja, P.; Dev, K.; Antonopoulos, A. Spin: Simulated poisoning and inversion network for federated learning-based 6g vehicular networks. In Proceedings of the ICC 2023-IEEE International Conference on Communications, Rome, Italy, 28 May–1 June 2023; pp. 6205–6210.
147. Renda, A.; Ducange, P.; Gallo, G.; Marcelloni, F. XAI models for quality of experience prediction in wireless networks. In Proceedings of the 2021 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Luxembourg, 11–14 July 2021; pp. 1–6.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.